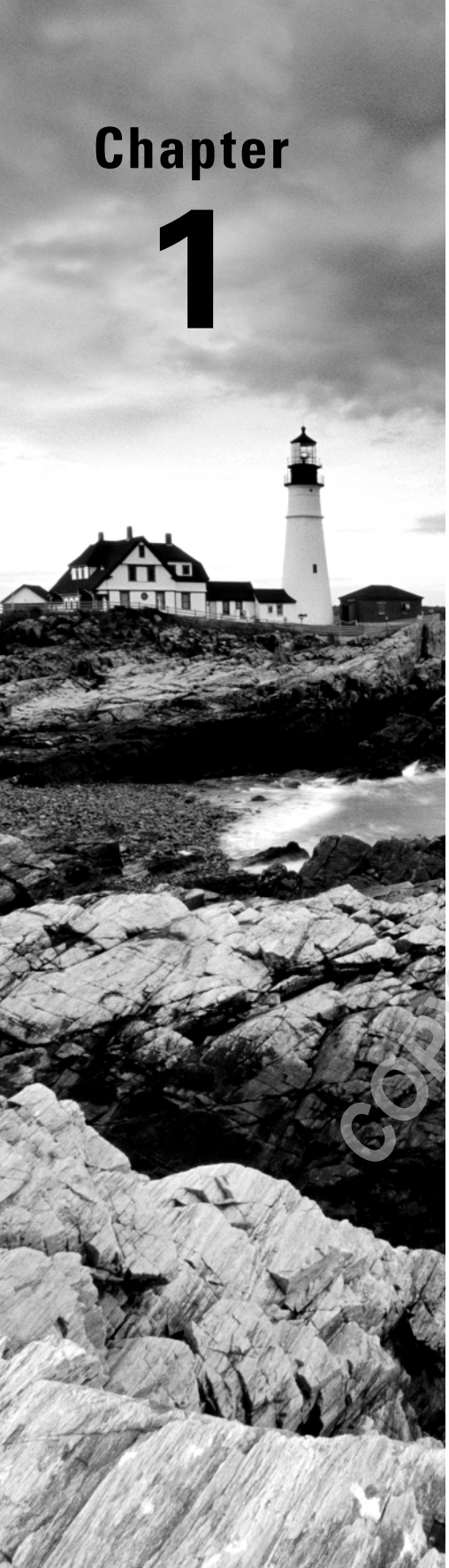

Chapter 1

Threats, Attacks, and Vulnerabilities

THE COMPTIA SECURITY+ EXAM SY0-501 TOPICS COVERED IN THIS CHAPTER INCLUDE THE FOLLOWING:

✓ **1.1 Given a scenario, analyze indicators of compromise and determine the type of malware.**

- Viruses
- Crypto-malware
- Ransomware
- Worm
- Trojan
- Rootkit
- Keylogger
- Adware
- Spyware
- Bots
- RAT
- Logic bomb
- Backdoor

✓ **1.2 Compare and contrast types of attacks.**

- Social engineering
  - Phishing
  - Spear phishing
  - Whaling
  - Vishing
  - Tailgating
  - Impersonation

- Dumpster diving
- Shoulder surfing
- Hoax
- Watering hole attack
- Principles (reasons for effectiveness)
  - Authority
  - Intimidation
  - Consensus
  - Scarcity
  - Familiarity
  - Trust
  - Urgency
- Application/service attacks
  - DoS
  - DDoS
  - Man-in-the-middle
  - Buffer overflow
  - Injection
  - Cross-site scripting
  - Cross-site request forgery
  - Privilege escalation
  - ARP poisoning
  - Amplification
  - DNS poisoning
  - Domain hijacking
  - Man-in-the-browser
  - Zero day
  - Replay
  - Pass the hash
  - Hijacking and related attacks
    - Clickjacking
    - Session hijacking

- URL hijacking
- Typo squatting
- Driver manipulation
- Shimming
- Refactoring
- MAC spoofing
- IP spoofing

- Wireless attacks
- Replay
- IV
- Evil twin
- Rogue AP
- Jamming
- WPS
- Bluejacking
- Bluesnarfing
- RFID
- NFC
- Disassociation

- Cryptographic attacks
- Birthday
- Known plain text/cipher text
- Rainbow tables
- Dictionary
- Brute force
- Online vs. offline
- Collision
- Downgrade
- Replay
- Weak implementations

✓ **1.3 Explain threat actor types and attributes.**

- Types of actors
  - Script kiddies
  - Hacktivist
  - Organized crime
  - Nation states/APT
  - Insiders
  - Competitors
- Attributes of actors
  - Internal/external
  - Level of sophistication
  - Resources/funding
  - Intent/motivation
- Use of open-source intelligence

✓ **1.4 Explain penetration testing concepts.**

- Active reconnaissance
- Passive reconnaissance
- Pivot
- Initial exploitation
- Persistence
- Escalation of privilege
- Black box
- White box
- Gray box
- Pen testing vs. vulnerability scanning

✓ **1.5 Explain vulnerability scanning concepts.**

- Passively test security controls
- Identify vulnerability
- Identify lack of security controls
- Identify common misconfigurations

- Intrusive vs. non-intrusive
- Credentialed vs. non-credentialed
- False positive

✓ **1.6 Explain the impact associated with types of vulnerabilities.**

- Race conditions
- Vulnerabilities due to:
  - End-of-life systems
  - Embedded systems
  - Lack of vendor support
- Improper input handling
- Improper error handling
- Misconfiguration/weak configuration
- Default configuration
- Resource exhaustion
- Untrained users
- Improperly configured accounts
- Vulnerable business processes
- Weak cipher suites and implementations
- Memory/buffer vulnerability
  - Memory leak
  - Integer overflow
  - Buffer overflow
  - Pointer dereference
  - DLL injection
- System sprawl/undocumented assets
- Architecture/design weaknesses
- New threats/zero day
- Improper certificate and key management

1. John is analyzing strange behavior on computers in his network. He believes there is malware on the machines. The symptoms include strange behavior that persists, even if he boots the machine to a Linux Live CD. What is the most likely cause?
   - **A.** Ransomware
   - **B.** Boot sector virus
   - **C.** Rootkit
   - **D.** Key logger

2. Ahmed is a sales manager with a major insurance company. He has received an email that is encouraging him to click on a link and fill out a survey. He is suspicious of the email, but it does mention a major insurance association, and that makes him think it might be legitimate. Which of the following best describes this attack?
   - **A.** Phishing
   - **B.** Social engineering
   - **C.** Spear phishing
   - **D.** Trojan horse

3. You are a security administrator for a medium-sized bank. You have discovered a piece of software on your bank's database server that is not supposed to be there. It appears that the software will begin deleting database files if a specific employee is terminated. What best describes this?
   - **A.** Worm
   - **B.** Logic bomb
   - **C.** Trojan horse
   - **D.** Rootkit

4. You are responsible for incident response at Acme bank. The Acme bank website has been attacked. The attacker used the login screen, but rather than enter login credentials, he or she entered some odd text: `' or '1' = '1`. What is the best description for this attack?
   - **A.** Cross-site scripting
   - **B.** Cross-site request forgery
   - **C.** SQL injection
   - **D.** ARP poisoning

5. Juanita is a network administrator for a small accounting firm. The users on her network are complaining of slow connectivity. When she examines the firewall logs, she observes a large number of half-open connections. What best describes this attack?
   - **A.** DDoS
   - **B.** SYN flood
   - **C.** Buffer overflow
   - **D.** ARP poisoning

6. Frank is deeply concerned about attacks to his company's e-commerce server. He is particularly worried about cross-site scripting and SQL injection. Which of the following would best defend against these two specific attacks?
   - **A.** Encrypted web traffic
   - **B.** Filtering user input
   - **C.** A firewall
   - **D.** An IDS

7. You are responsible for network security at Acme Company. Users have been reporting that personal data is being stolen when using the wireless network. They all insist they only connect to the corporate wireless access point (WAP). However, logs for the WAP show that these users have not connected to it. Which of the following could best explain this situation?
   - **A.** Session hijacking
   - **B.** Clickjacking
   - **C.** Rogue access point
   - **D.** Bluejacking

8. What type of attack depends on the attacker entering JavaScript into a text area that is intended for users to enter text that will be viewed by other users?
   - **A.** SQL injection
   - **B.** Clickjacking
   - **C.** Cross-site scripting
   - **D.** Bluejacking

9. A sales manager at your company is complaining about slow performance on his computer. When you thoroughly investigate the issue, you find spyware on his computer. He insists that the only thing he has downloaded recently was a freeware stock trading application. What would best explain this situation?
   - **A.** Logic bomb
   - **B.** Trojan horse
   - **C.** Rootkit
   - **D.** Macro virus

10. Your company outsourced development of an accounting application to a local programming firm. After three months of using the product, one of your accountants accidently discovers a way to log in and bypass all security and authentication. What best describes this?
    - **A.** Logic bomb
    - **B.** Trojan horse
    - **C.** Backdoor
    - **D.** Rootkit

11. Teresa is the security manager for a mid-sized insurance company. She receives a call from law enforcement, telling her that some computers on her network participated in a massive denial-of-service (DoS) attack. Teresa is certain that none of the employees at her company would be involved in a cybercrime. What would best explain this scenario?

A. It is a result of social engineering.

B. The machines all have backdoors.

C. The machines are bots.

D. The machines are infected with crypto-viruses.

12. Mike is a network administrator with a small financial services company. He has received a popup window that states his files are now encrypted and he must pay .5 bitcoins to get them decrypted. He tries to check the files in question, but their extensions have changed, and he cannot open them. What best describes this situation?

A. Mike's machine has a rootkit.

B. Mike's machine has ransomware.

C. Mike's machine has a logic bomb.

D. Mike's machine has been the target of whaling.

13. Terrance is examining logs for the company e-commerce web server. He discovers a number of redirects that cannot be explained. After carefully examining the website, he finds some attacker performed a watering hole attack by placing JavaScript in the website and is redirecting users to a phishing website. Which of the following techniques would be best at preventing this in the future?

A. An SPI firewall

B. An active IDS/IPS

C. Checking buffer boundaries

D. Checking user input

14. What type of attack is based on sending more data to a target variable than the data can actually hold?

A. Bluesnarfing

B. Buffer overflow

C. Bluejacking

D. DDoS

15. You have been asked to test your company network for security issues. The specific test you are conducting involves primarily using automated and semiautomated tools to look for known vulnerabilities with the various systems on your network. Which of the following best describes this type of test?

A. Vulnerability scan

B. Penetration test

C. Security audit

D. Security test

16. Jared discovers that attackers have breached his WiFi network. They have gained access via the wireless access point (WAP) administrative panel, and have logged on with the credentials the WAP shipped with. What best describes this issue?
    - **A.** Default configuration
    - **B.** Race conditions
    - **C.** Failure to patch
    - **D.** Weak encryption

17. Joanne is concerned about social engineering. She is particularly concerned that this technique could be used by an attacker to obtain information about the network, including possibly even passwords. What countermeasure would be most effective in combating social engineering?
    - **A.** SPI firewall
    - **B.** An IPS
    - **C.** User training
    - **D.** Strong policies

18. You are responsible for incident response at a mid-sized bank. You have discovered that someone was able to successfully breach your network and steal data from your database server. All servers are configured to forward logs to a central logging server. However, when you examine that central log, there are no entries after 2:13 a.m. two days ago. You check the servers, and they are sending logs to the right server, but they are not getting there. Which of the following would be most likely to explain this?
    - **A.** Your log server has a backdoor.
    - **B.** Your log server has been hit with a buffer overflow attack.
    - **C.** Your switches have been hit with ARP poisoning.
    - **D.** Your IDS is malfunctioning and blocking log transmissions.

19. Coleen is the web security administrator for an online auction website. A small number of users are complaining that when they visit the website and log in, they are told the service is down and to try again later. Coleen checks and she can visit the site without any problem, even from computers outside the network. She also checks the web server log and there is no record of those users ever connecting. Which of the following might best explain this?
    - **A.** Typosquatting
    - **B.** SQL injection
    - **C.** Cross-site scripting
    - **D.** Cross-site request forgery

20. Mahmoud is responsible for managing security at a large university. He has just performed a threat analysis for the network, and based on past incidents and studies of similar networks, he has determined that the most prevalent threat to his network is low-skilled attackers who wish to breach the system, simply to prove they can or for

some low-level crime, such as changing a grade. Which term best describes this type of attacker?

A. Hacktivist

B. Amateur

C. Insider

D. Script kiddie

21. Which of the following best describes a collection of computers that have been compromised and are being controlled from one central point?

A. Zombienet

B. Botnet

C. Nullnet

D. Attacknet

22. John is conducting a penetration test of a client's network. He is currently gathering information from sources such as `archive.org`, `netcraft.com`, social media, and information websites. What best describes this stage?

A. Active reconnaissance

B. Passive reconnaissance

C. Initial exploitation

D. Pivot

23. One of the salespeople in your company reports that his computer is behaving sluggishly. You check but don't see any obvious malware. However, in his temp folder you find JPEGs that look like screenshots of his desktop. Which of the following is the most likely cause?

A. He is stealing data from the company.

B. There is a backdoor on his computer.

C. There is spyware on his computer.

D. He needs to update his Windows.

24. What type of attack is based on entering fake entries into a target networks domain name server?

A. DNS poisoning

B. ARP poisoning

C. Bluesnarfing

D. Bluejacking

25. Frank has been asked to conduct a penetration test of a small bookkeeping firm. For the test, he has only been given the company name, the domain name for their website, and the IP address of their gateway router. What best describes this type of test?

A. White-box test

B. External test

C. Black-box test

D. Threat test

26. You work for a security company that performs penetration testing for clients. You are conducting a test of an e-commerce company. You discover that after compromising the web server, you can use the web server to launch a second attack into the company's internal network. What best describes this?

A. Internal attack

B. White-box testing

C. Black-box testing

D. A pivot

27. While investigating a malware outbreak on your company network, you discover something very odd. There is a file that has the same name as a Windows system DLL, and even has the same API interface, but handles input very differently, in a manner to help compromise the system, and it appears that applications have been attaching to this file, rather than the real system DLL. What best describes this?

A. Shimming

B. Trojan horse

C. Backdoor

D. Refactoring

28. Your company has hired a penetration testing firm to test the network. For the test, you have given the company details on operating systems you use, applications you run, and network devices. What best describes this type of test?

A. White-box test

B. External test

C. Black-box test

D. Threat test

29. Frank is a network administrator for a small college. He discovers that several machines on his network are infected with malware. That malware is sending a flood of packets to a target external to the network. What best describes this attack?

A. SYN flood

B. DDoS

C. Botnet

D. Backdoor

30. John is a salesman for an automobile company. He recently downloaded a program from an unknown website, and now his client files have their file extensions changed, and he cannot open them. He has received a popup window that states his files are now encrypted and he must pay .5 bitcoins to get them decrypted. What has happened?

A. His machine has a rootkit.

B. His machine has a logic bomb.

C. His machine has a boot sector virus.

D. His machine has ransomware.

31. When phishing attacks are so focused that they target a specific individual, they are called what?

A. Spear phishing

B. Targeted phishing

C. Phishing

D. Whaling

32. You are concerned about a wide range of attacks that could affect your company's web server. You have recently read about an attack wherein the attacker sends more data to the target than the target is expecting. If done properly, this could cause the target to crash. What would best prevent this type of attack?

A. An SPI firewall

B. An active IDS/IPS

C. Checking buffer boundaries

D. Checking user input

33. You work for a large retail company that processes credit card purchases. You have been asked to test your company network for security issues. The specific test you are conducting involves primarily checking policies, documentation, and past incident reports. Which of the following best describes this type of test?

A. Vulnerability scan

B. Penetration test

C. Security audit

D. Security test

34. Maria is a salesperson with your company. After a recent sales trip, she discovers that many of her logins have been compromised. You carefully scan her laptop and cannot find any sign of any malware. You do notice that she had recently connected to a public WiFi at a coffee shop, and it is only since that connection that she noticed her logins had been compromised. What would most likely explain what has occurred?

A. She connected to a rogue AP.

B. She downloaded a Trojan horse.

C. She downloaded spyware.

D. She is the victim of a buffer overflow attack.

35. You are the manager for network operations at your company. One of the accountants sees you in the hall and thanks you for your team keeping his antivirus software up to date. When you ask him what he means, he mentions that one of your staff, named Mike, called him and remotely connected to update the antivirus. You don't have an employee named Mike. What has occurred?

A. IP spoofing

B. MAC spoofing

C. Man-in-the-middle attack

D. Social engineering

36. You are a security administrator for a bank. You are very interested in detecting any breaches or even attempted breaches of your network, including those from internal personnel. But you don't want false positives to disrupt work. Which of the following devices would be the best choice in this scenario?

A. IPS

B. WAF

C. SIEM

D. IDS

37. One of your users cannot recall the password for their laptop. You want to recover that password for them. You intend to use a tool/technique that is popular with hackers, and it consists of searching tables of precomputed hashes to recover the password. What best describes this?

A. Rainbow table

B. Backdoor

C. Social engineering

D. Dictionary attack

38. You have noticed that when in a crowded area, you sometimes get a stream of unwanted text messages. The messages end when you leave the area. What describes this attack?

A. Bluejacking

B. Bluesnarfing

C. Evil twin

D. Rogue access point

39. Someone has been rummaging through your company's trash bins seeking to find documents, diagrams, or other sensitive information that has been thrown out. What is this called?

A. Dumpster diving

B. Trash diving

C. Social engineering

D. Trash engineering

40. You have noticed that when in a crowded area, data from your cell phone is stolen. Later investigation shows a Bluetooth connection to your phone, one that you cannot explain. What describes this attack?

A. Bluejacking

B. Bluesnarfing

C. Evil twin

D. RAT

41. Louis is investigating a malware incident on one of the computers on his network. He has discovered unknown software that seems to be opening a port, allowing someone to remotely connect to the computer. This software seems to have been installed at the same time as a small shareware application. Which of the following best describes this malware?

A. RAT

B. Backdoor

C. Logic bomb

D. Rootkit

42. This is a common security issue that is extremely hard to control in large environments. It occurs when a user has more computer rights, permissions, and privileges than what is required for the tasks the user needs to perform. What best describes this scenario?

A. Excessive rights

B. Excessive access

C. Excessive permissions

D. Excessive privileges

43. Jared is responsible for network security at his company. He has discovered behavior on one computer that certainly appears to be a virus. He has even identified a file he thinks might be the virus. However, using three separate antivirus programs, he finds that none can detect the file. Which of the following is most likely to be occurring?

A. The computer has a RAT.

B. The computer has a zero-day exploit.

C. The computer has a logic bomb.

D. The computer has a rootkit.

44. There are some computers on your network that use Windows XP. They have to stay on Windows XP due to a specific application they are running. That application won't run on newer operating systems. What security concerns does this situation give you?

A. No special concerns; this is normal.

B. The machines cannot be patched; XP is no longer supported.

C. The machines cannot coordinate with an SIEM since XP won't support that.

D. The machines are more vulnerable to DoS attacks.

45. Farès has discovered that attackers have breached his wireless network. They seem to have used a brute-force attack on the WiFi-protected setup PIN to exploit the WAP and recover the WPA2 password. What is this attack called?

A. Evil twin

B. Rogue WAP

C. IV attack

D. WPS Attack

46. Your wireless network has been breached. It appears the attacker modified a portion of data used with the stream cipher and utilized this to expose wirelessly encrypted data. What is this attack called?

A. Evil twin

B. Rogue WAP

C. IV attack

D. WPS Attack

47. John is concerned about disgruntled employees stealing company documents and exfiltrating them from the network. He is looking for a solution that will detect likely exfiltration and block it. What type of system is John looking for?

A. IPS

B. SIEM

C. Honeypot

D. Firewall

48. Some users on your network use Acme Bank for their personal banking. Those users have all recently been the victim of an attack, wherein they visited a fake Acme Bank website and their logins were compromised. They all visited the bank website from your network, and all of them insist they typed in the correct URL. What is the most likely explanation for this situation?

A. Trojan horse

B. IP spoofing

C. Clickjacking

D. DNS poisoning

49. Users are complaining that they cannot connect to the wireless network. You discover that the WAPs are being subjected to a wireless attack designed to block their WiFi signals. Which of the following is the best label for this attack?

A. IV attack

B. Jamming

C. WPS attack

D. Botnet

50. What type of attack involves users clicking on something different on a website than what they intended to click on?

A. Clickjacking

B. Bluesnarfing

C. Bluejacking

D. Evil twin

51. What type of attack exploits the trust that a website has for an authenticated user to attack that website by spoofing requests from the trusted user?

A. Cross-site scripting

B. Cross-site request forgery

C. Bluejacking

D. Evil twin

52. John is a network administrator for Acme Company. He has discovered that someone has registered a domain name that is spelled just one letter different than his company's domain. The website with the misspelled URL is a phishing site. What best describes this attack?

A. Session hijacking

B. Cross-site request forgery

C. Typosquatting

D. Clickjacking

53. Frank has discovered that someone was able to get information from his smartphone using a Bluetooth connection. The attacker was able to get his contact list and some emails he had received. What is this type of attack called?

A. Bluesnarfing

B. Session hijacking

C. Backdoor attack

D. CSRF

54. Juanita is a network administrator for Acme Company. Some users complain that they keep getting dropped from the network. When Juanita checks the logs for the wireless access point (WAP), she finds that a deauthentication packet has been sent to the WAP from the users' IP addresses. What seems to be happening here?

A. Problem with users' WiFi configuration

B. Disassociation attack

C. Session hijacking

D. Backdoor attack

55. John has discovered that an attacker is trying to get network passwords by using software that attempts a number of passwords from a list of common passwords. What type of attack is this?

A. Dictionary

B. Rainbow table

C. Brute force

D. Session hijacking

56. You are a network security administrator for a bank. You discover that an attacker has exploited a flaw in OpenSSL and forced some connections to move to a weak cipher suite version of TLS, which the attacker could breach. What type of attack was this?

A. Disassociation attack

B. Downgrade attack

C. Session hijacking

D. Brute force

57. When an attacker tries to find an input value that will produce the same hash as a password, what type of attack is this?

A. Rainbow table

B. Brute force

C. Session hijacking

D. Collision attack

58. Farès is the network security administrator for a company that creates advanced routers and switches. He has discovered that his company's networks have been subjected to a series of advanced attacks over a period of time. What best describes this attack?

A. DDoS

B. Brute force

C. APT

D. Disassociation attack

59. You are responsible for incident response at Acme Company. One of your jobs is to attempt to attribute attacks to a specific type of attacker. Which of the following would not be one of the attributes you consider in attributing the attack?

A. Level of sophistication

B. Resources/funding

C. Intent/motivation

D. Amount of data stolen

60. John is running an IDS on his network. Users sometimes report that the IDS flags legitimate traffic as an attack. What describes this?

A. False positive

B. False negative

C. False trigger

D. False flag

61. You are performing a penetration test of your company's network. As part of the test, you will be given a login with minimal access and will attempt to gain administrative access with this account. What is this called?

A. Privilege escalation

B. Session hijacking

C. Root grabbing

D. Climbing

62. Mary has discovered that a web application used by her company does not always handle multithreading properly, particularly when multiple threads access the same variable. This could allow an attacker who discovered this vulnerability to exploit it and crash the server. What type of error has Mary discovered?

A. Buffer overflow

B. Logic bomb

C. Race conditions

D. Improper error handling

63. An attacker is trying to get access to your network. He is sending users on your network a link to a freeware stock-monitoring program. However, that stock-monitoring program has attached to it software that will give the attacker access to any machine that it is installed on. What type of attack is this?

A. Rootkit

B. Trojan horse

C. Spyware

D. Boot sector virus

64. Acme Company uses its own internal certificate server for all internal encryption. However, their certificate authority only publishes a CRL once per week. Does this pose a danger, and if so what?

A. Yes, this means a revoked certificate could be used for up to seven days.

B. No, this is standard for all certificate authorities.

C. Yes, this means it would be easy to fake a certificate.

D. No, since this is being used only internally.

65. When a program has variables, especially arrays, and does not check the boundary values before inputting data, what attack is the program vulnerable to?

A. XSS

B. CRSF

C. Buffer overflow

D. Logic bomb

66. Which of the following best describes malware that will execute some malicious activity when a particular condition is met (i.e., if condition is met, then execute)?

A. Boot sector virus

B. Logic bomb

C. Buffer overflow

D. Sparse infector virus

67. Gerald is a network administrator for Acme Company. Users are reporting odd behavior on their computers. He believes this may be due to malware, but the behavior is different on different computers. What might best explain this?

A. It is not malware, but hardware failure.

B. It is a boot sector virus.

C. It is a macro virus.

D. It is a polymorphic virus.

68. Teresa is a security officer at ACME Inc. She has discovered an attack where the attacker sent multiple broadcast messages to the network routers, spoofing an IP address of one of the network servers. This caused the network to send a flood of packets to that server and it is no longer responding. What is this attack called?

A. Smurf attack

B. DDoS attack

C. TCP hijacking attack

D. TCP SYN flood attack

69. Which type of virus is able to alter its own code to avoid being detected by antivirus software?

A. Boot sector

B. Hoax

C. Polymorphic

D. Stealth

70. Gerald is a network administrator for a small financial services company. Users are reporting odd behavior that appears to be caused by a virus on their machines. After isolating the machines that he believes are infected, Gerald analyzes them. He finds that all the infected machines received an email purporting to be from accounting, with an Excel spreadsheet, and the users opened the spreadsheet. What is the most likely issue on these machines?

A. A macro virus

B. A boot sector virus

C. A Trojan horse

D. A RAT

71. Fred is on the incident response team for a major insurance company. His specialty is malware analysis. He is studying a file that is suspected of being a virus that infected the company network last month. The file seems to intermittently have bursts of malicious activity, interspersed with periods of being dormant. What best describes this malware?

A. A macro virus

B. A logic bomb

C. A sparse infector virus

D. A polymorphic virus

72. What is the term used to describe a virus that can infect both program files and boot sectors?

A. Polymorphic

B. Multipartite

C. Stealth

D. Multiple encrypting

73. Your company has hired an outside security firm to perform various tests of your network. During the vulnerability scan you will provide that company with logins for various systems (i.e., database server, application server, web server, etc.) to aid in their scan. What best describes this?

A. A white-box test

B. A gray-box test

C. A privileged scan

D. An authenticated user scan

74. Which of the following is commonly used in a distributed denial of service (DDoS) attack?

A. Phishing

B. Adware

C. Botnet

D. Trojan

75. You are investigating a recent breach at Acme Company. You discover that the attacker used an old account of someone no longer at the company. The account was still active. Which of the following best describes what caused this vulnerability to exist?

A. Improperly configured accounts

B. Untrained users

C. Using default configuration

D. Failure to patch systems

76. Juan is responsible for incident response at a large financial institution. He discovers that the company WiFi has been breached. The attacker used the same login credentials that ship with the wireless access point (WAP). The attacker was able to use those credentials

to access the WAP administrative console and make changes. Which of the following best describes what caused this vulnerability to exist?

A. Improperly configured accounts

B. Untrained users

C. Using default configuration

D. Failure to patch systems

77. Elizabeth is investigating a network breach at her company. She discovers a program that was able to execute code within the address space of another process by using the target process to load a specific library. What best describes this attack?

A. Logic bomb

B. Session hijacking

C. Buffer overflow

D. DLL injection

78. Zackary is a malware investigator with a cybersecurity firm. He is investigating malware that is able to compromise a target program by finding null references in the target program and dereferencing them, causing an exception to be generated. What best describes this type of attack?

A. DLL injection

B. Buffer overflow

C. Memory leak

D. Pointer dereference

79. Frank has just taken over as CIO of a mid-sized insurance company. One of the first things he does is order a thorough inventory of all network equipment. He discovers two routers that are not documented. He is concerned that if they are not documented, they might not be securely configured, tested, and safe. What best describes this situation?

A. Poor user training

B. System sprawl

C. Failure to patch systems

D. Default configuration

80. What is the primary difference between an intrusive and a nonintrusive vulnerability scan?

A. An intrusive scan is a penetration test.

B. A nonintrusive scan is just a document check.

C. An intrusive scan could potentially disrupt operations.

D. A nonintrusive scan won't find most vulnerabilities.

81. Daryl is investigating a recent breach of his company's web server. The attacker used sophisticated techniques and then defaced the website, leaving messages that were denouncing the company's public policies. He and his team are trying to determine the type of actor who most likely committed the breach. Based on the information provided, who was the most likely threat actor?

A. A script

B. A nation-state

C. Organized crime

D. Hacktivists

82. When investigating breaches and attempting to attribute them to specific threat actors, which of the following is not one of the indicators of an APT?

A. Long-term access to the target

B. Sophisticated attacks

C. The attack comes from a foreign IP address.

D. The attack is sustained over time.

83. What type of attack uses a second wireless access point (WAP) that broadcasts the same SSID as a legitimate access point, in an attempt to get users to connect to the attacker's WAP?

A. Evil twin

B. IP spoofing

C. Trojan horse

D. MAC spoofing

84. You are investigating a breach of a large technical company. You discover that there have been several different attacks over a period of a year. The attacks were sustained, each lasting several weeks of continuous attack. The attacks were somewhat sophisticated and originated from a variety of IP addresses, but all the IP addresses are within your country. Which threat actor would you most suspect of being involved in this attack?

A. Nation-state

B. Hacktivist

C. Script kiddie

D. A lone highly skilled hacker

85. Which of the following best describes a zero-day vulnerability?

A. A vulnerability that has been known to the vendor for zero days

B. A vulnerability that has not yet been breached

C. A vulnerability that can be quickly exploited (i.e., in zero days)

D. A vulnerability that will give the attacker brief access (i.e., zero days)

86. You have discovered that there are entries in your network's domain name server that point legitimate domains to unknown and potentially harmful IP addresses. What best describes this type of attack?

A. A backdoor

B. An APT

C. DNS poisoning

D. A Trojan horse

87. What best describes an attack that attaches some malware to a legitimate program so that when the user installs the legitimate program, they inadvertently install the malware?

A. Backdoor

B. Trojan horse

C. RAT

D. Polymorphic virus

88. Which of the following best describes software that will provide the attacker with remote access to the victim's machine, but that is wrapped with a legitimate program in an attempt to trick the victim into installing it?

A. RAT

B. Backdoor

C. Trojan horse

D. Macro virus

89. Which of the following is an attack that seeks to attack a website, based on the website's trust of an authenticated user?

A. XSS

B. CSRF

C. Buffer overflow

D. RAT

90. John is analyzing what he believes is a malware outbreak on his network. Many users report their machines are behaving strangely. The anomalous behavior seems to occur sporadically and John cannot find a pattern. What is the most likely cause?

A. APT

B. Boot sector virus

C. Sparse infector virus

D. Key logger

91. Farès is the CISO of a bank. He has received an email that is encouraging him to click on a link and fill out a survey. Being security conscious, he normally does not click on links. However, this email calls him by name and claims to be a follow-up to a recent conference he attended. Which of the following best describes this attack?

A. Clickjacking

B. Social engineering

C. Spear phishing

D. Whaling

92. You are responsible for technical support at your company. Users are all complaining of very slow Internet connectivity. When you examine the firewall, you find a large number of incoming connections that are not completed, all packets coming from a single IP address. What best describes this attack?

A. DDoS

B. SYN flood

C. Buffer overflow

D. ARP poisoning

93. An attacker is trying to get malformed queries sent to the backend database to circumvent the web page's security. What type of attack depends on the attacker entering text into text boxes on a web page that is not normal text, but rather odd-looking commands that are designed to be inserted into database queries?

A. SQL injection

B. Clickjacking

C. Cross-site scripting

D. Bluejacking

94. Tyrell is responsible for selecting cryptographic products for his company. The company wants to encrypt the drives of all laptops. The product they have selected uses 128-bit AES encryption for full disk encryption, and users select a password to decrypt the drive. What, if any, would be the major weakness in this system?

A. None; this is a good system.

B. The 128-bit AES key is too short.

C. The passwords users select are the weak link.

D. The AES algorithm is the problem; they should use DES.

95. Valerie is responsible for security testing applications in her company. She has discovered that a web application, under certain conditions, can generate a memory leak. What, type of attack would this leave the application vulnerable to?

A. DoS

B. Backdoor

C. SQL injection

D. Buffer overflow

96. When a multithreaded application does not properly handle various threads accessing a common value, what flaw is this?

A. Memory leak

B. Buffer overflow

C. Integer overflow

D. Race condition

97. Acme Company is using smart cards that use near-field communication (NFC) rather than needing to be swiped. This is meant to make physical access to secure areas more secure. What vulnerability might this also create?

A. Tailgating

B. Eavesdropping

C. IP spoofing

D. Race conditions

98. John is responsible for physical security at a large manufacturing plant. Employees all use a smart card in order to open the front door and enter the facility. Which of the following is a common way attackers would circumvent this system?

A. Phishing

B. Tailgating

C. Spoofing the smart card

D. RFID spoofing

99. Which of the following is the term for an attack wherein malware inserts itself as a library, such as a DLL, between an application and the real system library the application is attempting to communicate with?

A. Application spoofing

B. Jamming

C. Evil twin

D. Shimming

100. You are responsible for incident response at Acme Corporation. You have discovered that someone has been able to circumvent the Windows authentication process for a specific network application. It appears that the attacker took the stored hash of the password and sent it directly to the backend authentication service, bypassing the application. What type of attack is this?

A. Hash spoofing

B. Evil twin

C. Shimming

D. Pass the hash

101. A user in your company reports that she received a call from someone claiming to be from the company technical support team. The caller stated that there was a virus spreading through the company and he needed immediate access to the employee's computer to stop it from being infected. What social-engineering principles did the caller use to try to trick the employee?

A. Urgency and intimidation

B. Urgency and authority

C. Authority and trust

D. Intimidation and authority

102. Ahmed has discovered that someone has manipulated tables in one of the company's switches. The manipulation has changed the tables so that data destined for one specific MAC address will now be routed elsewhere. What type of attack is this?

A. ARP poisoning

B. DNS poisoning

C. Man-in-the-middle

D. Backdoor

103. You are investigating incidents at Acme Corporation and have discovered malware on several machines. It appears that this malware infects system files in the `Windows/System32/` directory and also affects the boot sector. What type of malware is this?

A. Multipartite

B. Boot sector

C. Macro virus

D. Polymorphic virus

104. What type of attack uses Bluetooth to access the data from a cell phone when in range?

A. Phonejacking

B. Bluejacking

C. Bluesnarfing

D. Evil twin

105. An attacker is using a table of precomputed hashes in order to try to get a Windows password. What type of technique is being used?

A. Dictionary

B. Brute force

C. Pass the hash

D. Rainbow table

106. Carlos works in incident response for a mid-sized bank. Users inform him that internal network connections are fine, but connecting to the outside world is very slow. Carlos reviews logs on the external firewall and discovers tens of thousands of ICMP packets coming from a wide range of different IP addresses. What type of attack is occurring?

A. Smurf

B. DoS

C. DDoS

D. SYN flood

107. What type of attack is it when the attacker attempts to get the victim's communication to abandon a high-quality/secure mode in favor of a lower-quality/less secure mode?

A. Downgrade

B. Brute force

C. Rainbow table

D. Bluesnarfing

108. What type of penetration test is being done when the tester is given extensive knowledge of the target network?

A. White-box

B. Full disclosure

C. Black-box

D. Red team

109. Your company is instituting a new security awareness program. You are responsible for educating end users on a variety of threats, including social engineering. Which of the following best defines social engineering?

A. Illegal copying of software

B. Gathering information from discarded manuals and printouts

C. Using people skills to obtain proprietary information

D. Phishing emails

110. Which of the following attacks can be caused by a user being unaware of their physical surroundings?

A. ARP poisoning

B. Phishing

C. Shoulder surfing

D. Smurf attack

111. Francine is a network administrator for Acme Corporation. She has noticed that one of the servers is now unreachable. After carefully reviewing various logs, she discovers that a large number of broadcast packets were sent to the network router, spoofing the server's IP address. What type of attack is this?

A. SYN flood

B. ICMP flood

C. Buffer overflow

D. Smurf attack

112. An attacker enters code into a text box on a website. That text box is used for product reviews. The attacker wants his code to execute the next time a visitor visits that page. What is this attack called?

A. SQL injection

B. Logic bomb

C. Cross-site scripting

D. Session hijacking

113. A user is redirected to a different website when the user requests the DNS record `www.xyz.com`. Which of the following is this an example of?

A. DNS poisoning

B. DoS

C. DNS caching

D. Smurf attack

114. Tom is the network administrator for a small accounting firm. As soon as he comes in to work, users report to him that they cannot connect to the network. After investigating, Tom discovers that none of the workstations can connect to the network and all have an IP address in the form of 169.254.x.x. What has occurred?

A. Smurf attack

B. Man-in-the-middle attack

C. DDoS

D. DHCP starvation

115. Which of the following would most likely use a group of bots to stop a web server from accepting new requests?

A. DoS

B. DDoS

C. Buffer overflow

D. Trojan horse

116. Which of the following would a former employee most likely plant on a server before leaving to cause disruption to the network?

A. Worm

B. Logic bomb

C. Trojan

D. Virus

117. A SYN flood is a DoS attack in which an attacker deliberately violates the three-way handshake and opens a large number of half-open TCP connections. The signature of a SYN flood attack is:

A. The source and destination address having the same value

B. The source and destination port numbers having the same value

C. A large number of SYN packets appearing on a network without the corresponding ACK packets

D. A large number of SYN packets appearing on a network with the corresponding reply RST

118. What does white-box testing mean?

A. The tester has full knowledge of the environment.

B. The tester has no knowledge of the environment.

C. The tester has permission to access the system.

D. The tester has no permission to access the system.

119. Ahmed has been hired to perform a penetration test of Acme Corporation. He begins by looking at IP address ranges owned by the company and details of domain name registration. He also visits social media and newsgroups to see if they contain any sensitive information or have any technical details online. Within the context of penetration-examining methodology, what phase is Ahmed conducting?

A. Passive information gathering

B. Active information gathering

C. Initial exploitation

D. Vulnerability scanning

120. Mary works for a large insurance company, on their cybersecurity team. She is investigating a recent incident and discovers that a server was breached using an authorized user's account. After investigating the incident further, Mary believes that the authorized user logged on, and then someone else took over their session. What best describes this attack?

A. Man-in-the-middle

B. Session hijacking

C. Backdoor

D. Smurf attack

121. Which of the following type of testing utilizes an automated process of proactively identifying vulnerabilities of the computing systems present on a network?

A. Security audit

B. Vulnerability scanning

C. White-box test

D. Black-box test

122. What type of attack is an NFC most susceptible to?

A. Eavesdropping

B. Man-in-the-middle

C. Buffer overflow

D. Smurf attack

123. John has been asked to do a penetration test of a company. He has been given general information but no details about the network. What kind of test is this?

A. Gray-box

B. White-box

C. Partial

D. Masked

124. Under which type of attack does an attacker's system appear to be the server to the real client and appear to be the client to the real server?

A. Denial of service

B. Replay

C. Eavesdropping

D. Man-in-the-middle

125. You are a security administrator for Acme Corporation. You have discovered malware on some of your company's machines. This malware seems to intercept calls from the web browser to libraries, and then manipulates the browser calls. What type of attack is this?

A. Man-in-the-browser

B. Man-in-the-middle

C. Buffer overflow

D. Session hijacking

126. Your company has hired a penetration testing firm to test the company network security. The penetration tester has just been able to achieve guest-level privileges on one low-security system. What best describes this phase of the test?

A. Vulnerability scanning

B. Initial exploit

C. Black-box testing

D. White-box testing

127. What is the primary risk from using outdated software?

A. It may not have all the features you need.

B. It may not have the most modern security features.

C. It may no longer be supported by the vendor.

D. It may be easier to break into than newer software.

128. You are responsible for software testing at Acme Corporation. You want to check all software for bugs that might be used by an attacker to gain entrance into the software or your network. You have discovered a web application that would allow a user to attempt to put a 64-bit value into a 4-byte integer variable. What is this type of flaw?

A. Memory overflow

B. Buffer overflow

C. Variable overflow

D. Integer overflow

129. Which type of virus is most difficult to analyze by reverse engineering?

A. Polymorphic

B. Macro

C. Armored

D. Boot sector

130. What type of attack attempts to deauthorize users from a resource, such as a wireless access point (WAP)?

A. Disassociation

B. Session hijacking

C. Man-in-the-middle

D. Smurf attack

131. John is a network administrator for a large retail chain. He has discovered that his DNS server is being attacked. The attack involves false DNS requests from spoofed IP addresses. The requests are far larger than normal. What type of attack is this?

A. Amplification

B. DNS poisoning

C. DNS spoofing

D. Smurf attack

132. Heidi is a security officer for an investment firm. Many of the employees in her firm travel frequently and access the company intranet from remote locations. Heidi is concerned about users logging in from public WiFi, as well as other people seeing information such as login credentials or customer data. Which of the following is Heidi's most significant concern?

A. Social engineering

B. Shoulder surfing

C. Man-in-the-middle attack

D. CSRF

133. Cross-site scripting is an attack on the _____ that is based on the _____ trusting the _____.

A. user, user, website

B. user, website, user

C. website, website, user

D. user, website, website

134. You are a security officer for a large investment firm. Some of your stock traders handle very valuable accounts with large amounts of money. You are concerned about someone targeting these specific traders to get their login credentials and access account information. Which of the following best describes the attack you are concerned about?

A. Spear phishing

B. Man-in-the-middle

C. Target phishing

D. Vishing

135. You lead an incident response team for a large retail chain store. You have discovered what you believe is spyware on the point-of-sale systems. But the malware in question is encrypted, preventing you from analyzing it. What best describes this?

A. An armored virus

B. Ransomware

C. Polymorphic virus

D. Trojan horse

136. Jared has discovered malware on the workstations of several users. This particular malware provides administrative privileges for the workstation to an external hacker. What best describes this malware?

A. Trojan horse

B. Logic bomb

C. Multipartite virus

D. Rootkit

137. Users in your company report someone has been calling their extension and claiming to be doing a survey for a large vendor. Based on the questions asked in the survey, you suspect that this is a scam to elicit information from your company's employees. What best describes this?

A. Spear phishing

B. Vishing

C. War dialing

D. Robocalling

138. Cross-site request forgery is an attack on the _____ that is based on the _____ trusting the _____.

A. website, website, user

B. user, user website

C. website, user, website

D. user, website, user

139. What type of virus can infect both a file in the operating system and the boot sector?

A. Multipartite

B. Rootkit

C. Ransomware

D. Worm

140. John is analyzing a recent malware infection on his company network. He discovers malware that can spread rapidly and does not require any interaction from the user. What best describes this malware?

A. Worm

B. Virus

C. Logic bomb

D. Trojan horse

141. Your company has issued some new security directives. One of these new directives is that all documents must be shredded before being thrown out. What type of attack is this trying to prevent?

A. Phishing

B. Dumpster diving

C. Shoulder surfing

D. Man-in-the-middle

142. What type of attack embeds malicious code into a document or spreadsheet?

A. Logic bomb

B. Rootkit

C. Trojan horse

D. Macro virus

143. You are a network security analyst for an online retail website. Users report that they have visited your site and had their credit cards stolen. You cannot find any evidence of any breach of your website. You begin to suspect that these users were lured to a fake site. You have found a website that is spelled exactly like your company site, with one letter different. What is this attack called?

A. URL hijacking

B. DNS poisoning

C. Cross-site scripting

D. Man-in-the-middle

144. You have discovered that someone has been trying to log on to your web server. The person has tried a wide range of likely passwords. What type of attack is this?

A. Rainbow table

B. Birthday attack

C. Dictionary attack

D. Spoofing

145. You have just started a new job as a security administrator for Acme Corporation. You discover they have weak authentication protocols. You are concerned that an attacker might simply capture and re-send a user's login credentials. What type of attack is this?

A. Replay attack

B. IP spoofing

C. Login spoofing

D. Session hijacking

146. What is the primary difference between active and passive reconnaissance?

A. Active will be done manually, passive with tools.

B. Active is done with black-box tests and passive with white-box tests.

C. Active is usually done by attackers and passive by testers.

D. Active will actually connect to the network and could be detected; passive won't.

147. What is the primary difference between a vulnerability scan and a penetration test?

A. Vulnerability scans are done by employees and penetration tests by outside teams.

B. Vulnerability scans only use tools; penetration tests are manual.

C. Vulnerability scans just identify issues; penetration tests attempt to exploit them.

D. Vulnerability scans are usually white-box tests; penetration tests are black-box tests.

148. When an attacker breaches one system and uses that as a base to attack a related system, what is this called?

A. Man-in-the-middle

B. Pivot

C. Shimming

D. Vishing

149. Terrance is conducting a penetration test for a client. The client is a major e-commerce company and is primarily concerned about security for their web server. He has just finished running Nmap and OWASP Zap on the target web server. What is this activity called?

A. Passive scanning

B. Black-box testing

C. Active scanning

D. White-box testing

150. You have just taken over as the CISO for a large bank. You are concerned about making sure all systems are secure. One major concern you have is security misconfiguration. Which of the following is not a common security misconfiguration?

A. Unpatched operating system

B. Default accounts with passwords

C. Unneeded services running

D. No firewall running