1. **As a cybersecurity professional, you are responsible for securing a high-traffic web application that uses MySQL as its backend database. Recently, there has been a surge of unauthorized login attempts, and you suspect that a seasoned black-hat hacker is behind them. This hacker has shown proficiency in SQL Injection and appears to be using the 'UNION' SQL keyword to trick the login process into returning additional data. However, your application's security measures include filtering special characters in user inputs, a method usually effective against such attacks. In this challenging environment, if the hacker still intends to exploit this SQL Injection vulnerability, which strategy is he most likely to employ?**

A. The hacker attempts to bypass the special character filter by encoding his malicious input, which could potentially enable him to successfully inject damaging SQL queries
B. The hacker tries to manipulate the 'UNION' keyword in such a way that it triggers a database error, potentially revealing valuable information about the database's structure
C. The hacker alters his approach and injects a 'DROP TABLE' statement, a move that could potentially lead to the loss of vital data stored in the application's database
D. The hacker switches tactics and resorts to a 'time-based blind' SQL Injection attack, which would force the application to delay its response, thereby revealing information based on the duration of the delay

Answer: A

2. **As a security consultant, you are advising a startup that is developing an IoT device for home security. The device communicates with a mobile app, allowing homeowners to monitor their homes in real time. The CEO is concerned about potential Man-in-the-Middle (MitM) attacks that could allow an attacker to intercept and manipulate the device's communication. Which of the following solutions would best protect against such attacks?**

A. Use CAPTCHA on the mobile app's login screen.
B. Implement SSL/TLS encryption for data transmission between the IoT device and the mobile app.
C. Limit the range of the IoT device's wireless signals.
D. Frequently change the IoT device's IP address.

Answer: B

3. **You are a cybersecurity consultant for a global organization. The organization has adopted a Bring Your Own Device (BYOD) policy, but they have recently experienced a phishing incident where an employee's device was compromised. In the investigation, you discovered that the phishing attack occurred through a third-party email app that the employee had installed. Given the need to balance security and user autonomy under the BYOD policy, how should the organization mitigate the risk of such incidents? Moreover, consider a measure that would prevent similar attacks without overly restricting the use of personal devices.**

A. Conduct regular cybersecurity awareness training, focusing on phishing attacks.

B. Provide employees with corporate-owned devices for work-related tasks.
C. Require all employee devices to use a company-provided VPN for internet access.
D. Implement a mobile device management solution that restricts the installation of non-approved applications.

Answer: D

4. **You're the security manager for a tech company that uses a database to store sensitive customer data. You have implemented countermeasures against SQL injection attacks. Recently, you noticed some suspicious activities and suspect an attacker is using SQL injection techniques. The attacker is believed to use different forms of payloads in his SQL queries. In the case of a successful SQL injection attack, which of the following payloads would have the most significant impact?**

A. 'OR username LIKE '%: This payload uses the LIKE operator to search for a specific pattern in a column
B. UNION SELECT NULL, NULL, NULL-: This payload manipulates the UNION SQL operator, enabling the attacker to retrieve data from different database tables
C. 'OR 'a'='a; DROP TABLE members; --: This payload combines the manipulation of the WHERE clause with a destructive action, causing data loss
D. OR '1'='1: This payload manipulates the WHERE clause of an SQL statement, allowing the attacker to view unauthorized data

Answer: C

5. **While working as an intern for a small business, you have been tasked with managing the company's web server. The server is being bombarded with requests, and the company's website is intermittently going offline. You suspect that this could be a Distributed Denial of Service (DDoS) attack. As an ethical hacker, which of the following steps would be your first course of action to mitigate the issue?**

A. Implement IP address whitelisting
B. Install a newer version of the server software
C. Contact your Internet Service Provider (ISP) for assistance
D. Increase the server's bandwidth

Answer: C

6. **While performing a security audit of a web application, an ethical hacker discovers a potential vulnerability. The application responds to logically incorrect queries with detailed error messages that divulge the underlying database's structure. The ethical hacker decides to exploit this vulnerability further. Which type of SQL Injection attack is the ethical hacker likely to use?**

A. Error-based SQL Injection
B. In-band SQL Injection
C. Blind/Inferential SQL Injection

D. UNION SQL Injection

Answer: A

7. **In the process of footprinting a target website, an ethical hacker utilized various tools to gather critical information. The hacker encountered a target site where standard web spiders were ineffective due to a specific file in its root directory. However, they managed to uncover all the files and web pages on the target site, monitoring the resulting incoming and outgoing traffic while browsing the website manually. What technique did the hacker likely employ to achieve this?**

A. Using the Netcraft tool to gather website information
B. User-directed spidering with tools like Burp Suite and WebScarab
C. Using Photon to retrieve archived URLS of the target website from archive.org
D. Examining HTML source code and cookies

Answer: B

8. **In an intricate web application architecture using an Oracle database, you, as a security analyst, have identified a potential SQL Injection attack surface. The database consists of 'x' tables, each with 'y' columns. Each table contains 'z' records. An attacker, well-versed in SQLi techniques, crafts 'u' SQL payloads, each attempting to extract maximum data from the database. The payloads include 'UNION SELECT statements and 'DBMS XSLPROCESSOR.READ2CLOB' to read sensitive files. The attacker aims to maximize the total data extracted 'E=xyz*u'. Assuming 'x=4','y=2', and varying '2' and 'u', which situation is likely to result in the highest extracted data volume?**

A. z=500, u=3: The attacker creates 3 SQL payloads and targets tables with 500 records each, exploiting all columns and tables
B. z=550, u=2: Here, the attacker formulates 2 SQL payloads and directs them towards tables containing 550 records, impacting all columns and tables
C. z=600, u=2: The attacker devises 2 SQL payloads, each aimed at tables holding 600 records, affecting all columns across all tables
D. z=400, u=4: The attacker constructs 4 SQL payloads, each focusing on tables with 400 records, influencing all columns of all tables

Answer: A

9. **As the lead security engineer for a retail corporation, you are assessing the security of the wireless networks in the company's stores. One of your main concerns is the potential for "Wardriving" attacks, where attackers drive around with a Wi-Fi- enabled device to discover vulnerable wireless networks. Given the nature of the retail stores, you need to ensure that any security measures you implement do not interfere with customer experience, such as their ability to access in-store Wi-Fi. Taking into consideration these factors, which of the following would be the most suitable measure to mitigate the risk of Wardriving attacks?**

A. Implement WPA3 encryption for the store's Wi-Fi network
B. Implement MAC address filtering
C. Limit the range of the store's wireless signals
D. Disable SSID broadcasting

Answer: A

10.**You have been hired as an intern at a start-up company. Your first task is to help set up a basic web server for the company's new website. The team leader has asked you to make sure the server is secure from common threats. Based on your knowledge from studying for the CEH exam, which of the following actions should be your priority to secure the web server?**

A. Encrypting the company's website with SSL/TLS
B. Regularly updating and patching the server software
C. Limiting the number of concurrent connections to the server
D. Installing a web application firewall

Answer: B

11. **During a penetration test, an ethical hacker is exploring the security of a complex web application. The application heavily relies on JavaScript for client-side input sanitization, with an apparent assumption that this alone is adequate to prevent injection attacks. During the investigation, the ethical hacker also notices that the application utilizes cookies to manage user sessions but does not enable the HttpOnly flag. This lack of flag potentially exposes the cookies to client-side scripts. Given these identified vulnerabilities, what would be the most effective strategy for the ethical hacker to exploit this application?**

A. Instigate a Distributed Denial of Service (DDoS) attack to overload the server, capitalizing on potential weak server-side security
B. Launch a Cross-Site Scripting (XSS) attack, aiming to bypass the client-side sanitization and exploit the exposure of session cookies
C. Employ a brute-force attack to decipher user credentials, considering the lack of server-side validation
D. Implement an SQL Injection attack to take advantage of potential unvalidated input and gain unauthorized database access

Answer: B

12. **A skilled ethical hacker was assigned to perform a thorough OS discovery on a potential target. They decided to adopt an advanced fingerprinting technique and sent a TCP packet to an open TCP port with specific flags enabled. Upon receiving the**

**reply, they noticed the flags were SYN and ECN-Echo. Which test did the ethical hacker conduct and why was this specific approach adopted?**

A. Test 1: The test was conducted because SYN and ECN-Echo flags enabled to allow the hacker to probe the nature of the response and subsequently determine the OS fingerprint
B. Test 2: This test was chosen because a TCP packet with no flags enabled is known as a NULL packet and this would allow the hacker to assess the OS of the target
C. Test 3: The test was executed to observe the response of the target system when a packet with URG, PSH, SYN, and FIN flags was sent, thereby identifying the OS
D. Test 6: The hacker selected this test because a TCP packet with the ACK flag enabled sent to a closed TCP port would yield more information about the OS

Answer: A

13. **An experienced cyber attacker has created a fake LinkedIn profile, successfully impersonating a high-ranking official from a well-established company, to execute a social engineering attack. The attacker then connected with other employees within the organization, receiving invitations to exclusive corporate events and gaining access to proprietary project details shared within the network. What advanced social engineering technique has the attacker primarily used to exploit the system and what is the most likely immediate threat to the organization?**

A. Pretexting and Network Vulnerability
B. Baiting and Involuntary Data Leakage
C. Spear Phishing and Spam
D. Whaling and Targeted Attacks

Answer: D

**14. As the chief security officer at SecureMobile, you are overseeing the development of a mobile banking application. You are aware of the potential risks of man-in-the- middle (MitM) attacks where an attacker might intercept communication between the app and the bank's servers. Recently, you have learned about a technique used by attackers where they use rogue Wi-Fi hotspots to conduct MitM attacks. To prevent this type of attack, you plan to implement a security feature in the mobile app. What should this feature accomplish?**

A. It should prevent the app from connecting to any unencrypted Wi-Fi networks.
B. It should require two-factor authentication for user logins.
C. It should prevent the app from communicating over a network if it detects a rogue access point.
D. It should require users to change their password every 30 days.

Answer: C

**15. During a penetration testing assignment, a Certified Ethical Hacker (CEH) used a set of scanning tools to create a profile of the target organization. The CEH wanted to scan for live hosts, open ports, and services on a target network. He used Nmap for network inventory and**

**Hping3 for network security auditing. However, he wanted to spoof IP addresses for anonymity during probing. Which command should the CEH use to perform this task?**

A. Hping3-S 192.168.1.1-a 192.168.1.254 -p 22 -flood
B. Hping3 -110.0.0.25 -ICMP
C. Nmap -SS -Pn -n-ww--packet-trace -p--script discovery -T4
D. Hping3 -2 10.0.0.25 -p80

Answer: D

**16. You are a cybersecurity trainee tasked with securing a small home network. The homeowner is concerned about potential "Wi-Fi eavesdropping," where unauthorized individuals could intercept the wireless communications. What would be the most effective first step to mitigate this risk, considering the simplicity and the residential nature of the network?**

A. Enable encryption on the wireless network
B. Reduce the signal strength of the wireless router
C. Enable MAC address filtering
D. Disable the network's SSID broadcast

Answer: A

**17. A large corporate network is being subjected to repeated sniffing attacks. To increase security, the company's IT department decides to implement a combination of several security measures. They permanently add the MAC address of the gateway to the ARP cache, switch to using IPv6 instead of IPv4, implement the use of encrypted sessions such as SSH instead of Telnet, and use Secure File Transfer Protocol instead of FTP. However, they are still faced with the threat of sniffing. Considering the countermeasures, what should be their next step to enhance network security?**

A. Enable network identification broadcasts
B. Use HTTP instead of HTTPS for protecting usernames and passwords
C. Retrieve MAC addresses from the OS
D. Implement network scanning and monitoring tools

Answer: D

18. **An ethical hacker is performing a network scan to evaluate the security of a company's IT infrastructure. During the scan, he discovers an active host with multiple open ports running various services. The hacker uses TCP communication flags to establish a connection with the host and starts communicating with it. He sends a SYN packet to a port on the host and receives a SYN/ACK packet back. He then sends an ACK packet for the received SYN/ACK packet, which triggers an open connection. Which of the following actions should the ethical backer perform next?**

A. Scan another port on the same host using the SYN, ACK, and RST flags
B. Send a PSH packet to inform the receiving application about the buffered data
C. Conduct a vulnerability scan on the open port to identify any potential weaknesses
D. Send a FIN or RST packet to close the connection

Answer: C

19. **A multinational corporation's computer system was infiltrated by an advanced persistent threat (APT). During forensic analysis, it was discovered that the malware was utilizing a blend of two highly sophisticated techniques to stay undetected and continue its operations. Firstly, the malware was embedding its harmful code into the actual binary or executable part of genuine system files rather than appending or prepending itself to the files. This made it exceptionally difficult to detect and eradicate, as doing so risked damaging the system files themselves.**
**Secondly, the malware exhibited characteristics of a type of malware that changes its code as it propagates, making signature-based detection approaches nearly impossible.**
**On top of these, the malware maintained a persistent presence by installing itself in the registry, making it able to survive system reboots.**
**Given these distinctive characteristics, which two types of malware techniques does this malware most closely embody?**

A. Polymorphic and Metamorphic malware
B. Polymorphic and Macro malware
C. Metamorphic and Rootkit malware
D. Macro and Rootkit malware

Answer: A

20. **You are a cybersecurity consultant at SecureloT Inc. A manufacturing company has contracted you to strengthen the security of their Industrial IOT (IoT) devices used in their operational technology (OT)environment. They are concerned about potential attacks that could disrupt their production lines and compromise safety. They have an advanced firewall system in place, but you know this alone is not enough. Which of the following measures should you suggest to provide comprehensive protection for their IIoT devices?**

A. Implement network segmentation to separate HoT devices from the rest of the network.
B. Increase the frequency of changing passwords on all llot devices.
C. Use the same encryption standards for IIoT devices as for IT devices.
D. Rely on the existing firewall and install antivirus software on each IIoT device.

Answer: A

**21. In your cybersecurity class, you are learning about common security risks associated with web servers. One topic that comes up is the risk posed by using default server settings. Why is using default settings on a web server considered a security risk, and what would be the best initial step to mitigate this risk?**

A. Default settings allow unlimited login attempts; setup account lockout
B. Default settings reveal server software type; change these settings
C. Default settings cause server malfunctions; simplify the settings
D. Default settings enable auto-updates; disable and manually patch

Answer: B

22. **Sarah, a system administrator, was alerted of potential malicious activity on the network of her company. She discovered a malicious program spread through the instant messenger application used by her team. The attacker had obtained access to one of her teammate's messenger accounts and started sending files across the contact list. Which best describes the attack scenario and what measure could have prevented it?**

A. Instant Messenger Applications; verifying the sender's identity before opening any files
B. Portable Hardware Medi/Removable Devices; disabling Autorun functionality
C. Rogue/Decoy Applications; ensuring software is labeled as TRUSTED
D. Insecure Patch Management; updating application software regularly

Answer: A

23. **During an attempt to perform an SQL injection attack, a certified ethical hacker is focusing on the identification of database engine type by generating an ODBC error. The ethical hacker, after injecting various payloads, finds that the web application returns a standard, generic error message that does not reveal any detailed database information. Which of the following techniques would the hacker consider next to obtain useful information about the underlying database?**

A. Attempt to compromise the system through OS-level command shell execution
B. Use the UNION operator to combine the result sets of two or more SELECT Statements
C. Utilize a blind injection technique that uses time delays or error signatures to extract information
D. Try to insert a string value where a number is expected in the input field

Answer: C

24. **A certified ethical hacker is conducting a Whois footprinting activity on a specific domain. The individual is leveraging various tools such as Batch IP Converter and Whols Analyzer Pro to retrieve vital details but is unable to gather complete Whois information from the registrar for a particular set of data. As the hacker, what might be the probable data model being utilized by the domain's registrar for storing and looking up Whois information?**

A. Thin Whois model with a malfunctioning server
B. Thin Whois model working correctly
C. Thick Whois model with a malfunctioning server
D. Thick Whois model working correctly

Answer: A

**25. A penetration tester is conducting an assessment of a web application for a financial institution. The application uses form-based authentication and does not implement account lockout policies after multiple failed login attempts. Interestingly, the application displays detailed error messages that disclose whether the username or password entered is incorrect. The tester also notices that the application uses HTTP headers to prevent clickjacking attacks but does not implement Content Security Policy (CSP). With these observations, which of the following attack methods would likely be the most effective for the penetration tester to exploit these vulnerabilities and attempt unauthorized access?**

A. The tester could execute a Man-in-the-Middle (MitM) attack to intercept and modify the HTTP headers for a Clickjacking attack
B. The tester could execute a Brute Force attack, leveraging the lack of account lockout policy and the verbose error messages to guess the correct credentials
C. The tester could launch a Cross-Site Scripting (XSS) attack to steal authenticated session cookies, potentially bypassing the clickjacking protection
D. The tester could exploit a potential SQL Injection vulnerability to manipulate the application's database

Answer: B

26. **A penetration tester was assigned to scan a large network range to find live hosts. The network is known for using strict TCP filtering rules on its firewall, which may obstruct common host discovery techniques. The tester needs a method that can bypass these firewall restrictions and accurately identify live systems. What host discovery technique should the tester use?**

A. ICMP ECHO Ping Scan
B. ICMP Timestamp Ping Scan
C. UDP Ping Scan
D. TCP SYN Ping Scan

Answer: A

27. **As a cybersecurity analyst for a large corporation, you are auditing the company's mobile device management (MDM) policy. One of your areas of concern is data leakage from company-provided smartphones. You are worried about employees unintentionally installing malicious apps that could access sensitive corporate data on their devices. Which of the following would be an effective measure to prevent such data leakage?**

A. Require biometric authentication for unlocking devices.
B. Mandate the use of VPNs when accessing corporate data.
C. Enforce a policy that only allows app installations from approved corporate app stores.
D. Regularly change Wi-Fi passwords used by the devices.

Answer: C

**28. Jason, a certified ethical hacker, is hired by a major e-commerce company to evaluat their network's security. As part of his reconnaissance, Jason is trying to gain as muc information as possible about the company's public-facing servers without arousing suspicion. His goal is to find potential points of entry and map out the network infrastructure for further examination. Which technique should Jason employ to gather this information without alerting the company's intrusion detection systems (IDS)?**

A. Jason should directly connect to each server and attempt to exploit known vulnerabilities
B. Jason should use passive reconnaissance techniques such as WHOIS lookups, NS lookups, and web research
C. Jason should perform a ping sweep to identify all the live hosts in the company's IP range
D. Jason should use a DNS zone transfer to gather information about the company's servers

Answer: B

29. **XYZ company recently discovered a potential vulnerability on their network, originating from misconfigurations. It was found that some of their host servers had enabled debugging functions and unknown users were granted administrative permissions. As a Certified Ethical Hacker, what would be the most potent risk associated with this misconfiguration?**

A. Weak encryption might be allowing man-in-the-middle attacks, leading to data tampering
B. Unauthorized users may perform privilege escalation using unnecessarily created accounts
C. An attacker may carry out a Denial-of-Service assault draining the resources of the server in the process
D. An attacker may be able to inject a malicious DLL into the current running process

Answer: B

30. **A Certified Ethical Hacker is attempting to gather information about a target organization's network structure through network footprinting. During the operation, they encounter ICMP blocking by the target system's firewall. The hacker wants to ascertain the path that packets take to the host system from a source, using an alternative protocol. Which of the following actions should the hacker consider next?**

A. Use the ARIN Whois database search tool to find the network range of the target network
B. Use UDP Traceroute in the Linux operating system by executing the 'traceroute' command with the destination IP or domain name
C. Use the ICMP Traceroute on the Windows operating system as it is the default utility
D. Utilize the Path Analyzer Pro to trace the route from the source to the destination target systems

Answer: B

31. **As a cybersecurity analyst at loT Defend, you are working with a large utility company that uses Industrial Control Systems (ICS) in its operational technology (OT) environment. The company has recently integrated lot devices into this environment to enable remote monitoring and control. They want to ensure these devices do not become a weak link in their security posture. To identify potential vulnerabilities in the lot devices, which of the following actions should you recommend as the first step?**

A. Install the latest antivirus software on each loT device.
B. Conduct a vulnerability assessment specifically for the lot devices.
C. Use stronger encryption algorithms for data transmission between IoT devices.
D. Implement network segmentation to isolate loT devices from the rest of the network.

Answer: B

32. **A malicious user has acquired a Ticket Granting Service from the domain controller using a valid user's Ticket Granting Ticket in a Kerberoasting attack. He exhorted the TGS tickets from memory for offine cracking. But the attacker was stopped before he could complete his attack. The system administrator needs to investigate and remediate the potential breach. What should be the immediate step the system administrator takes?**

A. Change the NTLM password hash used to encrypt the ST
B. Invalidate the TGS the attacker acquired
C. Perform a system reboot to clear the memory
D. Delete the compromised user's account

Answer: B

33. **An ethical hacker is scanning a target network. They initiate a TCP connection by sending an SYN packet to a target machine and receiving a SYN/ACK packet in response. But instead of completing the three-way handshake with an ACK packet, they send an RST packet. What kind of scan is the ethical backer likely performing and what is their goal?**

A. They are performing an SYN scan to stealthily identify open ports without fully establishing a connection

B. They are performing a vulnerability scan to identify any weaknesses in the target system
C. They are performing a TCP connect scan to identify open ports on the target machine
D. They are performing a network scan to identify live hosts and their IP addresses

Answer: A

34. **Your company has been receiving regular alerts from its IDS about potential intrusions. On further investigation, you notice that these alerts have been false positives triggered by certain goodware files. In response, you are planning to enhance the IDS with YARA rules, reducing these false positives while improving the detection of real threats. Based on the scenario and the principles of YARA and IDS, which of the following strategies would best serve your purpose?**

A. Writing YARA rules specifically to identify the goodware files triggering false positives
B. Implementing YARA rules that focus solely on known malware signatures
C. Incorporating YARA rules to detect patterns in all fles regardless of their nature
D. Creating YARA rules to examine only the private database for intrusions

Answer: A

35. **Being a Certified Ethical Hacker (CEH), a company has brought you on board to evaluate the safety measures in place for their network system. The company uses a network time protocol server in the demilitarized zone. During your enumeration, you decide to run a ntptrace command. Given the syntax: ntptrace [-1] [-m maxhosts]servername/IP_address], which command usage would best serve your objective to find where the NTP server obtains the time from and to trace the list of NTP servers connected to the network?**

A. ntptrace 192.168.1.1
B. ntptrace -n -m 5 192.168.1.1
C. ntptrace -m 5 192.168.1.1
D. ntptrace -n localhost

Answer: B

36. **In an advanced persistent threat scenario, an adversary follows a detailed set of procedures in the cyber kill chain. During one such instance, the adversary has successfully gained access to a corporate network and now attempts to obfuscate malicious traffic within legitimate network traffic. Which of the following actions would most likely be part of the adversary's current procedures?**

A. Establishing a command-and-control server to communicate with compromised systems.
B. Initiating DNS tunneling to communicate with the command-and-control server.

C. Conducting internal reconnaissance using PowerShell scripts.
D. Employing data staging techniques to collect and aggregate sensitive data.

Answer: B

37.**John, a security analyst, is analyzing a server suspected of being compromised. The attacker has used a non- admin account and has already gained a foothold on the system. John discovers that a new Dynamic Link Library is loaded in the application directory of the affected server. This DLL does not have a fully qualified path and seems to be malicious. What privilege escalation technique has the attacker likely used to compromise this server?**

A. DLL Hijacking
B. Named Pipe Impersonation
C. Spectre and Meltdown Vulnerabilities
D. Fxnlniting Misconfioured Services

Answer: A

**38. In the process of implementing a network vulnerability assessment strategy for a tech company, the security analyst is confronted with the following scenarios:**
**1) A legacy application is discovered on the network, which no longer receives updates from the vendor.**
**2) Several systems in the network are found running outdated versions of web browsers prone to distributed attacks.**
**3) The network firewall has been configured using default settings and passwords.**
**4) Certain TCP/IP protocols used in the organization are inherently insecure.**
**The security analyst decides to use vulnerability scanning software. Which of the following limitations of vulnerability assessment should the analyst be most cautious about in this context?**

A. Vulnerability scanning software cannot define the impact of an identified vulnerability on different business operations
B. Vulnerability scanning software is not immune to software engineering flaws that might lead to serious vulnerabilities being missed
C. Vulnerability scanning software is limited in its ability to perform live tests on web applications to detect errors or unexpected behavior
D. Vulnerability scanning software is limited in its ability to detect vulnerabilities at a given point in time

Answer: D

39.**As a cybersecurity analyst at TechSafe Inc,, you are working on a project to improve the security of a smart home system. This IoT-enabled system controls various aspects of the home, from heating and lighting to security cameras and door locks. Your client wants to ensure that even if one device is compromised, the rest of the system remains secure. Which of the following strategies would be most effective for this purpose?**

A. Advise using a dedicated network for the smart home system, separate from the

home's main Wi-Fi network.
B. Suggest implementing two-factor authentication for the smart home system's mobile app.
C. Recommend using a strong password for the smart home system's main control panel.
D. Propose frequent system resets to clear any potential malware.

Answer: A

40.**As an IT intern, you have been asked to help set up a secure Wi-Fi network for a local coffee shop. The owners want to provide free Wi-Fi to their customers, but they are concerned about potential security risks. They are looking for a simple yet effective solution that would not require a lot of technical knowledge to manage. Which of the following security measures would be the most suitable in this context?**

A. Enable MAC address filtering
B. Disable the network's SSID broadcast
C. Require customers to use VPN when connected to the Wi-Fi
D. Implement WPA2 or WPA3 encryption

Answer: D

41. **An organization suspects a persistent threat from a cybercriminal. They hire an ethical hacker, John, to evaluate their system security. John identifies several vulnerabilities and advises the organization on preventive measures. However, the organization has limited resources and opts to fix only the most severe vulnerability. Subsequently, a data breach occurs exploiting a different vulnerability. Which of the following statements best describes this scenario?**

A. John is at fault because he did not emphasize the necessity of patching all vulnerabilities.
B. Both the organization and John share responsibility because they did not adequately manage the vulnerabilities.
C. The organization is at fault because it did not fix all identified vulnerabilities.
D. The organization is not at fault because they used their resources as per their understanding.

Answer: B

42. **Recently, the employees of a company have been receiving emails that seem to be from their colleagues, but with suspicious attachments. When opened, these attachments appear to install malware on their systems. The IT department suspects that this is a targeted malware attack. Which of the following measures would be the most effective in preventing such attacks?**

A. Regularly scan systems for any new files and examine them
B. Disabling Autorun functionality on all drives
C. Avoiding the use of outdated web browsers and email software

D. Applying the latest patches and updating software programs

Answer: B

43. **You are the chief cybersecurity officer at CloudSecure Inc, and your team is responsible for securing a cloud- based application that handles sensitive customer data. To ensure that the data is protected from breaches, you have decided to implement encryption for both data-at-rest and data-in-transit. The development team suggests using SSL/TLS for securing data in transit. However, you want to also implement a mechanism to detect if the data was tampered with during transmission. Which of the following should you propose?**

A. Encrypt data using the AES algorithm before transmission.
B. Switch to using SSH for data transmission.
C. Implement IPsec in addition to SSL/TLS.
D. Use the cloud service provider's built-in encryption services.

Answer: C

44. **You are a cybersecurity consultant for a major airport that offers free Wi-Fi to travelers. The management is concerned about the possibility of "Evil Twin" attacks, where a malicious actor sets up a rogue access point that mimics the legitimate one. They are looking for a solution that would not significantly impact the user experience or require travelers to install additional software. What is the most effective security measure you could recommend that fits these constraints, considering the airport's unique operational environment?**

A. Regularly change the SSID of the airport's Wi-Fi network
B. Use MAC address filtering on the airport's Wi-Fi network
C. Implement WPA3 encryption for the airport's Wi-Fi network
D. Display a captive portal page that warns users about the possibility of Evil Twin attacks

Answer: D

45. **As the Chief Information Security Officer (CISO) at a large university, you are responsible for the security of a campus-wide Wi-Fi network that serves thousands of students, faculty, and staff. Recently, there has been a rise in reports of unauthorized network access, and you suspect that some users are sharing their login credentials. You are considering deploying an additional layer of security that could effectively mitigate this issue. What would be the most suitable measure to implement in this context?**

A. Implement network segmentation
B. Deploy a VPN for the entire campus
C. Implement 802.1X authentication
D. Enforce a policy of regularly changing Wi-Fi passwords

Answer: C

46. **You, as a cyber security expert, have been brought in to analyze a potential cryptographic vulnerability in an international banking system. The system uses RSA encryption with key sizes of 'n' bits for securing transaction data. The key generation process involves finding two large primes 'p' and 'q', such that 'n=p*q'. Given 'p=150' and 'q=200', the security level is deemed to be sufficient for current threats. The system can handle a decryption process with a time complexity of O(n^1.5) without compromising performance. However, an attacker using Shor's algorithm on a quantum computer could potentially crack RSA with a time complexity of O(log n) ^3. Assuming 'n=30000' and variables 'p' and 'q', which scenario will likely maximize the decryption time 'T' for the attacker?**

A. p=160, q=240: A modest increase in both 'p' and 'q' results in a larger key size 'n', increasing the complexity for the attacker.
B. p=130, q=230: By decreasing 'p' and increasing 'q', the key size 'n' decreases, reducing the complexity for the attacker.
C. p=175, q=250: The key size 'n' is adjusted by increasing both 'p' and 'q', thereby increasing the complexity of the attacker's decryption process.
D. Op=140, q=210: Here, 'p' decreases while 'q' increases, which could lead to a decrease in 'n', and thus a reduced complexity for the attacker.

Answer: C

47.**A Certified Ethical Hacker (CEH) is given the task to perform an LDAP enumeration on a target system. The system is secured and accepts connections only on secure LDAP. The CEH uses Python for the enumeration process. After successfully installing LDAP and establishing a connection with the target, he attempts to fetch details like the domain name and naming context but is unable to receive the expected response. Considering the circumstances, which of the following is the most plausible reason for this situation?**

A. The Python version installed on the CEH's machine is incompatible with the Idap3 library
B. The enumeration process was blocked by the target system's intrusion detection system
C. The system failed to establish a connection due to an incorrect port number
D. The secure LDAP connection was not properly initialized due to a lack of 'use_ssl : True' in the server object creation

Answer: D

48. **Your company suspects a potential security breach and has hired you as a Certified Ethical Hacker to investigate. You discover evidence of footprinting through search engines and advanced Google hacking techniques. The attacker utilized Google search operators to extract sensitive. You further notice queries that indicate the use of the Google Hacking Database (GHDB) with a notice on VPN footprinting. Which of the following Google advanced search operators would be the LEAST providing the attacker with sensitive VPN-related information?**

A. intitle: This operator restricts results to only the pages containing the specified term in the title
B. link: This operator searches websites or pages that contain links to the specified website or page
C. inurl: This operator restricts the results to only the pages containing the specified word in the URL
D. location: This operator finds information for a specific location

Answer: D

49. **You are a cybersecurity consultant for a smart city project. The project involves deploying a vast network of lot devices for public utilities like traffic control, water supply, and power grid management. The city administration is concerned about the possibility of a Distributed Denial of Service (DDoS) attack crippling these critical services. They have asked you for advice on how to prevent such an attack. What would be your primary recommendation?**
A. Establish strong, unique passwords for each loT device.
B. Implement IP address whitelisting for all loT devices.
C. Implement regular firmware updates for all loT devices.
D. Deploy network intrusion detection systems (IDS) across the loT network.

Answer: D

50. **A large corporation is planning to implement preventive measures to counter a broad range of social engineering techniques. The organization has implemented a signature-based IDS, intrusion detection system, to detect known attack payloads and network flow analysis to monitor data entering and leaving the network. The organization is deliberating on the next step. Considering the information provided about various social engineering techniques, what should be the organization's next course of action?**

A. Set up a honeypot to attract potential attackers into a controlled environment for analysis
B. Implement endpoint detection and response solution to oversee endpoint activities
C. Deploy more security personnel to physically monitor key points of access
D. Organize regular employee awareness training regarding social engineering techniques and preventive measures

Answer: D

51. **As a cybersecurity analyst for SecureNet, you are performing a security assessment of a new mobile payment application. One of your primary concerns is the secure storage of customer data on the device. The application stores sensitive information such as credit card details and**

**personal identification numbers (PINs) on the device. Which of the following measures would best ensure the security of this data?**

A. Implement biometric authentication for app access.
B. Encrypt all sensitive data stored on the device.
C. Enable GPS tracking for all devices using the app.
D. Regularly update the app to the latest version.

Answer: B

52. **As a certified ethical hacker, you are performing a system hacking process for a company that is suspicious about its security system. You found that the company's passwords are all known words, but not in the dictionary. You know that one employee always changes the password by just adding some numbers to the old password. Which attack is most likely to succeed in this scenario?**
A. Rule-based Attack
B. Hybrid Attack
C. Brute-Force Attack
Password Spraying Attack

Answer: B

53.**A penetration tester is tasked with gathering information about the subdomains of a target organization's website. The tester needs a versatile and efficient solution for the task. Which of the following options would be the most effective method to accomplish this goal?**
A. Analyzing LinkedIn profiles to find employees of the target company and their job titles
B. Using a people search service, such as Spokeo or Intelius, to gather information about the employees of the target organization
C. Employing a tool like Sublist3r, which is designed to enumerate the subdomains of websites using OSINT
D. Utilizing the Harvester tool to extract email addresses related to the target domain using a search engine like Google or Bing.

Answer: C

54.**A company recently experienced a debilitating social engineering attack that led to substantial identity theft. An inquiry found that the employee inadvertently provided critical information during an innocuous phone conversation. Considering the specific guidelines issued**

**by the company to thwart social engineering attacks, which countermeasure would have been the most successful in averting the incident?**

A. Conduct comprehensive training sessions for employees on various social engineering methodologies and the risks associated with revealing confidential data.
B. Implement a well-documented change management process for modifications related to hardware or software.
C. Reinforce physical security measures to limit access to sensitive zones within the company premises, thereby warding off unauthorized intruders
D. Adopt a robust software policy that restricts the installation of unauthorized applications.

Answer: A

55. **As part of a college project, you have set up a web server for hosting your team's application. Given your interest in cybersecurity, you have taken the lead in securing the server. You are aware that hackers often attempt to exploit server misconfigurations. Which of the following actions would best protect your web server from potential misconfiguration-based attacks?**

A. Implementing a firewall to filter traffic
B. Enabling multi-factor authentication for users
C. Performing regular server configuration audits
D. Regularly backing up server data

Answer: C

56. **In a recent cyber-attack against a large corporation, an unknown adversary compromised the network and began escalating privileges and lateral movement. The security team identified that the adversary used a sophisticated set of techniques, specifically targeting zero-day vulnerabilities. As a Certified Ethical Hacker (CEH) hired to understand this attack and propose preventive measures, which of the following actions will be most crucial for your initial analysis?**

A. Investigating the data exfiltration methods used by the adversary.
B. Analyzing the initial exploitation methods, the adversary used.
C. Checking the persistence mechanisms used by the adversary in compromised systems.
D. Identifying the specific tools used by the adversary for privilege escalation.

Answer: B

**57. A penetration tester is performing an enumeration on a client's network. The tester has acquired permission to perform enumeration activities. They have identified a remote inter-process communication (IPC) share and are trying to collect more information about it. The**

**tester decides to use a common enumeration technique to collect the desired data. Which of the following techniques would be most appropriate for this scenario?**

A. Extract usernames using email IDs
B. Probe the IPC share by attempting to brute force admin credentials
C. Brute force Active Directory
D. Conduct a DNS zone transfer

Answer: B

**58. You are a cloud security expert at CloudGuard Inc. working with a client who plans to transition their infrastructure to a public cloud. The client expresses concern about potential data breaches and wants to ensure that only authorized personnel can access certain sensitive resources. You propose implementing a Zero Trust security model. Which of the following best describes how the Zero Trust model would enhance the security of their cloud resources?**

A. It ensures secure data transmission by implementing SSL/TLS protocols.
B. It encrypts all data stored in the cloud, ensuring only authorized users can decrypt it.
C. It operates on the principle of least privilege, verifying each request as if it is from an untrusted source, regardless of its location.
D. It uses multi-factor authentication for all user accounts.

Answer: D

**59. You are the chief security officer at AlphaTech, a tech company that specializes in data storage solutions. Your company is developing a new cloud storage platform where users can store their personal files. To ensure data security, the development team is proposing to use symmetric encryption for data at rest. However, they are unsure of how to securely manage and distribute the symmetric keys to users. Which of the following strategies would you recommend to them?**

A. Use HTTPS protocol for secure key transfer.
B. Use digital signatures to encrypt the symmetric keys.
C. Use hash functions to distribute the keys.
D. Implement the Diffie-Hellman protocol for secure key exchange.

Answer: D

**60. A cyber attacker has initiated a series of activities against a high-profile organization following the Cyber Kill Chain Methodology. The attacker is presently in the "Delivery" stage. As an Ethical Hacker, you are trying to anticipate the adversary's next move. What is the most probable subsequent action from the attacker based on the Cyber Kill Chain Methodology?**

A. The attacker will start reconnaissance to gather as much information as possible about the target.

B. The attacker will initiate an active connection to the target system to gather more data.
C. The attacker will exploit the malicious payload delivered to the target organization and establish a foothold.
D. The attacker will attempt to escalate privileges to gain complete control of the compromised system.

Answer: C

61. **As a budding cybersecurity enthusiast, you have set up a small lab at home to learn more about wireless network security. While experimenting with your home Wi-Fi network, you decide to use a well-known hacking tool to capture network traffic and attempt to crack the Wi-Fi password. However, despite many attempts, you have been unsuccessful. Your home Wi-Fi network uses WPA2 Personal with AES encryption. Why are you finding it difficult to crack the Wi-Fi password?**
A. Your hacking tool is outdated
B. The network is using an uncrackable encryption method
C. The Wi-Fi password is too complex and long
D. The network is using MAC address filtering.

Answer: C

62. **An IT company has just implemented new security controls to their network and system setup. As a Certified Ethical Hacker, your responsibility is to assess the possible vulnerabilities in the new setup. You are given the information that the network and system are adequately patched with the latest updates, and all employees have gone through recent cybersecurity awareness training. Considering the potential vulnerability sources, what is the best initial approach to vulnerability assessment?**
A. Evaluating the network for inherent technology weaknesses prone to specific types of attacks
B. Conducting social engineering tests to check if employees can be tricked into revealing sensitive information
C. Investigating if any ex-employees still have access to the company's system and data
D. Checking for hardware and software misconfigurations to identify any possible loopholes

Answer: B

**63. An ethical hacker is attempting to crack NTLM hashed passwords from a Windows SAM file using a rainbow table attack. He has dumped the on-disk contents of the SAM file successfully and noticed that all LM hashes are blank. Given this scenario, which of the following would be the most likely reason for the blank LM hashes?**

A. The Windows system is using the Kerberos authentication protocol as the default method
B. The passwords exceeded 14 characters in length and therefore, the LM hashes were set to a "dummy" value
C. The Windows system is Vista or a later version, where LM hashes are disabled by default

D. The SAM file has been encrypted using the SYSKEY function

Answer: C

64. **A large e-commerce organization is planning to implement a vulnerability assessment solution to enhance its security posture. They require a solution that imitates the outside view of attackers, performs well-organized inference-based testing, scans automatically against continuously updated databases, and supports multiple networks. Given these requirements, which type of vulnerability assessment solution would be most appropriate?**

A. Product-based solution installed on a private network
B. Service-based solution offered by an auditing firm
C. Tree-based assessment approach
D. Inference-based assessment solution

Answer: B

65. **An ethical hacker is testing a web application for possible SQL injection vulnerabilities. He used the input "Bob" for the username and received an error message "Incorrect Syntax near 'Bob'. Unclosed quotation mark after the character string " AND Password='xxx". Based on this information, which type of SQL Injection attack is the ethical hacker most likely trying to perform?**

A. Error-based SOL Injection
B. Blind/Inferential SQL Injection
C. Union SQL Injection
D. Tautology-based SQL Injection

Answer: D

**66. As part of a penetration testing team, you've discovered a web application vulnerable to Cross-Site Scripting (XSS). The application sanitizes inputs against standard XSS payloads but fails to filter out HML-encoded characters. On further analysis, you've noticed that the web application uses cookies to track session IDs. You decide to exploit the XSS vulnerability to steal users' session cookies. However, the application implements HTTPOnly cookies, complicating your original plan. Which of the following would be the most viable strategy for a successful attack?**

A. Utilize an HTML-encoded XSS payload to trigger a buffer overflow attack, forcing the server to reveal the HTTPOnly cookies

B. Create a sophisticated XSS payload that leverages HTML encoding to bypass the input sanitization, and then use it to redirect users to a malicious site where their cookies can be captured
C. Build an XSS payload using HTML encoding and use it to exploit the server-side code, potentially disabling the HTTPOnly flag on cookies
D. Develop a browser exploit to bypass the HTTPOnly restriction, then use a HTML-encoded XSS payload to retrieve the cookies

Answer: B

67. **An organization has been experiencing intrusion attempts despite deploying an Intrusion Detection System (IDS) and Firewalls. As a Certified Ethical Hacker, you are asked to reinforce the intrusion detection process and recommend a better rule-based approach. The IDS uses Snort rules and the new recommended tool should be able to complement it. You suggest using YARA rules with an additional tool for rule generation. Which of the following tools would be the best choice for this purpose and why?**

A. yarGen - Because it generates YARA rules from strings identified in malware files while removing strings that also appear in goodware files
B. YaraRET - Because it helps in reverse engineering Trojans to generate YARA rules
C. Koodous Because it combines social networking with antivirus signatures and YARA rules to detect malware
D. Auto Yara - Because it automates the generation of YARA rules from a set of malicious and benign files

Answer: D

68. **A large enterprise has been experiencing sporadic system crashes and instability, resulting in limited access to its web services. The security team suspects it could be a result of a Denial of Service (DoS) attack. A significant increase in traffic was noticed in the network logs, with patterns suggesting packet sizes exceeding the prescribed size limit. Which among the following DoS attack techniques best describes this scenario?**

A. Pulse wave attack
B. UDP flood attack
C. Ping of Death attack
D. Smurf attack

Answer: D

69. **As a Certified Ethical Hacker, you are conducting a footprinting and reconnaissance operation against a target organization. You discover a range of IP addresses associated with the target using the SecurityTrails tool. Now, you need to perform a reverse DNS lookup on these IP addresses to find the associated domain names, as well as determine the nameservers and mail**

**exchange (MX) records. Which of the following DNSRecon commands would be most effective for this purpose?**

A. dnsrecon -r 10.0.0.0/24 -n ns1.example.com -t zonewalk

B. dnsrecon -r 162.241.216.0/24 -n ns1.example.com -t std

C. dnsrecon -r 192.168.1.0/24 -n nsl.example.com -t axfr

D. dnsrecon -r 162.241.216.0/24 -d example.com -t brt

Answer: B

**70. As a part of an ethical hacking exercise, an attacker is probing a target network that is suspected to employ various honeypot systems for security. The attacker needs to detect and bypass these honeypots without alerting the target. The attacker decides to utilize a suite of techniques. Which of the following techniques would NOT assist in detecting a honeypot?**

A. Implementing a brute force attack to verify system vulnerability

B. Using honeypot detection tools like Send-Safe Honeypot Hunter

C. Probing system services and observing the three-way bandshake

D. Analyzing the MAC address to detect instances running on VMware

Answer: C

71. **You are a security analyst for Cloud Sec, a company providing cloud security solutions. One of your clients, a financial institution, wants to shift its operations to a public cloud while maintaining a high level of security control. They want to ensure that they can monitor all their cloud resources continuously and receive real-time alerts about potential security threats. They also want to enforce their security policies consistently across all cloud workloads. Which of the following solutions would best meet these requirements?**

A. Implement a Virtual Private Network (VPN) for secure data transmission.

B. Deploy a Cloud Access Security Broker (CASB).

C. Use client-side encryption for all stored data.

D. Use multi-factor authentication for all cloud user accounts.

Answer: B

**71. Your network infrastructure is under a SYN flood attack. The attacker has crafted an automated botnet to simultaneously send 's' SYN packets per second to the server. You have put measures in place to manage 'f SYN packets per second, and the system is designed to deal with this number without any performance issues. If's' exceeds 'f, the network infrastructure begins to show signs of overload. The system's response time increases exponentially (2^k), where 'k' represents each additional SYN packet above the 'f limit. Now, considering 's=500' and different 'f values, in which scenario is the server most likely to experience overload and significantly increased response times?**

A. f=505: The server can handle 505 SYN packets per second. In this case, the response time increases but not as drastically (2^5 = 32 times the normal), and the system might still function, albeit slowly
B. f=495: The server can handle 495 SYN packets per second. The response time drastically rises (2^5 = 32 times the normal), indicating a probable system overload
C. f=490: The server can handle 490 SYN packets per second. With 's' exceeding 'f by 10, the response time shoots up (2^10 = 1024 times the usual response time), indicating a system overload
D. f=510: The server can handle 510 SYN packets per second, which is greater than what the attacker is sending. The system stays stable, and the response time remains unaffected

Answer: C

73. **In an advanced digital security scenario, a multinational enterprise is being targeted with a complex series of assaults aimed to disrupt operations, manipulate data integrity, and cause serious financial damage. As the Lead Cybersecurity Analyst with CEH and CISSP certifications, your responsibility is to correctly identify the specific type of attack based on the following indicators:**
**The attacks are exploiting a vulnerability in the target system's hardware, inducing misprediction of future instructions in a program's control flow. The attackers are strategically inducing the victim process to speculatively execute instructions sequences that would not have been executed in the absence of the misprediction, leading to subtle side effects. These side effects, which are observable from the shared state, are then utilized to infer the values of in-flight data.**
**What type of attack best describes this scenario?**

A. Privilege Escalation Attack
B. Rowhammer Attack
C. Side-Channel Attack
D. Watering Hole Attack

Answer: C

74. **In the process of setting up a lab for malware analysis, a cybersecurity analyst is tasked to establish a secure environment using a sheep dip computer. The analyst must prepare the testbed while adhering to best practices. Which of the following steps should the analyst avoid when configuring the environment?**

A. Installing multiple guest operating systems on the virtual machine(s)
B. Installing malware analysis tools on the guest OS
C. Connecting the system to the production network during the malware analysis
D. Simulating Internet services using tools such as INetSim

Answer: C

75. **During a reconnaissance mission, an ethical hacker uses Maltego, a popular footprinting tool, to collect information about a target organization. The information includes the target's Internet infrastructure details (domains, DNS names, Netblocks, IP address information). The hacker decides to use social engineering techniques to gain further information. Which of the following would be the least likely method of social engineering to yield beneficial information based on the data collected?**

A. Dumpster diving in the target company's trash bins for valuable printouts
B. Eavesdropping on internal corporate conversations to understand key topics
C. Shoulder surfing to obser rve sensitive credentials input on the target's computers
D. Impersonating an ISP technical support agent to trick the target into providing further network details

Answer: B

76. **Your company, Secure Tech Inc, is planning to transmit some sensitive data over an unsecured communication channel. As a cyber security expert, you decide to use symmetric key encryption to protect the data. However, you must also ensure the secure exchange of the symmetric key. Which of the following protocols would you recommend to the team to achieve this?**

A. Applying the Diffie-Hellman protocol to exchange the symmetric key.
B. Utilizing SSH for sec cure remote logins to the servers.
C. Implementing SSL certificates on your company's web servers.
D. Switching all data transmission to the HTTPS protocol.

Answer: A

77. **You are a security analyst of a large IT company and are responsible for maintaining the organization's security posture. You are evaluating multiple vulnerability assessment tools for your network. Given that your network has a hybrid IT environment with on-premise and cloud assets, which tool would be most**
**appropriate considering its comprehensive coverage and visibility, continuous scanning, and ability to monitor unexpected changes before they turn into breaches?**

A. OpenVAS
B. Qualys Vulnerability Management
C. Nessus Professional
D. GFI LanGuard

Answer: B

78. **As an IT Security Analyst, you've been asked to review the security measures of an e-commerce website that relies on a SQL database for storing sensitive customer data. Recently, an anonymous tip has alerted you to a possible threat: a seasoned hacker who specializes in SQL Injection attacks may be targeting your system. The site already employs input validation measures to prevent basic injection attacks, and it blocks any user inputs containing suspicious patterns. However, this hacker is known to use advanced SQL Injection techniques. Given this situation, which of the following strategies would the hacker most likely adopt to bypass your security measures?**

A. The hacker may resort to a DDoS attack instead, attempting to crash the server and thus render the e- commerce site unavailable
B. The hacker might employ a 'blind' SQL Injection attack, taking advantage of the application's true or false responses to extract data bit by bit
C. The hacker could deploy an 'out-of-band' SQL Injection attack, extracting data via a different communication channel, such as DNS or HTTP requests
D. The hacker may try to use SQL commands which are less known and less likely to be blocked by your system's security

Answer: B

**79. During a comprehensive security assessment, your cybersecurity team at XYZ Corp stumbles upon signs that point toward a possible Advanced Persistent Threat (APT) infiltration in the network infrastructure. These sophisticated threats often exhibit subtle indicators that distinguish them from other types of cyberattacks. To confirm your suspicion and adequately isolate the potential APT, which of the following actions should you prioritize?**

A. Vigilantly monitor for evidence of zero-day exploits that manage to evade your firewall or antivirus software
B. Scrutinize for repeat network login attempts from unrecognized geographical regions
C. Investigate for anomalies in file movements or unauthorized data access attempts within your database system
D. Search for proof of a spear-phishing attempt, such as the presence of malicious emails or risky attachments

Answer: C

80. **An ethical hacker is hired to evaluate the defenses of an organization's database system which is known to employ a signature-based IDS. The hacker knows that some SQL Injection evasion techniques may allow him to bypass the system's signatures. During the operation, he successfully retrieved a list of usernames from the database without triggering an alarm by employing an advanced evasion technique. Which of the following could he have used?**

A. Using the URL encoding method to replace characters with their ASCII codes in hexadecimal form
B. Utilizing the char encoding function to convert hexadecimal and decimal values into characters that pass-through SQL engine parsing

C. Manipulating white spaces in SQL queries to bypass signature detection
D. Implementing sophisticated matches such as "OR 'john' = 'john"" in place of classical matches like "OR 1=1"

Answer: C

**81.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 SSLv2 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?**
A. Padding oracle attack
B. DROWN attack
C. DUHK attack
D. Side-channel attack

Answer: B

82 .**Clark, 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?**
A. DuckDuckGo
B. AOL
C. ARIN
D. Baidu

Answer: C

83 .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?
A. The -g flag
B. The -A flag
C. The -f flag
D. The -D flag

Answer: D

**84.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?**
A. Application assessment
B. External assessment
C. Passive assessment
D. Host-based assessment

Answer: B

**85.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?**
A. SOX
B. FedRAMP
C. HIPAA
D. PCI DSS

Answer: A

86. **As a cybersecurity consultant for SafePath Corp, you have been tasked with implementing a system for secure email communication. The key requirement is to ensure both confidentiality and non-repudiation. While considering various encryption methods, you are inclined towards using a combination of symmetric and asymmetric cryptography. However, you are unsure which cryptographic technique would best serve the purpose. Which of the following options would you choose to meet these requirements?**

A. Apply asymmetric encryption with RSA and use the private key for signing.
B. Apply asymmetric encryption with RSA and use the public key for encryption.
C. Use symmetric encryption with the AES algorithm.
D. Use the Diffie-Hellman protocol for key exchange and encryption.

Answer: C

87. **A sophisticated attacker targets your web server with the intent to execute a Denial of Service (DoS) attack. His strategy involves a unique mixture of TCP SYN, UDP, and ICMP floods, using 'r' packets per second. Your server, reinforced with advanced security measures, can handle 'h' packets per second before it starts showing signs of strain. If'r' surpasses 'h', it overwhelms the server, causing it to become unresponsive. In a peculiar pattern, the attacker selects 'r' as a composite number and 'h' as a prime number, making the attack detection more challenging.**
**Considering r=2010' and different values for 'h', which of the following scenarios would potentially cause the server to falter?**

A. Oh=1987 (prime): The attacker's packet rate exceeds the server's capacity, causing potential unresponsiveness
B. h=1999 (prime): Despite the attacker's packet flood, the server can handle these requests, remaining responsive
C. h=1993 (prime): Despite being less than 'r', the server's prime number capacity keeps it barely operational, but the risk of falling is imminent
D. h=2003 (prime): The server can manage more packets than the attacker is sending, hence it stays operational

Answer: C

88. **You are a cybersecurity professional managing cryptographic systems for a global corporation. The company uses a mix of Elliptic Curve Cryptography (ECC) for key exchange and symmetric encryption algorithms for data encryption. The time complexity of ECC key pair generation is O(n^3), where 'n' is the size of the key. An advanced threat actor group has a quantum computer that can potentially break ECC with a time complexity of O((log n)^2). Given that the ECC key size is 'n=512' and varying symmetric encryption algorithms and key sizes, which scenario would provide the best balance of security and performance?**

A. Data encryption with 3DES using a 168-bit key: Offers high security but slower performance due to 3DES's inherent inefficiencies.
B. Data encryption with AES-128: Provides moderate security and fast encryption, offering a balance between the two.
C. data encryption with Blowfish using a 448-bit key: Offers high security but potential compatibility issues due to Blowfish's less widespread use.
D. Data encryption with AES-256: Provides high security with better performance than 3DES, but not as fast as other AES key sizes.

Answer: B

**89. A Certified Ethical Hacker (CEH) is analyzing a target network. To do this, he decides to utilize an IDLE/IPID header scan using Nmap. The network analysis reveals that the IPID number increases by 2 after following the steps of an IDLE scan. Based on this information, what can the CEH conclude about the target network?**

A. The target network has no firewall present
B. The ports on the target network are open
C. The target network has a stateful firewall present
D. The ports on the target network are closed

Answer: C

90. **A large organization has recently performed a vulnerability assessment using Nessus Professional, and the security team is now preparing the final report. They have identified a high-risk vulnerability, named XYZ, which could potentially allow unauthorized access to the network. In preparing the report, which of the following**

**elements would NOT be typically included in the detailed documentation for this specific vulnerability?**

A. The CVE ID of the vulnerability and its mapping to the vulnerability's name, XYZ
B. Proof of concept (POC) of the vulnerability, if possible, to demonstrate its potential impact on the system
C. The total number of high, medium, and low-risk vulnerabilities detected throughout the network
D. The list of all affected systems within the organization that are susceptible to the identified vulnerability

Answer: D

**91. You are a cybersecurity consultant for a healthcare organization that utilizes Internet of Medical Things (IoMT) devices, such as connected insulin pumps and heart rate monitors, to provide improved patientcare. Recently, the organization has been targeted by ransomware attacks. While the IT infrastructure was unaffected due to robust security measures, they are worried that the loMT devices could be potential entry points for future attacks. What would be your main recommendation to protect these devices from such threats?**

A. Regularly change the IP addresses of all IOMT devices.
B. Disable all wireless connectivity on loMT devices.
C. Use network segmentation to isolate loMT devices from the main network.
D. Implement multi-factor authentication for all IOMT devices.

Answer: C

92. **During a red team engagement, an ethical hacker is tasked with testing the security measures of an organization's wireless network. The hacker needs to select an appropriate tool to carry out a session hijacking attack. Which of the following tools should the hacker use to effectively perform session hijacking and subsequent security analysis, given that the target wireless network has the Wi-Fi Protected Access-pre- shared key (WPA-PSK) security protocol in place?**

A. bettercap
B. Hetty
C. FaceNiff
D. DroidSheep

Answer: A

93. **In an enterprise network assessment scenario, an ethical hacker is tasked with gathering information about a target organization. The goal is to gain a comprehensive understanding of the network topology, system vulnerabilities, and organizational details. While choosing his approach, he considered Passive and Active Footprinting. Which of the following options would be the most suitable**

**strategy?**

A. Only Active Footprinting, because it involves direct interaction and can provide more detailed information about the target organization

B. Only Passive Footprinting, to avoid any direct interaction and possible detection by the target organization

C. Passive Footprinting first, followed by Active Footprinting, to minimize chances of detection during initial information gathering

D. Active Footprinting first, as it requires more preparation than passive footprinting and may alert the target organization

Answer: C

94. **As a certified ethical hacker, you are tasked with gaining information about an enterprise's internal network. You are permitted to test the network's security using enumeration techniques. You successfully obtain a list of usernames using email IDs and execute a DNS Zone Transfer. Which enumeration technique would be most effective for your next move given that you have identified open TCP ports 25 (SMTP) and 139 (NetBIOS Session Service)?**

A. Exploit the NFS protocol on TCP port 2049 to gain control over a remote system V

B. Use SNMP to extract usernames given the community strings

C. Perform a brute force attack on Microsoft Active Directory to extract valid usernames

D. Exploit the NetBIOS Session Service on TCP port 139 to gain unauthorized access to the file system

Answer: D

95. **An ethical hacker is testing a web application of a financial firm. During the test, a 'Contact Us' form's input field is found to lack proper user input validation, indicating a potential Cross-Site Scripting (XSS) vulnerability. However, the application has a stringent Content Security Policy (CSP) disallowing inline scripts and scripts from external domains but permitting scripts from its own domain. What would be the hacker's next step to confirm the XSS vulnerability?**

A. Inject a benign script inline to the form to see if it executes

B. Utilize a script hosted on the application's domain to test the form

C. Load a scipt from an externa domain to test the vulnerability

D. Try to disable the CSP to bypass script restrictions

Answer: B

**96.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?**

A. Web services parsing attacks

B. WS-Address spoofing

C. SOAPAction spoofing

D. XML injection

Answer: B

**97.Attacker 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 IP address of the target website to that of a fake website.**

What is the technique employed by Steve to gather information for identity theft?

A. Pharming

B. Skimming

C. Pretexting

D. Wardriving

Answer: A

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

A. 22

B. 48101

C. 80

D. 443

Answer: B

**99.Clark is a professional hacker. He 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.**

A. Unspecified proxy activities

B. Use of command-line interface

C. Data staging

D. Use of DNS tunneling

Answer: A

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

A. Packet fragmentation scanning

B. Spoof source address scanning

C. Decoy scanning
D. Idle scanning

Answer: D

101. **A certified ethical hacker is carrying out an email footprinting exercise on a targeted organization using eMailTrackerPro. They want to map out detailed information about the recipient's activities after receiving the email. Which among the following pieces of information would NOT be directly obtained from eMailTrackerPro during this exercise?**

A. Geolocation of the recipient
B. The email accounts related to the domain of the organization
C. Type of device used to open the email
D. The time recipient spent reading the email

Answer: D

102. **An ethical hacker is testing the security of a website's database system against SQL Injection attacks. They discover that the IDS has a strong signature detection mechanism to detect typical SQL injection patterns. Which evasion technique can be most effectively used to bypass the IDS signature detection while performing a SQL Injection attack?**

A. Use Hex encoding to represent the SQL query string
B. Leverage string concatenation to break identifiable keywords
C. Employ IP fragmentation to obscure the attack payload
D. Implement case variation by altering the case of SQL statements

Answer: A

103. **An IT security team is co nducting an internal review of security protocols in their organization to identify potential vulnerabilities. During their investigation, they encounter a suspicious program running on several computers. Further examination reveals that the program has been logging all user keystrokes. How can the security team confirm the type of program and what countermeasures should be taken to ensure the same attack does not occur in the future?**

A. The program is spyware; the team should use password managers and encrypt sensitive
B. The program is a keylogger; the team should educate employees about phishing attacks and maintain regular backups
C. The program is a Trojan; the team should regularly update antivirus software and install a reliable firewall
D. The program is a keylogger; the team should employ intrusion detection systems and regularly update the system software

Answer: D

104. **A multinational organization has recently faced a severe information security breach. Investigations reveal that the attacker had a high degree of understanding of the organization's internal processes and systems. This knowledge was utilized to bypass security controls and corrupt valuable resources. Considering this event, the security team is contemplating the type of attack that occurred and the steps they could have taken to prevent it. Choose the most plausible type of attack and a countermeasure that the organization could have employed:**

A. Active attack and the organization could have used network traffic analysis.
B. Passive attack and the organization should have used encryption techniques.
C. Insider attacks and the organization should have implemented robust access control and monitoring.
D. Distribution attack and the organization could have ensured software and hardware integrity checks.

Answer: C

105. **During your summer internship at a tech company, you have been asked to review the security settings of their web server. While inspecting, you notice the server reveals detailed error messages to users, including database query errors and internal server errors. As a cybersecurity beginner, what is your understanding of this setting, and how would you advise the company?**

A. Increase the frequency of automated server backups
B. Suppress detailed error messages, as they can expose sensitive information
C. Implement stronger encryption to secure the error messages
D. Retain the setting as it aids in troubleshooting user issues

Answer: B

106. **An ethical hacker is hired to conduct a comprehensive network scan of a large organization that strongly suspects potential intrusions into their internal systems. The hacker decides to employ a combination of scanning tools to obtain a detailed understanding of the network. Which sequence of actions would provide the most comprehensive information about the network's status?**

A. Start with Hping3 for a UDP scan on random ports, then use Nmap for a version detection scan, and finally use Metasploit to exploit detected vulnerabilities
B. Use Hping3 for an ICMP ping scan on the entire subnet, then use Nmap for a SYN scan on identified active hosts, and finally use Metasploit to exploit identified vulnerabilities
C. Initiate with Nmap for a ping sweep, then use Metasploit to scan for open ports and services, and finally use Hping3 to perform remote OS fingerprinting
D. Begin with NetScanTools Pro for a general network scan, then use Nmap for OS detection,and version detection, and finally perform an SYN flooding with Hping3

Answer: C

107. **You are an ethical hacker contracted to conduct a security audit for a company. During the audit, you discover that the company's wireless network is using WEP encryption. You understand the vulnerabilities associated with WEP and plan to recommend a more secure encryption method. Which of the following would you recommend as a suitable replacement to enhance the security of the company's wireless network?**

A. WPA2-PSK with AES encryption
B. Open System authentication
C. MAC address filtering
D. SSID broadcast disabling

Answer: A

108. **In a large organization, a network security analyst discovered a series of packet captures that seem unusual. The network operates on a switched Ethernet environment. The security team suspects that an attacker might be using a sniffer tool. Which technique could the attacker be using to successfully carry out this attack, considering the switched nature of the network?**

A. The attacker is probably using a Trojan horse with in-built sniffing capability
B. The attacker might be implementing MAC flooding to overwhelm the switch's memory
C. The attacker might be compromising physical security to plug into the network directly
D. The attacker might be using passive sniffing, as it provides significant stealth advantages

Answer: B

109. **A cybersecurity analyst in an organization is using the Common Vulnerability Scoring System to assess and prioritize identified vulnerabilities in their IT infrastructure. They encountered a vulnerability with a base metric score of 7, a temporal metric score of 8, and an environmental metric score of 5. Which statement best describes this scenario?**

A. The vulnerability has a medium severity with a diminishing likelihood of exploitability over time, but a significant impact in their specific environment
B. The vulnerability has an overall high severity with a diminishing likelihood of exploitability over time, but it is less impactful in their specific environment
C. The vulnerability has a medium severity with a high likelihood of exploitability over time and a Considerable impact in their specific environment
D. The vulnerability has an overall high severity, the likelihood of exploitability is increasing over time, and it has a medium impact in their specific environment

Answer: B

110.**You are a cybersecurity specialist at CloudTech Inc, a company providing cloud-based services. You are managing a project for a client who wants to migrate their sensitive data to a public cloud service. To comply with regulatory requirements, the client insists on maintaining full control over the encryption keys even when the data is at rest on the cloud. Which of the following practices should you implement to meet this requirement?**

A. Use the cloud service provider's encryption services but store keys on-premises.
B. Rely on Secure Sockets Layer (SSL) encryption for data at rest.
C. Use the cloud service provider's default encryption and key management services.
D. Encrypt data client-side before uploading to the cloud and retain control of the encryption keys.

Answer: D

111. **As a cybersecurity consultant, you are working with a client who wants to migrate their data to a Software as a Service (SaaS) cloud environment. They are particularly concerned about maintaining the privacy of their sensitive data, even from the cloud service provider. Which of the following strategies would best ensure the privacy of their data in the SaaS environment?**

A. Implement a Virtual Private Network (VPN) for accessing the SaaS applications.
B. Rely on the cloud service provider's built-in security features.
C. Use multi-factor authentication for all user accounts accessing the SaaS applications.
D. Encrypt the data client-side before uploading to the SaaS environment and manage encryption keys independently.

Answer: D

112. **Given the complexities of an organization's network infrastructure, a threat actor has exploited an unidentified vulnerability, leading to a major data breach. As a Certified Ethical Hacker (CEH), you are tasked with enhancing the organization's security stance. To ensure a comprehensive security defense, you recommend a certain security strategy. Which of the following best represents the strategy you would likely suggest and why?**

A. Adopt a Continual/Adaptive Security Strategy involving ongoing prediction, prevention, detection, and response actions to ensure comprehensive computer network defense.
B. Establish a Defense-in-Depth strategy, incorporating multiple layers of security measures to increase the complexity and decrease the likelihood of a successful attack.
C. Develop an in-depth Risk Management process, involving identification, assessment,

treatment, tracking, and review of risks to control the potential effects on the organization.
D. Implement an Information Assurance (IA) policy focusing on ensuring the integrity, availability, confidentiality, and authenticity of information systems.

Answer: B

113. **Consider a scenario where a Certified Ethical Hacker is attempting to infiltrate a company's network without being detected. The hacker intends to use a stealth scan on a BSD-derived TCP /IP stack, but he suspects that the network security devices may be able to detect SYN packets. Based on this information, which of the following methods should he use to bypass the detection mechanisms and why?**

A. Xmas Scan, because it can pass through filters undetected, depending on the security mechanisms installed
B. ACK Flag Probe Scan, because it exploits the vulnerabilities within the BSD-derived TCP/IP stack
C. Maimon Scan, because it is very similar to NULL, FIN, and Xmas scans, but the probe used here is FIN/ACK
D. TCP Connect/Full-Open Scan, because it completes a three-way handshake with the target machine

Answer: A

114. **You work as a cloud security specialist at SkyNet Solutions. One of your clients is a healthcare organization that plans to migrate its electronic health record (EHR) system to the cloud. This system contains highly sensitive personal and medical data. As part of your job, you need to ensure the security and privacy of this data while it is being transferred and stored in the cloud. You recommend that data should be encrypted during transit and at rest. However, you also need to ensure that even if a cloud service provider(CSP) has access to encrypted data, they should not be able to decrypt it. Which of the following would be the most suitable strategy to meet this requirement?**

A. Use SSL/TLS for data transfer and allow the CSP to manage encryption keys.
B. Use client-side encryption and manage encryption keys independently of the CSP.
C. Utilize the CSP's built-in data encryption services.
D. Rely on network-level encryption protocols for data transfer.

Answer: B

115. **You have been given the responsibility to ensure the security of your school's web server. As a step towards this, you plan to restrict unnecessary services running on the server. In the context of web server security, why is this step considered important?**
A. Unnecessary services eat up server memory; save memory resources

B. Unnecessary services could contain vulnerabilities; minimize the attack surface
C. Unnecessary services reveal server software; hide software details
D. Unnecessary services slow down the server; optimize server speed

Answer: B

116. **During a red team assessment, a CEH is given a task to perform network scanning on the target network without revealing its IP address. They are also required to find an open port and the services available on the target machine. What scanning technique should they employ, and which command in Zenmap should they use?**

A. Use UDP Raw ICMP Port Unreachable Scanning with the command "-SU"
B. Use the IDLE/IPID header scan technique with the command "-sl"
C. Use SCTP INIT Scan with the command "-sy"
D. Use the ACK flag probe scanning technique with the command "-SA"

Answer: D

117. **During an ethical hacking engagement, you have been assigned to evaluate the security of a large organization's network. While examining the network traffic, you notice numerous incoming requests on various ports from different locations that show a pattern of an orchestrated attack. Based on your analysis, you deduce that the requests are likely to be automated scripts being run by unskilled hackers. What type of hacker classification does this scenario most likely represent?**

A. Gray Hats testing system vulnerabilities to help vendors improve security.
B. Black Hats trying to exploit system vulnerabilities for malicious intent.
C. Script Kiddies trying to compromise the system using pre-made scripts.
D. White Hats conducting penetration testing to identify security weaknesses.

Answer: C

118. **Jake, a network security specialist, is trying to prevent network-level session hijacking attacks in his company. While studying different types of such attacks, he learns about a technique where an attacker inserts their machine into the communication between a client and a server, making it seem like the packets are flowing through the original path. This technique is primarily used to reroute the packets. Which of the following types of network-level session hijacking attacks is Jake studying?**

A. Man-in-the-middle Attack Using Forged ICMP and ARP Spoofing
B. RST Hijacking
C. UDP Hijacking
D. TCP/IP Hijacking

Answer: A

119. **An ethical hacker has been tasked with assessing the security of a major corporation's network. She suspects the network uses default SNMP community strings. To exploit this, she plans to extract valuable network information using SNMP enumeration. Which tool could best help her to get the information without directly modifying any parameters within the SNMP agent's management information base (MIB)?**

A. SnmpWalk, with a command to change an OID to a different value
B. snmp-check (snmp-_enum Module) to gather a wide array of information about the target
C. Nmap, with a script to retrieve all running SNMP processes and associated ports
D. OpUtils, are mainly designed for device management and not SNMP enumeration

Answer: B

120. **As a security analyst for Sky Secure Inc, you are working with a client that uses a multi-cloud strategy, utilizing services from several cloud providers. The client wants to implement a system that will provide unified security management across all their cloud platforms. They need a solution that allows them to consistently enforce security policies, identify and respond to threats, and maintain visibility of all their cloud resources. Which of the following should you recommend as the best solution?**

A. Implement separate security management tools for each cloud platform.
B. Rely on the built-in security features of each cloud platform.
C. Use a hardware-based firewall to secure all cloud resources.
D. Use a Cloud Access Security Broker (CASB).

Answer: D

121. **Consider a hypothetical situation where an attacker, known for his proficiency in SQL Injection attacks, is targeting your web server. This adversary meticulously crafts 'q' malicious SQL queries, each inducing a delay of'd' seconds in the server response. This delay in response is an indicator of a potential attack. If the total delay, represented by the product'q*d', crosses a defined threshold 'T', an alert is activated in your security system. Furthermore, it is observed that the attacker prefers prime numbers for 'q', and 'd' follows a pattern in the Fibonacci sequence. Now, consider 'd=13' seconds (a Fibonacci number) and various values of'q' (a prime number) and 'T'. Which among the following scenarios will most likely trigger an alert?**

A. q=17, T=220: Even though the attacker increases 'q', the total delay ('q'd' = 221

seconds) just surpasses the threshold, possibly activating an alert
B. q=19, T=260: Despite the attacker's increased effort, the total delay ('q'd' = 247 seconds) does not exceed the threshold, thus no alert is triggered
C. q=13, T=180: In this case, the total delay caused by the attacker ('q'd' = 169 seconds) breaches the threshold, likely leading to the triggering of a security alert
D. q=11, T=150: Here, the total delay induced by the attacker ('q'd' = 143 seconds) does not surpass the threshold, so the security system remains dormant

Answer: A

122. **You are the lead cybersecurity analyst at a multinational corporation that uses a hybrid encryption system to secure inter-departmental communications. The system uses RSA encryption for key exchange and AES for data encryption, taking advantage of the strengths of both asymmetric and symmetric encryption. Each RSA key pair has a size of 'n' bits, with larger keys providing more security at the cost of slower performance. The time complexity of generating an RSA key pair is 0(n^2), and AES encryption has a time complexity of O(n). An attacker has developed a quantum algorithm with time complexity O((log n)^2) to crack RSA encryption. Given 'n=4000' and variable 'AES key size', which scenario is likely to provide the best balance of security and performance?**

A. AES key size=512 bits: This configuration provides the highest level of security but at a significant performance cost due to the large AES key size.
B. AES key size=256 bits: This configuration provides a high level of security, but RSA key generation may be slow.
C. AES key size=192 bits: This configuration is a balance between options A and B, providing moderate security and performance.
D. AES key size=128 bits: This configuration provides less security than option A, but RSA key generation and AES encryption will be faster.

Answer: C

123. **During a recent vulnerability assessment of a major corporation's IT systems, the security team identified several potential risks. They want to use a vulnerability scoring system to quantify and prioritize these vulnerabilities. They decide to use the Common Vulnerability Scoring System (CVSS). Given the characteristics of the identified vulnerabilities, which of the following statements is the most accurate regarding the metric types used by CVSS to measure these vulnerabilities?**

A. Temporal metric represents the inherent qualities of a vulnerability
B. Base metric represents the inherent qualities of a vulnerability
C. Temporal metric involves measuring vulnerabilities based on a specific environment or implementation
D. Environmental metric involves the features that change during the lifetime of the

vulnerability

Answer: B

124. **A large multinational corporation is in the process of evaluating its security infrastructure to identify potential vulnerabilities. After a comprehensive analysis, they found multiple areas of concern, including time of check/time of use (TOC/TOU) errors, improper input bandling, and poor patch management. Which of the following approaches will best help the organization mitigate the vulnerability associated with TOC/TOU errors?**

A. Regular patching of servers, firmware, operating system, and applications
B. Frequently updating firewall configurations to prevent intrusion attempts
C. Implementing stronger encryption algorithms for all data transfers
D. Ensuring atomicity of operations between checking and using data resources

Answer: D

125. **A security analyst is preparing to analyze a potentially malicious program believed to have infiltrated an organization's network. To ensure the safety and integrity of the production environment, the analyst decided to use a sheep dip computer for the analysis. Before initiating the analysis, what key step should the analyst take?**

A. Install the potentially malicious program on the sheep dip computer
B. Connect the sheep dip computer to the organization's internal network
C. Run the potentially malicious program on the sheep dip computer to determine its behavior
D. Store the potentially malicious program on an external medium, such as a CD-ROM

Answer: D

126. **An ethical hacker is preparing to scan a network to identify live systems. To increase the efficiency and accuracy of his scans, he is considering several different host discovery techniques. He expects several unused IP addresses at any given time, specifically within the private address range of the LAN, but he also anticipates the presence of restrictive firewalls that may conceal active devices. Which scanning method would be most effective in this situation?**

A. ICMP ECHO Ping Sweep
B. ICMP Timestamp Ping
C. ARP Ping Scan
D. TCP SYN Ping

Answer: D

127. **A network security analyst, while conducting penetration testing, is aiming to identify a service account password using the Kerberos authentication protocol. They have a valid user authentication ticket (TGT) and decided to carry out a Kerberoasting attack. In the scenario described, which of the following steps should the analyst take next?**

A. Extract plaintext passwords, hashes, PIN codes, and Kerberos tickets using a tool like Mimikatz
B. Carry out a passive wire sniffing operation using Internet packet sniffers
C. Request a service ticket for the service principal name of the target service account
D. D. Perform a Probability Infinite Chained Elements (PRINCE) attack

Answer: C

128. **You are an ethical hacker tasked with conducting an enumeration of a company's network. Given a Windows system with NetBIOS enabled, port 139 open, and file and printer sharing active, you are about to run some nbtstat commands to enumerate NetBIOS names. The company uses IPv6 for its network. Which of the following actions should you take next?**

A. Switch to an enumeration tool that supports IPv6
B. Utilize Nmap Scripting Engine (NSE) for NetBIOS enumeration
C. Use nbtstat -a followed by the IPv6 address of the target machine
D. Use nbtstat -c to get the contents of the NetBIOS name cache

Answer: A

129. **Your company, Encryptor Corp, is developing a new application that will handle highly sensitive user information. As a cybersecurity specialist, you want to ensure this data is securely stored. The development team proposes a method where data is hashed and then encrypted before storage. However, you want an added layer of security to verify the integrity of the data upon retrieval. Which of the following cryptographic concepts should you propose to the team?**

A. Switch to elliptic curve cryptography.
B. Implement a block cipher mode of operation.
C. Suggest using salt with hashing
D. Apply a digital signature mechanism.

Answer: D

130. **A security analyst is investigating a potential network-level session hijacking incident. During the investigation, the analyst finds that the attacker has been using a technique in which they injected an authentic-looking reset packet using a spoofed source IP address and a guessed acknowledgment number. As a result, the victim's connection was reset. Which of the following hijacking techniques bas the attacker most likely used?**

A. TCP/IP hijacking
B. RST hijacking
C. Blind hijacking
D. UDP hijacking

Answer: B

131. **An audacious attacker is targeting a web server you oversee. He intends to perform a Slow HTTP POST attack, by manipulating 'a' HTTP connection. Each connection sends a byte of data every 'b' second, effectively holding up the connections for an extended period. Your server is designed to manage 'm' connections per second, but any connections exceeding this number tend to overwhelm the system. Given 'a=100' and variable 'm', along with the attacker's intention of maximizing the attack duration**
**'D=a*b', consider the following scenarios. Which is most likely to result in the longest duration of server unavailability?**

A. m=95, b=10: Here, the server can handle 95 connections per second, but it falls short against the attacker's 100 connections, albeit the hold-up time per connection is lower
B. m=110, b=20: Despite the attacker sending 100 connections, the server can handle 110 connections per second, therefore likely staying operative, regardless of the hold-up time per connection
C. m=105, b=12: The server can manage 105 connections per second, more than the attacker's 100 connections, likely maintaining operation despite a moderate hold-up time
D. 90, b=15: The server can manage 90 connections per second, but the attacker's 100 connections exceed this, and with each connection held up for 15 seconds, the attack duration could be significant

Answer: B

132. **Martin, a Certified Ethical Hacker (CEH), is conducting a penetration test on a large enterprise network. He suspects that sensitive information might be leaking out of the network. Martin decides to use network sniffing as part of his testing**
**methodology. Which of the following sniffing techniques should Martin employ to get a comprehensive understanding of the data flowing across the network?**

A. ARP Poisoning
B. Raw Sniffing
C. DNS Poisoning
D. MAC Flooding

Answer: B

133. **A well-resourced attacker intends to launch a highly disruptive DDoS attack against a major online retailer. The attacker aims to exhaust all the network resources while keeping their identity concealed. Their method should be resistant to simple defensive measures such as**

**IP-based blocking. Based on these objectives, which of the following attack strategies would be most effective?**

A. The attacker should instigate a protocol-based SYN flood attack, consuming connection state tables on the retailer's servers
B. The attacker should initiate a volumetric flood attack using a single compromised machine to overwhelm the retailer's network bandwidth
C. The attacker should execute a simple ICMP flood attack from a single IP, exploiting the retailer's ICMP processing
D. The attacker should leverage a botnet to launch a Pulse Wave attack, sending high-volume traffic pulses at regular intervals

Answer: D

134. **A large organization is investigating a possible identity theft case where an attacker has created a new identity by combining multiple pieces of information from different victims to open a new bank account. The attacker also managed to receive government benefits using a fraudulent identity. Given the circumstances, which type of identity theft is the organization dealing with?**

A. Child Identity Theft
B. Identity Cloning and Concealment
C. Social Identity Theft
D. Synthetic Identity Theft

Answer: D

135. **As a junior security analyst for a small business, you are tasked with setting up the company's first wireless network. The company wants to ensure the network is secure from potential attacks. Given that the company's workforce is relatively small and the need for simplicity in managing network security, which of the following measures would you consider a priority to protect the network?**

A. Establish a regular schedule for changing the network password
B. Implement a MAC address whitelist
C. Hide the network SSID
D. Enable WPA2 or WPA3 encryption on the wireless router

Answer: D