Question #201

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. Inference-based assessment solution

B. Tree-based assessment approach

C. Product-based solution installed on a private network

D. Service-based solution offered by an auditing firm

Question #202

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 -1 10.0.0.25 -ICMP

B. Hping3 -2 10.0.0.25-p 80

C. Nmap -sS -Pn -n -vw --packet-trace -p- --script discovery -T4

D. Hping3 -S 192.168.1.1 -a 192.168.1.254 -p 22 --flood

Question #203

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. 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.

B. 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.

C. 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.

D. 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.

Question #204

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. Contact your Internet Service Provider (ISP) for assistance

B. Install a newer version of the server software

C. Implement IP address whitelisting

D. Increase the server's bandwidth

Question #205

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. Encrypt the data client-side before uploading to the SaaS environment and manage encryption keys independently.

D. Use multi-factor authentication for all user accounts accessing the SaaS applications

Question #206

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 hacker perform next?

A. Send a PSH packet to inform the receiving application about the buffered data.

B. Conduct a vulnerability scan on the open port to identify any potential weaknesses.

C. Scan another port on the same host using the SYN, ACK, and RST flags.

D. Send a FIN or RST packet to close the connection.

Question #207

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. Macro and Rootkit malware

D. Metamorphic and Rootkit malware

Question #208

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. Brute-Force Attack

B. Password Spraying Attack

C. Hybrid Attack

D. Rule-based Attack

Question #209

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 has the attacker most likely used?

A. Blind hijacking

B. UDP hijacking

C. RST hijacking

D. TCP/IP hijacking

Question #210

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. Hetty

B. bettercap

C. DroidSheep

D. FaceNiff

Question #211

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

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

C. Use SNMP to extract usernames given the community strings

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

Question #212

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. Use HTTP instead of HTTPS for protecting usernames and passwords

B. Implement network scanning and monitoring tools

C. Enable network identification broadcasts

D. Retrieve MAC addresses from the OS

Question #213

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 require two-factor authentication for user logins.

B. It should prevent the app from communicating over a network if it detects a rogue access point.

C. It should prevent the app from connecting to any unencrypted Wi-Fi networks.

D. It should require users to change their password every 30 days.

Question #214

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 attempt to escalate privileges to gain complete control of the compromised system.

B. The attacker will exploit the malicious payload delivered to the target organization and establish a foothold.

C. The attacker will initiate an active connection to the target system to gather more data.

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

Question #215

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 operates on the principle of least privilege, verifying each request as if it is from an untrusted source, regardless of its location.

B. It encrypts all data stored in the cloud, ensuring only authorized users can decrypt it.

C. It uses multi-factor authentication for all user accounts.

D. It ensures secure data transmission by implementing SSL/TLS protocols.

Question #216

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. Apply a digital signature mechanism.

D. Suggest using salt with hashing.

Question #217

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 HTML-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. Build an XSS payload using HTML encoding and use it to exploit the server-side code, potentially disabling the HTTPOnly flag on cookies.

B. Develop a browser exploit to bypass the HTTPOnly restriction, then use a HTML-encoded XSS payload to retrieve the cookies.

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

D. 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.

Question #218

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. Employ IP fragmentation to obscure the attack payload

B. Implement case variation by altering the case of SQL statements

C. Leverage string concatenation to break identifiable keywords

D. Use Hex encoding to represent the SQL query string

Question #219

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. Limiting the number of concurrent connections to the server

B. Installing a web application firewall

C. Regularly updating and patching the server software

D. Encrypting the company's website with SSL/TLS

Question #220

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. h=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.

Question #221

An IT security team is conducting 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 data.

B. The program is a keylogger; the team should employ intrusion detection systems and regularly update the system software.

C. The program is a keylogger; the team should educate employees about phishing attacks and maintain regular backups.

D. The program is a Trojan; the team should regularly update antivirus software and install a reliable firewall.

Question #222

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 [-n] [-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 -n -m 5192.168.1.1

B. ntptrace -m 5192.168.1.1

C. ntptrace -n localhost

D. ntptrace 192.168.1.1

Question #223

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 UDP Traceroute in the Linux operating system by executing the 'traceroute' command with the destination IP or domain name.

B. Use the ICMP Traceroute on the Windows operating system as it is the default utility.

C. Use the ARIN Whois database search tool to find the network range of the target network.

D. Utilize the Path Analyzer Pro to trace the route from the source to the destination target systems.

Question #224

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. TCP SYN Ping

D. ARP Ping Scan

Question #225

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. Employing a tool like Sublist3r, which is designed to enumerate the subdomains of websites using OSINT

C. Using a people search service, such as Spokeo or Intelius, to gather information about the employees of the target organization

D. Utilizing the Harvester tool to extract email addresses related to the target domain using a search engine like Google or Bing

Question #226

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=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.

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=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.

D. 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.

Question #227

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 exploit a potential SQL Injection vulnerability to manipulate the application's database.

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 execute a Man-in-the-Middle (MitM) attack to intercept and modify the HTTP headers for a Clickjacking attack.

D. The tester could launch a Cross-Site Scripting (XSS) attack to steal authenticated session cookies, potentially bypassing the clickjacking protection.

Question #228

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 might be compromising physical security to plug into the network directly.

B. The attacker might be implementing MAC flooding to overwhelm the switch's memory.

C. The attacker is probably using a Trojan horse with in-built sniffing capability.

D. The attacker might be using passive sniffing, as it provides significant stealth advantages.

Question #229

You are a cybersecurity consultant for a smart city project. The project involves deploying a vast network of IoT 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. Implement regular firmware updates for all IoT devices.

B. Establish strong, unique passwords for each IoT device.

C. Deploy network intrusion detection systems (IDS) across the IoT network.

D. Implement IP address whitelisting for all IoT devices.

Question #230

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. Maimon Scan, because it is very similar to NULL, FIN, and Xmas scans, but the probe used here is FIN/ACK

B. Xmas Scan, because it can pass through filters undetected, depending on the security mechanisms installed

C. TCP Connect/Full-Open Scan, because it completes a three-way handshake with the target machine

D. ACK Flag Probe Scan, because it exploits the vulnerabilities within the BSD-derived TCP/IP stack

Question #231

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. UNION SQL Injection

B. Error-based SQL Injection

C. In-band SQL Injection

D. Blind/Inferential SQL Injection

Question #232

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. GFI LanCuard

B. Qualys Vulnerability Management

C. Open VAS

D. Nessus Professional

Question #233

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. Raw Sniffing

B. MAC Flooding

C. ARP Poisoning

D. DNS Poisoning

Question #234

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. Use the Diffie-Hellman protocol for key exchange and encryption.

C. Apply asymmetric encryption with RSA and use the public key for encryption.

D. Use symmetric encryption with the AES algorithm.

Question #235

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. Enable GPS tracking for all devices using the app.

B. Regularly update the app to the latest version.

C. Encrypt all sensitive data stored on the device.

D. Implement biometric authentication for app access.

Question #236

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 handling, 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. Ensuring atomicity of operations between checking and using data resources

C. Frequently updating firewall configurations to prevent intrusion attempts

D. Implementing stronger encryption algorithms for all data transfers

Question #237

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. Store the potentially malicious program on an external medium, such as a CD-ROM.

C. Run the potentially malicious program on the sheep dip computer to determine its behavior.

D. Connect the sheep dip computer to the organization's internal network.

Question #238

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 might employ a 'blind' SQL Injection attack, taking advantage of the application's true or false responses to extract data bit by bit

B. The hacker may resort to a DDoS attack instead, attempting to crash the server and thus render the e-commerce site unavailable

C. The hacker may try to use SQL commands which are less known and less likely to be blocked by your system's security

D. The hacker could deploy an 'out-of-band' SQL Injection attack, extracting data via a different communication channel, such as DNS or HTTP requests

Question #239

Your company, SecureTech 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. Switching all data transmission to the HTTPS protocol.

B. Implementing SSL certificates on your company's web servers.

C. Utilizing SSH for secure remote logins to the servers.

D. Applying the Diffie-Hellman protocol to exchange the symmetric key.

Question #240

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. Disable the network's SSID broadcast

B. Enable MAC address filtering

C. Require customers to use VPN when connected to the Wi-Fi

D. Implement WPA2 or WPA3 encryption

Question #241

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. Implement an SQL Injection attack to take advantage of potential unvalidated input and gain unauthorized database access.

C. Employ a brute-force attack to decipher user credentials, considering the lack of server-side validation.

D. Launch a Cross-Site Scripting (XSS) attack, aiming to bypass the client-side sanitization and exploit the exposure of session cookies.

Question #242

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. Examining HTML source code and cookies

C. Using Photon to retrieve archived URLs of the target website from archive.org

D. User-directed spidering with tools like Burp Suite and WebScarab

Question #243

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. Investigate for anomalies in file movements or unauthorized data access attempts within your database system

B. Scrutinize for repeat network login attempts from unrecognized geographical regions

C. Vigilantly monitor for evidence of zero-day exploits that manage to evade your firewall or antivirus software

D. Search for proof of a spear-phishing attempt, such as the presence of malicious emails or risky attachments

Question #244

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 Wi-Fi password is too complex and long.

C. The network is using an uncrackable encryption method.

D. The network is using MAC address filtering.

Question #245

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

B. Try to disable the CSP to bypass script restrictions

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

D. Load a script from an external domain to test the vulnerability

Question #246

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. Wht 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. Exploiting Misconfigured Services

Question #247

Alex, a cloud security engineer working in Eyecloud Inc. is tasked with isolating applications from the underlying infrastructure and stimulating communication via well-defined channels. For this purpose, he used an open-source technology that helped him in developing, packaging, and running applications; further, the technology provides PaaS through OS-level virtualization, delivers containerized software packages, and promotes fast software delivery.

What is the cloud technology employed by Alex in the above scenario?

A. Virtual machine

B. Docker

C. Zero trust network

D. Serverless computing

Question #248

Henry is a penetration tester who works for XYZ organization. While performing enumeration on a client organization, he queries the DNS server for a specific cached DNS record. Further, by using this cached record, he determines the sites recently visited by the organization's user.

What is the enumeration technique used by Henry on the organization?

A. DNS zone walking

B. DNS cache snooping

C. DNS cache poisoning

D. DNSSEC zone walking

Question #249

Gregory, a professional penetration tester working at Sys Security Ltd., is tasked with performing a security test of web applications used in the company. For this purpose, Gregory uses a tool to test for any security loopholes by hijacking a session between a client and server. This tool has a feature of intercepting proxy that can be used to inspect and modify the traffic between the browser and target application. This tool can also perform customized attacks and can be used to test the randomness of session tokens.

Which of the following tools is used by Gregory in the above scenario?

A. Wireshark

B. Nmap

C. Burp Suite

D. CxSAST

Question #250

A bank stores and processes sensitive privacy information related to home loans. However, auditing has never been enabled on the system. What is the first step that the bank should take before enabling the audit feature?

A. Perform a vulnerability scan of the system.

B. Determine the impact of enabling the audit feature.

C. Perform a cost/benefit analysis of the audit feature.

D. Allocate funds for staffing of audit log review.