Question #150

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. Proof of concept (PoC) of the vulnerability, if possible, to demonstrate its potential impact on the system.

B. The total number of high, medium, and low-risk vulnerabilities detected throughout the network.

C. The list of all affected systems within the organization that are susceptible to the identified vulnerability.

D. The CVE ID of the vulnerability and its mapping to the vulnerability's name, XYZ.

Question #151

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. Disabling Autorun functionality on all drives

B. Avoiding the use of outdated web browsers and email software

C. Regularly scan systems for any new files and examine them

D. Applying the latest patches and updating software programs

Question #152

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. Carry out a passive wire sniffing operation using Internet packet sniffers

B. Perform a PRobability INfinite Chained Elements (PRINCE) attack

C. Extract plaintext passwords, hashes, PIN codes, and Kerberos tickets using a tool like Mimikatz

D. Request a service ticket for the service principal name of the target service account

Question #153

As a cybersecurity analyst at IoT 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 IoT 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 IoT devices, which of the following actions should you recommend as the first step?

A. Use stronger encryption algorithms for data transmission between IoT devices.

B. Implement network segmentation to isolate IoT devices from the rest of the network.

C. Conduct a vulnerability assessment specifically for the IoT devices.

D. Install the latest antivirus software on each IoT device.

Question #154

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. Probe the IPC share by attempting to brute force admin credentials

B. Brute force Active Directory

C. Extract usernames using email IDs

D. Conduct a DNS zone transfer

Question #155

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. Recommend using a strong password for the smart home system's main control panel.

B. Suggest implementing two-factor authentication for the smart home system's mobile app.

C. Propose frequent system resets to clear any potential malware.

D. Advise using a dedicated network for the smart home system, separate from the home's main Wi-Fi network.

Question #156

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. Retain the setting as it aids in troubleshooting user issues.

B. Suppress detailed error messages, as they can expose sensitive information.

C. Implement stronger encryption to secure the error messages.

D. Increase the frequency of automated server backups.

Question #157

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 hash functions to distribute the keys.

B. Use HTTPS protocol for secure key transfer.

C. Use digital signatures to encrypt the symmetric keys.

D. Implement the Diffie-Hellman protocol for secure key exchange.

Question #158

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. Rely on network-level encryption protocols for data transfer.

B. Use SSL/TLS for data transfer and allow the CSP to manage encryption keys.

C. Utilize the CSP's built-in data encryption services.

D. Use client-side encryption and manage encryption keys independently of the CSP.

Question #159

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 Whois 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 working correctly

B. Thin Whois model with a malfunctioning server

C. Thick Whois model with a malfunctioning server

D. Thick Whois model working correctly

Question #160

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 AES-128: Provides moderate security and fast encryption, offering a balance between the two.

B. Data encryption with AES-256: Provides high security with better performance than 3DES, but not as fast as other AES key sizes.

C. Data encryption with 3DES using a 168-bit key: Offers high security but slower performance due to 3DES's inherent inefficiencies.

D. Data encryption with Blowfish using a 448-bit key: Offers high security but potential compatibility issues due to Blowfish's less widespread use.

Question #161

You are a security analyst for CloudSec, 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 multi-factor authentication for all cloud user accounts.

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

Question #162

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=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.

C. 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.

D. 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.

Question #163

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. Open System authentication

B. WPA2-PSK with AES encryption

C. SSID broadcast disabling

D. MAC address filtering

Question #164

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 O(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=128 bits: This configuration provides less security than option A, but RSA key generation and AES encryption will be faster.

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=512 bits: This configuration provides the highest level of security but at a significant performance cost due to the large AES key size.

Question #165

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. Whaling and Targeted Attacks

B. Pretexting and Network Vulnerability

C. Spear Phishing and Spam

D. Baiting and Involuntary Data Leakage

Question #166

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. Regularly change Wi-Fi passwords used by the devices.

C. Mandate the use of VPNs when accessing corporate data.

D. Enforce a policy that only allows app installations from approved corporate app stores.

Question #167

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. Type of device used to open the email

C. The email accounts related to the domain of the organization

D. The time recipient spent reading the email

Question #168

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. Disable the network's SSID broadcast

B. Enable encryption on the wireless network

C. Enable MAC address filtering

D. Reduce the signal strength of the wireless router

Question #169

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 leverage a botnet to launch a Pulse Wave attack, sending high-volume traffic pulses at regular intervals

C. The attacker should initiate a volumetric flood attack using a single compromised machine to overwhelm the retailer's network bandwidth

D. The attacker should execute a simple ICMP flood attack from a single IP, exploiting the retailer's ICMP processing

Question #170

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. Identity Cloning and Concealment

B. Child Identity Theft

C. Social Identity Theft

D. Synthetic Identity Theft

Question #171

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. Adopt a robust software policy that restricts the installation of unauthorized applications.

D. Reinforce physical security measures to limit access to sensitive zones within the company premises, thereby warding off unauthorized intruders.

Question #172

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. Conducting social engineering tests to check if employees can be tricked into revealing sensitive information

B. Checking for hardware and software misconfigurations to identify any possible loopholes

C. Evaluating the network for inherent technology weaknesses prone to specific types of attacks

D. Investigating if any ex-employees still have access to the company's system and data

Question #173

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

Question #174

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.

Question #175

You are a cybersecurity consultant at SecureIoT Inc. A manufacturing company has contracted you to strengthen the security of their Industrial IoT (IIoT) 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. Increase the frequency of changing passwords on all IIoT devices.

B. Use the same encryption standards for IIoT devices as for IT devices.

C. Rely on the existing firewall and install antivirus software on each IIoT device.

D. Implement network segmentation to separate IIoT devices from the rest of the network.

Question #176

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. Rowhammer Attack

B. Watering Hole Attack

C. Side-Channel Attack

D. Privilege Escalation Attack

Question #177

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 detect vulnerabilities at a given point in time

D. Vulnerability scanning software is limited in its ability to perform live tests on web applications to detect errors or unexpected behavior

Question #178

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

Question #179

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. Hide the network SSID

B. Enable WPA2 or WPA3 encryption on the wireless router

C. Implement a MAC address whitelist

D. Establish a regular schedule for changing the network password

Question #180

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. Impersonating an ISP technical support agent to trick the target into providing further network details

C. Shoulder surfing to observe sensitive credentials input on the target’s computers

D. Eavesdropping on internal corporate conversations to understand key topics

Question #181

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. Koodous - Because it combines social networking with antivirus signatures and YARA rules to detect malware

C. YaraRET - Because it helps in reverse engineering Trojans to generate YARA rules

D. AutoYara - Because it automates the generation of YARA rules from a set of malicious and benign files

Question #182

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. Utilize a blind injection technique that uses time delays or error signatures to extract information

B. Try to insert a string value where a number is expected in the input field

C. Attempt to compromise the system through OS-level command shell execution

D. Use the UNION operator to combine the result sets of two or more SELECT statements

Question #183

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. Script Kiddies trying to compromise the system using pre-made scripts.

B. Gray Hats testing system vulnerabilities to help vendors improve security.

C. White Hats conducting penetration testing to identify security weaknesses.

D. Black Hats trying to exploit system vulnerabilities for malicious intent.

Question #184

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 information. You further notice queries that indicate the use of the Google Hacking Database (CHDB) with an emphasis on VPN footprinting. Which of the following Google advanced search operators would be the LEAST useful in providing the attacker with sensitive VPN-related information?

A. location: This operator finds information for a specific location

B. inurl: This operator restricts the results to only the pages containing the specified word in the URL

C. link: This operator searches websites or pages that contain links to the specified website or page

D. intitle: This operator restricts results to only the pages containing the specified term in the title

Question #185

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. Identifying the specific tools used by the adversary for privilege escalation.

B. Analyzing the initial exploitation methods, the adversary used.

C. Checking the persistence mechanisms used by the adversary in compromised systems.

D. Investigating the data exfiltration methods used by the adversary.

Question #186

Jason, a certified ethical hacker, is hired by a major e-commerce company to evaluate their network's security. As part of his reconnaissance, Jason is trying to gain as much 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 use a DNS zone transfer to gather information about the company's servers.

D. Jason should perform a ping sweep to identify all the live hosts in the company's IP range.

Question #187

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. Limit the range of the store's wireless signals

B. Implement MAC address filtering

C. Disable SSID broadcasting

D. Implement WPA3 encryption for the store's Wi-Fi network

Question #188

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 Timestamp Ping Scan

B. ICMP ECHO Ping Scan

C. TCP SYN Ping Scan

D. UDP Ping Scan

Question #189

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. Regularly backing up server data

B. Enabling multi-factor authentication for users

C. Implementing a firewall to filter traffic

D. Performing regular server configuration audits

Question #190

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. Implement IPsec in addition to SSL/TLS.

B. Switch to using SSH for data transmission.

C. Encrypt data using the AES algorithm before transmission.

D. Use the cloud service provider's built-in encryption services.

Question #191

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. Insecure Patch Management; updating application software regularly

B. Instant Messenger Applications; verifying the sender's identity before opening any files

C. Rogue/Decoy Applications; ensuring software is labeled as TRUSTED

D. Portable Hardware Media/Removable Devices; disabling Autorun functionality

Question #192

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. Insider attacks and the organization should have implemented robust access control and monitoring.

B. Distribution attack and the organization could have ensured software and hardware integrity checks.

C. Passive attack and the organization should have used encryption techniques.

D. Active attack and the organization could have used network traffic analysis.

Question #193

As a security analyst for SkySecure 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. Use a Cloud Access Security Broker (CASB).

B. Use a hardware-based firewall to secure all cloud resources.

C. Implement separate security management tools for each cloud platform.

D. Rely on the built-in security features of each cloud platform.

Question #194

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.

Question #195

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 ports on the target network are open

B. The target network has no firewall present

C. The ports on the target network are closed

D. The target network has a stateful firewall present

Question #196

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.

Question #197

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. Utilizing the char encoding function to convert hexadecimal and decimal values into characters that pass-through SQL engine parsing

B. Implementing sophisticated matches such as "OR john' = 'john'" in place of classical matches like "OR 1=1"

C. Manipulating white spaces in SQL queries to bypass signature detection

D. Using the URL encoding method to replace characters with their ASCII codes in hexadecimal form

Question #198

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. Enforce a policy of regularly changing Wi-Fi passwords

D. Implement 802.1X authentication

Question #199

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 hacker 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 network scan to identify live hosts and their IP addresses.

C. They are performing a TCP connect scan to identify open ports on the target machine.

D. They are performing a vulnerability scan to identify any weaknesses in the target system.

Question #200

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 malware analysis tools on the guest OS

B. Connecting the system to the production network during the malware analysis

C. Simulating Internet services using tools such as INetSim

D. Installing multiple guest operating systems on the virtual machine(s)