Question #101 *Topic 1*

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

A. Bryan's public key; Bryan's public key

B. Alice's public key; Alice's public key

C. Bryan's private key; Alice's public key

D. Bryan's public key; Alice's public key **Most Voted**

Correct Answer: *D*

Community vote distribution

D (100%)

Question #102 *Topic 1*

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

A. AndroidManifest.xml **Most Voted**

B. classes.dex

C. APK.info

D. resources.asrc

Correct Answer: *A*

Community vote distribution

A (100%)

Question #103 *Topic 1*

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

A. NetPass.exe

B. Outlook scraper

C. WebBrowserPassView

D. Credential enumerator **Most Voted**

Correct Answer: *D*

Community vote distribution

D (100%)

Question #104 *Topic 1*

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

A. Bluesmacking

B. Bluesnarfing **Most Voted**

C. Bluejacking

D. Bluebugging

Correct Answer: *B*

Community vote distribution

B (100%)

Question #105 *Topic 1*

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

A. Matt inadvertently provided the answers to his security questions when responding to the post. **Most Voted**

B. Matt inadvertently provided his password when responding to the post.

C. Matt’s computer was infected with a keylogger.

D. Matt’s bank account login information was brute forced.

Correct Answer: *A*

Community vote distribution

A (100%)

Question #106 *Topic 1*

Attacker Simon targeted the communication network of an organization and disabled the security controls of NetNTLMv1 by modifying the values of LMCompatibilityLevel, NTLMMinClientSec, and RestrictSendingNTLMTraffic. He then extracted all the non-network logon tokens from all the active processes to masquerade as a legitimate user to launch further attacks.
What is the type of attack performed by Simon?

A. Combinator attack

B. Dictionary attack

C. Rainbow table attack

D. Internal monologue attack **Most Voted**

Correct Answer: *D*

Community vote distribution

D (100%)

Question #107 *Topic 1*

Steve, an attacker, created a fake profile on a social media website and sent a request to Stella. Stella was enthralled by Steve's profile picture and the description given for his profile, and she initiated a conversation with him soon after accepting the request. After a few days, Steve started asking about her company details and eventually gathered all the essential information regarding her company.
What is the social engineering technique Steve employed in the above scenario?

A. Baiting

B. Piggybacking

C. Diversion theft

D. Honey trap **Most Voted**

Correct Answer: *D*

Community vote distribution

D (100%)

Question #108 *Topic 1*

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

A. Exploration

B. Investigation

C. Reconnaissance **Most Voted**

D. Enumeration

Correct Answer: *C*

Community vote distribution

C (100%)

Question #109 *Topic 1*

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

A. Incident triage **Most Voted**

B. Preparation

C. Incident recording and assignment

D. Eradication

Correct Answer: *A*

Community vote distribution

A (100%)

Question #110 *Topic 1*

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

A. Weaponization

B. Actions on objectives **Most Voted**

C. Command and control

D. Installation

Correct Answer: *B*

Community vote distribution

B (100%)

Question #111 *Topic 1*

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

A. Diversion theft

B. Quid pro quo **Most Voted**

C. Elicitation

D. Phishing

Correct Answer: *B*

Community vote distribution

B (88%) 13%

Question #112 *Topic 1*

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

A. AlienVault® OSSIMTM

B. Syhunt Hybrid **Most Voted**

C. Saleae Logic Analyzer

D. Cisco ASA

Correct Answer: *B*

Community vote distribution

B (100%)

Question #113 *Topic 1*

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

A. getsystem **Most Voted**

B. getuid

C. keylogrecorder

D. autoroute

Correct Answer: *A*

Community vote distribution

A (100%)

Question #114 *Topic 1*

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

A. Xmas scan

B. IDLE/IPID header scan

C. TCP Maimon scan **Most Voted**

D. ACK flag probe scan

Correct Answer: *C*

Community vote distribution

C (100%)

Question #115 *Topic 1*

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

A. Robotium

B. BalenaCloud

C. Flowmon **Most Voted**

D. IntentFuzzer

Correct Answer: *C*

Community vote distribution

C (100%)

Question #116 *Topic 1*

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

A. IaaS

B. SaaS **Most Voted**

C. PaaS

D. CaaS

Correct Answer: *B*

Community vote distribution

B (100%)

Question #117 *Topic 1*

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

A. Google advanced search

B. Meta search engines

C. Reverse image search **Most Voted**

D. Advanced image search

Correct Answer: *C*

Community vote distribution

C (100%)

Question #118 *Topic 1*

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

A. Pass the hash **Most Voted**

B. Internal monologue attack

C. LLMNR/NBT-NS poisoning

D. Pass the ticket

Correct Answer: *A*

Community vote distribution

A (100%)

Question #119 *Topic 1*

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

A. Credentialed assessment

B. Internal assessment

C. External assessment

D. Passive assessment **Most Voted**

Correct Answer: *D*

Community vote distribution

D (67%) B (33%)

Question #120 *Topic 1*

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

A. NTLM **Most Voted**

B. RADIUS

C. WPA

D. SSO

Correct Answer: *A*

Community vote distribution

A (75%) B (25%)

Question #121 *Topic 1*

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

A. Remote procedure call (RPC)

B. Telnet

C. Server Message Block (SMB)

D. Network File System (NFS)

Correct Answer: *C*

Question #122 *Topic 1*

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

A. Wardriving

B. Wireless sniffing

C. Evil twin **Most Voted**

D. Piggybacking

Correct Answer: *C*

Community vote distribution

C (60%) D (40%)

Question #123 *Topic 1*

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

A. domain.txt

B. Robots.txt **Most Voted**

C. Document root

D. index.html

Correct Answer: *B*

Community vote distribution

B (100%)

Question #124 *Topic 1*

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

A. DNSSEC zone walking

B. DNS cache snooping

C. DNS enumeration

D. DNS tunneling method **Most Voted**

Correct Answer: *D*

Community vote distribution

D (100%)

Question #125 *Topic 1*

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

A. RADIUS

B. WPA

C. WEP **Most Voted**

D. WPA3

Correct Answer: *C*

Community vote distribution

C (100%)

Question #126 *Topic 1*

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. Encrypt data client-side before uploading to the cloud and retain control of the encryption keys. **Most Voted**

B. Use the cloud service provider's encryption services but store keys on-premises.

C. Rely on Secure Sockets Layer (SSL) encryption for data at rest.

D. Use the cloud service provider's default encryption and key management services.

Correct Answer: *A*

Community vote distribution

A (100%)

Question #127 *Topic 1*

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. Employing data staging techniques to collect and aggregate sensitive data.

B. Initiating DNS tunneling to communicate with the command-and-control server. **Most Voted**

C. Establishing a command-and-control server to communicate with compromised systems.

D. Conducting internal reconnaissance using PowerShell scripts.

Correct Answer: *B*

Community vote distribution

B (100%)

Question #128 *Topic 1*

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 **Most Voted**

B. Probing system services and observing the three-way handshake

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

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

Correct Answer: *A*

Community vote distribution

A (100%)

Question #129 *Topic 1*

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 3: The test was executed to observe the response of the target system when a packet with URC, PSH, SYN, and FIN flags was sent, thereby identifying the OS

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 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 **Most Voted**

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

Correct Answer: *C*

Community vote distribution

C (100%)

Question #130 *Topic 1*

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 'z' and 'u', which situation is likely to result in the highest extracted data volume?

A. z=600, u=2: The attacker devises 2 SQL payloads, each aimed at tables holding 600 records, affecting all columns across all 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=500, u=3: The attacker creates 3 SQL payloads and targets tables with 500 records each, exploiting all columns and 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. **Most Voted**

Correct Answer: *D*

Community vote distribution

D (100%)

Question #131 *Topic 1*

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. Smurf attack

B. UDP flood attack

C. Pulse wave attack

D. Ping of Death attack **Most Voted**

Correct Answer: *D*

Community vote distribution

D (100%)

Question #132 *Topic 1*

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 **Most Voted**

B. Implementing YARA rules that focus solely on known malware signatures

C. Creating YARA rules to examine only the private database for intrusions

D. Incorporating YARA rules to detect patterns in all files regardless of their nature

Correct Answer: *A*

Community vote distribution

A (100%)

Question #133 *Topic 1*

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. TCP/IP Hijacking

B. RST Hijacking

C. UDP Hijacking

D. Man-in-the-middle Attack Using Forged ICMP and ARP Spoofing **Most Voted**

Correct Answer: *D*

Community vote distribution

D (100%)

Question #134 *Topic 1*

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. Develop an in-depth Risk Management process, involving identification, assessment, treatment, tracking, and review of risks to control the potential effects on the organization.

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. **Most Voted**

C. Implement an Information Assurance (IA) policy focusing on ensuring the integrity, availability, confidentiality, and authenticity of information systems.

D. Adopt a Continual/Adaptive Security Strategy involving ongoing prediction, prevention, detection, and response actions to ensure comprehensive computer network defense.

Correct Answer: *B*

Community vote distribution

B (83%) D (17%)

Question #135 *Topic 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 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.

B. 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.

C. 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. **Most Voted**

D. 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.

Correct Answer: *C*

Community vote distribution

C (100%)

Question #136 *Topic 1*

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. UNION SELECT NULL, NULL, NULL -- : This payload manipulates the UNION SQL operator, enabling the attacker to retrieve data from different database tables

B. ' OR username LIKE '%': This payload uses the LIKE operator to search for a specific pattern in a column

C. ' OR '1'='l: This payload manipulates the WHERE clause of an SQL statement, allowing the attacker to view unauthorized data

D. ' OR 'a'='a; DROP TABLE members; --: This payload combines the manipulation of the WHERE clause with a destructive action, causing data loss Most Voted

Correct Answer: *D*

Community vote distribution

D (83%) A (17%)

Question #137 *Topic 1*

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 offline 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. Perform a system reboot to clear the memory

B. Delete the compromised user's account

C. Change the NTLM password hash used to encrypt the ST Most Voted

D. Invalidate the TGS the attacker acquired

Correct Answer: *C*

Community vote distribution

C (89%) 11%

Question #138 *Topic 1*

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 IoMT devices could be potential entry points for future attacks. What would be your main recommendation to protect these devices from such threats?

A. Disable all wireless connectivity on IoMT devices.

B. Regularly change the IP addresses of all IoMT devices.

C. Use network segmentation to isolate IoMT devices from the main network. **Most Voted**

D. Implement multi-factor authentication for all IoMT devices.

Correct Answer: *C*

Community vote distribution

C (100%)

Question #139 *Topic 1*

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. Provide employees with corporate-owned devices for work-related tasks.

B. Require all employee devices to use a company-provided VPN for internet access.

C. Implement a mobile device management solution that restricts the installation of non-approved applications.

D. Conduct regular cybersecurity awareness training, focusing on phishing attacks. **Most Voted**

Correct Answer: *D*

Community vote distribution

D (62%) C (38%)

Question #140 *Topic 1*

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. An attacker may be able to inject a malicious DLL into the current running process

B. Weak encryption might be allowing man-in-the-middle attacks, leading to data tampering

C. Unauthorized users may perform privilege escalation using unnecessarily created accounts **Most Voted**

D. An attacker may carry out a Denial-of-Service assault draining the resources of the server in the process

Correct Answer: *C*

Community vote distribution

C (80%) A (20%)

Question #141 *Topic 1*

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. The organization is at fault because it did not fix all identified vulnerabilities. **Most Voted**

B. Both the organization and John share responsibility because they did not adequately manage the vulnerabilities.

C. John is at fault because he did not emphasize the necessity of patching all vulnerabilities.

D. The organization is not at fault because they used their resources as per their understanding.

Correct Answer: *A*

Community vote distribution

A (95%) 5%

Question #142 *Topic 1*

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 SAM file has been encrypted using the SYSKEY function.

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. **Most Voted**

D. The Windows system is using the Kerberos authentication protocol as the default method.

Correct Answer: *C*

Community vote distribution

C (100%)

Question #143 *Topic 1*

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 system failed to establish a connection due to an incorrect port number.

B. The enumeration process was blocked by the target system's intrusion detection system.

C. The secure LDAP connection was not properly initialized due to a lack of 'use_ssl = True' in the server object creation. **Most Voted**

D. The Python version installed on the CEH's machine is incompatible with the ldap3 library.

Correct Answer: *C*

Community vote distribution

C (100%)

Question #144 *Topic 1*

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 **Most Voted**

D. Display a captive portal page that warns users about the possibility of Evil Twin attacks

Correct Answer: *C*

Community vote distribution

C (67%) D (33%)

Question #145 *Topic 1*

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 192.168.1.0/24 -n nsl.example.com -t axfr

B. dnsrecon -r 10.0.0.0/24 -n nsl.example.com -t zonewalk

C. dnsrecon -r 162.241.216.0/24 -n nsl.example.com -t std **Most Voted**

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

Correct Answer: *C*

Community vote distribution

C (100%)

Question #146 *Topic 1*

You are an ethical hacker tasked with conducting an enumeration of a company's network. Given a Windows Answered Marked for Review 37.6% 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 **Most Voted**

B. Use nbtstat -a followed by the IPv6 address of the target machine

C. Use nbtstat -c to get the contents of the NetBIOS name cache

D. Utilize Nmap Scripting Engine (NSE) for NetBIOS enumeration

Correct Answer: *A*

Community vote distribution

A (67%) B (17%) D (17%)

Question #147 *Topic 1*

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 SCTP INIT Scan with the command "-sY"

B. Use UDP Raw ICMP Port Unreachable Scanning with the command "-sU"

C. Use the ACK flag probe scanning technique with the command "-sA"

D. Use the IDLE/IPID header scan technique with the command "-sI" **Most Voted**

Correct Answer: *D*

Community vote distribution

D (100%)

Question #148 *Topic 1*

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. Implement endpoint detection and response solution to oversee endpoint activities

B. Set up a honeypot to attract potential attackers into a controlled environment for analysis

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 **Most Voted**

Correct Answer: *D*

Community vote distribution

D (100%)

Question #149 *Topic 1*

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=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. **Most Voted**

B. 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.

C. 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.

D. 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.

Correct Answer: *A*

Community vote distribution

A (100%)

Question #150 *Topic 1*

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. **Most Voted**

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.

Correct Answer: *B*

Community vote distribution

B (100%)

← Previous Questions

Next Questions →