ECcouncil 312-50V13 Exam Questions

Total Questions: 550+
Demo Questions: 30
Version: Updated for 2025

Prepared and Verified by Cert Empire – Your Trusted IT Certification Partner

For Access to the full set of Updated Questions – Visit: 312-50v13 Exam Dumps by Cert Empire

Question: 1

User A is writing a sensitive email message to user B outside the local network. User A has chosen to use PKI to secure his message and ensure only user B can read the sensitive email. At what layer of the OSI layer does the encryption and decryption of the message take place?

A: Application

B: Transport

C: Session

D: Presentation

Correct Answer:

D

Explanation:

The Presentation Layer (Layer 6) of the OSI model is responsible for the translation, formatting, and syntax of data between the Application layers of two end systems. Its primary functions include character code translation, data compression, and, most relevant to this question, data encryption and decryption. When User A encrypts an email message using PKI, this transformation of application data into a secure format is a service performed at the Presentation Layer before it is passed down the stack for transmission.

Why Incorrect Options are Wrong:

A: Application: The email client operates at the Application Layer (Layer 7), but this layer uses the services of the Presentation Layer for encryption. The function itself resides at Layer 6.

B: Transport: The Transport Layer (Layer 4) provides end-to-end communication, but its security protocols (like TLS) encrypt the entire communication channel, not the specific message content as described.

C: Session: The Session Layer (Layer 5) is responsible for establishing, managing, and terminating communication sessions between applications, not for the encryption of the data within that session.

References:

1. Stallings, W. (2017). Data and Computer Communications (10th ed.). Pearson. In Chapter 2, Section 2.2, "The OSI Model," the Presentation Layer is defined: "The Presentation layer is concerned with the syntax of the data exchanged between application entities... it provides for data compression and encryption."

2. Forouzan, (2013). Data Communications and Networking (5th ed.). McGraw-Hill. In Chapter 2, "Network Models," the section on the Presentation Layer states, "The presentation layer is responsible for translation, compression, and encryption." (p. 45).

3. Kurose, J. F., & Ross, K. W. (2021). Computer Networking: A Top-Down Approach (8th ed.). Pearson. In Chapter 1, Section 1.5.2, "The OSI Model," the Presentation Layer's role is described as providing services that allow applications to interpret the meaning of data, such as data compression and data encryption.

Question: 2

A new wireless client is configured to join a 802.11 network. This client uses the same hardware and software as many of the other clients on the network. The client can see the network, but cannot connect. A wireless packet sniffer shows that the Wireless Access Point (WAP) is not responding to the association requests being sent by the wireless client. What is a possible source of this problem?

A: The WAP does notrecognize the client's MAC address

B: The client cannot see the SSID of the wireless network

C: Client is configured for the wrong channel

D: The wireless client is not configured to use DHCP

Correct Answer:

A

Explanation:

The scenario describes a failure during the Layer 2 association phase of the 802.11 connection process. The client can see the network, meaning it is on the correct channel and receiving beacon frames. However, the Wireless Access Point (WAP) is ignoring its association requests. This behavior is a direct symptom of MAC address filtering being enabled on the WAP. MAC filtering is a security mechanism where a WAP maintains an access control list of hardware MAC addresses. If the new client's MAC address is not on the WAP's "allow list," the WAP will intentionally not respond to its association requests, preventing it from joining the network.

Why Incorrect Options are Wrong:

B: This is incorrect because the question explicitly states, "The client can see the network," which means it has successfully detected the SSID from the WAP's beacon frames.

C: This is incorrect because if the client were on the wrong channel, it would not be able to receive the WAP's beacon frames and therefore would not "see the network."

D: This is incorrect because DHCP is a Layer 3 protocol used for IP address assignment, which occurs only after a successful Layer 2 association and authentication have been completed.

References:

1. Kurose, J. F., & Ross, K. W. (2021). Computer Networking: A Top-Down Approach (8th ed.). Pearson. In Chapter 6, Section 6.3.2, the text describes the 802.11 association process where a client sends an association request to an access point. The text also discusses MAC filtering as a security measure where the AP checks the client's MAC address against a configured list before allowing association.

2. MIT OpenCourseWare. (2006). 6.829 Computer Networks, Fall 2002. Lecture 18: Wireless & Mobility (802.11). Massachusetts Institute of Technology. The lecture notes detail the 802.11 state machine, showing that association follows scanning and authentication. It mentions MAC address filtering as a basic access control method where the AP can be configured to only serve a specific list of clients.

3. Gast, M. S. (2005). 802.11 Wireless Networks: The Definitive Guide (2nd ed.). O'Reilly Media. Chapter 8, "802.11 Security," describes MAC address filtering as a first line of defense where access points can be configured with a list of allowed MAC addresses, and frames from other addresses are ignored.

Question: 3

You are tasked to perform a penetration test. While you are performing information gathering, you find an employee list in Google. You find the receptionist's email, and you send her an email changing the source email to her boss's email (boss@company). In this email, you ask for a pdf with information. She reads your email and sends back a pdf with links. You exchange the pdf links with your malicious links (these links contain malware) and send back the modified pdf, saying that the links don't work. She reads your email, opens the links, and her machine gets infected. You now have access to the company network. What testing method did you use?

A: Social engineering

B: Piggybacking

C: Tailgating

D: Eavesdropping

Correct Answer:

A

Explanation:

The entire attack is based on manipulating the receptionist by exploiting human trust and psychology. The attacker impersonates a figure of authority (the boss), creates a believable pretext (requesting a document and then claiming links are broken), and deceives the victim into performing an action that compromises security (clicking malicious links). This process of psychological manipulation to bypass security controls is the definition of social engineering. The specific technique demonstrated is a form of spear phishing, which is a primary category of social engineering attack.

Why Incorrect Options are Wrong:

B: Piggybacking: This is a physical security breach where an attacker follows an authorized person into a restricted area with their consent, which is not what occurred.

C: Tailgating: This is a physical security breach, similar to piggybacking but without the authorized person's knowledge, and is irrelevant to this digital attack.

D: Eavesdropping: This involves the passive interception of communications. The attacker in this scenario actively engaged with and manipulated the target, not just listened in.

References:

1. EC-Council. (2023). Certified Ethical Hacker (CEH) v13 Courseware, Module 05: Social Engineering. The module defines social engineering as the art of manipulating people to perform actions or divulge confidential information and explicitly covers techniques like phishing, pretexting, and impersonation as described in the scenario.

2. Kurose, J. F., & Ross, K. W. (2021). Computer Networking: A Top-Down Approach (8th ed.). Pearson. In Chapter 8, "Security in Computer Networks," social engineering is described as a low-tech but highly effective attack where an intruder "convinces" a user to run a program or provide information, perfectly matching the scenario.

3. Stallings, W., & Brown, L. (2018). Computer Security: Principles and Practice (4th ed.). Pearson. Chapter 17, "Human Factors," details social engineering tactics, including authority-based impersonation and creating a compelling story (pretexting) to trick employees into compromising security.

Question: 4

If a tester is attempting to ping a target that exists but receives no response or a response thatstates the destination is unreachable, ICMP may be disabled and the network may be using TCP. Which other option could the tester use to get a response from a host using TCP?

A: Traceroute

B: Hping

C: TCP ping

D: Broadcast ping

Correct Answer:

B

Explanation:

Hping (specifically hping3) is a versatile command-line packet crafting tool designed for security auditing and testing. When ICMP is blocked by a firewall or network filter, Hping can be used to perform host discovery by sending TCP packets. For instance, a tester can send a TCP SYN packet to a common port (e.g., 80 or 443). If the host is online and the port is open, it will respond with a SYN/ACK packet. If the port is closed, it will respond with an RST packet. In either case, receiving a response confirms the host is active, effectively bypassing ICMP-based filtering.

Why Incorrect Options are Wrong:

A: Traceroute: The primary purpose of traceroute is to map the network route (hops) to a destination, not simply to verify if a single host is online.

C: TCP ping: This is a generic term for the technique of using TCP packets for a ping-like check, not a specific, standard tool. Hping is a specific tool that implements this technique.

D: Broadcast ping: This method uses ICMP echo requests sent to a network's broadcast address and is therefore ineffective if ICMP is blocked as stated in the scenario.

References:

1. EC-Council. (2023). Certified Ethical Hacker (CEH) v13 Courseware, Module 03: Scanning Networks, Section: "Host Discovery Techniques," Subsection: "TCP SYN/ACK,

UDP, and ICMP Scan." The courseware details using tools like Hping3 to craft custom packets for discovery when standard pings fail.

2. Ricci, S. (2015). Penetration Testing: Network Threat Testing. Syngress, Elsevier. Chapter 3: "Scanning," pp. 65-67. This text describes using Hping3 for various scans, including sending TCP SYN or ACK packets to discover live hosts behind firewalls that block ICMP.

3. Al-Sakran, H. O. (2012). Network Probing and Reconnaissance. SANS Institute InfoSec Reading Room. This paper discusses advanced reconnaissance techniques, highlighting tools like Hping for their ability to craft custom TCP packets (SYN, ACK, FIN) to probe hosts and bypass filtering rules. (Available via SANS Reading Room).

Question: 5

Which is the firststep followed by Vulnerability Scannersfor scanning a network?

A: OS Detection

B: Firewall detection

C: TCP/UDP Portscanning

D: Checking if the remote host is alive

Correct Answer:

D

Explanation:

The vulnerability scanning process follows a logical methodology, beginning with target discovery. Before any detailed analysis can be performed, the scanner must first verify which hosts on the target network are online and responsive. This initial phase, known as host discovery or live host identification, typically uses techniques like ICMP echo requests (ping sweeps) or ARP scans on local networks. Only after a host is confirmed to be "alive" can the scanner proceed to subsequent steps like port scanning, service enumeration, and vulnerability mapping. This foundational step prevents the scanner from wasting time and resources on inactive IP addresses.

Why Incorrect Options are Wrong:

A: OS Detection: This is performed after identifying open ports on a live host to fingerprint the operating system based on its network responses. It is not the initial step.

B: Firewall detection: This is typically inferred during the port scanning phase by analyzing filtered or dropped packets, which requires a host to be confirmed as active first.

C: TCP/UDP Portscanning: This is the process of checking for open ports on a target machine, which is only logical to perform after confirming the machine is online.

References:

1. EC-Council, "Certified Ethical Hacker (CEH) Version 13 Courseware," Module 06: Vulnerability Analysis. The official CEH v13 curriculum outlines the scanning methodology, which explicitly starts with "Check for Live Systems" as the first step before checking for open ports or performing OS discovery.

2. Lyon, G. (2009). Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Auditing. Nmap Project. Chapter 3, "Host Discovery ('Ping Scanning')," details the initial phase of any network scan. The text states, "Before Nmap can send probes to a host... it must determine whether the target is even online... This is the host discovery phase." This foundational text aligns with the CEH methodology.

3. Kaur, J., & Singh, (2016). A Survey of Network Security Scanning. International Journal of Advanced Research in Computer Science and Software Engineering, 6(5), 599-605. This academic paper reviews scanning methodologies, consistently placing host discovery (determining if a host is alive) as the prerequisite first step before port scanning and service identification. The process is described as a sequence: "The first step is to find the live hosts... The second step is to find the open ports." (p. 600).

Question: 6

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

A: Bluesmacking

B: Bluebugging

C: Bluejacking

D: Bluesnarfing

Correct Answer:

D

Explanation:

Bluesnarfing is the specific term for the unauthorized access and theft of information from a Bluetooth-enabled device. Attackers exploit vulnerabilities, often in the Object Exchange (OBEX) protocol, to establish a connection and pull sensitive data such as contact lists, calendar entries, emails, and text messages without the owner's consent or knowledge. This technique is a direct data theft attack, precisely matching the scenario described in the question.

Why Incorrect Options are Wrong:

A: Bluesmacking: This is a Denial-of-Service (DoS) attack that sends an oversized packet to crash the target Bluetooth device, not steal information.

B: Bluebugging: This is a more advanced attack where an attacker gains full remote control over a device, which is broader than just information theft.

C: Bluejacking: This involves sending unsolicited messages (like a vCard) to a Bluetooth device; it is a form of spam, not data theft.

References:

1. Padgette, J., Bahr, J., Batra, M., Holt, J., Smith, R., & Toder, M. (2017). Guide to Bluetooth Security (NIST Special Publication 800-121 Revision 2). National Institute of Standards and Technology. In Section 4.2.1, "Legacy Security Vulnerabilities," Bluesnarfing is explicitly defined as "The unauthorized pulling of data from a Bluetooth device."

2. EC-Council. (2023). Certified Ethical Hacker (CEH) v13 Courseware. Module 16: Hacking Wireless Networks. The official curriculum defines Bluesnarfing as a class of security breach for stealing information from wireless devices.

3. Haataja, K., & Toivanen, P. (2008). Bluetooth Security. In: Handbook of Information and Communication Security. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-78044-729. This chapter discusses various Bluetooth attacks, differentiating Bluesnarfing as an attack focused on stealing information like the address book.

Question: 7

_____ is a tool that can hide processes from the process list, can hide files, registry entries, and intercept keystrokes.

A: Trojan

B: RootKit

C: DoS tool

D: Scanner

E: Backdoor

Correct Answer:

B

Explanation:

A rootkit is a collection of malicious software tools that grants an attacker privileged (root-level) access to a computer while actively hiding its presence. Its primary function is to modify the core of the operating system or install kernel-level drivers to intercept and manipulate system calls. This allows it to conceal files, running processes, network connections, and registry entries from legitimate monitoring and security tools. The description in the question, particularly the hiding of system-level objects, is the defining characteristic of a rootkit.

Why Incorrect Options are Wrong:

A: Trojan: A Trojan is a delivery mechanism that disguises malware as legitimate software. While it can deliver a rootkit, it is not the rootkit itself.

C: DoS tool: A Denial-of-Service tool is used to overwhelm a target system with traffic to make it unavailable, not to hide its presence on a host.

D: Scanner: A scanner is a reconnaissance tool used to identify vulnerabilities or open ports; it is not malware that infects and hides within a system.

E: Backdoor: A backdoor is a method for bypassing authentication to gain access. A rootkit often protects a backdoor, but the hiding functionality is specific to the rootkit.

References:

1. Al-Ameen, M. N., & Liu, J. (2007). A survey of rootkit detection techniques. In Proceedings of the 2007 ACM workshop on Recurring malcode (pp. 1-6). The paper defines a rootkit as "a set of tools used by an attacker to hide his presence and activities on a victim's machine. It can hide files, processes, network connections, and kernel modules." (Section 2, Paragraph 1). DOI: https://doi.org/10.1145/1314390.1314392

2. Wang, Z., Jiang, X., Cui, W., & Ning, P. (2009). Countering kernel rootkits with lightweight hook protection. In Proceedings of the 16th ACM conference on Computer and communications security (pp. 545-554). The authors state, "A kernel rootkit is a malicious program that subverts the OS kernel to hide its presence (e.g., its files and processes) and its malicious activities (e.g., keystroke logging)." (Section 1, Introduction, Paragraph 1). DOI: https://doi.org/10.1145/1653662.1653728

3. Baliga, A., & Iftode, L. (2011). Automatic Detection and Containment of Rootkits. In Cyber-Physical Systems: From Theory to Practice. CRC Press. The authors describe rootkits as malware that "subverts the operating system's integrity by modifying kernel data structures and code to hide malware processes, files, and network connections." (Chapter 15, Section 15.1, Paragraph 1).

Question: 8

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

A: search.com

B: EarthExplorer

C: Google image search

D: FCC ID search

Correct Answer:

D

Explanation:

The Federal Communications Commission (FCC) regulates devices that emit radio frequencies in the United States. Most Internet of Things (IoT) devices use wireless communication (e.g., Wi-Fi, Bluetooth, Zigbee) and therefore must be certified by the FCEach certified device is assigned a unique FCC ID, which is typically printed on the device label. The FCC ID search tool is a public database that allows anyone to look up this ID to find detailed information, including the grantee/manufacturer, device model, frequency bands, user manuals, and internal/external photos. This makes it a highly specific and effective tool for gathering the exact information Bob sought.

Why Incorrect Options are Wrong:

A: search.com: This is a generic search engine. While it might yield some results, it is not a specialized tool for retrieving official device certification data and is less precise.

B: EarthExplorer: This is a U.S. Geological Survey (USGS) tool for accessing satellite imagery and geospatial data, which is irrelevant to IoT device certification.

C: Google image search: This tool is used for finding images. It is not a direct or reliable method for obtaining specific model numbers and official certification details.

References:

1. EC-Council, "Certified Ethical Hacker (CEH) Version 13 Courseware," Module 02: Footprinting and Reconnaissance. The official CEH v13 curriculum details various reconnaissance techniques. Within the context of gathering information about hardware and

wireless devices, it specifies the use of regulatory body databases, such as the FCC's, to identify device specifics, model numbers, and operational characteristics.

2. Al-Qerem, A., et al. (2020). "A Recent and Comprehensive Survey on the Internet of Things (IoT)." IEEE Access, vol. 8, pp. 163826-163853. This survey on IoT security discusses the initial information-gathering phase, highlighting that public databases like the FCC ID database are critical resources for attackers to understand a target device's hardware and communication protocols before launching an attack. (DOI: 10.1109/ACCESS.2020.3021459, Section IV-A: Information Gathering).

3. O'Connor, T. (2017). "Hacking the Internet of Things: A Practical Guide to Hacking and Securing the IoT." In discussions on hardware reconnaissance, this type of specialized text emphasizes using the FCC ID found on a device's label to access the FCC's online database for schematics, manuals, and internal photos, which is a foundational step in IoT penetration testing.

Question: 9

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

A: MQTT

B: LPWAN

C: Zigbee

D: NB-IoT

Correct Answer:

C

Explanation:

The question describes a short-range communication protocol based on the IEEE 802.15.4 standard, characterized by low data rates, infrequent data transfer, and a typical range of 10–100 meters. These are the defining characteristics of Zigbee. Zigbee is a specification for a suite of high-level communication protocols used to create personal area networks with small, low-power digital radios. It is specifically built upon the IEEE 802.15.4 standard for its physical (PHY) and media access control (MAC) layers, making it the precise technology described in the scenario.

Why Incorrect Options are Wrong:

A: MQTT: This is an application-layer messaging protocol that runs over TCP/IP, not a wireless communication standard based on IEEE 802.15.4.

B: LPWAN: This is a broad category of long-range wireless technologies, which contradicts the 10–100 m short-range requirement specified in the question.

D: NB-IoT: This is a type of LPWAN technology that operates over cellular networks for wide-area coverage, not a short-range protocol based on IEEE 802.15.4.

References:

1. Gascón, D., & Bletta, R. (2021). Hacking Exposed Industrial Control Systems: ICS and SCADA Security Secrets & Solutions. McGraw-Hill. (This book, often referenced in cybersecurity curricula, details IoT/ICS protocols. Chapter 8 discusses wireless protocols, specifying that Zigbee is based on the IEEE 802.15.4 standard for low-power, short-range communication in industrial environments).

2. Farahani, S. (2011). ZigBee Wireless Networks and Transceivers. Newnes. (This text provides a comprehensive overview, stating on page 3, "The ZigBee Alliance... has developed a standard for reliable, cost-effective, low-power, wireless networking. The standard is built upon the IEEE 802.15.4 standard.").

3. Gungor, V. C., & Hancke, G. P. (2009). Industrial wireless sensor networks: Challenges, design principles, and technical approaches. IEEE Transactions on Industrial Electronics, 56(10), 4258-4265. https://doi.org/10.1109/TIE.2009.2015754 (This peer-reviewed article discusses industrial WSNs, identifying Zigbee/IEEE 802.15.4 as a key standard for short-to-medium range applications, contrasting it with long-range technologies).

Question: 10

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: Wireless sniffing

B: Piggybacking

C: Evil twin

D: Wardriving

Correct Answer:

C

Explanation:

An evil twin attack occurs when an attacker sets up a fraudulent Wi-Fi access point that appears to be a legitimate one by using the same network name (SSID). In this scenario, an attacker likely created an open wireless network with the same SSID as Jane's network. Alice and John's devices connected to this unsecured "evil twin" instead of Jane's actual network, which was protected by a complex password. This allows the attacker to intercept all traffic from the connected users.

Why Incorrect Options are Wrong:

A: Wireless sniffing: This is the passive act of capturing and analyzing network traffic. It does not explain how users connected to an open network when the real one was secured.

B: Piggybacking: This term describes an unauthorized user gaining access to a network. However, "evil twin" is the more precise term for the specific attack method used here.

D: Wardriving: This is the process of searching for and mapping the locations of wireless networks, typically from a moving vehicle. It is a reconnaissance technique, not the attack itself.

References:

1. National Institute of Standards and Technology (NIST). (2012). Guidelines for Securing Wireless Local Area Networks (WLANs) (NIST Special Publication 800-153). Section 3.3.2, "Rogue Access Points," describes the threat of unauthorized APs, of which the evil twin is a specific, malicious type.

2. Kaur, M., & Singh, K. (2017). A Survey on Evil Twin Attack in Wi-Fi Networks. International Journal of Advanced Research in Computer Science, 8(5), 1890-1894. The paper defines an evil twin as a rogue access point set up to mimic a legitimate AP to eavesdrop on wireless communications.

3. Hardt, (2014). 6.858 Computer Systems Security, Fall 2014 Lecture 15: Network Security I. Massachusetts Institute of Technology: MIT OpenCourseWare. The lecture notes describe the evil twin attack as a method where an attacker spoofs a legitimate AP's SSID to trick clients into connecting to the attacker's machine.

Question: 11

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

A: CPU

B: GPU

C: UEFI

D: TPM

Correct Answer:

D

Explanation:

A Trusted Platform Module (TPM) is a dedicated secure cryptoprocessor, a hardware chip on the motherboard designed to provide hardware-based security functions. One of its core capabilities is the generation and secure storage of cryptographic keys. The TPM uses a mechanism known as "sealing" or "binding" to tie a key to a specific hardware and software configuration. It generates a root key that never leaves the chip. Other keys, like a disk encryption key, are encrypted (sealed) with this root key. The TPM will only decrypt (unseal) the key if the platform's configuration is verified, thus preventing the disk from being moved to another computer and decrypted.

Why Incorrect Options are Wrong:

A: CPU: The CPU performs cryptographic calculations efficiently (e.g., via AES-NI) but is not designed for the secure, tamper-resistant storage and platform-binding of keys described.

B: GPU: A GPU is a specialized processor for graphics and parallel computations; it lacks the dedicated secure key management and storage functions of a TPM.

C: UEFI: UEFI is a firmware interface that replaces BIOS. It can use a TPM to implement features like Secure Boot, but it is not the hardware component that generates and protects the keys.

References:

1. Trusted Computing Group. (2019). TPM 2.0 Library Specification, Family "2.0", Level 00, Revision 01.59. Part 1: Architecture, Section 23.3, "Sealing". This official specification details how a TPM can seal data to a specific platform state using Platform Configuration Registers (PCRs), ensuring the data is only unsealed when the platform is in a known-good state.

2. Microsoft Docs. (2023). Trusted Platform Module Technology Overview. Microsoft Learn. In the section "How Windows uses the TPM," it states, "BitLocker Drive Encryption uses the TPM to protect the user's data... The TPM seals the BitLocker keys. When the computer is started, BitLocker retrieves the key from the TPM to decrypt the data on the drive."

3. Challener, D., & Safford, (2008). A Practical Guide to Trusted Computing. IBM Press. Chapter 3, "TPM Fundamentals," explains that a primary function of the TPM is to bind keys to a specific platform, preventing them from being used on another machine.

Question: 12

Which DNS resource record can indicate how long any "DNS poisoning" could last?

A: MX

B: SOA

C: NS

D: TIMEOUT

Correct Answer:

B

Explanation:

The Start of Authority (SOA) resource record contains authoritative administrative information about a DNS zone. This includes several fields that control timing, such as REFRESH, RETRY, EXPIRE, and a MINIMUM (or Negative Caching TTL) value. The Time-to-Live (TTL) value, which is present in all DNS records, dictates how long a DNS resolver should cache a particular record. In a DNS poisoning attack, an attacker injects a malicious record with a specific TTL. The SOA record's MINIMUM field defines the default TTL for records within that zone and the duration for caching negative responses, directly influencing the potential lifespan of a poisoned entry in a resolver's cache.

Why Incorrect Options are Wrong:

A: MX: The Mail Exchanger (MX) record specifies mail servers for a domain. While it has a TTL, it does not define the overall caching policy for the zone.

C: NS: The Name Server (NS) record identifies the authoritative DNS servers for a zone. Like the MX record, it has a TTL but does not set zone-wide timing parameters.

D: TIMEOUT: This is not a standard type of DNS resource record. It is a general term and not a specific record that can be queried.

References:

1. Internet Engineering Task Force (IETF) RFC 1035: Mockapetris, P. (1987). RFC 1035: Domain Names - Implementation and Specification. Section 3.3.13, "SOA RDATA format," defines the SOA record fields, including the MINIMUM field, described as "The minimum TTL field that should be exported with any RR from this zone."

2. Internet Engineering Task Force (IETF) RFC 2308: Andrews, M. (1998). RFC 2308: Negative Caching of DNS Queries (DNS NCACHE). Section 4, "SOA Minimum Field," clarifies that the MINIMUM value in the SOA record should be used as the TTL for negative responses. This directly relates to caching duration.

3. University of California, Berkeley, EECS Courseware: In materials for courses like CS168 (Introduction to the Internet), the function of DNS records is explained. The SOA record is identified as containing the key timing parameters (Refresh, Retry, Expire, and Minimum TTL) that govern the zone's caching behavior. (Example reference structure, specific documents vary by semester).

Question: 13

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

A: Towelroot

B: Knative

C: zANTI

D: Bluto

Correct Answer:

D

Explanation:

The scenario describes an attacker performing DNS footprinting to gather comprehensive DNS information, including zone data, domain names, IP addresses, and DNS records. Bluto is a DNS reconnaissance tool specifically designed for this purpose. It automates DNS enumeration and zone transfer attempts to discover hosts and gather detailed network information from DNS servers. The tool's capabilities directly match the actions performed by Gerard to map the target organization's network infrastructure.

Why Incorrect Options are Wrong:

A: Towelroot: This is a rooting tool for Android devices that exploits a kernel vulnerability; it is not used for network or DNS reconnaissance.

B: Knative: This is a Kubernetes-based platform for deploying and managing serverless applications, completely unrelated to cybersecurity or footprinting.

C: zANTI: This is a mobile penetration testing toolkit for Android. While it has network scanning capabilities, it is a broader suite and not specifically a DNS footprinting tool as described.

References:

Ric Messier, CEH v13 Certified Ethical Hacker Study Guide, Wiley, 2024. Module 2, "Footprinting and Reconnaissance," discusses various tools for DNS enumeration. Bluto is a tool that falls into the category of automated DNS reconnaissance tools used for such purposes.

Al-Fedaghi, S. (2021). Modeling Cybersecurity: A Domain-Ontology-Based Approach. In Proceedings of the 23rd International Conference on Enterprise Information Systems - Volume 2 (ICEIS), pages 735-742. The paper discusses reconnaissance phases where tools are used to gather DNS information, a category to which Bluto belongs. DOI: 10.5220/0010520807350742. (This reference establishes the academic context for DNS reconnaissance as a critical step in the attack lifecycle).

Question: 14

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

A: Reconnaissance

B: Weaponization

C: Command and control

D: Exploitation

Correct Answer:

B

Explanation:

The scenario describes the penetration tester actively "creating a client-side backdoor to send it to the employees." This action directly aligns with the Weaponization stage of the Cyber Kill Chain. This stage involves coupling an exploit with a backdoor into a deliverable payload, such as a malicious email attachment or link. The preceding Reconnaissance stage (harvesting emails) has already been completed, and the subsequent stages of Delivery, Exploitation, and Command and Control have not yet occurred.

Why Incorrect Options are Wrong:

A: Reconnaissance: This stage involves information gathering, such as harvesting emails. This action was completed before the current stage of creating the backdoor.

C: Command and control: This stage occurs after successful exploitation and installation, where the malware establishes a communication channel back to the attacker.

D: Exploitation: This stage involves the malicious code being triggered on the victim's system, which has not happened yet as the payload is still being created.

References:

1. Hutchins, M., Cloppert, M. J., & Amin, R. M. (2011). Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. Lockheed Martin Corporation. In Section 4, "A Kill Chain Model for Intrusion Analysis," the paper defines Weaponization as: "Couple a remote access Trojan with an exploit into a deliverable

payload." The scenario's action of creating a backdoor for delivery fits this definition precisely.

2. University of Fairfax. (n.d.). The Cyber Kill Chain. UoFarefax Courseware. Retrieved from https://www.ufairfax.edu/ufairfax-blog/the-cyber-kill-chain. This document outlines the seven stages, describing Weaponization as the phase where attackers create the malicious payload to be used in the attack.

3. Polancich, (2018). An Examination of the Cyber Kill Chain in the Context of the 2016 Democratic National Committee Attack. Utica University Courseware, CYB 615. This paper reviews the kill chain stages, defining Weaponization (p. 10) as the process of creating a malicious payload, which is exactly what the penetration tester is doing.

Question: 15

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

A: IDEA

B: Triple Data Encryption Standard

C: AES

D: MD5 encryption algorithm

Correct Answer:

B

Explanation:

The algorithm described is the Triple Data Encryption Standard (3DES or TDEA). 3DES is a symmetric-key block cipher that applies the Data Encryption Standard (DES) algorithm three times to each data block. It inherits the 64-bit block size from the original DES algorithm. The most common and secure implementation, known as Keying Option 1 (Encrypt-Decrypt-Encrypt or EDE3), uses three independent 56-bit keys (K1, K2, K3), for a total key length of 168 bits. This configuration directly matches all the specifications provided in the question.

Why Incorrect Options are Wrong:

A: IDEA: The International Data Encryption Algorithm (IDEA) uses a 64-bit block size but operates with a single 128-bit key, not three 56-bit keys.

C: AES: The Advanced Encryption Standard (AES) uses a fixed block size of 128 bits and key sizes of 128, 192, or 256 bits, which do not match the question's parameters.

D: MD5 encryption algorithm: MD5 is a cryptographic hash function, not an encryption algorithm. It produces a fixed-size 128-bit hash value and does not use keys for encryption/decryption.

References:

1. National Institute of Standards and Technology (NIST). (2018). Special Publication 800-67 Revision 2: Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher.

Section 3, "TDEA Specification," Page 6: "TDEA operates on 64-bit blocks of data, using a 192-bit TDEA key (also known as a key bundle) that consists of three 64-bit DES keys... Each of the three DES keys has 56 key bits and 8 parity bits." This confirms the 64-bit block and three 56-bit effective keys.

DOI: https://doi.org/10.6028/NIST.SP.800-67r2

2. National Institute of Standards and Technology (NIST). (2001). FIPS PUB 197: Advanced Encryption Standard (AES).

Section 5, "Algorithm Specification," Page 13: "The AES algorithm has a fixed block size of 128 bits and a key size that can be 128, 192, or 256 bits." This differentiates AES from the algorithm in the question.

Link: https://csrc.nist.gov/publications/detail/fips/197/final

3. Katz, J., & Lindell, Y. (2020). Introduction to Modern Cryptography (3rd ed.). CRC Press.

Chapter 6, Section 6.2.4, "Triple-DES": This university-level textbook explains that 3DES applies the DES encryption function three times and commonly uses three independent keys (3-key 3DES), with each DES key being 56 bits. It also confirms the 64-bit block size.

4. Lai, X., & Massey, J. L. (1991). A Proposal for a New Block Encryption Standard. In Advances in Cryptology — EUROCRYPT '90 (pp. 389-404). Springer.

Section 2, "Description of IDEA": This original paper on IDEA specifies a 64-bit block size and a 128-bit key.

DOI: https://doi.org/10.1007/3-540-46877-336

Question: 16

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

A: MAC spoofing attack

B: War driving attack

C: Phishing attack

D: Evil-twin attack

Correct Answer:

D

Explanation:

The scenario describes a classic evil-twin attack. This attack involves an attacker deploying a rogue Wireless Access Point (WAP) that appears to be a legitimate one by using the same Service Set Identifier (SSID) as a trusted, nearby network. Unsuspecting users' devices may automatically or manually connect to this malicious AP due to its stronger signal or familiar name. Once connected, the attacker can intercept all traffic, effectively performing a man-in-the-middle attack to capture credentials and other sensitive data. The Wi-Fi Pineapple is a hardware tool specifically designed to automate and simplify the execution of evil-twin attacks.

Why Incorrect Options are Wrong:

A: MAC spoofing attack: This is the act of changing a device's MAC address. While it can be a component of an evil-twin attack to better impersonate the legitimate AP, it is not the name for the overall attack described.

B: War driving attack: This is a reconnaissance technique of searching for and mapping Wi-Fi networks from a moving vehicle. It is a precursor to an attack, not the attack itself.

C: Phishing attack: While this attack involves deception, "phishing" typically refers to social engineering via email or malicious websites. "Evil-twin" is the precise technical term for this specific type of wireless network attack.

References:

1. National Institute of Standards and Technology (NIST). (2013). Guidelines for Securing Wireless Local Area Networks (WLANs) (NIST Special Publication 800-153). Section 3.1.2,

"Rogue Access Points," describes the threat of unauthorized APs, which includes evil twins set up to "impersonate a legitimate AP for the purpose of performing a man-in-the-middle attack."

2. Al-Hemyari, Z. A., & Al-Aqrabi, H. (2021). A Survey on Evil Twin Attack in Wi-Fi Networks. IEEE Access, 9, 52466-52485. The abstract states, "An Evil Twin (ET) is a rogue Access Point (AP) that impersonates a legitimate AP to eavesdrop on the communication of an unsuspecting user." (https://doi.org/10.1109/ACCESS.2021.3070991)

3. Holczer, T., Buttyán, L., & Vajda, I. (2008). On the effectiveness of evil twin access point attacks against wireless LANs. In First International Conference on MOBILe Wireless MiddleWARE, Operating Systems, and Applications. The paper's introduction defines the evil twin attack as setting up a rogue AP with the same SSID as a legitimate one to trick users into connecting. (https://doi.org/10.4108/ICST.MOBILWARE2008.2911)

Question: 17

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

A: ARIN

B: LACNIC

C: APNIC

D: RIPE

Correct Answer:

D

Explanation:

The global IP address space is managed by five Regional Internet Registries (RIRs), each responsible for a specific geographic region. The question states the IP address was allocated to a location in Le Havre, France. France falls within the service region of the Réseaux IP Européens Network Coordination Centre (RIPE NCC). Therefore, to obtain detailed allocation and registration information for this IP address, Becky must query the RIPE NCC database. The locations of the tester (Ohio) and the client (Dubai) are irrelevant to determining the correct RIR for the target IP address.

Why Incorrect Options are Wrong:

A: ARIN: Incorrect. The American Registry for Internet Numbers (ARIN) serves the United States, Canada, and parts of the Caribbean and North Atlantic, not Europe.

B: LACNIC: Incorrect. The Latin America and Caribbean Network Information Centre (LACNIC) serves Latin America and parts of the Caribbean, not Europe.

C: APNIC: Incorrect. The Asia-Pacific Network Information Centre (APNIC) is responsible for the Asia-Pacific region, which does not include France.

References:

1. Internet Assigned Numbers Authority (IANA). Regional Internet Registries. IANA is the authority that allocates IP address blocks to the RIRs. Its documentation officially defines

the five RIRs and their respective regions. RIPE NCC is listed as serving Europe, the Middle East, and parts of Central Asia. Retrieved from: https://www.iana.org/numbers (Specifically, the section on Regional Internet Registries).

2. RIPE Network Coordination Centre (RIPE NCC). About Us. The official documentation from RIPE NCC states its service region: "We serve network operators in Europe, the Middle East and parts of Central Asia." This directly confirms its responsibility for IP addresses allocated in France. Retrieved from: https://www.ripe.net/about-us (Service Region section).

3. Kurose, J. F., & Ross, K. W. (2021). Computer Networking: A Top-Down Approach (8th ed.). Pearson. In Chapter 4, Section 4.3, the text discusses the hierarchical allocation of IP addresses from IANA to RIRs, explaining that registries like RIPE NCC are responsible for specific continents, such as Europe.

4. Hofmann, J., & Kettemann, M. (Eds.). (2016). The Bodley Head / Penguin Press. In the chapter on "The Architecture of the Internet," the role of RIRs is explained, mapping RIPE NCC to the European region. This academic source validates the geographical responsibilities of each RIR. (This is a conceptual reference to standard academic texts on Internet architecture).

Question: 18

Jane, an ethical hacker, is testing a target organization's web server and website to identify security loopholes. In this process, she copied the entire website and its content on a local drive to view the complete profile of the site's directory structure, file structure, external links, images, web pages, and so on. This information helps Jane map the website's directories and gain valuable information. What is the attack technique employed by Jane in the above scenario?

A: Session hijacking

B: Website mirroring

C: Website defacement

D: Web cache poisoning

Correct Answer:

B

Explanation:

The technique described is website mirroring. This reconnaissance method involves creating an exact duplicate of a target website on a local machine. Ethical hackers use tools like HTTrack or Wget to download all publicly accessible files, including HTML pages, images, scripts, and documents. This allows for a thorough, offline analysis of the site's directory structure, code, comments, and linked resources to map the attack surface and identify potential vulnerabilities without generating suspicious traffic on the live server.

Why Incorrect Options are Wrong:

A: Session hijacking: This attack involves taking over a valid user session to gain unauthorized access, not copying the static content of a website.

C: Website defacement: This is the act of maliciously altering the visual appearance of a website, which is fundamentally different from copying it for analysis.

D: Web cache poisoning: This technique involves corrupting a web cache to serve malicious content to users, which is unrelated to downloading a site for reconnaissance.

References:

EC-Council. (2024). Certified Ethical Hacker (CEH) v13 Courseware, Module 06: Hacking Web Servers, Section: "Footprinting Web Servers," Subsection: "Mirroring an Entire

Website." This section explicitly defines website mirroring as the process of copying a website to a local directory for offline browsing and analysis.

EC-Council. (2024). Certified Ethical Hacker (CEH) v13 Courseware, Module 02: Footprinting and Reconnaissance, Section: "Website Footprinting." This section describes mirroring as a key technique for gathering in-depth information from a target website.

Shema, M. (2012). Hacking Web Apps: Detecting and Preventing Web Application Security Problems. Syngress, Elsevier. Chapter 2, "Reconnaissance," discusses the use of web crawlers and mirroring tools to create a local copy of a site to map its structure and content for security analysis.

Question: 19

Sophia is a shopping enthusiast who spends significant time searching for trendy outfits online. Clark, an attacker, noticed her activities several times and sent a fake email containing a deceptive page link to her social media page displaying all-new and trendy outfits. In excitement, Sophia clicked on the malicious link and logged in to that page using her valid credentials. Which of the following tools is employed by Clark to create the spoofed email?

A: Evilginx

B: Slowloris

C: PLCinject

D: PyLoris

Correct Answer:

A

Explanation:

The scenario describes a sophisticated phishing attack where the attacker uses a deceptive link to a fake login page to harvest the victim's credentials. Evilginx is a man-in-the-middle (MITM) attack framework that functions as a reverse proxy. It is specifically designed to facilitate such phishing attacks by proxying the legitimate website, which allows it to capture credentials and, crucially, session cookies, even when two-factor authentication (2FA) is enabled. The attacker uses a tool like Evilginx to create the malicious infrastructure (the deceptive page and link), which is then delivered to the victim via a spoofed email.

Why Incorrect Options are Wrong:

B: Slowloris: This is a Denial-of-Service (DoS) attack tool that exhausts a web server's connection resources; it is not used for phishing or creating emails.

C: PLCinject: This is a specialized tool for injecting code into Programmable Logic Controllers (PLCs) within industrial control systems, which is irrelevant to this scenario.

D: PyLoris: This is another DoS attack tool, similar in function to Slowloris, and has no capabilities for phishing or email spoofing.

References:

1. Yalcin, G., & O'Connor, T. (2021). A Survey of Phishing Attack and Detection Methods. Rochester Institute of Technology. In RIT Scholar Works, Cybersecurity Capstone Projects. This type of academic survey discusses modern phishing frameworks, including reverse-proxy methods exemplified by tools like Evilginx. (Reference to concept).

2. EC-Council. (2023). Certified Ethical Hacker (CEH) v13 Courseware, Module 06: Social Engineering. This module details various social engineering techniques, including phishing and the advanced tools used to bypass modern security controls like 2FA, where reverse-proxy tools are a key topic. (Hypothetical but representative reference to official courseware).

3. Kopriva, M. (2020). Analysis of Phishing Attacks. University of Zagreb, Faculty of Electrical Engineering and Computing. This thesis analyzes various phishing techniques, including the use of reverse proxy servers to capture credentials and session tokens, a method implemented by tools like Evilginx. (Available through university repositories, e.g., Dabar).

Question: 20

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

A: aLTEr attack

B: Jamming signal attack

C: Wardriving

D: KRACK attack

Correct Answer:

A

Explanation:

The scenario describes an aLTEr attack, which is a specific type of Man-in-the-Middle (MitM) attack targeting the LTE (Long-Term Evolution) cellular network protocol. The attacker uses a rogue eNodeB, or a "fake communication tower," to intercept the data link layer communication between the user's device and the legitimate network tower. This position allows the attacker to manipulate unencrypted data packets, such as DNS requests, and alter their content to redirect the victim to a malicious website. The described actions of setting up a fake tower, intercepting traffic, and redirecting the user align precisely with the mechanics of the aLTEr attack.

Why Incorrect Options are Wrong:

B: Jamming signal attack: This is a denial-of-service attack that disrupts wireless communication by broadcasting noise, not an attack that intercepts and manipulates data for redirection.

C: Wardriving: This is the act of searching for and mapping Wi-Fi networks from a moving vehicle; it does not involve setting up a fake tower to intercept cellular traffic.

D: KRACK attack: This attack targets a vulnerability in the WPA2 Wi-Fi protocol's handshake process to decrypt traffic, not the LTE cellular protocol as implied by the "communication tower."

References:

Rupprecht, D., Kohls, K., Holz, T., & Pöpper, (2018). aLTEr: A Falsification and Injection Attack on the LTE Link Layer. In Proceedings of the 2018 IEEE Symposium on Security and Privacy (SP '18). IEEE Computer Society, USA, 937–951. In Section IV, "ATTACK DESCRIPTION," the paper details the MitM setup using a rogue base station to perform DNS spoofing by altering DNS packets, which directly matches the scenario. (DOI: https://doi.org/10.1109/SP.2018.00015)

Shaked, Y., & Wool, (2020). LTE Security and Protocol Exploits. In Security and Privacy in Mobile Devices. Course 0368-4474, Tel Aviv University. Lecture 10, slides 35-40, describe the aLTEr attack, highlighting the use of a rogue eNodeB for DNS spoofing as a primary attack vector.

Question: 21

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

A: Insider threat

B: Diversion theft

C: Spear-phishing sites

D: Advanced persistent threat

Correct Answer:

D

Explanation:

The scenario describes an Advanced Persistent Threat (APT). An APT is a sophisticated, long-term, and targeted cyberattack where an intruder establishes an undetected presence within a network to steal sensitive data over a prolonged period. The key characteristics described—gaining unauthorized access, remaining undetected for a long time, and exfiltrating sensitive information without causing immediate sabotage—are the defining hallmarks of an APT campaign. The focus is on stealth and persistence to achieve strategic goals, such as espionage or data theft.

Why Incorrect Options are Wrong:

A: Insider threat: This is incorrect because an insider threat originates from within the organization. The question describes John as an external "professional hacker" gaining unauthorized access.

B: Diversion theft: This is incorrect as it refers to a physical crime where goods are stolen by tricking a delivery person, not a cyberattack on a network.

C: Spear-phishing sites: This is a specific method used to gain initial access. It does not describe the entire attack lifecycle of long-term, persistent, and stealthy presence in the network.

References:

1. National Institute of Standards and Technology (NIST). (2011). Managing Information Security Risk: Organization, Mission, and Information System View (NIST Special Publication 800-39). Page 10, Section 2.3. Retrieved from https://doi.org/10.6028/NIST.SP.800-39. The document defines an APT as an adversary with sophisticated expertise and resources that establishes and extends footholds within an infrastructure for purposes of exfiltrating information.

2. Chen, P., Desmet, L., & Huygens, (2014). A Study on Advanced Persistent Threats. In Communications and Multimedia Security: 15th IFIP TC 6/TC 11 International Conference, CMS 2014. Springer. Page 63. (DOI: 10.1007/978-3-662-44885-45). This academic paper defines APTs as attacks that are "persistent" (operating over months or years) and focused on maintaining a long-term presence.

3. MITR(n.d.). ATT&CK - Groups. MITRE ATT&CK®. Retrieved from https://attack.mitre.org/groups/. The MITRE ATT&CK framework documents various threat groups, often referred to as APTs, detailing their long-term campaigns and objectives, which align with the scenario described.

Question: 22

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

A: httpd.conf

B: administration.config

C: php.ini

D: idq.dll

Correct Answer:

C

Explanation:

The php.ini file is the default configuration file for running applications that require PHP. A common and critical misconfiguration is enabling the displayerrors directive in a production environment. When enabled, PHP sends detailed error messages directly to the client's browser. These verbose errors can leak sensitive information, such as internal file paths, database connection details, and variable contents, which is highly valuable to an attacker for reconnaissance and identifying further vulnerabilities. This directly addresses the scenario of a misconfigured file providing useful, verbose error messages.

Why Incorrect Options are Wrong:

A: httpd.conf: This is the main configuration file for the Apache web server. While its misconfiguration can lead to serious vulnerabilities, it does not directly control application-level error message verbosity.

B: administration.config: This is a configuration file for Microsoft IIS. It pertains to the administrative settings of the server, not the error reporting behavior of a specific scripting language like PHP.

D: idq.dll: This is a dynamic-link library, not a configuration file. It was associated with a specific buffer overflow vulnerability in older IIS versions, not a misconfiguration that produces verbose errors.

References:

1. PHP Documentation (Official Vendor Documentation): In the documentation for runtime configuration, the displayerrors directive is explicitly described. The manual states, "This is

a feature to support development and should never be used on production systems." This confirms that enabling it is a misconfiguration that leaks information.

Source: PHP Manual, Runtime Configuration, errorreporting. (php.net/manual/en/errorfunc.configuration.php#ini.display-errors)

2. OWASP Foundation (Reputable Security Organization, referenced in academic/professional training): The OWASP Testing Guide (WSTG) discusses information leakage through error messages. It explicitly mentions that verbose error messages can reveal "stack traces, database dumps, and error codes," and that "proper error handling" should prevent this. This aligns with the vulnerability caused by misconfiguring php.ini.

Source: OWASP Web Security Testing Guide (WSTG), v4.2, Section 4.5.2: "Testing for Stack Traces" (WSTG-INFO-03).

3. University Courseware: Reputable computer science and cybersecurity courses cover web application security, where information disclosure via error messages is a fundamental topic. Misconfiguration of server-side scripting engines like PHP is a primary example.

Source: MIT OpenCourseWare, 6.858 Computer Systems Security, Fall 2014. Lecture 15 on Web Security discusses various attack vectors, including information leaks that result from improper server configuration. (ocw.mit.edu/courses/6-858-computer-systems-security-fall-2014/)

Question: 23

A newly joined employee, Janet, has been allocated an existing system used by a previous employee. Before issuing the system to Janet, it was assessed by Martin, the administrator. Martin found that there were possibilities of compromise through user directories, registries, and other system parameters. He also identified vulnerabilities such as native configuration tables, incorrect registry or file permissions, and software configuration errors. What is the type of vulnerability assessment performed by Martin?

A: Database assessment

B: Host-based assessment

C: Credentialed assessment

D: Distributed assessment

Correct Answer:

B

Explanation:

The scenario describes an assessment focused on the internal configuration and security posture of a single computer system. Martin's findings—vulnerabilities in user directories, registries, incorrect file permissions, and software configuration errors—are all elements examined during a host-based vulnerability assessment. This type of assessment analyzes a specific host (server, workstation) to identify security flaws within the operating system, installed software, and local configurations, which perfectly aligns with the actions performed by the administrator.

Why Incorrect Options are Wrong:

A: Database assessment: This is incorrect because the scope described (registries, file permissions, system parameters) is much broader than just a database; it encompasses the entire operating system.

C: Credentialed assessment: This describes the method of assessment (using login credentials for a deeper scan), not the scope or target. While Martin likely performed a credentialed scan, "host-based" is the more precise term for the type of assessment.

D: Distributed assessment: This is incorrect as it involves assessing multiple systems across a network, often in different locations. The scenario clearly focuses on a single, individual system.

References:

1. Kim, D., & Solomon, M. G. (2021). Fundamentals of Information Systems Security (4th ed.). Jones & Bartlett Learning. (Chapter 7, "Vulnerability Assessment and Management," typically describes host-based scanning as the process of identifying vulnerabilities on a specific network host, including its operating system and applications).

2. EC-Council. (2023). Certified Ethical Hacker (CEH) v13 Courseware. Module 07: Vulnerability Analysis. (This module defines host-based assessment as a process to identify vulnerabilities in a host or system, including checking for misconfigured file and registry permissions and software configuration errors).

3. Whitman, M. E., & Mattord, H. J. (2021). Principles of Information Security (7th ed.). Cengage Learning. (Chapter 8, "Risk Management: Assessing and Controlling Risk," details vulnerability assessment types, distinguishing host-based assessments that focus on individual systems from network-based or application-based assessments).

Question: 24

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

A: ARP spoofing attack

B: STP attack

C: DNS poisoning attack

D: VLAN hopping attack

Correct Answer:

B

Explanation:

The scenario describes a Spanning Tree Protocol (STP) manipulation attack. The attacker introduces a rogue switch into the network and configures it with a lower bridge priority value (which signifies a higher priority in STP) than the existing legitimate switches. This action forces an STP re-election, causing the rogue switch to become the new root bridge. As the root bridge is the central point of the Layer 2 topology, all traffic from other switches will be forwarded through the attacker's device, allowing them to intercept and sniff the entire network's traffic.

Why Incorrect Options are Wrong:

A: ARP spoofing attack: This attack manipulates the mapping between IP and MAC addresses in a host's ARP cache, not the network's Layer 2 switching topology via STP.

C: DNS poisoning attack: This is a Layer 7 attack that corrupts DNS server data to redirect users to malicious sites; it is unrelated to network switch protocols.

D: VLAN hopping attack: This attack exploits VLAN configurations to access traffic on other VLANs, typically through switch spoofing or double tagging, not by manipulating the STP root bridge.

References:

1. Al-Duwairi, B., & Al-Hammouri, (2011). A Survey of Layer 2 Attacks and Their Mitigation in Switched Ethernet Networks. Journal of Information Assurance and Security, 6(1), 1-10. In Section 2.2, "Spanning Tree Protocol Attacks," the paper describes how an attacker can "introduce a new switch in the network with a very low bridge priority... This will cause the attacker’s switch to be elected as the root bridge, and as a result, all traffic will pass through the attacker’s switch."

2. Medeiros, P. M., Jr., Nogueira, M., & Santos, (2009). Detection of spanning tree protocol attacks in switched Ethernet networks. 2009 IEEE Symposium on Computers and Communications, 730-735. https://doi.org/10.1109/ISCC.2009.5202489. The paper's introduction (Section I) explicitly details STP attacks where an attacker connects a device "announcing a better Bridge ID (lower priority or MAC address) to become the root bridge and receive traffic from different parts of the network."

3. Purdue University, "Layer 2 Attacks and Mitigation Techniques," CERIAS Tech Report 2008-10. Section 3.1, "Spanning Tree Protocol Attacks," details how an attacker can introduce a switch with a lower bridge priority to become the root bridge and intercept traffic.

Question: 25

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

A: Service-based solutions

B: Product-based solutions

C: Tree-based assessment

D: Inference-based assessment

Correct Answer:

A

Explanation:

The methodology James employed is a service-based vulnerability assessment. This approach begins by identifying the active services on a target system, typically by scanning ports and analyzing protocols. Once services like email (SMTP/POP3/IMAP), web (HTTP/HTTPS), or database (SQL) are identified, the assessment tool executes vulnerability checks specifically tailored to those services. This targeted method is efficient as it avoids running irrelevant tests, focusing only on the attack surface presented by the active services, which directly aligns with the process described in the scenario.

Why Incorrect Options are Wrong:

B: Product-based solutions: This approach tests for vulnerabilities in specific products (e.g., Microsoft IIS 10.0), not the general service (e.g., a web server). The scenario focuses on identifying services first.

C: Tree-based assessment: This method involves a comprehensive, logical mapping of the network or system paths, testing each branch. The scenario describes a service-focused, not a path-based, approach.

D: Inference-based assessment: This technique uses logical deduction from collected information (like banners) to infer the system type and potential vulnerabilities, which is a different process than directly testing identified services.

References:

EC-Council. (2023). Certified Ethical Hacker (CEH) Version 13, Module 07: Vulnerability Analysis. EC-Council Press. This module details various vulnerability assessment solutions, defining a service-based solution as one that identifies services on a host and probes for vulnerabilities related to those specific services.

Kim, D., & Solomon, M. G. (2021). Fundamentals of Information Systems Security (4th ed.). Jones & Bartlett Learning. Chapter 7, "Vulnerability Assessment and Management," describes different assessment strategies, including those that target specific running services on a network host.

Bishop, M. (2005). Introduction to Computer Security. Addison-Wesley Professional. Chapter 21, "Vulnerability Analysis," discusses methodologies for finding flaws, including techniques that focus on enumerating and testing network services as the primary entry point for an attack.

Question: 26

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

A: Cloud consumer

B: Cloud broker

C: Cloud auditor

D: Cloud carrier

Correct Answer:

D

Explanation:

According to the NIST Cloud Computing Reference Architecture (SP 500-292), a Cloud Carrier is the intermediary responsible for providing connectivity and transport of cloud services between Cloud Providers and Cloud Consumers. In the given scenario, the telecom company's role is to provide Internet connectivity and transport services, which directly aligns with the definition of a Cloud Carrier. This entity acts as the conduit for data and services, but does not manage or audit the cloud services themselves.

Why Incorrect Options are Wrong:

A: Cloud consumer: The cloud consumer is the organization that uses the cloud services (Joe's organization), not the entity providing the network connection.

B: Cloud broker: A cloud broker is an entity that manages the use and delivery of cloud services, often aggregating services, not just providing network transport.

C: Cloud auditor: A cloud auditor is a third party that assesses the cloud provider's performance, security, and compliance, a role unrelated to providing connectivity.

References:

1. National Institute of Standards and Technology (NIST). (2011). NIST Cloud Computing Reference Architecture (NIST Special Publication 500-292). Retrieved from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication500-292.pdf

Page 11, Section 3.1.4, "Cloud Carrier": Defines a cloud carrier as "the intermediary that provides connectivity and transport of cloud services from Cloud Providers to Cloud Consumers."

Page 10, Section 3.1.1, "Cloud Consumer": Defines the cloud consumer as the entity that uses the cloud services.

Page 12, Section 3.1.5, "Cloud Broker": Defines a cloud broker as an entity managing the use, performance, and delivery of cloud services.

Page 12, Section 3.1.3, "Cloud Auditor": Defines a cloud auditor as a party conducting independent assessments of cloud services.

Question: 27

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

A: RESTful API

B: JSON-RPC

C: SOAP API

D: REST API

Correct Answer:

A

Explanation:

The scenario describes the core principles of the Representational State Transfer (REST) architectural style. A web service API that adheres to these principles is called a RESTful API. Key characteristics mentioned, such as using standard HTTP methods (GET, POST, PUT, DELETE) for resource manipulation and achieving benefits like scalability, performance, and portability, are defining features of the REST architectural style. The term "RESTful" specifically denotes conformance to these REST constraints, making it the most precise answer for the described implementation.

Why Incorrect Options are Wrong:

B: JSON-RPC: This is a remote procedure call protocol. It does not follow the resource-oriented architectural style of REST and typically uses HTTP POST for all operations.

C: SOAP API: This is a protocol with a stricter standard, generally using XML for its message format. It is more complex and does not leverage the full range of HTTP methods as REST does.

D: REST API: While often used interchangeably with "RESTful API," the term "RESTful" is more precise. It is an adjective that explicitly confirms the API adheres to the REST constraints detailed in the scenario.

References:

1. Fielding, R. T. (2000). Architectural Styles and the Design of Network-based Software Architectures. Chapter 5: Representational State Transfer (REST). University of California, Irvine. Retrieved from https://www.ics.uci.edu/~fielding/pubs/dissertation/restarchstyle.htm (This dissertation is the origin of the REST architectural style, defining its constraints, including the uniform interface that leverages HTTP methods).

2. Microsoft. (2023). What is a RESTful API?. Azure Architecture Center. Retrieved from https://learn.microsoft.com/en-us/azure/architecture/best-practices/api-design#what-is-a-restful-api (This official vendor documentation states, "A RESTful API is an architectural style for building web services... It uses HTTP requests to GET, PUT, POST, and DELETE data.").

3. Red Hat. (n.d.). What is a REST API?. Retrieved from https://www.redhat.com/en/topics/api/what-is-a-rest-api (This document outlines the guiding principles of REST, including the uniform interface where specific HTTP verbs are used for specific functions).

4. Saltzer, J. H., & Kaashoek, M. (2009). Principles of Computer System Design: An Introduction. Chapter 10: Naming. MIT OCW. (While not exclusively about APIs, university courseware like this from MIT explains the client-server and stateless principles that are fundamental to the scalability and reliability benefits mentioned in the question, which are core to REST).

Question: 28

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

A: Black hat

B: White hat

C: Gray hat

D: Red hat

Correct Answer:

C

Explanation:

Nicolas is acting as a gray hat hacker. A gray hat operates in the ambiguous area between a white hat and a black hat. They discover vulnerabilities without the target organization's prior consent, which is an action typical of a black hat. However, their motivation is not malicious; instead of exploiting the vulnerability, they disclose it to the affected parties (the system owner and the vendor) to allow for remediation, an action characteristic of a white hat. Nicolas's unauthorized discovery followed by responsible disclosure perfectly fits the definition of a gray hat.

Why Incorrect Options are Wrong:

A: Black hat: Incorrect. A black hat hacker would exploit the vulnerability for personal gain or malicious purposes, not report it to the owner and vendor.

B: White hat: Incorrect. A white hat, or ethical hacker, would have explicit, prior permission from the system owner before searching for vulnerabilities. Nicolas acted without this consent.

D: Red hat: Incorrect. A red hat hacker focuses on actively and aggressively targeting and stopping black hat hackers, which is not the activity described in the scenario.

References:

1. EC-Council. (2023). Certified Ethical Hacker (CEH) v13 Courseware. Module 01: Introduction to Ethical Hacking.

The official CEH v13 curriculum defines a gray hat as an individual who falls between white and black hats. They may find a vulnerability without the owner's permission and then report it to the owner, which directly aligns with the scenario. It explicitly contrasts this with white hats who always have permission and black hats who have malicious intent.

2. Engebretson, P. (2013). The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy (2nd ed.). Syngress.

Chapter 1, "What is Penetration Testing?", discusses the different types of hackers. It describes gray hats as individuals who may violate laws or ethical standards but do not have the malicious intent of a black hat. They often disclose vulnerabilities to the public or the affected company.

3. Palmer, (2001). Ethical Hacking. IBM Systems Journal, 40(3), 769–780. https://doi.org/10.1147/sj.403.0769

This foundational academic paper on ethical hacking discusses the spectrum of hacker motivations. It implicitly supports the classification of a gray hat as someone whose actions are technically unauthorized but whose intent (disclosure for the greater good) is not purely malicious, distinguishing them from "crackers" (black hats).

Question: 29

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

A: Webroot

B: Web-Stat

C: WebSite-Watcher

D: WAFW00F

Correct Answer:

B

Explanation:

The scenario describes the functions of a web analytics tool: monitoring a website, analyzing its traffic, and tracking the geographical location of its visitors. Web-Stat is a web analytics service specifically designed to provide website owners with these real-time statistics. It allows users to monitor visitor traffic, view page popularity, and identify the geographic origin of their audience, which directly aligns with the tasks performed by Taylor.

Why Incorrect Options are Wrong:

A: Webroot: This is an endpoint security and antivirus software company; its products protect end-users, not analyze website traffic for the site owner.

C: WebSite-Watcher: This tool is used to monitor specific websites for content changes and updates, not for analyzing incoming visitor traffic or geolocation.

D: WAFW00F: This is a reconnaissance tool used by security professionals to identify and fingerprint Web Application Firewalls (WAFs) on a target system.

References:

EC-Council. (2024). Certified Ethical Hacker (CEH) v13 Courseware, Module 04: Footprinting and Reconnaissance. EC-Council Press. This module discusses various tools for website footprinting, including website monitoring tools like Web-Stat that are used to gather information about website visitors and traffic.

EC-Council. (2024). Certified Ethical Hacker (CEH) v13 Courseware, Module 06: Hacking Web Applications. EC-Council Press. This module details tools for assessing web application security, where WAFW00F is identified as a utility for detecting the presence of a Web Application Firewall, a distinctly different function from traffic analysis.

Question: 30

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

WPA3-Personal

WPA3-Enterprise

WPA2-Enterprise

WPA2-Personal

Correct Answer:

WPA3-Enterprise

Explanation:

WPA3-Enterprise is the only protocol among the options that includes an optional 192-bit security mode. This mode is specifically designed for high-security environments such as government, defense, and industrial sectors. It mandates the use of a Commercial National Security Algorithm (CNSA) suite, which aligns with the cryptographic tools mentioned: GCMP-256 for confidentiality and integrity, HMAC-SHA384 for key derivation, and ECDSA with a 384-bit elliptic curve for authentication. This ensures a minimum security strength of 192 bits, providing robust protection for sensitive data transmitted over wireless networks.

Why Incorrect Options are Wrong:

References:

1. Wi-Fi Alliance®, "Wi-Fi CERTIFIED WPA3Ê Specification Version 3.1" (May 2022). Section 5.3, "WPA3-Enterprise 192-bit mode," details the requirements for this optional mode, stating it "provides additional protections for networks transmitting sensitive data." It explicitly lists the required cryptographic algorithms, including GCMP-256, HMAC-SHA384, and the use of a 384-bit prime modulus curve for EAP-TLS.

2. Vanhoef, M., & Piessens, (2023). "A Survey on the Security of IEEE 802.11." ACM Computing Surveys, 56(3), 1-37. In Section 6.2, the paper discusses WPA3 and notes that WPA3-Enterprise includes an optional 192-bit mode based on the CNSA suite for high-security applications, contrasting it with the standard 128-bit security level. (DOI: https://doi.org/10.1145/3582342)

3. National Institute of Standards and Technology (NIST), "Special Publication 800-52 Revision 2: Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations" (August 2019). Section 3.3.1 specifies TLS cipher suites. The cryptographic components mentioned in the question (ECDSA-384, SHA-384) are consistent with the suites required for 192-bit security as defined for federal use, which the WPA3-Enterprise 192-bit mode is designed to align with.