- **Vendor: EC-Council**
- **Exam Code: 312-50v12**
- **Exam Name: Certified Ethical Hacker Exam (CEH v12)**
- **New Updated Questions from Braindump2go (Updated in August/2023)**

QUESTION 62
After an audit, the auditors inform you that there is a critical finding that you must tackle immediately. You read the audit report, and the problem is the service running on port 389.
Which service is this and how can you tackle the problem?

A. The service is NTP, and you have to change it from UDP to TCP in order to encrypt it.
B. The service is LDAP, and you must change it to 636, which is LDAPS.
C. The findings do not require immediate actions and are only suggestions.
D. The service is SMTP, and you must change it to SMIME, which is an encrypted way to send emails.

Answer: B
Explanation:
The service running on port 369 is Lightweight Directory Access Protocol (LDAP). LDAP is a protocol used to access and manage directory information, such as user accounts and passwords. LDAP is typically used over UDP port 389, but it can also be used over TCP port 369.
The auditors have found that the LDAP service on your network is running over UDP port 369. This is a security risk because UDP is a connectionless protocol, which means that packets can be lost or corrupted. If an attacker is able to intercept an LDAP packet, they could potentially steal user credentials or other sensitive information.
To address this security risk, you should change the LDAP service to run over TCP port 636. TCP is a connection-oriented protocol, which means that packets are guaranteed to be delivered. LDAPS is a secure version of LDAP that uses Transport Layer Security (TLS) to encrypt the communication between the client and server.

QUESTION 63
Mike, a security engineer, was recently hired by BigFox Ltd. The company recently experienced disastrous DoS attacks. The management had instructed Mike to build defensive strategies for the company's IT infrastructure to thwart DoS/DDoS attacks. Mike deployed some countermeasures to handle jamming and scrambling attacks.
What is the countermeasure Mike applied to defend against jamming and scrambling attacks?

A. Allow the transmission of all types of addressed packets at the ISP level
B. Disable TCP SYN cookie protection
C. Allow the usage of functions such as gets and strcpy
D. Implement cognitive radios in the physical layer

Answer: D
Explanation:
Cognitive radios can sense the environment, sense other RF devices' signals, and use different frequencies in response to the sensing results. This makes the device very flexible in terms of being able to adjust to different environments and also to be able to detect and evade jamming or scrambling attacks. By deploying cognitive radios, Mike can mitigate the effects of DoS/DDoS attacks that use jamming or scrambling techniques.

QUESTION 64

You are using a public Wi-Fi network inside a coffee shop. Before surfing the web, you use your VPN to prevent intruders from sniffing your traffic.
If you did not have a VPN, how would you identify whether someone is performing an ARP spoofing attack on your laptop?

A. You should check your ARP table and see if there is one IP address with two different MAC addresses.
B. You should scan the network using Nmap to check the MAC addresses of all the hosts and look for duplicates.
C. You should use netstat to check for any suspicious connections with another IP address within the LAN.
D. You cannot identify such an attack and must use a VPN to protect your traffic.

Answer: A
Explanation:
ARP spoofing is a type of attack where an attacker sends fake ARP (Address Resolution Protocol) messages to associate their MAC address with the IP address of another host on the network. This allows the attacker to intercept and modify traffic intended for the victim. By checking the ARP table on your laptop, you can see if there is any IP address with two different MAC addresses, which would indicate an ARP spoofing attack is in progress.

QUESTION 65
Lewis, a professional hacker, targeted the IoT cameras and devices used by a target venture-capital firm. He used an information-gathering tool to collect information about the IoT devices connected to a network, open ports and services, and the attack surface area. Using this tool, he also generated statistical reports on broad usage patterns and trends. This tool helped Lewis continually monitor every reachable server and device on the Internet, further allowing him to exploit these devices in the network.
Which of the following tools was employed by Lewis in the above scenario?

A. NeuVector
B. Lacework
C. Censys
D. Wapiti

Answer: C
Explanation:
Censys is a popular information-gathering tool used to collect information about devices connected to a network, open ports and services, and the attack surface area. It is used to generate statistical reports on broad usage patterns and trends, and to continually monitor every reachable server and device on the Internet, making it an ideal tool for hackers to gather information about their targets.

QUESTION 66
Techno Security Inc. recently hired John as a penetration tester. He was tasked with identifying open ports in the target network and determining whether the ports are online and any firewall rule sets are encountered.
John decided to perform a TCP SYN ping scan on the target network.
Which of the following Nmap commands must John use to perform the TCP SYN ping scan?

A. nmap -sn -PO < target IP address >
B. nmap -sn -PS < target IP address >
C. nmap -sn -PA < target IP address >
D. nmap -sn -PP < target IP address >

Answer: B
Explanation:
In a TCP SYN ping scan, Nmap sends a TCP SYN packet to the target port, expecting a SYN-ACK or RST response from an open port. If the response is RST, it means the port is closed. If there is no response, the port may be either open or filtered. This method is used to detect whether a port is open or closed.
The -sn option in Nmap is used for host discovery, and it disables port scanning. The -PS option is used to specify a

TCP SYN ping scan, while the -PA and -PP options are used for TCP ACK and ICMP ping scans, respectively. Therefore, the correct command for a TCP SYN ping scan in Nmap is:
nmap -sn -PS < target IP address >

QUESTION 67
Ricardo has discovered the username for an application in his target's environment. As he has a limited amount of time, he decides to attempt to use a list of common passwords he found on the Internet. He compiles them into a list and then feeds that list as an argument into his password-cracking application.
What type of attack is Ricardo performing?

A. Brute force
B. Known plaintext
C. Dictionary
D. Password spraying

Answer: C
Explanation:
A dictionary attack is an attack that tries to guess at the key of a ciphertext by attempting many different common passwords and possible passwords that are likely to be used by humans.

QUESTION 68
What would be the fastest way to perform content enumeration on a given web server by using the Gobuster tool?

A. Performing content enumeration using the bruteforce mode and 10 threads
B. Performing content enumeration using the bruteforce mode and random file extensions
C. Skipping SSL certificate verification
D. Performing content enumeration using a wordlist

Answer: D
Explanation:
Performing content enumeration using a wordlist is the fastest way to perform content enumeration on a given web server using the Gobuster tool. This is because a wordlist includes common paths, directories, and files that are likely to exist on the web server, and it is a pre-built list, so there is no need to generate a list on the fly. This approach avoids the overhead of trying to brute force filenames or extensions and reduces the time it takes to discover content.

QUESTION 69
When analyzing the IDS logs, the system administrator noticed an alert was logged when the external router was accessed from the administrator's Computer to update the router configuration.
What type of an alert is this?

A. False negative
B. True negative
C. True positive
D. False positive

Answer: D
Explanation:
True Positive - IDS referring a behavior as an attack, in real life it is
True Negative - IDS referring a behavior not an attack and in real life it is not
False Positive - IDS referring a behavior as an attack, in real life it is not
False Negative - IDS referring a behavior not an attack, but in real life is an attack

QUESTION 70
Garry is a network administrator in an organization. He uses SNMP to manage networked devices from a remote location. To manage nodes in the network, he uses MIB, which contains formal descriptions of all network objects managed by SNMP. He accesses the contents of MIB by using a web browser either by entering the IP address and Lseries.mib or by entering the DNS library name and Lseries.mib. He is currently retrieving information from an MIB

that contains object types for workstations and server services.
Which of the following types of MIB is accessed by Garry in the above scenario?

A. LNMIB2.MIB
B. DHCP.MIB
C. MIB_II.MIB
D. WINS.MIB

Answer: A
Explanation:
* DHCP.MIB: Monitors network traffic between DHCP servers and remote hosts
* HOSTMIB.MIB: Monitors and manages host resources
* LNMIB2.MIB: Contains object types for workstation and server services
* MIB_II.MIB: Manages TCP/IP-based Internet using a simple architecture and system
* WINS.MIB: For the Windows Internet Name Service (WINS)

QUESTION 71
Emily, an extrovert obsessed with social media, posts a large amount of private information, photographs, and location tags of recently visited places. Realizing this, James, a professional hacker, targets Emily and her acquaintances, conducts a location search to detect their geolocation by using an automated tool, and gathers information to perform other sophisticated attacks.
What is the tool employed by James in the above scenario?

A. ophcrack
B. VisualRoute
C. Hootsuite
D. HULK

Answer: C
Explanation:
Conducting location search on social media sites such as Twitter, Instagram, and Facebook helps attackers to detect the geolocation of the target. This information further helps attackers to perform various social engineering and non-technical attacks. Many online tools such as Followerwonk, Hootsuite, and Meltwater are available to search for both geotagged and non-geotagged information on social media sites. Attackers search social media sites using these online tools using keywords, usernames, date, time, and so on.

QUESTION 72
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

Answer: D
Explanation:
Alice should Use Bryan's public key so only Brian can decrypt it with his private key. Bryan will use Alice's public key to confirm this msg came from Alice as she is the only one with the private key.

QUESTION 73
What is the file that determines the basic configuration (specifically activities, services, broadcast receivers, etc.) in an Android application?

A. AndroidManifest.xml

B. classes.dex
C. APK.info
D. resources.asrc

Answer: A
Explanation:
The AndroidManifest.xml file contains information of your package, including components of the appliance like activities, services, broadcast receivers, content providers etc.
It performs another tasks also:
- It's responsible to guard the appliance to access any protected parts by providing the permissions.
- It also declares the android api that the appliance goes to use.
- It lists the instrumentation classes. The instrumentation classes provides profiling and other informations. These informations are removed just before the appliance is published etc. This is the specified xml file for all the android application and located inside the basis directory.

QUESTION 74
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

Answer: D
Explanation:
Credential enumerator: a self-extracting RAR file containing two components, a bypass and a service component. The bypass component is used for enumeration of network resources and either finds writable share drives using Server Message Block (SMB) or tries to brute force user accounts, including the administrator account. Once an available system is found, Emotet then writes the service component on the system, which writes Emotet onto the disk. Access to SMB can result in entire domains (servers and clients) becoming infected.

QUESTION 75
Which of the following Bluetooth hacking techniques refers to the theft of information from a wireless device through Bluetooth?

A. Bluesmacking
B. Bluesnarfing
C. Bluejacking
D. Bluebugging

Answer: B
Explanation:
Bluesnarfing is the unauthorized access of information from a wireless device through a Bluetooth connection, often between phones, desktops, laptops, and PDAs (personal digital assistant).

QUESTION 76
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.

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.

Answer: A
Explanation:
Security questions are often used as a way to verify a user's identity when they are trying to reset their password. The answers to these questions are typically personal information that is known only to the user, such as their mother's maiden name or their childhood pet's name.
In this case, Matt responded to a post that asked him a number of personal questions. These questions were likely security questions for his bank account. By answering these questions, Matt inadvertently provided the answers to his security questions to the attacker. This allowed the attacker to reset Matt's password and gain access to his bank account.

QUESTION 77
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

Answer: D
Explanation:
The attacker disables the security controls of NetNTLMv1 by modifying the values of LMCompatibilityLevel, NTLMMinClientSec, and RestrictSendingNTLMTraffic.

QUESTION 78
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

Answer: D
Explanation:
The honey trap is a technique where an attacker targets a person online by pretending to be an attractive person and then begins a fake online relationship to obtain confidential information about the target company. In this technique, the victim is an insider who possesses critical information about the target organization.

QUESTION 79
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
D. Enumeration

Answer: C
Explanation:
Reconnaissance is the process of gathering information about a target. This information can be used to plan and execute an attack. In the case of phishing, reconnaissance would involve gathering information about the target company, such as its logo, formatting, and names of its employees. This information can be used to make the phishing message more likely to be opened and clicked on by the victim.

QUESTION 80
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
B. Preparation
C. Incident recording and assignment
D. Eradication

Answer: A
Explanation:
In this phase, the identified security incidents are analyzed, validated, categorized, and prioritized. The IH&R team further analyzes the compromised device to find incident details such as the type of attack, its severity, target, impact, and method of propagation, and any vulnerabilities it exploited.

QUESTION 81
At what stage of the cyber kill chain theory model does data exfiltration occur?

A. Weaponization
B. Actions on objectives
C. Command and control
D. Installation

Answer: B
Explanation:
The adversary controls the victim’s system from a remote location and finally accomplishes their intended goals. The adversary gains access to confidential data, disrupts the services or network, or destroys the operational capability of the target by gaining access to its network and compromising more systems. Also, the adversary may use this as a launching point to perform other attacks.

QUESTION 82
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
C. Elicitation
D. Phishing

Answer: C
Explanation:
Attackers call numerous random numbers within a company, claiming to be from technical support.
They offer their service to end users in exchange for confidential data or login credentials.

QUESTION 83
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
C. Saleae Logic Analyzer
D. Cisco ASA

Answer: B
Explanation:
The Syhunt Hybrid scanner automates web application security testing and guards the organization's web infrastructure against web application security threats. Syhunt Dynamic crawls websites and detects XSS, directory transversal problems, fault injection, SQL injection, attempts to execute commands, and several other attacks. Syhunt Hybrid creates signatures to detect application vulnerabilities and prevents logout. It analyzes JavaScript (JS), logs suspicious responses, and tests errors for review.

QUESTION 84
Which of the following Metasploit post-exploitation modules can be used to escalate privileges on Windows systems?

A. getsystem
B. getuid
C. keylogrecorder
D. autoroute

Answer: A
Explanation:
The getsystem module is a built-in Metasploit module that attempts to elevate the privileges of the current user to the highest possible level, including SYSTEM-level privileges. The getuid module is used to retrieve the user ID of the current user on the target system. The keylogrecorder module is used to log keystrokes on the target system, and the autoroute module is used to add a route to the target system. Neither of these modules is used for privilege escalation.

QUESTION 85
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
D. ACK flag probe scan

Answer: C
Explanation:
*Probe packet (FIN/ACK)
==> No response - Port is open
==> ICMP unreachable error response - Port is filtered
==> RST packet response - Port is closed

QUESTION 86
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
D. IntentFuzzer

Answer: C
Explanation:
Flowmon is an OT security tool that is designed to protect against security incidents such as cyber espionage, zero-day attacks, and malware in critical infrastructure environments. It can detect and prevent network anomalies and attacks on industrial control systems and help ensure the reliability and availability of industrial networks. Robotium is a mobile app testing framework, BalenaCloud is a container-based platform for building and deploying IoT applications, and IntentFuzzer is an Android app testing tool. None of these tools are designed for OT security or protecting critical infrastructure.

QUESTION 87
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
C. PaaS
D. CaaS

Answer: B
Explanation:
In a SaaS model, the software application is hosted on the cloud provider's infrastructure, and the provider is responsible for managing the underlying hardware, operating system, and software. The user accesses the software through a web browser or an application, and the provider is responsible for patching, updating, and monitoring the application. In this scenario, the customer relationship management tool is hosted on the cloud provider's infrastructure, and Heather's company is only responsible for managing user accounts. IaaS (Infrastructure as a Service) provides access to virtualized computing resources over the internet, PaaS (Platform as a Service) provides a platform for developers to build and deploy applications, and CaaS (Containers as a Service) provides a container-based platform for deploying and managing applications.

QUESTION 88
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
D. Advanced image search

Answer: C

Explanation:
Reverse image search - Juliet used the images as search queries and searched the web for similar images, allowing her to track down the original source and details of the images. This technique can be done using search engines such as Google Images or TinEye, and is used to determine the origin and authenticity of images.

QUESTION 89
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
B. Internal monologue attack
C. LLMNR/NBT-NS poisoning
D. Pass the ticket

Answer: A
Explanation:
Pass the hash is a type of attack where the attacker does not need to know the password in order to authenticate to a system. Instead, the attacker can use the password hash to authenticate to the system.
In this case, Mary has found password hashes in a client system. She can use these hashes to perform a pass the hash attack in order to authenticate to the system and continue with the test.

QUESTION 90
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

Answer: D
Explanation:
Passive assessments sniff the traffic present on the network to identify the active systems, network services, applications, and vulnerabilities. Passive assessments also provide a list of the users who are currently accessing the network.

QUESTION 91
Which of the following protocols can be used to secure an LDAP service against anonymous queries?

A. NTLM
B. RADIUS
C. WPA
D. SSO

Answer: A
Explanation:
Use NT LAN Manager (NTLM), Kerberos, or any basic authentication mechanism to limit access to legitimate users.

QUESTION 92
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)

Answer: C
Explanation:
Server Message Block (SMB) is a network protocol that allows computers to share files, printers, and other resources. It is typically used on Windows-based networks. SMB runs on TCP port 445.
In this scenario, Lawrence is performing banner grabbing to obtain information about the services running on the target machine. He is able to obtain the OS details and versions of services running on TCP port 445. This means that the service that he enumerated is SMB.

QUESTION 93
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
D. Piggybacking

Answer: C
Explanation:
An evil twin is a wireless AP that pretends to be a legitimate AP by imitating its SSID.

QUESTION 94
Which file is a rich target to discover the structure of a website during web-server footprinting?

A. domain.txt
B. Robots.txt
C. Document root
D. index.html

Answer: B
Explanation:
Robots.txt is a file that webmasters use to communicate with web crawlers and other automated agents visiting their site. This file is often used to exclude certain directories or pages from being crawled, but it can also contain valuable information about the site's directory structure and organization. By examining the robots.txt file, an attacker can gain insight into the site's organization and potentially identify hidden or sensitive directories. Domain.txt is not a standard file used in web server configuration or operation. Document root is the root directory of the web server, and index.html is the default home page file. While these files can provide information about the web server and its configuration, they do not necessarily reveal the structure of the website.

QUESTION 95
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

Answer: D
Explanation:
DNS tunneling is a technique used to bypass network security controls by encapsulating non-DNS traffic within DNS packets. By embedding malicious data into the DNS protocol packets, an attacker can bypass firewalls and other security controls that are not configured to inspect DNS traffic. DNSSEC zone walking is a technique used to extract information from DNSSEC-signed zones by iterating over the DNS tree. DNS cache snooping is a technique used to obtain information about a DNS server's cache by sending queries for non-existent domain names. DNS enumeration is a technique used to gather information about a target network by querying DNS servers for information about the network's hosts and services.

QUESTION 96
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
D. WPA3

Answer: C
Explanation:
WEP is an old and outdated encryption protocol that was designed to provide wireless networks with a level of security similar to that of wired networks. However, it has been found to be vulnerable to a number of attacks, including key cracking and packet injection. WPA (Wi-Fi Protected Access) and WPA3 are more recent and secure encryption protocols for wireless networks. RADIUS (Remote Authentication Dial-In User Service) is a networking protocol used for centralized authentication, authorization, and accounting management.

QUESTION 97
Jacob works as a system administrator in an organization. He wants to extract the source code of a mobile application and disassemble the application to analyze its design flaws. Using this technique, he wants to fix any bugs in the application, discover underlying vulnerabilities, and improve defense strategies against attacks.
What is the technique used by Jacob in the above scenario to improve the security of the mobile application?

A. Reverse engineering
B. App sandboxing
C. Jailbreaking
D. Social engineering

Answer: A
Explanation:
Reverse engineering is the process of analyzing and extracting the source code of a software or application, and if needed, regenerating it with required modifications.Reverse engineering is used to disassemble a mobile application to analyze its design flaws and fix any bugs that are residing in it.

QUESTION 98
Calvin, a grey-hat hacker, targets a web application that has design flaws in its authentication mechanism. He enumerates usernames from the login form of the web application, which requests users to feed data and specifies the incorrect field in case of invalid credentials. Later, Calvin uses this information to perform social engineering.
Which of the following design flaws in the authentication mechanism is exploited by Calvin?

A. Insecure transmission of credentials
B. Verbose failure messages
C. User impersonation
D. Password reset mechanism

Answer: B
Explanation:
Attack Authentication Mechanism - Username Enumeration
Exploit design and implementation flaws in web applications, such as failure to check password strength or insecure transmission of credentials, to bypass authentication mechanisms.
verbose failure messages - In a typical login system, the user enters two fields, namely username and password. In some cases, an application will ask for additional information.

QUESTION 99
Henry is a penetration tester who works for XYZ organization. While performing enumeration on a client organization, he queries the DNS server for a specific cached DNS record. Further, by using this cached record, he determines the sites recently visited by the organization's user. What is the enumeration technique used by Henry on the organization?

A. DNS zone walking
B. DNS cache snooping
C. DNS SEC zone walking
D. DNS cache poisoning

Answer: B
Explanation:
DNS cache snooping is a type of DNS enumeration technique in which an attacker queries the DNS server for a specific cached DNS record. By using this cached record, the attacker can determine the sites recently visited by the user.

QUESTION 100
An attacker decided to crack the passwords used by industrial control systems. In this process, he employed a loop strategy to recover these passwords. He used one character at a time to check whether the first character entered is correct; if so, he continued the loop for consecutive characters. If not, he terminated the loop. Furthermore, the attacker checked how much time the device took to finish one complete password authentication process, through which he deduced how many characters entered are correct.
What is the attack technique employed by the attacker to crack the passwords of the industrial control systems?

A. Side-channel attack
B. Denial-of-service attack
C. HMI-based attack
D. Buffer overflow attack

Answer: A
Explanation:
Attackers perform a side-channel attack by monitoring its physical implementation to obtain critical information from a target system.
Timing Analysis - Passwords are often transmitted through a serial channel. Attackers employ a loop strategy to recover these passwords. The timing-based attacks can be easily detected and blocked.