Number: ECSS
Passing Score: 800
Time Limit: 120
File Version: 13.0

Exam Code: ECSS

Exam Name: EC-Council Certified Security Specialist (ECSSv10)

Exam A

QUESTION 1
Bob has secretly installed smart CCTV devices (IoT devices) outside his home and wants to access the recorded data from a remote location. These smart CCTV devices send sensed data to an intermediate device that carries out pre-processing of data online before transmitting it to the cloud for storage and analysis. The analyzed data is then sent to Bob for initiating actions.
Identify the component of IoT architecture that collects data from IoT devices and performs data preprocessing.

A. Data lakes
B. Streaming data processor
C. Gateway
D. A Machine learning

Correct Answer: C
Section:
Explanation:
In the context of IoT architecture, the component that collects data from IoT devices and performs data preprocessing is typically referred to as aGateway. This device acts as an intermediary between the IoT devices and the cloud infrastructure. It is responsible for aggregating data, performing initial processing, and then transmitting the data to the cloud for further storage and analysis. Gateways are crucial for reducing latency, providing local data buffering, and ensuring that only necessary data is sent to the cloud, thereby optimizing network and storage resources.

QUESTION 2
Which of the following MAC forensic data components saves file information and related events using a token with a binary structure?

A. Kexts
B. User account
C. Command-line inputs
D. Basic Security Module

Correct Answer: D
Section:
Explanation:
In the context of MAC (Mandatory Access Control) forensics, the Basic Security Module (BSM) is known to save file information and related events using a token with a binary structure. BSM is part of the auditing system that records security-related events and data. Each BSM audit record is composed of one or more tokens, where each token has a specific type identifier followed by data relevant to that token type. This structure allows for a detailed and organized way to store and retrieve event data, which is crucial for forensic analysis.

QUESTION 3
Roxanne is a professional hacker hired by an agency to disrupt the business services of their rival company. Roxanne employed a special type of malware that consumes a server's memory and network bandwidth when triggered. Consequently, the target server is overloaded and stops responding.
Identify the type of malware Roxanne has used in the above scenario.

A. Rootkit
B. Armored virus
C. worm
D. Spyware

Correct Answer: C

Section:
Explanation:
In the scenario described, the malware that consumes a server's memory and network bandwidth, causing the server to overload and stop responding, is typically aworm. Worms are a type of malware that replicate themselves and spread to other computers across a network, often consuming significant system resources and network bandwidth in the process. Unlike viruses, which require human action to spread, worms typically exploit vulnerabilities or use automated methods to propagate without the need for user intervention.

QUESTION 4
James is a professional hacker attempting to gain access to an industrial system through a remote control device. In this process, he used a specially designed radio transceiver device to sniff radio commands and inject arbitrary code into the firmware of the remote controllers to maintain persistence.
Which of the following attacks is performed by James in the above scenario?

A. Malicious reprogramming attack
B. Re pairing with a malicious RF controller
C. Command injection
D. Abusing reprogramming attack

Correct Answer: A
Section:
Explanation:
James is performing amalicious reprogramming attackin the given scenario. He uses a specially designed radio transceiver device to sniff radio commands and inject arbitrary code into the firmware of the remote controllers. This allows him to maintain persistence and potentially gain unauthorized access to the industrial system.
EC-Council Certified Security Specialist (E|CSS) documents and study guide12.

QUESTION 5
While investigating a web attack on a Windows-based server, Jessy executed the following command on her system:
C:\> net view <10.10.10.11>
What was Jessy's objective in running the above command?

A. Verify the users using open sessions
B. Check file space usage to look for a sudden decrease in free space
C. Check whether sessions have been opened with other systems
D. Review file shares to ensure their purpose

Correct Answer: D
Section:
Explanation:
Thenet viewcommand in Windows is used to display a list of resources being shared on a computer.When used with a specific computer name or IP address, as innet view <10.10.10.11>, it displays the shared resources available on that particular computer1. Jessy's objective in running this command was likely to review the file shares on the server with the IP address 10.10.10.11 to ensure that they are correctly purposed and not maliciously altered or added as part of the web attack.
This command does not verify users using open sessions, check file space usage, or check whether sessions have been opened with other systems. Instead, it specifically lists the shared resources, which can include file shares and printer shares, providing insight into what is being shared from the server in question. This information is crucial during a forensic investigation of a web attack to understand if and how the server's shared resources were compromised or utilized by the attacker.

QUESTION 6
Identify the backup mechanism that is performed within the organization using external devices such as hard disks and requires human interaction to perform the backup operations, thus, making it suspect able to theft or natural disasters.

A. Offsite data backup

B. Cloud data backup
C. Online data backup
D. Onsite data backup

Correct Answer: D
Section:
Explanation:
The backup mechanism described in the scenario, which involves using external devices (such as hard disks) and requires human interaction for backup operations, is known asonsite data backup. In this approach, backups are stored within the organization's premises, making them susceptible to theft, damage, or natural disasters. It is essential to consider additional offsite or cloud-based backup solutions to enhance data resilience and security.

QUESTION 7
Michael, a forensic expert, was assigned to investigate an incident that involved unauthorized intrusion attempts. In this process, Michael identified all the open ports on a system and disabled them because these open ports can allow attackers to install malicious services and compromise the security of the system or network.
Which of the following commands assisted Michael in identifying open ports in the above scenario?

A. nmap -sT localhost
B. netstat -i
C. ilconfig promise
D. netstat rn

Correct Answer: B
Section:
Explanation:
Michael used thenetstatcommand with the-ioption to identify open ports on the system. The-iflag displays network interfaces and their statistics, including information about open ports. By analyzing this output, Michael could determine which ports were active and potentially vulnerable to unauthorized access.
EC-Council Certified Security Specialist (E|CSS) course materials and study guide12.
EC-Council Certified Security Specialist (ECSS) program information1.
EC-Council ECSS Certification Syllabus and Prep Guide.
EC-Council ECSS Certification Sample Questions and Practice Exam.
EC-Council ECSS brochure3.

QUESTION 8
Alana, an employee in an organization, took a short break after spending exhausting hours on a project. For relaxation, she went to a cafeteria with her laptop, where she connected to the public Internet. While browsing the web, she received a project modifications file on her mail and reverted with another file that contained the required changes.
Which of the following BYOD risks has emerged from the above scenario?

A. Mixing personal and private data
B. Endpoint security issue
C. Improper disposing of devices
D. Sharing confidential data on unsecured networks

Correct Answer: D
Section:
Explanation:
In the given scenario, Alana's actions pose a risk related tosharing confidential data on unsecured networks. Here's why:
BYOD (Bring Your Own Device): Alana used her personal laptop in a public cafeteria. This falls under the BYOD concept, where employees use their personal devices for work-related tasks.
Unsecured Network: Connecting to the public Internet in a cafeteria means she is using an unsecured network. Public Wi-Fi networks are often vulnerable to eavesdropping and unauthorized access.

Email Communication: Alana received a project modifications file via email and sent back another file with changes. Email communication over an unsecured network can expose sensitive information to potential attackers.
Risk: By sharing project-related files over an unsecured network, Alana risks exposing confidential data to unauthorized individuals.
EC-Council Certified Security Specialist (E|CSS) course materials and study guide.
EC-Council Certified Security Specialist (E|CSS) documents and course content12.

QUESTION 9
Bob, a security professional, was recruited by an organization to ensure that application services are being delivered as expected without any delay. To achieve this. Bob decided to maintain different backup servers for the same resources so that if one backup system fails, another will serve the purpose.
Identify the IA principle employed by Bob in the above scenario.

A. Integrity
B. Confidentiality
C. Authentication
D. Availability

Correct Answer: D
Section:
Explanation:
In the given scenario, Bob's decision to maintain different backup servers for the same resources demonstrates the principle ofavailability. By having redundant backup systems, Bob ensures that the services remain accessible even if one system fails.

QUESTION 10
Peter, a network defender, was instructed to protect the corporate network from unauthorized access. To achieve this, he employed a security solution for wireless communication that uses dragonfly key exchange for authentication, which is the strongest encryption algorithm that protects the network from dictionary and key recovery attacks.
Identify the wireless encryption technology implemented in the security solution selected by Peter in the above scenario.

A. WPA
B. WPA3
C. WEP
D. EAP

Correct Answer: B
Section:
Explanation:
Peter's security solution for wireless communication uses thedragonfly key exchangefor authentication. This key exchange method is a crucial component ofWPA3(Wi-Fi Protected Access 3). WPA3 is an improved wireless security protocol that enhances protection against dictionary attacks and provides forward secrecy. The dragonfly handshake in WPA3 makes it impossible for attackers to record the 4-Way Handshake and launch offline dictionary attacks.Additionally, WPA3 introduces perfect forward secrecy, preventing attackers from decrypting past traffic after a key breach12.
EC-Council Certified Security Specialist (E|CSS) documents and study guide
EC-Council Certified Security Specialist (E|CSS) course materials3

QUESTION 11
Which of the following environmental controls options saves the hardware from humidity and heat, increases hardware performance, and maintains consistent room temperature?

A. Hot and cold aisles
B. Lighting system
C. EMI shielding
D. Temperature indicator

Correct Answer: A
Section:
Explanation:
Hot and cold aisle containment systems are environmental control strategies used in data centers to manage the temperature and humidity levels. This setup involves alternating rows of cold air intakes and hot air exhausts. The cold aisles face air conditioner output ducts, while the hot aisles face air conditioner return ducts. This arrangement can significantly improve the efficiency of cooling systems, protect hardware from overheating and humidity, enhance hardware performance, and maintain a consistent room temperature.

QUESTION 12
Martin, a hacker, aimed to crash a target system. For this purpose, he spoofed the source IP address with the target's IP address and sent many ICMP ECHO request packets to an IP broadcast network, causing all the hosts to respond to the received ICMP ECHO requests and ultimately crashing the target machine.
Identify the type of attack performed by Martin in the above scenario.

A. UDP flood attack
B. Multi vector attack
C. Smurf attack
D. Fragmentation attack

Correct Answer: C
Section:
Explanation:
In the scenario described, Martin conducted a Smurf attack. This type of attack involves spoofing the source IP address with the target's IP address and sending ICMP ECHO request packets to an IP broadcast network. The broadcast network then amplifies the traffic by directing it to all hosts, which respond to the ICMP ECHO requests. This flood of responses is sent back to the spoofed source IP address, which is the target system, leading to its overload and potential crash.The Smurf attack is a type of distributed denial-of-service (DDoS) attack that exploits the vulnerabilities of the Internet Protocol (IP) and the Internet Control Message Protocol (ICMP).Reference: EC-Council Certified Security Specialist (E|CSS) course materials and documents

QUESTION 13
Kevin, an attacker, is attempting to compromise a cloud server. In this process, Kevin intercepted the SOAP messages transmitted between a user and the server, manipulated the body of the message, and then redirected it to the server as a legitimate user to gain access and run malicious code on the cloud server.
Identify the attack initiated by Kevin on the target cloud server.

A. Side-channel attack
B. Wrapping attack
C. Cross guest VM breaches
D. DNS spoofing

Correct Answer: B
Section:
Explanation:
The attack described involves intercepting and manipulating SOAP messages, which is characteristic of a wrapping attack. In a wrapping attack, the attacker intercepts the SOAP message and alters the body content to perform unauthorized actions, such as running malicious code on the server. This type of attack exploits the XML signature or encryption of SOAP messages, allowing the attacker to impersonate a legitimate user and gain unauthorized access.

QUESTION 14
Joseph, a security professional, was instructed to secure the organization's network. In this process, he began analyzing packet headers to check whether any indications of source and destination IP addresses and port numbers are being changed during transmission.
Identify the attack signature analysis technique performed by Joseph in the above scenario.

A. Composite-signature-based analysis

B. Context based signature analysis
C. Content based signature analysis
D. Atomic signature based analysis

Correct Answer: B
Section:
Explanation:
Joseph's analysis of packet headers to check for changes in source and destination IP addresses and port numbers during transmission is indicative of a context-based signature analysis technique. This method focuses on understanding the context or circumstances under which network data operates, rather than just the content of the packets themselves. By analyzing the changes in IP addresses and port numbers, Joseph is looking for patterns or anomalies that could suggest a security threat or an ongoing attack, such as IP spoofing or port redirection, which are common tactics in network intrusions.
Context-based signature analysis differs from other types, such as atomic and composite signature analysis, by focusing on the behavioral aspects and the situational context of the network traffic. Atomic signature analysis, for instance, relies on single, unique identifiers within a piece of malware or an attack vector, while composite signature analysis looks at multiple attributes or behaviors combined to identify a threat. Content-based signature analysis, another common technique, examines the actual payload of packets for specific malicious content or patterns known to be associated with malware.
Joseph's approach is particularly effective in identifying sophisticated attacks that may not have a known signature or a specific malicious payload but exhibit unusual patterns in how they manipulate network traffic. By understanding the context and the normal baseline of network activities, security professionals like Joseph can detect and mitigate threats that would otherwise go unnoticed with more conventional signature-based methods.

QUESTION 15
John, a forensic officer, was working on a criminal case. He employed imaging software to create a copy of data from the suspect device on a storage medium for further investigation. For developing an image of the original data, John used a software application that does not allow an unauthorized user to alter the image content on storage media, thereby retaining an unaltered image copy.
Identify the data acquisition step performed by John in the above scenario.

A. Validated data acquisition
B. Planned for contingency
C. Sanitized the target media
D. Enabled write protection on the evidence media

Correct Answer: D
Section:
Explanation:
In digital forensics, write protection is a crucial step during data acquisition to ensure that the data being imaged cannot be altered during the process. This is essential to maintain the integrity of the evidence. John's use of imaging software that prevents unauthorized alteration indicates that he enabled write protection, which is a standard practice to safeguard the original data on storage media.

QUESTION 16
Melissa, an ex-employee of an organization, was fired because of misuse of resources and security violations. She sought revenge against the company and targeted its network, as she is already aware of its network topology. Which of the following categories of insiders does Melissa belong to?

A. Malicious insider
B. Professional insider
C. Compromised insider
D. Negligent insider

Correct Answer: A
Section:
Explanation:
Melissa's actions classify her as a malicious insider. This category includes individuals who intentionally misuse access to harm the organization. Her intent to seek revenge and her deliberate targeting of the company's network due to a grudge from being fired are indicative of a malicious insider threat.Reference: This explanation is based on general cybersecurity knowledge and definitions of insider threats. For specific references, please consult the EC-Council Certified Security Specialist (E|CSS) documents and study materials.

QUESTION 17
John, from a remote location, was monitoring his bedridden grandfather's health condition at his home. John has placed a smart wearable ECC on his grandfather's wrist so that he can receive alerts to his mobile phone and can keep a track over his grandfather's health condition periodically.
Which of the following types of IoT communication model was demonstrated in the above scenario?

A. Cloud-lo-cloud communication model
B. Device to gateway model
C. Device to device model
D. Device-to-cloud model

Correct Answer: D
Section:
Explanation:
In the scenario described, John is using aDevice-to-cloud modelof IoT communication. This model involves direct communication between the smart wearable ECC (IoT device) and the cloud, where the data is stored and analyzed. Alerts and health condition updates are then sent from the cloud to John's mobile phone. This model is efficient for scenarios where IoT devices need to send data directly to a cloud service for storage, analysis, and further action, without the need for an intermediary device or gateway.

QUESTION 18
A system that a cybercriminal was suspected to have used for performing an anti-social activity through the Tor browser. James reviewed the active network connections established using specific ports via Tor.
Which of the following port numbers does Tor use for establishing a connection via Tor nodes?

A. 1026/64666
B. 9150/9151
C. 3024/4092
D. 31/456

Correct Answer: B
Section:
Explanation:
Tor Network Functionality:The Tor network is designed to protect user anonymity by routing traffic through a series of relays (nodes). This obfuscates the source of the traffic and makes it difficult to trace.
SOCKS Proxy:Tor primarily functions as a SOCKS proxy to facilitate this anonymization. Applications configured to use Tor's SOCKS proxy will have their traffic routed through the Tor network.
Default Ports:
9050:The standard SOCKS port used by standalone Tor installations.
9150:The typical SOCKS port for the Tor Browser Bundle, a self-contained package with Tor and a pre-configured browser.

QUESTION 19
Bob. a network specialist in an organization, is attempting to identify malicious activities in the network. In this process. Bob analyzed specific data that provided him a summary of a conversation between two network devices, including a source IP and source port, a destination IP and destination port, the duration of the conversation, and the information shared during the conversation.
Which of the following types of network-based evidence was collected by Bob in the above scenario?

A. Statistical data
B. Alert data
C. Session data
D. Full content data

Correct Answer: C
Section:
Explanation:

In the scenario described, Bob collected data that summarizes a conversation between two network devices. This type of data typically includes the source and destination IP addresses and ports, the duration of the conversation, and the information exchanged during the session. This aligns with the definition of session data, which is a type of network-based evidence that provides an overview of communication sessions between devices without including the actual content of the data packets.

QUESTION 20
Which of the following practices makes web applications vulnerable to SQL injection attacks?

A. Use the most restrictive SQL account types for applications
B. Never build Transact SQL statements directly from user input
C. Avoid constructing dynamic SQL with concatenated input values
D. A Accept entries that contain binary data, escape sequences, and comment characters

Correct Answer: C
Section:
Explanation:
SQL Injection (SQLi) is a prevalent vulnerability in web applications that occurs when an attacker can insert or manipulate SQL queries using untrusted user input. This vulnerability is exploited by constructing dynamic SQL statements that include user-provided data without proper validation or sanitization. When applications concatenate user input values directly into SQL queries, they become susceptible to SQLi, as attackers can craft input that alters the intended SQL command structure, leading to unauthorized access or manipulation of the database.
To mitigate SQL injection risks, it's crucial to avoid creating dynamic SQL queries by concatenating input values. Instead, best practices such as using prepared statements with parameterized queries, employing stored procedures, and implementing proper input validation and sanitization should be followed. These measures help ensure that user input is treated as data rather than part of the SQL code, thus preserving the integrity of the SQL statement and preventing injection attacks.
SQL Injection (SQLi): This common web application vulnerability arises when untrusted user input is directly used to construct SQL queries. Attackers can manipulate the input to alter the structure of the query, leading to data exposure, modification, or even deletion.
Dynamic SQL and Concatenation: Dynamically constructing SQL statements by concatenating user input is highly dangerous. Consider this example:
SQL
SELECT * FROM users WHERE username = userInput ;
An attacker can provide input like: ' OR '1'='1'-- resulting in this query:
SQL
SELECT * FROM users WHERE username = '' OR '1'='1' -- ;
This query will always return true due to the OR condition and the comment (--) effectively bypassing authentication.

QUESTION 21
Melanie, a professional hacker, is attempting to break into a target network through an application server. In this process, she identified a logic flaw in the target web application that provided visibility into the source code. She exploited this vulnerability to launch further attacks on the target web application.
Which of the web application vulnerabilities was identified by Melanie in the above scenario?

A. Insecure deserialization
B. Security misconfiguration
C. Command injection
D. Broken authentication

Correct Answer: B
Section:
Explanation:
Melanie discovered alogic flawin the target web application that allowed her to view thesource code. This flaw indicates asecurity misconfiguration, which can lead to further attacks.Security misconfigurations occur when an application or system is not properly configured, leaving it vulnerable to exploitation.Reference: EC-Council Certified Security Specialist (E|CSS) documents and study guide12.

QUESTION 22
Harry, a security professional, was hired to identify the details of an attack that was initiated on a Windows system. In this process, Harry decided to check the logs of currently running applications and the information related

to previously uninstalled or removed applications for suspicious events.
Which of the following folders in a Windows system stores information on applications run on the system?

A. C:\Windows\debug
B. C:\Windows\Book
C. C:\subdir
D. C:\Windows\Prefelch

Correct Answer: D
Section:
Explanation:
The Prefetch folder in Windows is used to store information about applications that are run on the system. This data helps in optimizing the loading times of applications. The correct path is typicallyC:\Windows\Prefetch, notC:\Windows\Prefelchas listed in the options.It's important to note that while the Prefetch folder does contain logs that can be useful for understanding application behavior, it does not store logs for currently running applications or details about previously uninstalled applications1.

QUESTION 23
Bob. a security specialist at an organization, extracted the following IIS log from a Windows-based server: ''2019-12-12 06:11:41 192.168.0.10 GET /images/content/bg_body_l.jpg - 80 - 192.168.0.27 Mozilla/5.0 (Windows*NT6.3:*WOW64)*AppleWebKit/537.36*(KHTML.*likeCecko)*Chrome/48.0.2564.103Safari/537.36 http://www.movie5cope.com/css/style.c5s 200 0 0 365'
Identify the element in the above IIS log entry that indicates the request was fulfilled without error.

A. 192
B. 80
C. 200
D. 537

Correct Answer: C
Section:
Explanation:
The element in the given IIS log entry that indicates the request was fulfilled without error isC. 2001.The HTTP status code200signifies a successful response, indicating that the server successfully processed the client's request1.

QUESTION 24
Which of the following techniques is referred to as a messaging feature that originates from a server and enables the delivery of data or a message from an application to a mobile device without any explicit request from the user?

A. Geofencing
B. PIN feature
C. Containerization
D. Push notification

Correct Answer: D
Section:
Explanation:
Apush notificationis a messaging feature that originates from a server and enables the delivery of data or a message from an application to a mobile device without any explicit request from the user. It allows applications to notify users of new messages, updates, or events even when the app is not actively running on the device. Push notifications are commonly used in mobile apps to engage users and provide timely information.

QUESTION 25
Johnson is a professional hacker who targeted an organization's customers and decided to crack their system passwords. In this process, he found a list of valid customers, created a list of possible passwords, ranked the

passwords from high to low probability, and started keying in each password in the target system until the correct password is discovered.
Identify the type of attack performed by Johnson in the above scenario.

A. Password guessing
B. Rainbow table attack
C. Dictionary attack
D. Brute force attack

Correct Answer: C
Section:
Explanation:
The scenario described involves Johnson using a list of possible passwords, which he has ranked by probability, and systematically entering them into the system to discover the correct one. This method is known as a dictionary attack, where an attacker uses a prearranged list of likely passwords---often derived from lists of common passwords or phrases---and tries them one by one. This is different from a brute force attack, which would involve trying all possible combinations, and a rainbow table attack, which uses precomputed hash values to crack encrypted passwords.Password guessing is a less systematic approach that doesn't necessarily involve a ranked list of passwords.Reference: The information provided aligns with the knowledge domains of the EC-Council Certified Security Specialist (E|CSS) program, which includes understanding various types of attacks and their methodologies as part of the ethical hacking and network defense curriculum1.
The scenario described involves Johnson, who has a list of valid customers and a list of possible passwords ranked by probability, which he uses to systematically attempt to log in to the target system. This method is known as adictionary attack. In a dictionary attack, the hacker uses a list of likely passwords---often derived from lists of common passwords or phrases---and tries them one by one. This differs from a brute force attack, which involves trying all possible combinations of characters until the correct one is found.
A dictionary attack is more efficient than brute force because it relies on the likelihood that people will use common words or phrases for passwords, making it a targeted approach based on probability rather than random attempts. Therefore, the correct answer is C, as it best describes the technique used by Johnson in the given scenario.

QUESTION 26
Below are the various steps involved in establishing a network connection using the shared key authentication process.
l .The AP sends a challenge text to the station.
2 .The station connects to the network.
3 .The station encrypts the challenge text using its configured 128-bit key and sends the encrypted text to the AP.
4 .The station sends an authentication frame to the AP.
5 .The AP uses its configured WEP key to decrypt the encrypted text and compares it with the original challenge text.
What is the correct sequence of steps involved in establishing a network connection using the shared key authentication process?

A. 2 >4 >3
B. 4--->2--->1--->3--->5
C. 4--->1--->3--->5--->2
D. 4-->5->3->2-->1

Correct Answer: C
Section:
Explanation:
The AP sends a challenge text to the station.
The Access Point (AP) initiates the authentication process by sending a challenge text to the station (client device).
The station connects to the network.
The station (client device) associates with the wireless network by connecting to the AP.
The station encrypts the challenge text using its configured 128-bit key and sends the encrypted text to the AP.
The station encrypts the challenge text using the shared secret key (configured on both the station and the AP).
It then sends the encrypted challenge text back to the AP.
The station sends an authentication frame to the AP.
The station constructs an authentication frame containing the encrypted challenge text.
This frame is sent to the AP for verification.

The AP uses its configured WEP key to decrypt the encrypted text and compares it with the original challenge text.
The AP decrypts the received encrypted challenge text using its configured WEP (Wired Equivalent Privacy) key.
If the decrypted text matches the original challenge text, the station is authenticated successfully.
Therefore, the correct sequence isC. 4--->1--->3--->5--->21. This order ensures that the challenge text is exchanged securely and verified by both the station and the AP during the shared key authentication process.
EC-Council Certified Security Specialist (E|CSS) documents and study guide.
EC-Council Certified Security Specialist (E|CSS) course materials1234

QUESTION 27
Sarah was accessing confidential office files from a remote location via her personal computer connected to the public Internet. Accidentally, a malicious file was downloaded onto Sarah's computer without her knowledge. This download might be due to the free Internet access and the absence of network defense solutions.
Identify the Internet access policy demonstrated in the above scenario.

A. Promiscuous policy
B. Paranoid policy
C. Permissive policy
D. Prudent policy

Correct Answer: C
Section:
Explanation:
In the given scenario, Sarah's personal computer connected to the public Internet allowed a malicious file to be downloaded without her knowledge. This situation reflects apermissive policy, where unrestricted access to the Internet is allowed, potentially leading to security risks.Reference: EC-Council Certified Security Specialist (E|CSS) documents and study guide .

QUESTION 28
Finch, a security professional, was instructed to strengthen the security at the entrance. At the doorway, he implemented a security mechanism that allows employees to register their retina scan and a unique six-digit code, using which they can enter the office at any time.
Which of the following combinations of authentication mechanisms is implemented in the above scenario?

A. Password and two-factor authentication
B. Two-factor and smart card authentication
C. Biometric and password authentication
D. Smart card and password authentication

Correct Answer: C
Section:
Explanation:
In the scenario described, Finch implemented a combination ofbiometric authentication(retina scan) andpassword authentication(unique six-digit code). Biometric authentication relies on unique physical or behavioral characteristics (such as retina scans) to verify identity, while password authentication requires users to enter a secret code (the six-digit code in this case).Combining these two mechanisms enhances security by requiring both something the user knows (password) and something the user is (biometric) for access.Reference: EC-Council Certified Security Specialist (E|CSS) documents and study guide12.

QUESTION 29
Which of th following titles of Th Electronic Communications Privacy Act protects the privacy of the contents of files stored by service providers and records held about the subscriber by service providers, such as subscriber name, billing records, and IP addresses?

A. Title II
B. Title I
C. Title IV
D. Title III

Correct Answer: A
Section:
Explanation:
Title II of the Electronic Communications Privacy Act (ECPA), known as the Stored Communications Act (SCA), protects the privacy of the contents of files stored by service providers and records held about the subscriber by service providers.This includes information such as subscriber names, billing records, and IP addresses1.
The correct answer isTitle II. It specifically safeguards communications held in electronic storage, particularly messages stored on computers.While Title I of the ECPA protects wire, oral, and electronic communications while in transit, Title II focuses on the privacy of stored communications3.

QUESTION 30
William is an attacker who is attempting to hack Bluetooth-enabled devices at public places. Within the target's range, he used special software to obtain the data stored in the victim's device. He used a technique that exploits the vulnerability in the OBject Exchange (OBEX) protocol that Bluetooth uses to exchange information.
Identify the attack performed by William in the above scenario.

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

Correct Answer: B
Section:
Explanation:
William performed theBluesnarfingattack. Bluesnarfing is a technique where an attacker exploits a vulnerability in theOBject Exchange (OBEX)protocol used by Bluetooth to exchange information. By doing so, the attacker gains unauthorized access to data stored on the victim's Bluetooth-enabled device.
EC-Council Certified Security Specialist (E|CSS) documents and study guide.
EC-Council Certified Security Specialist (E|CSS) course materials1234

QUESTION 31
In which of the following levels of the OSI model does an attacker gain control over the HTTP user session by obtaining the session IDs and create new unauthorized sessions by using the stolen data?

A. Presentation level
B. Transport level
C. Network-level
D. Application-level

Correct Answer: D
Section:
Explanation:
In the OSI model, theapplication layer(Layer 7) is closest to users and establishes communication between the user and applications. It deals with user interfaces, protocols, and application-specific data. An attacker who gains control over the HTTP user session by obtaining session IDs and creating new unauthorized sessions operates at the application level. By manipulating session IDs, the attacker can impersonate legitimate users and perform unauthorized actions.
EC-Council Certified Security Specialist (E|CSS) documents and study guide1.
EC-Council Certified Security Specialist (E|CSS) course materials2.
The application layer is where HTTP operates, making it the relevant layer for session management and security. Attackers exploit vulnerabilities in web applications to gain unauthorized access, manipulate sessions, and potentially compromise user data. Ensuring secure session management practices is crucial to prevent such attacks.

QUESTION 32
Andrew, a system administrator, is performing a UEFI boot process. The current phase of the UEFI boot process consists of the initialization code that the system executes after powering on the EFI system. This phase also manages platform reset events and sets up the system so that it can find, validate, install, and run the PEI.
Which of the following UEFI boot phases is the process currently in?

A. Pre-EFI initialization phase
B. Security phase
C. Boot device selection phase
D. Driver execution environment phase

Correct Answer: A
Section:
Explanation:
The scenario accurately describes the functions of the PEI phase within the UEFI boot process:
PEI Phase Key Characteristics:
Early Hardware Initialization:The PEI phase is responsible for finding and initializing essential hardware components, like the CPU and the minimum amount of RAM needed for the system to function.
Foundation for Later Stages:It establishes the groundwork for subsequent UEFI phases by creating data structures (Hand-Off Blocks or HOBs) that communicate vital information.
Focus on DXE Initiation:The primary goal of the PEI phase is to prepare the system for the Driver Execution Environment (DXE) phase.
The UEFI boot process is divided into several distinct phases. The phase described in the question involves the initialization code executed after powering on the EFI system, managing platform reset events, and setting up the system to find, validate, install, and run the PEI (Pre-EFI Initialization).This description corresponds to thePre-EFI initialization phase1.
During this phase, the system's firmware is responsible for initializing the processor, memory, and other hardware components to a point where the firmware can hand off control to the operating system loader.It's a critical part of the UEFI boot process, as it prepares the system for the subsequent phases, which include the Security (SEC) phase, the Driver Execution Environment (DXE) phase, and the Boot Device Selection (BDS) phase1. The correct answer is A, as it aligns with the tasks and responsibilities of the Pre-EFI initialization phase as described in the scenario.

QUESTION 33
Wesley, a professional hacker, deleted a confidential file in a compromised system using the '/bin/rm/ command to deny access to forensic specialists.
Identify the operating system on which Don has performed the file carving activity.

A. Windows
B. Mac OS
C. Linux
D. Android

Correct Answer: C
Section:
Explanation:
In the scenario described, Wesley used the''/bin/rm/'' commandto delete a confidential file. The ''/bin/rm/'' command is commonly associated withLinuxoperating systems. It is used to remove files and directories. By deleting the file, Wesley aimed to hinder forensic specialists' access to it.Therefore, the operating system on which Wesley performed the file carving activity isLinux.Reference: EC-Council Certified Security Specialist (E|CSS) documents and study guide12.

QUESTION 34
Christian is working as a software developer in a reputed MNC. He received a message from XIM bank that claims to be urgent and requests to call a phone number mentioned in the message. Worried by this, he called the number to check on his account, believing it to be an authentic XIM Bank customer service phone number. A recorded message asks him to provide his credit or debit card number, as well as his password.
Identify the type of social engineering attack being performed on Christian in the above scenario.

A. SMiShing
B. Spam mail
C. Phishing
D. Eavesdropping

Correct Answer: A
Section:

Explanation:
The scenario described is a classic example ofSMiShing, a form of social engineering attack that uses text messages (SMS) to deceive individuals into providing sensitive information. In this case, Christian receives an urgent message prompting him to call a phone number, which is a tactic used in SMiShing attacks to create a sense of urgency and legitimacy. Upon calling the number, he is asked to provide personal financial information, which is the ultimate goal of the attacker.
SMiShing attacks often impersonate legitimate entities, such as banks, to trick victims into believing that the request is authentic.The use of a recorded message asking for credit or debit card numbers and passwords is a telltale sign of a SMiShing attempt, as legitimate banks would not ask for such sensitive information via a phone call initiated by an unsolicited text message1. Therefore, the correct answer is A, SMiShing, which specifically refers to phishing attacks conducted through SMS.

QUESTION 35
James is a professional hacker who managed to penetrate the target company's network and tamper with software by adding a malicious script in the production that holds persistence on the network.
Which of the following phases of hacking is James currently in?

A. Clearing tracks
B. Maintaining access
C. Gaining access
D. Scanning

Correct Answer: B
Section:
Explanation:
James is currently in theMaintaining accessphase of hacking. In this phase, an attacker ensures continued access to the compromised system or network. By adding a malicious script for persistence, James aims to maintain control over the target company's network.
EC-Council Certified Security Specialist (E|CSS) documents and study guide.
EC-Council Certified Security Specialist (E|CSS) course materials1234

QUESTION 36
An organization decided to strengthen the security of its network by studying and analyzing the behavior of attackers. For this purpose. Steven, a security analyst, was instructed to deploy a device to bait attackers. Steven selected a solution that appears to contain very useful information to lure attackers and find their locationsand techniques.
Identify the type of device deployed by Steven in the above scenario.

A. Firewall
B. Router
C. Intrusion detection system
D. Honeypot

Correct Answer: D
Section:
Explanation:
Steven deployed ahoneypotin the scenario. A honeypot is a simulation of an IT system or software application that acts as bait to attract the attention of attackers. While it appears to be a legitimate target, it is actually fake and carefully monitored by an IT security team.The purpose of a honeypot includes distraction (diverting attackers' attention), threat intelligence (revealing attack methods), and research/training for security professionals1.
EC-Council Certified Security Specialist (E|CSS) documents and study guide1.
EC-Council Certified Security Specialist (E|CSS) course materials2.

QUESTION 37
Kane, an investigation specialist, was appointed to investigate an incident in an organization's network. In this process, Kane executed a command and identified that a network interface is running in the promiscuous mode and is allowing all incoming packets without any restriction.
In the above scenario, which of the following commands did Kane use to check whether the network interface is set to the promiscuous mode?

A. ipconfig < interface name >
B. ifconfig < interface name >
C. nmap -sT localhost
D. netstat -i

Correct Answer: B
Section:
Explanation:
Kane used theifconfigcommand to check whether the network interface is set to promiscuous mode. Theifconfigcommand displays information about network interfaces, including their configuration settings. When a network interface is in promiscuous mode, it allows all incoming packets to be captured without any filtering or restriction.
EC-Council Certified Security Specialist (E|CSS) documents and study guide.
EC-Council Certified Security Specialist (E|CSS) course materials123456789101112131415 16

QUESTION 38
Mark, a network administrator in an organization, was assigned the task of preventing data from falling into the wrong hands. In this process, Mark implemented authentication techniques and performed full memory encryption for the data stored on RAM.
In which of the following states has Steve encrypted the data in the above scenario?

A. Data in transit
B. Data in rest
C. Data in use
D. Data inactive

Correct Answer: C
Section:
Explanation:
Mark implemented full memory encryption for the data stored in RAM. This means that the data is encrypted while it is actively being used by the system (e.g., during processing, execution, or manipulation). Data in use refers to the state when data resides in memory and is accessible by running processes. By encrypting data in use, Mark ensures that even if an attacker gains access to the system's memory, they won't be able to read sensitive information directly.
EC-Council Certified Encryption Specialist (E|CES) documents and study guide1.
EC-Council Certified Encryption Specialist (E|CES) course materials2.