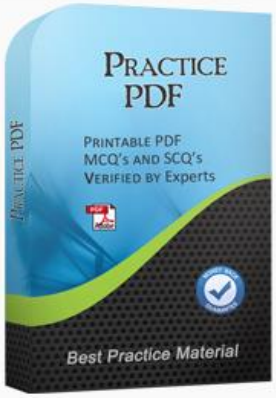
ITPass4Sure

itPass4sure

- Online Tool, Convenient, easy to study.
- Instant Online Access
- Supports All Web Browsers
- Practice Online Anytime
- Test History and Performance Review
- Supports Windows / Mac / Android / iOS, etc.

- Installable Software Application
- Simulates Real Exam Environment
- Builds Exam Confidence
- Supports MS Operating System
- Two Modes For Practice
- Practice Offline Anytime



- Printable PDF Format
- Prepared by IT Experts
- Instant Access to Download
- Study Anywhere, Anytime
- 365 Days Free Updates
- Free PDF Demo Available

Security & Privacy

We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.

365 Days Free Updates

Free update is available within 365 days after your purchase. After 365 days, you will get 50% discounts for updating.

Money Back Guarantee

Full refund if you fail the corresponding exam in 90 days after purchasing. And Free get any another product.

Instant Download

After Payment, our system will send you the products you purchase in mailbox in a minute after payment. If not received within 2 hours, please contact us.

Exam : **ECSS**

Title : EC-Council Certified Security Specialist (ECSSv10)

Vendor : ECCouncil

Version : DEMO

NO.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 cloudfor 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

Answer: C

Explanation:
In the context of IoT architecture, the component that collects data from IoT devices and performs data preprocessing is typically referred to as a Gateway. 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.
References: The information provided aligns with the EC-Council Certified Security Specialist (E|CSS) curriculum, which covers IoT device security, including how security works in IoT-enabled environments and the role of different components within the IoT architecture12.

NO.2 Michael is an attacker who aims to hack Bob's system. He started collecting data without any active interaction with Bob's system. Using this technique. Michael can extract sensitive information from unencrypted data.
Identify the class of attack Michael has launched in the above scenario.

A. Ac live attack

B. Insider attack

C. Close in attack

D. Passive attack

Answer: D

* In a passive attack, the attacker observes or collects information without actively interacting with the target system. Michael's action of collecting data from Bob's system without any active interaction falls under this category. Passive attacks aim to extract sensitive information without altering the system's state or causing any disruption.
* References: EC-Council Certified Security Specialist (E|CSS) documents and study guide12.

NO.3 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
Answer: C
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 a permissive policy, where unrestricted access to the Internet is allowed, potentially leading to security risks. References: EC-Council Certified Security Specialist (E|CSS) documents and study guide .

NO.4 Below is an extracted Apache error log entry.
"(Wed Aug 28 13:35:38.878945 2020] (core:error] (pid 12356:tid 8689896234] (client 10.0.0.8] File not found: /images/folder/pic.jpg" Identify the element in the Apache error log entry above that represents the IP address from which the request was made.
A. 10.0.0.8
B. 8689896234
C. 13:35:38.878945
D. 12356
Answer: A
Explanation:
Certainly! Let's analyze the Apache error log entry to identify the IP address:
* The IP address from which the request was made is 10.0.0.8 (option A).
This address appears in the log entry as follows:
(client 10.0.0.8] File not found: /images/folder/pic.jpg"
References:
* EC-Council Certified Security Specialist (E|CSS) documents and study guide provide insights into network security and log analysis1.
* Apache error logs follow a specific format, where the client IP address is indicated1.

NO.5 Jay, a network administrator, was monitoring traffic flowing through an IDS. Unexpectedly, he received an event triggered as an alarm, although there is no active attack in progress.
Identify the type of IDS alert Jay has received in the above scenario.
A. True negative alert
B. False negative alert
C. True positive alert
D. False positive alert
Answer: D
* In the given scenario, Jay received an alarm from the IDS even though there was no active attack. This situation corresponds to a false positive alert. A false positive occurs when the IDS incorrectly identifies benign or legitimate traffic as malicious or suspicious. It can lead to unnecessary alerts and additional workload for network administrators.
* References: EC-Council Certified Security Specialist (E|CSS) documents and study guide12.

NO.6 Kevin, a forensic investigator at FinCorp Ltd., was investigating a cybercrime against the company. As part of the investigation process, he needs to recover corrupted and deleted files from a Windows system. Kevin decided to use an automated tool to recover the damaged, corrupted, or

deleted files.
Which of the following forensic tools can help Kevin in recovering deleted files?
A. Cain & Abel
B. Rohos Mini Drive
C. R-Sludio
D. Ophcrack
Answer: C
Explanation:
Kevin, as a forensic investigator, can use the R-Sludio tool to recover corrupted and deleted files from a Windows system. R-Sludio is a powerful forensic tool that assists in data recovery and analysis. It allows investigators to examine filesystem images, analyze cache, cookies, history recorded in web browsers, and perform memory forensics1.
References:
* EC-Council Certified Security Specialist (E|CSS) documents and study guide.
* EC-Council Certified Security Specialist (E|CSS) course materials.

NO.7 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
Answer: C
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). References: EC-Council Certified Security Specialist (E|CSS) course materials and documents

NO.8 Jessica, a user, wanted to access the Internet from her laptop and therefore sends a connection request to the access point. To identify the wireless client, the access point forwarded that request to a RADIUS server. The RADIUS server transmitted authentication keys to both the access point and Jessica's laptop. This key helps the access point identify a particular wireless client.
Identify the authentication method demonstrated in the above scenario.
A. Open system authentication
B. Null authentication
C. Shared key authentication

D. Centralized authentication

Answer: D

Explanation:

The scenario described involves the use of a RADIUS (Remote Authentication Dial-In User Service) server. RADIUS is a client-server protocol that provides centralized network authentication12. In this case, the access point (client) forwards the connection request to the RADIUS server, which then sends authentication keys to both the access point and the user's laptop (supplicant). This process helps the access point identify the wireless client12.

RADIUS servers are also known as AAA (Authentication, Authorization, and Accounting) servers because they provide these three services1. The authentication process begins when a user attempts to log into the network. Their device will request access either through the use of credentials or by presenting an X.509 digital certificate1. The RADIUS server then compares the user's information with a list of users stored in a directory or IDP (Identity Provider)1.

Therefore, the authentication method demonstrated in the scenario is centralized authentication (Option D), where a central server (in this case, the RADIUS server) handles the authentication of users.

NO.9 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

Answer: B

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.

References: The information is based on common knowledge regarding SOAP vulnerabilities and attacks, as described in resources like the EC-Council's Certified Security Specialist (E|CSS) program and other cybersecurity literature. Specific details about SOAP message security and wrapping attacks can be found in the EC-Council's E|CSS study materials and official courseware.

NO.10 Daniel, a networking specialist, identifies a glitch in a networking tool and fixes it on a priority using a system.

Daniel was authorized to make a copy of computers programs while maintaining or repairing the system.

Which of the following acts was demonstrated in the above scenario?

A. Data Protection Act 2018 (DPA)

B. The Digital Millennium Copyright Act (DMCA)

C. Sarbanes Oxley Act (SOX)

D. Gramm Leach Bliley Act (GLBA)

Answer: B

Explanation:

Daniel's action of making a copy of computer programs while maintaining or repairing the system aligns with the provisions of the Digital Millennium Copyright Act (DMCA). The DMCA allows for certain exemptions related to circumventing technological protection measures (TPMs) for purposes of maintenance or repair1.

Specifically, section 117 of the U.S. Copyright Code permits the owner or lessee of a machine to make a copy of a computer program solely for maintenance or repair if certain conditions are met1. In this case, Daniel's authorized copying falls within the scope of this provision. References: U.S. Copyright Code, Title 17, Section

1171.