Eccouncil ECSS Practice Questions

Shared by Valdez on 17-08-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

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.

Options:

A- True negative alert
B- False negative alert
C- True positive alert
D- False positive alert

Answer:

D

Explanation:

In the given scenario, Jay received an alarm from the IDS even though there was no active attack. This situation corresponds to afalse 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.

Question 2

Question Type: MultipleChoice

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.

Options:

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

Answer:

C

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 3

Question Type: MultipleChoice

Cibel.org, an organization, wanted to develop a web application for marketing its products to the public. In this process, they consulted a cloud service provider and requested provision of development tools, configuration management, and deployment platforms for developing customized applications.

Identify the type of cloud service requested by Cibel.org in the above scenario.

Options:

A- Security-as-a-service (SECaaS)
B- Infrastructure-as-a-service (laaS)
C- identity-as-a-service (IDaaS)
D- Platform-as-a-service

Answer:

D

Explanation:

Cibel.org requested a cloud service that providesdevelopment tools, configuration management, and deployment platformsfor developing customized applications.This aligns with the characteristics ofPlatform-as-a-service (PaaS), which offers a platform for developers to build, deploy, and manage applications without worrying about infrastructure management.Reference: EC-Council Certified Security Specialist (E|CSS) course materials12.

Question 4

Question Type: MultipleChoice

Bruce, a professional hacker, targeted an OT network. He initiated a looping strategy to recover the password of the target system. He started sending one character at a time to check whether the first character entered is correct: If so, he continued the loop for consecutive characters. Using this technique. Bruce identified how much time the device takes to finish one complete password authentication process, through which he determined the correct characters in the target password.

Identify the type of attack launched by Bruce on the target OT network.

Options:

A- Code injection attack
B- Buller overflow attack
C- Reconnaissance attack
D- Side-channel attack

Answer:

D

Explanation:

Bruce's strategy of sending one character at a time and measuring the time it takes for the device to complete the password authentication process is characteristic of aside-channel attack. In side-channel attacks, attackers exploit information leaked during the execution of cryptographic algorithms or other security protocols. In this case, the timing information provides clues about the correct characters in the password.

EC-Council Certified Security Specialist (E|CSS) documents and study guide.

EC-Council Certified Security Specialist (E|CSS) course materials.

Question 5

Question Type: MultipleChoice

Which option best environmental controls options saves the hardware from humidity and heat, increases hardware performance, and maintains consistent room temperature?

Options:

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

Answer:

A

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 6

Question Type: MultipleChoice

Sam is a hacker who decided to damage the reputation of an organization. He started collecting information about the organization using social engineering techniques. Sam aims to gather critical information such as admin passwords and OS versions to plan for an attack.

Identify the target employee in the organization from whom Sam can gather the required information.

Options:

A- Helpdesk
B- Third-party service provider
C- System administrators
D- Customer support learn

Answer:

C

Explanation:

Social engineering attacks exploit human psychology to manipulate individuals into divulging sensitive information or performing actions that compromise security. In Sam's case, he aims to gather critical information about the organization using social engineering techniques.

System administrators are prime targets for social engineering attacks due to their privileged access and knowledge of the organization's infrastructure. They often have access to admin passwords, OS versions, and other critical information. By targeting system administrators, Sam can gather the required details to plan his attack effectively.

EC-Council Certified Security Specialist (E|CSS) course materials and study guide1.

EC-Council's focus on social engineering concepts and techniques in its training programs2.

Question 7

Question Type: MultipleChoice

Clark, a digital forensic expert, was assigned to investigate a malicious activity performed on an organization's network. The organization provided Clark with all the information related to the incident. In this process, he assessed the impact of the incident on the organization, reasons for and source of the incident, steps required to tackle the incident, investigating team required to handle the case, investigative procedures, and possible outcome of the forensic process.

Identify the type of analysis performed by Clark in the above scenario.

Options:

A- Data analysis
B- Log analysis
C- Traffic analysis
D- Case analysis

Answer:

D

Explanation:

In the given scenario, Clark performed acase analysis. This involves assessing the impact of the incident, understanding its reasons and source, determining the necessary steps to address it, assembling an investigative team, defining investigative procedures, and considering potential outcomes of the forensic process. Case analysis is crucial in digital forensics to effectively handle incidents and gather relevant evidence.

https://www.eccouncil.org/train-certify/certified-soc-analyst-csa/

Question 8

Question Type: MultipleChoice

Sarah, a forensic investigator, is working on a criminal case. She was provided with all the suspect devices. Sarah employs an imaging software tool for duplicating the original data from the suspect devices. However, the tool she employed failed to image the data as the suspect version of the drive was very old and incompatible with imaging software. Hence, Sarah used an alternative data acquisition technique and succeeded in imaging the data.

Which of the following types of data acquisition techniques did Sarah employ in the above scenario?

Options:

A- Bit-stream disk-to-disk
B- Bit-stream disk-to-image file
C- Sparse acquisition
D- Logical acquisition

Answer:

D

Explanation:

Sarah employed theLogical acquisitiontechnique in the given scenario. Logical acquisition

involves selectively extracting specific files, folders, or data from a device, bypassing the need for a full disk image.It is useful when traditional imaging methods fail due to compatibility issues or other constraints1. In this case, Sarah successfully imaged the data using an alternative approach, focusing on specific data rather than creating a bit-stream image of the entire drive.The logical acquisition method allowed her to work around the limitations posed by the outdated suspect drive version1.

EC-Council Certified Security Specialist (E|CSS) documents and study guide.

EC-Council Certified Security Specialist (E|CSS) course materials.

1:How to Handle Data Acquisition in Digital Forensics

Question 9

Question Type: MultipleChoice

Which option best cloud computing threats arises from authentication vulnerabilities, user-provisioning and de-provisioning vulnerabilities, hypervisor vulnerabilities, unclear roles and responsibilities, and misconfigurations?

Options:

A- Supply-chain failure
B- Isolation failure
C- Subpoena and e discovery
D- Privilege escalation

Answer:

D

Explanation:

The cloud computing threat described in the question arises from various vulnerabilities and misconfigurations related to authentication, user provisioning, hypervisors, and roles.Privilege escalationoccurs when an attacker gains more privileges than initially acquired. In this context, it refers to unauthorized elevation of access rights within a cloud environment.The mentioned vulnerabilities contribute to this risk, allowing an attacker to escalate their privileges beyond what is intended.Reference: EC-Council Certified Security Specialist (E|CSS) documents and study guide12.

Question 10

Question Type: MultipleChoice

James, a forensic specialist, was appointed to investigate an incident in an organization. As part of the investigation, James is attempting to identify whether any external storage devices are connected to the internal systems. For this purpose, he employed a utility to capture the list of all devices connected to the local machine and removed suspicious devices.

Identify the tool employed by James in the above scenario.

Options:

A- Promise Detect
B- DriveLetlerView
C- ESEDatabaseView
D- ProcDump

Answer:

B

Explanation:

In the given scenario, James employed theDriveLetterViewutility to capture the list of all devices connected to the local machine. DriveLetterView is a tool that displays a list of drive letters assigned to drives on a computer, including external storage devices.By using this utility, James can identify any suspicious devices connected to the internal systems.Reference: EC-Council Certified Security Specialist (E|CSS) documents and study guide12.