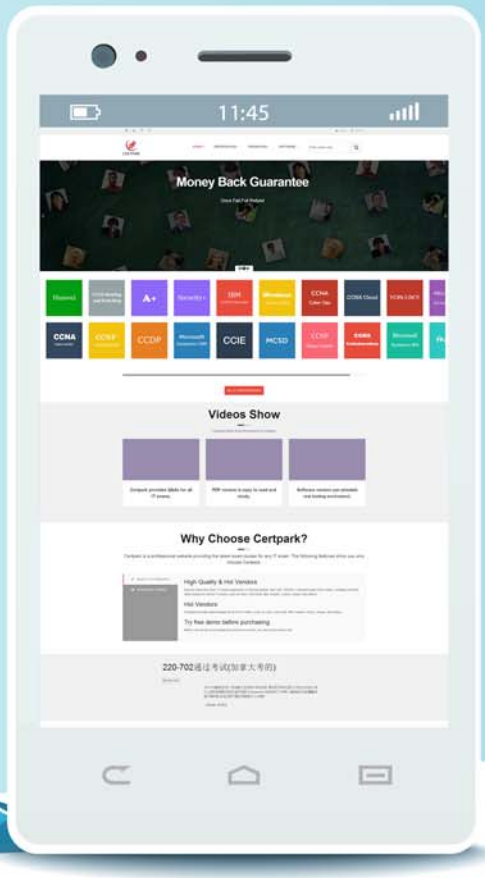
CERTPARK

QUESTION & ANSWER

CERTPARK.COM

Accurate Study Guides,
High Passing Rate!
provides update
free of charge
in one year!



https://www.certpark.com

Exam : **ECSS**

Title : EC-Council Certified Security Specialist Practice Test

Version : DEMO

1.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
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.
Reference: The explanation provided is based on general knowledge of environmental control systems in IT infrastructure. For detailed information, it is recommended to refer to the EC-Council Certified Security Specialist (E|CSS) study materials and official documentation.

2.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).
Reference: EC-Council Certified Security Specialist (E|CSS) course materials and documents

3.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.
Reference: 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.

4.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
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.
Reference: 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.

5.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
Answer: D

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.
Reference: The explanation provided is based on general knowledge of MAC forensics and the role of BSM in such environments. For detailed information, it is recommended to refer to the EC-Council Certified Security Specialist (E|CSS) study materials and official documentation.