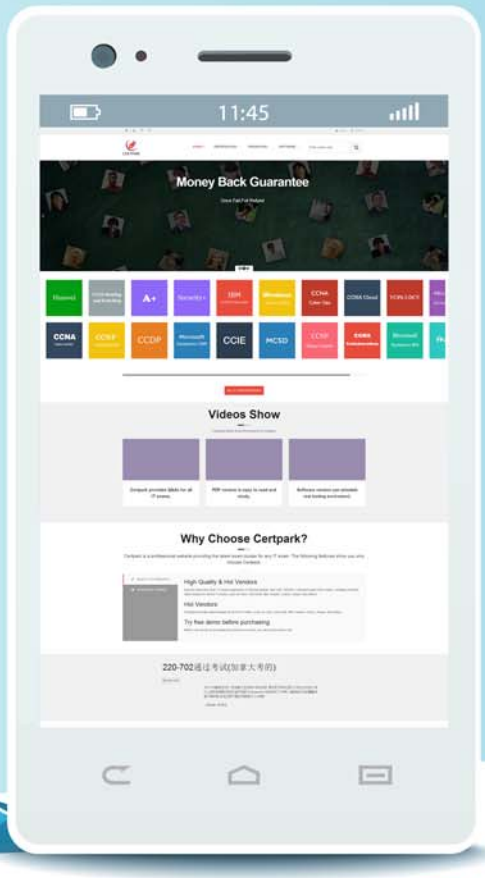
CERTPARK

QUESTION & ANSWER

CERTPARK.COM

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



https://www.certpark.com

Exam : **212-89**

Title : EC Council Certified Incident Handler (ECIH v2)

Version : DEMO

1.Patrick is doing a cyber forensic investigation. He is in the process of collecting physical evidence at the crime scene.
Which of the following elements he must consider while collecting physical evidence?
A. Published nameservers and web application source code
B. DNS information including domain and subdomains
C. Removable media, cable, and publications
D. Open ports, services, and operating system (OS) vulnerabilities
Answer: C

2.Eric works as a system administrator at ABC organization and previously granted several users with access privileges to the organizations systems with unlimited permissions. These privileged users could prospectively misuse their rights unintentionally, maliciously, or could be deceived by attackers that could trick them to perform malicious activities.
Which of the following guidelines would help incident handlers eradicate insider at tacks by privileged users?
A. Do not allow administrators to use unique accounts during the installation process
B. Do not use encryption methods to prevent administrators and privileged users from accessing backup tapes and sensitive information
C. Do not control the access to administrators and privileged users
D. Do not enable default administrative accounts to ensure accountability
Answer: D

3.Which of the following email security tools can be used by an incident handler to prevent the organization against evolving email threats?
A. Mx Toolbox
B. G Suite Toolbox
C. Email Header Analyzer
D. Gpg4win
Answer: D

4.Racheal is an incident handler working at an organization called Inception Tech. Recently, numerous employees have been complaining about receiving emails from unknown senders. In order to prevent employees from spoof ng emails and keeping security in mind, Racheal was asked to take appropriate actions in this matter. As a part of her assignment, she needs to analyze the email headers to check the authenticity of received emails.
Which of the following protocol/authentication standards she must check in email header to analyze the email authenticity?
A. POP
B. SNMP
C. DKIM
D. ARP
Answer: C

5.Bonney's system has been compromised by a gruesome malware.

What is the primary step that is advisable to Bonney in order to contain the malware incident from spreading?
What is the cause of this issue?
A. Complaint to police in a formal way regarding the incident
B. Turnoff the infected machine
C. Leave it to the network administrators to handle
D. Call the legal department in the organization and info m about the incident
Answer: B