CertNexus CFR-410 Mock Exam

Shared by Alford on 17-06-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

It was recently discovered that many of an organization's servers were running unauthorized cryptocurrency mining software. Which option best assets were being targeted in this attack? (Choose two.)

Options:

A- Power resources
B- Network resources
C- Disk resources
D- Computing resources
E- Financial resources

Answer:

A, B

Question 2

Question Type: MultipleChoice

A company website was hacked via the following SQL query:

email, passwd, login_id, full_name FROM members

WHERE email = ''attacker@somewhere.com''; DROP TABLE members; --''

Which of the following did the hackers perform?

Options:

A- Cleared tracks of attacker@somewhere.com entries
B- Deleted the entire members table
C- Deleted the email password and login details
D- Performed a cross-site scripting (XSS) attack

Answer:

C

Question 3

Question Type: MultipleChoice

The incident response team has completed root cause analysis for an incident. Which option best actions should be taken in the next phase of the incident response process? (Choose two.)

Options:

A- Providing a briefing to management
B- Updating policies and procedures
C- Training staff for future incidents
D- Investigating responsible staff
E- Drafting a recovery plan for the incident

Answer:

B, E

Question 4

Question Type: MultipleChoice

Which of the following actions should be done by the incident response team after completing the recovery phase of the cyber incident caused by malware?

Options:

A- Eradicate the malware.
B- Conduct lessons learned.
C- Isolate the malware from the system.
D- Collect evidence for the lawsuit.
E- Analyze the behavior of the malware.

Answer:

B

Explanation:

After completing the recovery phase of a cyber incident, the incident response team should conduct lessons learned. This phase involves reviewing the incident to identify what went well, what could be improved, and how to better prepare for future incidents. This helps improve incident response processes, policies, and defenses moving forward.

Question 5

Question Type: MultipleChoice

An incident handler is assigned to initiate an incident response for a complex network that has been affected

by malware. Which of the following actions should be taken FIRST?

Options:

A- Make an incident response plan.
B- Prepare incident response tools.
C- Isolate devices from the network.
D- Capture network traffic for analysis.

Answer:

D

Question 6

Question Type: MultipleChoice

An incident responder was asked to analyze malicious traffic. Which of the following tools would be BEST for this?

Options:

A- Hex editor
B- tcpdump
C- Wireshark

D- Snort

Answer:

C

Question 7

Question Type: MultipleChoice

Which of the following attack vectors capitalizes on a previously undisclosed issue with a software application?

Options:

A- Zero-Day Exploit
B- Brute Force
C- Misconfiguration
D- Ransomware
E- Phishing

Answer:

A

Explanation:

A Zero-Day Exploit targets vulnerabilities in software that are unknown to the software vendor or the public. Since the issue has not been disclosed or patched yet, attackers can exploit it before any fix or mitigation is made available, hence the term 'zero-day.' Would you like to explore how organizations can defend against such threats?

Question 8

Question Type: MultipleChoice

Which option best attacks involves sending a large amount of spoofed User Datagram Protocol (UDP) traffic to a router's broadcast address within a network?

Options:

A- Land attack
B- Fraggle attack
C- Smurf attack
D- Teardrop attack

Answer:

C

Question 9

Question Type: MultipleChoice

Which of the following security best practices should a web developer reference when developing a new web- based application?

Options:

A- Control Objectives for Information and Related Technology (COBIT)
B- Risk Management Framework (RMF)
C- World Wide Web Consortium (W3C)
D- Open Web Application Security Project (OWASP)

Answer:

D

Question 10

Question Type: MultipleChoice

Which approach to cybersecurity involves a series of defensive mechanisms that are layered to protect valuable data and information?

Options:

A- Network segmentation
B- Defense in depth

C- Tiered security
D- Endpoint detection and response

Answer:

B

Explanation:

Defense in depth is a cybersecurity strategy that uses multiple layers of security controls and measures to protect data and systems. This layered approach ensures that if one security measure is bypassed, others will still provide protection, making it more difficult for attackers to succeed.