CertNexus CFR-410 Practice Questions

Shared by White on 21-10-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which part of a proactive approach to system security is responsible for identifying all possible threats to a system to be categorized and analyzed?

Options:

A- Threat assessment
B- Threat intelligence
C- Threat modeling
D- Threat hunting

P2P exams

Answer:

C

Explanation:

Threat modeling is the process of identifying, categorizing, and analyzing potential threats to a system. It helps organizations understand the security risks they face and allows them to design controls to mitigate those risks proactively.

Question 2

Question Type: MultipleChoice

P2P exams

After a security breach, a security consultant is hired to perform a vulnerability assessment for a company's web application. Which option best tools would the consultant use?

Options:

A- Nikto
B- Kismet
C- tcpdump
D- Hydra

Answer:

A

Question 3

Question Type: MultipleChoice

Based on Payment Card Industry Data Security Standard (PCI DSS) compliance requirements, an organization must retain logs for what length of time?

Options:

A- 3 months
B- 6 months
C- 1 year
D- 5 years

Answer:

C

Question 4

Question Type: MultipleChoice

An administrator believes that a system on VLAN 12 is Address Resolution Protocol (ARP) poisoning clients on the network. The administrator attaches a system to VLAN 12 and uses Wireshark to capture traffic. After

reviewing the capture file, the administrator finds no evidence of ARP poisoning. Which option best actions should the administrator take next?

Options:

A- Clear the ARP cache on their system.
B- Enable port mirroring on the switch.
C- Filter Wireshark to only show ARP traffic.
D- Configure the network adapter to promiscuous mode.

Answer:

D

Question 5

Question Type: MultipleChoice

What is the definition of a security breach?

Options:

A- An event or series of correlated events that indicate a potential violation of some control or policy.
B- Unauthorized access that violates the authentication, authorization, and accounting of an information asset through intentional access, destruction, or manipulation of an information asset.
C- An event or series of uncorrelated events that indicate a potential violation of some control or policy has occurred.
D- Unauthorized access that violates the confidentiality, integrity, or availability of an information asset in the form of unintentional access, destruction, or manipulation of an information asset.

Answer:

B

Explanation:

A security breach refers to unauthorized access that compromises the security of an information asset, violating controls such as authentication, authorization, or accounting. This breach often involves intentional actions like accessing, destroying, or manipulating the asset without proper authorization.

Question 6

Question Type: MultipleChoice

A security operations center (SOC) analyst observed an unusually high number of login failures on a particular database server. The analyst wants to gather supporting evidence before

escalating the observation to management. Which of the following expressions will provide login failure data for 11/24/2015?

Options:

A- grep 20151124 security_log | grep --c ''login failure''
B- grep 20150124 security_log | grep ''login_failure''
C- grep 20151124 security_log | grep ''login''
D- grep 20151124 security_log | grep --c ''login''

Answer:

C

Question 7

Question Type: MultipleChoice

During which phase of the incident response process should an organization develop policies and procedures for incident handling?

Options:

A- Containment
B- Preparation
C- Identification
D- Recovery

Answer:

B

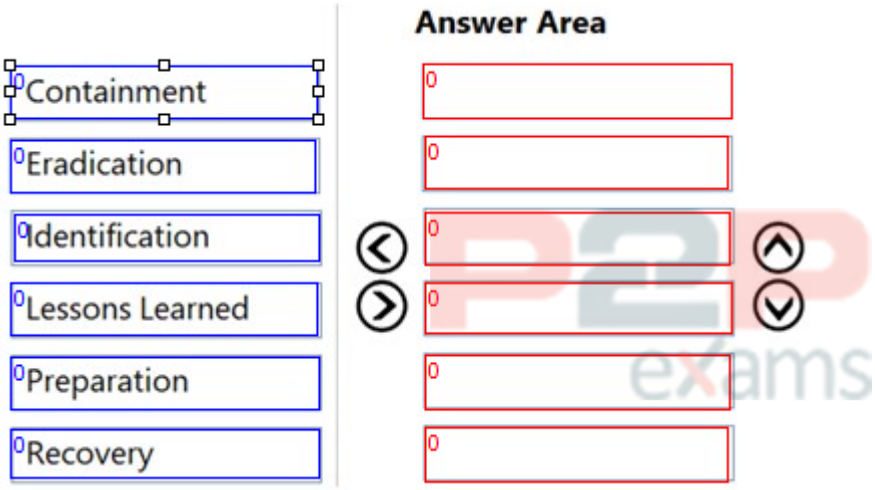
Explanation:

The Preparation phase is when an organization should develop policies, procedures, and strategies for handling incidents. This phase ensures that the organization is ready to respond effectively by having the necessary tools, resources, and plans in place before an incident occurs.

Question 8

Question Type: OrderList

What is the correct order of the DFIR phases?



Answer:

PreparationIdendificationContainmentEradicationRecoveryLessons Learned

Question 9

Question Type: MultipleChoice

During the forensic analysis of a compromised computer image, the investigator found that critical files are missing, caches have been cleared, and the history and event log files are empty. According to this scenario, which of the following techniques is the suspect using?

Options:

A- System hardening techniques
B- System optimization techniques
C- Defragmentation techniques
D- Anti-forensic techniques

Answer:

D

Question 10

Question Type: MultipleChoice

A security administrator notices a process running on their local workstation called SvrsScEsdKexzCv.exe.

The unknown process is MOST likely:

Options:

A- Malware
B- A port scanner
C- A system process
D- An application process

Answer:

A

To Get Premium Files for CFR-410 Visit

https://www.p2pexams.com/products/cfr-410

For More Free Questions Visit

https://www.p2pexams.com/certnexus/pdf/cfr-410

