

CERTPARK



QUESTION & ANSWER



CERTPARK.COM

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



Exam : **312-38**

Title : **Certified Network Defender**

Version : **DEMO**

1.Management decides to implement a risk management system to reduce and maintain the organization's risk at an acceptable level.

Which of the following is the correct order in the risk management phase?

- A. Risk Identification, Risk Assessment, Risk Treatment, Risk Monitoring & Review
- B. Risk Treatment, Risk Monitoring & Review, Risk Identification, Risk Assessment
- C. Risk Assessment, Risk Treatment, Risk Monitoring & Review, Risk Identification
- D. Risk Identification. Risk Assessment. Risk Monitoring & Review, Risk Treatment

Answer: A

Explanation:

The correct order in the risk management phase starts with Risk Identification, where potential business risks are determined. This is followed by Risk Assessment, which involves analyzing and prioritizing the identified risks. Next is Risk Treatment, where plans are made to mitigate the risks. Finally, Risk Monitoring & Review is conducted to oversee the risk management process and make necessary adjustments. This sequence ensures a structured and effective approach to managing risks within an organization.

Reference: The sequence aligns with the widely recognized ISO 31000 risk management standard, which outlines these core steps in managing risks¹²³.

2.John has implemented_____in the network to restrict the limit of public IP addresses in his organization and to enhance the firewall filtering technique.

- A. DMZ
- B. Proxies
- C. VPN
- D. NAT

Answer: D

Explanation:

Network Address Translation (NAT) is a network function that translates private IP addresses into a public IP address. This technique restricts the number of public IP addresses required by an organization, as multiple devices on a private network can share a single public IP address. NAT also enhances firewall filtering techniques by hiding the internal IP addresses from the external network, which adds a layer of security by making it more difficult for attackers to target specific devices within the organization's network. It is a common practice in network security to use NAT in conjunction with firewalls to manage the traffic entering and leaving the network, ensuring that only authorized access is permitted.

Reference: The information provided aligns with the Certified Network Defender (CND) program's focus on network defense fundamentals, including the application of network security controls like NAT¹². Additionally, NAT's role in conserving IP addresses and providing security by hiding internal network addresses is well-documented and is part of the network security best practices³⁴⁵.

3.What command is used to terminate certain processes in an Ubuntu system?

- A. #grep Kill [Target Process}
- B. #kill-9[PID]
- C. #ps ax Kill
- D. # netstat Kill [Target Process]

Answer: B

Explanation:

In Ubuntu, to terminate a specific process, you would use the kill command followed by the signal you want to send and the Process ID (PID) of the target process. The -9 signal is the SIGKILL signal, which forcefully terminates the process. The correct syntax is kill -9 [PID], where [PID] is replaced with the actual numerical ID of the process you wish to terminate.

Reference: This information is consistent with standard Linux documentation and practices as well as the Certified Network Defender (CND) course material, which covers system administration and security tasks including process management. The kill command is a fundamental tool for process management in Unix-like operating systems, which is covered in the CND curriculum.

4. Consider a scenario consisting of a tree network. The root Node N is connected to two main nodes N1 and N2. N1 is connected to N11 and N12. N2 is connected to N21 and N22.

What will happen if any one of the main nodes fail?

- A. Failure of the main node affects all other child nodes at the same level irrespective of the main node.
- B. Does not cause any disturbance to the child nodes or its transmission
- C. Failure of the main node will affect all related child nodes connected to the main node
- D. Affects the root node only

Answer: C

Explanation:

In a tree network, each node is connected in a hierarchical manner, with the root node at the top. If a main node (such as N1 or N2) fails, all the child nodes connected to it (N11, N12 for N1 and N21, N22 for N2) will be affected because the tree structure relies on the connectivity of the parent node to its children. The failure of a main node will disrupt the transmission path from the root to the child nodes, leading to a loss of connectivity for those child nodes. This is consistent with the principles of network resilience and fault tolerance as outlined in the EC-Council's Certified Network Defender (CND) program, which emphasizes the importance of each node in maintaining the network's overall integrity.

Reference: The explanation is based on the standard network topologies and fault tolerance principles covered in the EC-Council's Certified Network Defender (CND) curriculum.

5. Stephanie is currently setting up email security so all company data is secured when passed through email. Stephanie first sets up encryption to make sure that a specific user's email is protected. Next, she needs to ensure that the incoming and the outgoing mail has not been modified or altered using digital signatures.

What is Stephanie working on?

- A. Confidentiality
- B. Availability
- C. Data Integrity
- D. Usability

Answer: C

Explanation:

Stephanie is working on ensuring data integrity for her company's email communications. Data integrity refers to the assurance that data has not been altered or tampered with during transit. By setting up encryption, Stephanie is ensuring confidentiality, which protects the contents of the email from being

read by unauthorized parties. However, to ensure that the emails have not been modified, she is implementing digital signatures. Digital signatures provide a means to verify the authenticity of the sender and to ensure that the message has not been changed, which directly relates to the concept of data integrity in cybersecurity.

Reference: The information aligns with the objectives and documents of the EC-Council's Certified Network Defender (CND) program, which emphasizes the importance of protecting data integrity through measures like digital signatures as part of a defense-in-depth security strategy¹.