Eccouncil 312-38 CND Practice Questions

Shared by Soto on 17-08-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which of the information below can be gained through network sniffing? (Select all that apply)

Options:

A- Telnet Passwords
B- Syslog traffic
C- DNS traffic
D- Programming errors

Answer:

A, B, C

Explanation:

Network sniffing is a technique used to capture and analyze packets traveling across a network. Through network sniffing, one can potentially gain access to a variety of sensitive information, depending on the protocols being used and the security measures in place.

Telnet Passwords (A): Telnet is an older protocol that transmits data, including login credentials, in clear text.This makes Telnet passwords particularly vulnerable to network sniffing1.

Syslog Traffic (B): Syslog is a standard for message logging.If not properly secured, syslog traffic can be intercepted, revealing system messages and metadata about network activities1.

DNS Traffic : DNS traffic includes queries and responses that can be captured to reveal which domains are being requested by users on the network.This can provide insights into user behavior and network structure1.

Programming Errors (D): While network sniffing can capture packets that may contain the results of programming errors, such as error messages or malformed packets, it does not directly reveal the programming errors themselves. Sniffing tools capture the traffic but do not analyze the code within the applications generating that traffic.

Question 2

Question Type: MultipleChoice

Leslie, the network administrator of Livewire Technologies, has been recommending multilayer inspection firewalls to deploy the company's infrastructure. What layers of the TCP/IP model can it protect?

Options:

A- Network interface, TCP, and IP
B- Application, TCP, and IP
C- IP. application, and network interface
D- Application, IP, and network interface

Answer:

B

Explanation:

Multilayer inspection firewalls, also known as Next-Generation Firewalls (NGFWs), are designed to provide comprehensive security by inspecting traffic across multiple layers of the TCP/IP model. These firewalls offer protection at the:

Application Layer: They can analyze and filter traffic based on application-level protocols and payloads, such as HTTP, FTP, and DNS, providing protection against application-specific attacks.

Transport Layer (TCP): They inspect the transport layer to monitor and control TCP/UDP traffic, preventing threats such as port scans and DoS attacks.

Internet Layer (IP): They filter and monitor IP packets, enforcing security policies based on IP addresses and ensuring protection against IP-level attacks like IP spoofing.

By operating at these layers, multilayer inspection firewalls provide a robust defense mechanism against a wide range of network threats.

EC-Council Certified Network Defender (CND) Study Guide

Documentation on Next-Generation Firewalls and their functionalities

Question 3

Question Type: MultipleChoice

Which of the following interfaces uses hot plugging technique to replace computer components without the need to shut down the system?

Options:

A- SCSI
B- SATA
C- SDRAM
D- IDE

Answer:

B

Explanation:

The hot plugging technique allows for the replacement of computer components without the need to shut down the system. SATA (Serial Advanced Technology Attachment) is known for supporting hot plugging, which is particularly useful for hard drives and solid-state drives. This feature enables users to connect or disconnect the device while the system is running without risking data loss or damage. SCSI (Small Computer System Interface) also supports hot plugging for some devices, but SATA is more commonly associated with this capability for consumer-level computer components.

Question 4

Question Type: MultipleChoice

An organization's web server was recently compromised triggering its admin team into action to

defend the network. The admin team wants to place the web server in such a way that, even if it is

attacked, the other network resources will be unavailable to the attacker. Moreover, the network

monitoring will easily detect the future attacks. How can the admin team implement this plan?

Options:

A- They can place the web server outside of the organization in a remote place
B- They can remove the web server from their organization
C- They can place it in a separate DMZ area behind the firewall
D- They can place it beside the firewall

Answer:

C

Explanation:

Placing the web server in a separate Demilitarized Zone (DMZ) behind the firewall is a security best practice that allows an organization to isolate its public-facing services from the internal network. This setup ensures that if the web server is compromised, the attacker would not have direct access to the internal network resources. Additionally, the DMZ provides a controlled environment where network traffic to and from the web server can be monitored effectively, facilitating the detection of any future attacks. The firewall serves as a barrier, with specific rules that only allow necessary communication to and from the DMZ, thereby enhancing the overall security posture of the organization.

Question 5

Question Type: MultipleChoice

Wallcot, a retail chain in US and Canada, wants to improve the security of their administration

offices. They want to implement a mechanism with two doors. Only one of the doors can be opened at a

time. Once people enter from the first door, they have to be authorized to open the next one. Failing

the authorization, the person will be locked between the doors until an authorized person lets him or

her out. What is such a mechanism called?

Options:

A- Mantrap
B- Physical locks
C- Concealed detection device
D- Alarm system

Answer:

A

Explanation:

Theapt-getcommand is a powerful and free package management utility for Debian-based Linux distributions. It is used for handling packages and is utilized to install, update, and remove software on Debian systems. Theapt-getcommand is the recommended tool for doing upgrades from one Debian GNU/Linux release to another, as it effectively manages dependencies and ensures that all necessary changes are made during an upgrade.

Question 6

Question Type: MultipleChoice

Will is working as a Network Administrator. Management wants to maintain a backup of all the company data as soon as it starts operations. They decided to use a RAID backup storage technology for their data backup

plan. To implement the RAID data backup storage, Will sets up a pair of RAID disks so that all the data written to one disk is copied automatically to the other disk as well. This maintains an additional copy of the dat

a.

Which RAID level is used here?

Options:

A- RAID 3
B- RAID 1
C- RAID 5
D- RAID 0

Answer:

B

Explanation:

The RAID level used here is RAID 1, which is also known as disk mirroring. In this setup, all the

data written to one disk is automatically copied to another disk, creating an exact duplicate of the data. This ensures that if one disk fails, the data is still available on the other disk, providing redundancy and protecting against data loss. RAID 1 is a common choice for systems where data availability and integrity are critical.

Question 7

Question Type: MultipleChoice

Which of the following best describes the Log Normalization process?

Options:

A- It is a process of accepting logs from homogenous sources with the same formats and converting them into a different format
B- It is a process of accepting logs from homogenous sources with different formats and converting them into a common format
C- It is a process of accepting logs from heterogeneous sources with different formats and converting them into a common format
D- It is a process of accepting logs from heterogeneous sources with the same formats and converting them into a different format

Answer:

C

Explanation:

Log normalization is a critical process in network security, particularly within the context of Security Information and Event Management (SIEM) systems. The primary goal of log normalization is to standardize the format of log data received from various sources, which often have different formats and structures. This standardization allows for more efficient and effective analysis, correlation, and storage of log data. By converting disparate log data into a common format, SIEM systems can more easily identify patterns, detect anomalies, and trigger alerts for potential security incidents. This process is essential for managing the complexity and volume of log data in modern network environments.