Download WGU Network-and-Security-Foundation Exam Dumps Free

Shared by Martinez on 17-06-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

An attacker sends emails claiming that an online account has been locked. The email provides a fake link with the goal of tricking users into providing login credentials.

Which malicious attack strategy is represented in the scenario?

Options:

A- Phishing
B- IP address spoofing
C- Session hijacking
D- Man-in-the-middle attack

Answer:

A

Explanation:

Phishing is a cyberattack where attackers impersonate legitimate entities (e.g., banks, companies) and send fraudulent emails or messages designed to trick recipients into revealing sensitive information, such as usernames, passwords, or financial details. The fake link in the email directs victims to a malicious site that captures their credentials.

IP address spoofing disguises a system's identity but does not involve email deception.

Session hijacking takes over an active session but does not involve email scams.

Man-in-the-middle attack intercepts communication rather than tricking users via emails.

Question 2

Question Type: MultipleChoice

What is the layer of the OSI model that creates, maintains, and disconnects process communications over the network?

Options:

A- Data link
B- Physical
C- Session
D- Transport

Answer:

C

Explanation:

The Session layer (Layer 5 of the OSI model) is responsible for establishing, maintaining, and terminating communication sessions between network applications. It ensures that data exchanges remain synchronized and structured.

Data link layer handles error detection and frame transmission.

Physical layer deals with hardware-level transmission.

Transport layer ensures reliable data delivery but does not manage sessions.

Question 3

Question Type: MultipleChoice

Users of a network have been experiencing issues. In the course of troubleshooting, an administrator wants to test DNS resolution against a host.

Which command in Linux should be used for this purpose?

Options:

A- traceroute
B- netstat
C- dig
D- ifconfig

Answer:

C

Explanation:

The dig command in Linux is used for DNS troubleshooting. It queries DNS records and provides detailed information about domain name resolutions.

traceroute tracks the path packets take to a destination but does not diagnose DNS.

netstat lists active connections, not DNS records.

ifconfig is used for managing network interfaces.

Question 4

Question Type: MultipleChoice

A computer network has software that tracks successful and unsuccessful connection attempts to the network in order to better identify attacks.

Which network security concept does this scenario address?

Options:

A- Accounting
B- Authentication
C- Availability
D- Authorization

Answer:

A

Explanation:

Accounting (also known as auditing or logging) is a network security concept that tracks user activities, including successful and failed authentication attempts, system changes, and resource access. This helps in detecting and mitigating security breaches.

Authentication verifies user identity but does not track activity.

Availability ensures systems remain operational.

Authorization controls user permissions but does not log activities.

Question 5

Question Type: MultipleChoice

When setting up a network, a technician needs a router that connects computers together and connects computers to the internet.

Which router should be used?

Options:

A- Inter-provider border router
B- Subscriber edge router
C- Broadband router
D- Core router

Answer:

C

Explanation:

A broadband router is a type of network router that connects multiple computers within a local network while also providing internet access. It functions as a gateway between the local network and the internet by handling data packet transmission and routing. Broadband routers are widely used in small offices and homes because they offer essential networking services, including DHCP, NAT, and sometimes wireless connectivity.

Inter-provider border routers are used by ISPs to route data between different providers and do not serve as an internet gateway for end users.

Subscriber edge routers are typically deployed at the edge of an ISP's network to connect subscriber networks but do not provide full internet routing functionalities.

Core routers operate at the backbone level of a network, facilitating high-speed data transfer but not connecting end-user devices directly.

Question 6

Question Type: MultipleChoice

A company wants to implement a cloud service to obtain access to virtual machines. The company wants to be able to choose the operating systems and configure each of the machines.

What is the type of cloud service model that fits the needs of this company?

Options:

A- Function as a Service (FaaS)
B- Infrastructure as a Service (IaaS)
C- Platform as a Service (PaaS)
D- Software as a Service (SaaS)

Answer:

B

Explanation:

Infrastructure as a Service (IaaS) provides virtualized computing resources over the cloud, including virtual machines where users can install and configure their own operating systems and applications. It offers flexibility and scalability without requiring hardware investment. Examples include AWS EC2 and Microsoft Azure Virtual Machines.

FaaS executes small code functions without infrastructure management.

PaaS provides a managed platform but not full OS control.

SaaS offers ready-to-use applications without infrastructure control.

Question 7

Question Type: MultipleChoice

An attacker uses a network device to take over an existing connection between two network computers.

Which malicious attack strategy is represented in the scenario?

Options:

A- Dictionary attack
B- Social engineering
C- Session hijacking
D- IP address spoofing

Answer:

C

Explanation:

Session hijacking occurs when an attacker takes over an established connection between two devices, often by stealing session tokens or manipulating network traffic. This allows the attacker to impersonate a legitimate user and gain unauthorized access.

Dictionary attack involves password guessing, not hijacking active connections.

Social engineering tricks users into providing information but does not hijack sessions.

IP address spoofing disguises the attacker's identity but does not necessarily take over a session.