WGU Network-and-Security-Foundation D315 Practice Questions

Shared by Day on 02-11-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

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

P2P exams

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.

P2P exams

Question 2

Question Type: MultipleChoice

A company's internal messaging system is being redesigned. The authentication procedures were so cumbersome that employees were using personal email to communicate.

What is the security principle implemented in this scenario?

Options:

A- Zero-trust model
B- Least common mechanism
C- Psychological acceptability
D- Fail-safe

Answer:

C

Explanation:

Psychological acceptability states that security measures should be user-friendly and not overly burdensome. If security controls are too complex, users may bypass them, leading to weaker security. In this case, employees used personal email because authentication procedures were too cumbersome.

Zero-trust model enforces strict access control, not usability.

Least common mechanism limits shared resources.

Fail-safe ensures secure failure handling, not usability.

Question 3

Question Type: MultipleChoice

An organization is the victim of an attack in which an attacker gains unauthorized access to a computer to steal information and forward it via the internet to another attacker.

What is the purpose of this attack?

Options:

A- Launch point
B- Denial of availability
C- Data export
D- Data modification

Answer:

C

Explanation:

This scenario describes a data export attack, where an attacker steals sensitive information (e.g., personal data, trade secrets, or financial records) and transfers it to another entity, often for malicious purposes.

Launch point refers to using a compromised system for further attacks.

Denial of availability disrupts access to resources.

Data modification involves unauthorized changes rather than theft.

P2P exams

Question 4

Question Type: MultipleChoice

A host is already set up with an operating system. An administrator wants to install a hypervisor atop the operating system to allow for setting up virtual machines.

Which hypervisor should be used?

Options:

A- Open source
B- Proprietary
C- Type 1
D- Type 2

P2P exams

Answer:

D

Explanation:

A Type 2 hypervisor (hosted hypervisor) runs on top of an existing operating system and allows for the creation of virtual machines. Examples include VMware Workstation and Oracle VirtualBox.

Type 1 hypervisors run directly on hardware without an OS (e.g., VMware ESXi, Microsoft Hyper-V).

Open-source and proprietary describe licensing models, not hypervisor types.

Question 5

Question Type: MultipleChoice

A company is designing an information system and is maintaining a focus on the user experience and resulting productivity rather than on the technology itself.

What is the security principle implemented in this scenario?

Options:

A- Least common mechanism
B- Fail-safe
C- Zero-trust model
D- Human-centeredness

Answer:

D

Explanation:

Human-centeredness in security design prioritizes user experience and productivity while implementing security measures. It ensures that security policies are intuitive and do not excessively burden users, reducing resistance to security compliance.

Least common mechanism minimizes shared resources to enhance security.

Fail-safe ensures secure defaults in case of system failure.

Zero-trust model assumes no inherent trust in users or devices.

Question 6

Question Type: MultipleChoice

An organization is the victim of an attack in which an attacker targets a computer to use as a

tool to infect and target other computers in a larger attack.

What is the purpose of this attack?

Options:

A- Denial of availability
B- Data export
C- Data modification
D- Launch point

Answer:

D

Explanation:

A launch point attack occurs when an attacker compromises a system and uses it as a foothold to spread malware, conduct reconnaissance, or launch further attacks against other systems. Botnets and command-and-control (C2) servers operate this way.

Denial of availability disrupts service, but does not spread attacks.

Data export steals data instead of launching further attacks.

Data modification changes existing information but does not involve propagating threats.

Question 7

Question Type: MultipleChoice

A company is specifically worried about rogue access points.

Which strategy should be used as a mitigation against this type of attack?

Options:

A- Decrease the wireless range
B- Disable unnecessary services
C- Configure switch port tracing
D- Monitor normal traffic patterns

Answer:

C

Explanation:

Configuring switch port tracing helps detect unauthorized devices, such as rogue access points, that are connected to the network. Network administrators can use port security and intrusion detection systems (IDS) to monitor and block unauthorized access points.

Decreasing wireless range may limit exposure but does not actively detect rogue APs.

Disabling unnecessary services improves security but does not prevent rogue APs.

Monitoring traffic patterns helps detect anomalies but does not directly stop rogue APs.

Question 8

Question Type: MultipleChoice

An organization has experienced rogue access points in the past and wants to take actions to mitigate this type of attack.

What should this organization do?

Options:

A- Require complex passwords
B- Use monitor mode scanning
C- Use server-side validation
D- Disallow ICMP packets on the firewall

Answer:

B

Explanation:

Monitor mode scanning allows administrators to detect unauthorized or rogue access points broadcasting in the network. This technique, along with wireless intrusion detection systems (WIDS), helps identify and block unauthorized devices.

Requiring complex passwords enhances security but does not prevent rogue APs.

Server-side validation secures applications, not wireless networks.

Disallowing ICMP packets is a security measure but does not address rogue APs.

Question 9

Question Type: MultipleChoice

A company wants to use a cloud service to obtain virtual machines with pre-installed and configured software.

Which cloud service model should be used?

Options:

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

Answer:

C

Explanation:

Platform as a Service (PaaS) provides a pre-configured computing environment that includes an operating system, runtime, and development tools, making it ideal for developers who want a ready-to-use platform. Examples include Google App Engine and Microsoft Azure App Services.

SaaS provides fully hosted applications, not just pre-configured virtual machines.

IaaS provides infrastructure without pre-installed software.

FaaS executes specific functions without persistent infrastructure.

Question 10

Question Type: MultipleChoice

An attacker changes a computer's identification to appear as an authorized computer in a target network.

Which type of cyberattack is described?

Options:

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

Answer:

D

Explanation:

IP address spoofing is a cyberattack where an attacker disguises their system by falsifying its IP address, making it appear as a trusted device in a network. This technique is used for bypassing security controls, launching denial-of-service (DoS) attacks, or impersonating legitimate users.

Pharming redirects users to fake websites to steal credentials.

Man-in-the-middle attack intercepts communications between two parties.

Session hijacking takes over an active session but does not involve falsifying an IP address.

Question 11

Question Type: MultipleChoice

In the process of setting up a Linux-based network system, a technician needs to determine if there is connectivity to a hostname.

Which command should be used?

Options:

A- ping
B- nslookup
C- ifconfig
D- dig

Answer:

A

Explanation:

The ping command in Linux is used to check network connectivity to a specific hostname or IP address. It sends ICMP Echo Request packets and measures response times.

nslookup is used for DNS lookups, not connectivity testing.

ifconfig displays network interface configurations but does not test connectivity.

dig is used for detailed DNS queries.

To Get Premium Files for Network-and-Security-Foundation Visit

https://www.p2pexams.com/products/network-and-security-foundation

For More Free Questions Visit

https://www.p2pexams.com/wgu/pdf/network-and-security-foundation

