M01B_Midterm2_Ch7-10_Fall_2024_Net_Learn

Candidate: Richard Habib (richard_habib1)
Date: 11/5/2024, 3:32:10 PM • **Time Spent:** 02:45:24

Score: 95%

Passing Score: 70%

Question 1.

✓ Correct

Which feature allows Nmap to work out hop counts?

○ --script switch

○ -sn switch

→ ● --traceroute switch

○ -p switch

Explanation

The --traceroute switch in Nmap is used to work out hop counts, helping to map the path packets take from the scanner to the target host.

The -sn switch is used for host discovery without port scanning, not for tracing routes.

The --script switch is used to specify scripts for Nmap to execute, not for tracing routes.

The -p switch is used to specify port ranges for scanning, not for tracing routes.

References

7.2.8 Lab: Scan for Web Services with Nmap

8.2.2 Nmap

8.2.3 Nmap Port Scanning

q_nmap_traceroute_purpose_n09.question.fex

Question 2. ✓ Correct

Which of the following is a potential consequence of a rogue DHCP server changing the default gateway address for a subnet?

○ Increased internet speed for all clients

○ Automatic resolution of IP address conflicts

○ Improved network security and encryption

→ ● Routing communications through the attacker's machine

Explanation

A rogue DHCP server can be used by an attacker to change the default gateway address, directing all subnet traffic through the attacker's machine. This enables on-path (man-in-the-middle) attacks, where the attacker can intercept, modify, or redirect network traffic.

Changing the default gateway to a rogue server would not increase internet speed; it could actually degrade performance or disrupt connectivity.

This action would decrease, not improve, network security by potentially exposing all traffic to interception or manipulation by an attacker.

Altering the default gateway address does not resolve IP address conflicts; it changes the path traffic takes to reach external networks.

References

9.4.2 Rogue DHCP

9.4.3 Setting Up DHCP Snooping

9.4.6 Lab: Discover a Rogue DHCP Server

9.4.7 Lab: Configure DHCP Snooping

12.3.11 Lab: Enable Wireless Intrusion Prevention

q_rogue_dhcp_default_gateway_change_n09.question.fex

Question 3. ✓ Correct

What is an implicit deny in firewall configuration?

- ○ A rule that only denies traffic from specific countries
- → ● A default behavior to block traffic that does not match any rule
- ○ A temporary rule that denies access during peak hours
- ○ A rule that explicitly allows all traffic

Explanation

The implicit deny principle is a fundamental security measure in firewall configurations. It ensures that any traffic not explicitly allowed by the defined rules is automatically denied. This default blocking stance helps prevent unauthorized access by ensuring that only traffic that has been explicitly permitted can pass through the firewall.

A rule that explicitly allows all traffic is the opposite of implicit deny, as it would permit all traffic by default, which is not secure.

Implicit deny is not a temporary measure nor is it based on time-of-day conditions; it is a constant default behavior.

Implicit deny applies to all traffic that does not match any rule, not just traffic from specific geographic locations.

References

- **1.3.5 Transport and Application Layer and Security Functions**
- **5.4.1 Firewall Uses and Types**
- **5.4.2 Firewall Selection and Placement**
- **10.5.1 Security Rules and ACL Configuration**
- **10.5.4 Misconfigured Firewall and ACL Issues**
- **10.5.5 Creating Firewall ACLs**
- **10.5.7 Lab: Configure a Security Appliance**
- **10.5.8 Lab: Configure a Perimeter Firewall**
- **14.3.5 Cloud Firewall Security**

q_acl_implicit_deny_n09.question.fex

Question 4. ✓ Correct

What is a major security weakness of SNMP v2c?

→ ● It sends community strings in plaintext.

○ It uses strong encryption by default.

○ It supports too many users.

○ It restricts management operations to known hosts.

Explanation

The correct answer is that it sends community strings in plaintext. SNMP v2c's major security weakness is that it sends community strings in plaintext. This means that if the data is intercepted, the community strings can be easily read, posing a significant security risk.

SNMP v2c does not support encryption, let alone strong encryption.

The number of users supported is not a security weakness. SNMP v2c's security concerns are related to its lack of encryption and authentication mechanisms.

Restricting management operations to known hosts is actually a recommended security measure, not a weakness. Restricting operations to known hosts helps to improve security.

References

8.2.1 Network Discovery

8.3.1 SNMP Agents and Monitors

8.3.2 SNMP Security

8.3.3 Configuring an SNMP System on a Router

8.3.4 Monitoring a Switch with SNMP

8.3.5 Configuring SNMP Trap

q_snmp_security_v2c_security_weakness_n09.question.fex

Question 5. ✓ Correct

What is a potential diagnostic step for a host-based firewall issue?

○ Encrypting all outgoing traffic

○ Upgrading the firewall's firmware

→ ● Attempting a connection with the host firewall disabled

○ Increasing the firewall's memory allocation

Explanation

The correct answer is attempting a connection with the disabled host firewall. Disabling the host firewall temporarily can help diagnose if it is the cause of a connection issue. If the connection succeeds with the firewall disabled, it indicates the host firewall's configuration was blocking the connection.

Increasing the firewall's memory allocation does not directly address diagnosing configuration issues.

Upgrading the firewall's firmware might be necessary for other reasons but is not a direct diagnostic step for configuration issues.

Encrypting all outgoing traffic is a security measure and does not help diagnose firewall configuration problems.

References

- **1.3.5 Transport and Application Layer and Security Functions**
- **5.4.1 Firewall Uses and Types**
- **5.4.2 Firewall Selection and Placement**
- **10.5.1 Security Rules and ACL Configuration**
- **10.5.4 Misconfigured Firewall and ACL Issues**
- **10.5.5 Creating Firewall ACLs**
- **10.5.7 Lab: Configure a Security Appliance**
- **10.5.8 Lab: Configure a Perimeter Firewall**
- **14.3.5 Cloud Firewall Security**

q_misconfig_acl_firewall_diagnostic_step_n09.question.fex

Question 6. ✓ Correct

In a Windows environment, which protocol is typically used to access Microsoft Exchange mailboxes?

○ IMAP

→ ● MAPI

○ HTTPS

○ SMTP

Explanation

In a Windows environment, the proprietary Messaging Application Programming Interface (MAPI) protocol is typically used to access Microsoft Exchange mailboxes. MAPI allows for integration with Microsoft products and provides functionalities specific to Exchange.

IMAP is a general email access protocol and not specific to Microsoft Exchange.

SMTP is used for sending emails, not for accessing mailboxes.

HTTPS is a secure transport protocol used on the web, not specifically for accessing Microsoft Exchange mailboxes.

References

7.3.2 Internet Message Access Protocol

q_mailbox_mapi_exchange_n09.question.fex

Question 7. × Incorrect

What is the primary difference between ARP spoofing and ARP poisoning?

→ ○ ARP spoofing involves broadcasting fake ARP messages, while ARP poisoning refers to the state of the ARP cache.

● ~~ARP spoofing and ARP poisoning are terms for the same process, with no difference between them.~~

○ ARP poisoning is used to secure network communications, whereas ARP spoofing is a malicious activity.

○ ARP spoofing is a passive attack while ARP poisoning is an active attack.

Explanation

ARP spoofing is the act of sending out false ARP messages (unsolicited ARP replies) to a local network. These messages are designed to associate the attacker's MAC address with the IP address of another host, such as the default gateway. ARP poisoning, on the other hand, is the result of ARP spoofing. It describes the corrupted state of the ARP cache, where devices on the network have been tricked into sending data to the wrong MAC address. This distinction is crucial because it differentiates between the action (spoofing) and the consequence (poisoning).

ARP spoofing is actually an active attack; it involves actively sending out false ARP messages to manipulate the ARP cache of devices on the network. ARP poisoning is the result of these active attempts, not a separate form of attack.

ARP poisoning is not a security measure; it is the harmful result of ARP spoofing, which is a malicious activity aimed at compromising network security by corrupting the ARP cache.

ARP spoofing and ARP poisoning are terms for the same process is incorrect because it fails to distinguish between the act of sending spoofed ARP messages (ARP spoofing) and the resultant corrupted state of the ARP cache (ARP poisoning). Understanding the difference is important for diagnosing and mitigating such attacks.

References

9.3.3 Poison ARP

9.3.7 Lab: Poison ARP and Analyze with Wireshark

q_path_attack_arp_spoof_vs_poison_n09.question.fex

Question 8. ✓ Correct

What is an on-path attack?

→ ● A type of spoofing attack where a threat actor intercepts communications between two hosts.

○ A type of physical attack where the attacker physically intercepts a data transmission.

○ A cyber-attack that exclusively targets the path of data storage devices.

○ An attack where the threat actor creates a new path in a network to reroute data.

Explanation

The correct answer is a specific type of spoofing attack where a threat actor intercepts and possibly modifies communications between two hosts. This accurately describes an on-path attack, where the attacker positions themselves in the communication path between two hosts, allowing them to intercept and potentially alter the data being exchanged. This is a form of spoofing attack that targets the integrity and confidentiality of the data in transit.

The following are incorrect answers:

- A type of physical attack where the attacker physically intercepts a data transmission. This describes a physical interception, which is different from the digital interception and manipulation involved in on-path attacks.
- A cyber-attack that exclusively targets the path of data storage devices. On-path attacks target data in transit between two hosts, not the data storage paths or devices.
- An attack where the threat actor creates a new path in a network to reroute data. While this might involve manipulation of network paths, it doesn't capture the essence of intercepting and potentially modifying data between two hosts, which is central to on-path attacks.

References

9.3.1 On-Path Attacks

9.3.2 Performing an On-Path DHCP Attack

9.3.9 Lab: Perform a DHCP Spoofing On-Path Attack

9.4.8 Lab: Poison DNS

q_path_attack_description_n09.question.fex

Question 9. ✓ Correct

Which layer's diagram would show asset IDs, cable links, and wall/patch panel/switch port IDs?

→ ● PHY (Physical layer)

○ Application

○ Data Link (Layer 2)

○ Logical (IP/Layer 3)

Explanation

The PHY (Physical layer) diagram focuses on the physical components of the network, including asset IDs, cable links, and the identification of ports on wall panels, patch panels, and switches, providing a detailed view of the physical connections.

The Data Link layer deals with the interconnections between switches and routers at a protocol level, not the physical connections.

The Logical (IP/Layer 3) layer deals with IP addressing and routing, not physical connections.

The Application layer focuses on server instances and TCP/UDP ports in use, not physical network infrastructure.

References

8.1.8 Logical Network Diagrams

q_logi_diagram_physical_layer_n09.question.fex

Question 10. ✓ Correct

What are latency and jitter in the context of network performance?

○ Measures of network speed and efficiency

○ Techniques for optimizing bandwidth usage

○ Types of network security protocols

→ ● Problems of timing and sequence of packet delivery

Explanation

Latency refers to the delay before a transfer of data begins following an instruction for its transfer, while jitter is the variation in the delay of received packets. Both are crucial in determining the quality of real-time applications like VoIP and video streaming, as they affect the smoothness and quality of the transmission.

Latency and jitter are not security protocols but are related to the performance of data transmission.

While they can affect network speed and efficiency, latency and jitter specifically refer to timing and sequence issues in packet delivery.

These are not techniques for optimizing bandwidth usage but are issues that can negatively impact the quality of network services.

References

8.6.1 Common Performance Issues

q_qos_metrics_latency_and_jitter_description_n09.question.fex

Question 11. ✓ Correct

Why might an aggregation TAP drop frames under heavy load?

- ○ Because it requires a direct internet connection
- → ● Because it rebuilds streams into a single channel
- ○ Because it does not support gigabit signaling
- ○ Because it cannot handle encrypted traffic

Explanation

An aggregation TAP combines the upstream and downstream traffic into a single channel for monitoring. Under heavy load, the capacity of this single channel may be exceeded, leading to dropped frames as it cannot keep up with the volume of data.

Aggregation TAPs handle all types of traffic, including encrypted. The issue of dropping frames is related to load, not encryption.

Aggregation TAPs can support high-speed signaling. The potential for dropping frames is a matter of traffic volume, not the speed of the signaling.

The need for a direct internet connection is unrelated to an aggregation TAP's function or its potential to drop frames under heavy load.

References

8.5.1 Packet Capture

q_sniffers_aggregation_tap_issue_n09.question.fex

Question 12. × Incorrect

What is the minimum recommended password length for network appliances according to the document?

- ● ~~12 characters~~
- → ○ 14 characters
- ○ 10 characters
- ○ 8 characters

Explanation

For critical infrastructure like network appliances, the document recommends passwords to be 14 characters or longer to resist guessing and cracking attacks effectively.

8 characters is the minimum for general passwords, not for network appliances.

10 characters falls short of the recommendation for critical infrastructure.

12 characters is closer but still below the recommended length.

References

10.3.2 Device and Service Hardening

q_hardening_password_length_n09.question.fex

Question 13. ✓ Correct

How are the rules in a firewall's ACL processed?

○ Simultaneously

→ ● From top to bottom

○ From bottom to top

○ Randomly

Explanation

Firewall ACLs are processed sequentially from the top to the bottom. This order of processing is crucial for ensuring that the most specific rules are applied first. Once a rule that matches the traffic is found, the firewall takes the corresponding action (allow or block) and stops evaluating the rest of the rules. This method allows for efficient and precise control over network traffic.

From bottom to top is incorrect because it would mean the most general rules are evaluated first, which could lead to unintended access or blocking.

Random processing would result in unpredictable and unreliable firewall behavior, which is not acceptable in security contexts.

Firewalls do not process all rules simultaneously. Sequential processing is necessary to determine the specific action to take based on the order of the rules.

References

10.5.1 Security Rules and ACL Configuration

10.5.5 Creating Firewall ACLs

10.5.6 Lab: Configure Network Security Appliance Access

10.5.7 Lab: Configure a Security Appliance

10.5.8 Lab: Configure a Perimeter Firewall

10.5.10 Lab: Permit Traffic

10.5.11 Lab: Block Source Hosts

q_acl_rules_top_to_bottom_n09.question.fex

Question 14. ✓ Correct

What type of events does an audit log generally record?

→ ● Success/fail type events related to authentication

○ System configuration backups

○ Detailed descriptions of all user activities

○ Performance metrics for compute resources

Explanation

Audit logs are focused on recording the success or failure of authentication and authorization attempts, providing a clear record of who has accessed or attempted to access the system.

While user activities related to access may be recorded, audit logs specifically track authentication and authorization events.

System configuration backups are not the purpose of audit logs.

Performance metrics are recorded in performance/traffic logs, not audit logs.

References

8.4.1 Network Device Logs

8.4.2 Log Collectors and Syslog

8.4.3 Event Prioritization and Alerting

8.4.4 Security Information and Event Management

8.4.5 Log Reviews

8.4.6 Lab: Configure Logging in pfSense

8.4.7 Lab: Evaluate Event Logs in pfSense

8.4.8 Lab: Auditing Device Logs on a Cisco Switch

8.4.9 Lab: Configure Logging on Linux

8.4.10 Lab: View Event Logs

q_net_logs_audit_success_fail_n09.question.fex

Question 15. ✓ Correct

What is a reverse proxy used for?

○ Storing data permanently

○ Managing outbound traffic

→ ● Managing inbound traffic

○ Directly connecting clients to the Internet

Explanation

A reverse proxy is used for managing inbound traffic, acting as an intermediary for requests from the Internet to internal servers. It can provide additional security, load balancing, and caching services.

Managing outbound traffic is the role of a forward proxy.

Directly connecting clients to the Internet is not the purpose of a reverse proxy.

Storing data permanently is not a function of a reverse proxy; it may cache data temporarily to improve performance.

References

10.5.2 Proxy Servers

q_proxy_reverse_role_n09.question.fex

Question 16. ✓ Correct

What role does a Change Advisory Board (CAB) play in change management?

→ ● It approves major or significant changes.

○ It documents the need for change.

○ It creates the Request for Change (RFC) documents.

○ It implements the changes directly.

Explanation

The Change Advisory Board (CAB) is involved in the approval process for major or significant changes, ensuring that these changes are reviewed at an appropriate level and that they align with the organization's goals and risk tolerance.

The need for change is documented in the RFC, not by the CAB.

The CAB does not implement changes directly; it approves them.

RFC documents are created to propose changes, not by the CAB but by those identifying the need for change.

References

8.1.3 Change Management

q_agreements_cab_role_n09.question.fex

Question 17. ✓ Correct

Which of the following is NOT information that CDP can report?

→ ● MAC address table sizes

○ Device ID/hostname

○ Power over Ethernet usage

○ IOS version

Explanation

CDP can report various information such as device ID/hostname, IOS version, interface addresses and statistics, VLAN information, and Power over Ethernet usage. However, it does not report MAC address table sizes, as this information is not part of the CDP announcements.

Device ID/hostname is one of the basic pieces of information CDP reports to identify devices.

IOS version is reported by CDP to help in managing and troubleshooting Cisco devices.

Power over Ethernet usage is reported by CDP, which can be crucial for managing devices that rely on PoE for power.

References

8.2.4 Discovery Protocols

q_discovery_protocols_mac_address_not_n09.question.fex

Question 18. ✓ Correct

What is a common consequence of rogue devices and services in a network?

- ○ Increased network security.
- ○ Reduction in IT department workload.
- → ● Creation of new unmonitored attack surfaces.
- ○ Improved network efficiency.

Explanation

Rogue devices and services create new unmonitored attack surfaces that malicious adversaries can exploit, posing significant security risks.

Rogue devices and services typically compromise network efficiency by introducing security risks.

Rogue devices and services decrease network security by operating outside of administrative control.

The introduction of rogue devices and services increases the IT department's workload due to the need to identify and mitigate these security risks.

References

9.4.1 Rogue Devices and Services

q_rogue_devices_common_consequence_n09.question.fex

Question 19. ✓ Correct

What is the primary difference between footprinting and fingerprinting in network attacks?

○ Footprinting is used to enhance network security, while fingerprinting is used to decrease it.

→ ● Footprinting gathers general network information, while fingerprinting identifies specific device types.

○ Fingerprinting is a legal method of gathering information, while footprinting is not.

○ Footprinting aims to improve network performance, while fingerprinting does not.

Explanation

Footprinting and fingerprinting are both information gathering techniques used in network attacks, but they serve different purposes. Footprinting is about discovering the topology and general configuration of the network and security systems, while fingerprinting goes a step further to identify specific device and operating system types and versions. This distinction is crucial for attackers to tailor their attacks more effectively.

Neither footprinting nor fingerprinting aims to improve network performance. Both are used for gathering information for potential attacks.

The legality of footprinting and fingerprinting depends on the context and intent, not the method itself. Both can be used maliciously.

Neither technique is used to enhance network security. Both are used by attackers to gather information that could be exploited.

References

9.2.2 Attack Types

q_attack_types_footprinting_vs_fingerprinting_n09.question.fex

Question 20. ✓ Correct

What mode in SNMP v3 does not encrypt packets?

○ privAuth

○ noAuthNoPriv

○ authPriv

→ ● authNoPriv

Explanation

The correct answer is authNoPriv. In SNMP v3, the authNoPriv mode requires authentication but does not encrypt packets, providing a level of security without encryption.

authPriv mode in SNMP v3 provides both authentication and encryption, ensuring secure communication between agents and monitors, contrary to authNoPriv which lacks encryption.

noAuthNoPriv mode offers neither authentication nor encryption, making it the least secure configuration in SNMP v3, suitable only for environments where security is not a concern.

privAuth is not a valid mode within SNMP v3's security model, which categorizes security levels as noAuthNoPriv, authNoPriv, and authPriv, focusing on the presence of authentication and encryption.

References

8.2.1 Network Discovery

8.3.1 SNMP Agents and Monitors

8.3.2 SNMP Security

8.3.3 Configuring an SNMP System on a Router

8.3.4 Monitoring a Switch with SNMP

8.3.5 Configuring SNMP Trap

q_snmp_authnopriv_n09.question.fex

Question 21. ✓ Correct

What is the purpose of using the -sV or -A switch with Nmap?

○ To disable logging of the scan results

○ To increase the speed of the scan

→ ● To probe for software versions on each port

○ To limit the scan to the local network only

Explanation

The -sV and -A switches are used with Nmap to perform more intensive probes on a host. This can help in discovering the software or software versions operating on each port, a process known as service version detection or fingerprinting.

These switches do not increase the speed of the scan; they make it more detailed and potentially slower.

Disabling logging of scan results is not the purpose of these switches; they are used for detailed scanning.

Limiting the scan to the local network only is not the function of these switches; they are used for detailed service and version detection.

References

7.2.8 Lab: Scan for Web Services with Nmap

8.2.2 Nmap

8.2.3 Nmap Port Scanning

q_port_scanner_sv_a_purpose_n09.question.fex

Question 22. ✓ Correct

You are setting up a secure website for your online store. You want to ensure that all data transmitted between your website and your customers is encrypted.

Which of the following steps is essential for you to achieve this?

○ Install a web analytics tool.

○ Implement a CAPTCHA system on your website.

→ ● Obtain and install a digital certificate.

○ Increase your website's bandwidth.

Explanation

To secure data transmission between your website and your customers, you need to implement HTTPS, which is the secure version of HTTP enabled by TLS. Obtaining and installing a digital certificate from a trusted CA is essential for this process. The digital certificate will authenticate your website's identity to your customers and enable encrypted communication.

While useful for tracking website traffic and user behavior, web analytics tools do not encrypt data transmission.

Increasing bandwidth can improve website performance but does not secure data transmission.

CAPTCHA systems help differentiate human users from bots but do not encrypt or secure data transmission.

References

6.5.10 DNS Security

q_tls_digital_certificate_scenario_n09.question.fex

Question 23. ✓ Correct

What does an availability monitor check for in an HTTP service to confirm availability?

→ ● A 200 status code

○ A 302 status code

○ A 500 status code

○ A 404 status code

Explanation

A 200 status code indicates that an HTTP request has succeeded, which is what an availability monitor looks for to confirm that a service is available.

A 404 status code indicates that the requested resource could not be found, which would suggest unavailability.

A 500 status code indicates an internal server error, also suggesting a problem with availability.

A 302 status code indicates a temporary redirection, not necessarily that the service is available.

References

8.2.5 Performance Monitoring

8.2.6 Availability Monitoring

q_availability_monitoring_200-status_code_n09.question.fex

Question 24.

× Incorrect

What do "top talkers" and "top listeners" refer to in network analysis?

- ● ~~Top talkers are the most secure connections in a network, and top listeners are the least secure connections.~~
- ○ Top talkers are devices with the highest error rates in the network, while top listeners are devices with the highest packet loss rates.
- → ○ Top talkers are interfaces generating the most outgoing traffic, while top listeners are the interfaces receiving the most incoming traffic.
- ○ Top talkers are the fastest network connections, while top listeners are the slowest network connections.

Explanation

In network analysis, "top talkers" and "top listeners" are terms used to identify network interfaces based on their traffic volume. Top talkers are those interfaces that send out the most data, indicating high outgoing traffic. This could be due to applications or devices that are heavily transmitting data across the network. On the other hand, top listeners are interfaces that receive the most data, indicating high incoming traffic. Identifying these interfaces helps network administrators understand traffic flow, pinpoint potential bottlenecks, and optimize network performance.

"Top talkers" and "top listeners" do not refer to error rates or packet loss rates. Instead, these terms specifically relate to the volume of traffic being sent or received by network interfaces. Error rates and packet loss are different metrics used in network analysis to assess the quality of connections and the reliability of data transmission, not the volume of traffic.

The concepts of "top talkers" and "top listeners" have nothing to do with security levels of connections. These terms are used to quantify traffic volume, not to evaluate the security or vulnerability of network connections. Security assessments in a network involve analyzing encryption standards, authentication protocols, and other security measures, not traffic volume.

"Top talkers" and "top listeners" refer to the amount of data being transmitted or received, not the speed of the connections. The speed of a network connection is determined by its bandwidth and latency, among other factors, and is a separate consideration from the volume of traffic that a connection handles. Identifying top talkers and top listeners helps in understanding traffic distribution and potential bottlenecks but does not directly measure the speed of network connections.

References

- **8.6.1 Common Performance Issues**
- **8.6.3 Flow Data**
- **8.6.4 Traffic Testing Tools**
- **8.6.5 Bandwidth Management**

q_traffic_analyze_top_talkers_listeners_n09.question.fex

Question 25. ✓ Correct

Which version of SNMP supports encryption and strong user-based authentication?

○ SNMP v4

→ ● SNMP v3

○ SNMP v1

○ SNMP v2c

Explanation

SNMP v3 is the only version among the options that supports encryption and strong user-based authentication. It introduces security features that were not present in earlier versions, such as SNMP v1 and v2c, which lack robust authentication and encryption capabilities.

The SNMP v1 version does not support encryption or strong user-based authentication. It is the first version of SNMP and has minimal security features.

While it is an improvement over SNMP v1, SNMP v2c still does not support encryption or strong user-based authentication. It sends community strings in plaintext, which is a security risk.

There is no SNMP v4. The development of SNMP versions jumped from SNMP v3 directly to SNMP v5 (which is not widely adopted or standardized).

References

8.2.1 Network Discovery

8.3.1 SNMP Agents and Monitors

8.3.2 SNMP Security

8.3.3 Configuring an SNMP System on a Router

8.3.4 Monitoring a Switch with SNMP

8.3.5 Configuring SNMP Trap

q_snmp_security_snmp_v3_n09.question.fex

Question 26. ✓ Correct

What does a syslog message comprise?

- ○ A severity level and a message part
- → ● A PRI code, a header, and a message part
- ○ Only a message part with content
- ○ Only a header containing a timestamp

Explanation

A syslog message consists of three main components: a PRI code (calculated from the facility and a severity level), a header (containing a timestamp and host name), and a message part (which includes a tag showing the source process plus content). This structure allows for detailed and standardized logging of events.

A header containing a timestamp is only one part of a syslog message, not the entirety of it.

A message part with content is also only one component of a syslog message.

A severity level is part of the PRI code calculation, and while a message part is included, this choice omits the PRI code and header, which are essential components.

References

8.4.2 Log Collectors and Syslog

8.4.3 Event Prioritization and Alerting

8.4.8 Lab: Auditing Device Logs on a Cisco Switch

8.4.9 Lab: Configure Logging on Linux

8.4.10 Lab: View Event Logs

q_syslog_message_contents_n09.question.fex

Question 27. ✓ Correct

What is the purpose of the STARTTLS command in SMTP?

- ○ To create a new email account
- ○ To encrypt the entire email message content
- → ● To upgrade an existing unsecure connection to use TLS
- ○ To downgrade the connection to an unsecure state

Explanation

STARTTLS is used to upgrade an existing unsecure SMTP connection to a secure one using TLS, enhancing the security of email transmission.

STARTTLS upgrades, not downgrades, the connection to a secure state.

While STARTTLS helps secure the connection, encrypting the entire email content is not its sole purpose.

Creating a new email account is not related to the STARTTLS command or SMTP's functionality.

References

6.1.6 Common TCP and UDP Ports

7.3.1 Simple Mail Transfer Protocol

7.3.2 Internet Message Access Protocol

q_smtp_starttls_purpose_n09.question.fex

Question 28. ✓ Correct

What does the Secure Erase (SE) command do on HDDs?

- ○ Encrypts all data on the drive
- → ● Performs a single pass of zero-filling
- ○ Marks all blocks as empty
- ○ Physically destroys the drive

Explanation

On HDDs, the Secure Erase command performs a single pass of zero-filling, effectively overwriting the data on the drive to sanitize it.

Marking all blocks as empty is what happens on SSDs, not HDDs.

Encrypting all data on the drive is not the function of the SE command.

The SE command does not physically destroy the drive.

References

8.1.6 Decommissioning

q_disposal_se_hdds_n09.question.fex

Question 29. ✓ Correct

Which of the following is NOT a traffic class defined by DiffServ?

- ○ Best Effort
- ○ Expedited Forwarding
- → ● Maximum Throughput
- ○ Assured Forwarding

Explanation

The correct answer is maximum throughput. DiffServ traffic classes include Best Effort, Assured Forwarding, and Expedited Forwarding. Maximum Throughput is not a defined traffic class within the DiffServ framework, which focuses on prioritizing packets based on their classification.

Best Effort is a basic DiffServ traffic class where packets are delivered based on available capacity without special priority.

Assured Forwarding is a DiffServ traffic class that provides guaranteed delivery under specified conditions.

Expedited Forwarding is a high-priority DiffServ traffic class designed for time-sensitive data.

References

8.6.1 Common Performance Issues

8.6.2 Interface Statistics

8.6.5 Bandwidth Management

8.6.6 Traffic Shaping

8.6.7 Lab: Configure QoS

12.4.1 Wireless Performance Assessment

12.4.6 Overcapacity Issues

q_band_manage_maximum_throughput_n09.question.fex

Question 30. ✓ Correct

What is a Distributed Reflection DoS (DRDoS) attack?

○ An attack that directly targets the attacker's network

○ A method to reduce network bandwidth consumption

○ An attack that improves server reflection capabilities

→ ● A type of attack where the victim's IP address is spoofed

Explanation

In a DRDoS attack, the attacker spoofs the victim's IP address, causing multiple servers to send responses to the victim, overwhelming their bandwidth.

DRDoS attacks do not improve server capabilities; they exploit them to flood the victim.

These attacks aim to consume bandwidth, not reduce it.

The attack targets the victim's network, not the attacker's.

References

9.2.2 Attack Types

9.2.3 Distributed DoS Attacks and Botnets

9.2.5 Lab: Analyze a DoS Attack

9.2.6 Lab: Analyze a DDoS Attack

12.3.11 Lab: Enable Wireless Intrusion Prevention

q_ddos_drdos_attack_n09.question.fex

Question 31. ✓ Correct

What is the role of regular expression pattern matching in URL filtering?

○ To increase the speed of filtering

○ To encrypt the URL

→ ● To filter by keywords

○ To identify the user's location

Explanation

Regular expression pattern matching is used in URL filtering to filter URLs based on specific keywords or the path and query parameters contained within them. This allows for more granular control over which URLs are blocked or allowed.

Increasing the speed of filtering is not the primary role of regular expression pattern matching; it's about precision in filtering.

Encrypting the URL is not related to regular expression pattern matching; it's a function of security protocols like HTTPS.

Identifying the user's location is not the purpose of regular expression pattern matching in URL filtering.

References

10.5.1 Security Rules and ACL Configuration

10.5.7 Lab: Configure a Security Appliance

10.5.8 Lab: Configure a Perimeter Firewall

10.5.9 Lab: Restrict Telnet and SSH Access

10.5.10 Lab: Permit Traffic

q_content_filter_regular_expression_n09.question.fex

Question 32. ✓ Correct

What is the primary purpose of ARP poisoning in an on-path attack?

○ To encrypt all data packets on the network.

○ To physically damage the network infrastructure.

○ To increase the efficiency of the ARP protocol.

→ ● To redirect traffic through the attacker.

Explanation

The correct answer is to redirect traffic through the attacker, allowing them to intercept or modify it. ARP poisoning manipulates the ARP cache so that traffic intended for a specific host is misdirected to the attacker instead. This enables the attacker to intercept, monitor, or alter the traffic, which is the primary goal of such an attack.

ARP poisoning is a malicious activity aimed at compromising network security, not improving protocol efficiency.

ARP poisoning does not involve encryption; it involves deceiving network devices about the true MAC address associated with an IP address.

ARP poisoning is a software-based attack that affects network traffic flow and data integrity, not the physical infrastructure of the network.

References

9.3.3 Poison ARP

9.3.7 Lab: Poison ARP and Analyze with Wireshark

q_path_attack_arp_poisoning_on-path_n09.question.fex

Question 33. ✓ Correct

Which of the following can be considered a rogue device?

- ○ A firewall configured by the network security team
- → ● A wireless access point installed without IT approval
- ○ An officially sanctioned DHCP server
- ○ A company-issued laptop with up-to-date security software

Explanation

A wireless access point installed without the knowledge or approval of the IT department is not under administrative control, making it a rogue device.

An officially sanctioned DHCP server is approved and controlled by the IT department, making it not rogue.

A firewall configured by the network security team is an example of a device that is under the administrative control of the network staff.

A company-issued laptop with up-to-date security software is sanctioned and monitored by the IT department.

References

9.4.1 Rogue Devices and Services

q_rogue_devices_example_n09.question.fex

Question 34. ✓ Correct

What is MAC spoofing?

○ Physically altering the network interface to change its MAC address

○ Intercepting MAC addresses during data transmission

○ Using malware to reveal the MAC address of a device

→ ● Changing the MAC address of a network interface to any arbitrary value

Explanation

MAC spoofing involves changing the Media Access Control (MAC) address of a device's network interface to a different value. This can be done for various reasons, including impersonating another device on the network.

MAC spoofing is done through software, not by physically altering the network interface.

Revealing a MAC address does not constitute spoofing. Spoofing involves changing or masquerading the MAC address.

Intercepting MAC addresses is different from spoofing, which involves changing the MAC address.

References

9.3.1 On-Path Attacks

q_path_attack_mac_spoofing_role_n09.question.fex

Question 35. ✓ Correct

What is a honeypot in the context of cybersecurity?

→ ● A computer system set up to attract attackers

○ A firewall configuration technique

○ A type of malware designed to steal data

○ A software tool used for encrypting data

Explanation

A honeypot is deliberately designed to appear vulnerable and attractive to attackers. Its purpose is to lure cybercriminals so that their behavior can be studied, which helps in understanding attack strategies and tools. This information can be used to improve security measures and provide early warning of attack attempts.

A honeypot is not malware but a security mechanism designed to trap attackers.

It is not a tool for encrypting data but rather a decoy for monitoring and analyzing attacks.

It is not related to firewall configurations but is a separate entity designed to mimic real systems to attract attackers.

References

9.1.6 Deception Technologies

9.1.7 Lab: Create a Honeypot

q_deception_honeypot_n09.question.fex

Question 36. ✓ Correct

How has the concept of the network edge changed due to the erosion of the perimeter security model?

○ It has been eliminated entirely.

○ It has become more focused on the physical location of the network.

→ ● It has expanded to include access switches and wireless access points.

○ It has become synonymous with the firewall.

Explanation

As the traditional perimeter security model has become less effective, the concept of the network edge, or perimeter, has expanded. It now includes not just the boundary between the private and public networks but also internal components like access switches and wireless access points, which were previously considered "internal."

The change in the network edge concept is not about focusing more on physical location but expanding what is considered the edge.

While firewalls are part of the network edge, the concept has expanded beyond just the firewall to include other components.

The concept of the network edge has not been eliminated but rather expanded to adapt to new security challenges.

References

- **1.3.3 Data Link Layer Functions**
- **3.2.1 Hubs**
- **3.2.3 Switches**
- **3.2.4 Ethernet Switch Types**
- **3.2.5 Switch Interface Configuration**
- **3.2.7 Lab: Install a Switch in the Rack**
- **3.2.8 Lab: Secure a Switch**

q_defense_depth_network_edge_change_n09.question.fex

Question 37. ✓ Correct

What is the role of a packet sniffer in the context of a protocol analyzer?

○ To physically connect different network segments

○ To provide encryption for data packets

○ To increase the bandwidth of the network

→ ● To capture frames moving over the network medium

Explanation

A packet sniffer captures frames moving over the network, providing the raw data that a protocol analyzer needs to inspect and analyze network traffic. It is a foundational tool for network diagnostics and monitoring.

Increasing bandwidth is a function of network design and infrastructure, not something a packet sniffer does.

Physical network connections are made through hardware like switches and routers, not through software tools like packet sniffers.

Encryption is a security function, not the role of a packet sniffer, which is focused on capturing and analyzing network traffic.

References

8.6.1 Common Performance Issues

8.6.3 Flow Data

8.6.4 Traffic Testing Tools

8.6.5 Bandwidth Management

q_sniffers_role_n09.question.fex

Question 38. ✓ Correct

What is a transparent proxy also known as?

○ Private proxy

○ Secure proxy

○ Direct proxy

→ ● Forced proxy

Explanation

A transparent proxy is also known as a forced or intercepting proxy. It intercepts client traffic without requiring the client to be reconfigured to use the proxy.

Direct proxy is not a term commonly used to describe a transparent proxy.

Secure proxy refers to proxies that provide additional security features, not necessarily transparency.

Private proxy refers to a proxy service dedicated to a single user or group, not to its transparency.

References

10.5.2 Proxy Servers

q_proxy_forced_proxy_n09.question.fex

Question 39. ✓ Correct

What might a firewall be incorrectly doing if an application fails to function correctly?

○ Allowing all TCP and UDP ports

○ Increasing bandwidth for all applications

→ ● Blocking TCP or UDP ports that should be open

○ Decrypting all incoming traffic

Explanation

If an application is not functioning correctly, it could be due to the firewall blocking TCP or UDP ports that are necessary for the application's communication. This prevents the application from sending or receiving data as intended.

Allowing all TCP and UDP ports would not cause an application to fail; it would potentially create a security risk by not filtering any traffic.

Increasing bandwidth for all applications would generally improve or maintain application performance, not hinder it.

Decrypting all incoming traffic is a function of security appliances for inspection purposes and does not directly cause application failures.

References

1.3.5 Transport and Application Layer and Security Functions

5.4.1 Firewall Uses and Types

5.4.2 Firewall Selection and Placement

10.5.1 Security Rules and ACL Configuration

10.5.4 Misconfigured Firewall and ACL Issues

10.5.5 Creating Firewall ACLs

10.5.7 Lab: Configure a Security Appliance

10.5.8 Lab: Configure a Perimeter Firewall

14.3.5 Cloud Firewall Security

q_misconfig_acl_blocking_ports_n09.question.fex

Question 40. ✓ Correct

What role does a grandmaster clock play in a PTP domain?

○ It serves as the primary network router.

○ It acts as the primary backup time source.

○ It synchronizes directly with satellite clocks.

→ ● It is the authoritative time source.

Explanation

In a PTP domain, the grandmaster clock is the authoritative time source to which other clocks in the domain synchronize, ensuring high precision across the network.

The grandmaster clock is not a backup; it is the primary time source.

There is no mention of direct synchronization with satellite clocks for the grandmaster clock.

The grandmaster clock's role is related to time synchronization, not routing network traffic.

References

7.1.1 Transport Layer Security

7.1.3 Precision Time Protocol

q_ntp_issues_grandmaster_clock_n09.question.fex

Question 41. ✓ Correct

Which Nmap scan type is less stealthy due to its use of the operating system to attempt a full TCP connection?

○ UDP scans (-sU)

→ ● TCP connect (-sT)

○ TCP SYN (-sS)

○ Port range (-p)

Explanation

The TCP connect scan (-sT) uses the operating system to attempt a full TCP connection, making it less stealthy because it completes the TCP handshake, which is more likely to be logged by the target system.

TCP SYN (-sS) is more stealthy because it does not complete the TCP handshake.

UDP scans (-sU) involve UDP ports and do not attempt a full TCP connection.

Specifying a port range (-p) is an option that can be used with various scan types and does not pertain to the method of scanning.

References

7.2.8 Lab: Scan for Web Services with Nmap

8.2.2 Nmap

8.2.3 Nmap Port Scanning

q_port_scanner_st_purpose_n09.question.fex

Question 42. ✓ Correct

What distinguishes a Passive TAP from a SPAN/port mirroring connection?

○ It requires special software to function.

○ It can only monitor encrypted traffic.

→ ● It physically copies the signal from the cabling to a monitor port.

○ It can increase network speed.

Explanation

A Passive TAP is a hardware device that makes a physical copy of the data passing through a network cable to a monitoring port without affecting the original data flow. This ensures that all data, including potentially corrupt or malformed frames, is captured for analysis.

Passive TAPs monitor all traffic, not just encrypted traffic. Encryption does not affect a TAP's ability to copy data.

Passive TAPs are hardware devices and do not require software to operate. They work independently of software, making a direct copy of the traffic at the hardware level.

Passive TAPs do not affect network speed. They are designed to be transparent to the network, merely copying data for monitoring purposes without influencing network performance.

References

8.5.1 Packet Capture

q_sniffers_passive_tap_vs_mirroring_n09.question.fex

Question 43. ✓ Correct

What is referred to as configuration drift?

○ The initial setup of a CI's configuration

○ The process of updating a CI's baseline

○ The act of backing up a CI's configuration

→ ● The deviation of a CI from its baseline

Explanation

Configuration drift refers to the situation where the current state of a Configuration Item (CI) deviates, either temporarily or persistently, from its documented baseline configuration. This can occur due to changes not being properly documented or authorized.

Updating a CI's baseline is a controlled process, not drift.

Backing up a CI's configuration is a separate process from drift, which is about deviations from the baseline.

The initial setup of a CI's configuration establishes the baseline, not drift.

References

8.1.1 Configuration Management

q_operating_configuration_drift_n09.question.fex

Question 44. ✓ Correct

Which factor determines the type of credential a subject can use for authentication?

→ ● Authentication factor

○ Identification process

○ Accounting system

○ Authorization model

Explanation

The correct answer is authentication factor. Authentication factors are criteria used to verify an entity's identity. These can include something the entity knows (password), something the entity has (token), or something the entity is (biometric).

The authorization model determines access rights and permissions, not the type of credentials used for authentication.

The accounting system tracks and records access and actions within the system, unrelated to the determination of authentication credentials.

While identification is the process of recognizing an entity, it does not determine the type of credentials used for authentication.

References

10.1.1 Access Control

10.1.2 Authentication Methods

10.1.3 Local Authentication

10.1.4 Single Sign-On and Kerberos

10.1.8 Remote Authentication

10.3.4 Scanning for Unsecure Protocols

13.2.1 Remote Access Considerations

q_access_control_authenticaton_factor_n09.question.fex

Question 45. ✓ Correct

Which of the following is a vulnerability that still exists even with restricted access to physical switch ports and hardware?

- → ● Rogue administrators
- ○ Incompatibility with older network protocols
- ○ Overheating of network equipment
- ○ Increased network latency

Explanation

The correct answer is rogue administrators or theft of equipment room keys. Physical security measures can be bypassed by internal threats such as rogue administrators or by external threats through the theft of keys, highlighting the need for comprehensive security strategies.

Restricted access to physical components is a security measure that does not directly affect network latency.

Overheating is related to environmental and hardware issues, not security vulnerabilities associated with physical access control.

Incompatibility with older network protocols refers to technical compatibility issues, not security vulnerabilities stemming from physical access control.

References

10.4.1 Network Access Control and Port Security

10.4.2 Lab: Secure Access to a Switch

10.4.3 Lab: Secure Access to a Switch 2

10.4.4 Lab: Disable Switch Ports - GUI

10.4.6 Port Guards

10.4.7 Lab: Harden a Switch

10.4.8 Port Mirroring

q_port_security_vulnerability_n09.question.fex

Question 46. ✓ Correct

What distinguishes an external threat actor from an internal threat actor?

- ○ The type of malware they use
- ○ The geographical location of the actor
- → ● Whether they have authorized access to the system
- ○ The sophistication of the attack

Explanation

The key difference between external and internal threat actors is whether they have authorized access to the target system. External threat actors do not have such access and must find ways to infiltrate the system, often using malware or social engineering. In contrast, internal threat actors already have some level of authorized access due to their role within or relationship to the organization.

The type of malware used can vary among all threat actors and does not define whether they are internal or external.

The geographical location of the actor is irrelevant to their classification as internal or external.

The sophistication of the attack can vary widely among both internal and external actors and is not a distinguishing factor.

References

9.1.1 Common Security Terminology

9.1.5 Vulnerability and Exploit Types

9.2.1 Threat Types and Assessment

9.3.5 Using SMAC to Spoof MAC Addresses

9.3.8 Lab: Spoof MAC Addresses with SMAC

q_threat_types_external_vs_internal_n09.question.fex

Question 47. ✓ Correct

What is a forward proxy primarily used for?

→ ● Outbound traffic management

○ Data encryption only

○ Inbound traffic management

○ Data storage

Explanation

A forward proxy is used for managing outbound traffic from a private network to the Internet. It can control and monitor the traffic that exits the internal network, providing security and caching services.

Inbound traffic management is the role of a reverse proxy, not a forward proxy.

While a proxy can handle encryption/decryption, it's not its primary use.

Data storage is not a primary function of a forward proxy, although caching does temporarily store data.

References

10.5.2 Proxy Servers

q_proxy_forward_proxy_n09.question.fex

Question 48. ✓ Correct

What distinguishes a Layer 7 switch from a Layer 4 switch in load balancing?

→ ● Layer 7 switch makes forwarding decisions based on application-level data.

○ Layer 7 switch is used exclusively for encrypting data traffic.

○ Layer 7 switch increases the storage capacity of servers.

○ Layer 7 switch operates at the network layer.

Explanation

A Layer 7 switch, also known as a content switch, operates at the application layer and can make forwarding decisions based on the content of the traffic, such as URL requests or data types, allowing for more sophisticated load balancing.

Layer 7 switch operates at the network layer is incorrect as Layer 7 operates at the application layer.

Encryption is not the primary function of a Layer 7 switch.

Layer 7 switch increases the storage capacity of servers is unrelated to the function of a Layer 7 switch in load balancing.

References

7.4.5 Load Balancers

7.4.8 Lab: Configure NIC Teaming

q_balance_layer_4_vs_layer_7_switch_n09.question.fex

Question 49. ✓ Correct

What is the result of a successful ARP poisoning attack?

→ ● The attacker receives all traffic destined for remote networks.

○ All network traffic is encrypted automatically.

○ The attacker's device is disconnected from the network.

○ The network's speed is significantly increased.

Explanation

The correct answer is that the attacker receives all traffic destined for remote networks. By successfully poisoning the ARP cache, the attacker can redirect traffic intended for another host (such as the network's gateway) to themselves, allowing them to intercept, inspect, and potentially modify the traffic.

The goal of ARP poisoning is to intercept traffic, not to disconnect the attacker's device from the network.

ARP poisoning does not result in the automatic encryption of network traffic; it compromises the integrity and confidentiality of the network.

ARP poisoning does not affect the speed of the network in a positive way; it can actually cause network disruptions and slow down traffic due to misrouted packets.

References

9.3.3 Poison ARP

9.3.7 Lab: Poison ARP and Analyze with Wireshark

q_path_attack_arp_poisoning_results_n09.question.fex

Question 50. ✓ Correct

What is the primary function of Cisco Discovery Protocol (CDP)?

○ To assign IP addresses to devices on a network

○ To provide a secure tunnel for data transmission

○ To encrypt data traffic between Cisco devices

→ ● To discover information about directly connected Cisco devices

Explanation

The primary function of CDP is to discover information about directly connected Cisco devices. It allows devices to learn about each other, facilitating easier network management and troubleshooting.

Encrypting data traffic is not the function of CDP; it is typically handled by security protocols such as IPsec.

Assigning IP addresses to devices on a network is generally the role of DHCP, not CDP.

Providing a secure tunnel for data transmission is the function of VPN protocols, not CDP.

References

8.2.4 Discovery Protocols

q_discovery_protocols_cdp_primary_role_n09.question.fex

Question 51. ✓ Correct

What does role-based access control aim to achieve?

- ○ Allow all users equal access.
- ○ Reduce the complexity of permissions.
- → ● Limit permissions based on administrative roles.
- ○ Increase the number of administrators.

Explanation

Role-based access control is designed to limit the permissions to what is necessary for users' roles, thereby reducing the risk associated with compromised accounts and enhancing security through the principle of least privilege.

The goal is not to increase administrators but to manage permissions effectively.

Reducing complexity is beneficial but not the primary aim of role-based access.

Equal access for all users would negate the purpose of role-based access control.

References

10.2.1 Authorization and Role-Based Access Control

10.2.5 Lab: Manage Account Policies

q_hardening_role-based_access_n09.question.fex

Question 52. ✓ Correct

Which password cracking method involves trying every possible combination to find the matching password?

○ Phishing

○ Social Engineering

○ Dictionary

→ ● Brute Force

Explanation

The correct answer is brute force. Brute force attacks involve systematically checking all possible combinations until the correct one is found. This method does not rely on any insight into the likely composition of the password and is purely based on trial and error. It is computationally intensive and the time to success can vary greatly depending on the complexity and length of the password.

Dictionary attacks use a list of pre-defined words or phrases (like those found in a dictionary) to guess passwords. This method relies on the assumption that many users choose common words or simple variations of them as passwords. It is faster than brute force when passwords are simple or common, but less effective against complex passwords.

Social engineering involves manipulating individuals into divulging confidential information, such as passwords. This method relies on psychological manipulation rather than technical means to breach security. It targets human vulnerabilities rather than exploiting software or hardware vulnerabilities.

Phishing is a technique used to deceive individuals into providing sensitive information, including passwords, by masquerading as a trustworthy entity in electronic communications. Unlike brute force attacks, phishing does not involve trying combinations of passwords but rather tricks the user into revealing them directly.

References

9.2.2 Attack Types

9.2.4 Malware Attacks

q_password_attacks_brute_force_n09.question.fex

Question 53. ✓ Correct

What is the preferred system for Windows network authentication?

○ SAML

○ OAuth

○ NT LAN Manager (NTLM)

→ ● Kerberos

Explanation

Kerberos is the preferred system for network authentication in Windows environments due to its ability to securely manage user credentials and its support for mutual authentication between the user and the service.

NT LAN Manager (NTLM) is a legacy authentication protocol used by Windows but is not the preferred system due to its lesser security compared to Kerberos.

OAuth is an open standard for access delegation, commonly used as a way for internet users to grant websites or applications access to their information on other websites but without giving them the passwords. It's not specifically used for Windows network authentication.

SAML (Security Assertion Markup Language) is used for exchanging authentication and authorization data between parties, particularly between an identity provider and a service provider, not specifically for Windows network authentication.

References

10.1.1 Access Control

10.1.2 Authentication Methods

10.1.3 Local Authentication

10.1.4 Single Sign-On and Kerberos

10.1.8 Remote Authentication

10.3.4 Scanning for Unsecure Protocols

13.2.1 Remote Access Considerations

q_authentication_kerberos_n09.question.fex

Question 54. ✓ Correct

What is considered an acceptable error rate in general terms?

○ Exactly 5 percent

○ Under 10 percent

→ ● Under 1 percent

○ Over 15 percent

Explanation

A general guideline is that error rates should be under 1 percent. Higher rates may indicate issues that need addressing.

5 percent is significantly higher than the acceptable threshold.

10 percent is far above the acceptable error rate, indicating serious issues.

15 percent would suggest critical problems with the network.

References

8.6.1 Common Performance Issues

8.6.2 Interface Statistics

q_int_stats_error_rate_acceptable_n09.question.fex

Question 55. ✓ Correct

What is established between a server and a client after successful authentication with TLS?

- ○ A public network
- → ● An encrypted tunnel
- ○ A direct physical connection
- ○ A data compression protocol

Explanation

After successful authentication with TLS, an encrypted tunnel is established between the server and the client. This tunnel ensures that all data transmitted between the two parties is encrypted, providing confidentiality and integrity. The encryption prevents unauthorized parties from eavesdropping or tampering with the data.

TLS operates over existing network connections and does not establish new physical connections. It secures data transmitted over these connections through encryption.

While TLS can secure data transmitted over public networks, it does not establish the network itself. Its role is to provide security for data in transit, regardless of the network type.

TLS is focused on securing communications through encryption, not on compressing data. While some protocols may include options for compression, the primary function of TLS is to authenticate the server and client and to encrypt their communications.

References

6.5.10 DNS Security

q_tls_encrypted_tunnel_n09.question.fex

Question 56. × Incorrect

What role does a NetFlow exporter play in a network?

○ It increases the bandwidth of the network.

○ It aggregates flows from multiple collectors.

● ~~It analyzes and reports flow information.~~

→ ○ It defines cache flows.

Explanation

A NetFlow exporter is a component configured on network devices like routers and switches. It is responsible for defining traffic flows based on specific characteristics and caching this data for transmission to a NetFlow collector.

Aggregating flows from multiple collectors is the role of a NetFlow collector, not an exporter.

Analysis and reporting are functions of a NetFlow analyzer, not an exporter.

A NetFlow exporter's role is to define and cache traffic flows, not to increase network bandwidth.

References

8.6.1 Common Performance Issues

8.6.3 Flow Data

8.6.4 Traffic Testing Tools

8.6.5 Bandwidth Management

q_netflow_exporter_role_n09.question.fex

Question 57. ✓ Correct

How does RBAC differ from using security groups for assigning permissions?

→ ● RBAC focuses on job roles, while security groups are about user identity.

○ Security groups encrypt data, while RBAC does not.

○ RBAC is discretionary, while security groups are nondiscretionary.

○ RBAC assigns permissions directly to users, while security groups do not.

Explanation

RBAC is centered around the concept of roles, which are defined by the tasks or job functions an employee performs, and permissions are assigned to these roles. Security groups, on the other hand, are used to group user accounts for administrative purposes and can be used to assign permissions, but they do not inherently focus on job functions or roles.

Both RBAC and security groups do not assign permissions directly to individual users; they both use a form of grouping (roles or security groups) to manage permissions.

RBAC is nondiscretionary, and while security groups can be used in a discretionary manner, the key difference lies in their focus and purpose, not their discretionary nature.

Neither RBAC nor security groups directly deal with data encryption; they are mechanisms for managing access and permissions.

References

10.2.1 Authorization and Role-Based Access Control

10.2.5 Lab: Manage Account Policies

q_rbac_vs_security_groups_n09.question.fex

Question 58. ✓ Correct

What is the function of a content filtering firewall or proxy?

○ To provide a VPN service

→ ● To restrict access

○ To serve as a backup data center

○ To increase bandwidth

Explanation

The primary function of a content filtering firewall or proxy is to restrict access to the Internet based on various criteria, such as URLs, content categories, and time-of-day restrictions, to protect the organization's network and enforce policies.

Increasing bandwidth is not the function of a content filtering firewall or proxy.

Serving as a backup data center is not related to the role of content filtering firewalls or proxies.

Providing a VPN service is not the purpose of content filtering firewalls or proxies, which focus on restricting access to content.

References

10.5.1 Security Rules and ACL Configuration

10.5.3 Content Filtering

10.5.7 Lab: Configure a Security Appliance

10.5.8 Lab: Configure a Perimeter Firewall

10.5.10 Lab: Permit Traffic

q_content_filter_content_filtering_firewall_n09.question.fex

Question 59. ✓ Correct

What is the primary purpose of content filtering in an organization's network?

- ○ To increase network speed
- ○ To monitor employee productivity
- → ● To block access to malicious websites
- ○ To encrypt network traffic

Explanation

Content filtering plays a crucial role in protecting an organization's network by preventing users from accessing websites that could be harmful or not suitable for the workplace. This is essential for maintaining network security and compliance with company policies.

Increasing network speed is not the primary purpose of content filtering, although it might be a secondary benefit if bandwidth-consuming sites are blocked.

Monitoring employee productivity might be a result of content filtering but is not its primary purpose.

Encrypting network traffic is the function of encryption protocols like TLS, not content filtering.

References

- **10.5.1 Security Rules and ACL Configuration**
- **10.5.3 Content Filtering**
- **10.5.7 Lab: Configure a Security Appliance**
- **10.5.8 Lab: Configure a Perimeter Firewall**
- **10.5.10 Lab: Permit Traffic**

q_content_filter_primary_purpose_n09.question.fex

Question 60. ✓ Correct

What framework does Windows use to provide Single Sign-On (SSO) authentication?

→ ● Kerberos

○ SAML

○ LDAP

○ OAuth

Explanation

Windows uses the Kerberos framework to provide Single Sign-On (SSO) authentication. Kerberos allows users to authenticate once to a local device and then access compatible application servers without needing to re-enter credentials. It is particularly used for authenticating users within Active Directory environments.

OAuth is an open standard for access delegation, not specifically used for SSO in Windows.

LDAP is a protocol for accessing and maintaining distributed directory information services, not for SSO.

SAML (Security Assertion Markup Language) is used for SSO but is not the framework used by Windows for this purpose.

References

10.1.3 Local Authentication

10.1.4 Single Sign-On and Kerberos

10.3.4 Scanning for Unsecure Protocols

q_kerberos_sso_authentication_n09.question.fex

Question 61. × Incorrect

What does the term "stateless protocol" imply about HTTP?

○ The server stores data in a centralized database for all requests.

○ The server requires authentication for every request.

○ The server retains information about client requests indefinitely.

→ ○ Each request from a client to a server is treated as a new request.

Explanation

The correct answer is that each request from a client to a server is treated as a new request. Being a stateless protocol means that HTTP does not retain any memory of past requests. Each request is treated independently, without any knowledge of previous interactions.

The server does not retain information about client requests indefinitely; this would imply stateful behavior.

Storing data in a centralized database for all requests is a design choice for managing state and is not inherent to the stateless protocol itself.

References

6.1.6 Common TCP and UDP Ports

7.2.1 Hyper Text Transfer Protocol

q_http_stateless_protocol_n09.question.fex

Question 62. ✓ Correct

What is a DHCP starvation attack?

→ ● An attack that exhausts a DHCP server's address pool

○ An attack that physically damages the DHCP server

○ An attack that floods the network with excessive data

○ An attack that encrypts all DHCP traffic

Explanation

A DHCP starvation attack involves sending numerous fake DHCP requests to use up all available IP addresses that a DHCP server can assign. This prevents legitimate clients from obtaining IP addresses, potentially forcing them to connect to a rogue DHCP server.

Flooding the network with excessive data describes a different type of attack, not specifically related to DHCP.

Encrypting DHCP traffic is not an attack but could be part of securing communication; attacks aim to disrupt or subvert.

Physically damaging the DHCP server is a form of sabotage, not a DHCP starvation attack which is conducted through network traffic.

References

9.4.2 Rogue DHCP

9.4.3 Setting Up DHCP Snooping

9.4.6 Lab: Discover a Rogue DHCP Server

9.4.7 Lab: Configure DHCP Snooping

12.3.11 Lab: Enable Wireless Intrusion Prevention

q_rogue_dhcp_starvation_attack_n09.question.fex

Question 63. ✓ Correct

What is LDAP primarily used for?

- ○ Managing network devices and configurations
- → ● Querying and updating directory services
- ○ Transferring files between computers
- ○ Encrypting data transmissions over the Internet

Explanation

LDAP is specifically designed for querying and updating directory services, allowing for the management of user identities, groups, and access permissions in a networked environment.

LDAP is not primarily used for encrypting data transmissions; protocols like SSL/TLS are used for encryption.

Managing network devices and configurations is typically handled by protocols like SNMP, not LDAP.

Transferring files between computers is the function of protocols like FTP, not LDAP.

References

6.1.6 Common TCP and UDP Ports

10.2.3 Lightweight Directory Access Protocol

10.2.5 Lab: Manage Account Policies

q_ldap_primary_use_n09.question.fex

Question 64. ✓ Correct

Under what condition can an organization process credit card transactions directly?

→ ● If they adopt the PCI DSS standard

○ If they encrypt all their emails

○ If they use cloud storage

○ If they have an internet presence

Explanation

Organizations that directly process credit card transactions must comply with the PCI DSS standard to ensure the security of the cardholder data environment. Adoption of these standards is mandatory for processing transactions.

Using cloud storage does not directly relate to the ability to process credit card transactions.

Having an internet presence is common for businesses but does not qualify them to process credit card transactions without PCI DSS compliance.

Encrypting emails is a good security practice but does not fulfill the requirements for directly processing credit card transactions.

References

9.1.3 Regulatory Compliance

q_reg_comp_direct_transactions_n09.question.fex

Question 65. ✓ Correct

Why are passwords stored as cryptographic hashes?

→ ● To prevent a password from being easily compromised

○ To ensure passwords can be easily recovered if forgotten

○ To allow users to choose simpler passwords

○ To increase the speed of the authentication process

Explanation

The correct answer is to prevent the original password from being easily compromised. Storing passwords as cryptographic hashes increases security by ensuring that even if the data storage is compromised, the original passwords are not easily retrievable. This is because a well-designed hash function makes it infeasible to reverse the hash back to the original plaintext password.

Storing passwords as hashes does not necessarily increase the speed of authentication.

Hashes are designed to be irreversible to increase security, not to allow easy recovery of forgotten passwords.

The purpose of hashing is not to allow simpler passwords but to secure whatever password is chosen.

References

10.1.1 Access Control

10.1.2 Authentication Methods

10.1.3 Local Authentication

10.1.4 Single Sign-On and Kerberos

10.1.8 Remote Authentication

10.3.4 Scanning for Unsecure Protocols

13.2.1 Remote Access Considerations

q_authentication_passwords_hashes_n09.question.fex

Question 66. ✓ Correct

What poses a greater threat than zero-day vulnerabilities?

- ○ Newly released software
- ○ Strong password policies
- → ● Unpatched or legacy systems
- ○ Encrypted data storage

Explanation

Unpatched or legacy systems represent a significant security risk because they contain known vulnerabilities that have not been remediated. These systems are more common and can be exploited by a wider range of attackers compared to the relatively rare and sophisticated zero-day exploits.

While newly released software can contain vulnerabilities, it does not inherently pose a greater threat than zero-day vulnerabilities. Developers often patch known issues quickly after release.

Strong password policies are a security measure designed to protect against unauthorized access, not a threat.

Encrypted data storage is a security best practice that protects data confidentiality, making it an asset rather than a threat to security.

References

9.1.1 Common Security Terminology

9.1.5 Vulnerability and Exploit Types

q_vuln_types_unpatched_legacy_threats_n09.question.fex

Question 67. ✓ Correct

What does "protect mode" do when a switch port enters a violation state?

→ ● It drops frames from the invalid source address but keeps the interface open.

○ It encrypts traffic from the invalid source address.

○ It reroutes traffic from the invalid source address to a quarantine VLAN.

○ It disables the port and sends alerts.

Explanation

The correct answer is that it drops frames from the invalid source address but keeps the interface open. Protect mode allows the port to continue operating for authorized traffic while blocking frames from unauthorized sources, providing a balance between security and network functionality.

It disables the port and sends alerts is incorrect because this describes the shutdown mode, not protect mode.

It encrypts traffic from the invalid source address is incorrect because protect mode involves dropping unauthorized frames, not encrypting them.

It reroutes traffic from the invalid source address to a quarantine VLAN is incorrect because protect mode specifically drops frames rather than rerouting traffic.

References

10.4.1 Network Access Control and Port Security

10.4.2 Lab: Secure Access to a Switch

10.4.3 Lab: Secure Access to a Switch 2

10.4.4 Lab: Disable Switch Ports - GUI

10.4.6 Port Guards

10.4.7 Lab: Harden a Switch

10.4.8 Port Mirroring

q_port_security_protect_mode_n09.question.fex

Question 68. ✓ Correct

What does Recovery Time Objective (RTO) measure in disaster recovery planning?

○ The maximum amount of data loss that is acceptable

○ The time it takes to detect a system failure

○ The amount of time needed to perform system maintenance

→ ● The time following a disaster within which a system must be restored

Explanation

RTO is the maximum amount of time allowed for restoring a system after a disaster has occurred, ensuring that operations can resume within this timeframe.

The maximum amount of data loss that is acceptable describes the Recovery Point Objective (RPO), not RTO.

RTO is about recovery time, not detection time.

RTO deals with disaster recovery, not regular maintenance.

References

7.4.2 Disaster Recovery Metrics

q_redundancy_rto_measurement_n09.question.fex

Question 69. ✓ Correct

What does an IP scanner do?

○ Creates spreadsheets

→ ● Establishes the logical topology of the network

○ Encrypts network traffic

○ Edits images

Explanation

An IP scanner is used for host discovery, helping to map out the network's logical structure in terms of subnets and routers, aiding in network management and security.

Editing images is a function of software like Adobe Photoshop, not an IP scanner.

Creating spreadsheets is a function of applications like Microsoft Excel.

Encrypting network traffic is related to security protocols, not the function of an IP scanner.

References

8.2.1 Network Discovery

q_ip_scanner_logical_topology_n09.question.fex

Question 70. ✓ Correct

Why is it important to track software license usage in an asset inventory?

→ ● To ensure compliance with the vendor's licensing agreement

○ To track the company's profit margins

○ To evaluate the company's branding strategies

○ To monitor employee internet usage

Explanation

The correct answer is to ensure compliance with the vendor's licensing agreement. Tracking software license usage is important to ensure that all installations comply with the vendor's licensing agreement. This helps avoid legal and financial penalties for unauthorized use of software.

Monitoring employee internet usage is unrelated to software license compliance.

Tracking the company's profit margins is a financial operation, not directly related to software licensing.

Evaluating the company's branding strategies is not related to the technical and legal aspects of software license management.

References

8.1.4 Asset Inventory Documentation

q_license_track_license_usage_n09.question.fex

Question 71. ✓ Correct

What does an availability of "five-nines" (99.999%) signify in disaster recovery?

→ ● The system is available for 99.999% of the time.

○ The system requires maintenance 99.999% of the time.

○ The system can recover from any disaster in 99.999% of cases.

○ The system is unavailable for 99.999% of the time.

Explanation

An availability of "five-nines" means the system is designed to be operational and accessible 99.999% of the time, indicating extremely high reliability and minimal downtime.

Five-nines indicates high availability, not unavailability.

The system requires maintenance 99.999% of the time is incorrect because this level of availability refers to operational time, not maintenance requirements.

The system can recover from any disaster in 99.999% of cases is incorrect because it refers to system availability, not the probability of recovery from disasters.

References

7.4.2 Disaster Recovery Metrics

q_redundancy_five_nines_n09.question.fex

Question 72. ✓ Correct

What is the primary purpose of using Quality of Service (QoS) mechanisms in a network?

○ To reduce the cost of network infrastructure

○ To decrease network security

→ ● To prioritize certain types of traffic over others

○ To increase the number of devices that can connect to the network

Explanation

The primary purpose of QoS mechanisms is to manage bandwidth and prioritize certain types of traffic, such as VoIP or streaming video, over less critical applications. This ensures that important applications receive the necessary bandwidth and performance levels, even during times of high network congestion.

QoS mechanisms are designed to manage traffic and bandwidth, not to decrease network security.

Increasing the number of devices that can connect to the network is more related to network capacity and infrastructure than to QoS.

While effective use of QoS can optimize the use of existing network infrastructure, its primary purpose is not to reduce costs but to prioritize traffic.

References

8.6.1 Common Performance Issues

8.6.6 Traffic Shaping

q_band_manage_qos_purpose_n09.question.fex

Question 73. ✓ Correct

What does SMTP use to discover the IP address of the recipient's SMTP server?

→ ● The domain name part of the recipient's email address

○ The sender's IP address

○ The recipient's email password

○ The recipient's physical address

Explanation

The SMTP server uses the domain name part of the recipient's email address to discover the IP address of the recipient SMTP server through DNS.

The recipient's email password is not used in the process of discovering the recipient's SMTP server IP address.

The sender's IP address is irrelevant to discovering the recipient's SMTP server IP address.

The recipient's physical address has no role in the electronic process of SMTP.

References

6.1.6 Common TCP and UDP Ports

7.3.1 Simple Mail Transfer Protocol

7.3.2 Internet Message Access Protocol

q_smtp_domain_name_discover_n09.question.fex

Question 74. ✓ Correct

What is the purpose of installing a special driver for a software-based sniffer?

- ○ To encrypt the captured frames
- ○ To decrease the network's latency
- → ● To allow the frames to be read from the network stack
- ○ To increase the sniffer's processing speed

Explanation

A special driver is required for a software-based sniffer to intercept and read the frames directly from the network adapter's stack. This allows the sniffer to capture the traffic for analysis, including saving it to a file for later review.

Installing a special driver for a sniffer does not affect network latency. Its purpose is to capture traffic, not to optimize network performance.

The driver's role is to enable traffic capture, not to encrypt data. Encryption is a separate process handled by other tools or protocols.

While the driver enables the sniffer to access network frames, it does not directly increase the processing speed of the sniffer software. The efficiency of the sniffer depends on its design and the capabilities of the host system.

References

8.6.1 Common Performance Issues

8.6.3 Flow Data

8.6.4 Traffic Testing Tools

8.6.5 Bandwidth Management

q_sniffers_special_drive_n09.question.fex

Question 75. ✓ Correct

What should be done to secure SNMP traffic?

→ ● Configure SNMPv3 or use IPSec for encryption.

○ Limit SNMP traffic to internal networks.

○ Disable SNMP entirely.

○ Use the original versions of SNMP.

Explanation

To secure SNMP traffic, it's recommended to use SNMPv3, which supports encryption, or encapsulate SNMP traffic with a protocol like IPSec, ensuring the confidentiality and integrity of the data.

Disabling SNMP may not be practical for network management needs.

The original versions of SNMP are unencrypted and thus insecure.

Limiting traffic to internal networks does not protect against internal threats or data interception.

References

6.1.6 Common TCP and UDP Ports

8.3.1 SNMP Agents and Monitors

8.3.2 SNMP Security

8.3.3 Configuring an SNMP System on a Router

q_hardening_secure_snmp_traffic_n09.question.fex

Question 76. ✓ Correct

In which scenario is the Extensible Authentication Protocol (EAP) typically used?

→ ● When a user is accessing a wireless network

○ When a user is downloading a file from the Internet

○ When browsing social media platforms

○ When sending an email

Explanation

EAP is commonly used when a user is accessing a wireless network to authenticate the user or device with the network directory server. This ensures that only authorized users and devices can access the network, providing a secure connection and protecting the network from unauthorized access.

Downloading a file from the Internet does not typically require EAP for authentication. The process of downloading files is generally managed by the application layer protocols like HTTP or FTP, and authentication, if required, is handled at the application level rather than the network access level.

Browsing social media platforms does not involve EAP for authentication at the network access level. While accessing social media platforms may require user authentication, this is done through the platform's login mechanisms and not through network access control methods like EAP.

Sending an email does not directly involve EAP for authentication at the network access level. Email clients may require user authentication to access the email server, but this authentication is separate from the network access control provided by EAP. EAP is focused on authenticating devices and users before they join a network, not on the authentication processes within specific applications like email clients.

References

10.4.5 Extensible Authentication Protocol and IEEE 802.1X

10.4.6 Port Guards

10.4.7 Lab: Harden a Switch

q_eap_use_n09.question.fex

Question 77. ✓ Correct

Which of the following examples BEST describes shoulder surfing?

→ ● Someone nearby watching you enter your password on your computer and recording it

○ Finding someone's password in the trash can and using it to access their account

○ Guessing someone's password because it is so common or simple

○ Giving someone you trust your username and account password

Explanation

Shoulder surfing is watching and recording a password, pin, or access code that is being entered by someone nearby.

Password guessing happens when someone is able to easily guess a password, typically because it is very common, like their pet's name or their hobby.

Dumpster diving relies on finding sensitive information that has been discarded in garbage cans, dumpsters, or other unsecure places.

Social engineering attacks rely on human error. They work by convincing someone to give the attacker access because he or she tricks them into trusting him or her.

References

9.5.1 Social Engineering Attacks

q_social_engineering_shoulder_example_02_n09.question.fex

Question 78. ✓ Correct

How are botnets typically created?

→ ● Through malware that opens a backdoor

○ Through the use of strong passwords

○ By installing security software on devices

○ By updating devices with the latest firmware

Explanation

Botnets are typically created by infecting devices with malware that opens a backdoor, allowing attackers remote control to coordinate attacks or spread further malware.

Security software aims to prevent, not create, botnets.

Updating devices with the latest firmware is a security measure against botnets.

Using strong passwords is a preventive measure against the creation of botnets.

References

- **9.2.2 Attack Types**
- **9.2.3 Distributed DoS Attacks and Botnets**
- **9.2.5 Lab: Analyze a DoS Attack**
- **9.2.6 Lab: Analyze a DDoS Attack**
- **12.3.11 Lab: Enable Wireless Intrusion Prevention**

q_ddos_botnet_creation_n09.question.fex

Question 79. ✓ Correct

Which backup mode creates a snapshot-type image of the whole system?

- ○ Incremental backup
- → ● State/bare metal
- ○ Configuration file
- ○ Differential backup

Explanation

The state/bare metal backup mode creates a snapshot-type image of the whole system, which can be re-deployed to any device of the same make and model as a system restore.

The configuration file mode involves a copy of the configuration data in a structured format, not a complete system image.

Incremental backup refers to backing up only the changes since the last backup, not creating a complete system image.

Differential backup involves backing up changes made since the last full backup, not creating a complete system image.

References

8.1.1 Configuration Management

8.1.2 Network Device Backup Management

q_network_backup_state_bare_metal_n09.question.fex

Question 80. ✓ Correct

In the context of IEEE 802.1X, what is the role of a switch configured as a RADIUS client?

- ○ To manage network storage
- → ● To forward authentication data
- ○ To encrypt network traffic
- ○ To distribute IP addresses

Explanation

In the context of IEEE 802.1X, a switch configured as a RADIUS client forwards authentication data between the RADIUS server and the supplicant device. This allows the RADIUS server to validate authentication credentials without the switch having to store any authentication information itself.

Distributing IP addresses is typically the role of a DHCP server, not a switch configured as a RADIUS client in the context of IEEE 802.1X.

Encrypting network traffic is not the primary role of a switch configured as a RADIUS client; it focuses on forwarding authentication data.

Managing network storage is unrelated to the function of a switch configured as a RADIUS client in the context of IEEE 802.1X.

References

10.4.5 Extensible Authentication Protocol and IEEE 802.1X

10.4.6 Port Guards

10.4.7 Lab: Harden a Switch

q_eap_radius_switch_n09.question.fex

Question 81. ✓ Correct

Why are longer and more complex passwords more secure against brute force attacks?

- ○ They are less likely to be stored in password files.
- ○ They take less time to crack.
- → ● They increase the amount of time the attack takes to run.
- ○ They are easier to remember.

Explanation

The correct answer is that they increase the amount of time the attack takes to run. Longer and more complex passwords exponentially increase the number of possible combinations, making brute force attacks significantly more time-consuming and, therefore, less feasible.

That they are easier to remember is generally not true; longer and more complex passwords are often harder to remember.

That they take less time to crack is the opposite of the correct answer.

The complexity and length of a password do not affect whether it is stored in password files.

References

9.2.2 Attack Types

9.2.4 Malware Attacks

q_password_attacks_complex_passwords_n09.question.fex

Question 82. ✓ Correct

What is the role of encryption in an access control solution?

○ To physically secure devices and resources

○ To give readable access to data

○ To serve as the only method of access control

→ ● To convert plaintext into ciphertext

Explanation

Encryption is a logical security system that converts human-readable plaintext into unreadable ciphertext. This process ensures data confidentiality, as the ciphertext can only be decrypted and read by those who possess the correct key.

Encryption is a form of logical security, not physical security.

Encryption is one of many methods used in access control solutions, not the sole method.

Encryption restricts access to data by making it unreadable without the correct decryption key.

References

9.1.4 Encryption

q_encryption_acs_encryption_n09.question.fex

Question 83. ✓ Correct

What does a ciphertext represent in the context of encryption?

- ○ The conversion of plaintext into a hash
- ○ The original human-readable information
- → ● The encrypted version of plaintext
- ○ The key used to encrypt the plaintext

Explanation

Ciphertext is the result of the encryption process, where plaintext (human-readable information) is converted into an encrypted, unreadable format. This ensures confidentiality, as the ciphertext can only be decrypted back into plaintext by those who possess the correct decryption key.

The original human-readable information is referred to as plaintext, not ciphertext.

The key is a separate entity used in the encryption and decryption processes, not the ciphertext itself.

Converting plaintext into a hash is a different process, related to cryptographic hashing, not encryption.

References

9.1.4 Encryption

q_encryption_cyphertext_n09.question.fex

Question 84. ✓ Correct

Which type of scanners use specially crafted probes to locate hosts that might be configured not to respond to pings?

○ Graphic design software

○ Spreadsheet analysis tools

○ Email management systems

→ ● Security-oriented scanners

Explanation

Security-oriented scanners are designed to identify and assess potential vulnerabilities within a network. They use specially crafted probes to detect hosts that are intentionally configured to remain hidden or not respond to conventional methods like pings, making them crucial for comprehensive security assessments.

Graphic design software is used for creating and editing visual content, such as images and graphics, and has no functionality related to network scanning or security.

Spreadsheet analysis tools are designed for data organization, analysis, and calculation tasks. They do not have capabilities for network scanning or the use of specially crafted probes for security purposes.

Email management systems are used to organize, send, and receive emails. They do not involve network scanning or the use of specially crafted probes to detect hidden network hosts, as their primary function is related to email communication management.

References

8.2.1 Network Discovery

q_ip_scanner_security-oriented_n09.question.fex

Question 85. ✓ Correct

What does MTTF stand for, and how is it different from MTBF?

○ Maximum Time to Fix; MTTF is used for repairable components, while MTBF is for non-repairable ones.

○ Mean Time to Fix; MTTF and MTBF are interchangeable terms.

○ Maximum Time to Failure; MTTF is used for predicting the longest operational time, while MTBF is an average.

→ ● Mean Time to Failure; MTTF is used for non-repairable components, while MTBF is for repairable ones.

Explanation

MTTF (Mean Time to Failure) is used to express the expected lifetime or reliability of non-repairable components, providing an average time until failure. MTBF (Mean Time Between Failures) is used for repairable components, indicating the average time between failures. The key difference is in the applicability to repairable versus non-repairable components.

Maximum Time to Fix is not what MTTF stands for, and the explanation incorrectly swaps the uses of MTTF and MTBF.

Mean Time to Fix is not the correct meaning of MTTF, and MTTF and MTBF are not interchangeable; they apply to different types of components.

Maximum Time to Failure is not the correct interpretation of MTTF, which represents an average, not a maximum. MTBF is also an average time between failures, not a specific prediction of operational time.

References

7.4.2 Disaster Recovery Metrics

7.4.4 Fault Tolerance and Redundancy

q_multipathing_mttf_vs_mtbf_n09.question.fex

Question 86. ✓ Correct

Why are behavioral, location, and time factors not reliable enough to be used as single factors in authentication?

→ ● They are not specific or reliable enough.

○ They are not recognized by authentication systems.

○ They are too easy to fake.

○ They are too difficult to measure.

Explanation

Behavioral, location, and time factors lack the specificity and reliability needed for secure authentication on their own. They can, however, supplement other factors to strengthen the authentication system.

While some behavioral factors might be easier to mimic than others, the main issue is their lack of specificity and reliability.

Difficulty in measurement is not the primary issue; it's their effectiveness as standalone factors that is in question.

These factors are recognized by systems but are not sufficient on their own for secure authentication.

References

10.1.1 Access Control

10.1.2 Authentication Methods

10.1.3 Local Authentication

10.1.4 Single Sign-On and Kerberos

10.1.8 Remote Authentication

10.3.4 Scanning for Unsecure Protocols

13.2.1 Remote Access Considerations

q_mfa_single_unreliable_n09.question.fex

Question 87. ✓ Correct

What is the purpose of a community string in SNMP?

○ To increase network speed

→ ● To serve as a type of password

○ To encrypt data packets

○ To identify the network topology

Explanation

A community string in SNMP acts as a rudimentary type of password, allowing only management systems configured with the same community string to communicate with the agent.

While encryption is crucial for secure communication, the community string in SNMP serves as a password for access control, not for encrypting data packets.

The community string's purpose is to control access to SNMP agents, not to directly influence network performance metrics like speed.

Identifying network topology involves mapping the physical and logical arrangement of a network, a task unrelated to the function of a community string, which is to authenticate access to SNMP agents.

References

8.2.1 Network Discovery

8.3.1 SNMP Agents and Monitors

8.3.2 SNMP Security

8.3.3 Configuring an SNMP System on a Router

8.3.4 Monitoring a Switch with SNMP

8.3.5 Configuring SNMP Trap

q_snmp_community_string_role_n09.question.fex

Question 88. ✓ Correct

What is Personally Identifiable Information (PII)?

○ Information related to a company's financial status

○ Any data that can be publicly accessed

→ ● Data that can identify, contact, or locate an individual

○ Data that is encrypted and stored securely

Explanation

PII includes any data that can be used on its own or with other information to identify, contact, locate, or describe a single person. Examples include Social Security Numbers, names, addresses, email addresses, and biometric data.

PII is specifically about data that can identify individuals, not publicly accessible data.

Information related to a company's financial status is not considered PII as it does not identify individuals.

Whether data is encrypted and stored securely is irrelevant to its classification as PII; it's about the nature of the data itself.

References

9.1.3 Regulatory Compliance

q_reg_comp_pii_role_n09.question.fex

Question 89. ✓ Correct

Which of the following combinations represents two-factor authentication?

→ ● Password and a smart card

○ Password and a user's favorite color

○ Password and the time of login

○ Two different passwords

Explanation

The correct answer is a password and a smart card. Two-factor authentication requires two different types of authentication factors. A password is a knowledge factor, and a smart card is an ownership factor, making this combination a valid two-factor authentication method.

Two different passwords both fall under the knowledge factor and do not constitute two-factor authentication.

A favorite color, like a password, is knowledge-based and does not combine two distinct factors.

The time of login does not represent a separate authentication factor in the context of verifying identity.

References

10.1.2 Authentication Methods

10.1.3 Local Authentication

10.3.4 Scanning for Unsecure Protocols

q_mfa_two-factor_n09.question.fex

Question 90. ✓ Correct

In an LDAP distinguished name (DN), how are the components of the name structured?

○ Through a sequence of encrypted tokens

○ As a list of user-defined keywords

○ In a hierarchical tree structure

→ ● As a series of attribute=value pairs

Explanation

In LDAP, a distinguished name (DN) is structured as a series of attribute=value pairs, separated by commas. This format allows for the precise identification of objects within the directory by specifying attributes such as Common Name (CN), Organizational Unit (OU), and others in a specific order. The most specific attribute is listed first, with successive attributes becoming progressively broader, ensuring a unique identifier within the directory.

While LDAP entries are indeed organized in a hierarchical tree structure, this option describes the overall organization of the directory rather than the specific structure of a distinguished name. The DN itself is a string composed of attribute=value pairs, not a tree structure.

Distinguished names are not structured as a list of user-defined keywords. Instead, they follow a specific syntax using attribute=value pairs to ensure consistency and interoperability across different LDAP implementations.

Distinguished names are not structured through a sequence of encrypted tokens. Encryption may be used to secure the transmission of LDAP data, including DNs, but the DN itself is composed of clear-text attribute=value pairs for the purpose of uniquely identifying directory objects.

References

6.1.6 Common TCP and UDP Ports

10.2.3 Lightweight Directory Access Protocol

10.2.5 Lab: Manage Account Policies

q_ldap_attribute_value_pairs_n09.question.fex

Question 91. ✓ Correct

What does the principle of least privilege entail in the context of PAM?

→ ● Granting users only the rights necessary to perform their job

○ Providing all users with administrative privileges

○ Granting users unlimited rights to perform their job

○ Allowing users to determine their access rights

Explanation

The principle of least privilege means ensuring that users are granted only those rights which are essential for them to perform their job functions. This minimizes the risk associated with compromised accounts and limits the potential damage that can be done by threat actors.

Granting unlimited rights contradicts the principle of least privilege, which aims to minimize rights to what is necessary.

Allowing users to determine their access rights can lead to excessive privileges and security risks.

Providing all users with administrative privileges would violate the principle of least privilege and significantly increase security risks.

References

10.2.2 Privileged Access Management

10.2.5 Lab: Manage Account Policies

q_pam_least_privilege_n09.question.fex

Question 92. ✓ Correct

What is the purpose of spoofing attacks?

→ ● To disguise the attacker's identity

○ To provide legitimate services to users

○ To enhance the performance of ARP services

○ To improve the security of DNS services

Explanation

Spoofing attacks involve disguising the attacker's identity or forging the source of information to appear legitimate. This can include creating false websites, manipulating network packets, or using social engineering techniques to deceive and exploit victims.

Spoofing attacks do not aim to improve the security of DNS services but rather exploit them to mislead or deceive.

Enhancing the performance of ARP services is not the goal of spoofing attacks. These attacks may abuse ARP services for malicious purposes.

Providing legitimate services is not the intent behind spoofing attacks. The goal is deception and exploitation.

References

9.3.1 On-Path Attacks

q_attack_types_spoofing_attacks_n09.question.fex

Question 93. ✓ Correct

What role does separation of duties play in PAM?

○ It allows users to choose their responsibilities.

→ ● It divides responsibilities among individuals to prevent abuse of power.

○ It ensures all users have the same level of access.

○ It consolidates duties to streamline management.

Explanation

Separation of duties is a control mechanism that divides critical responsibilities among different individuals. This is done to prevent ethical conflicts, misuse, or abuse of powers, especially in areas where insider threats could compromise critical systems or procedures.

Separation of duties does not aim to equalize access levels but to distribute responsibilities to enhance security.

Consolidating duties would increase risk by concentrating power, contrary to the goal of separation of duties.

Allowing users to choose their responsibilities could lead to security risks and is not the purpose of separation of duties.

References

10.1.1 Access Control

q_pam_separation_of_duties_n09.question.fex

Question 94. ✓ Correct

What distinguishes an application log from a system log?

○ An application log cannot record errors.

○ An application log is only used for security purposes.

○ An application log records data for the entire operating system.

→ ● An application log records data for a single specific service.

Explanation

Application logs are specific to a single service or application, recording events and data relevant to its operation, unlike system logs that record events at the OS level.

Recording data for the entire operating system describes a system log, not an application log.

Application logs are used for more than just security; they track a wide range of operational data.

Application logs can and do record errors specific to the application.

References

- **8.4.1 Network Device Logs**
- **8.4.2 Log Collectors and Syslog**
- **8.4.3 Event Prioritization and Alerting**
- **8.4.4 Security Information and Event Management**
- **8.4.5 Log Reviews**
- **8.4.6 Lab: Configure Logging in pfSense**
- **8.4.7 Lab: Evaluate Event Logs in pfSense**
- **8.4.8 Lab: Auditing Device Logs on a Cisco Switch**
- **8.4.9 Lab: Configure Logging on Linux**
- **8.4.10 Lab: View Event Logs**

q_net_logs_app_vs_system_log_n09.question.fex

Question 95. ✓ Correct

Why might TFTP not be suitable for transferring large files?

→ ● It operates over UDP, which does not guarantee delivery.

○ It encrypts the data, causing overhead.

○ It requires manual confirmation for each packet.

○ It only works within local networks.

Explanation

The correct answer is that it operates over UDP, which does not guarantee delivery. TFTP's use of UDP means it lacks mechanisms like error checking and retransmission, making it unsuitable for large files where reliability is crucial.

TFTP does not provide encryption; its unsuitability for large files is due to its use of UDP.

TFTP's suitability is not limited by network scope but by its reliability and feature set.

TFTP's limitations stem from its use of UDP, not from requiring manual packet confirmation.

References

6.1.6 Common TCP and UDP Ports

7.2.3 File Transfer Protocol

q_ftp_transfer_large_files_n09.question.fex

Question 96. ✓ Correct

What does Nmap use to determine whether a host is present when used without switches?

- ○ It listens for any active Bluetooth devices.
- ○ It sends an email to the network administrator.
- ○ It performs a full database scan.
- → ● It pings and sends a TCP ACK packet to ports 80 and 443.

Explanation

When used without switches, Nmap's default behavior is to ping and send a TCP ACK packet to ports 80 and 443 to determine whether a host is present, which is a basic method for host discovery.

Nmap does not send emails for host discovery; it uses network protocols.

Nmap does not perform database scans for host discovery; it uses network scanning techniques.

Nmap does not listen for Bluetooth devices; it focuses on IP-based network scanning.

References

7.2.8 Lab: Scan for Web Services with Nmap

8.2.2 Nmap

8.2.3 Nmap Port Scanning

q_nmap_tcp_ack_packet_n09.question.fex

Question 97. ✓ Correct

What is a mandatory model in authorization?

→ ● A model where rights are predetermined by system-enforced rules

○ A model based on the subject's role

○ A model based on the subject's attributes

○ A model where rights are allocated by the system administrator

Explanation

The mandatory access control (MAC) model is characterized by access rights and permissions being predetermined by system-enforced rules, typically based on security classifications and clearances.

A model where rights are allocated by the system administrator more closely aligns with discretionary access control (DAC), where the object owner or system administrator can allocate rights.

Role-based access control (RBAC) assigns permissions based on predefined roles within an organization, not on system-enforced rules.

Attribute-based access control (ABAC) uses policies that evaluate attributes of users, resources, and the environment, differing from the mandatory model's system-enforced rules.

References

10.1.1 Access Control

10.1.2 Authentication Methods

10.2.2 Privileged Access Management

10.2.5 Lab: Manage Account Policies

q_access_control_mandatory_model_n09.question.fex

Question 98. ✓ Correct

What is the purpose of a Business Impact Analysis (BIA) in continuity planning?

→ ● To identify risk disruption for primary business functions

○ To evaluate the effectiveness of sales strategies

○ To assess the impact of new hires on the business

○ To identify the most profitable business areas

Explanation

A BIA is conducted to understand which business functions are critical (mission essential and primary) and to assess the risks and impacts that would arise if the organization is unable to fulfill these functions due to a disruption.

Identifying profitable business areas is a strategic business decision, not the focus of a BIA, which is concerned with continuity planning.

Assessing the impact of new hires is related to human resources management, not the objective of a BIA.

Evaluating sales strategies is a marketing function and not the purpose of conducting a BIA in continuity planning.

References

7.4.1 Disaster Recovery Concepts

q_availability_bia_role_n09.question.fex

Question 99. ✓ Correct

What is an example of an inadvertent vulnerability that users can create?

→ ● Using shadow IT without authorization

○ Implementing strong encryption algorithms

○ Employing multi-factor authentication

○ Regularly updating software and applications

Explanation

Shadow IT refers to devices, software, or services used within an organization without explicit IT department approval. This can create inadvertent vulnerabilities because these tools might not adhere to the organization's security policies or may not be covered by its security controls, potentially serving as vectors for exploits.

Implementing strong encryption algorithms is a security best practice, not an inadvertent vulnerability.

Regularly updating software and applications is a preventive measure against vulnerabilities, not a cause of them.

Employing multi-factor authentication enhances security and does not create inadvertent vulnerabilities.

References

9.2.2 Attack Types

q_attack_types_user_vulnerability_n09.question.fex

Question 100. ✓ Correct

Why is it important to stay up to date with system security advisories?

○ To keep track of new IT products

→ ● To stay informed about vulnerabilities

○ To monitor the stock market for technology companies

○ To ensure compliance with IT audit standards

Explanation

The correct answer is to stay informed about vulnerabilities and how to address them. Security advisories provide critical information about vulnerabilities in systems and the necessary steps to mitigate them, helping to maintain system security.

Security advisories focus on vulnerabilities, not new product releases.

While staying updated may help with compliance, the primary purpose of advisories is security, not audit standards.

Security advisories are unrelated to financial monitoring of technology companies.

References

8.1.5 Lifecycle Management

q_life_cycle_vulnerabilities_n09.question.fex

Question 101. ✓ Correct

What is considered a knowledge factor in authentication?

→ ● A password

○ A smart card

○ A mobile device

○ A fingerprint

Explanation

A knowledge factor is something the user knows, such as a password, PIN, or any secret information that can be used to verify their identity.

A smart card is an example of an ownership factor, something the user has.

A fingerprint is a biometric factor, which is something the user is.

A mobile device falls under the ownership factor category, as it's something the user possesses.

References

10.1.2 Authentication Methods

10.1.3 Local Authentication

10.3.4 Scanning for Unsecure Protocols

q_mfa_knowledge_factor_n09.question.fex

Question 102. ✓ Correct

What does "availability" in the CIA Triad refer to?

→ ● Information is accessible to those authorized to view or modify it.

○ The data is stored and transferred as intended and that any modification is authorized.

○ Information is accessible to those authorized to view or modify it.

○ The system is protected against unauthorized access and attacks.

Explanation

The correct answer is that information is accessible to those authorized to view or modify it. Availability ensures that data, systems, and services are available to authorized users when needed. This involves protecting against attacks that can lead to unauthorized denial of service, ensuring system uptime, and providing reliable access to resources.

The data is stored and transferred as intended and that any modification is authorized describes "integrity," which is about ensuring data remains unchanged unless the change is authorized.

Information is accessible to those authorized to view or modify it describes "confidentiality," which is about restricting access to information to authorized individuals only.

The system is protected against unauthorized access and attacks is a broader security goal, not specifically related to the "availability" aspect of the CIA Triad.

References

9.1.1 Common Security Terminology

q_sec_concepts_availability_n09.question.fex

Question 103. ✓ Correct

Which of the following is a limitation of active FTP mode regarding firewalls?

○ It only works with TCP port 22.

○ It encrypts the data transfer by default.

○ It requires HTTPS for data transfer.

→ ● It can cause configuration problems due to unpredictable port usage.

Explanation

Active mode FTP can lead to firewall configuration issues because the server initiates connections to random client ports, which can be blocked by firewalls not configured to allow such connections.

FTP does not require HTTPS; this is a separate protocol used for secure web browsing.

Active mode FTP uses TCP ports 20 and 21, not 22, which is for SSH.

FTP does not provide encryption by default; secure versions like FTPS or SFTP are needed for encryption.

References

6.1.6 Common TCP and UDP Ports

7.2.3 File Transfer Protocol

7.2.4 Secure File Transfer Protocol

q_ftp_active_limitation_n09.question.fex

Question 104. ✓ Correct

Which of the following time standards does NTP use?

○ CDT

○ PDT

→ ● UTC

○ EDT

Explanation

Network Time Protocol (NTP) uses Coordinated Universal time (UTC) instead of time zones. Each device is responsible for converting the time to the local time zone.

The other options are United States time zones:

- EDT = Eastern Time
- PDT = Pacific Time
- CDT = Central Time

References

7.1.1 Transport Layer Security

7.1.2 Network Time Protocol

7.1.3 Precision Time Protocol

7.1.4 Lab: Configure NTP on Linux

q_ntp_utc_n09.question.fex

Question 105. ✓ Correct

What does a health policy in NAC solutions typically require from a client?

→ ● An attestation report

○ A user activity log

○ A network performance analysis

○ A financial report

Explanation

A health policy in NAC solutions typically requires a client to submit an attestation report. This secure report proves that the client is running an authorized OS and has up-to-date patches and security scanner configurations, ensuring the device meets security standards before accessing the network.

A financial report is unrelated to the security and health policies enforced by NAC solutions.

A user activity log is used for monitoring and auditing purposes, not as a requirement of a health policy in NAC solutions.

A network performance analysis is not what a health policy typically requires; it focuses on the security posture of the client device.

References

10.4.5 Extensible Authentication Protocol and IEEE 802.1X

q_eap_healthy_policy_n09.question.fex

Question 106. ✓ Correct

What does "integrity" in the context of the CIA Triad mean?

○ Information is accessible to those authorized to view or modify it.

○ Certain information should only be known to certain people.

→ ● The data is stored and transferred as intended and that any modification is authorized.

○ The system is protected against unauthorized access and attacks.

Explanation

The correct answer is that data is stored and transferred as intended and that any modification is authorized. Integrity ensures that data remains accurate and consistent during its lifecycle. This means that unauthorized changes to the data, whether in storage, processing, or transit, are prevented or detected.

Information is accessible to those authorized to view or modify it describes "availability," which is about ensuring authorized users have access to information and resources.

Certain information should only be known to certain people describes "confidentiality," which is about ensuring that information is only accessible to those who are authorized.

The system is protected against unauthorized access and attacks is a broader security goal, not specifically related to the "integrity" aspect of the CIA Triad.

References

9.1.1 Common Security Terminology

q_sec_concepts_integrity_n09.question.fex

Question 107. ✓ Correct

Which of the following statements BEST describes a key principle of the Discretionary Access Control (DAC) model?

→ ● Every resource has an owner.

○ Permissions are centrally managed by a security administrator.

○ Access permissions are assigned based on the sensitivity of the data.

○ Users are assigned roles based on their job functions.

Explanation

In the Discretionary Access Control (DAC) model, a fundamental principle is that every resource, such as a file or service, has an owner. The owner, who initially creates the resource, has full control over it, including the ability to modify its Access Control List (ACL) to grant or restrict access to others. This ownership model allows for a flexible and user-centric approach to access control, where the discretion of access lies primarily with the resource owner.

While the sensitivity of data can influence access decisions in various access control models, DAC is primarily characterized by the ownership of resources rather than the sensitivity of the data they contain.

In DAC, permissions are not centrally managed by a security administrator. Instead, the control over access permissions is discretionary and lies with the individual owners of resources, who can delegate access as they see fit.

Assigning users to roles based on their job functions is a characteristic of Role-Based Access Control (RBAC), not DAC. RBAC focuses on defining roles with specific permissions to streamline access management, whereas DAC is centered around the concept of resource ownership and individual discretion.

References

10.1.1 Access Control

10.1.2 Authentication Methods

10.2.2 Privileged Access Management

10.2.5 Lab: Manage Account Policies

q_rbac_dac_key_principle_n09.question.fex

Question 108. ✓ Correct

What does MAC filtering on a switch allow an administrator to do?

- ○ Assign specific IP addresses to MAC addresses.
- ○ Limit the bandwidth usage per MAC address.
- → ● Define which MAC addresses are permitted to connect to a particular port.
- ○ Monitor the amount of data transmitted by each MAC address.

Explanation

MAC filtering enhances security by allowing only devices with specific MAC addresses to connect to a port, effectively controlling access based on hardware identifiers.

MAC filtering is about access control, not bandwidth management.

Assigning specific IP addresses to MAC addresses is incorrect as this task is typically handled by DHCP services, not MAC filtering.

Monitoring the amount of data transmitted by each MAC address is incorrect because MAC filtering's purpose is to control access, not to monitor data usage.

References

3.1.6 Media Access Control Address Format

3.4.5 MAC Address Table

10.4.1 Network Access Control and Port Security

10.4.2 Lab: Secure Access to a Switch

10.4.3 Lab: Secure Access to a Switch 2

10.4.4 Lab: Disable Switch Ports - GUI

10.4.6 Port Guards

10.4.7 Lab: Harden a Switch

q_port_security_mac_filtering_n09.question.fex

Question 109. ✓ Correct

What does enabling Root Guard on ports not used as trunk lines accomplish?

→ ● It prevents unauthorized changes to the root bridge selection.

○ It allows for faster convergence of the spanning tree.

○ It increases the number of allowable VLANs on a port.

○ It encrypts BPDU packets for secure transmission.

Explanation

Root Guard is used on ports not designated as trunk lines to maintain the network's spanning tree topology by preventing unauthorized changes to the root bridge selection. If a Root Guard-enabled port receives a BPDU that could alter the root bridge, it blocks that port, thus maintaining the integrity of the spanning tree structure.

Root Guard's purpose is not to speed up spanning tree convergence but to secure the network's spanning tree topology.

Root Guard does not encrypt BPDU packets; it blocks unauthorized BPDUs to prevent topology changes.

It does not affect the number of VLANs allowable on a port; its role is to secure the spanning tree protocol's root bridge selection.

References

10.4.1 Network Access Control and Port Security

10.4.2 Lab: Secure Access to a Switch

10.4.3 Lab: Secure Access to a Switch 2

10.4.4 Lab: Disable Switch Ports - GUI

10.4.6 Port Guards

10.4.7 Lab: Harden a Switch

10.4.8 Port Mirroring

q_switch_security_root_guard_n09.question.fex

Question 110. ✓ Correct

What is a significant difference between a TDM PBX and a VoIP PBX?

○ A VoIP PBX requires a separate data channel for each call, while a TDM PBX does not.

→ ● A TDM PBX is supplied as vendor-specific hardware, while a VoIP PBX can be implemented as software.

○ A TDM PBX can only support voice mail, while a VoIP PBX cannot.

○ A TDM PBX uses the Internet for all calls, while a VoIP PBX uses the PSTN.

Explanation

A key difference between TDM and VoIP PBX systems is that TDM PBXes are typically provided as specific hardware solutions, whereas VoIP PBXes can be implemented as software running on general-purpose servers, offering more flexibility.

Both TDM and VoIP PBX systems can support voice mail.

A VoIP PBX does not require a separate data channel for each call; it can multiplex multiple calls over the same IP network.

It's the other way around; a TDM PBX primarily uses the PSTN, while a VoIP PBX uses the Internet for transmitting voice communications.

References

7.3.3 Voice and Video Services

q_voice_video_tdm_vs_voip_n09.question.fex

Copyright © The Computing Technology Industry Association, Inc. All rights reserved.