Chp 5 NS

Candidate: Dunkan Gibson (dunkan.gibson)
Date: 2/24/2022 8:30:47 pm • Time spent: 20:41

Score: 86%

Passing Score: 80%

Question 1: ✔ Correct

You are deploying a brand new router. After you change the factory default settings, what should you do next?

- ➡ Update the firmware.
- Configure SSH to access the router configuration.
- Secure the configuration file.
- Configure anti-spoofing rules.

EXPLANATION

After changing the default settings on the router, you should update the firmware. Updates to the firmware fix any vulnerabilities that have been resolved by the manufacturer in the past.

After updating the firmware, you should configure the protocol used to connect to the router.

The configuration file stores all the configuration settings for the router, including open ports, usernames, firewall settings, and more. If possible, store the router configuration file in an encrypted form and back up the file to a secure location.

Anti-spoofing rules counter spoofing attacks where IP packets have a source address that does not belong to the sender. This is configured after the router is set up.

REFERENCES

- 2.4.1 Vulnerability Concerns
- 2.4.2 Vulnerability Concerns Facts
- 2.4.3 Impact of Vulnerabilities
- 2.4.4 Impact of Vulnerabilities Facts
- 4.1.1 Manageable Network Plan
- 4.1.2 Manageable Network Plan 2
- 4.1.3 Manageable Network Plan Facts
- 5.13.3 Router Security Facts

q_router_sec_firmware_secp7.question.fex

Question 2: ✔ Correct

A VPN is primarily used for which of the following purposes?

- Allow the use of network-attached printers
- ➡ Support secured communications over an untrusted network
- Support the distribution of public web documents
- Allow remote systems to save on long-distance charges

EXPLANATION

A VPN (virtual private network) is used primarily to support secured communications over an untrusted network. A VPN can be used over a local area network, across a WAN connection, over the internet, and even between a client and a server over a dial-up internet connection. All of the other items listed in this question are benefits or capabilities that are secondary to this primary purpose.

REFERENCES

5.5.6 VPN Facts

q_vpn_secure_secp7.question.fex

Question 3: ✔ Correct

Which of the following terms describes a network device that is exposed to attacks and has been hardened against those attacks?

- ➡ Bastion or sacrificial host
- Multi-homed
- Circuit proxy
- Kernel proxy

EXPLANATION

A bastion or sacrificial host is one that is unprotected by a firewall. The term bastion host is used to describe any device fortified against attack (such as a firewall). A sacrificial host might be a device intentionally exposed to attack, such as a honeypot.

Circuit proxy and kernel proxy are types of firewall devices.

Multi-homed describes a device with multiple network interface cards.

REFERENCES

5.2.4 DMZ Facts

q_dmz_bastion_secp7.question.fex

Question 4: ✔ Correct

You are implementing a new application control solution.

Prior to enforcing your application whitelist, you want to monitor user traffic for a period of time to discover user behaviors and log violations for later review.

How should you configure the application control software to handle applications not contained in the whitelist?

- Tarpit
- Drop
- Block
- Flag

EXPLANATION

When using an application control solution, an application whitelist is defined centrally and applied to all network devices. Only applications contained in the whitelist are allowed. Applications not whitelisted can have several actions applied:

- Blocked applications are not allowed. The session is dropped if it uses UDP and reset if it uses TCP.
- Flagged applications are allowed, but a violation is logged when they are identified.
- Tarpitted applications are not allowed. However, the connection between hosts is kept alive while the application data itself is silently dropped. This makes it appear to both hosts that the other host is receiving the data but not responding.

Not all application control solutions support tarpitting application traffic.

REFERENCES

5.10.3 Network Application Facts

q_net_app_white_secp7.question.fex

Question 5: ✕ Incorrect

Which area of focus do public-facing servers, workstations, Wi-Fi networks, and personal devices fall under?

- Network baseline
- Entry points
- Network segmentation
- ~~Inherent vulnerabilities~~

EXPLANATION

Public-facing servers, workstations, Wi-Fi networks, and personal devices are all examples of entry points for possible attacks. You must account for anything that connects to the network as a possible entry point.

Inherent vulnerabilities are any system that lacks proper security controls.

Network segmentation is the process of splitting the network into different sections.

A network baseline tells you the normal activity level on a network.

REFERENCES

5.8.2 Network Threats Facts

q_net_threat_public_secp7.question.fex

Question 6: ✔ Correct

You are adding switches to your network to support additional VLANs. Unfortunately, the new switches are from a different vendor than the current switches.

Which standard do you need to ensure that the switches are supported?

- ➡ 802.1Q
- 802.3
- 802.1x
- 802.11

EXPLANATION

If you want to implement VLANs when using multiple vendors in a switched network, be sure each switch supports the 802.1Q standard.

802.1x defines port-based network access controls.

802.11 defines wireless standards.

802.3 defines Ethernet standards.

REFERENCES

5.12.2 VLAN Facts

q_vlan_facts_802_secp7.question.fex

Question 7: ✕ Incorrect

Which of the following types of proxies can be used for web filtering?

- VPN
- Transparent
- Reverse
- ~~Content filter~~

EXPLANATION

Transparent proxies are located between a user and the internet, and they can redirect requests without changing them. These can also be used for web filtering.

Reverse proxies can be used for caching and authentication.

A VPN is not a type of proxy and is not used for web filtering.

Content filtering is not a type of proxy server.

REFERENCES

5.6.4 Web Threat Protection Facts

q_web_threat_prot_web_filter_secp7.question.fex

Question 8: ✕ Incorrect

Which 802.1Q priority is IP phone traffic on a voice VLAN tagged with by default?

- 3
- 5
- 1
- 8

EXPLANATION

By default, IP phone traffic on a voice VLAN is tagged with an 802.1Q priority of 5.

REFERENCES

5.12.2 VLAN Facts

q_vlan_facts_priority_secp7.question.fex

Question 9: ✔ Correct

Which area of focus helps to identify weak network architecture or design?

- Entry points
- Documentation
- Inherent vulnerabilities
- Network baseline

EXPLANATION

Documentation is one of the most important components of knowing a network. Proper network documentation and diagrams not only help identify a weak network architecture or design, but they also protect against system sprawl and unknown systems.

Entry points are any possible way into the network. Identifying entry points do not identify weak network architecture or design.

Inherent vulnerabilities are any system that lacks proper security controls. Identifying inherent vulnerabilities does not identify weak network architecture or design.

A network baseline tells you the normal activity level on a network. This does not help in identifying weak network architecture or design.

REFERENCES

5.8.2 Network Threats Facts

q_net_threat_docs_secp7.question.fex

Question 10: ✔ Correct

When designing a firewall, what is the recommended approach for opening and closing ports?

- ➡ Close all ports; open only ports required by applications inside the DMZ.
- Close all ports; open ports 20, 21, 53, 80, and 443.
- Open all ports; close ports that expose common network attacks.
- Open all ports; close ports that show improper traffic or attacks in progress.
- Close all ports.

EXPLANATION

When designing a firewall, the recommended practice is to close all ports and then only open those ports that allow the traffic that you want to allow inside the DMZ or the private network. Ports 20, 21, 53, 80, and 443 are common ports that are opened, but the exact ports you open depends on the services provided inside the DMZ.

REFERENCES

5.3.2 Firewall Facts

q_firewall_ports_secp7.question.fex

Question 11: ✔ Correct

You are part of a committee that is meeting to define how Network Access Control (NAC) should be implemented in the organization. Which step in the NAC process is this?

- Review
- Plan
- Apply
- Define

EXPLANATION

Planning is the first step in the NAC implementation process. In this step, a committee should convene and make decisions that define how NAC should work.

The third step in implementing NAC is to apply the policies. This occurs after the policies have been defined.

Review is the final step in the NAC implementation process. As business needs change, the process must be reviewed to determine whether changes are required.

Define is the second step in the NAC implementation process. After the committee has decided how NAC should work, the roles, identities, and permissions (policies) must be defined.

REFERENCES

5.7.2 Network Access Control Facts

q_nac_plan_secp7.question.fex

Question 12: ✔ Correct

You are the security analyst for your organization and have recently noticed a large amount of spim on the company mobile devices. Employees rely on the IM app to communicate with each other.

Which of the following countermeasures should you implement?

- Encrypt all IM traffic.
- Disable instant messaging.
- Use an IM blocker.
- Create a blacklist.

EXPLANATION

Spim is a type of spam that targets users of instant messaging services. Creating a whitelist or using an IM blocker are countermeasures that can be implemented against spim.

Creating a blacklist does not help much against spim.

Disabling instant messaging would stop the spim, but this would also stop employees from communicating with each other.

Encrypting IM traffic would not stop the spim messages.

REFERENCES

- 2.3.1 Social Engineering Overview
- 2.3.2 Social Engineering Overview Facts
- 2.3.3 Social Engineering Motivation
- 2.3.4 Social Engineering Motivation Facts
- 2.3.5 Social Engineering Techniques
- 2.3.6 Social Engineering Techniques Facts
- 2.3.7 Phishing and Internet-Based Techniques
- 2.3.8 Phishing and Internet-Based Techniques Facts
- 2.3.9 Use the Social Engineer Toolkit
- 2.3.10 Investigating a Social Engineering Attack
- 2.3.11 Identify Social Engineering
- 5.10.3 Network Application Facts

q_net_app_spim_02_secp7.question.fex

Question 13: ✔ Correct

An attacker has gained access to the administrator's login credentials. Which type of attack has most likely occurred?

- Privilege escalation
- ➡ Password cracking
- Buffer overflow
- Backdoor

EXPLANATION

Password cracking is the process of recovering secret passwords from data that has been stored in or transmitted by a computer system. If an attacker has gained access to the administrator's login credentials, this is most likely the cause of a password-cracking attack.

Privilege escalation allows a user to take advantage of a software bug or design flaw in an application to gain access to system resources or additional privileges that would typically not be available to the user.

A backdoor is an unprotected access method or pathway. Backdoors may include hard-coded passwords or hidden service accounts.

A buffer overflow attack occurs when the operating system or an application does not properly enforce boundaries for how much and which type of data can be inputted.

REFERENCES

5.9.2 Device Vulnerability Facts

11.7.2 Password Attack Facts

11.7.5 Crack Passwords

11.7.6 Crack Password Protected Files

11.7.7 Crack a Password with John the Ripper

q_dev_vuln_cracking_secp7.question.fex

Question 14: ✕ Incorrect

You've just deployed a new Cisco router that connects several network segments in your organization.

The router is physically located in a server room that requires an ID card to gain access. You've backed up the router configuration to a remote location in an encrypted file. You access the router configuration interface from your notebook computer by connecting it to the console port on the router. You've configured the management interface with a username of admin and a password of password.

What should you do to increase the security of this device?

- Include hard-coded passwords and hidden service accounts.
- Use a stronger administrative password.
- ~~Move the device to a secure data center.~~
- Use an SSH client to access the router configuration.

EXPLANATION

In this scenario, the password assigned to the device is weak and can be easily guessed. The password should be replaced with a strong one that is at least eight characters long, uses uppercase and lowercase letters, and uses numbers or symbols.

Including hard-coded passwords and hidden service accounts is an option for avoiding backdoor vulnerabilities.

Using the console port to access the device creates a dedicated connection, making the use of SSH unnecessary.

Because the device has been installed in a secured room, it's not necessary to move it to a data center.

REFERENCES

5.9.2 Device Vulnerability Facts

q_dev_vuln_password_secp7.question.fex

Question 15: ✔ Correct

Which of the following NAC agent types creates a temporary connection?

- Zero-trust
- Dissolvable
- Permanent
- Agentless

EXPLANATION

A dissolvable agent is downloaded, or a temporary connection is established. The agent is removed once the user is done with it. The user has to download or connect to the agent again if it is needed.

An agentless agent is housed on the domain controller. This is not the most convenient type of agent.

Zero-trust security means nothing is trusted unless it can pass both the authentication and authorization stages.

A permanent agent resides on a device permanently.

REFERENCES

5.7.2 Network Access Control Facts

q_nac_dissolvable_secp7.question.fex

Question 16: ✔ Correct

You've just deployed a new Cisco router that connects several network segments in your organization.

The router is physically located in a locked server closet. You use an FTP client to regularly back up the router configuration to a remote server in an encrypted file. You access the router configuration interface from a notebook computer that is connected to the router's console port. You've configured the device with the username admin01 and the password P@ssW0rd. You have used the MD5 hashing algorithm to protect the password.

What should you do to increase the security of this device?

- Move the router to a secure data center.
- Use an SSH client to access the router configuration.
- Use encrypted Type 7 passwords.
- ➡ Use SCP to back up the router configuration to a remote location.

EXPLANATION

In this scenario, the router configuration is being copied to a remote location using an unsecure protocol (File Transfer Protocol) that transfers data in cleartext. You should instead use the Secure Copy Protocol (SCP) to transfer the backup from the router to the remote storage location.

It is not necessary to use an SSH client when using the console port to configure the router. It is also not necessary to move the device to a data center if it is currently located in a locked server closet. Encrypted Type 7 passwords on a Cisco device are less secure than those protected with MD5.

REFERENCES

5.13.3 Router Security Facts

q_router_sec_ssh_02_secp7.question.fex

Question 17: ✔ Correct

A proxy server can be configured to do which of the following?

- Act as a unified threat security device or web security gateway.
- Allow all content except for the content you have identified as restricted.
- ➡ Restrict users on the inside of a network from getting out to the internet.
- Block all content except for the content you have identified as permissible.

EXPLANATION

Proxies can be configured to:

- Restrict users on the inside of a network from getting out to the internet.
- Restrict access by user or by specific website.
- Restrict users from using certain protocols.
- Use access controls to control inbound or outbound traffic.
- Shield or hide a private network to provide online anonymity and make it more difficult to track web surfing behavior.
- Cache heavily accessed web content to improve performance.

An internet content filter is software used to monitor and restrict content delivered across the web to an end user. Two types of configurations are commonly used, which are:

- Allow all content except for the content you have identified as restricted.
- Block all content except for the content you have identified as permissible.

All-in-one security appliances combine many security functions into a single device. All-in-one security appliances are also known as unified threat security devices or web security gateways.

REFERENCES

5.1.5 Security Solution Facts

q_sec_sol_proxy_secp7.question.fex

Question 18: ✕ Incorrect

To answer this question, complete the lab using the information below. **Launch Lab**

You did not attempt the lab.

REFERENCES

5.5.1 Virtual Private Networks

5.5.2 Configuring a VPN

5.5.4 Configure a Remote Access VPN

c91d48b2-dfec-4369-a28e-a43a9ac0b70c

Question 19: ✓ Correct

Which VPN protocol typically employs IPsec as its data encryption mechanism?

- PPP
- PPTP
- L2F
- L2TP

EXPLANATION

L2TP (Layer 2 Tunneling Protocol) is the VPN protocol that typically employs IPsec as its data encryption mechanism. L2TP is the recommended VPN protocol to use on dial-up VPN connections.

PPTP and PPP only support CHAP and PAP for data encryption. L2F offers no data encryption.

REFERENCES

5.5.7 VPN Protocol Facts

q_vpn_prot_l2tp_secp7.question.fex

Question 20: ✔ Correct

An attacker sets up 100 drone computers that flood a DNS server with invalid requests. This is an example of which kind of attack?

- Backdoor
- Spamming
- DDoS
- Replay

EXPLANATION

A denial-of-service (DoS) attack generates excessive traffic to overload communication channels or exploit software flaws. A distributed denial-of-service (DDoS) attack employs multiple attackers.

Spamming is just a traffic generation form of attack where unrequested messages are sent to a victim. Replay and backdoor attacks are both flaw-exploitation attack forms. Replay attacks exploit software flaws by capturing traffic, possibly editing it, and then replaying the traffic in an attempt to gain access to a system. Backdoor attacks exploit software flaws by obtaining access codes or account credentials to bypass security. Backdoors can also be planted by hackers to allow easy re-access to a compromised system.

REFERENCES

5.8.2 Network Threats Facts

q_net_threat_ddos_secp7.question.fex

Question 21: ✔ Correct

Jessica needs to set up a firewall to protect her internal network from the internet. Which of the following would be the BEST type of firewall for her to use?

- ➡ Hardware
- Stateful
- Software
- Tunneling

EXPLANATION

Hardware firewalls are physical devices that are usually placed at the junction or gateway between two networks, generally a private network and a public network like the internet. Hardware firewalls can be a standalone product or can also be built into devices like broadband routers.

Software firewalls are generally used to protect individual hosts.

Tunneling is when an attacker wraps a malicious command in an HTTP, ICMP, or ACK tunneling packet that bypasses the firewall and reaches an internal system.

Stateful firewalls, also referred to as stateful multilayer firewalls, determine the legitimacy of traffic based on the state of the connection from which the traffic originated.

REFERENCES

5.3.2 Firewall Facts

q_firewall_hardware_secp7.question.fex

Question 22: ✔ Correct

Which problem does NAT help address?

- ➡ The shortage of IPv4 addresses
- The shortage of IPv6 addresses
- IPSec not working properly
- Registering IP addresses with an ISP

EXPLANATION

Network Address Translation helps address the shortage of registered IPv4 addresses. A NAT router translates multiple private addresses into a single registered IP address.

The internet is classified as a public network. All devices on a public network must have a registered IP address assigned by an Internet Service Provider (ISP). NAT does not address any issues in this process.

There is no shortage of IPv6 addresses.

NAT can cause IPSec to malfunction because NAT changes packet headers. IPSec detects changes to packet headers as part of the security process.

REFERENCES

5.4.4 NAT Facts

q_nat_nat_01_secp7.question.fex

Question 23: ✔ Correct

Which of the following defines all the prerequisites a device must meet in order to access a network?

- Authorization
- Zero-trust security
- Authentication
- Identity Services Engine (ISE)

EXPLANATION

Authentication defines all the prerequisites a device must meet in order to access a network. These criteria are detailed for such things as anti-malware, OS, and patch level.

Authorization looks at the authentication information and applies the appropriate policies to provide the device with the access it's defined to receive.

Zero-trust security means nothing is trusted unless it can pass both the authentication and authorization stages.

Identity Services Engine (ISE) is Cisco's NAC solution.

REFERENCES

5.7.2 Network Access Control Facts

6.1.6 Access Control Model Facts

6.3.3 Authorization Facts

6.9.2 Remote Access Facts

q_nac_authentication_secp7.question.fex

Question 24: ✔ Correct

The IT manager has asked you to create a separate VLAN to be used exclusively for wireless guest devices to connect to.

Which of the following is the primary benefit of creating this VLAN?

- You can load-balance wireless guest network traffic to have a lower priority than the rest of the traffic on the network.
- ➡ You can control security by isolating wireless guest devices within this VLAN.
- You can control broadcast traffic and create a collision domain for just the wireless guest devices.
- You can create a wireless guest network more affordably with a VLAN than you can with a router.

EXPLANATION

The primary benefit of creating a VLAN for wireless guest devices to connect to is it allows you to control security by isolating wireless guest devices within this VLAN. Devices on this VLAN cannot communicate with other devices in other VLANs unless you allow traffic to get through with a router or Layer 3 switch. In this case, you would likely keep this wireless guest VLAN isolated from the rest of your network and only allow traffic from this VLAN to communicate with the internet.

The following are also benefits of creating VLANs in general (but these are not the primary benefit of creating a wireless guest VLAN):

- You can create virtual LANs based on criteria other than physical location (such as workgroup, protocol, or service).
- You can simplify device moves (devices are moved to new VLANs by modifying the port assignment).
- You can control broadcast traffic and create collision domains based on logical criteria.
- You can load-balance network traffic (divide traffic logically rather than physically).

REFERENCES

5.12.2 VLAN Facts

q_vlan_facts_security_secp7.question.fex

Question 25: ✔ Correct

You are configuring web threat protection on the network and want to prevent users from visiting www.videosite.org. Which of the following needs to be configured?

- Anti-phishing software
- Website filtering
- Content filtering
- Virus scanner

EXPLANATION

To block users from visiting a specific site, you should configure website filtering.

Content filtering can block users from visiting specific categories of websites.

Virus scanners identify infected content and dispose of it.

Anti-phishing software scans content to identify and dispose of phishing attempts, preventing outside attempts to access confidential information.

REFERENCES

5.6.4 Web Threat Protection Facts

q_web_threat_prot_url_filter_secp7.question.fex

Question 26: ✔ Correct

In which of the following situations would you most likely implement a demilitarized zone (DMZ)?

- ➡ You want to protect a public web server from attack.
- You want to detect and respond to attacks in real time.
- You want to encrypt data sent between two hosts using the internet.
- You want internet users to see a single IP address when accessing your company network.

EXPLANATION

Use a demilitarized zone (DMZ) to protect public hosts on the internet, such as a web server, from attack. The DMZ uses an outer firewall that prevents internet attacks. All publicly-accessible hosts are inside the DMZ. A second firewall protects the private network from the internet.

Use a Virtual Private Network (VPN) to encrypt data between two hosts on the Internet. Use Network Address Translation (NAT) to hide internal IP addresses from the internet. Use an Intrusion Prevention System (IPS) to detect and respond to threats in real time.

REFERENCES

5.2.4 DMZ Facts

q_dmz_public_secp7.question.fex

Question 27: ✔ Correct

A network device is given an IP address of 172.16.0.55. Which type of network is this device on?

- IPv6 private network
- Class C private network
- Class B private network
- Class A private network

EXPLANATION

A device with the IP address of 172.16.0.55 is on a Class B private network. A private network can use IPv4 addresses in the following ranges that have been reserved for private use (meaning they are not used by hosts on the internet).

- 10.0.0.0 to 10.255.255.255 (known as Class A private network addresses)
- 172.16.0.0 to 172.31.255.255 (known as Class B private network addresses)
- 192.168.0.0 to 192.168.255.255 (known as Class C private network addresses)

IPv6 reserves all addresses beginning with a binary 1111 1110 11 (hexadecimal FEC0::/48) for private IP networks. This address range is called the site-local address range.

REFERENCES

5.4.4 NAT Facts

q_nat_private_secp7.question.fex

Question 28: ✔ Correct

A relatively new employee in the data entry cubical farm was assigned a user account similar to the other data entry employees' accounts. However, audit logs have shown that this user account has been used to change ACLs on several confidential files and has accessed data in restricted areas.

This situation indicates which of the following has occurred?

- External attack
- Physical security
- Privilege escalation
- Social engineering

EXPLANATION

This situation describes the result of a successful privilege escalation attack. If a low-end user account is detected performing high-level activities, it is obvious that the user account has somehow gained additional privileges.

Physical security is the protection of corporate assets from threats such as theft or damage.

Social engineering attacks involve stealing information or convincing someone to perform an inappropriate activity via email, phone, or in person.

External attacks are when unauthorized individuals try to breach a network from off-site.

REFERENCES

2.4.2 Vulnerability Concerns Facts

5.9.2 Device Vulnerability Facts

6.1.4 Access Control Best Practices

q_dev_vuln_privilege_01_secp7.question.fex

Question 29: ✔ Correct

You manage a single subnet with three switches. They are connected to provide redundant paths between the switches.

Which feature prevents switching loops and ensures there is only a single active path between any two switches?

- 802.1x
- ➡ Spanning Tree Protocol
- PoE
- Bonding
- Trunking

EXPLANATION

Spanning Tree Protocol is a protocol on a switch that allows the switch to maintain multiple paths between switches within a subnet. Spanning Tree Protocol runs on each switch and is used to select a single path between any two switches.

- Without Spanning Tree Protocol, switches that are connected together with multiple links would form a switching loop where frames are passed back and forth continuously.
- Spanning Tree Protocol provides only a single active path between switches. Switch ports that are part of that path are placed in a forwarding state.
- Switch ports that are part of redundant but unused paths are placed in a blocking (non-forwarding) state.
- When an active path goes down, Spanning Tree Protocol automatically recovers and activates the backup ports necessary to provide continued connection between devices.

Bonding does the opposite of Spanning Tree Protocol. Bonding allows multiple switch ports to be used at the same time to reach a specific destination. 802.1x is an authentication protocol used with port security (or port authentication). Power over Ethernet (PoE) supplies power to end devices through the RJ-45 Ethernet switch port. Trunking identifies ports that are used to carry VLAN traffic between switches. A trunk port is a member of all VLANs defined on all switches.

REFERENCES

5.11.3 Switch Security Facts

q_sec_swi_spanning_secp7.question.fex

Question 30: ✔ Correct

Travis is sending a highly confidential email to Craig that contains sensitive data. Which of the following should Travis implement to ensure that only Craig is able to read the email?

- Anti-phishing software
- Encryption
- Virus scanner
- Spam filter

EXPLANATION

Encryption causes data, such as the content of an email, to be unintelligible except to those who have the proper key to decrypt it. Travis should make sure to encrypt the email before sending it so that only Craig is able to open the email and read the contents.

Virus scanners identify infected content and dispose of it.

Gateway email spam filters prevent spam emails from reaching your network, servers, and computers.

Anti-phishing software scans content to identify and dispose of phishing attempts, preventing outside attempts to access confidential information.

REFERENCES

5.6.4 Web Threat Protection Facts

q_web_threat_prot_encryption_secp7.question.fex

Question 31: ✔ Correct

You want to create a collection of computers on your network that appear to have valuable data but actually store fake data that could entice a potential intruder. Once the intruder connects, you want to be able to observe and gather information about the attacker's methods.

Which feature should you implement?

- NIDS
- NIPS
- Extranet
- ➡ Honeynet

EXPLANATION

A honeypot is a device or virtual machine that entices intruders by displaying a vulnerable trait or flaw or by appearing to contain valuable data. A honeynet is a network of honeypots.

A network-based IDS (NIDS) is a dedicated device installed on a network that's used to analyze all traffic on the network. An NIPS is a network-based intrusion prevention system that can take actions in response to intrusion.

An extranet is a privately controlled network located between the internet and a private LAN, but distinct from both. An extranet is often used to grant resource access to business partners, suppliers, and even customers outside of the organization.

REFERENCES

5.1.3 Security Zone Facts

q_sec_zone_honeynet_secp7.question.fex

Question 32: ✔ Correct

Which of the following should be configured on the router to filter traffic at the router level?

- Anti-spoofing rules
- SSH
- ➡ Access control list
- Telnet

EXPLANATION

Router access control lists (ACLs) can be configured to increase security and limit traffic, much like a firewall but on the router level. ACLs filter the traffic and determine if the data should be blocked or forwarded.

Anti-spoofing rules counter spoofing attacks where IP packets have a source address that does not belong to the sender.

Secure Shell (SSH) is a secure protocol that can be used to connect to the router.

Telnet is an older protocol used to connect to remote devices. It should not be used any longer.

REFERENCES

4.3.3 File Permission Facts

5.3.2 Firewall Facts

5.13.3 Router Security Facts

6.3.3 Authorization Facts

q_router_sec_acl_secp7.question.fex

Question 33: ✔ Correct

When configuring VLANs on a switch, what is used to identify which VLAN a device belongs to?

- IP address
- MAC address
- Switch port
- Host name

EXPLANATION

VLAN membership is configured by assigning a switch port to a VLAN. A switch can have multiple VLANs configured on it, but each switch port can only be a member of a single VLAN. All devices connected to a switch port are members of the same VLAN.

REFERENCES

5.12.2 VLAN Facts

q_vlan_facts_port_secp7.question.fex

Question 34: ✕ Incorrect

Your network devices are categorized into the following zone types:

- No-trust zone
- Low-trust zone
- Medium-trust zone
- High-trust zone

Your network architecture employs multiple VLANs for each of these network zones. Each zone is separated by a firewall that ensures only specific traffic is allowed.

Which of the following is the secure architecture concept that is being used on this network?

- ~~Trust-zone networking~~
- Virtual local area networking
- Network firewalling
- ➡ Network segmentation

EXPLANATION

The secure network architecture concept that is being used in this example is network segmentation. The most common way to segment networks is to create multiple VLANs for each network zone. These zones can also be separated by firewalls to ensure only specific traffic is allowed. One way to segment a network is to categorize systems into different zones (for example, a no-trust zone, low-trust zone, medium-trust zone, high-trust zone, and highest-trust zone).

REFERENCES

5.8.2 Network Threats Facts

q_net_threat_segment_secp7.question.fex

Question 35: ✔ Correct

Which of the following is a benefit of P2P applications?

- ➡ Shared resources
- Strong security
- Low-upload bandwidth
- Real-time communication

EXPLANATION

Peer-to-peer (P2P) software allows users to share content and access content shared by other users without using centralized servers or centralized access control. Peer-to-peer applications can be a great way to share bandwidth and resources.

Strong security is not a benefit of P2P applications. Many of these applications pose high security risks.

Real-time communication is a strength of instant messaging clients.

Low-upload bandwidth is not a benefit of P2P applications. P2P applications consume large amounts of upload bandwidth.

REFERENCES

5.10.3 Network Application Facts

q_net_app_peer_04_secp7.question.fex

Question 36: ✔ Correct

Which of the following is another name for a firewall that performs router functions?

- ➡ Screening router
- Screened subnet
- Screened-host gateway
- Dual-homed gateway

EXPLANATION

A firewall performing router functions is considered a screening router. A screening router is the router that is most external to your network and closest to the internet. It uses access control lists (ACLs) to filter packets as a form of security.

A dual-homed gateway is a firewall device that typically has three network interfaces: one connected to the internet, one connected to the public subnet, and one connected to the private network.

A screened-host gateway resides within the DMZ, requiring users to authenticate in order to access resources within the DMZ or the intranet.

A screened subnet uses two firewalls. The external firewall is connected to the internet and allows access to public resources. The internal firewall connects the screened subnet to the private network.

REFERENCES

5.2.4 DMZ Facts

q_dmz_screen_secp7.question.fex

Question 37: ✔ Correct

Which of the following scenarios would typically utilize 802.1x authentication?

- Authenticating remote access clients
- ➡ Controlling access through a switch
- Controlling access through a router
- Authenticating VPN users through the internet

EXPLANATION

802.1x authentication is an authentication method used on a LAN to allow or deny access based on a port or connection to the network. 802.1x is used for port authentication on switches and requires an authentication server for validating user credentials. This server is typically a RADIUS server.

Remote access authentication is handled by remote access servers or a combination of remote access servers and a RADIUS server for centralized authentication. VPN connections can be controlled by remote access servers or by a special device called a VPN concentrator.

REFERENCES

5.11.3 Switch Security Facts

q_sec_swi_802x_02_secp7.question.fex

Question 38: ✕ Incorrect

To answer this question, complete the lab using the information below.
You have already answered this question.
You are not allowed to view the lab again.

Launch Lab

You did not complete the lab correctly.

Loading

REFERENCES

5.3.1 Firewalls

cf2ab8bc-7492-4dc2-ae41-f2204b6f63e1

Question 39: ✔ Correct

You are configuring the security settings for your network. You have decided to configure a policy that requires any computer connecting to the network to run at least Windows 10 version 2004. Which of the following have you configured?

- ISE
- NAP
- NAC
- NAT

EXPLANATION

Network Access Control (NAC) is a policy-driven control process that allows or denies network access to devices connecting to a network. For example, you may want to have policies that require connecting devices to meet certain criteria, such as having a particular version of Windows, the latest antivirus definitions, or Windows Firewall enabled.

Network Address Translation (NAT) translates multiple private addresses into a single registered IP address.

Network Access Protection (NAP) is Microsoft's NAC solution.

Identity Services Engine (ISE) is Cisco's NAC solution.

REFERENCES

5.7.2 Network Access Control Facts

q_nac_nac_secp7.question.fex

Question 40: ✔ Correct

Which of the following attacks, if successful, causes a switch to function like a hub?

- ARP poisoning
- MAC spoofing
- Replay attack
- MAC flooding

EXPLANATION

MAC flooding overloads the switch's MAC forwarding table to make the switch function like a hub. The attacker floods the switch with packets, each containing different source MAC addresses. The flood of packets fills up the forwarding table and consumes so much of the memory in the switch that it causes the switch to enter a state called fail open mode. While in this mode, all incoming packets are broadcast out of all ports (as with a hub), instead of just to the correct ports, as per normal operation.

ARP poisoning associates the attacker's MAC address with the IP address of victim devices. When computers send an ARP request to get the MAC address of a known IP address, the attacker's system responds with its own MAC address. MAC spoofing is changing the source MAC address on frames sent by the attacker.

In a replay attack, the attacker uses a protocol analyzer or sniffer to capture authentication information going from the client to the server. The attacker then uses this information to connect at a later time and pretend to be the client.

REFERENCES

5.11.7 Switch Attack Facts

q_swi_attack_mac_flood_secp7.question.fex

Question 41: ✔ Correct

Which of the following best describes the concept of a virtual LAN?

- Devices connected by a transmission medium other than a cable (microwave, radio transmissions).
- Devices connected through the internet that can communicate without using a network address.
- Devices in separate networks (different network addresses) logically grouped as if they were in the same network.
- Devices on different networks that can receive multicast packets.
- ➡ Devices on the same network logically grouped as if they were on separate networks.

EXPLANATION

A virtual LAN is created by identifying a subset of devices on the same network and logically identifying them as if they were on separate networks. Think of VLANs as subdivisions of a LAN.

REFERENCES

5.11.3 Switch Security Facts

q_sec_swi_vlan_02_secp7.question.fex

Question 42: ✔ Correct

A honeypot is used for which purpose?

- To prevent sensitive data from being accessed
- ➡ To delay intruders in order to gather auditing data
- To disable an intruder's system
- To entrap intruders

EXPLANATION

A honeypot is used to delay intruders in order to gather auditing data. A honeypot is a fake network or system that hosts false information but responds as a real system should. Honeypots usually entice intruders to spend considerable time on the system and allow extensive logging of the intruder's activities. A honeypot often allows companies to discover and even prosecute intruders.

Honeypots should not be used to entrap intruders. Entrapment is an illegal activity. Honeypots are not direct countermeasures to preventing unwanted access. Rather, they are an enticement to prevent intruders from getting into the private network in the first place. Honeypots rarely take offensive action against intruders. They may prevent malicious activities from being launched by an intruder, but they do not direct attacks at him or her.

REFERENCES

5.1.3 Security Zone Facts

q_sec_zone_honeypot_secp7.question.fex

Question 43: ✔ Correct

An attacker was able to gain unauthorized access to a mobile phone and install a Trojan horse so that he or she could bypass security controls and reconnect later.

Which type of attack is this an example of?

- Social engineering
- Privilege escalation
- Replay
- ➡ Backdoor

EXPLANATION

A backdoor is an unprotected access method or pathway. Backdoors:

- Include hard-coded passwords and hidden service accounts.
- Are often added during development as a shortcut to circumvent security. If they are not removed, they present a security problem.
- Can be added by attackers who have gained unauthorized access to a device. When added, the backdoor can be used at a future time to easily bypass security controls.
- Can be used to remotely control the device at a later date.
- Rely on secrecy to maintain security.

Social engineering attacks involve stealing information or convincing someone to perform an inappropriate activity via email, via phone, or in person.

A replay attack is a network attack that occurs when an attacker intercepts data and fraudulently delays or re-transmits it.

Privilege escalation allows a user to take advantage of a software bug or design flaw in an application to gain access to system resources or additional privileges that aren't typically available to that user.

REFERENCES

5.9.2 Device Vulnerability Facts

q_dev_vuln_backdoor_02_secp7.question.fex

Question 44: ✔ Correct

How many concurrent connections does NAT support?

- 90
- 300
- Unlimited
- ➡ 5,000

EXPLANATION

NAT supports a limit of 5,000 concurrent connections.

REFERENCES

5.4.4 NAT Facts

q_nat_nat_03_secp7.question.fex

Question 45: ✔ Correct

Which IPSec subprotocol provides data encryption?

- AES
- SSL
- AH
- ➡ ESP

EXPLANATION

Encapsulating Security Payload (ESP) Protocol provides data encryption for IPSec traffic.

Authentication Header (AH) provides message integrity through authentication, verifying that data is received unaltered from the trusted destination. AH provides no privacy and is often combined with ESP to achieve integrity and confidentiality.

REFERENCES

5.5.7 VPN Protocol Facts

q_vpn_prot_esp_01_secp7.question.fex

Question 46: ✔ Correct

You have a company network that is connected to the internet. You want all users to have internet access, but you need to protect your private network and users. You also need to make a web server publicly available to internet users.

Which solution should you use?

- Use firewalls to create a DMZ. Place the web server and the private network inside the DMZ.
- Use a single firewall. Put the web server and the private network behind the firewall.
- ➡ Use firewalls to create a DMZ. Place the web server inside the DMZ and the private network behind the DMZ.
- Use a single firewall. Put the web server in front of the firewall and the private network behind the firewall.

EXPLANATION

A demilitarized zone (DMZ), also called a screened subnet, is a buffer network (or subnet) that sits between the private network and an untrusted network such as the internet. A common configuration uses two firewalls, one connected to the public network and one connected to the private network. Publicly-accessible resources (servers) are placed inside the screened subnet. Examples of publicly-accessible resources include web, FTP, or email servers. Private resources that are not accessible from the internet are placed behind the DMZ (behind the inner firewall).

Placing the web server inside the private network would mean opening ports in the firewall leading to the private network, which could expose other devices to attack. Placing the web server outside of the firewall would leave it unprotected.

REFERENCES

5.2.4 DMZ Facts

q_dmz_firewall_secp7.question.fex

Question 47: ✔ Correct

You want to connect your small company network to the internet. Your ISP provides you with a single IP address that is to be shared between all hosts on your private network. You do not want external hosts to be able to initiate connection to internal hosts. Which type of Network Address Translation (NAT) should you implement?

- Dynamic
- Shared
- Restricted
- Static

EXPLANATION

Use dynamic NAT to share public addresses with multiple private hosts. Dynamic NAT allows private hosts to access the internet but does not allow internet hosts to initiate contact with private hosts.

REFERENCES

5.4.4 NAT Facts

q_nat_dynamic_secp7.question.fex

Question 48: ✔ Correct

You are configuring web threat protection on the network and want to block emails coming from a specific sender. Which of the following should be configured?

- Anti-phishing software
- Spam filter
- Virus scanner
- Encryption

EXPLANATION

Gateway email spam filters prevent spam emails from reaching your network, servers, and computers. Spam filters can be configured to block specific senders, emails containing threats (such as false links), and emails containing specific content. Content filtering can block users from visiting specific categories of websites.

Virus scanners identify infected content and dispose of it.

Encryption causes data, such as the content of an email, to be unintelligible except to those who have the proper key to decrypt it.

Anti-phishing software scans content to identify and dispose of phishing attempts, preventing outside attempts to access confidential information.

REFERENCES

5.6.4 Web Threat Protection Facts

q_web_threat_prot_spam_02_secp7.question.fex

Question 49: ✔ Correct

You connect your computer to a wireless network available at the local library. You find that you can access all of the websites you want on the internet except for two.

What might be causing the problem?

- A firewall is blocking ports 80 and 443.
- The router has not been configured to perform port forwarding.
- ➡ A proxy server is blocking access to the websites.
- Port triggering is redirecting traffic to the wrong IP address.

EXPLANATION

A proxy server can be configured to block internet access based on website or URL. Many schools and public networks use proxy servers to prevent access to websites with objectionable content.

Ports 80 and 443 are used by HTTP to retrieve all web content. If a firewall were blocking these ports, access would be denied to all websites. Port forwarding directs incoming connections to a host on the private network. Port triggering dynamically opens firewall ports based on applications that initiate contact from the private network.

REFERENCES

5.3.2 Firewall Facts

q_firewall_proxy_01_secp7.question.fex

Question 50: ✔ Correct

Which of the following BEST describes a honeyfile?

- A file that has been digitally signed.
- A file used to authenticate.
- ➡ A single file setup to entice and trap attackers.
- A default file in the /etc/security directory.

EXPLANATION

A honeyfile is a single file setup to entice and trap attackers and to figure out what they're trying to do.

A token is a device or a file used to authenticate.

A honeyfile could be placed in the /etc/security directory. The file would not be a default file in the directory.

A digitally signed file is like putting a lock on the document.

REFERENCES

5.1.5 Security Solution Facts

q_sec_sol_honey_files_secp7.question.fex