Section Quiz

Candidate: Dunkan Gibson (dunkan.gibson)
Date: 2/24/2022 8:01:44 pm • Time spent: 00:18

Score: 0% Passing Score: 80%

Question 1: ✕ Incorrect

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

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

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 2: ✕ Incorrect

You are the network administrator for a city library. Throughout the library are several groups of computers that provide public access to the internet. Supervision of these computers has been difficult. You've had problems with patrons bringing personal laptops into the library and disconnecting the network cables from the library computers to connect their laptops to the internet.

The library computers are in groups of four. Each group of four computers is connected to a hub that is connected to the library network through an access port on a switch. You want to restrict access to the network so that only library computers are permitted connectivity to the internet.

What can you do?

- Remove the hub and place each library computer on its own access port.
- ➡ Configure port security on the switch.
- Create static MAC addresses for each computer and associate each address with a VLAN.
- Create a VLAN for each group of four computers.

EXPLANATION

Configuring port security on the switch can restrict access so that only specific MAC addresses can connect to the configured switch port. This would prevent the laptop computers from being permitted connectivity.

Placing each library computer on its own access port would have no effect.

VLANs are used to group broadcast traffic and do not restrict connectivity of devices as needed in this scenario.

REFERENCES

5.11.3 Switch Security Facts

q_sec_swi_port_sec_02_secp7.question.fex

Question 3: ✕ Incorrect

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?

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

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 4: ✕ Incorrect

When configuring VLANs on a switch, which type of switch ports are members of all VLANs defined on the switch?

- ➡ Trunk ports
- Gigabit and higher Ethernet ports
- Each port can only be a member of a single VLAN
- Any port not assigned to a VLAN
- Uplink ports

EXPLANATION

A trunk port is a member of all VLANs defined on a switch and carries traffic between the switches. When trunking is used, frames that are sent over a trunk port are tagged by the first switch with the VLAN ID so that the receiving switch knows to which VLAN the frame belongs. Typically, uplink ports (which are faster than the other switch ports) are used for trunk ports, although any port can be designated as a trunk port.

On an unconfigured switch, ports are members of a default VLAN (often designated VLAN 1). When you remove the VLAN membership of a port, it is reassigned back to the default VLAN. Therefore, the port is always a member of at least one VLAN.

REFERENCES

5.11.3 Switch Security Facts

q_sec_swi_vlan_01_secp7.question.fex

Question 5: ✕ Incorrect

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

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

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 6: ✕ Incorrect

Which of the following switch attacks associates the attacker's MAC address with the IP address of the victim's devices?

- ➡ ARP spoofing/poisoning
- MAC spoofing
- DNS poisoning
- Cross-site scripting (XSS)

EXPLANATION

ARP spoofing/poisoning associates the attacker's MAC address with the IP address of the victim.

MAC spoofing is changing the source MAC address on frames sent by the attacker.

DNS poisoning occurs when a name server receives malicious or misleading data that incorrectly maps host names and IP addresses.

Cross-site scripting (XSS) attacks are a type of injection attack where malicious code is saved onto an otherwise benign site.

REFERENCES

5.11.7 Switch Attack Facts

q_swi_attack_arp_poison_secp7.question.fex

Question 7: ✕ Incorrect

Drag each description on the left to the appropriate switch attack type on the right.

ARP spoofing/poisoning

Dynamic Trunking Protocol

MAC flooding

MAC spoofing

The source device sends frames to the attacker's MAC address instead of to the correct device.

Should be disabled on the switch's end user (access) ports before implementing the switch configuration into the network.

Causes packets to fill up the forwarding table and consumes so much of the switch's memory that it enters a state called Fail Open Mode.

Can be used to hide the identity of the attacker's computer or impersonate another device on the network.

EXPLANATION

Common attacks that are perpetrated against switches are MAC flooding, ARP spoofing/poisoning, and MAC spoofing.

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 a different source MAC address.
- 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 into 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.
- The attacker captures all the traffic with a protocol analyzer/sniffer.

ARP spoofing/poisoning associates the attacker's MAC address with the IP address of victim devices.

- When computers send an ARP request for the MAC address of a known IP address, the attacker's system responds with its own MAC address.
- The source device sends frames to the attacker's MAC address instead of to the correct device.
- Switches are indirectly involved in the attack because they do not verify the MAC address/IP address association.

MAC spoofing changes the source MAC address on frames sent by the attacker.

- MAC spoofing is typically used to bypass 802.1x port-based security.
- MAC spoofing can be used to bypass wireless MAC filtering.
- MAC spoofing can be used to hide the identity of the attacker's computer or to impersonate another device on the network.

Dynamic Trunking Protocol (DTP) switches have the ability to automatically detect trunk ports and negotiate the trunking protocol used between devices. DTP is not secure and allows unauthorized devices to possibly modify configuration information. You should disable the DTP services on the switch's end user (access) ports before implementing the switch configuration into the network.

REFERENCES


5.11.7 Switch Attack Facts

q_swi_attack_l2_attack_secp7.question.fex

Question 8: ✕ Incorrect

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

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

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 9: ✕ Incorrect

Which of the following is a typical goal of MAC spoofing?

- Cause a switch to enter fail open mode
- Bypass 802.1x port-based security
- Reroute local switch traffic to a specified destination
- Cause incoming packets to broadcast to all ports

EXPLANATION

MAC spoofing is changing the source MAC address on frames sent by the attacker. It is typically used to bypass 802.1x port-based security, to bypass wireless MAC filtering or hide the identity of the attacker's computer.

MAC flooding causes a switch to enter fail open mode, which causes incoming packets to be broadcast out to all ports. ARP spoofing/poisoning associates the attacker's MAC address with the IP address of the victim.

REFERENCES

5.11.7 Switch Attack Facts

q_swi_attack_mac_spoof_secp7.question.fex

Question 10: ✕ Incorrect

Which protocol should you disable on the user access ports of a switch?

- TCP
- PPTP
- DTP
- IPsec

EXPLANATION

Switches have the ability to automatically detect ports that are trunk ports and to negotiate the trunking protocol used between devices. DTP is not secure and allows unauthorized devices to possibly modify configuration information. You should disable DTP services on the switch's end user (access) ports.

REFERENCES

5.11.7 Switch Attack Facts

q_swi_attack_port_sec_secp7.question.fex