Exam Report: 6.4.3 Practice Questions

Date: 1/21/2020 4:24:59 pm
Time Spent: 1:24

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 80%

Passing Score: 80%

View results by: ○ Objective Analysis ● Individual Responses

Individual Responses

Question 1: Correct

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

○ ARP poisoning

○ MAC spoofing

➡ ◉ MAC flooding

○ Replay

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 *failopen mode*, in which all incoming packets are broadcast out 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 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

LabSim for Security Pro, Section 6.4.
[All Questions SecPro2017_v6.exm SWITCH_ATTACKS_01]

Question 2: Incorrect

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

◉ ~~MAC spoofing~~

○ Cross-site scripting

○ DNS poisoning

➡ ○ ARP spoofing/poisoning

Explanation

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

References

LabSim for Security Pro, Section 6.4.
[All Questions SecPro2017_v6.exm SWITCH_ATTACKS_02]

Question 3: Correct

Which is a typical goal of MAC spoofing?

- ○ Causing a switch to enter fail open mode
- ○ Causing incoming packets to broadcast to all ports
- ➡ ● Bypassing 802.1x port-based security
- ○ Rerouting local switch traffic to a specified destination

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, 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

LabSim for Security Pro, Section 6.4.
[All Questions SecPro2017_v6.exm SWITCH_ATTACKS_03]

Question 4: Correct

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

- ○ PPTP
- ○ IPsec
- ○ TCP
- ➡ ● DTP

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 the DTP services on the switch's end user (access) ports.

References

LabSim for Security Pro, Section 6.4.
[All Questions SecPro2017_v6.exm SWITCH_ATTACKS_04]

Question 5: Correct

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

ARP Spoofing/Poisoning

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

Dynamic Trunking Protocol

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

MAC Flooding

✓ 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.

MAC Spoofing

✓ 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:

MAC Flooding overloads the switch's MAC forwarding table to make the switch function like a hub. MAC flooding is performed using the following method:

- 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, in which all incoming packets are broadcast out 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 MAC address.
- The source device sends frames to the attacker's MAC address instead of the correct device.
- Switches are indirectly involved in the attack because they do not verify the MAC address/IP address association.

MAC Spoofing is changing 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

LabSim for Security Pro, Section 6.4.
[All Questions SecPro2017_v6.exm SWITCH_ATTACKS_05]