Layer 2 Concerns and Solutions Overview

1. Which switch security feature restricts port access based on a digital certificate or username and password? ?

A. Port security
B. PVLANs
C. SPAN
D. 802.1x

Answers

1.

- ☑ **D.** 802.1x restricts port access based on a digital certificate or username and password.
- ☒ **A** restricts MAC addresses connected to an interface and can disable ports where unauthorized access occurs. **B** sets layer 2 restrictions concerning what ports can interconnect to other ports in the same VLAN/subnet. **C** copies packets to a port connected to an IDS or protocol analyzer to examine traffic.

CAM Table Overflow and MAC Spoofing Attacks

2. What dsniff tool can be used by an attacker to fill up a switch's CAM table with spoofed MAC addresses? ?

A. macos
B. macif
C. macof
D. dtool

3. Which of the following are default configurations for a port configured with port security? ?

A. 1 MAC address, shutdown violation mode
B. 2 MAC addresses, restrict mode
C. 132 MAC addresses, shutdown mode
D. 1 MAC address, protect mode

4. Which port security learning mode learns the MAC addresses associated with an interface and places these as entries in the running-config? ?

A. Dynamic
B. Sticky
C. Learning
D. DTP

5. You need to set up the port security feature to limit the number of MAC addresses to one, where the port is disabled if there is an invalid MAC address connected to the interface. The interface is fa0/1, where sticky learning should be employed. The interface is an access port and associated with VLAN 10. Enter the commands to accomplish this. ?

Answers

2.

- ☑ **C.** The macof tool is used by an attacker to fill up a switch's CAM table so

that the switch can no longer perform its learning function to add new MAC addresses to the CAM table.
- ☒ **A**, **B**, and **D** are nonexistent tools.

3.
- ☑ **A.** The default configuration for a port configured with port security is to allow one MAC address, where the violation mode is shutdown.
- ☒ **B** and **C** have the wrong number of MAC addresses. **D** has the wrong violation mode.

4.
- ☑ **B.** The sticky learning mode learns the MAC addresses associated with an interface and places these as entries in the running-config.
- ☒ **A** doesn't place the MAC addresses in the running-config. **C** is an invalid mode. **D** is used on trunk connections.

5.
- ☑ Here is the correct configuration:
-
- `switch(config)# interface fastethernet0/1`
- `switch(config-if)# switchport mode access`
- `switch(config-if)# switchport access vlan 10`
- `switch(config-if)# switchport port-security`
- `switch(config-if)# switchport port-security maximum 1`
- `switch(config-if)# switchport port-security violation shutdown`
- `switch(config-if)# switchport port-security mac-address sticky`

VLAN Attacks

6. Which of the following are recommendations to prevent a trunk spoofing attack that would allow an attacker to hop VLANs? (Choose two.) ?

A. Disable DTP.
B. Disable STP.
C. Set the native VLAN to 1.
D. Set the native VLAN to an unused VLAN.

Answers

6.
- ☑ **A** and **D.** To prevent a trunk spoofing attack that would allow an attacker to hop VLANs, disable DTP and set the native VLAN to an unused VLAN.
- ☒ **B** has nothing to do with VLAN hopping. **C** should be an unused VLAN and not VLAN 1.

Spanning Tree Protocol Attacks

7. Which switch security feature will disable a port configured for PortFast if a BPDU is received on it? ?

A. Root Guard
B. STP Guard

C. BPDU Guard
D. VLAN Guard

Answers

7.
- ☑ **C.** BPDU Guard will disable a port configured for PortFast if a BPDU is received on it.
- ☒ **A** prevents the election of a root switch off a port configured with this security feature. **B** and **D** are nonexistent Guard features.

Flood Attacks

8. The storm control feature controls packet storms of what packet types? ?

A. Broadcasts
B. Broadcasts and multicasts
C. Broadcasts, multicasts, and unicasts

Answers

8.
- ☑ **C.** The storm control feature controls packet storms involving broadcasts, multicasts, and unicast packets.
- ☒ **A** and **B** don't specify all the valid answers.

Unauthorized Access

9. What device in 802.1x is being authenticated? ?

A. Wireless
B. PC
C. Supplicant
D. Server

10. At what layer of the OSI Reference Model does EAP function? ?

A. Physical
B. Data link
C. Network
D. Application

Answers

9.
- ☑ **C.** A supplicant is an 802.1x device that is authenticated by the authenticator.
- ☒ **A**, **B**, and **D** are examples of supplicants.

10.
- ☑ **B.** EAP and 802.1x function at the data-link layer of the OSI Reference Model.
- ☒ Because EAP and 802.1x function at the data-link layer, answers **A**, **C**, and **D** are incorrect.