[Updated Constantly]

HERE

CCNP SWITCH Chapter 10 Exam Answers (Version 7) – Score 100%

How to find: Press “Ctrl + F” in the browser and fill in whatever wording is in the question to find that question/answer.

NOTE: If you have the new question on this test, please comment Question and Multiple-Choice list in form below this article. We will update answers for you in the shortest time. Thank you! We truly value your contribution to the website.

1. **Which statement describes the purpose of the configuration that is shown?**

```
Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan 3
Switch(configif)#ip dhcp snooping trust
Switch(configif)#ip dhcp snooping limit rate 30
```

   - It is meant to disable any host that is configured to be in VLAN 3.
   - It is meant to disable any rogue DHCP servers that are attached to VLAN 3.
   - **It is meant to monitor VLAN 3 for DHCP attacks that will deplete the DHCP pool.***
   - It is meant to monitor VLAN 3 and disable any hosts that are using static IP addresses rather than DHCP addresses.

2. **What IOS feature is executed with the *traceroute mac* command?**
   - **Layer 2 traceroute***
   - MAC port security
   - Embedded Event Manager
   - Switched Port Analyzer

3. **Which countermeasure can be implemented to determine the validity of an ARP packet, based on the valid MACaddresstoIP address bindings stored in a DHCP snooping database?**
   - DHCP spoofing
   - **dynamic ARP inspection***
   - CAM table inspection
   - MAC snooping

4. **A network administrator is tasked with protecting a server farm by implementing private VLANs. Each server should only be allowed to communicate with the default gateway. Which type of pVLAN should be configured on the switch port that connects to a server?**
   - **isolated***
   - promiscuous
   - community
   - secondary VLAN
5. **What can be used to mitigate MAC table flooding attacks?**
   - DHCP snooping
   - private VLANs
   - **port security***
   - root guard
6. **How does MAC address flooding cause a vulnerability in the network?**
   - **The CAM table will be full, causing legitimate frames to be forwarded out all ports within the VLAN and allowing unauthorized users to capture data.***
   - An attacking device can send or receive packets on various VLANs and bypass Layer 3 security measures.
   - An attacking device can exhaust the address space available to the DHCP servers for a period of time or establish itself as a DHCP server in maninthemiddle attacks.
   - Information that is sent through CDP is transmitted in clear text and is unauthenticated, allowing it to be captured and to divulge network topology information.
7. **Which type of output would be produced on a switch after entering the command, Switch# show ip dhcp snooping binding?**
   - **DHCP servers on the snooped network***
   - DHCP clients on all DHCP snooped switches on the network
   - DHCP clients that are connected to DHCP snooped ports on the switch
   - all active protocols on all DHCP clients that are connected to DHCP snooped ports on the switch
8. **What are two purposes for an attacker launching a MAC table flood? (Choose two.)**
   - to initiate a maninthemiddle attack
   - **to initiate a denial of service (DoS) attack***
   - **to capture data from the network***
   - to gather network topology information
   - to exhaust the address space available to the DHCP
9. **How does VLAN hopping cause a vulnerability in the network?**

- The CAM table will be full, causing legitimate frames to be forwarded out all ports and allowing unauthorized users to capture data.
- **An attacking device can send or receive packets on various VLANs and bypass Layer 3 security measures.***
- An attacking device can exhaust the address space available to the DHCP servers for a period of time or establish itself as a DHCP server in maninthemiddle attacks.
- Information sent through CDP is transmitted in clear text and is unauthenticated, allowing it to be captured and to divulge network topology information.

10. **What *switchport portsecurity* keyword causes MAC addresses to be added to the running configuration?**
    - aging
    - **mac-address sticky***
    - maximum
    - violation
11. **In which location or situation is a private VLAN appropriate?**
    - a DMZ segment
    - ISP SOHO connections
    - **a web hosting environment at an ISP***
    - two recently merged companies that have overlapping IP addressing schemes
12. **A network administrator is tasked with protecting a server farm by implementing private VLANs (PVLANs). A server is only allowed to communicate with its default gateway and other related servers. Which type of PVLAN should be configured on the switch ports that connect to the servers?**
    - isolated
    - promiscuous
    - secondary VLAN
    - **community***
13. **Which statement best describes how traffic is handled between different port types within a primary pVLAN?**
    - The traffic is forwarded from promiscuous ports to promiscuous ports in the same primary VLAN.
    - The traffic is forwarded from promiscuous ports to community and promiscuous ports in the same primary VLAN.
    - The traffic is forwarded from promiscuous ports to isolated and community ports in the same primary VLAN.

- **The traffic is forwarded from promiscuous ports to isolated, community, and other promiscuous ports in the same primary VLAN.***

14. **What is one way to mitigate spanningtree compromises?**
    - **Statically configure the primary and backup root bridge.***
    - Implement private VLANs.
    - Place all unused ports into a common VLAN (not VLAN 1).
    - Configure MAC address VLAN access maps.
15. **How should unused ports on a switch be configured in order to prevent VLAN hopping attacks?**
    - Configure them with the UDLD feature.
    - Configure them with the PAgP protocol.
    - Configure them as trunk ports for the native VLAN 1.
    - **Configure them as access ports and associate them with an unused VLAN.***
16. **What technology can be used to help mitigate MAC address flooding attacks?**
    - root guard
    - Private VLANs
    - DHCP snooping
    - **VLAN access maps***
    - Dynamic ARP Inspection
17. **Which configuration guideline applies to using the capture option in VACL?**
    - Capture ports transmit traffic that belongs to all VLANs.
    - The capture port captures all packets that are received on the port.
    - The switch has a restriction on the number of capture ports.
    - **The capture port needs to be in the spanningtree forwarding state for the VLAN.***
18. **All access ports on a switch are configured with the administrative mode of dynamic auto. An attacker, connected to one of the ports, sends a malicious DTP frame. What is the intent of the attacker?**
    - **VLAN hopping***
    - DHCP spoofing attack
    - MAC flooding attack
    - ARP poisoning attack
19. **Refer to the exhibit. After the configuration has been applied to ACSw22, frames that are bound for the node on port FastEthernet 0/1 are periodically being dropped. What**

should be done to correct the issue?

```
ACSw22(config)# interface FastEthernet 0/1
ACSw22(config-if)# switchport
ACSw22(config-if)# switchport mode access
ACSw22(config-if)# switchport access vlan 103
ACSw22(config-if)# switchport block unicast
ACSw22(config-if)# speed 100
ACSw22(config-if)# duplex full
ACSw22(config-if)# end
ACSw22# copy running-config startup-config
```

- **Add the *switchport portsecurity mac-address sticky* command to the interface configuration.***
- Change the port speed to speed auto with the interface configuration mode.
- Use the switchport mode trunk command in the interface configuration.
- Remove the switchport command from the interface configuration.

20. **What is one way to mitigate ARP spoofing?**

- **Enable dynamic ARP inspection.***
- Configure MAC address VLAN access maps.
- Enable root guard.
- Implement private VLANs.