CCNA Security v2.0 Chapter 6 Exam Answers

itexamanswers.net/ccna-security-v2-0-chapter-6-exam-answers.html

February 9, 2016

How to find: Press **"Ctrl + F"** in the browser and fill in whatever wording is in the question to find that question/answer. If the question is not here, find it in **Questions Bank**.

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 type of VLAN-hopping attack may be prevented by designating an unused VLAN as the native VLAN?

- DTP spoofing
- DHCP spoofing
- **VLAN double-tagging***
- DHCP starvation

Spoofing DTP messages forces a switch into trunking mode as part of a VLAN-hopping attack, but VLAN double tagging works even if trunk ports are disabled. Changing the native VLAN from the default to an unused VLAN reduces the possibility of this type of attack. DHCP spoofing and DHCP starvation exploit vulnerabilities in the DHCP message exchange.

2. What component of Cisco NAC is responsible for performing deep inspection of device security profiles?

- Cisco NAC Profiler
- **Cisco NAC Agent***
- Cisco NAC Manager
- Cisco NAC Server

The Cisco NAC Agent is a lightweight agent that runs on endpoint devices. The function of this agent is to perform deep inspection of the security profile of the endpoints. This includes inspecting the registry settings, services, and files.

3. Which three functions are provided under Cisco NAC framework solution? (Choose three.)

- VPN connection
- **AAA services***

- intrusion prevention
- **scanning for policy compliance***
- secure connection to servers
- **remediation for noncompliant devices***

The goal of both the Cisco NAC framework and the Cisco NAC Appliance is to ensure that only hosts that are authenticated and have their security posture examined and approved are permitted onto the network. They provide four important functions: authentication, authorization, and accounting; posture assessment (evaluating an incoming device against the security policies), quarantining of non-compliant systems, and remediation of noncompliant devices. They do not provide VPN connection or intrusion detection/prevention services.

4. Which feature is part of the Antimalware Protection security solution?

- **file retrospection***
- user authentication and authorization
- data loss prevention
- spam blocking

The Antimalware Protection (AMP) security solution can enable malware detection and blocking, continuous analysis, and retrospective alerting with the following:
File reputation – analysis of files inline and blocking or applying policies
File sandboxing – analysis of unknown files to understand true file behavior
File retrospection – continuing to analyze files for changing threat levels

5. What protocol should be disabled to help mitigate VLAN hopping attacks?

- STP
- ARP
- CDP
- **DTP***

Mitigating a VLAN hopping attack can be done by disabling Dynamic Trunking Protocol (DTP) and by setting the native VLAN of trunk links to a VLAN not in use.

6. What network attack seeks to create a DoS for clients by preventing them from being able to obtain a DHCP lease?

- DHCP spoofing
- CAM table attack
- IP address spoofing
- **DHCP starvation***

DCHP starvation attacks are launched by an attacker with the intent to create a DoS for DHCP clients. To accomplish this goal, the attacker uses a tool that sends many DHCPDISCOVER messages in order to lease the entire pool of available IP addresses, thus denying them to legitimate hosts.

7. What is the only type of port that an isolated port can forward traffic to on a private VLAN?

- a community port
- **a promiscuous port***
- another isolated port
- any access port in the same PVLAN

PVLANs are used to provide Layer 2 isolation between ports within the same broadcast domain. The level of isolation can be specified
with three types of PVLAN ports:
Promiscuous ports that can forward traffic to all other ports
Isolated ports that can only forward traffic to promiscuous ports
Community ports that can forward traffic to other community ports and promiscuous ports

8. What security countermeasure is effective for preventing CAM table overflow attacks?

- DHCP snooping
- Dynamic ARP Inspection
- IP source guard
- **port security***

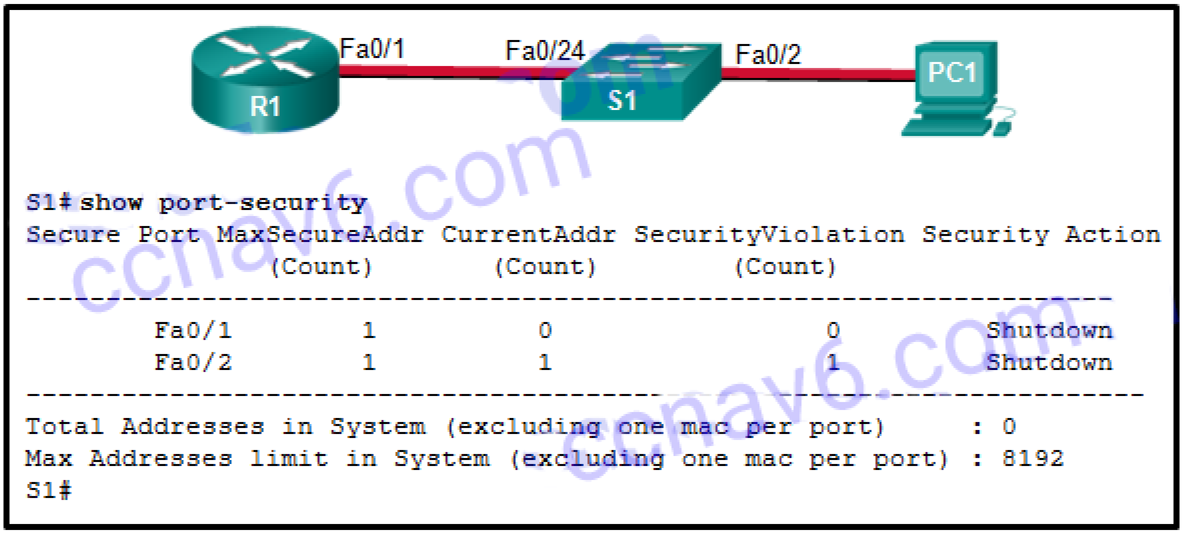
Port security is the most effective method for preventing CAM table overflow attacks. Port security gives an administrator the ability to manually specify what MAC addresses should be seen on given switch ports. It provides a method for limiting the number of MAC addresses that can be dynamically learned over a switch port.

9. In what situation would a network administrator most likely implement root guard?

- on all switch ports (used or unused)
- on all switch ports that connect to a Layer 3 device
- on all switch ports that connect to host devices
- on all switch ports that connect to another switch
- **on all switch ports that connect to another switch that is not the root bridge***

Root guard in conjunction with PortFast, and BPDU guard is used to prevent an STP manipulation attack.

10. Refer to the exhibit. The Fa0/2 interface on switch S1 has been configured with the switchport port-security mac-address 0023.189d.6456 command and a workstation has been connected. What could be the reason that the Fa0/2 interface is shutdown?



```
S1#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)          (Count)
--------------------------------------------------------------------
        Fa0/1        1          0                 0          Shutdown
        Fa0/2        1          1                 1          Shutdown
----------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 8192
S1#
```

- The connection between S1 and PC1 is via a crossover cable.
- The Fa0/24 interface of S1 is configured with the same MAC address as the Fa0/2 interface.
- S1 has been configured with a switchport port-security aging command.
- **The MAC address of PC1 that connects to the Fa0/2 interface is not the configured MAC address.***

The security violation counter for Fa0/2 has been incremented (evidenced by the 1 in the SecurityViolation column). The most secure addresses allowed on port Fa0/2 is 1 and that address was manually entered. Therefore, PC1 must have a different MAC address than the one configured for port Fa0/2. Connections between end devices and the switch, as well as connections between a router and a switch, are made with a straight-through cable.

11. Two devices that are connected to the same switch need to be totally isolated from one another. Which Cisco switch security feature will provide this isolation?

- **PVLAN Edge***
- DTP
- SPAN
- BPDU guard

The PVLAN Edge feature does not allow one device to see traffic that is generated by another device. Ports configured with the PVLAN Edge feature are also known as protected ports. BPDU guard prevents unauthorized connectivity to a wired Layer 2 switch. SPAN is port mirroring to capture data from one port or VLAN and send that data to another port. DTP (Dynamic Trunking Protocol) is automatically enabled on some switch models to create a trunk if the attached device is configured for trunking. Cisco recommends disabling DTP as a best practice.

12. Which two functions are provided by Network Admission Control? (Choose two.)

- protecting a switch from MAC address table overflow attacks
- **enforcing network security policy for hosts that connect to the network***
- **ensuring that only authenticated hosts can access the network***
- stopping excessive broadcasts from disrupting network traffic
- limiting the number of MAC addresses that can be learned on a single switch port

The port security feature can be used to limit how many MAC addresses can be learned on a switch port and help prevent MAC address table overflow attacks. Storm control is a feature that can prevent excessive broadcasts and multicasts from disrupting other LAN traffic. These functions are not provided by Network Admission Control (NAC).

13. Which spanning-tree enhancement prevents the spanning-tree topology from changing by blocking a port that receives a superior BPDU?

- BDPU filter
- PortFast
- BPDU guard
- **root guard***

Root guard prevents the placement of the root bridge from changing by blocking any port that receives a superior BPDU. A superior BPDU is one with a higher root bridge ID than the currently selected root bridge has.

14. What is the role of the Cisco NAC Manager in implementing a secure networking infrastructure?

- **to define role-based user access and endpoint security policies***
- to assess and enforce security policy compliance in the NAC environment
- to perform deep inspection of device security profiles
- to provide post-connection monitoring of all endpoint devices

Cisco NAC authenticates users and assess the policy compliance of the device the user is using to connect to the network. The role of the Cisco NAC Manager is to define the security policies of user access and endpoint security policies.

15. What is the role of the Cisco NAC Server within the Cisco Secure Borderless Network Architecture?

- providing the ability for company employees to create guest accounts
- providing post-connection monitoring of all endpoint devices
- defining role-based user access and endpoint security policies
- **assessing and enforcing security policy compliance in the NAC environment***

Cisco NAC is used in the Cisco Borderless Network Architecture to authenticate users and ensure user devices are compliant with security policies. The Cisco NAC server assesses and enforces security policy compliance.

16. What is the role of the Cisco NAC Guest Server within the Cisco Borderless Network architecture?

- It defines role-based user access and endpoint security policies.
- **It provides the ability for creation and reporting of guest accounts.***
- It provides post-connection monitoring of all endpoint devices.
- It performs deep inspection of device security profiles.

Cisco NAC is used in the Cisco Borderless Network Architecture to authenticate users and ensure that user devices are compliant with security policies. The Cisco NAC Guest Server manages guest network access and the ability to create guest accounts.

17. Which security feature should be enabled in order to prevent an attacker from overflowing the MAC address table of a switch?

- root guard
- **port security***
- storm control
- BPDU filter

Port security limits the number of source MAC addresses allowed through a switch port. This feature can prevent an attacker from flooding a switch with many spoofed MAC addresses.

18. What is the behavior of a switch as a result of a successful CAM table attack?

- **The switch will forward all received frames to all other ports.***
- The switch will drop all received frames.
- The switch interfaces will transition to the error-disabled state.

- The switch will shut down.

As a result of a CAM table attack, a switch can run out of memory resources to store MAC addresses. When this happens, no new MAC addresses can be added to the CAM table and the switch will forward all received frames to all other ports. This would allow an attacker to capture all traffic that is flooded by the switch.

19. What additional security measure must be enabled along with IP Source Guard to protect against address spoofing?

- port security
- BPDU Guard
- root guard
- **DHCP snooping***

Like Dynamic ARP Inspection (DAI), IP Source Guard (IPSG) needs to determine the validity of MAC-address-to-IP-address bindings. To do this IPSG uses the bindings database built by DHCP snooping.

20. Which mitigation technique would prevent rogue servers from providing false IP configuration parameters to clients?

- **turning on DHCP snooping***
- implementing port security
- implementing port-security on edge ports
- disabling CDP on edge ports

When DHCP snooping is enabled, a switch will deny packets containing unauthorized DHCP server messages coming from an untrusted port.

21. What are three techniques for mitigating VLAN hopping attacks? (Choose three.)

- **Set the native VLAN to an unused VLAN.***
- **Disable DTP.***
- Enable Source Guard.
- **Enable trunking manually.***
- Enable BPDU guard.
- Use private VLANs.

Mitigating a VLAN hopping attack can be done by disabling Dynamic Trunking Protocol (DTP), manually setting ports to trunking mode, and by setting the native VLAN of trunk links to VLANs not in use.

22. What two mechanisms are used by Dynamic ARP inspection to validate ARP packets for IP addresses that are dynamically assigned or IP addresses that are static? (Choose two.)

- **MAC-address-to-IP-address bindings***
- RARP
- **ARP ACLs***
- IP ACLs
- Source Guard

Two methods can be used by Dynamic ARP Inspection (DAI) to determine the validity of MAC-address-to-IP-address bindings. One is a bindings database built by DHCP snooping. The other method is through the use of user-configured ARP ACLs.

23. Which STP stability mechanism is used to prevent a rogue switch from becoming the root switch?

- Source Guard
- BPDU guard
- **root guard***
- loop guard

24. How can a user connect to the Cisco Cloud Web Security service directly?

- through the connector that is integrated into any Layer 2 Cisco switch
- **by using a proxy autoconfiguration file in the end device***
- by accessing a Cisco CWS server before visiting the destination web site
- by establishing a VPN connection with the Cisco CWS

A client can connect to the Cisco CWS service directly by using a proxy autoconfiguration (PAC) file installed on the end device. The Cisco CWS connector is a software component integrated into four Cisco products including Cisco ASA, Cisco WSA, and Cisco AnyConnect Secure Mobility Client. A client can use the Cisco CWS service through these products.

25. What security benefit is gained from enabling BPDU guard on PortFast enabled interfaces?

- enforcing the placement of root bridges
- preventing buffer overflow attacks
- **preventing rogue switches from being added to the network***
- protecting against Layer 2 loops

BPDU guard immediately error-disables a port that receives a BPDU. This prevents rogue switches from being added to the network. BPDU guard should only be applied to all end-user ports.

26. Fill in the blank.
DHCP **snooping** is a mitigation technique to prevent rogue DHCP servers from providing false IP configuration parameters.

Download PDF File below:

[sociallocker id=”54558″]

ITexamanswers.net – CCNA Security v2.0 Chapter 6 Exam Answers.pdf
859.49 KB 1870 downloads

…

Download

[/sociallocker]