Vendor: Cisco

Exam Code: 640-554

Exam Name: Implementing Cisco IOS Network Security (IINS v2.0)

Version: DEMO

QUESTION 1
Which statement describes a best practice when configuring trunking on a switch port?

A. Disable double tagging by enabling DTP on the trunk port.
B. Enable encryption on the trunk port.
C. Enable authentication and encryption on the trunk port.
D. Limit the allowed VLAN(s) on the trunk to the native VLAN only.
E. Configure an unused VLAN as the native VLAN.

Answer: E
Explanation:
Double Encapsulation Attack
When double-encapsulated 802.1Q packets are injected into the network from a device whose VLAN happens to be the native VLAN of a trunk, the VLAN identification of those packets cannot be preserved from end to end since the 802.1Q trunk would always modify the packets by stripping their outer tag. After the external tag is removed, the internal tag permanently becomes the packet's only VLAN identifier. Therefore, by double encapsulating packets with two different tags, traffic can be made to hop across VLANs.
This scenario is to be considered a misconfiguration, since the 802.1Q standard does not necessarily force the users to use the native VLAN in these cases. As a matter of fact, the proper configuration that should always be used is to clear the native VLAN from all 802.1Q trunks (alternatively, setting them to 802.1q-all-tagged mode achieves the exact same result). In cases where the native VLAN cannot be cleared, then always pick an unused VLAN as native VLAN of all the trunks; don't use this VLAN for any other purpose. Protocols like STP, DTP, and UDLD (check out [3]) should be the only rightful users of the native VLAN and their traffic should be completely isolated from any data packets.

http://www.cisco.com/en/US/products/hw/switches/ps708/products_white_paper09186a008013159f.shtml

QUESTION 2
Which type of Layer 2 attack causes a switch to flood all incoming traffic to all ports?

A. MAC spoofing attack
B. CAM overflow attack
C. VLAN hopping attack
D. STP attack

Answer: B
Explanation:
Summary
The MAC Address Overflow attack is effective if the proper mitigation techniques are not in place on the Cisco Catalyst 6500 series switch. By using publicly (free) and available Layer 2 attack tools found on the Internet, anyone who understands how to setup and run these tools could potentially launch an attack on your network.
MAC address monitoring is a feature present on Cisco Catalyst 6500 Series switches. This feature helps mitigate MAC address flooding and other CAM overflow attacks by limiting the total number of MAC addresses learned by the switch on per-port or per-VLAN basis. With MAC Address Monitoring, a maximum threshold for the total number of MAC addresses can be configured and enforced on a per-port and/or per-VLAN basis.
MAC address monitoring in Cisco IOS Software allows the definition of a single upper (maximum) threshold. In addition, the number of MAC addresses learned can only be monitored on a per-port or per-VLAN basis, and not a per-port-per-VLAN. By default, MAC address monitoring is disabled

in Cisco IOS Software. However, the maximum threshold for all ports and VLANs is configured to 500 MAC address entries, and when the threshold is exceeded the system is set to generate a system message along with a syslog trap. These default values take effect only when MAC address monitoring is enabled. The system can be configured to notify or disable the port or VLAN every time the number of learned MAC addresses exceeds the predefined threshold. In our test, we used the "mac-address-table limit" command on the access layer port interface to configure the MAC address monitoring feature.

http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps708/white_paper_c11_603836.html

QUESTION 3
What is the best way to prevent a VLAN hopping attack?

A. Encapsulate trunk ports with IEEE 802.1Q.
B. Physically secure data closets.
C. Disable DTP negotiations.
D. Enable BDPU guard.

Answer: C
Explanation:
802.1Q and ISL Tagging Attack
Tagging attacks are malicious schemes that allow a user on a VLAN to get unauthorized access to another VLAN. For example, if a switch port were configured as DTP auto and were to receive a fake DTP packet, it might become a trunk port and it might start accepting traffic destined for any VLAN. Therefore, a malicious user could start communicating with other VLANs through that compromised port.
Sometimes, even when simply receiving regular packets, a switch port may behave like a full-fledged trunk port (for example, accept packets for VLANs different from the native), even if it is not supposed to. This is commonly referred to as "VLAN leaking" (see [5] for a report on a similar issue).

http://www.cisco.com/en/US/products/hw/switches/ps708/products_white_paper09186a008013159f.shtml

QUESTION 4
Which statement about PVLAN Edge is true?

A. PVLAN Edge can be configured to restrict the number of MAC addresses that appear on a single port.
B. The switch does not forward any traffic from one protected port to any other protected port.
C. By default, when a port policy error occurs, the switchport shuts down.
D. The switch only forwards traffic to ports within the same VLAN Edge.

Answer: B
Explanation:
Some switches (as specified in the Private VLAN Catalyst Switch Support Matrix) currently support only the PVLAN Edge feature. The term "protected ports" also refers to this feature. PVLAN Edge ports have a restriction that prevents communication with other protected ports on the same switch. Protected ports on separate switches, however, can communicate with each other. Do not confuse this feature with the normal PVLAN configurations that this document shows. For more information on protected ports, refer to the Configuring Port Security section of the document Configuring Port-Based Traffic Control.

http://www.cisco.com/en/US/docs/switches/lan/catalyst3550/software/release/12.1_13_ea1/configuration/guide/swtrafc.html

Configuring Protected Ports
Some applications require that no traffic be forwarded between ports on the same switch so that one neighbor does not see the traffic generated by another neighbor. In such an environment, the use of protected ports ensures that there is no exchange of unicast, broadcast, or multicast traffic between these ports on the switch.

Protected ports have these features:
A protected port does not forward any traffic (unicast, multicast, or broadcast) to any other port that is also a protected port. Traffic cannot be forwarded between protected ports at Layer 2; all traffic passing between protected ports must be forwarded through a Layer 3 device.
Forwarding behavior between a protected port and a nonprotected port proceeds as usual.
The default is to have no protected ports defined.

http://www.cisco.com/en/US/tech/tk389/tk814/technologies_configuration_example09186a008017acad.shtml

QUESTION 5
If you are implementing VLAN trunking, which additional configuration parameter should be added to the trunking configuration?

A. no switchport mode access
B. no switchport trunk native VLAN 1
C. switchport mode DTP
D. switchport nonnegotiate

Answer: D
Explanation:
Layer 2 LAN Port Modes
Table 17-2 lists the Layer 2 LAN port modes and describes how they function on LAN ports. switchport mode access Puts the LAN port into permanent nontrunking mode and negotiates to convert the link into a nontrunk link. The LAN port becomes a nontrunk port even if the neighboring LAN port does not agree to the change.
switchport mode dynamic desirable
Makes the LAN port actively attempt to convert the link to a trunk link. The LAN port becomes a trunk port if the neighboring LAN port is set to trunk, desirable, or auto mode. This is the default mode for all LAN ports.

switchport mode dynamic auto
Makes the LAN port willing to convert the link to a trunk link. The LAN port becomes a trunk port if the neighboring LAN port is set to trunk or desirable mode. switchport mode trunk Puts the LAN port into permanent trunking mode and negotiates to convert the link into a trunk link. The LAN port becomes a trunk port even if the neighboring port does not agree to the change.

switchport nonegotiate
Puts the LAN port into permanent trunking mode but prevents the port from generating DTP frames. You must configure the neighboring port manually as a trunk port to establish a trunk link.

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/layer2.html

QUESTION 6
Which three applications comprise Cisco Security Manager? (Choose three.)

A. Configuration Manager
B. Packet Tracer
C. Device Manager
D. Event Viewer
E. Report Manager
F. Syslog Monitor

Answer: ADE

QUESTION 7
When a network transitions from IPv4 to IPv6, how many bits does the address expand to?

A. 64 bits
B. 128 bits
C. 96 bits
D. 156 bits

Answer: B

QUESTION 8
On which Cisco Configuration Professional screen do you enable AAA?

A. AAA Summary
B. AAA Servers and Groups
C. Authentication Policies
D. Authorization Policies

Answer: A

QUESTION 9
Under which option do you create a AAA authentication policy in Cisco Configuration Professional?

A. Authentication Policies
B. Authentication Policies ?Login
C. AAA Servers and Groups
D. AAA Summary

Answer: B

QUESTION 10
Which three statements about TACACS+ are true? (Choose three.)

A. TACACS+ uses TCP port 49.
B. TACACS+ uses UDP ports 1645 and 1812.
C. TACACS+ encrypts the entire packet.

D. TACACS+ encrypts only the password in the Access-Request packet.
E. TACACS+ is a Cisco proprietary technology.
F. TACACS+ is an open standard.

Answer: ACE

QUESTION 11
Which three statements about RADIUS are true? (Choose three.)

A. RADIUS uses TCP port 49.
B. RADIUS uses UDP ports 1645 or 1812.
C. RADIUS encrypts the entire packet.
D. RADIUS encrypts only the password in the Access-Request packet.
E. RADIUS is a Cisco proprietary technology.
F. RADIUS is an open standard.

Answer: BDF

QUESTION 12
Which network security framework is used to set up access control on Cisco Appliances?

A. RADIUS
B. AAA
C. TACACS+
D. NAS

Answer: B

QUESTION 13
Which two protocols are used in a server-based AAA deployment? (Choose two.)

A. RADIUS
B. TACACS+
C. HTTPS
D. WCCP
E. HTTP

Answer: AB

QUESTION 14
Which Cisco IOS command will verify authentication between a router and a AAA server?

A. debug aaa authentication
B. test aaa group
C. test aaa accounting
D. aaa new-model

Answer: B

Thank You for Trying Our Product

Braindump2go Certification Exam Features:

★ More than 99,900 Satisfied Customers Worldwide.

★ Average 99.9% Success Rate.

★ Free Update to match latest and real exam scenarios.

★ Instant Download Access! No Setup required.

★ Questions & Answers are downloadable in PDF format and VCE test engine format.

★ Multi-Platform capabilities - Windows, Laptop, Mac, Android, iPhone, iPod, iPad.

★ 100% Guaranteed Success or 100% Money Back Guarantee.

★ Fast, helpful support 24x7.

View list of all certification exams: http://www.braindump2go.com/all-products.html

10% Discount Coupon Code: **BDNT2014**