Exam Report: 6.5.8 Practice Questions

Date: 1/21/2020 6:24:01 pm
Time Spent: 14:59

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

A virtual LAN can be created using which of the following?

- Hub
- Switch
- Gateway
- Router

Explanation

Use a switch to create virtual LANs (VLANs). The various ports on a switch can be assigned to a specific VLAN to create logically distinct networks on the same physical network topology.

Routers, gateways, and hubs are common network devices, but they do not support the creation of VLANs.

References

LabSim for Security Pro, Section 6.5.
[All Questions SecPro2017_v6.exm SWITCH_SECURITY_01]

Question 2: Incorrect

When configuring VLANs on a switch, what is used to identify which VLAN a device belongs to?

- ~~IP address~~
- MAC address
- Switch port
- Host name

Explanation

VLAN membership is configured by assigning a switch port to a VLAN. A switch can have multiple VLANs configured on it, but each switch port can only be a member of a single VLAN. All devices connected to a switch port are members of the same VLAN.

References

LabSim for Security Pro, Section 6.5.
[All Questions SecPro2017_v6.exm SWITCH_SECURITY_02]

Question 3: Incorrect

You want to increase the security of your network by allowing only authenticated users to access network devices through a switch.

Which of the following should you implement?

- IPsec
- Spanning tree
- 802.1x
- ~~Port security~~

Explanation

802.1x authentication is an authentication method used on a LAN to allow or deny access based on a port or connection to the network. 802.1x is used for port authentication on switches and authentication to wireless access points. 802.1x requires an authentication server for validating user credentials. This server is typically a RADIUS server. Authenticated users are allowed full access to the network; unauthenticated users only have access to the RADIUS server.

Port security uses the MAC address to allow or deny connections based on the MAC address of the device, not user authentication. Spanning tree is a protocol for identifying multiple paths through a switched network. IPsec is a tunneling protocol that adds encryption to packets.

References

LabSim for Security Pro, Section 6.5.
[All Questions SecPro2017_v6.exm SWITCH_SECURITY_03]

Question 4: Correct

Which of the following applications typically use 802.1x authentication? (Select two.)

- [x] Controlling access through a switch
- [ ] Controlling access through a router
- [ ] Authenticating remote access clients
- [ ] Authenticating VPN users through the Internet
- [x] Controlling access through a wireless access point

Explanation

802.1x authentication is an authentication method used on a LAN to allow or deny access based on a port or connection to the network. 802.1x is used for port authentication on switches and authentication to wireless access points. 802.1x requires an authentication server for validating user credentials. This server is typically a RADIUS server.

Remote access authentication is handled by remote access servers or a combination of remote access servers and a RADIUS server for centralized authentication. VPN connections can be controlled by remote access servers or by special devices called a VPN concentrator.

References

LabSim for Security Pro, Section 6.5.
[All Questions SecPro2017_v6.exm SWITCH_SECURITY_04]

Question 5: Correct

You manage a network that uses a single switch. All ports within your building connect through the single switch.

In the lobby of your building are three RJ-45 ports connected to the switch. You want to allow visitors to plug into these ports to gain Internet access, but they should not have access to any other devices on your private network. Employees connected throughout the rest of your building should have both private and Internet access.

Which feature should you implement?

- Port authentication

- DMZ
- NAT
- VLANs

Explanation

Use VLANs to segregate hosts based on switch ports. You could define two VLANs: one for employees connected throughout the building, and another for the ports in the lobby. The ports in the lobby would have only Internet access, while devices connected to ports in the rest of the building could communicate with other devices within the same VLAN.

Use port authentication to control access to the network based on things such as username and password. Port authentication would allow or deny access, but would not restrict access once authenticated, or provide any type of access if not authenticated.

A *demilitarized zone* (DMZ) is a buffer network (or subnet) that sits between the private network and an untrusted network (such as the Internet). Network Address Translation (NAT) modifies the IP addresses in packets as they travel from one network (such as a private network) to another (such as the Internet). NAT allows you to connect a private network to the Internet without obtaining registered addresses for every host. Hosts on the private network share the registered IP addresses.

References

LabSim for Security Pro, Section 6.5.
[All Questions SecPro2017_v6.exm SWITCH_SECURITY_05]

Question 6: Correct

When configuring VLANs on a switch, what type of switch ports are members of all VLANs defined on the switch?

- Gigabit and higher Ethernet ports
- Trunk ports
- Any port not assigned to a VLAN
- Each port can only be a member of a single VLAN
- Uplink ports

Explanation

A *trunk* port is a member of all VLANs defined on a switch, and carries traffic between the switches. When trunking is used, frames that are sent over a trunk port are tagged by the first switch with the VLAN ID so that the receiving switch knows to which VLAN the frame belongs. Typically, uplink ports (that are faster than the other switch ports) are used for trunk ports, although any port can be designated as a trunking port.

On an unconfigured switch, ports are members of a default VLAN (often designated VLAN 1). When you remove the VLAN membership of a port, it is reassigned back to the default VLAN, therefore the port is always a member of one VLAN.

References

LabSim for Security Pro, Section 6.5.
[All Questions SecPro2017_v6.exm SWITCH_SECURITY_06]

Question 7: Correct

You manage a network that uses switches. In the lobby of your building are three RJ-45 ports connected to a switch.

You want to make sure that visitors cannot plug in their computers to the free network jacks and connect to the network. However, employees who plug into those same jacks should be able to connect to the network.

What feature should you configure?

- VLANs

- Spanning tree
- Port authentication
- Bonding
- Mirroring

Explanation

Use port authentication to prevent unauthorized access through switch ports. Port authentication is provided by the 802.1x protocol, and allows only authenticated devices to connect to the LAN through the switch. Authentication uses usernames and passwords, smart cards, or other authentication methods.

- When a device first connects, the port is set to an unauthorized state. Ports in unauthorized states can only be used for 802.1x authentication traffic.
- After the server authenticates the device or the user, the switch port is placed in an authorized state, and access to other LAN devices is allowed.

With a VLAN, you assign each port to a VLAN. If the ports in the lobby were assigned to one VLAN, you could control the type of access through the switch for those ports, but could not modify the access based on user. Using a VLAN, both visitors and employees would have the same access through those ports.

Spanning tree is a protocol on a switch that allows the switch to maintain multiple paths between switches within a subnet. The spanning tree protocol runs on each switch and is used to select a single path between any two switches. *Mirroring* sends traffic from all switch ports to a switch port you designate as the mirrored port. *Bonding* allows multiple switch ports to be used at the same time to reach a specific destination.

References

LabSim for Security Pro, Section 6.5.
[All Questions SecPro2017_v6.exm SWITCH_SECURITY_07]

Question 8: Correct

Which of the following solutions would you implement to eliminate switching loops?

- Auto-duplex
- Inter-vlan routing
- CSMA/CD
- Spanning tree

Explanation

Run the spanning tree protocol to prevent switching loops. A switching loop occurs when there are multiple active paths between switches. The spanning tree protocol runs on each switch and is used to select a single path between any two switches. Switch ports that are part of that path are placed in a forwarding state. Switch ports that are part of redundant but unused paths are placed in a blocking (non-forwarding) state.

Use inter-vlan routing to enable devices in different VLANs to communicate. The auto-duplex setting allows a switch port to detect the duplex setting of connected devices (either half or full-duplex). CSMA/CD is a method for detecting and recovering from collisions.

References

LabSim for Security Pro, Section 6.5.
[All Questions SecPro2017_v6.exm SWITCH_SECURITY_08]

Question 9: Correct

You manage a single subnet with three switches. The switches are connected to provide redundant paths between the switches.

Which feature prevents switching loops and ensures there is only a single active path between any two

switches?

- Bonding
- Spanning tree
- Trunking
- PoE
- 802.1x

Explanation

Spanning tree is a protocol on a switch that allows the switch to maintain multiple paths between switches within a subnet. The spanning tree protocol runs on each switch and is used to select a single path between any two switches.

- Without the spanning tree protocol, switches that are connected together with multiple links would form a switching loop, where frames are passed back and forth continuously.
- Spanning tree provides only a single active path between switches. Switch ports that are part of that path are placed in a forwarding state.
- Switch ports that are part of redundant but unused paths are placed in a blocking (non-forwarding) state.
- When an active path goes down, the spanning tree protocol automatically recovers and activates the backup ports necessary to provide continued connection between devices.

Bonding does the opposite of spanning tree--it allows multiple switch ports to be used at the same time to reach a specific destination. 802.1x is an authentication protocol used with port security (or port authentication). Power over Ethernet (PoE) supplies power to end devices through the RJ-45 Ethernet switch port. *Trunking* identifies ports that are used to carry VLAN traffic between switches. A trunk port is a member of all VLANs defined on all switches.

References

LabSim for Security Pro, Section 6.5.
[All Questions SecPro2017_v6.exm SWITCH_SECURITY_09]

Question 10: Correct

In which of the following situations would you use port security?

- You want to control the packets sent and received by a router.
- You want to restrict the devices that could connect through a switch port.
- You want to prevent sniffing attacks on the network.
- You want to prevent MAC address spoofing.

Explanation

Use port security on a switch to restrict the devices that can connect to a switch. Port security uses the MAC address to identify allowed and denied devices. When an incoming frame is received, the switch examines the source MAC address to decide whether to forward or drop the frame.

Port security cannot prevent sniffing or MAC address spoofing attacks. Use an access list on a router to control sent and received packets.

References

LabSim for Security Pro, Section 6.5.
[All Questions SecPro2017_v6.exm SWITCH_SECURITY_10]

Question 11: Correct

You are the network administrator for a city library. Throughout the library are several groups of computers that provide public access to the Internet. Supervision of these computers has been difficult. You've had problems with patrons bringing personal laptops into the library and disconnecting the network cables from the library computers to connect their laptops to the Internet.

The library computers are in groups of four. Each group of four computers is connected to a hub that is connected to the library network through an access port on a switch. You want to restrict access to the network so only the library computers are permitted connectivity to the Internet.

What can you do?

- Create static MAC addresses for each computer and associate it with a VLAN.
- Remove the hub and place each library computer on its own access port.
- Create a VLAN for each group of four computers.
- Configure port security on the switch.

Explanation

Configuring port security on the switch can restrict access so that only specific MAC addresses can connect to the configured switch port. This would prevent the laptop computers from being permitted connectivity.

Placing each library computer on its own access port would have no effect.

VLANs are used to group broadcast traffic and do not restrict connectivity of devices as needed in this scenario.

References

LabSim for Security Pro, Section 6.5.
[All Questions SecPro2017_v6.exm SWITCH_SECURITY_11||/]

Question 12: Correct

You run a small network for your business that has a single router connected to the Internet and a single switch. You keep sensitive documents on a computer that you would like to keep isolated from other computers on the network. Other hosts on the network should not be able to communicate with this computer through the switch, but you still need to access the network through the computer.

What should you use for this situation?

- VPN
- VLAN
- Port security
- Spanning tree

Explanation

Define virtual LANs (VLANs) on the switch. With a VLAN, a port on the switch is associated with a VLAN. Only devices connected to ports that are members of the same VLAN can communicate with each other. Routers are used to allow communication between VLANs if necessary.

Use virtual private network (VPN) to connect two hosts securely through an unsecured network (such as the Internet). VPN tunneling protocols protect data as it travels through the unsecured network. Spanning tree is a switch feature that allows for redundant paths between switches. Port security is a method of requiring authentication before a network connection is allowed.

References

LabSim for Security Pro, Section 6.5.
[All Questions SecPro2017_v6.exm SWITCH_SECURITY_12]

Question 13: Correct

Which of the following best describes the concept of a *virtual LAN*?

- Devices in separate networks (i.e. different network addresses) logically grouped as if they were in the same network
- Devices on different networks that can receive multicast packets

- Devices on the same network logically grouped as if they were on separate networks
- Devices connected through the Internet that can communicate without using a network address
- Devices connected by a transmission medium other than cable (i.e. microwave, radio transmissions)

Explanation

A virtual LAN is created by identifying a subset of devices on the same network, and logically identifying them as if they were on separate networks. Think of VLANs as a subdivision of a LAN.

References

LabSim for Security Pro, Section 6.5.
[All Questions SecPro2017_v6.exm SWITCH_SECURITY_13]

Question 14: Correct

Your company is a small start-up company that has leased office space in a building shared by other businesses. All businesses share a common network infrastructure. A single switch connects all devices in the building to the router that provides Internet access.

You would like to make sure that your computers are isolated from computers used by other companies. Which feature should you request to have implemented?

- Spanning tree
- VLAN
- Port security
- VPN

Explanation

Define virtual LANs (VLANs) on the switch. With a VLAN, a port on the switch is associated with a VLAN. Only devices connected to ports that are members of the same VLAN can communicate with each other. Routers are used to allow communication between VLANs if necessary.

Use virtual private network (VPN) to connect two hosts securely through an unsecured network (such as the Internet). VPN tunneling protocols protect data as it travels through the unsecured network. Spanning tree is a switch feature that allows for redundant paths between switches. Port security is a method of requiring authentication before a network connection is allowed.

References

LabSim for Security Pro, Section 6.5.
[All Questions SecPro2017_v6.exm SWITCH_SECURITY_14]

Question 15: Incorrect

You manage a network that uses multiple switches. You want to provide multiple paths between switches so that if one link goes down, an alternate path is available.

Which feature should your switch support?

- Mirroring
- ~~Trunking~~
- OSPF
- Spanning tree
- PoE

Explanation

Spanning tree is a protocol on a switch that allows the switch to maintain multiple paths between

switches within a subnet. The spanning tree protocol runs on each switch and is used to select a single path between any two switches.

- Without the spanning tree protocol, switches that are connected together with multiple links would form a switching loop, where frames are passed back and forth continuously.
- Spanning tree provides only a single active path between switches. Switch ports that are part of that path are placed in a forwarding state.
- Switch ports that are part of redundant but unused paths are placed in a blocking (non-forwarding) state.
- When an active path goes down, the spanning tree protocol automatically recovers and activates the backup ports necessary to provide continued connection between devices.

Trunking identifies ports that are used to carry VLAN traffic between switches. A trunk port is a member of all VLANs defined on all switches. *Mirroring* sends traffic from all switch ports to a switch port you designate as the mirrored port. Power over Ethernet (PoE) supplies power to end devices through the RJ-45 Ethernet switch port. OSPF is a routing protocol used by routers to learn about and select routes to destination networks.

References

LabSim for Security Pro, Section 6.5.
[All Questions SecPro2017_v6.exm SWITCH_SECURITY_15]