Exam Report: 13.9.5 Practice Questions

Date: 4/15/2020 5:14:53 pm
Time Spent: 1:00

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 18%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Incorrect

You are a security consultant and have been hired to evaluate an organization's physical security practices. All employees must pass through a locked door to enter the main work area. Access is restricted using a smart card reader. Network jacks are provided in the reception area such that employees and vendors can access the company network for work-related purposes. Users within the secured work area have been trained to lock their workstations if they will be leaving them for any period of time.

Which of the following recommendations would you MOST likely make to this organization to increase their security?

- Move the receptionist's desk into the secured area.
- Disable the switch ports connected to the network jacks in the reception area.
- Replace the smart card reader with a key code lock.
- ~~Require users to use screensaver passwords.~~

Explanation

You should recommend the company disable the switch ports connected to the network jacks in the reception area. Having active network jacks in an unsecured area allows anyone who comes into the building to connect to the company's network.

Smart card readers are generally considered more secure than key code locks because access codes can be easily shared or observed. Training users to lock their workstations is more secure than screensaver passwords, although this may be a good idea as a safeguard in case a user forgets.

References

TestOut PC Pro - 13.9 Network Security
[e_netsec_pp6.exam.xml Q_WIRED_SEC_01]

Question 2: Incorrect

Your organization is frequently visited by sales reps. While on-site, they frequently plug their notebook systems into any available wall jack, hoping to get internet

Which of the following would BEST protect you from guest malware infection? (Select TWO).

- [ ] Implement static IP addressing.
- [ ] Enable port analysis on your network switch.
- [ ] Implement MAC address filtering.
- [x] ~~Implement private IP addressing with a Network Address Translation (NAT) router facing the internet.~~
- [ ] Implement SNMP traps on your network switch.

Explanation

You should consider enabling MAC address filtering. MAC filtering is configured on your network switches and is used to restrict network access to only systems with specific MAC addresses. You could also consider assigning static IP addresses to your network hosts. By not using DHCP, visitor laptops connected to a wired Ethernet jack won't receive a valid IP address and won't be able to communicate with other hosts on your network.

Implementing SNMP traps, port analysis, or a NAT router will not prevent visitors from connecting to your network.

References

TestOut PC Pro - 13.9 Network Security
[e_netsec_pp6.exam.xml Q_WIRED_SEC_02]

Question 3: Correct

Which of the following is the most secure security protocol for wireless networks?

- ( ) WPA
- (•) WPA2
- ( ) WEP
- ( ) 802.11n
- ( ) BitLocker

Explanation

WEP, WPA, and WPA2 are all security protocols for wireless networks. However, WPA2 provides much stronger security than WEP or WPA.

802.11n is a wireless standard with specific parameters for wireless data transmission. BitLocker is a Microsoft solution that provides hard drive disk encryption.

References

TestOut PC Pro - 13.9 Network Security
[e_netsec_pp6.exam.xml Q_WIRELESS_SEC_01]

Question 4: Incorrect

- [ ] Filtering of traffic based on packet characteristics
- [ ] Identification of the network
- [ ] Authentication
- [x] ~~Centralized access for clients~~
- [x] Encryption
- [ ] Refusal of client connections based on MAC address

Explanation

Wi-Fi Protected Access 2 (WPA2) provides encryption and authentication for wireless networks.

MAC address filtering allows or rejects client connections based on the hardware address. The SSID is the network name or identifier. A wireless access point (called an AP or WAP) is the central connection point for wireless clients. A firewall allows or rejects packets based on packet characteristics (such as address, port, or protocol type).

References

TestOut PC Pro - 13.9 Network Security
[e_netsec_pp6.exam.xml Q_WIRELESS_SEC_02]

Question 5: Correct

Which of the following measures will make your wireless network less visible to the casual attacker?

- ( ) Implement MAC address filtering
- ( ) Use a form of authentication other than Open authentication
- (•) Disable SSID broadcast
- ( ) Change the default SSID
- ( ) Implement WPA2 Personal

Explanation

Wireless access points are transceivers which transmit and receive radio signals on a wireless network. Each access point has a service set ID (SSID) which identifies the wireless network. By default, access points broadcast the SSID to announce their presence and make it easy for clients to find and connect to the wireless network. You can turn off the SSID broadcast to keep a wireless 802.11 network from being automatically discovered. When SSID broadcasting is turned off, users must know the SSID to connect to the wireless network. This helps to prevent casual attackers from connecting to the network, but any serious hacker with the right tools can still connect to the wireless network.

Using authentication with WPA2 helps prevent attackers from connecting to your wireless network, but does not hide the network. Changing the default SSID to a different value does not disable the SSID broadcast. Implementing MAC address

References

TestOut PC Pro - 13.9 Network Security
[e_netsec_pp6.exam.xml Q_WIRELESS_SEC_03]

Question 6: Incorrect

What is the least secure place to locate an omnidirectional access point when creating a wireless network?

- In common or community work areas
- Above the third floor
- ~~In the center of the building~~
- Near a window

Explanation

The least secure location for an omnidirectional wireless access point is against a perimeter wall. So, placement near a window would be the worst option from this list of selections.

For the best security, omnidirectional wireless access points should be located in the center of the building. This will reduce the likelihood that the wireless network's access radius will extend outside of the physical borders of your environment. It is important to place wireless access points where they are needed, such as in a common or community work area.

References

TestOut PC Pro - 13.9 Network Security
[e_netsec_pp6.exam.xml Q_WIRELESS_SEC_04]

Question 7: Incorrect

You've just finished installing a wireless access point for a client. Which action best protects the access point from unauthorized tampering with its configuration settings?

- Disabling SSID broadcast
- ~~Implementing MAC address filtering~~
- Disabling DHCP
- Changing the default administrative password

Explanation

To prevent administrative access to the access point, change the default administrator password. If you do not change the password, users can search the internet for the default password and use it to gain access to the access point and make configuration changes.

Disabling SSID broadcast, disabling DHCP, and using MAC address filtering helps prevent unauthorized access to the wireless network.

References

[e_netsec_pp6.exam.xml Q_WIRELESS_SEC_05]

Question 8: Incorrect

You have just installed a wireless access point (WAP) for your organization's network. You know that the radio signals used by the WAP extend beyond your organization's building and are concerned that unauthorized users outside may be able to access your internal network.

Which of the following steps will BEST protect the wireless network? (Select TWO. Each option is a complete solution.)

- [ ] Install a radio signal jammer at the perimeter of your organization's property.
- [x] Configure the WAP to filter out unauthorized MAC addresses.
- [ ] Disable the spread-spectrum radio signal feature on the WAP.
- [ ] Implement a WAP with a shorter range.
- [ ] Disable SSID broadcast on the WAP.
- [ ] Use the WAP's configuration utility to reduce the radio signal strength.

Explanation

To increase the security of the wireless network, you can use the WAP's configuration utility to reduce the radio signal strength. This will reduce or even eliminate signal emanation outside of your building. You can also configure the WAP to filter out unauthorized MAC addresses. Enabling MAC address filtering denies access to unauthorized systems.

References

TestOut PC Pro - 13.9 Network Security
[e_netsec_pp6.exam.xml Q_WIRELESS_SEC_06]

Question 9: Incorrect

A small business named Widgets, Inc. has hired you to evaluate their wireless network security practices. As you analyze their facility, you note the following using a wireless network locator device:

- They use an 802.11n wireless network.
- The wireless network is broadcasting the SID Linksys.
- The wireless network uses WPA2 with AES security.
- Directional access points are positioned around the periphery of the building.

Which of the following would you MOST likely recommend your client do to increase their wireless network security? (Select TWO).

- [ ] Upgrade to an 802.11g wireless network.
- [ ] Change the SSID to something other than the default.
- [x] ~~Implement omnidirectional access points.~~

☐ Configure the wireless network to use WPA with TKIP security.

Explanation

You should recommend the following:

- Disable SSID broadcast. This makes the network harder (but not impossible) to locate.
- Change the SSID to something other than the default. This obscures what type of AP is in use.

Using WPA instead of WPA2 would decrease the security of the wireless network, as would implementing omnidirectional APs. Switching to an 802.11g network would dramatically reduce the speed of the network without providing any security enhancements.

References

TestOut PC Pro - 13.9 Network Security
[e_netsec_pp6.exam.xml Q_WIRELESS_SEC_07]

Question 10: Incorrect

A small business named BigBikes, Inc. has hired you to evaluate their wireless network security practices. As you analyze their facility, you note the following:

- They use an 802.11a wireless network.
- The wireless network SSID is set to BWLAN.
- The wireless network is not broadcasting the network SSID.
- The wireless network uses WPA2 with AES security.
- Omnidirectional access points are positioned around the periphery of the building.

Which of the following would you MOST likely recommend your client do to increase their wireless network security?

○ Enable SSID broadcast.

○ Configure the wireless network to use WEP security.

➡ ○ Implement directional access points.

○ Change the SSID to something similar to BigBikeInc.

◉ ~~Upgrade to an 802.11g wireless network.~~

Explanation

You should recommend that they implement directional access points along the periphery of the building. Using omnidirectional APs in these locations can cause the wireless network radio signal to emanate outside the building, making it readily available to malicious individuals.

Enabling SSID broadcasts and using an SSID that is easily identifiable reduces the security of the wireless network, as would switching to WEP security. Switching to an 802.11g network offers no speed or security benefits and would require retrofitting all wireless equipment in the organization.

References

[e_netsec_pp6.exam.xml Q_WIRELESS_SEC_08]

Question 11: Incorrect

A small company hires a technician to review their wireless security. The technician discovers that the wireless signal is available outside of the building.

Which of the following could the technician recommend to correct this problem? (Select TWO).

- [x] Decrease radio power levels.
- [ ] Update firmware.
- [x] Implement a directional antennae.
- [ ] Enable MAC filtering.
- [ ] Disable SSID broadcast.

Explanation

Directional antennae can be positioned to point wireless signals toward more desired areas and away from less desired areas.

Decreasing radio power levels can limit the radius of the effective wireless signal.

MAC filtering can be used to block devices from connecting, but does not limit the wireless signal.

Disabling SSID broadcast can make a wireless network more secure, but does not limit the wireless signal.

Updating firmware is a good practice, but does not limit the wireless signal.

References

TestOut PC Pro - 13.9 Network Security
[e_netsec_pp6.exam.xml Q_WIRELESS_SEC_SOHO_NETWORKS_01]