Chp 8 NS

Candidate: Dunkan Gibson (dunkan.gibson)
Date: 3/15/2022 9:20:12 pm • Time spent: 03:31

Score: 88% Passing Score: 80%

Question 1: ✔ Correct

The IT manager has tasked you with installing the new wireless LAN controller (WLC).

Where should you install the controller?

- ➡ Network closet
- Manager's Office
- Roof
- Lobby

EXPLANATION

A WLC should be placed in the networking closet and connected to a switch so it can communicate with and manage the wireless access points.

None of the other locations are valid locations to install the WLC.

REFERENCES

8.1.3 Wireless Networking Facts

q_wireless_placement_02_secp7.question.fex

Question 2: ✔ Correct

Which type of wireless access point is generally used in a residential setting?

- Bridge
- WLC
- SOHO
- LWAP

EXPLANATION

In a small office or residential location, a Small Office Home Office (SOHO) wireless router is often used. These devices are three different devices in one:

- A router function connects the internal LAN to the internet.
- A switch portion connects the internal wired LAN devices together.
- An access point portion allows the internal wireless devices to connect to the network.

Lightweight access points (LWAPs) are used in conjunction with a wireless controller.

A wireless bridge connects two wireless networks together.

A wireless LAN controller (WLC) is used in an enterprise environment to manage multiple access points.

REFERENCES

8.1.3 Wireless Networking Facts

q_wireless_security_01_secp7.question.fex

Question 3: ✔ Correct

Which of the following types of site surveys should be performed first?

- Passive
- Predictive
- Active
- Ad hoc

EXPLANATION

An initial site survey performed should be a passive survey. This survey is performed without the analyzer connecting to any specific WAP and is instead in a listen-only mode.

An active survey is performed after multiple passive surveys have been completed and the wireless access points have been placed. An active survey verifies proper coverage has been achieved.

A predictive survey uses software programs to load the building blueprints and determines where to install the WAPs.

An ad hoc wireless configuration mode provides wireless communication without a wireless access point. Ad hoc mode is not a type of site survey.

REFERENCES

8.1.3 Wireless Networking Facts

q_wireless_site_survey_02_secp7.question.fex

Question 4: ✔ Correct

Which of the following is generated after a site survey and shows the Wi-Fi signal strength throughout the building?

- Analyzer
- Diagram
- ➡ Heat map
- Ad hoc

EXPLANATION

A heat map is generated following a site survey. A heat map shows the Wi-Fi signal strength in different locations.

A diagram of the location is needed so survey results can be overlaid.

A Wi-Fi analyzer is used to perform a site survey.

Ad hoc wireless configuration mode provides wireless communication without a wireless access point. This is not a type of site survey.

REFERENCES

8.1.3 Wireless Networking Facts

q_wireless_heat_map_secp7.question.fex

Question 5: ✔ Correct

Which of the following is used on a wireless network to identify the network name?

- MAC address
- Subnet mask
- IP address
- SSID

EXPLANATION

Wireless devices use the service set identifier (SSID) to identify a network name. All devices on a wireless network use the same SSID.

The MAC address is a unique physical device address. The IP address is a logical address that includes both the logical network and the logical device address. The subnet mask is used with the IP address to identify the network portion of the IP address.

REFERENCES

8.1.3 Wireless Networking Facts

q_wireless_access_point_secp7.question.fex

Question 6: ✔ Correct

Your company security policy states that wireless networks are not to be used because of the potential security risk they present to your network.

One day, you find that an employee has connected a wireless access point to the network in his office.

Which type of security risk is this?

- Phishing
- Man-in-the-middle attack
- Physical security
- ➡ Rogue access point
- Social engineering

EXPLANATION

A rogue access point is an unauthorized access point added to a network, or it is an access point that is configured to mimic a valid access point. Examples include:

- An attacker or an employee with access to the wired network installs a wireless access point on a free port. The access port then provides a way to remotely access the network.
- An attacker near a valid wireless access point installs an access point with the same (or similar) SSID. The access point is configured to prompt for credentials, allowing the attacker to steal those credentials or use them in a man-in-the-middle attack to connect to the valid wireless access point.
- An attacker configures a wireless access point in a public location and then monitors traffic to see who connects to the access point.

A man-in-the-middle attack is used to intercept information passing between two communication partners. A rogue access point might be used to initiate a man-in-the-middle attack. But in this case, the rogue access point was connected without malicious intent. Social engineering exploits human nature by convincing someone to reveal information or perform an activity. Phishing uses an email and a spoofed website to gain sensitive information.

REFERENCES

8.2.2 Wireless Attack Facts

q_wl_attacks_rogue_secp7.question.fex

Question 7: ✕ Incorrect

You want to connect a laptop computer running Windows to a wireless network.

The wireless network uses multiple access points and WPA2-Personal. You want to use the strongest authentication and encryption possible. SSID broadcast has been disabled.

What should you do?

- Configure the connection with a pre-shared key and TKIP encryption.
- ➡ Configure the connection with a pre-shared key and AES encryption.
- Configure the connection to use 802.1x authentication and TKIP encryption.
- ~~Configure the connection to use 802.1x authentication and AES encryption.~~

EXPLANATION

To connect to a wireless network using WPA2-Personal, you need to use a pre-shared key for authentication. Advanced Encryption Standard (AES) encryption is supported by WPA2 and is the strongest encryption method.

WPA and WPA2 designations that include Personal or PSK use a pre-shared key for authentication. Methods that include Enterprise use a RADIUS server for authentication and 802.1x authentication with usernames and passwords.

REFERENCES

8.3.2 Wireless Security Facts

q_wl_security_psk_secp7.question.fex

Question 8: ✔ Correct

Which of the following best describes Bluesnarfing?

- Sending anonymous electronic business cards
- ➡ Viewing calendar, emails, and messages on a mobile device without authorization
- Executing commands on a mobile device
- Cloning a mobile device

EXPLANATION

Bluesnarfing is the use of a Bluetooth connection to gain unauthorized access to an existing Bluetooth connection between phones, desktops, laptops, or PDAs. Bluesnarfing allows access to view the calendar, emails, text messages, and contact lists. Many Bluetooth devices have built-in features to prevent bluesnarfing, but it is still a known vulnerability.

Bluejacking is a rather harmless practice that entails an unknown sender sending business cards anonymously to a Bluetooth recipient within a distance of 10-100 meters, depending on the class of the Bluetooth device. The business cards usually include a flirtatious message so the attacker can see a visual reaction from the recipient. Multiple messages are sent to the device if the attacker thinks there is a chance they will be added as a contact. Bluetooth devices are not susceptible to bluejacking if they are set to non-discoverable mode.

Bluebugging gives an attacker access to all mobile phone commands that use Bluetooth technology, such as initiating phone calls, sending and receiving messages, eavesdropping, and reading and writing phone book contacts. Only highly skilled individuals can perform bluebugging.

REFERENCES

8.2.2 Wireless Attack Facts

q_wl_attacks_bluesnarfing_secp7.question.fex

Question 9: ✔ Correct

Which of the following do switches and wireless access points use to control access through a device?

- MAC address filtering
- Port number filtering
- Session filtering
- IP address filtering

EXPLANATION

Both switches and wireless access points are Layer 2 devices, meaning they use the MAC address to make forwarding decisions. Both devices typically include some form of security that restricts access based on the MAC address.

Routers and firewalls operate at Layer 3 and can use the IP address or port number for filtering decisions. A circuit-level gateway is a firewall that can make forwarding decisions based on the session information.

REFERENCES

8.3.4 Wireless Authentication and Access Methods Facts

q_wl_auth_access_mac_secp7.question.fex

Question 10: ✔ Correct

You are the security analyst for your organization. Clients are complaining about being unable to connect to the wireless network. After looking into the issue, you have noticed short bursts of high-intensity RF signals are interfering with your wireless network's signal.

Which type of attack are you most likely experiencing?

- Bluesnarfing
- Disassociation
- Cloning
- ➡ Jamming

EXPLANATION

In a jamming attack, a transmitter is tuned to the same frequency and type of modulation as the wireless network. The jamming signal overrides the legitimate wireless network radio signals. This scenario is a spark jamming attack.

A disassociation attack occurs when a user is tricked into giving a fake router responsibility for forwarding packets.

Bluesnarfing is a Bluetooth attack.

Cloning is an RFID attack.

REFERENCES

8.2.2 Wireless Attack Facts

q_wl_attacks_jamming_secp7.question.fex

Question 11: ✕ Incorrect

You need to implement a wireless network link between two buildings on a college campus. A wired network has already been implemented within each building. The buildings are 100 meters apart.

Which type of wireless antenna should you use on each side of the link? (Select two.)

- ➡ ☑ Parabolic
- ☐ Omni-directional
- ➡ ☐ High-gain
- ☐ Normal-gain
- ☑ ~~Directional~~

EXPLANATION

You should use a high-gain parabolic antenna on each side of the link. A high-gain antenna usually has a gain rating of 12 dBi or higher. A parabolic antenna uses a parabolic-shaped reflector dish. It is highly directional, concentrating the radio waves transmitted from the sender into a very narrow beam. When the receiver uses a parabolic antenna, it can only receive a signal from one specific direction. It supports very high-gain radio signals that can be transmitted over long distances, but it requires a clear line of sight between the sender and the receiver.

A normal-gain antenna usually has a gain rating between 2 and 9 dBi. An omni-directional antenna radiates and absorbs signals equally in every direction around the antenna. Because it spreads its gain in a 360-degree pattern, the overall range of an omni-directional antenna is typically much less than that of a directional antenna. A directional antenna focuses its radiation and absorption of signals in a specific direction. However, these typically have a much shorter range than a parabolic antenna.

REFERENCES

8.1.3 Wireless Networking Facts

q_wireless_placement_01_secp7.question.fex

Question 12: ✔ Correct

An attacker has intercepted near-field communication (NFC) data and is using that information to masquerade as the original device.

Which type of attack is being executed?

- Relay
- Bluesnarfing
- Cloning
- Disassociation

EXPLANATION

This scenario describes a relay attack. A relay attack occurs when an attacker can capture NFC data in transit and use the information to masquerade as the original device.

A disassociation attack occurs when a user is tricked into giving a fake router responsibility for forwarding packets. This is not performed on NFC devices.

Bluesnarfing is a Bluetooth attack.

Cloning occurs when an attacker creates a copy of an existing RFID tag and uses the fake tag to gain access to a secure system.

REFERENCES

8.2.2 Wireless Attack Facts

q_wl_attacks_nfc_secp7.question.fex

Question 13: ✔ Correct

You need to add security for your wireless network, and you would like to use the most secure method.

Which method should you implement?

- WPA
- ➡ WPA2
- WEP
- Kerberos

EXPLANATION

Wi-Fi Protected Access 2 (WPA2) is currently the most secure wireless security specification. WPA2 includes specifications for both encryption and authentication.

WPA was an earlier implementation of security specified by the 802.11i committee. WEP was the original security method for wireless networks. WPA is more secure than WEP but less secure than WPA2.

Kerberos is an authentication method, not a wireless security method.

REFERENCES

8.3.2 Wireless Security Facts

q_wl_security_wpa2_03_secp7.question.fex

Question 14: ✔ Correct

You have physically added a wireless access point to your network and installed a wireless networking card in two laptops that run Windows. Neither laptop can find the network. You have come to the conclusion that you must manually configure the access point (AP).

Which of the following values uniquely identifies the network AP?

- WEP
- SSID
- Channel
- PS

EXPLANATION

The SSID (service set identifier) identifies the wireless network. All PCs and access points in a LAN share the same SSID.

WEP (Wired Equivalent Privacy) is used to add a layer of security to the transmission, while the channel identifies the frequency that the card and AP communicate on.

REFERENCES

8.3.4 Wireless Authentication and Access Methods Facts

q_wl_auth_access_ap_02_secp7.question.fex

Question 15: ✕ Incorrect

To answer this question, complete the lab using the information below. **Launch Lab**

You did not attempt the lab.

You are a network technician for a small corporate network. You need to increase the security of your wireless network. Your new wireless controller provides several security features that you want to implement.

> Access the Wireless Controller console through Chrome on **http://192.168.0.6** with the username **admin** and the password **password**. The username and password are case sensitive.

In this lab, your task is to:

- Change the admin username and password for the Zone Director controller to the following:
  - Admin Name: **WxAdmin**
  - Password: **ZDAdminsOnly!$** (O is the capital letter O)
- Set up MAC address filtering (L2 Access Control) to create a whitelist called **Allowed Devices** that includes the following wireless devices:
  - **00:18:DE:01:34:67**
  - **00:18:DE:22:55:99**
  - **00:02:2D:23:56:89**
  - **00:02:2D:44:66:88**
- Implement a device access policy called **NoGames** that blocks gaming consoles from the wireless network.

REFERENCES

5.5.3 Configuring a VPN Client

8.3.5 Hardening a Wireless Access Point

8.3.7 Configure WIPS

8.3.9 Configuring a Captive Portal

31910253-85d4-40b4-b2a5-e0f21810e171

Question 16: ✔ Correct

Which EAP implementation is MOST secure?

- EAP-MD5
- EAP-FAST
- LEAP
- EAP-TLS

EXPLANATION

EAP-TLS uses Transport Layer Security (TLS) and is considered one of the most secure EAP standards available. A compromised password is not enough to break into EAP-TLS enabled systems because the attacker must also have the client's private key.

EAP-MD5 offers minimal security and is susceptible to dictionary attacks and man-in-the-middle attacks. Lightweight Extensible Authentication Protocol (LEAP) does a poor job of protecting user authentication credentials and is also susceptible to dictionary attacks. EAP-FAST is a replacement for LEAP that uses a protected access credential (PAC) to establish a TLS tunnel in which client authentication credentials are transmitted. While more secure than EAP-MD5 and LEAP, EAP-FAST can still be compromised if the attacker intercepts the PAC.

REFERENCES

8.3.4 Wireless Authentication and Access Methods Facts

q_wl_auth_access_eap_tls_secp7.question.fex

Question 17: ✔ Correct

You are concerned that wireless access points may have been deployed within your organization without authorization.

What should you do? (Select two. Each response is a complete solution.)

- [ ] Implement a network access control (NAC) solution.
- [ ] Implement an intrusion detection system (IDS).
- [x] Conduct a site survey.
- [x] Check the MAC addresses of devices connected to your wired switch.
- [ ] Implement an intrusion prevention system (IPS).

EXPLANATION

A rogue host is an unauthorized system that has connected to a wireless network. It could be an unauthorized wireless device, or it could even be an unauthorized wireless access point that someone connected without permission to a wired network jack. Rogue hosts could be benign in nature, or they could be malicious. Either way, rogue hosts on your wireless network could represent a security risk and should be detected and removed if necessary. Four commonly used techniques for detecting rogue hosts include:

- Using site survey tools to identify hosts and APs on the wireless network
- Checking connected MAC addresses to identify unauthorized hosts
- Conducting an RF noise analysis to detect a malicious rogue AP that is using jamming to force wireless clients to connect to it instead of legitimate APs
- Analyzing wireless traffic to identify rogue hosts

Using an IDS or an IPS would not be effective, as these devices are designed to protect networks from perimeter attacks. Rogue APs are internal threats. A NAC solution can be used to remediate clients that connect to a network, but a NAC solution can't be used to detect a rogue AP.

REFERENCES

8.2.2 Wireless Attack Facts

q_wl_attacks_site_survey_secp7.question.fex

Question 18: ✔ Correct

Which of the following devices would you use to perform a site survey?

- Wireless interface
- ➡ Wi-Fi analyzer
- Wireless access point
- Heat map

EXPLANATION

A Wi-Fi analyzer is used to perform a site survey. A Wi-Fi analyzer can be a specialized tool or a software program running on a laptop, smartphone, or tablet.

A heat map is generated following a site survey. A heat map shows the Wi-Fi signal strength in different locations.

A wireless access point (WAP) broadcasts information and data over radio waves. WAPs function as wireless hubs.

A wireless interface in a device, such as a laptop or smartphone, connects to a wireless access point.

REFERENCES

8.1.3 Wireless Networking Facts

q_wireless_site_survey_01_secp7.question.fex

Question 19: ✔ Correct

You've just finished installing a wireless access point for a client. What should you do to prevent unauthorized users from using the access point (AP) configuration utility?

- Isolate the AP from the client's wired network.
- Change the administrative password on the AP.
- Implement MAC address filtering.
- Change the channel used by the AP's radio signal.

EXPLANATION

You should change the administrative password used by the AP. Many AP manufacturers use a default administrative username and password that are well known. If you don't change these parameters, anyone connecting to the AP can easily guess the password required to access the AP's configuration utility.

REFERENCES

8.3.4 Wireless Authentication and Access Methods Facts

q_wl_auth_access_security_secp7.question.fex

Question 20: ✔ Correct

Which class of wireless access point (WAP) has everything necessary to manage clients and broadcast a network already built into its functionality?

- Bridge
- Ad hoc
- Fat
- Thin

EXPLANATION

Fat access points have everything necessary to manage wireless clients and broadcast a network. Fat access points are standalone devices.

Thin access points are basically a radio and antenna. Thin access points can broadcast a network, but require another system to manage clients and the network.

A wireless bridge connects two wireless networks together.

Ad hoc wireless configuration mode provides wireless communication without a wireless access point.

REFERENCES

8.1.3 Wireless Networking Facts

q_wireless_wap_02_secp7.question.fex

Question 21: ✔ Correct

Which type of interference is caused by motors, heavy machinery, and fluorescent lights?

- RFID
- EMI
- NFC
- RFI

EXPLANATION

Electromagnetic interference (EMI) is interference caused by motors, heavy machinery, and fluorescent lights.

Radio frequency interference (RFI) is interference on the radio channel. It is caused by nearby wireless devices using the same channel, cordless phones, or microwave ovens.

Near frequency communication (NFC) allows two-way communication between two devices. The devices must be within a few centimeters of each other.

Radio frequency identification (RFID) uses radio waves to transmit data from small circuit boards, called RFID tags, to special scanners.

REFERENCES

8.2.2 Wireless Attack Facts

q_wl_attacks_emi_secp7.question.fex

Question 22: ✔ Correct

Which type of attack is WEP extremely vulnerable to?

- Evil twin
- IV attack
- Cloning
- Bluesnarfing

EXPLANATION

Wired Equivalent Privacy (WEP) is extremely vulnerable to initialization vector (IV) attacks because WEP reuses the IVs. This makes it easy for attackers to crack them and compromise the encryption.

An evil twin attack is a type of rogue access point attack.

Bluesnarfing is a Bluetooth attack.

Cloning is an RFID attack.

REFERENCES

8.2.2 Wireless Attack Facts

q_wl_attacks_iv_secp7.question.fex

Question 23: ✔ Correct

Which of the following sends unsolicited business cards and messages to a Bluetooth device?

- Bluejacking
- Bluesnarfing
- Bluebugging
- Slamming

EXPLANATION

Bluejacking is a rather harmless practice that entails an unknown sender sending business cards anonymously to a Bluetooth recipient within a distance of 10-100 meters, depending on the class of the Bluetooth device. The business cards usually include a flirtatious message so the attacker can see a visual reaction from the recipient. Multiple messages ware sent to the device if the attacker thinks there is a chance they will be added as a contact. Bluetooth devices are not susceptible to bluejacking if they are set to non-discoverable mode.

Bluesnarfing is the use of a Bluetooth connection to gain unauthorized access to an existing Bluetooth connection between phones, desktops, laptops, or PDAs. Bluesnarfing allows the attacker to view calendars, emails, text messages, and contact lists. Bluebugging gives an attacker access to all mobile phone commands that use Bluetooth technology, such as initiating phone calls, sending and receiving messages, eavesdropping, and reading and writing phone book contacts.

Slamming entails unauthorized or fraudulent changes made to a subscriber's telephone service or DSL internet service.

REFERENCES

8.2.2 Wireless Attack Facts

q_wl_attacks_bluejacking_secp7.question.fex

Question 24: ✔ Correct

Which of the following is responsible for broadcasting information and data over radio waves?

- Wireless bridge
- ➡ Wireless access point
- Wireless LAN controller
- Wireless interface

EXPLANATION

A wireless access point (WAP) broadcasts information and data over radio waves. WAPs function as wireless hubs.

A wireless bridge connects two wireless networks together.

A wireless interface in a device, such as a laptop or smartphone, connects to a wireless access point.

A wireless LAN controller is used in an enterprise environment to manage multiple access points.

REFERENCES

8.1.3 Wireless Networking Facts

q_wireless_wap_01_secp7.question.fex

Question 25: ✔ Correct

You are replacing a wired business network with an 802.11g wireless network. You currently use Active Directory on the company network as your directory service. The new wireless network has multiple wireless access points, and you want to use WPA2 on the network. What should you do to configure the wireless network? (Select two.)

- [ ] Use shared secret authentication
- [x] Configure devices to run in infrastructure mode
- [ ] Configure devices to run in ad hoc mode
- [ ] Use open authentication with MAC address filtering
- [x] Install a RADIUS server and use 802.1x authentication

EXPLANATION

When using wireless access points, configure an infrastructure network. Because you have multiple access points and an existing directory service, you can centralize authentication by installing a RADIUS server and using 802.1x authentication.

Use ad hoc mode when you need to configure a wireless connection between two hosts. Use open authentication with WEP or when you do not want to control access to the wireless network. Use shared secret authentication with WPA or WPA2 when you can't use 802.1x.

REFERENCES

8.3.4 Wireless Authentication and Access Methods Facts

q_wl_auth_access_radius_04_secp7.question.fex