Exam Report: 10.6.7 Practice Questions

Date: 11/5/2019 7:06:26 pm
Time Spent: 19:06

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 13%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

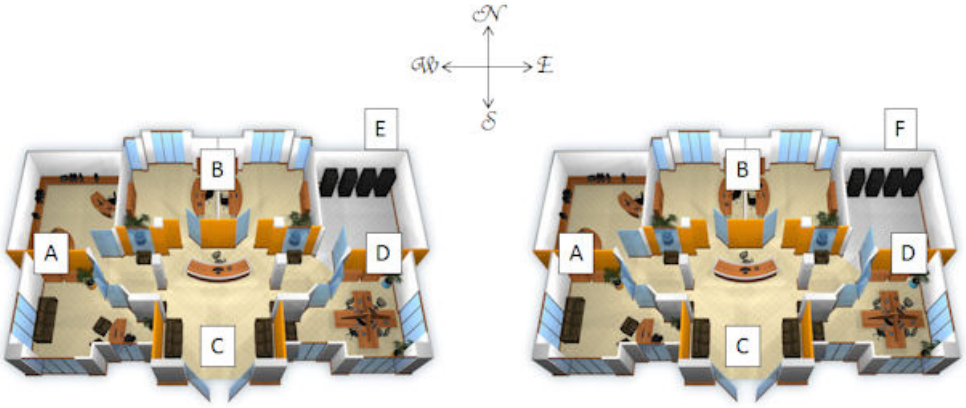
Individual Responses

Question 1: Incorrect

Your consulting firm has been hired by a small business to implement a wireless network. The company leases two office suites within a business park approximately 200m apart, as shown below. The objectives of the implementation are as follows:

- Create a secure wireless network that doesn't emanate beyond each office space by implementing access points in locations A-D in each building.
- Connect the wireless networks at each office together with a secure outdoor wireless link using locations E and F.

Drag the antenna type from the list on the left to the appropriate location on the right. Each antenna type can be used more than once or not at all.



A

~~Normal gain directional antenna aimed west~~ Normal gain directional antenna aimed east

B

✓ Normal gain directional antenna aimed south

C

✓ Normal gain directional antenna aimed north

D

~~Normal gain directional antenna aimed east~~ Normal gain directional antenna aimed west

E

✓ High-gain directional antenna aimed east

F

✓ High-gain directional antenna aimed west

Explanation

In this scenario, directional antennae can be implemented along the exterior walls that are aimed inward. This reduces signal emanation outside the organization. To reduce coverage gaps, you could also implement an omni-directional antenna in the center of each office complex with the power turned to prevent signal emanation.

To establish a wireless link between offices, you can implement high-gain directional parabolic antennae at each site. Because this radio signal will be transmitted outdoors, you will need to use the strongest encryption available on the link.

References

LabSim for Network Pro, Section 10.6.
[netpro18v5_all_questions_en.exm D&D3]

Question 2: Incorrect

Which of the following wireless security methods uses a common shared key configured on the wireless access point and all wireless clients?

- WEP, WPA Personal, WPA Enterprise, WPA2 Personal, and WPA2 Enterprise
- ~~WPA Personal and WPA2 Enterprise~~
- WEP, WPA Personal, and WPA2 Personal
- WPA Enterprise and WPA2 Enterprise

Explanation

Shared key authentication can be used with WEP, WPA, and WPA2. Shared key authentication used with WPA and WPA2 is often called WPA Personal or WPA2 Personal.

WPA Enterprise and WPA2 Enterprise use 802.1x for authentication. 802.1x authentication uses usernames and passwords, certificates, or devices such as smart cards to authenticate wireless clients.

References

LabSim for Network Pro, Section 10.6.
[netpro18v5_all_questions_en.exm NP09 1-7 8]

Question 3: Correct

What is the **least** secure place to locate an access point with an omni-directional antenna when creating a wireless cell?

- In the center of the building
- Near a window
- Above the 3rd floor
- In common or community work areas

Explanation

The least secure location for a wireless cell access point is against a perimeter wall. Placement near a window would be the worst option from this list of selections.

For the best security, access points that use directional antennae would be a more appropriate choice for placement near an exterior wall. This placement reduces the likelihood that the wireless cell's access radius will extend outside of the physical borders of your environment. It is important to place wireless cell access points where they are needed, such as in a common or community work area.

References

LabSim for Network Pro, Section 10.6.
[netpro18v5_all_questions_en.exm SP02_5-1 [37]]

Question 4: Incorrect

Which of the following measures will make your wireless network invisible to the casual attacker performing war driving?

- Use a form of authentication other than open authentication
- Implement WPA2 Personal
- Disable SSID broadcast
- ~~Change the default SSID~~

Explanation

Wireless access points are transceivers that transmit and receive information on a wireless network. Each access point has a service set ID (SSID) that 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. Turn off the SSID broadcast to keep a wireless 802.11x 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 WPA or WPA2 help 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.

References

LabSim for Network Pro, Section 10.6.
[netpro18v5_all_questions_en.exm SP08_2-7 7]

Question 5: Incorrect

Which of the following provides security for wireless networks?

- CSMA/CD
- ~~802.11a~~
- WPA
- WAP
- 802.3u

Explanation

Wi-Fi protected access (WPA) provides encryption and user authentication for wireless networks. Wired equivalent privacy (WEP) also provides security, but WPA is considered more secure than WEP.

A wireless access point (WAP) is a hardware device like a switch that provides access to the wireless network. 802.11a is a wireless networking standard that defines the signal characteristics for communicating on the wireless network. CSMA/CD is a media access control method that controls when a device can communicate on the network.

References

LabSim for Network Pro, Section 10.6.
[netpro18v5_all_questions_en.exm APESS_6-1 MULTIPLE CHOICE [230]]

Question 6: Incorrect

Which of the following features are supplied by WPA2 on a wireless network?

- ~~Client connection refusals based on MAC address~~
- Network identification
- Encryption
- A centralized access point for clients
- Traffic filtering based on packet characteristics

Explanation

Wi-Fi protected access (WPA) provides encryption and user 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

LabSim for Network Pro, Section 10.6.
[netpro18v5_all_questions_en.exm APESS_6-1 MULTIPLE CHOICE [239]]

Question 7: Incorrect

You need to configure a wireless network. You want to use WPA2 Enterprise. Which of the following components will be part of your design? (Select two.)

- [ ] WEP encryption
- [x] AES encryption
- [ ] Open authentication
- [ ] 802.1x
- [ ] TKIP encryption
- [ ] Preshared keys

Explanation

To configure WPA2 Enterprise, you need a RADIUS server to support 802.1x authentication. WPA2 uses AES for encryption.

WPA2-PSK, also called WPA2 Personal, uses pre-shared keys for authentication. WPA uses TKIP for encryption.

References

LabSim for Network Pro, Section 10.6.
[netpro18v5_all_questions_en.exm C802_500 MC [264]]

Question 8: Incorrect

You want to implement 802.1x authentication on your wireless network. Where would you configure passwords that are used for authentication?

- ~~On the wireless access point~~
- On the wireless access point and each wireless device
- On a certificate authority (CA)
- On a RADIUS server

Explanation

802.1x authentication uses usernames and passwords, certificates, or devices such as smart cards to authenticate wireless clients. Authentication requests received by the wireless access point are passed to a RADIUS server that validates the logon credentials (such as the username and password).

If you are using preshared keys for authentication, configure the same key on the wireless access point and each wireless device. A CA is required to issue a certificate to the RADIUS server. The certificate proves the identity of the RADIUS server or can be used to issue certificates to individual clients.

References

LabSim for Network Pro, Section 10.6.
[netpro18v5_all_questions_en.exm NP09_1-7 #7]

Question 9: Incorrect

You are the wireless network administrator for your organization. As the size of the organization has grown, you've decided to upgrade your wireless network to use 802.1x authentication instead of using preshared keys.

To do this, you need to configure a RADIUS server and RADIUS clients. You want the server and the clients to mutually authenticate with each other.

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

- [ ] Configure the RADIUS server with a server certificate.
- [x] ~~Configure all RADIUS clients with a preshared key.~~
- [ ] Configure all wireless workstations with client certificates.
- [ ] Configure all wireless access points with client certificates.
- [ ] Configure the RADIUS server with a preshared key.

Explanation

When using 802.1x authentication for wireless networks, a RADIUS server is implemented to centralize authentication. A centralized authentication database is used to allow wireless clients to roam between cells and authenticate to each using the same account information. PKI is required for issuing certificates. At a minimum, the RADIUS server must have a server certificate; however, to support mutual authentication, each RADIUS client must also have a certificate. Remember that each wireless access point in a RADIUS solution is a RADIUS client, not the wireless devices. The wireless access points forward the credentials from wireless devices to the RADIUS server for authentication.

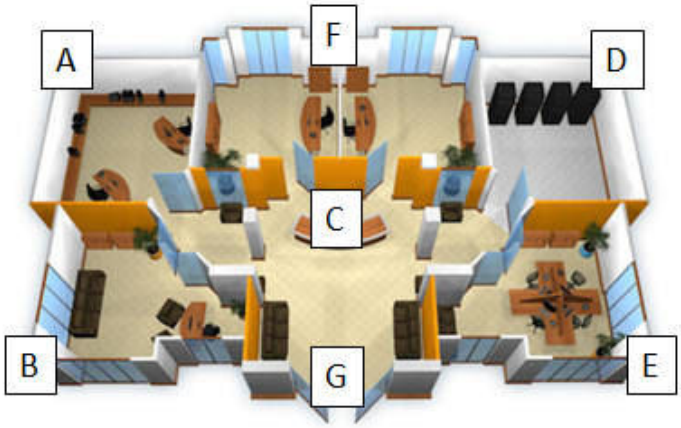
Preshared keys are not used for authentication in an 802.1x solution.

References

LabSim for Network Pro, Section 10.6.
[netpro18v5_all_questions_en.exm MCS8]

Question 10: Incorrect

This question includes an image to help you answer the question. Close



You are designing a wireless network implementation for a small business. The business deals with sensitive customer information, so data emanation must be reduced as much as possible.

The floor plan of the office is shown below. Match each type of access point antenna on the left with the appropriate location on the floor plan on the right. Each antenna type can be used once, more than once, or not at all.

A	B	C	D
✓ Directional	~~Omni-directional~~ Directional	✓ Omni-directional	✓ Directional

E	F	G
~~Parabolic~~	~~Parabolic~~	

Directional Directional Directional

Explanation

There are three types of antennas you should be aware of:

- A directional antenna creates a narrow, focused signal in a particular direction. The focused signal provides greater signal strength, increasing the transmission distance. It provides a stronger point-to-point connection, better equipping devices to handle obstacles.
- An omni-directional antenna disperses the RF wave in an equal 360-degree pattern. It is used to provide access to many clients in a radius.
- A parabolic antenna uses a parabolic reflector shaped like a dish. It is highly directional, concentrating the radio waves transmitted from the sender into a very narrow beam. Using a parabolic antenna on the receiver restricts it to receiving radio signals from only a single, very specific direction. It supports very high gain radio signals that can be transmitted over long distances, but requires a clear line-of-sight (LOS) between the sender and the receiver.

In this scenario, data emanation can be reduced as follows:

- Directional antennae should be implemented along the perimeter of the office in locations A, B, D, E, F, and G with the radio pattern aimed towards the center of the office.
- An omnidirectional antenna can be implemented in the center of the office in location C.
- A parabolic antenna is not appropriate in this scenario and should not be implemented.

A site survey should be conducted to verify that the radio signal from all of the access points does not emanate excessively outside the office.

References

LabSim for Network Pro, Section 10.6.
[netpro18v5_all_questions_en.exm RT-SP-6.14-1]

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.

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

- [ ] Normal-gain
- [ ] Bridge
- [x] High-gain
- [ ] Omni-directional
- [ ] Directional

Explanation

You should use high-gain directional antennae on each side of the link. A high-gain antenna usually has a gain rating of 12 dBi or higher. A highly directional antenna concentrates the radio waves transmitted from the sender in to a very narrow beam. When the receiver uses a directional 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 (LOS) between the sender and the receiver.

A normal-gain antenna usually has a gain rating between 2 and 9 dBi. An omnidirectional 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 omnidirectional antenna is typically much less than the range of a directional antenna. A directional antenna focuses its radiation and absorption of signals in a specific direction, but typically has a much shorter range than a parabolic antenna.

References

LabSim for Network Pro, Section 10.6.
[netpro18v5_all_questions_en.exm RT-SP-6.12-1]

Question 12: 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.

What type of security risk is this?

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

Explanation

A rogue access point is an unauthorized access point added to a network or 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 method for remotely accessing 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, then monitors traffic of those who connect 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

LabSim for Network Pro, Section 10.6.
[netpro18v5_all_questions_en.exm NP09_6-6 #MCS2]

▼ Question 13: Incorrect

An attacker is trying to compromise a wireless network that has been secured using WPA2-PSK and AES. She first tried using AirSnort to capture packets, but found that she couldn't break the encryption.

As an alternative, she used software to configure her laptop to function as an access point. She configured the fake access point with the same SSID as the wireless network she is trying to break into. When wireless clients connect to her access point, she presents them with a web page asking them to enter the WPA2 passphrase. When they do, she then uses it to connect a wireless client to the real access point.

Which attack techniques did the attacker use in this scenario? (Select two.)

- ➡ ☐ Pharming
- ☑ ~~Denial of service~~
- ☐ Man-in-the-middle
- ☐ Smurf
- ➡ ☑ Evil twin

Explanation

The attacker in this scenario used the following attack techniques:

- Evil twin: In this exploit, an attacker near a valid wireless access point installs an access point with the same (or similar) SSID.

- Pharming: In this exploit, the access point is configured to display a bogus web page that prompts for credentials, allowing the attacker to steal those credentials.

Denial of service attacks overload a target system to the point that it can no longer perform its desired function on the network. A man-in-the-middle attack occurs when the attacker gets in between a sender and receiver, posing as the sender to the receiver and as the receiver to the sender. A Smurf attack is a type of denial of service attack that uses spoofed ICMP echo response packets from an amplifier network to overload a target host.

References

LabSim for Network Pro, Section 10.6.
[netpro18v5_all_questions_en.exm MCM3]

Question 14: Incorrect

You want to connect your client computer to a wireless access point that is connected to your wired network at work. The network administrator tells you that the access point is configured to use WPA2 Personal with the strongest encryption method possible. SSID broadcast is turned off.

Which of the following must you configure manually on the client? (Select three.)

- [x] Preshared key
- [ ] Channel
- [ ] TKIP
- [ ] SSID
- [ ] AES
- [x] ~~Username and password~~

Explanation

WPA2 Personal uses a shared key for authentication. Once authenticated, dynamic keys are generated to be used for encryption. WPA2 supports AES and TKIP encryption, with AES being the stronger encryption method. With the SSID broadcast turned off, you will need to manually configure the SSID on the client.

Channels are detected automatically as well. If you were using WPA2 Enterprise, you would need to configure the authentication method, such as a username and password or a smart card.

References

LabSim for Network Pro, Section 10.6.
[netpro18v5_all_questions_en.exm NP09_3-4 #5]

Question 15: Incorrect

Which of the following protocols or mechanisms is used to provide security on a wireless network? (Select three.)

- [ ] WPA
- [ ] IPsec
- [ ] RDP
- [x] 802.1x

Explanation

Remote Desktop Protocol (RDP) is used by Microsoft Windows Terminal Services applications, such as Remote Desktop. It is not used to provide security on wireless networks.

IPsec is an encryption and authentication mechanism designed to provide security for the TCP/IP protocol suite. It is often used on wireless networks to ensure data integrity and authenticity. Wi-Fi Protected Access (WPA) is a robust security protocol designed to provide additional security to wireless networks. WPA authenticates devices to the wireless network and provides encryption services to protect data as it travels across the wireless network.

802.1x is an authentication mechanism for wireless networks. 802.1x generally uses a Remote Authentication Dial-In User Service (RADIUS) server to authenticate users to the wireless network.

References

LabSim for Network Pro, Section 10.6.
[netpro18v5_all_questions_en.exm NP05_2-17 #58]