Exam Report: 5.11.6 Practice Questions

Date: 1/21/2020 2:24:22 pm
Time Spent: 13:07

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 67%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: 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?

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

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 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, 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

LabSim for Security Pro, Section 5.11.
[All Questions SecPro2017_v6.exm WIRELESS_ATTACKS_02]

Question 2: Correct

Which of the following best describes *Bluesnarfing*?

- Sending anonymous electronic business cards
- Executing commands on a mobile device
-

Cloning a mobile device

Viewing calendar, emails, and messages on a mobile device without authorization

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 to 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

LabSim for Security Pro, Section 5.11.
[All Questions SecPro2017_v6.exm WIRELESS_ATTACKS_05]

Question 3: Correct

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

Bluesnarfing

Bluebugging

Slamming

Bluejacking

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

LabSim for Security Pro, Section 5.11.
[All Questions SecPro2017_v6.exm WIRELESS_ATTACKS_06]

Question 4: Incorrect

Which of the following is the best protection to prevent attacks on mobile phones through the Bluetooth protocol?

Add a user account and strong password for Bluetooth access

Apply the latest patches and updates

Disable Bluetooth on the phone

~~Set the phone to non-discoverable mode~~

Explanation

The best method to protect against Bluetooth attacks is to disable Bluetooth on the device. If Bluetooth is required, then configure the device for non-discoverable mode. Applying the latest patches and updates also ensures that the device is protected against known vulnerabilities for which patches exist.

References

LabSim for Security Pro, Section 5.11.
[All Questions SecPro2017_v6.exm WIRELESS_ATTACKS_07]

Question 5: Incorrect

You are troubleshooting a wireless connectivity issue in a small office. You determine that the 2.4 GHz cordless phones used in the office are interfering with the wireless network transmissions.

If the cordless phones are causing the interference, which of the following wireless standards could the network be using? (Select two.)

- Infrared
- 802.11g
- 802.3a
- ~~802.11a~~
- Bluetooth

Explanation

Both the 802.11g and Bluetooth wireless standards use the 2.4GHz RF range to transmit data. Cordless phones that operate at the same frequency can cause interference on the wireless network. Other devices, such as microwaves and electrical devices, may also cause interference.

802.11a uses 5GHz radio frequency. Therefore, it would not be affected by the 2.4GHz phones used in the office. Infrared uses a light beam to connect computer and peripheral devices to create a personal area network (PAN).

References

LabSim for Security Pro, Section 5.11.
[All Questions SecPro2017_v6.exm WIRELESS_ATTACKS_08]

Question 6: Correct

Your organization uses an 802.11g wireless network. Recently, other tenants installed the following equipment in your building:

- A wireless television distribution system running at 2.4 GHz
- A wireless phone system running at 5.8 GHz
- A wireless phone system running at 900 MHz
- An 802.11n wireless network running in the 5 GHz frequency range

Since this equipment was installed, your wireless network has been experiencing significant interference. Which system is to blame?

- The wireless TV system
- The 802.11n wireless network
- The 5.8 GHz wireless phone system
- The 900 MHz wireless phone system

Explanation

Because the 802.11g standard operates within the 2.4 GHz to 2.4835 GHz radio frequency range, the most likely culprit is the wireless TV distribution system.

References

LabSim for Security Pro, Section 5.11.
[All Questions SecPro2017_v6.exm WIRELESS_ATTACKS_09]

Question 7: Correct

A user calls to report that she is experiencing intermittent problems while accessing the wireless network from her laptop computer. While she normally works from her office, today she is trying to access the wireless network from a conference room across the hall and next to the elevator.

What is the most likely cause of her connectivity problem?

- MAC filtering is preventing the computer from connecting.
- Interference is affecting the wireless signal.
- The client computer is using the wrong channel number.
- The user has not yet rebooted her laptop computer while at her new location.
- SSID broadcast has been disabled.

Explanation

In this scenario, interference from the elevator motor is the most likely cause. Cordless phones and motors can generate interference that affects wireless signals. Interference is a common cause of intermittent problems.

Windows clients automatically detect the channel to use. If the SSID had changed or MAC filtering were preventing access, the computer would not be able to connect at all, even from her office.

References

LabSim for Security Pro, Section 5.11.
[All Questions SecPro2017_v6.exm WIRELESS_ATTACKS_10]

Question 8: Correct

Which of the following best describes an *evil twin*?

- A threat agent that marks the outside of buildings to indicate the presence of a wireless network.
- An access point that is configured to mimic a valid access point to obtain logon credentials and other sensitive information.
- An access point that is added to the network by an internal employee to provide unauthorized network access.
- A Bluetooth device that receives mobile phone commands via bluebugging.

Explanation

An *evil twin* is a rogue access point that is configured to mimic a valid access point; in contrast, a *rogue access point* is *any* unauthorized access point added to a network. The evil twin may be 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.

War chalking is marking the outside of buildings to indicate the presence of a wireless network. Attackers might use these marks to alert others of open or secured wireless networks. Businesses might even use these marks to advertise free wireless networks. 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

LabSim for Security Pro, Section 5.11.
[All Questions SecPro2017_v6.exm WIRELESS_ATTACKS_11]

Question 9: Correct

Network packet sniffing is often used to gain the information necessary to conduct more specific and detailed attacks. Which of the following is the best defense against packet sniffing?

- Switches
- Hubs
- Promiscuous NICs
- Encryption

Explanation

Encryption provides the best protection from sniffing attacks. Technologies such as SSL, SSH, and IPSEC provide a level of protection beyond traditional network layout and design countermeasures.

Switches are frequently used to segment networks. Switches reduce the size of the shared media space and have long been regarded as the frontline defense against packet sniffing. Switched Ethernet does not, however, provide protection from advanced attacks, such as ARP redirection and cache poisoning.

Hubs provide no protection from packet sniffing. The shared media architecture broadcasts traffic to all hosts on the segment.

Network Interface Cards (NICs) in promiscuous mode are configured to see all packets on the local segment, regardless of source and destination. This mode is required for the proper operation of many packet-sniffing applications.

References

LabSim for Security Pro, Section 5.11.
[All Questions SecPro2017_v6.exm WIRELESS_ATTACKS_12]

Question 10: Correct

Which of the following common network monitoring or diagnostic activities can be used as a passive malicious attack?

- Denial of service
- Packet capture, edit, and re-transmission
- Sniffing
- Logic bombs

Explanation

Sniffing is a common network monitoring or diagnostic activity that can be used as a passive malicious attack. Sniffing is considered passive because it simply duplicates the packets it sees on the communication medium without altering or interfering with traffic flow. When performed properly, it is impossible to detect true passive sniffing on a network.

Denial of service and logic bombs are not common network monitoring and diagnostic activities, nor are they passive. Packet capture, edit, and retransmission can be a form of network monitoring and diagnostic activity, and a malicious attack, but it is not a passive activity.

References

LabSim for Security Pro, Section 5.11.
[All Questions SecPro2017_v6.exm WIRELESS_ATTACKS_13]

Question 11: Incorrect

Match the malicious interference type on the right with the appropriate characteristic on the left. Each characteristic can be used once, more than once, or not at all.

Spark Jamming

- Repeatedly blasts receiving equipment with high-intensity, short-duration RF bursts at a rapid pace

Random Noise Jamming

~~Uses radio signal pulses of random amplitude and frequency~~

Produces RF signals using random amplitudes and frequencies

Random Pulse Jamming

✓ Uses radio signal pulses of random amplitude and frequency

Explanation

Some interference is malicious in nature, designed to disrupt wireless network communications. Malicious interference is sometimes referred to as jamming. In a jamming attack, a transmitter is tuned to the same frequency as a wireless network and uses the same type of modulation. The jamming signal overrides the legitimate wireless network radio signals at the receiving devices. The following list describes different types of jamming signals that can be used to disrupt a Wi-Fi network:

- *Spark jamming* is the most effective type of Wi-Fi interference attack. It repeatedly blasts receiving equipment with high-intensity, short-duration RF bursts at a rapid pace. Experienced RF signal technicians can usually identify this type of attack quickly because of the regular nature of the signal.
- *Random noise jamming* produces radio signals using random amplitudes and frequencies. While not as effective as a spark attack, the random noise attack is harder to identify due to the intermittent jamming it produces and the random nature of the interference. In fact, this type of signal is frequently mistaken for normal background radio noise that occurs naturally.
- *Random pulse jamming* uses radio signal pulses of random amplitude and frequency to interfere with a Wi-Fi network.

References

LabSim for Security Pro, Section 5.11.
[All Questions SecPro2017_v6.exm WIRELESS_ATTACKS_14]

Question 12: Incorrect

An attacker has hidden an NFC reader behind an NFC-based kiosk in an airport.

The attacker uses the device to capture NFC data in transit between end user devices and the reader in the kiosk. She then uses that information to masquerade as the original end user device and establish an NFC connection to the kiosk.

What kind of attack has occurred in this scenario?

- NFC denial of services (DoS)
- NFC jamming
- NFC relay attack
- ~~NFC man-in-the-middle attack~~

Explanation

In this scenario, an *NFC relay attack* has occurred. NFC devices and readers are susceptible to relay attacks where the attacker captures NFC data in transit and then use that information to masquerade as the original device.

In NFC jamming, signals are jammed by malicious interference. In an NFC man-in-the-middle exploit, an attacker captures transmissions from the reader and then forwards them on to the device, potentially capturing or modifying data in transit. Currently, no NFC-based DoS-type attacks have been detected and identified.

References

LabSim for Security Pro, Section 5.11.
[All Questions SecPro2017_v6.exm WIRELESS_ATTACKS_15]

Question 13: Correct

You are implementing a wireless network in a dentist's office. The dentist's practice is small, so you choose to use an inexpensive consumer-grade access point.

While reading the documentation, you notice that the access point supports Wi-Fi Protected Setup (WPS)

using a PIN. You are concerned about the security implications of this functionality.

What should you do to reduce risk?

- ○ Require a complex PIN in the access point's configuration
- ○ Require a complex PIN in the configuration of each wireless device
- ○ Update the access point's firmware
- ➡ ◉ Disable WPS in the access point's configuration

Explanation

Because WPS automates the Wi-Fi association process, it is a target attackers can try to exploit to gain unauthorized access to the wireless network. The push-button, USB, and NFC WPS implementations are considered more secure because they require physical contact with the access point. However, WPS implementations that only require a PIN are susceptible to brute force attacks. For this reason, the best security practice is to disable WPS functionality in access points that support it.

There is no way to make a PIN more complex because the WPS standard specifies the use of an 8-digit number. Updating the device's firmware may or may not address the access point's vulnerability to WPS brute force attacks, depending upon the manufacturer. The only sure way to close the security hole is to disable the functionality altogether.

References

LabSim for Security Pro, Section 5.11.
[All Questions SecPro2017_v6.exm WIRELESS_ATTACKS_16]

Question 14: Incorrect

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
- ➡ ☐ Check the MAC addresses of devices connected to your wired switch
- ☐ Implement an intrusion prevention system (IPS)
- ➡ ☑ Conduct a site survey
- ☑ ~~Implement an intrusion detection system (IDS)~~

Explanation

A rogue host is an unauthorized system that has connected to a wireless network. It could be an unauthorized wireless device, or even 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, and rogue APs are internal threats. A NAC solution can be used to remediate clients that connect to the network, but it can't be used to detect a rogue AP.

References

LabSim for Security Pro, Section 5.11.
[All Questions SecPro2017_v6.exm WIRELESS_ATTACKS_17]

Question 15: Correct

Which of the following locations contributes the greatest amount of interference for a wireless access point? (Select two.)

- [x] Near backup generators
- [ ] In the top floor of a two-story building
- [x] Near cordless phones
- [ ] Near DCHP servers

Explanation

Other wireless transmitting devices (such as cordless phones or microwaves) and generators cause interference for wireless access points.

In general, place access points higher up to avoid interference problems caused by going through building foundations. DHCP servers provide IP information for clients and do not cause interference.

References

LabSim for Security Pro, Section 5.11.
[All Questions SecPro2017_v6.exm WIRELESS_ATTACKS_01]