Section Quiz

Candidate: Dunkan Gibson (dunkan.gibson)
Date: 3/15/2022 8:39:17 pm • Time spent: 02:41

Score: 80% Passing Score: 80%

▼ Question 1: ✓ Correct

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

- ○ Bluebugging
- ➡ ● Bluejacking
- ○ Bluesnarfing
- ○ 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 2:** ✓ 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 3: ✓ Correct

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

○ RFID

➡ ● EMI

○ RFI

○ NFC

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 4: ✓ Correct

Which of the following best describes an evil twin?

○ An access point that is added to a network by an internal employee to provide unauthorized network access.

○ A Bluetooth device that receives mobile phone commands via bluebugging.

➡ ● An access point that is configured to mimic a valid access point to obtain logon credentials and other sensitive information.

○ A threat agent that marks the outside of buildings to indicate the presence of a wireless network.

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.

Warchalking 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

8.2.2 Wireless Attack Facts

q_wl_attacks_evil_twin_secp7.question.fex

Question 5: ✓ Correct

Which type of attack is WEP extremely vulnerable to?

- ○ Evil twin
- ○ Bluesnarfing
- ➡ ● IV attack
- ○ Cloning

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 6: ✓ 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?

- ➡ ● Jamming
- ○ Cloning
- ○ Disassociation
- ○ Bluesnarfing

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 7: ✕ Incorrect

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?

- ○ Disassociation
- ○ Bluesnarfing
- ➡ ○ Relay
- ● ~~Cloning~~

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 8: ✗ Incorrect

Which type of RFID tag can send a signal over a long distance?

○ NFC

● ~~Bluetooth~~

○ Passive

➡ ○ Active

EXPLANATION

Active RFID tags have onboard batteries and can send signals over a long distance. Road toll passes and other types of passes use active RFID.

Passive RFID is not powered and relies on the energy of the scanner to transmit data. These tags are seen in ID badges, credit cards, and similar devices.

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

Bluetooth is designed to allow devices to communicate within a personal area network of close proximity.

REFERENCES

8.2.2 Wireless Attack Facts

q_wl_attacks_rfid_secp7.question.fex

▼ **Question 9:** ✓ 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?

➡ ● Rogue access point

○ Social engineering

○ Phishing

○ Man-in-the-middle attack

○ Physical security

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 10: ✓ 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.)

- ➡ ☑ Check the MAC addresses of devices connected to your wired switch.
- □ Implement a network access control (NAC) solution.
- □ Implement an intrusion detection system (IDS).
- ➡ ☑ Conduct a site survey.
- □ 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