Study Guide

Certified Ethical Hacking: Sniffing

# Checklist of Exam Objectives: Areas to Study

## Breakdown footprinting and reconnaissance to gain primary information about a potential target

### Review wireless networking concepts and types of wireless networks

### Review the process of protecting the wireless network from attacks using encryption standards

### Examine the types of security risks, threats, and attacks associated with wireless networks

### Compare wireless hacking tools

### Explore bluetooth hacking concepts, threats, and tools\*

### Examine wireless hacking countermeasures to prevent hacking attempts by threat actors

### 

### **Exam Essentials: What you need to know**

# Wireless networks are convenient, easy to use, and provide numerous benefits over traditional wired networks. Connectivity beyond walls, wireless connection, access to the internet even in locations where laying cables is difficult, and sharing are just a few of them. However, there are some drawbacks with wireless networks that should be considered before choosing one for your business.

**BSSID**

Basic Service Set Identifier (BSSID) - MAC address of the wireless access point

**SSID**

Service Set Identifier (SSID) - Is a name of a network; text word (<= 32 char) that identifies network; provides no security.

**ESSID**

Extended Service Set Identifier (ESSID) - An extended basic service set (ESS) is made up of all of the BSSs in the network. This is called a "ESSID." For the most part, the ESSID and the SSID are the same thing. Many people use the term SSID.

**Wireless Standards:**

| **Wireless Standard** | **Operating Speed (Mbps)** | **Frequency (GHz)** | **Modulation Type** |
| --- | --- | --- | --- |
| 802.11 | 3Mbps | 2.4Ghz | DSSS/FHSSS |
| 802.11a | 54 Mbps | 5 GHz | OFDM |
| 802.11b | 11 Mbps | 2.4 GHz | DSSS |
| 802.11g | 54 Mbps | 2.4 GHz | OFDM and DSSS |
| 802.11n | 600 Mbps | 2.4-5 GHz | OFDM |
| 802.11ac | 1000 Mbps | 5 GHz | QAM |
| 802.11ax | 14 Gps | 2.4 and 5 Ghz | QAM |

* **802.15.1** - Bluetooth
* **Basic Service Set (BSS)** - communication between a single AP and its clients
* **Orthogonal Frequency-Division Multiplexing (OFDM)** - carries waves in various channels.
* **Multiple-Input Multiple-Output (MIMO)** - Multiple antennas are used on both the transmitting and receiving sides to improve spectral efficiency by taking advantage of transmission and spatial diversity as well as multipath propagation.
* **ISM Band** - The ISM radio bands are parts of the radio spectrum that are used for industrial, scientific, and medical (ISM) purposes that are not used for telecommunications. People use radio frequency (RF) energy to do things like heat things with radio-frequency heating and microwave ovens, and heat things with medical diathermy machines.
* **Direct-Sequence Spread Spectrum (DSSS)** - Combines all available waveforms into a single purpose.
* **Frequency-hopping spread spectrum (FHSS)** – This is a way to send radio signals by quickly switching the carrier frequency between many different frequencies that make up a wide range of frequencies.
* **Spectrum Analyzer** - verifies the wireless quality, detects rogue access points, and detects attacks

**Authentication**

* **Types of Authentication**
  + **Open System** - no authentication
  + **Shared Key Authentication** - authentication through a shared key (password)
  + **Centralized Authentication** - authentication through something like RADIUS
* **Association** is the act of connecting; authentication is the act of identifying the client

**Antenna Types:**

**Omnidirectional antenna -** Signals go in every direction like a dome.

**Dipole antenna -** Goes in two directions.

**Directional antenna -** Long individual beam, increased distances.

**Yagi antenna -** Very directional and high gain.

**Parabolic antenna -** Focus the signal to a single point.

**Wireless Security**

**WEP - Wireless Equivalency Privacy**

* 64/128-bit RC4 ICV
* **RC4** - Rivest Cipher 4 Stream Cipher Algorithm

**WPA - Wi-Fi Protected Access**

Uses RC4 with TKIP (Temporal Key Integrity Protocol)

* + Initialization Vector (IV) is larger and an encrypted hash
  + Every packet gets a unique 128-bit encryption key
* **Personal | WPA-PSK**
  + TKIP + **PSK**
  + 64/128-bit **RC4 MIC**
  + Everyone uses the same 256-bit key
* **Enterprise | WPA-802.1X**
  + TKIP + **RADIUS**
  + 64/128-bit **RC4 MIC**
  + Authenticates users individually with an authentication server (e.g., RADIUS)

**TKIP - Temporal Key Integrity Protocol**

* Mixed the keys
  + Combines the secret root key with the IV
* Adds sequence counter
  + Prevents replay attacks
* Implements a 64-bit Message Integrity Check
  + Protecting against tampering
* TKIP has its own set of vulnerabilities
  + Deprecated in the 802.11-2012 standard

**WPA2 - Wi-Fi Protected Access v2**

* Enterprise
  + CCMP + **RADIUS**
  + 128-bit **AES MIC Encryption**
* Personal
  + CCMP + **PSK** (Pre-Shared Key)
  + 128-bit **AES MIC Encryption**
* AES (Advanced Encryption Standard) replaced RC4
* CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) replaced TKIP
* **CCMP**
  + Uses AES for data confidentiality
  + 128-bit key and a 128-bit block size
  + Requires additional computing resources
  + CCMP provides Data confidentiality (AES), authentication, and access control

**Wireless Attacks**

* **Rogue Access Point** - Unauthorized access point plugged into a wired one. (Could be accidental)
  + Tools for Rogue AP: Wi-Fi Pumpkin, Wi-Fi Pineapple, or Airegeddon
* **Evil Twin** - Is a Rogue AP that is broadcasting the same (or very similar) SSID.
  + Also known as a mis-association attack
* **Honeyspot** - faking a well-known hotspot with a rogue AP
* **Ad Hoc Connection Attack** - connecting directly to another phone via an Ad-hoc network
  + Not very successful as the other user must accept connection
* **DoS Attack** - either sends de-auth packets to the AP or jam the wireless signal
  + With a de-auth, you can have the users connect to your AP instead if it has the same name
  + Jammers are very dangerous as they are illegal
* **MAC Filter** - only allows certain MAC addresses on a network
  + Easily broken because you can sniff out MAC addresses already connected devices and spoof them.
  + Tools for spoofing include: **SMAC** and **TMAC**

**Wireless Encryption Attacks**

**WEP Cracking**

* To crack the WEP key for an access point, we need to gather lots of initialization vectors (IVs). Attackers can use injection to speed up the process by replaying packets

**Process:**

* 1. Start the wireless interface in monitor mode on the specific AP channel
  2. Test the injection capability of the wireless device to the AP
  3. Use aireplay-ng to do a fake authentication with the access point
  4. Start airodump-ng on AP channel with a BSSID filter to collect the new unique IVs
  5. Start aireplay-ng in ARP request replay mode to inject packets
  6. Run aircrack-ng to crack key using the IVs collected

**WPA/WPA2 Cracking**

* Uses a constantly changing temporal key and a user-defined password
* **Key Reinstallation Attack** (KRACK) - replay attack that uses the third handshake of another device's session
* Most other attacks are simply brute forcing the password
* **Process:**
  1. Start monitoring and find the BSSID
  2. Start monitoring only the BSSID with .cap output file
  3. The goal is to grab a WPA handshake; The attacker can wait to some client to connect to grab the handshake /or use a deauth attack to deauthenticate a client to make him/her connect again.
  4. Use aircrack-ng using a good wordlist to brute force the .cap file that you recorded on step 2.

**Tools:**

* **Aircrack-ng Suite** - is a complete suite of tools to assess WiFi network security.
  + **airodump-ng** - Airodump-ng is used for packet capturing of raw 802.11 frames and is particularly suitable for collecting WEP IVs (Initialization Vector).
  + **airmon-ng** - Used to enable monitor mode on wireless interfaces.
  + **aireplay-ng** - Is used to inject frames for arp replay or deauth attacks.
  + **aircrack-ng** – This is an WEP/WPA/WPA2-PSK key cracking program.
* **KisMAC** - MacOS tool to brute force WEP or WPA passwords
* **Fern WiFi Cracker**
* **WEPAttack**
* **WEPCrack**

**Bluetooth Attacks**

* **Bluesmacking** - Denial of service against device
* **Bluejacking** - Sending unsolicited messages
* **Bluebugging** - Remotely using a device's features
* **Bluesnarfing** - Theft of data from a device

**Wireless Sniffing**

Very similar to sniffing a wired network

* **Tools**
  + **NetStumbler**
  + **Kismet** - is a network detector, packet sniffer, and IDS for 802.11 wireless LANs.
  + **OmniPeek** - provides data like Wireshark in addition to network activity and monitoring
  + **AirMagnet WiFi Analyzer Pro** - sniffer, traffic analyzer and network-auditing suite

**Protecting Wireless Networks - Best practices**

Countermeasures:

* Always use WPA/WPA2 encryption.
* Do not share your credentials.
* Do not open untrusted emails.
* Use IDS/Firewalls to filter the connections.
* Change the default configurations.
* Enable MAC-address filtering.
* Use centralized server for authentication.
* Do not connect to untrusted/public Wi-Fi hotspots.

# **Self-Assessment Questions: Test your Understanding**

1)Which of the following are true statements? (Choose all that apply.)

**A.** WEP uses shared key encryption with TKIP.

**B.** WEP uses shared key encryption with RC4.

**C.** WPA2 uses shared key encryption with RC4.

**D.** WPA2 uses TKIP and AES encryption.

2) Which of the following best describes the “evil twin” wireless hacking attack?

**A.** Attackers sets up a system using the same MAC as an authorized target.

**B.** An attacker connects using the same username and password as an authorized user.

**C.** An attacker sets up an access point inside the network range for clients to connect to.

**D.** An attacker sets up an authentication server on the wireless network.

3) Bruce has turned off SSID broadcasting, enabled MAC filtering, and instituted wireless encryption. He notices someone using an HP laptop, and the organization purchases only Dell systems. Reviewing access logs and site survey information, Bruce determines there are no rogue access points, and all connection attempts in wireless appear to be valid. How did the person get onto the network with an HP laptop?

**A.** The employee has brute-forced the encryption.

**B.** The employee has spoofed a legitimate MAC address.

**C.** The laptop choice is irrelevant, as long as the OUI is the same.

**D.** An evil twin attack is in place.

4) An attacker is attempting to crack a WEP code to gain access to the network. After enabling monitor mode on wlan0 and creating a monitoring interface (mon 0), she types this command: “aireplay-ng -0 0 -a 0A:00:2B:15:22:AC -c mon0”. What is the attacker trying to do?

**A.** Gain access to the WEP access code by examining the response to deauthentication packets, which contain the WEP code

**B.** Use deauthentication packets to generate lots of network traffic

**C.** Determine the BSSID of the access point

**D.** Discover the cloaked SSID of the network

5) Which wireless standard is designed to work at 54Mbps on a frequency range of 2.4GHz?

**A.**802.11a

**B.**802.11b

**C.**802.11g

**D.**802.11n

**E**. 802.11ac

**F**. 802.11ax

6) The team has discovered an access point configured with WEP encryption. What is needed to perform a fake authentication to the AP to crack WEP? (Choose all that apply.)

A. A replay of a captured authentication packet

B. The IP address of the AP

C. The MAC address of the AP

D. The SSID

7) Which of the following statements are true regarding TKIP? (Choose all that apply.)

A. Temporal Key Integrity Protocol forces a key change every 10,000 packets.

B. Temporal Key Integrity Protocol ensures keys do not change during a session.

C. Temporal Key Integrity Protocol is an integral part of WEP.

D. Temporal Key Integrity Protocol is an integral part of WPA

8) Which of the following is true regarding wireless network architecture?

A. The service area provided by a single AP is known as an ESS.

B. The service area provided by a single AP is known as a BSSID.

C. The service area provided by multiple APs acting within the same network is known as an ESS.

D. The service area provided by multiple APs acting within the same network is known as an ESSID.

9) You are examining the physical configuration of a target’s wireless network. You notice on the site survey that omnidirectional antenna access points are in the corners of the building. Which of the following statements are true regarding this configuration? (Choose all that apply.)

A. The site may be vulnerable to sniffing from locations outside the building.

B. The site is not vulnerable to sniffing from locations outside the building.

C. The use of dipole antennas may improve the security of the site.

D. The use of directional antennas may improve the security of the site.

10) Which of the following is a true statement regarding wireless security?

A. WPA2 is a better encryption choice than WEP.

B. WEP is a better encryption choice than WPA2.

C. Cloaking the SSID and implementing MAC filtering eliminate the need for encryption.

D. Increasing the length of the SSID to its maximum increases security for the system.

11) Lois attempts to make a call using her cell phone; however, it seems unresponsive. After a few minutes of effort, she turns it off and turns it on again. During her next phone call, the phone disconnects and becomes unresponsive again. Which Bluetooth attack is underway?

A. Bluesmacking

B. Bluejacking

C. Bluesniffing

D. Bluesnarfing

# 12) Which wireless standard achieves high data rate speeds by implementing MIMO antenna technology?

# A. 802.11b

# B. 802.11g

# C. 802.11n

# D. 802.16

# Answers to Self-Assessment Questions:

1. B and D
2. C
3. B
4. B
5. C
6. C and D
7. A and D
8. C
9. A and D
10. A
11. A
12. C