Chapter 11 – Hacking Wireless Networks

Notes

Overview

This chapter provides an overview of wireless technology. You will learn about different wireless networking standards. Next, you will learn the process of authentication in relation to wireless networks. Wardriving and other wireless hacking techniques are also described. Finally, you will practice using the hacking tools that are utilized by hackers and security professionals to either attack or protect a wireless network.

Chapter Objectives

After reading this chapter and completing the exercises, you will be able to:

- Explain wireless technology
- Describe wireless networking standards
- Describe the process of authentication
- Describe wardriving
- Describe wireless hacking and tools used by hackers and security professionals

Tips

Understanding Wireless Technology

1. Understand the main components of a wireless network. For a wireless network to function, you must have the right hardware and software.

Components of a Wireless Network

1. The basic components of a wireless network: a wireless network interface card (WNICs), an access point (AP), wireless networking protocols, and a portion of the RF spectrum.

Access Points

1. An access point (AP) is a radio transceiver that connects to an Ethernet cable and that bridges the wireless LAN with the wired network. An AP enables users to connect to a LAN using wireless technology.

2. An AP is where RF channels are configured.

3. See how AP channels are detected in Figure 11-1.

Tip	Visit http://kb.netgear.com/app/answers/detail/a_id/235/~/what-is-a-wireless-access-point%3F?cid=wmt_netgear_organic for more information on access points (APs).

Service Set Identifiers

1. A service set identifier (SSID) is a name used to identify the wireless local area network (WLAN). The SSID is a unique one-to-32-character alphanumeric name that is configured on the AP.

2. Wireless computers need to configure the SSID before connecting to a wireless network.

3. It is not recommended to have default SSIDs configured on your company's APs. See Table 11-1 for the different default SSIDs used by several AP vendors.

Configuring an Access Point

1. Configuring an AP varies depending on the embedded OS. Configure a wireless router running dd-wrt. See Figures 11-3 through 11-5 for the configuration process.

2. Change the SSID and disable the SSID broadcast to better protect your WLAN.

Tip	Read https://heimdalsecurity.com/blog/home-wireless-network-security/ for tips for improving your wireless network.

Wireless NICs

1. Understand the role of a wireless NIC (WNIC) in a wireless network. For wireless technology to work, each node or computer must have a WNIC. It converts the radio waves it receives into digital signals the computer understands.

Understanding Wireless Network Standards

1. There are several standards defined by the Institute of Electrical and Electronic Engineers (IEEE) that apply to wireless networks.

2. Understand the process of creating, reviewing, and approving a new standard.

The 802.11 Standard

1. Understand the main characteristics of 802.11, the first wireless technology standard.

2. Understand carrier sense multiple access/collision avoidance (CSMA/CA) and why it is used on wireless networks instead of CSMA/CD.

Tip	The following Web page defines CSMA/CA and how it relates to WLANs: http://www.science.uva.nl/research/air/projects/old_projects/wlan/simulations/Intro_-_WLAN/Intro_-_CSMA_CA/intro_-_csma_ca.html.

3. Other terms of wireless LANs such as stations, mobile stations, and portable stations.

The Basic Architecture of 802.11

1. The main components of the 802.11 architecture are the basic service set (BSS), basic service area (BSA), distribution system (DS), and access point (AP).

2. Understand how data sent by one station moves between these three components to reach a second station.

3. Understand operating frequency range, frequency band, channels, wavelength, amplitude, frequency, cycle, Hertz, and bands.

An Overview of Wireless Technology

1. Techniques in which wireless LANs can operate:
   a. Infrared (IR)
   b. Narrowband
   c. Spread spectrum
      i. Frequency-hopping spread spectrum (FHSS)
      ii. Direct sequence spread spectrum (DSSS)
      iii. Orthogonal frequency division multiplexing (OFDM)

Additional IEEE 802.11 Projects

1. Understand the main characteristics of 802.11b – its operating frequency range, throughput, channels frequencies, and WEP.

2. Understand the main characteristics of 802.11a, – its operating frequency range, throughput, and bands or frequencies.

3. Understand the main characteristics of 802.11g – its operating frequency range, throughput, and modulation technique.

4. Understand the security improvements of 802.11i over 802.11b.

5. The improvements of 802.11e over 802.11b address the problem of interference.

6. The 802.11e standard that was released in 2005.

7. 802.11n uses the same frequency and encoding as 802.11g, but by using multiple antennas and wider bandwidth channels, throughput is increased to 600 Mbps.

8. The 802.11ac standard allows for higher throughput by multiplying the number of MIMO links and using high-density modulation.

9. The 802.11ad standard allows for transfer rates of up to 7 gigabits per second over the 2.4 GHz, 5 GHz, and 60 GHz bands.

Additional IEEE 802 Standards

1. 802.15 is a technique to address networking devices within one person's workspace. This is usually referred as wireless personal area networks (WPANs). Bluetooth is a good example of this technology.

2. 802.16 is the standard for wireless metropolitan area networks (MANs).

3. 802.20 is the standard that addresses wireless MANs for mobile users who are sitting in trains, subways, or cars traveling at speeds up to 150 miles per hour.

4. See Table 11-3 for the approved wireless standards.

Tip	Find more complete specifications about these standards at http://standards.ieee.org/getieee802/.

Understanding Authentication

1. This section explains several technologies to protect your wireless networks.

The 802.1X Standard

1. The 802.1X standard defines the process of authenticating and authorizing users on a WLAN. To understand how authentication can take place on a wireless network, explore some basic concepts such as:
    a. Point-to-Point Protocol (PPP)
    b. Extensible Authentication Protocol (EAP)
    c. Wired Equivalent Privacy (WEP)
    d. Wi-Fi Protected Access (WPA)
    e. Wi-Fi Protected Setup (WPS)

Point-to-Point Protocol (PPP)

1. Understand how PPP can be used to authenticate users.

Extensible Authentication Protocol (EAP)

1. EAP is an enhancement to PPP. The main difference between PPP and EAP is that with EAP, a company can select the authentication method to use, including certificates and Kerberos.

2. The methods used by EAP to protect wireless networks, include:
    a. Extensible Authentication Protocol-Transport Layer Security (EAP-TLS)
    b. Protected EAP (PEAP)
    c. Microsoft PEAP

3. The three 802.1X components that interact when authenticating a user include:
    a. Supplicant
    b. Authenticator
    c. Authentication server

Tip	Read RFC 2284: PPP Extensible Authentication Protocol (EAP) at http://www.faqs.org/rfcs/rfc2284.html.

Wired Equivalent Privacy

1. Wired Equivalent Privacy is part of the 802.11b standard and was implemented specifically to encrypt data that traversed a wireless network.

2. Understand the security problems related to WEP.

Wi-Fi Protected Access

1. WPA was introduced with the 802.11i standard to replace WEP, which was known to have many cryptographic problems. WPA improves encryption by using Temporal Key Integrity Protocol (TKIP).

2. The four enhancements introduced by TKIP, include:
    a. Message Integrity Check (MIC)
    b. Extended Initialization Vector (IV) with sequencing rules
    c. Per-packet key mixing
    d. Rekeying mechanism

Wi-Fi Protected Setup (WPS)

1. WPS is a wireless authentication standard created to allow users to easily add devices to a wireless network securely. A major security flaw was discovered in late 2011 that allows an attacker to gain access to a network remotely without knowing the WPA2 password.

Understanding Wardriving

1. Wardriving is driving around with inexpensive hardware and software that enables attackers to detect access points that haven't been secured.

2. Warflying is a variant of wardriving where an airplane is used to detect unsecured APs.

3. The equipment used by attackers or security testers when wardriving includes:
    a. Laptop computer
    b. Wireless NIC
    c. Antenna
    d. Software that scans the area for SSIDs

Tip	More on wardriving at http://compnetworking.about.com/cs/wireless/g/bldef_wardrive.htm

Vistumbler

1. Vistumbler is a freeware tool written for Windows that enables you to detect WLANs using 802.11a, 802.11b, and 802.11g.

2. Understand the main uses of Vistumbler, including its ability to interface with GPS.

3. All the information that can be logged by this tool:
    a. SSID
    b. MAC address of the AP
    c. Manufacturer of the AP
    d. Channel on which the signal was heard
    e. Strength of the signal
    f. Encryption

Kismet

1. Kismet is another wardriving tool written by Mike Kershaw.

2. Kismet runs on Linux, BSD UNIX, MAC OS X, and Linux PDAs.

3. Kismet is more than just a wireless network detector.

4. Features available with Kismet include:
   a. Wireshark- and Tcpdump-compatible data logging
   b. Compatible with AirSnort and AirCrack
   c. Network IP range detection
   d. Hidden network SSID detection
   e. Graphical mapping of networks
   f. Client-server architecture
   g. Manufacturer and model identification of APs and clients
   h. Detection of known default access point configurations
   i. XML output
   j. Supports more than 25 card types

Understanding Wireless Hacking

1. The following sections describe some additional tools that attackers use. They can also be used to conduct a security test.

Tools of the Trade

1. A wireless hacker usually has a laptop computer, a WNIC, an antenna, sniffers (Tcpdump or Wireshark, for example), tools such as Vistumbler or Kismet, and lots of patience.

Aircrack-ng

1. Aircrack-ng is the tool most hackers use who want to access WEP-enabled WLANs.

2. Aircrack-ng replaced AirSnort. It has some useful add-ons, such as a GUI front-end called Fern WiFi Cracker.

Tip	See http://www.aircrack-ng.org for more information on Aircrack-ng.

WiFi Pineapple

1. A WiFi Pineapple can perform scans for wireless APs and can set up fake APs to social-engineer users. It has a dangerous feature that allows an attacker to emulate any network that a client requests.

Countermeasures for Wireless Attacks

1. Countermeasures for wireless attacks are described in the book.

2. Use the Internet to find other recommendations for protecting wireless networks.

Additional Resources

1. Some Tips for Setting up Wireless Home Networks: http://harvest.cals.ncsu.edu/caat/index.cfm?pageID=1326

2. Top 10 Tips for Wireless Home Network Security: http://compnetworking.about.com/od/wirelesssecurity/tp/wifisecurity.htm

3. What is WPA2: http://compnetworking.about.com/od/wirelesssecurity/f/what-is-wpa2.htm

4. Hacking Techniques in Wireless Networks: http://www.cs.wright.edu/~pmateti/InternetSecurity/Lectures/WirelessHacks/Mateti-WirelessHacks.htm

5. Practically Networked, Securing Your Wireless Network: http://www.practicallynetworked.com/support/wireless_secure.htm

Key Terms

- **802.11**
- **802.1X standard**
- **access point (AP**)
- **ad-hoc network**
- **amplitude**
- **basic service area (BSA)**
- **basic service set (BSS)**
- **channels**
- **chipping code**
- **Extensible Authentication Protocol (EAP)**
- **frequency**
- **infrared (IR)**
- **infrastructure mode**
- **Institute of Electrical and Electronics Engineers (IEEE)**
- **metropolitan area networks (MANs)**
- **Mobile Broadband Wireless Access (MBWA)**
- **modulation**
- **narrowband**
- **Protected EAP (PEAP)**
- **service set identifier (SSID)**
- **spread spectrum**
- **station (STA)**
- **supplicant**
- **wardriving**
- **Wi-Fi Protected Access (WPA and WPA2)**
- **Wi-Fi Protected Setup (WPS)**
- **Wired Equivalent Privacy (WEP)**
- **wireless LAN (WLAN)**
- **wireless network interface cards (WNICs)**
- **wireless personal area network (WPAN)**
- **Worldwide Interoperability for Microwave Access (WiMAX)**