Wireless Attacks

Offensive Security
# Table of Contents

1. **IEEE 802.11**
   1.1 IEEE
   1.2 802.11 Standards and Amendments
      1.2.1 IEEE 802.11
      1.2.2 IEEE 802.11b
      1.2.3 IEEE 802.11a
      1.2.4 IEEE 802.11g
      1.2.5 IEEE 802.11n
      1.2.6 IEEE 802.11ac
      1.2.7 IEEE 802.11ad
      1.2.8 IEEE 802.11ax
      1.2.9 IEEE 802.11h
      1.2.10 802.11 Standard and Amendments Overview
   1.3 Antenna Diversity vs MIMO
      1.3.1 Antenna Diversity
      1.3.2 MIMO
   1.4 Wrapping Up

2. **Wireless Networks**
   2.1 Overview
   2.2 Infrastructure
   2.3 Wireless Distribution Systems
   2.4 Ad-Hoc Networks
      2.4.1 Ad-Hoc Demo
   2.5 Mesh Networks
   2.6 Wi-Fi Direct
   2.7 Monitor Mode
   2.8 Wrapping Up

3. **Wi-Fi Encryption**
   3.1 Open Wireless Networks
   3.2 Wired Equivalent Privacy
      3.2.1 RC4
      3.2.2 WEP Authentication
   3.3 Wi-Fi Protected Access
      3.3.1 WPA Ciphers
3.3.2 WPA Network Connection
3.3.3 WPA Authentication
3.4 Wi-Fi Protected Access 3
3.5 Opportunistic Wireless Encryption
3.6 Wireless Protected Setup
  3.6.1 WPS Architecture
  3.6.2 WPS Configuration Methods
  3.6.3 WPS Protocol
  3.6.4 WPS Registration Protocol Messages
3.7 802.11w
  3.7.1 Connection
  3.7.2 Security Association Teardown Protection
3.8 Wrapping Up

4 Linux Wireless Tools, Drivers, and Stacks
4.1 Loading and Unloading Wireless Drivers
4.2 Wireless Tools
  4.2.1 ifconfig and Other Utilities
  4.2.2 The iw Utility
  4.2.3 The rfkill Utility
4.3 Wireless Stacks and Drivers
  4.3.1 The ieee80211 Wireless Subsystem
  4.3.2 The mac80211 Wireless Framework
4.4 Wrapping Up

5 Wireshark Essentials
5.1 Getting Started
  5.1.1 Welcome Screen
  5.1.2 Packet Display
  5.1.3 Wireless Toolbar
  5.1.4 Saving and Exporting Packets
5.2 Wireshark Filters
  5.2.1 Wireshark Display Filters
  5.2.2 Wireshark Capture Filters
5.3 Wireshark at the Command Line
5.4 Remote Packet Capture
  5.4.1 Remote Packet Capture Setup
5.4.2 Built-in Wireshark

5.5 Advanced Preferences
  5.5.1 Coloring Rules
  5.5.2 Wireshark Columns
  5.5.3 Capture snaplen
  5.5.4 IEEE 802.11 Preferences
  5.5.5 WEP and WPA1/2 Decryption
  5.5.6 WLAN Statistics

5.6 Wrapping Up

6 Frames and Network Interaction
  6.1 Packets vs Frames
  6.2 802.11 MAC Frames
    6.2.1 MAC Header
  6.3 Frame Types
    6.3.1 Management Frames
    6.3.2 Control Frames
    6.3.3 Data Frames
  6.4 Interacting with Networks
    6.4.1 Open Network
    6.4.2 WEP
    6.4.3 EAPoL
  6.5 Wrapping Up

7 Aircrack-ng Essentials
  7.1 Airmon-ng
    7.1.1 Airmon-ng check
    7.1.2 Airmon-ng start
    7.1.3 Airmon-ng stop
  7.2 Airodump-ng
    7.2.1 Airodump-ng Usage
    7.2.2 Sniffing with Airodump-ng
    7.2.3 Precision Sniffing
    7.2.4 Airodump-ng Output Files
    7.2.5 Airodump-ng Interactive Mode
    7.2.6 Airodump-ng Troubleshooting
  7.3 Aireplay-ng
7.3.1 Aireplay-ng Replay Options
7.3.2 Aireplay-ng Injection Test
7.3.3 Aireplay-ng Troubleshooting
7.4 Aircrack-ng
7.4.1 Aircrack-ng Benchmark
7.5 Airedecap-ng
7.5.1 Removing Wireless Headers
7.6 Airgraph-ng
7.6.1 Clients to AP Relationship Graph
7.6.2 Clients Probe Graph
7.7 Wrapping Up
8 Cracking Authentication Hashes
8.1 Aircrack-ng Suite
8.2 Custom Wordlists with Aircrack-ng
8.2.1 Using Aircrack-ng with John the Ripper
8.2.2 Editing John the Ripper Rules
8.2.3 Using Aircrack-ng with JTR
8.2.4 Using Aircrack-ng with Crunch
8.2.5 Using Aircrack-ng with RSMangler
8.3 Hashcat
8.3.1 OpenCL for GPUs
8.3.2 Device Properties
8.3.3 Hashcat Benchmark
8.3.4 Hashcat Utilities
8.3.5 Passphrase Cracking with Hashcat
8.4 Airolib-ng
8.4.1 Using Airolib-ng
8.5 coWPAtty
8.5.1 Rainbow Table Mode
8.6 Wrapping Up
9 Attacking WPS Networks
9.1 WPS Technology Details
9.2 WPS Vulnerabilities
9.3 WPS Attack
9.3.1 Implementation Variations
9.3.2 Overcoming Unexpected Errors
9.4 Wrapping Up

10 Rogue Access Points
10.1 The Basics of Rogue APs
10.2 Discovery
10.3 Creating a Rogue AP
   10.3.1 Building the hostapd-mana Configuration
   10.3.2 Capturing Handshakes
10.4 Wrapping Up

11 Attacking WPA Enterprise
11.1 Basics
11.2 PEAP Exchange
11.3 Attack
11.4 Wrapping Up

12 Attacking Captive Portals
12.1 Basic Functionality
12.2 The Captive Portal Attack
   12.2.1 Discovery
   12.2.2 Building the Captive Portal
   12.2.3 Networking Setup
   12.2.4 Setting Up and Running the Rogue AP
12.3 Additional Behaviors Surrounding Captive Portals
12.4 Wrapping Up

13 bettercap Essentials
13.1 Installation and Executing
13.2 Modules vs. Commands
13.3 Wi-Fi Module
   13.3.1 Discovering APs
   13.3.2 Deauthenticating a Client
13.4 Additional Methods of Interacting with Bettercap
   13.4.1 Caplets
   13.4.2 Web Interface
13.5 Wrapping Up

14 Kismet Essentials
14.1 Installation
14.2 Configuration Files
   14.2.1 Output Files
   14.2.2 Data Sources
14.3 Starting Kismet
14.4 Web Interface
   14.4.1 Securing the Web Interface
14.5 Remote Capture
14.6 Log Files
   14.6.1 Reading Log Files
14.7 Exporting Data
   14.7.1 Pcap
   14.7.2 JSON
14.8 Wrapping Up
15 Determining Chipsets and Drivers
   15.1 Determining the Wireless Chipset
   15.2 Determining the Wireless Driver
   15.3 Example: Alfa AWUS036AC
16 Manual Network Connections
   16.1 Connecting to an Access Point
   16.2 Setting up an Access Point
      16.2.1 Internet Access
      16.2.2 Static IP on Access Point Wireless Interface
      16.2.3 DHCP Server
      16.2.4 Routing
      16.2.5 Access Point Mode