Chapter 7 Wireless Network Hacking

Wireless Hacking

- Types
  - Access Control Attacks
  - Integrity Attacks
  - Confidentiality Attacks
  - Availability Attacks
  - Authentication Attacks
- Tools
  - NetStumbler
  - Aircrack
  - AirPcap
  - WiGLE
  - Wireshark
  - Kismet
  - WiFi Analyzer Pro
  - AirMagnet
  - Omnipeek
  - tcpdump
  - Korek
  - Cain Abel
- Wardriving
  - Drive Car Using WiFi Device and Register Wireless APs
- Attacks
  - Rogue AP/Evil Twin
    - SSID Matching Original AP
    - Faking a Legit AP
    - Honeyspot
  - Ad Hoc Connection
    - Advertise Connection with Laptop
  - aLTEr Attack
    - Place Virtual Tower Between 2 LTE Devices
  - Denial-of-Service
    - Send De-Auth Packets
    - Jam WiFi Signal (Interference)
  - MAC Spoofing
    - Bypass ACLs

Wireless Encryption

- WEP
  - Wired Equivalent Privacy
  - 40 to 232 Bit Keys
  - "Encryption"
    - RC4 Algorithm
    - 40-bit Key
    - 64-bit Version
    - 104-bit Key
    - 128-bit Version
    - 232-bit Key
    - 256-bit Version
  - Initialization Vector (IV)
  - 32-bit Integrity Check Value (ICV) Append to End of Payload
  - 24-bit IV Combined with Key to Input on RC4
  - CRC32 Integrity Check
  - Attack
    - Generate Enough Packets
    - Inspect IVs
    - Identify Key Used
    - Decrypt WEP Key On-the-Fly
- WPA
  - Wifi Protected Access
  - Encryption
    - RC4
    - Temporal Key Integrity Protocol (TKIP)
    - WPA Changes Key Every 10.000 Packets
    - 128-bit Key
    - 48-Bit IV
    - Client MAC Address
  - Integrity
    - Message Integrity Code (MIC)
  - Keys Transferred via Extensible Auth Protocol (EAP)
    - Sessions
    - 4-Step Handshake
- WPA2
  - Enterprise
    - EAP or RADIUS Server
    - Allow Kerberos Tickets
  - Personal
    - Pre-shared Key
  - Properties
    - AES for Encryption
    - Cipher Block Chaining Message Authentication Code Protocol (CCMP)
    - MICs, CBC-MAC
    - 48-Bit IV
    - 128 Key
    - Integrity Hashes
    - FIPS 140-2 compliance
  - Hole196 Vulnerability
    - MitM
    - DoS
  - KRACK Attack
    - WPA2 Disconnections May Occur On Handshake
    - WPA2 Allow Reconnection Using Same Value for 3rd Handshake
    - Attacker May Send Repeatedly 3rd Handshake of Another Device Session
    - Manipulate or Reset WPA2 Encryption Key
  - Tools
    - Aircrack
    - KisMAC
- WPA3
  - Personal
    - AES-GCMP-256 (Encryption)
    - HMAC-SHA-384 (Authentication)
    - Dragonfly Key Exchange
    - Resistent to Offline and Key Recovery Attacks
  - Enterprise
    - Multiple Encryption Algorithms
    - ECDSA-384 for Key Exchange

Wireless Standards

- 802.11
  - a — 54 Mbps — 5 GHz — OFDM
  - b — 11 Mbps — 2.4 GHz — DSSS
  - d — Variation of a/b
  - e — QoS providing guidance for data and voice prioritization
  - g — 54 Mbps — 2.4 GHz — OFDM/DSSS
  - i — WPA/WPA2 Encryption
  - n — 100+ Mbps — 2.4/5 GHz — OFDM
- 802.15
  - .1 (Bluetooth) — 25/50 Mbps — 2.4 GHz
  - .4 (Zigbee) — 0.02/0.04/0.025 Mbps — 0.868/0.915/2.4 GHz
- 802.16 (WiMax) — 34/1000 Mbps — 2/11 GHz — SOFDMA
- Modulation
  - Manipulate Properties of Waveform
  - Encoding Method
- Orthogonal Frequency-Division Multiplex (OFDM)
- Direct-Sequence Spread Spectrum (DSSS)
- Network Setup
  - Ad Hoc Mode — Point-to-Point Network
  - Infrastructure Mode
    - Make Use of AP (Access Point)
    - Funnel All Wifi Connections Through AP
    - AP has Link to Internet

Wireless Concepts

- Basic Service Set (BSS)
  - Single Access Point — Basic Service Area (BSA)
  - AP <-> Clients
- Multiple AP
  - Setup Channels
  - Extended Service Set (ESS)
- Client Moves from AP to Another AP in Subnet
  - Deassociate
  - (Re)associate
  - Roaming
- Basic Service Set ID (BSSID) — MAC Address of AP
- Service Set ID (SSID)
  - 32 Char String
  - Name of Wireless Network
- Authentication
  - Open System
    - 802.11 Auth Frame
    - Contain SSID
  - Shared Key
    - Challenge/Request Scenario
    - AP Send Challenge Text
    - AP Verify Decrypted Key
  - Encryption
    - WEP
    - WPA/WPA2
  - Centralized (e.g. RADIUS)

Wireless Antennas

- Omnidirection Antenna
  - 360 Degrees
  - Same Signal Strength
- Directional Antenna (Yagi)
  - Focus Signal in Direction
  - Increase Signal Strength and Distance
- Cantenna (Pringles Can) — Directional Home-made
- Dipole
  - Two Signal Towers
  - Omnidirectional
- Parabolic Grid
  - Satellite Dishes
  - Great Range (Up to 10 miles)
- Loop Antenna
  - Circle
  - Directional
- Spectrum Analyzer
  - Wireless Quality
  - Detect Rogue AP
  - Detect Various Attacks