

- Filename: eccouncil-ceh31250-v12-16-1-1-wireless-basics.md
- Show Name: CEHv12 (312-50)
- Topic Name: Wireless Network Hacking - Hacking Wireless Networks
- Episode Name: Wireless Basics

=====

Wireless Basics

Objectives:

- Wireless features
 - AP (Access Point)
 - WLAN (Wireless Local Area Network)
 - BSSID (Basic Service Set Identifier)
 - MAC address of the AP
 - SSID (Service Set Identifier)
 - The 'name' of the AP
 - Maximum length of 32 bytes
 - Association
 - Connecting to an AP
- Wireless Standards
 - 802.11 is the main standard
 - 802.11a
 - 5Ghz
 - 35-100 meters
 - 54 Mbps
 - 802.11b
 - 2.4Ghz
 - 35-140 meters
 - 11 Mbps
 - 802.11g
 - 2.4Ghz
 - 38-140 meters
 - 54 Mbps
 - 802.11n
 - 2.4Ghz | 5Ghz
 - 70-250 meters
 - 54 -600 Mbps
- Authentication Types
 - Open
 - Any device can 'authenticate' or associate with the AP
 - Pre-Shared Key
 - Basically a password
 - Centralized Authentication
 - RADIUS server
- Types of antenna
 - Directional
 - Yagi (UHF/VHF)

- Omnidirectional
- Parabolic Grid (grid meaning 'what the dish material is made of')
- Reflector
 - Reflects and concentrates EM radiation
- Wireless Encryption
 - WEP
 - 24-bit static IV
 - Sent in cleartext
 - RC4 (Rivest Cypher 4)
 - The IV makes up part of the encryption key
 - 40 - 104 bit length
 - CRC-32
 - No cryptographic integrity protection
 - WPA
 - 48-bit IV
 - RC4 + TKIP (Temporal Key Integrity Protocol)
 - Generates new key for each packet
 - 128 bit length
 - Predictable Group Temporal Key(GTK)
 - From an insecure Random Number Generator
 - Allows for injection and decryption of traffic
 - Password cracking
 - WPA2
 - 48-bit IV
 - AES-CCMP
 - Counter Mode Cypher Block Chaining Message Authentication Code Protocol
 - 128 bits
 - 2 modes
 - Personal
 - Uses PSK
 - Enterprise
 - Uses centralized authentication
 - WPA3
 - AES-GCMP 256
 - Galois/Counter Mode
 - 192 bit
 - Personal and Enterprise modes