- Filename: eccouncil-ceh31250-v10-16-1-1-wireless_hacking_concepts.md
- Show Name: CEHv10 (312-50)
- Topic Name: Attacks and Exploits
- Episode Name: Wireless Hacking Concepts
- Description: In this episode, Daniel and Zach discuss the pertinent concepts with regards to hacking wireless technologies. Here they start by building a wireless vocabulary including terms like BSSID, ESSID, ISM, MIMO, and FSSS, etc. Then they look at a few common wireless standards, authentication mechanisms, and antennas. Finally, they walk you through common encryption schemes like WEP, WPA, and WPA2.

==

Wireless Hacking Concepts

- **We live in a wireless world, but what specific things do we need to be knowledgable about in order to be ready for wireless hacking?**
    - Terms and Definitions associated with wireless tech
        - SSID
            - ESSID
                - Extended Service Set Identifier
                - Human readable "network name"
            - BSSID
                - Basic Service Set Identifier
                - MAC of AP (in infrastructure mode)
                - Randomly generated (in ad-hoc mode)
        - ISM band
            - Industrial, Scientific, and Medical
        - Access Point (AP)
        - Hotspot
        - MIMO
        - DSSS
        - FSSS
    - Standards
        - 802.11a/b/g/n
            - *DIAGRAM*
    - Authentication
        - Open
        - Shared Key
        - Centralized
            - RADIUS (Remote Authentication Dial-In User Service)
                - *DIAGRAM*
                - Utilizes EAP (Extensible Authentication Protocol)
                    1. Client request
                    2. AP send EAP request to Client
                    3. Client sends EAP response with Client identity
                    4. AP forwards Client's identity to RADIUS
                    5. RADIUS defines/sends auth mechanism to Client via AP
                    6. Client sends creds to RADIUS via AP
                    7. RADIUS authenticates Client creds, sends back auth key to AP, AP sends session key to Client
    - Antennas (*Search www for examples*)

  - Directional
    - Yagi
  - Omnidirectional
  - Bidirectional
    - Dipole
  - Parabolic
    - Satellite dish
- Encryption Schemes
  - Wired Equivalent Privacy (WEP)
  - Wifi Protected Access (WPA)
    - Stronger than WEP
      - TKIP (Temporal Key Integrity Protocol)
  - Wifi Protected Access 2 (WPA2)
    - Stronger than WPA and WEP
      - CCMP
      - Counter Mode with Cipher Block Chaining Message Authentication Code Protocol
        - AES (Advanced Encryption Standard)
      - Personal and Enterprise
        - Personal uses PSK
        - Enterprise uses EAP/RADIUS
          - Allows the use of...
            - Tokens
            - Kerberos