- Filename: eccouncil-ceh31250-v12-16-2-1-wireless-threats.md
- Show Name: CEHv12 (312-50)
- Topic Name: Wireless Network Hacking - Hacking Wireless Networks
- Episode Name: Wireless Threats
  ==========

Wireless Threats

Objectives:

- Authentication Attacks
    - Brute-force the password/PSK
- Rouge AP
    - Installed into target network allowing 'backdoor' access
- Evil Twin
    - Client mis-association
- Honeypot AP
    - Looks like a commonly trusted SSID
        - Coffee shop
        - Restaurants
- Soft AP (Soft as in Software)
    - Installed as malware
    - Malware turns device into AP allowing attacker to access internal resources
- Denial of Service Attacks
    - De-authentication attack
        - Attacker sends de-authentication frame
    - Disassociation attack
        - Attacker sends disassociation frame
    - Jamming
        - Cell and WiFi
- KRACK
    - Key Re-installation Attack (WPA/WPA2 vuln)
    - Performed by blocking message 3 of the 4-way handshake
        - AP will re-transmit M3 multiple times with the same nonce
            - This reuse will make the encryption susceptible to attack
    - Attacker creates a fake access point with same ESSID on a different channel
        - Attacker performs MITM attack
- Spoofing Client MAC
    - Bypass MAC filtering