

Crack WiFi WPA2 via Aircrack-ng

- Aircrack vs. WPA2

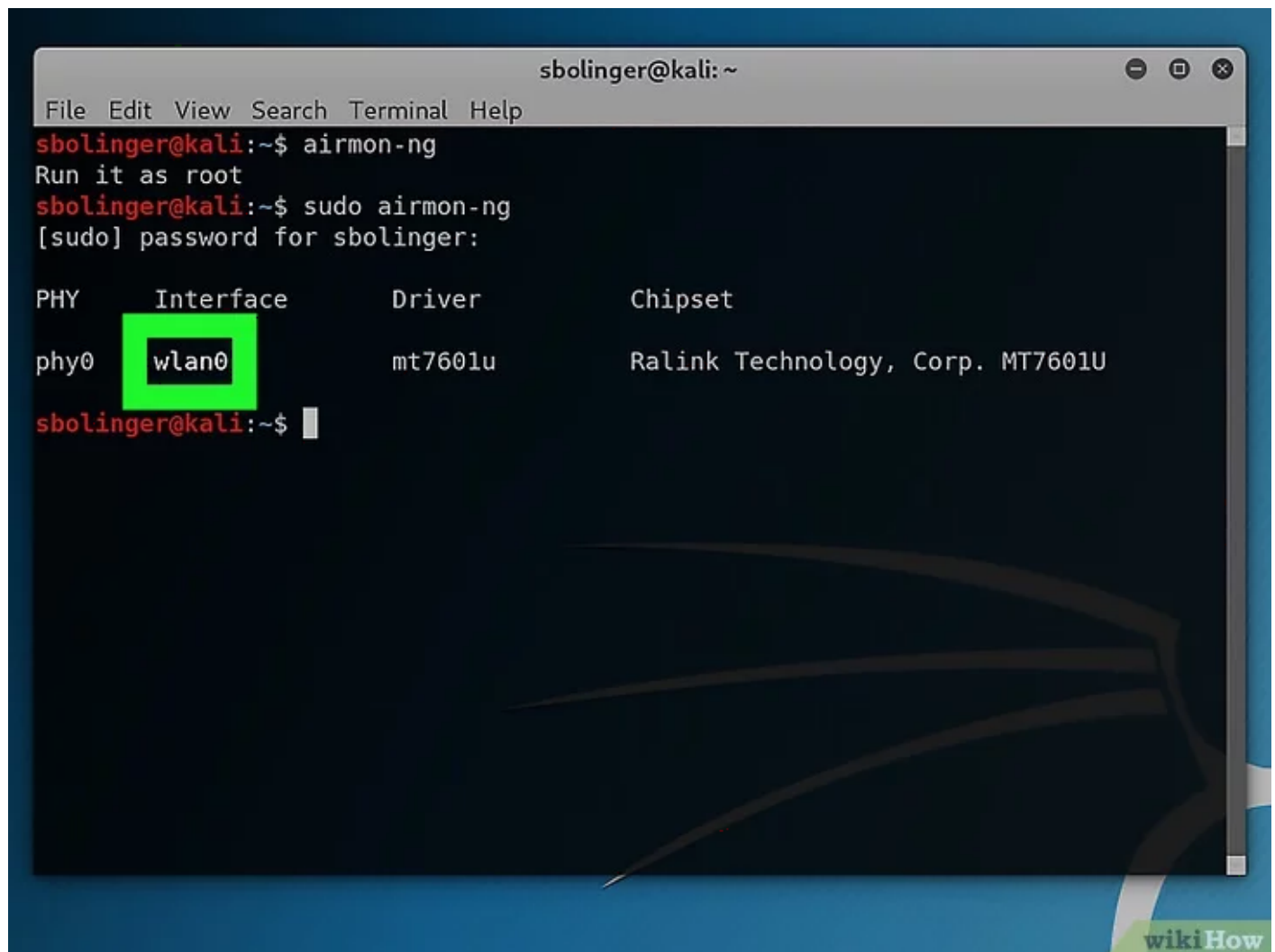
Aircrack vs. WPA2

Install Aircrack

```
sudo apt-get install aircrack-ng
```

Search for Wlan Adapters

```
sudo airmon-ng
```



```
sbolinger@kali:~$ airmon-ng
Run it as root
sbolinger@kali:~$ sudo airmon-ng
[sudo] password for sbolinger:

PHY      Interface      Driver      Chipset
phy0     wlan0           mt7601u     Ralink Technology, Corp. MT7601U
sbolinger@kali:~$
```

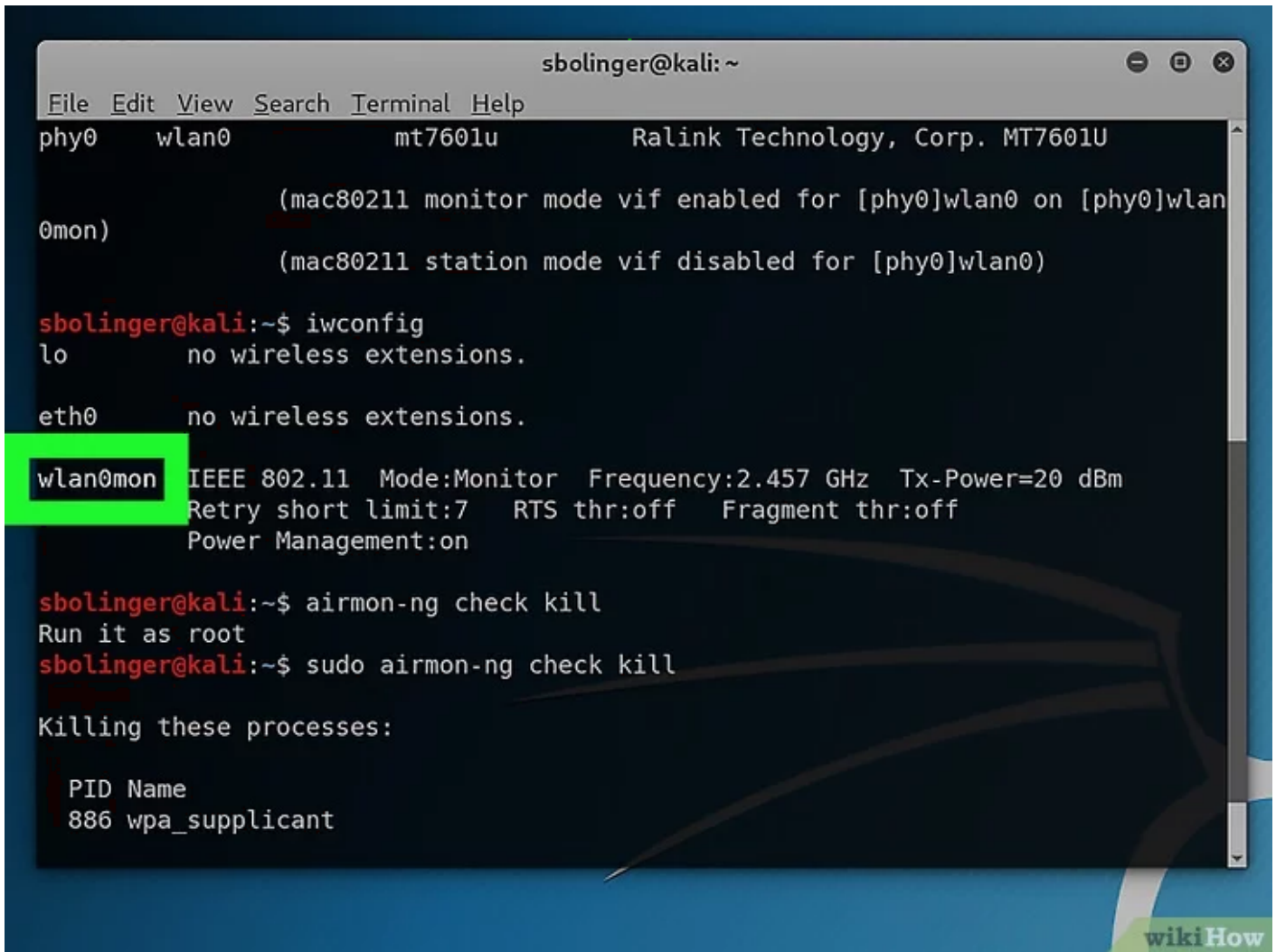
Enable Monitor Mode

```
sudo airmon-ng start wlan0
```

Kill all previous airmon processes

```
sudo airmon-ng check kill
```

Look out for the wireless monitor device

A terminal window titled 'sbolinger@kali: ~' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal shows the output of 'iwconfig' for phy0, wlan0, and eth0. wlan0 is in monitor mode. Then, 'airmon-ng check kill' is run, showing it should be run as root. Finally, 'sudo airmon-ng check kill' is run, showing it kills the wpa_supplicant process.

```
sbolinger@kali: ~  
File Edit View Search Terminal Help  
phy0      wlan0      mt7601u      Ralink Technology, Corp. MT7601U  
  
          (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan  
0mon)  
          (mac80211 station mode vif disabled for [phy0]wlan0)  
  
sbolinger@kali:~$ iwconfig  
lo          no wireless extensions.  
  
eth0        no wireless extensions.  
  
wlan0mon    IEEE 802.11 Mode:Monitor Frequency:2.457 GHz Tx-Power=20 dBm  
            Retry short limit:7 RTS thr:off Fragment thr:off  
            Power Management:on  
  
sbolinger@kali:~$ airmon-ng check kill  
Run it as root  
sbolinger@kali:~$ sudo airmon-ng check kill  
  
Killing these processes:  
  
PID Name  
886 wpa_supplicant
```

Exec airodump-ng with the Monitor device

```
sudo airodump-ng wlan0mon
```

work in progress