Create Wi-Fi Sniffer and Deauthenticator on Raspberry PI

I will need to revert my Raspberry PI to a USB ethernet device. Used sudo nano /boot/cmdline.txt and changed the line modules- load=dwc2,g hit to modules-load=dwc, g ether and pressed CRTL and X, then Y, and enter for save to file. Rebooted, and updated using sudo apt update && sudo apt upgrade -y.

I then installed the re4son-kernel to enable monitoring mode on the onboard Wi-Fi adapter.

After I had installed the kernel/rebooted, I was not able to access Wi-Fi any longer. I inserted looked at the micro SD card and put in a new ssh file and a new wpa_supplicant.conf. I plugged it back in and let it boot up, but I could not see it in the client list on my router. I looked at the microSD card again and saw that the ssh file and wpa_supplicant.conf had disappeared, so I figured that the raspberry pi Zero W just had not booted at all. The version was still 11 and not 10 and after it was reimaged, I could continue.

I connected the device, and it would not connect to WiFi. I looked at the client list and it was not there. I created a new ssh file and a new wpa supplicant.conf:

```
country=us

update_config=1

ctrl_interface=/var/run/wpa_supplicant


network={

ssid="[redacted]"

psk="[redacted]"

}
```

I had to delete the keys entered in the known hosts in my .ssh file under C:\\Users\[redacted]/.ssh/known_hosts and I was let in. I updated and upgraded using the command:

```
sudo apt update && sudo apt upgrade -y
```

This update took over 15 minutes.

I downloaded the re4son kernel, extracted it using tar -xjf re4son-kernel_current.tar.xz and installed using commands cd re4son-kernel_4* sudo ./install.sh and it took about 40 minutes, but this time when I rebooted, I was able to connect to WiFi.

I used command iw phy phy0 info to make sure the wireless adapter was placed in monitor mode and when looked for the list of modes supported, I saw that monitor was there.

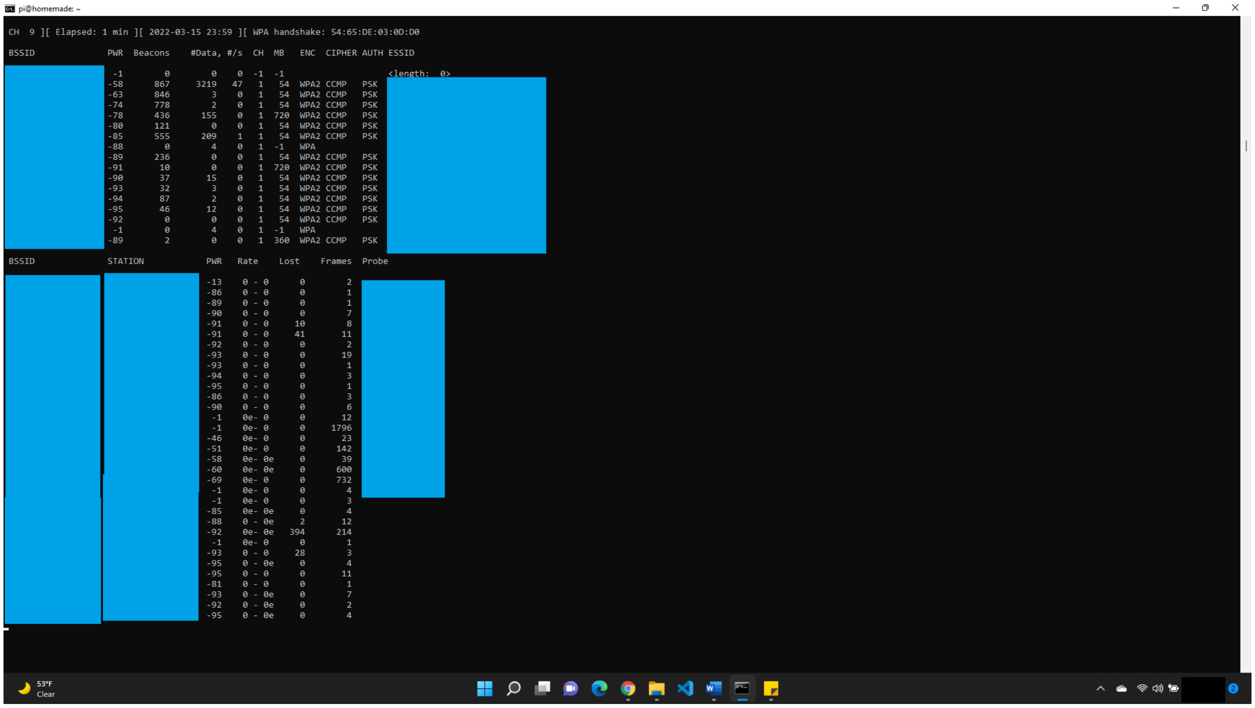
Since I did a reimage, I just added the following lines before the exit 0 line:

sudo iw phy phy0 interface add mon0 type monitor
sudo ifconfig mon0 up and I rebooted using: sudo reboot

I used the command sudo ifconfig mon0 to make sure mon0 still exists and saw mon in there.

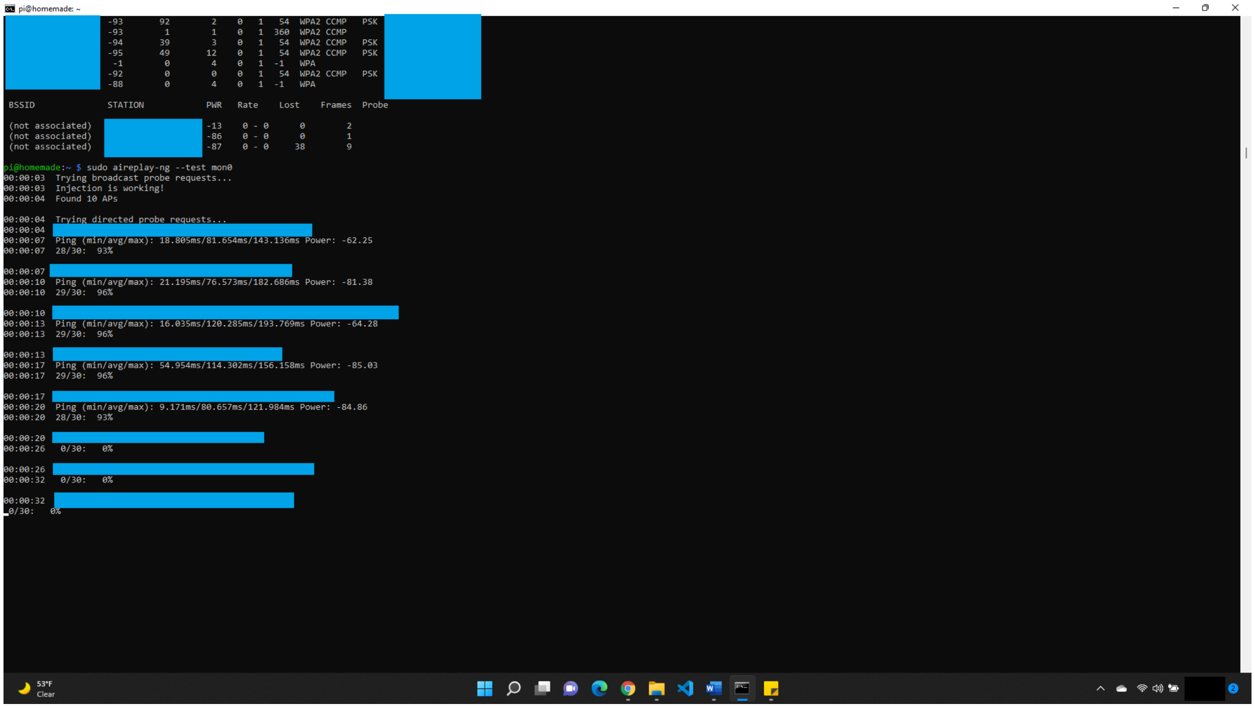
To install aircrack-ng I used the command: sudo apt install -y aircrack-ng

I tested the monitor mode by using the command sudo airodump-ng mon0:



```
CH  9 ][ Elapsed: 1 min ][ 2022-03-15 23:59 ][ WPA handshake: 54:65:DE:03:0D:D0

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

[redacted]          -1        0        0    0  -1  -1                   <length:  0>
                   -58      867     3219   47   1   54  WPA2 CCMP   PSK  [redacted]
                   -63      846        3    0   1   54  WPA2 CCMP   PSK
                   -74      778        2    0   1   54  WPA2 CCMP   PSK
                   -78      436      155    0   1  720  WPA2 CCMP   PSK
                   -80      121        0    0   1   54  WPA2 CCMP   PSK
                   -85      555      209    1   1   54  WPA2 CCMP   PSK
                   -88        0        4    0   1  -1   WPA
                   -89      236        0    0   1   54  WPA2 CCMP   PSK
                   -91       10        0    0   1  720  WPA2 CCMP   PSK
                   -90       37       15    0   1   54  WPA2 CCMP   PSK
                   -93       32        3    0   1   54  WPA2 CCMP   PSK
                   -94       87        2    0   1   54  WPA2 CCMP   PSK
                   -95       46       12    0   1   54  WPA2 CCMP   PSK
                   -92        0        0    0   1   54  WPA2 CCMP   PSK
                    -1        0        4    0   1  -1   WPA
                   -89        2        0    0   1  360  WPA2 CCMP   PSK

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

[redacted]         [redacted]         -13    0 - 0      0        2  [redacted]
                                      -86    0 - 0      0        1
                                      -89    0 - 0      0        1
                                      -90    0 - 0      0        7
                                      -91    0 - 0     10        8
                                      -91    0 - 0     41       11
                                      -92    0 - 0      0        2
                                      -93    0 - 0      0       19
                                      -93    0 - 0      0        1
                                      -94    0 - 0      0        3
                                      -95    0 - 0      0        1
                                      -86    0 - 0      0        3
                                      -90    0 - 0      0        6
                                       -1    0e- 0      0       12
                                       -1    0e- 0      0     1796
                                      -46    0e- 0      0       23
                                      -51    0e- 0      0      142
                                      -58    0e- 0e     0       39
                                      -60    0e- 0e     0      600
                                      -69    0e- 0      0      732
                                       -1    0e- 0      0        4
                                       -1    0e- 0      0        3
                                      -85    0e- 0e     0        4
                                      -88    0 - 0e     2       12
                                      -92    0e- 0e   394      214
                                       -1    0e- 0      0        1
                                      -93    0 - 0     28        3
                                      -95    0 - 0e     0        4
                                      -95    0 - 0      0       11
                                      -81    0 - 0      0        1
                                      -93    0 - 0e     0        7
                                      -92    0 - 0e     0        2
                                      -95    0 - 0e     0        4
```

I then performed an injection test by using the command sudo aireplay-ng –test mon0:



```
[redacted]  -93       92         2    0   1   54  WPA2 CCMP   PSK  [redacted]
            -93        1         1    0   1  360  WPA2 CCMP
            -94       39         3    0   1   54  WPA2 CCMP   PSK
            -95       49        12    0   1   54  WPA2 CCMP   PSK
             -1        0         4    0   1  -1   WPA
            -92        0         0    0   1   54  WPA2 CCMP   PSK
            -88        0         4    0   1  -1   WPA

 BSSID              STATION            PWR   Rate    Lost    Frames  Probe

 (not associated)   [redacted]         -13    0 - 0      0        2
 (not associated)                      -86    0 - 0      0        1
 (not associated)                      -87    0 - 0     38        9

pi@homemade:~ $ sudo aireplay-ng --test mon0
00:00:03  Trying broadcast probe requests...
00:00:03  Injection is working!
00:00:04  Found 10 APs

00:00:04  Trying directed probe requests...
00:00:04  [redacted]
00:00:07  Ping (min/avg/max): 18.805ms/81.654ms/143.136ms Power: -62.25
00:00:07  28/30:  93%

00:00:07  [redacted]
00:00:10  Ping (min/avg/max): 21.195ms/76.573ms/182.686ms Power: -81.38
00:00:10  29/30:  96%

00:00:10  [redacted]
00:00:13  Ping (min/avg/max): 16.035ms/120.285ms/193.769ms Power: -64.28
00:00:13  29/30:  96%

00:00:13  [redacted]
00:00:17  Ping (min/avg/max): 54.954ms/114.302ms/156.158ms Power: -85.03
00:00:17  29/30:  96%

00:00:17  [redacted]
00:00:20  Ping (min/avg/max): 9.171ms/80.657ms/121.984ms Power: -84.86
00:00:20  28/30:  93%

00:00:20  [redacted]
00:00:26   0/30:   0%

00:00:26  [redacted]
00:00:32   0/30:   0%

00:00:32  [redacted]
 0/30:   0%
```