ATTACK
DEFENSE
by PentesterAcademy

Name	SSID Sniffer (Raw Sockets)
URL	https://www.attackdefense.com/challengedetails?cid=1275
Type	WiFi Pentesting : Scapy-Fu

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Objective: Write python code to list SSIDs using Raw sockets.

Solution:

Step 1: Check the WiFi interfaces available on the machine.

Command: iw dev

There are two WiFi interfaces (i.e. wlan0 and wlan1) on the machine. Both are in monitor mode.

Step 2: Put wlan0 in monitor mode.

Command: iw dev wlan0 set monitor none

```
root@attackdefense:~# iw dev wlan0 set monitor none
root@attackdefense:~#
root@attackdefense:~# iw dev
phy#3
        Interface wlan1
                ifindex 7
                wdev 0x300000001
                addr 02:00:00:00:01:00
                type managed
                txpower 0.00 dBm
phy#2
        Interface wlan0
                ifindex 6
                wdev 0x200000001
                addr 02:00:00:00:00:00
                type monitor
                txpower 0.00 dBm
root@attackdefense:~#
```

The wlan0 interface is in monitor mode now. However, it is not UP yet.

Step 3: Enable the interface wlan0.

Command: ifconfig wlan0 up

```
root@attackdefense:~#
root@attackdefense:~# ifconfig wlan0 up
root@attackdefense:~#
```

After enabling the interface, the current channel of the interface should be visible.

```
root@attackdefense:~# iw dev
phy#3
        Interface wlan1
                ifindex 7
                wdev 0x300000001
                addr 02:00:00:00:01:00
                type managed
                txpower 0.00 dBm
phy#2
        Interface wlan0
                ifindex 6
                wdev 0x200000001
                addr 02:00:00:00:00:00
                type monitor
                channel 1 (2412 MHz), width: 20 MHz (no HT), center1: 2412 MHz
                txpower 20.00 dBm
root@attackdefense:~#
```

Currently the interface is not hopping channels. Hence, it will only capture packets from channel 1 (and neighbour channels due to the overlapping).

Step 3: One can either use airodump-ng to jump the channels or can do it manually using iw dev command.

Airodump-ng Command: airodump-ng wlan0

iw command: iw dev wlan0 set channel 2   (and similarly 3,4,5 … 14)

Step 4: Open another tab and check the contents of the present working directory.

Command: ls -l

```
root@attackdefense:~# ls -l
-rw-r--r--    1 root      root            847 Oct 23 04:23 ssid-sniffer-python-raw-sockets.py
root@attackdefense:~#
```

Step 5: Run the python script and wait for the output.

Command: python ssid-sniffer-python-raw-sockets.py

```
root@attackdefense:~# python ssid-sniffer-python-raw-sockets.py
SSID: EvilCorp  AP MAC: b80df76e795a
SSID: Home_Network  AP MAC: 6c198f5f8174
SSID: Home_Network  AP MAC: d2691037f594
SSID: XYZ-Enterprise  AP MAC: 6c5e3bd30310
```

In this manner, the SSID and BSSID list can be printed using raw socket code in Python.