

[illegible]

| | |
|-------------|---|
| Name | Scapy: All probes from a Client |
| URL | https://attackdefense.com/challengedetails?cid=1280 |
| 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 print the packet summary using scapy.

Solution:

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

Command: iw dev

```
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 managed
        txpower 0.00 dBm
```

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:~#
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      1082 Oct 23  2019 all-probes-from-same-client.py
root@attackdefense:~#

```

Step 5: This script takes two arguments

```
# Command arguments: <wlan_interface> <number_of_packets> <client_mac>
```

<interface_name> : Interface to be used for sniffing. Use “wlan0” here.

<number_of_packets> : Number of packets to sniff. Use a numeric value here, say 100.

<client_mac> : MAC of the client

Step 6: Run the python script and wait for the output.

Command: python all-probes-from-same-client.py wlan0 10000 5C:51:88:31:A0:3B

```
root@attackdefense:~# python all-probes-from-same-client.py wlan0 10000 5C:51:88:31:A0:3B
Probe Request - Client: 5c:51:88:31:a0:3b  SSID: ParleysElectronics
Probe Request - Client: 5c:51:88:31:a0:3b  SSID: Ruther_SSID
```

In this manner, the probes sent by a specific client can be printed.