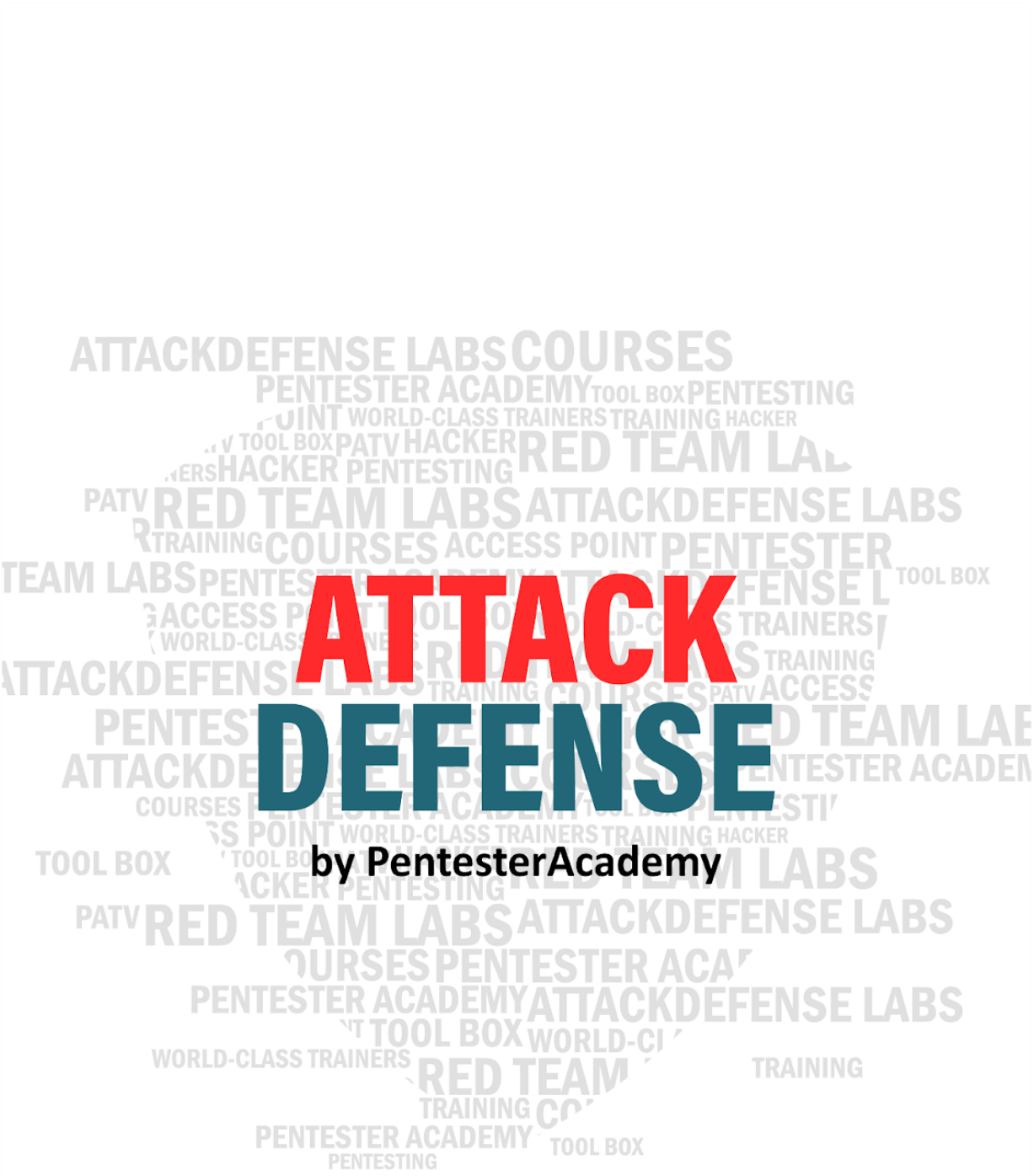
ATTACK
DEFENSE
by PentesterAcademy

Name	Scapy: SSID Sniffer
URL	https://www.attackdefense.com/challengedetails?cid=1283
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

```
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           959 Oct 23 04:23 ssid-sniffer.py
root@attackdefense:~#
```

Step 5: This script takes two arguments

```
# Command Arguments: <interface_name> <number_of_packets>
```

<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.

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

Command: python ssid-sniffer.py wlan0 100

```
root@attackdefense:~# python ssid-sniffer.py wlan0 100
Beacon Frame - BSSID: b8:0d:f7:6e:79:5a  SSID: EvilCorp
Beacon Frame - BSSID: 6c:19:8f:5f:81:74  SSID: Home_Network
```

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