ATTACK DEFENSE

by PentesterAcademy

Name	Parsing Beacons from PCAP
URL	https://www.attackdefense.com/challengedetails?cid=1273
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 using scapy to read the PCAP and print SSID list from Beacon frames.

Solution:

Step 1: Check the contents of current working directory (/root)

Command: ls -l

```
root@attackdefense:~# ls -l
-rw-r--r--    1 root     root          157259 Oct 23 04:01 capture.pcap
-rw-r--r--    1 root     root             938 Oct 23 04:01 parse-beacons-from-pcap.py
root@attackdefense:~#
```

There is a PCAP file and a Python script. The script will parse the beacon frames present in the PCAP and print the list of BSSIDs/SSIDs.

Step 2: Run the script

Command: python parse-beacons-from-pcap.py capture.pcap

```
root@attackdefense:~# python parse-beacons-from-pcap.py capture.pcap
Beacon Frame - BSSID: f4:f2:6d:47:1c:a6 SSID: Board room
Beacon Frame - BSSID: c8:3a:35:55:54:20 SSID: NWPUNE
Beacon Frame - BSSID: f4:f2:6d:46:dd:6a SSID: HIDER-2
Beacon Frame - BSSID: f0:92:1c:fc:de:52 SSID: HP-Print-52-Deskjet 3540 series
Beacon Frame - BSSID: 50:c7:bf:c8:2a:1b SSID: PA_NET
Beacon Frame - BSSID: 40:49:0f:b9:9d:96 SSID: HP-Print-96-LaserJet Pro MFP
Beacon Frame - BSSID: 20:a6:80:b7:53:3d SSID: Destek
Beacon Frame - BSSID: 74:da:da:17:da:ef SSID: eFinserve
Beacon Frame - BSSID: f4:f2:6d:46:d9:dc SSID: Mancer
Beacon Frame - BSSID: b0:e5:ed:c4:ea:18 SSID: Idea4G-SmrtWiFiHBEA18
Beacon Frame - BSSID: 20:e5:2a:44:28:88 SSID: webshar-pune
Beacon Frame - BSSID: f4:f2:6d:46:da:4a SSID: Coriant
Beacon Frame - BSSID: 5c:f9:6a:5a:2b:67 SSID: AIRTEL_E5172_2B67
Beacon Frame - BSSID: f4:f2:6d:4e:3a:aa SSID: KUMOLUS
Beacon Frame - BSSID: 00:17:7c:74:24:d5 SSID: JEBITECH
Beacon Frame - BSSID: c0:38:96:7e:a2:c7 SSID: DIRECT-iGHPmsNb
Beacon Frame - BSSID: a8:86:dd:b3:16:4f SSID: Neutron
Beacon Frame - BSSID: 76:29:af:fb:64:0f SSID: DIRECT-JCDESKTOP-J9MCMHSmsIX
Beacon Frame - BSSID: a6:e4:b8:90:d3:fe SSID: BlackBerry STV100-4 e74f
Beacon Frame - BSSID: 90:cd:b6:14:47:cb SSID: HP-Print-CB-LaserJet Pro MFP
Beacon Frame - BSSID: 60:e3:27:56:2b:18 SSID: Operation EFC
Beacon Frame - BSSID: f4:f2:6d:46:e5:ec SSID: VLMS
Beacon Frame - BSSID: f4:f2:6d:47:1e:76 SSID: EFC Tech Space
Beacon Frame - BSSID: 1c:5f:2b:9f:85:e2 SSID: Unit 16
root@attackdefense:~#
```

The list is printed by the script.