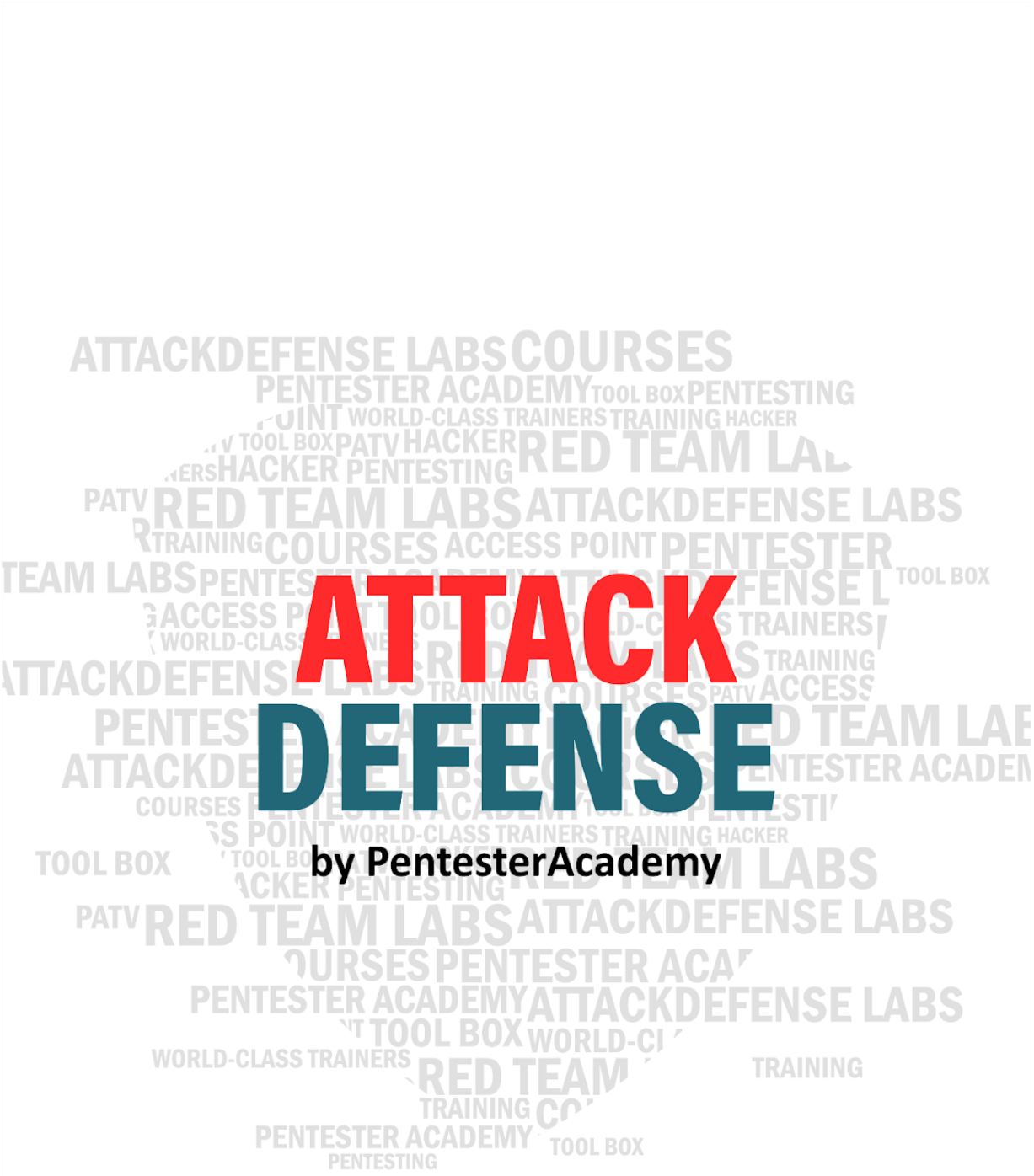
ATTACK
DEFENSE
by PentesterAcademy

Name	Tool: EAPHammer
URL	https://www.attackdefense.com/challengedetails?cid=1331
Type	WiFi Attack-Defense : WiFi Tools

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: Use Bettercap to perform the following tasks:

Q.1 Start WiFi recon mode and list all WiFi networks operating in the vicinity.

Solution:

Step 1: Check the list of available WiFi network interfaces on the machine

Command: iw dev.

```
root@attackdefense:~# iw dev
phy#1
        Interface wlan1
                ifindex 5
                wdev 0x100000001
                addr 02:00:00:00:01:00
                type managed
                txpower 0.00 dBm
phy#0
        Interface wlan0
                ifindex 4
                wdev 0x1
                addr 02:00:00:00:00:00
                type managed
                txpower 0.00 dBm
root@attackdefense:~#
```

wlan0 and wlan1 interfaces are present on the machine.

Step 2: Put wlan0 in monitor mode.

Command: iw dev wlan0 set monitor none

```
root@attackdefense:~# iw dev wlan0 set monitor none
```

```
root@attackdefense:~# iw dev
phy#1
        Interface wlan1
                ifindex 5
                wdev 0x100000001
                addr 02:00:00:00:01:00
                type managed
                txpower 0.00 dBm
phy#0
        Interface wlan0
                ifindex 4
                wdev 0x1
                addr 02:00:00:00:00:00
                type monitor
                txpower 0.00 dBm
root@attackdefense:~#
```

Step 3: Run bettercap on wlan0 interface.

Command: bettercap -iface wlan0

Command: wifi.recon on

```
root@attackdefense:~# bettercap -iface wlan0
bettercap v2.26.1 (built for linux amd64 with go1.13.3) [type 'help' for a list of commands]

 wlan0  » wifi.recon on
[00:21:34] [sys.log] [inf] wifi using interface wlan0 (02:00:00:00:00:00)
[00:21:34] [sys.log] [war] wifi could not set interface wlan0 txpower to 30, 'Set Tx Power' requests not supported
[00:21:34] [sys.log] [inf] wifi started (min rssi: -200 dBm)
 wlan0  » [00:21:34] [sys.log] [inf] wifi channel hopper started.
 wlan0  » [00:21:35] [wifi.ap.new] wifi access point EvilCorp (-30 dBm) detected as b8:0d:f7:6e:79:5a.
```

Step 3: Listing all APs

```
wlan0 » wifi.show
```

RSSI ▲	BSSID	SSID	Encryption	WPS	Ch	Clients	Sent	Recvd	Seen
-30 dBm	68:7f:77:c2:c2:9a	EvilCorp-covert	WPA2 (CCMP, PSK)		104				00:23:30
-30 dBm	b8:0d:f7:6e:79:5a	EvilCorp	WPA2 (CCMP, PSK)		1				00:23:46
-30 dBm	b8:0d:f7:83:79:bb	Forex_Magic	WPA (TKIP, PSK)		1				00:23:46
-30 dBm	b8:0d:f7:84:79:bd	TV-Store-99	WPA2 (CCMP, PSK)	2.0	3				00:23:36
-30 dBm	b8:0d:f7:d5:79:a9	Airport-Free-WiFi	OPEN		1				00:23:46
-30 dBm	b8:0d:f7:d5:79:f9	Ron_Home_WiFi	OPEN		6				00:23:38
-30 dBm	b8:67:e3:34:9a:4b	EvilCorp	WPA2 (CCMP, PSK)		11				00:23:40
-30 dBm	b8:67:e3:57:d6:5c	XYZ-Enterprise	WPA2 (CCMP, MGT)		11				00:23:40
-30 dBm	f2:a8:3e:c2:72:ac	EvilCorp	WPA2 (CCMP, PSK)		6				00:23:38
-30 dBm	f2:a8:3e:c2:9f:0c	<hidden>	OPEN		6				00:23:38

Q.2 Which network supports WPS? Also check out its details.

Solution:

From the BSSID/SSID list, it is clear that ‘TV-Store-99’ supports WPS.

The details can be viewed for it.

Command: wifi.show.wps all

```
wlan0 » wifi.show.wps all
```

Name	Value
essid	TV-Store-99
bssid	b8:0d:f7:84:79:bd
Config Methods	Label, Display, Keypad
Device Name	TV Store AP
Manufacturer	J-Link
Model Name	JL
Model Number	101
Primary Device Type	AP (oui:0050f204)
Response Type	AP
Serial Number	564378
State	Configured
UUID-E	876543219abcdef0123456789abc0000
Version	2.0