ATTACK DEFENSE

by PentesterAcademy

Name	Preferred Network List (PNL) Basics
URL	https://www.attackdefense.com/challengedetails?cid=1264
Type	Wi-Fi Attack-Defense : Reconnaissance

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.

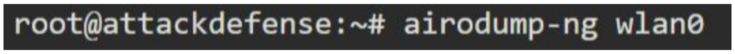
Q1: How many clients are probing?

Answer: 2

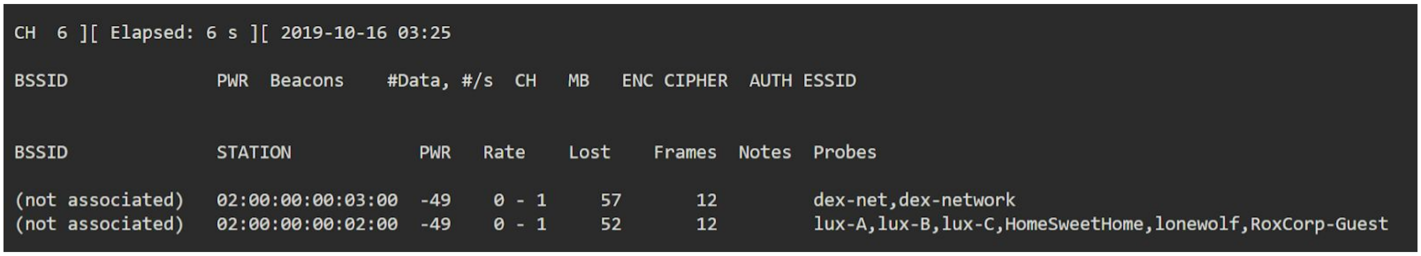
Solution:

Run airodump-ng on the interface wlan0 to view the WiFi activity.

Command: airodump-ng wlan0



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



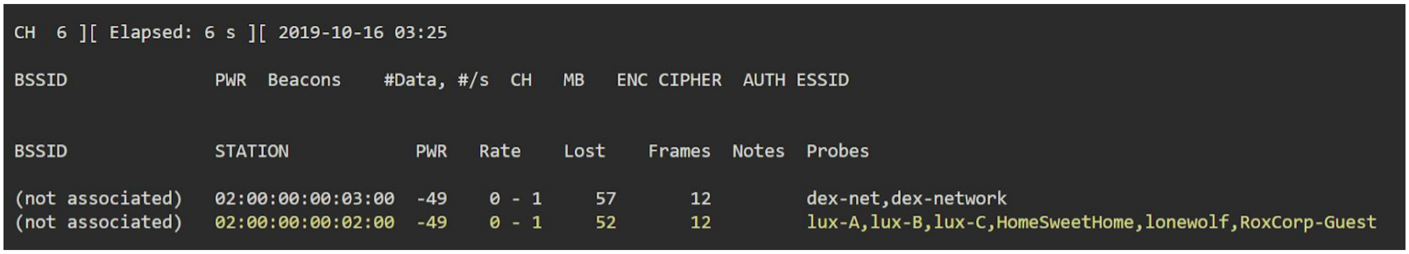
```
CH  6 ][ Elapsed: 6 s ][ 2019-10-16 03:25

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


BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

(not associated)   02:00:00:00:03:00  -49    0 - 1     57       12         dex-net,dex-network
(not associated)   02:00:00:00:02:00  -49    0 - 1     52       12         lux-A,lux-B,lux-C,HomeSweetHome,lonewolf,RoxCorp-Guest
```

Q2: What is the Preferred Network List (PNL) length of the client with MAC address 02:00:00:00:02:00?

Answer: 6

Solution:

From airodump-ng’s output, one can observe that there are 6 individual networks for which the client with MAC 02:00:00:00:02:00 is probing. Hence the list length is 6.



```
CH  6 ][ Elapsed: 6 s ][ 2019-10-16 03:25

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


BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

(not associated)   02:00:00:00:03:00  -49    0 - 1     57       12         dex-net,dex-network
(not associated)   02:00:00:00:02:00  -49    0 - 1     52       12         lux-A,lux-B,lux-C,HomeSweetHome,lonewolf,RoxCorp-Guest
```

Q3: The client 02:00:00:00:03:00 connects to which network first if all networks in its PNL are available? Assume that all networks in PNL are WPA2-PSK networks.

Answer: dex-network

Solution:

Deploy the honeypots for all networks present in PNL on the same channel and then observe to which SSID the client connects first.

Step 1: Create a Hostapd configuration file (i.e. honeypot.conf) for both SSIDs. It is mentioned in the question that both networks are WPA2-PSK in nature (In the absence of this information, one has to create honeypots with all possible security scenarios i.e. OPEN/WEP/WPA-PSK etc.)

Hostapd configuration:

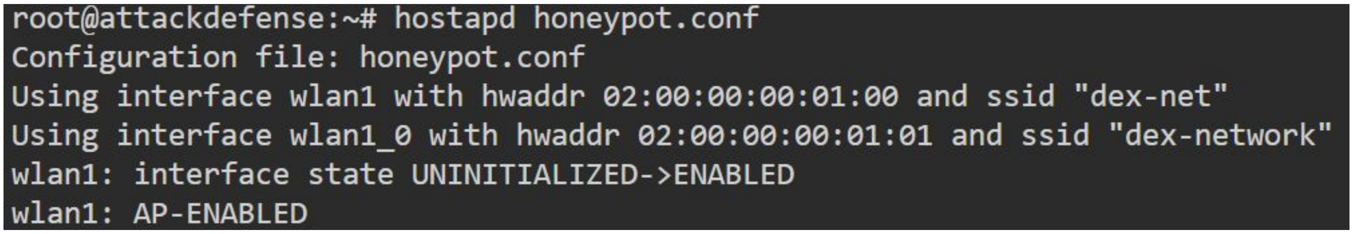
```
# SSID 1
interface=wlan1
driver=nl80211
ssid=dex-net
wpa=2
wpa_passphrase=123456789
wpa_key_mgmt=WPA-PSK
rsn_pairwise=CCMP
channel=1
```

```
# SSID 2
bss=wlan1_0
ssid=dex-network
wpa=2
wpa_passphrase=123456789
wpa_key_mgmt=WPA-PSK
rsn_pairwise=CCMP
channel=1
```

Please note that the secret passphrase given here is wrong (something chosen by the attacker who doesn’t know the real passphrase)

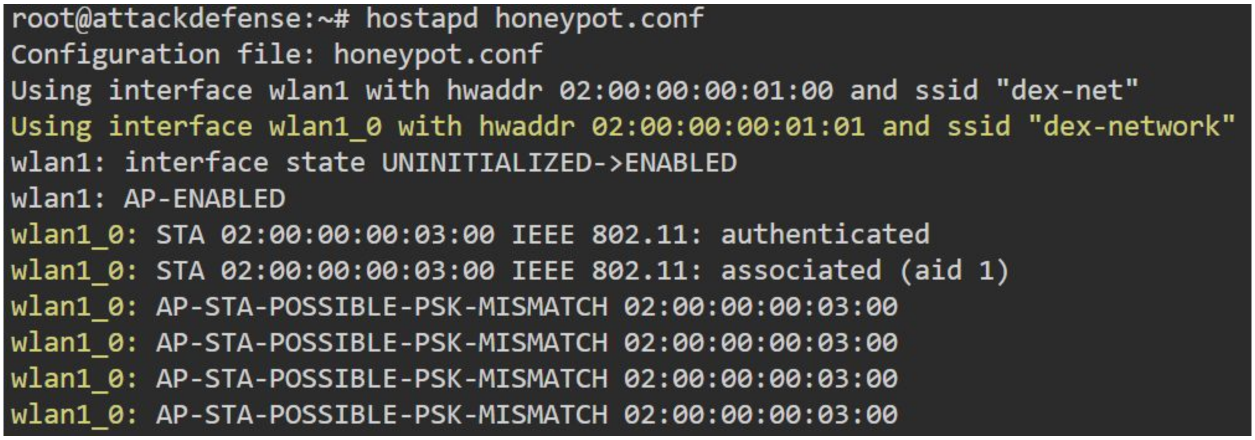
Step 2: Start the Hostpad with this configuration.

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 "dex-net"
Using interface wlan1_0 with hwaddr 02:00:00:00:01:01 and ssid "dex-network"
wlan1: interface state UNINITIALIZED->ENABLED
wlan1: AP-ENABLED
```

After a few seconds, the client should try to connect to these.



```
root@attackdefense:~# hostapd honeypot.conf
Configuration file: honeypot.conf
Using interface wlan1 with hwaddr 02:00:00:00:01:00 and ssid "dex-net"
Using interface wlan1_0 with hwaddr 02:00:00:00:01:01 and ssid "dex-network"
wlan1: interface state UNINITIALIZED->ENABLED
wlan1: AP-ENABLED
wlan1_0: STA 02:00:00:00:03:00 IEEE 802.11: authenticated
wlan1_0: STA 02:00:00:00:03:00 IEEE 802.11: associated (aid 1)
wlan1_0: AP-STA-POSSIBLE-PSK-MISMATCH 02:00:00:00:03:00
wlan1_0: AP-STA-POSSIBLE-PSK-MISMATCH 02:00:00:00:03:00
wlan1_0: AP-STA-POSSIBLE-PSK-MISMATCH 02:00:00:00:03:00
wlan1_0: AP-STA-POSSIBLE-PSK-MISMATCH 02:00:00:00:03:00
```

The client first tried to connect to wlan1_0 interface which is hosting “dex-network” SSID.