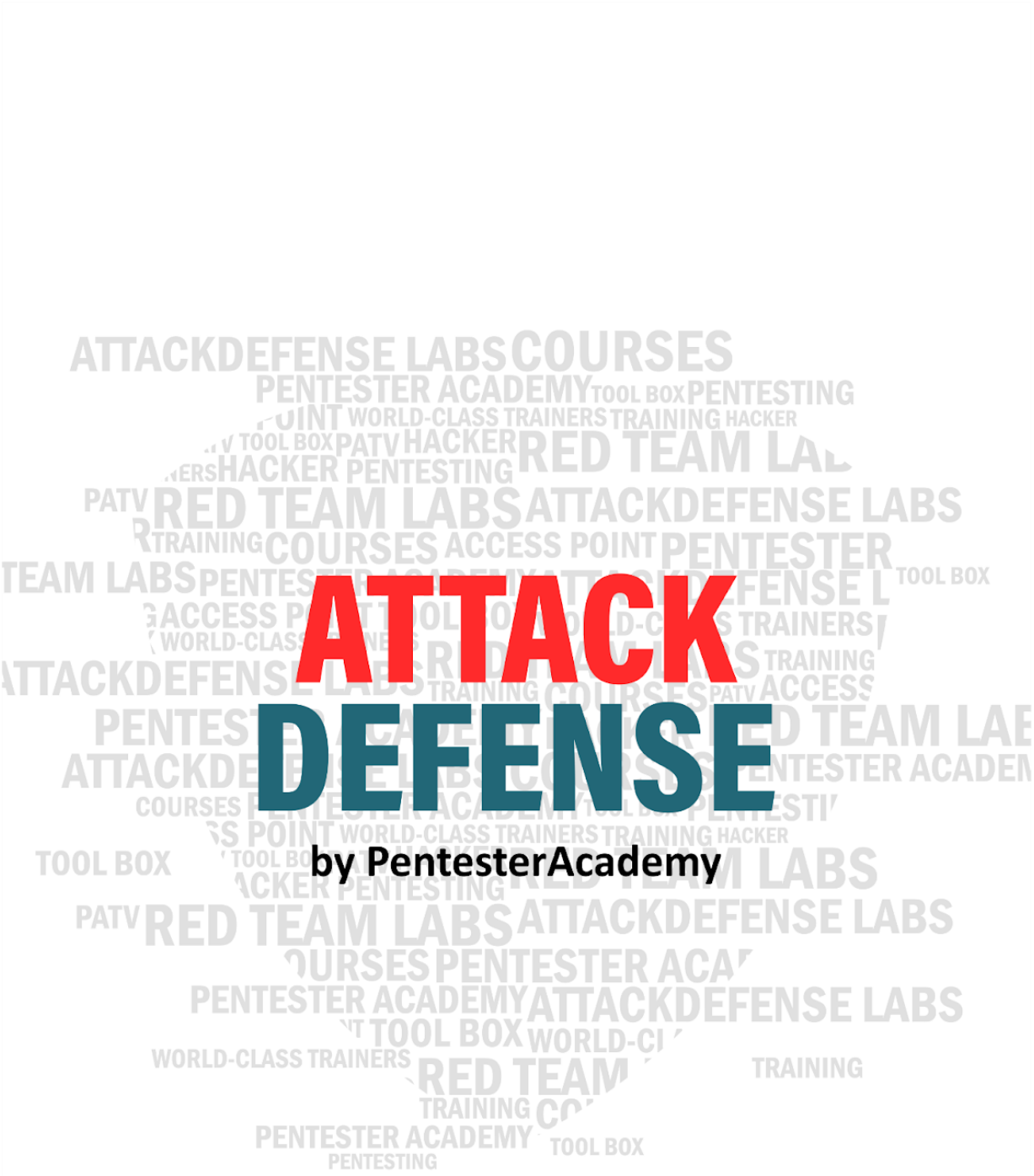
ATTACK
DEFENSE
by PentesterAcademy

Name	WPA Supplicant: Enhanced Open
URL	https://www.attackdefense.com/challengedetails?cid=1311
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: Connect to the Enhanced Open network using wpa_supplicant.

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  5 ][ Elapsed: 6 s ][ 2019-10-29 06:01

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

D2:E9:6A:D3:B3:50  -28       77        0    0   1   54   WPA3 CCMP   OWE  Secure-Public-WiFi

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes
```

There is an Enhanced Open network “Secure-public-WiFi” in the vicinity.

Step 4: Create a WPA supplicant configuration file to connect to this network .

WPA Supplicant configuration

```
network={
   ssid="Secure-Public-WiFi"
   key_mgmt=OWE
}
```

```
root@attackdefense:~# cat wpa_supplicant.conf
network={
    ssid="Secure-Public-WiFi"
    key_mgmt=OWE
}
root@attackdefense:~#
```

Step 6: Start the wpa_supplicant with above configuration.

Command: wpa_supplicant -Dnl80211 -iwlan1 -c wpa_supplicant.conf

```
root@attackdefense:~# wpa_supplicant -Dnl80211 -iwlan1 -c wpa_supplicant.conf
Successfully initialized wpa_supplicant
wlan1: SME: Trying to authenticate with d2:e9:6a:d3:b3:50 (SSID='Secure-Public-WiFi' freq=2412 MHz)
wlan1: Trying to associate with d2:e9:6a:d3:b3:50 (SSID='Secure-Public-WiFi' freq=2412 MHz)
wlan1: PMKSA-CACHE-ADDED d2:e9:6a:d3:b3:50 0
wlan1: Associated with d2:e9:6a:d3:b3:50
wlan1: CTRL-EVENT-SUBNET-STATUS-UPDATE status=0
wlan1: WPA: Key negotiation completed with d2:e9:6a:d3:b3:50 [PTK=CCMP GTK=CCMP]
wlan1: CTRL-EVENT-CONNECTED - Connection to d2:e9:6a:d3:b3:50 completed [id=0 id_str=]
```

From the console logs of wpa_suppicant, it is clear that it is connected to the network. The same can also be verified in Airodump-ng output

```
CH 13 ][ Elapsed: 3 mins ][ 2019-10-29 06:05 ][ WPA handshake: D2:E9:6A:D3:B3:50

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

D2:E9:6A:D3:B3:50  -28     1905       24    0   1   54   WPA3 CCMP   OWE  Secure-Public-WiFi

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

D2:E9:6A:D3:B3:50  02:00:00:00:01:00  -29    1 - 1      0       19  EAPOL  Secure-Public-WiFi
```

On observing it closely, one can observe that the WPA-handshake is also captured by the Airodump-ng. However, unlike WPA/WPA2-PSK, OWE is not vulnerable to dictionary attack. So, there is nothing that one can do with a captured handshake.