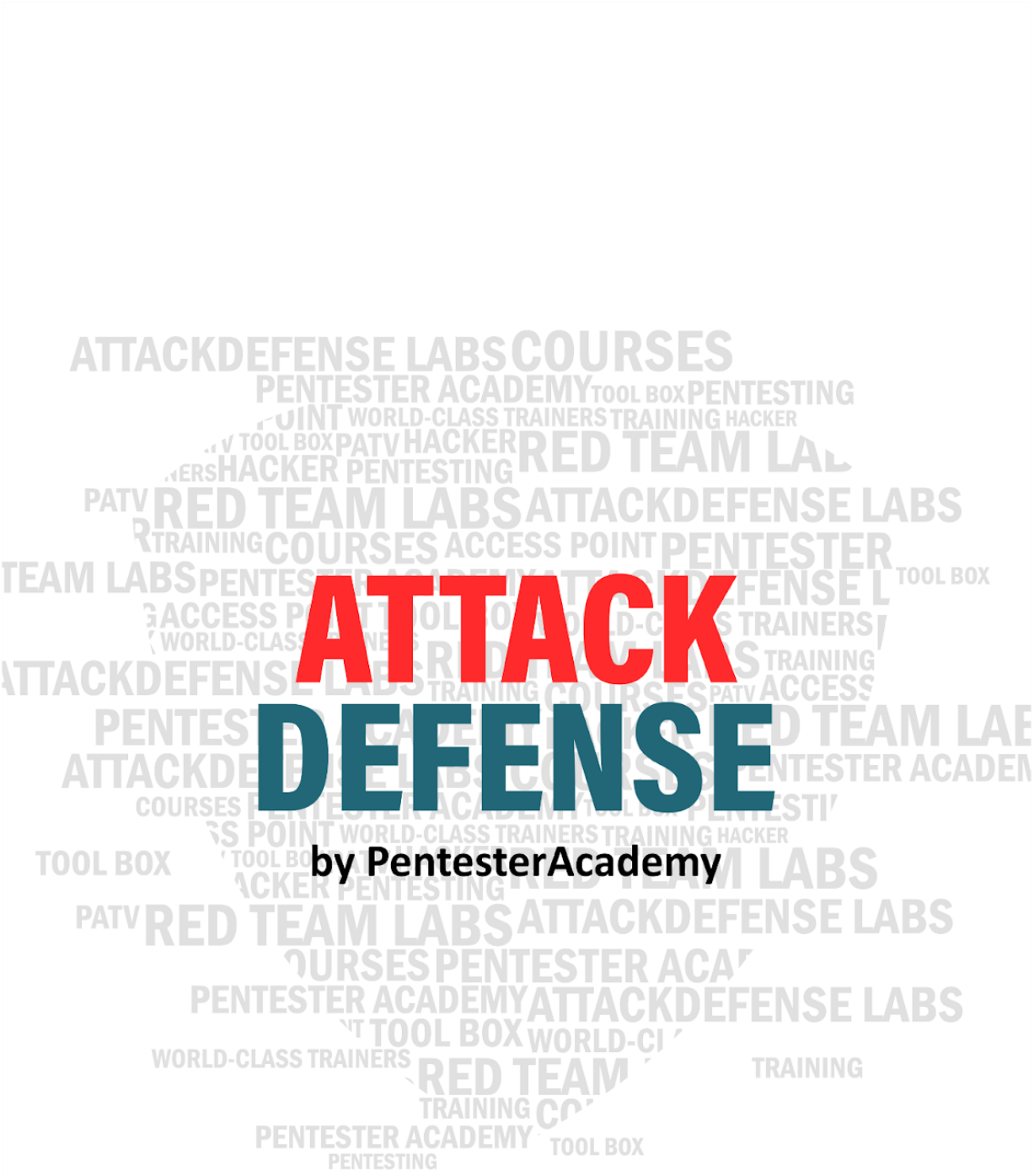
ATTACK
DEFENSE
by PentesterAcademy

Name	WPA Supplicant: WPA-PSK Network
URL	https://www.attackdefense.com/challengedetails?cid=1262
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 WPA-PSK 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#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 14 ][ Elapsed: 12 s ][ 2019-10-16 01:44

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

68:F5:70:C2:12:9B  -28       15        0    0   6   11   WPA  TKIP   PSK  Home_Network

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes
```

A WPA-PSK network “Home_Network” is present in the vicinity.

Step 3: The secret shared passphrase for the WPA-PSK network is provided in the challenge description. Create wpa_supplicant configuration (i.e. wpa_supplicant.conf) for this network.

WPA Supplicant config

```
network={
        ssid="Home_Network"
        scan_ssid=1
        key_mgmt=WPA-PSK
        psk="password123"
}
```

```
root@attackdefense:~# cat wpa_supplicant.conf
network={
        ssid="Home_Network"
        scan_ssid=1
        key_mgmt=WPA-PSK
        psk="password123"
}
root@attackdefense:~#
```

Step 4: Start the wpa_supplicant and it should connect to the “Home_Network” SSID.

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 68:f5:70:c2:12:9b (SSID='Home_Network' freq=2437 MHz)
wlan1: Trying to associate with 68:f5:70:c2:12:9b (SSID='Home_Network' freq=2437 MHz)
wlan1: Associated with 68:f5:70:c2:12:9b
wlan1: CTRL-EVENT-SUBNET-STATUS-UPDATE status=0
wlan1: WPA: Key negotiation completed with 68:f5:70:c2:12:9b [PTK=TKIP GTK=TKIP]
wlan1: CTRL-EVENT-CONNECTED - Connection to 68:f5:70:c2:12:9b completed [id=0 id_str=]
```

The wlan1 interface is now connected to SSID “Home_Network”.