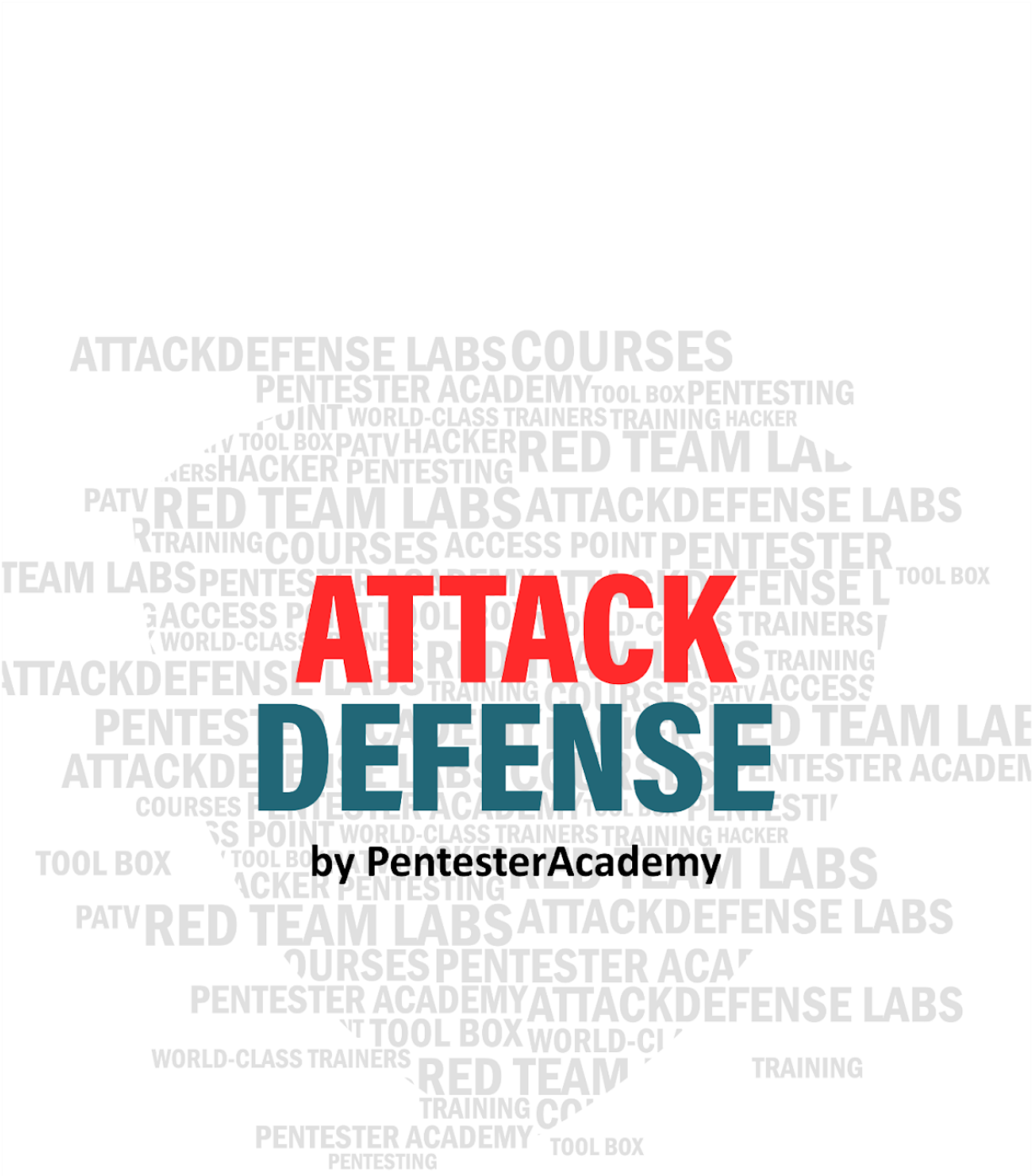
ATTACK
DEFENSE
by PentesterAcademy

Name	WPA Supplicant: WEP Network
URL	https://www.attackdefense.com/challengedetails?cid=1261
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 WEP 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  9 ][ Elapsed: 6 s ][ 2019-10-15 18:09

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

68:7F:77:C2:C2:9A  -28      108        0    0   1   11   WEP  WEP         secure_network

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes
```

A WEP network “secure_network” is present in the vicinity.

Step 3: The secret for the WEP network is provided in the challenge description. Create wpa_supplicant configuration (i.e. supplicant.conf) for given WEP network.

WPA Supplicant config

```
network={
        ssid="secure_network"
        key_mgmt=NONE
        wep_key0="34567"
        wep_tx_keyidx=0
}
```

```
root@attackdefense:~# cat supplicant.conf
network={
        ssid="secure_network"
        key_mgmt=NONE
        wep_key0="34567"
        wep_tx_keyidx=0
}
```

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

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

```
root@attackdefense:~# wpa_supplicant -Dnl80211 -iwlan1 -c supplicant.conf
Successfully initialized wpa_supplicant
wlan1: SME: Trying to authenticate with 68:7f:77:c2:c2:9a (SSID='secure_network' freq=2412 MHz)
wlan1: Trying to associate with 68:7f:77:c2:c2:9a (SSID='secure_network' freq=2412 MHz)
wlan1: Associated with 68:7f:77:c2:c2:9a
wlan1: CTRL-EVENT-CONNECTED - Connection to 68:7f:77:c2:c2:9a completed [id=0 id_str=]
wlan1: CTRL-EVENT-SUBNET-STATUS-UPDATE status=0
```

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