

The image features a word cloud in the shape of the map of India. The words are arranged to fit the geographical outline of the country. The most prominent words, shown in larger fonts, include "ATTACK", "DEFENSE", "LABS", "COURSES", "PENTESTER ACADEMY", "RED TEAM", "ACCESS POINT", "TOOL BOX", "TRAINING", "HACKER", "PATV", "WORLD-CLASS TRAINERS", "PENTESTING", "TEAM LABS", "ACADEMY", "POINT", "DEFENSE L", "ACCESS P", "WORLD-CLAS", "TRAINING", "PENTESTER ACADEN", "COURSES", "PENTESTER ACADEMY", "TOOL BOX", "PENTESTI", "SS POINT", "WORLD-CLASS TRAINERS", "TRAINING HACKER", "TOOL BOX", "HACKER PENTESTING", "RED TEAM LABS", "ATTACK DEFENSE LABS", "COURSES PENTESTER ACA", "PENTESTER ACADEMY ATTACK DEFENSE LABS", "TOOL BOX WORLD-CI", "TRAINING", "PENTESTER ACADEMY", "TOOL BOX", and "PENTESTING". The words "ATTACK" and "DEFENSE" are the largest and are colored red and dark blue respectively, while the others are in various shades of gray. The overall composition uses the density and size of the text to represent the relative importance or frequency of these concepts in the field of cybersecurity training.

Name	WPA Supplicant: WPA2-PSK Network
URL	https://www.attackdefense.com/challengedetails?cid=1263
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: Connect to the WPA2-PSK network using wpa_supplicant.

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: Launch airodump-ng to check for other traffic.

Command: airodump-ng wlan0

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

```
CH 14 ][ Elapsed: 6 s ][ 2019-10-16 01:40
```

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC CIPHER	AUTH	ESSID
68:E4:A3:C6:12:9B	-28	5	0 0	11	11	WPA2 CCMP	PSK	university-campus-a

BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
-------	---------	-----	------	------	--------	-------	--------

A WPA2-PSK network “university-campus-a” is present in the vicinity.

Step 3: The secret shared passphrase for the WPA2-PSK network is provided in the challenge description. Create wpa_supplicant configuration (i.e. wpa_supplicant.conf) for this network.

WPA Supplicant config

```
network={
    ssid="university-campus-a"
    scan_ssid=1
    key_mgmt=WPA-PSK
    psk="secure@12345"
}
```

```
root@attackdefense:~# cat wpa_supplicant.conf
network={
    ssid="university-campus-a"
    scan_ssid=1
    key_mgmt=WPA-PSK
    psk="secure@12345"
}
root@attackdefense:~#
```

Step 4: Start the wpa_supplicant and it should connect to the “university-campus-a” SSID.

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

```
root@attackdefense:~# wpa_supplicant -Dnl80211 -iwlan1 -c wpa_supplicant.conf
Successfully initialized wpa_supplicant
wlan1: SME: Trying to authenticate with 68:e4:a3:c6:12:9b (SSID='university-campus-a' freq=2462 MHz)
wlan1: Trying to associate with 68:e4:a3:c6:12:9b (SSID='university-campus-a' freq=2462 MHz)
wlan1: Associated with 68:e4:a3:c6:12:9b
wlan1: CTRL-EVENT-SUBNET-STATUS-UPDATE status=0
wlan1: WPA: Key negotiation completed with 68:e4:a3:c6:12:9b [PTK=CCMP GTK=CCMP]
wlan1: CTRL-EVENT-CONNECTED - Connection to 68:e4:a3:c6:12:9b completed [id=0 id_str=]
```

The wlan1 interface is now connected to SSID “university-campus-a”.