



## WPA3 Reconnaissance

### Objective

Install the latest version of aircrack-ng from source-code and identify the SSID of an active WPA3 type Access Point.

After successful identification, verify the SSID name via **Verify Flags** section.

#### TABLE OF CONTENTS

1. [INSTALL DEPENDENCIES](#)
2. [DOWNLOAD AIRCRACK-NG SOURCE](#)
3. [CONFIGURE SOURCE](#)
4. [COMPILE BINARIES](#)
5. [DETECT WPA3 NETWORK](#)
6. [VERIFY FLAGS](#)

## Step 1 - Install Dependencies

Aircrack-ng v1.6 is available on your Desktop. Extract the `tar.gz` file, install dependencies and compile the aircrack-ng suite of tools.

As an alternative you can also download the aircrack-ng Github repo: <https://github.com/aircrack-ng/aircrack-ng>

```
apt update
```

```
apt-get install build-essential autoconf automake libtool pkg-config libnl-3-dev libnl-genl-3-dev libssl-dev ethtool shtool rfkill zlib1g-dev libpcap-dev libsqlite3-dev libpcr3-dev libhwloc-dev libcmocka-dev hostapd wpasupplicant tcpdump screen iw usbutils
```

## Step 3 - Extract aircrack-ng source

Extract aircrack-ng source code

```
cd /root/Desktop  
tar zxvf aircrack-ng.tar.gz  
cd aircrack-ng/
```

## Step 4 - Configure source

```
autoreconf -i
```

```
libtoolize: putting auxiliary files in AC_CONFIG_AUX_DIR, '.'.
libtoolize: copying file './ltmain.sh'
libtoolize: putting macros in AC_CONFIG_MACRO_DIRS, 'build/m4/stubs'.
libtoolize: copying file 'build/m4/stubs/libtool.m4'
libtoolize: copying file 'build/m4/stubs/ltoptions.m4'
configure.ac:58: installing './config.guess'
configure.ac:58: installing './config.sub'
parallel-tests: installing './test-driver'
< - - - SNIP - - - >
```

Configure the project for building with the appropriate options specified for your environment

```
./configure
```

## Step 5 - Compile binaries

Compile the binaries from the configured source code.

```
make && make check
```

Note that this will not install `aircrack-ng` on your Kali machine. This will only compile the binaries in the `aircrack-ng` current working directory.

## Step 6 - Detect WPA3 Network

```
./airodump-ng wlan0
```

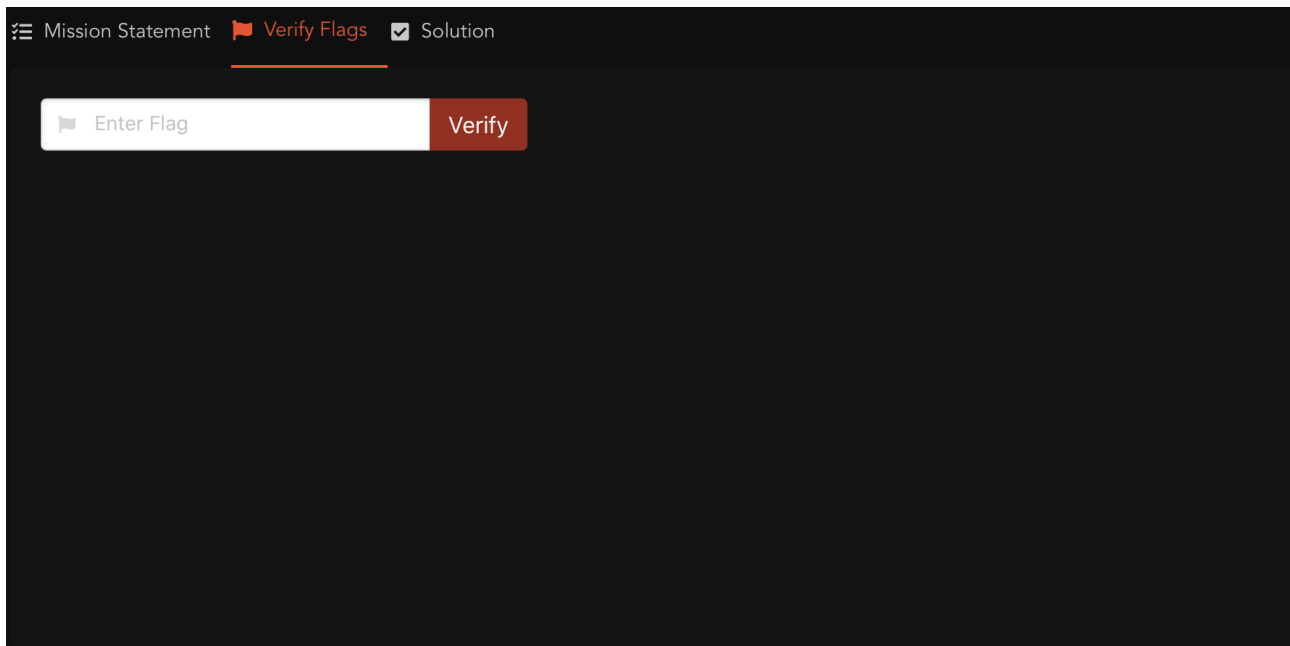
```
CH 12 ][ Elapsed: 0 s ][ 2019-11-27 14:46 ][ paused output
```

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
F4:8C:EB:12:A2:78	-48	4	0	0	1	130	WPA2 CCMP	PSK	Saikat
C4:E9:84:FD:7D:4E	-48	15	0	0	1	54e.	WPA2 CCMP	PSK	TP-LINK_7D4E
08:86:3B:D1:8B:9D	-48	10	0	0	1	135	WPA2 CCMP	PSK	Old_Trafford
B8:C1:AC:A2:02:95	-48	30	0	0	1	270	WPA2 CCMP	PSK	Airtel_7290996555
2C:30:33:20:6B:68	-48	63	0	0	1	130	WPA2 CCMP	PSK	Ghosh
13:44:EF:ED:3F:FA	-28	35	0	0	1	54	WPA3 CCMP	SAE	<b>TARGET_Network</b>
BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes		

`airodump-ng` now detects WPA3 network. Follow the steps above and verify the SSID you see corresponding to your WPA3 network according to the scan output.

## Step 7 - Verify Flags

Go to Verify Flags section on the lab details page, enter the WPA3 Network's SSID then hit Verify.



The screenshot shows a dark-themed web interface. At the top, there is a navigation bar with three items: 'Mission Statement' with a hamburger menu icon, 'Verify Flags' with a red flag icon and an underline, and 'Solution' with a checkmark icon. Below the navigation bar, there is a large dark area. In the top-left corner of this area, there is a white input field with a red flag icon and the text 'Enter Flag'. To the right of the input field is a red button with the text 'Verify'.