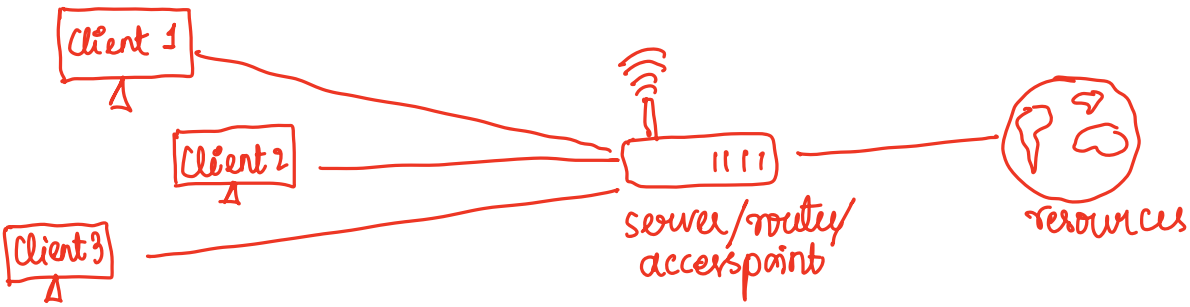
1. Network Hacking

everything - computer, server, any device, company are connected to internet

- Pre-connection attacks - attacks to be done before connecting to network
- Gaining access - crack wifi key, access to wireless network (WPA, WEP)
- Post-connection attacks - intercept connection, modify requests

Typical network

clients are connected to each other, which are connected to network to share data or resources



Router/AP - has direct access to resource. Clients access resource through router. The data transferred between clients & access point is packets transferred in air (wireless network).

∴ If you are within range or have wireless card, you will be able to capture all the requests & responses, see the URL visited by others (as you are in same network as they are in), any passwords or usernames they enter, chat messages & analyse the data

Wireless adapter

needed for gaining access — WEP Cracking
WPA/WPA2 Cracking

A simple USB device connected to the computer & it allows your computer to communicate with WiFi network.

Built in wireless adapter can't be used as wireless adaptors should support following requirements

- monitor mode
- packet injection
- AP mode.

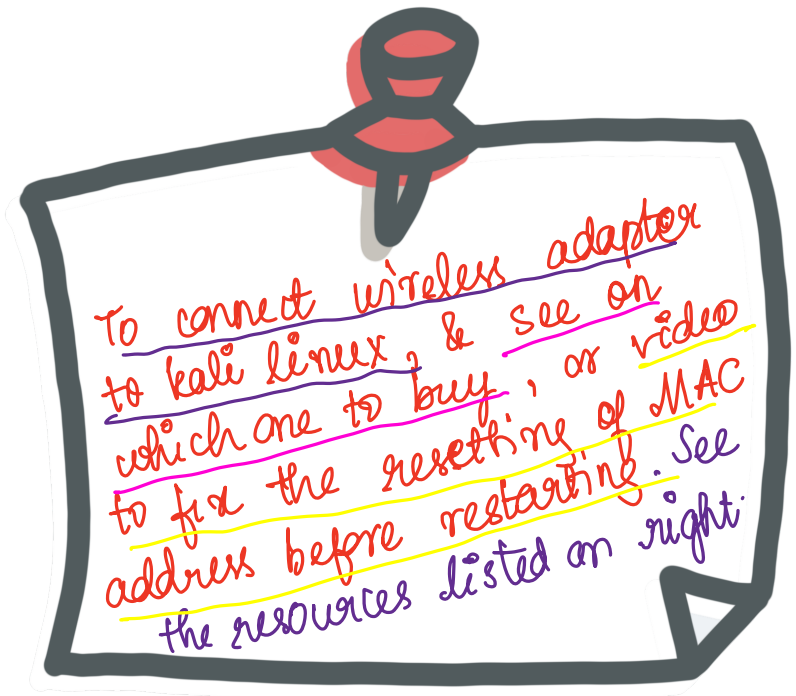
also they should support kali linux & recommended chipset is
- RealTek RTL8812AU
- Atheros AR9271

For connecting USB wireless adaptor, make sure to disconnect the wireless adaptor from USB port of computer before starting kali.

We don't use the wireless adapter to connect to WiFi-networks, we use them to actually discover wireless networks & hack them.

MAC address:

Media Access control - is a permanent, physical & unique address assigned to network interfaces by device manufacturer. So a wireless or wired card or Ethernet card have a unique MAC address. No two devices in world that have same MAC address



- search on z security or youtube
- https://www.youtube.com/watch?v=7AUGQNBCddo
- https://www.youtube.com/watch?v=7AUGQNBCddo

IP address:

IP address is used to identify computers & communicate between devices on the internet. The MAC address is used within the network to identify the devices & transfer data between them.

∴ Every packet has source & destination MAC address

Why change MAC address?

- Increase anonymity (hide identity)
- Impersonate other devices
- Bypass filters.

Command to change MAC address: (on wlan0)

1. disable the interface (wlan0)

- On doing ifconfig we get list of all network interfaces available on (Kali) machine

Network interface means any device that allows us to connect to a network Eg: Wifi card, Ethernet card

- eth0 : a virtual ethernet interface created by virtual box when we set Kali to use inet network. It has IP address as it is connected to network.
- lo : virtual loopback interface used in Linux.
- wlan0 : interface for wireless adapter that is connected to Kali. lo & wlan0 have no IP address because they are not connected to internet.

ifconfig wlan0 down

2. Change the MAC address (option)

ifconfig wlan0 hw ether 00:11:22:33:44:55

hw ether — hardware MAC address

00:11:22:33:44:55 — value should start with 00

3. Enable the interface

ifconfig wlan0 up

4. see the changes

ifconfig

Note: The MAC address will revert back to original one once you restart the computer because we are only changing MAC address.

But if it is reseting to original value without restarting then problem is network manager is reseting MAC address. To fix it refer:

https://www.youtube.com/watch?v=7AUGQNBCddo

Command to enter monitor mode:

To capture the packets sent in the air, we need to operate the network mode.

iwconfig - to see list of wireless interfaces

From the list, it shows that wlan0 is in managed mode.

Managed mode is the default mode for all wireless devices.

It means that the device will only capture packets that has destination MAC as the current device, (packets that are directed towards my Kali machine).

Monitor mode: To capture all the packets within the range that are sent to the router, we need monitor mode.

1. disable wlan0
   #ifconfig wlan0 down
2. kill any process with using inteface in monitor mode (optional)
   # airmon-ng check kill

This kill network manager running, you will lose internet connection. Also we are doing pre-connection attacks using monitor mode which don't need internet

3. Enable monitor mode
   # iwconfig wlan0 mode monitor.
4. Enable wlan0 inteface
   #iwconfig wlan0 up.

Another method to enable monitor mode

https://www.youtube.com/watch?v=wIoR_0epvs