network scanning:

angryIP scanner --> open angryip.org

Download Deb file (32 bit or 64bit depending on your machine's architecture)

open terminal navigate to the downloaded path and give the command

root@kali~# dpkg -i <filename.deb>

press windows key or cmd key (mac) and type angryip and press eneter

---

nmap ping sweep --> root@kali~# nmap -sn <ip range>

---

fping syntax --> root@kali~# fping -c <the count of packets you want to send> -g <range of IP address>

---

netdiscover syntax --> root@kali~# netdiscover -i (interface through which you are connect to internet) -r (range of IP (optional))

how to find the interface? and how to find the range of IP address?

1)finding interface : open terminal and give the command ifconfig

and the result would be

```
root@kali:/home/kali# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.5  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::a00:27ff:fef4:2efa  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:f4:2e:fa  txqueuelen 1000  (Ethernet)
        RX packets 259872  bytes 113256079 (108.0 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 15424  bytes 1209390 (1.1 MiB)
```

```
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 2017  bytes 200508 (195.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2017  bytes 200508 (195.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

in the above result you are able to see eth0 is the interface where you are able to get the internet for your machine.

---

2) finding the range of IP:

in ifconfig result you find your IP address as 192.168.0.5 as you know the classes of IP address the range in which this 192.168.0.5 falls is 192.168.0.1-255 which is represented as 192.168.0.1/24

if in ifconfig result you find your IP address as 192.168.11.5 as you know the classes of IP address the range in which this 192.168.11.5 falls is 192.168.11.1-255 which is represented as 192.168.11.1/24

PORT Scanning:

What is a PORT?

A single point of contact to enter or exit out of a machine where a few services would be running. the number of ports in each and every machine is 65,535.

List of common ports you need to remember

20 - FTP Data
21 - FTP

22 - SSH
23 - Telnet
25 - SMTP
53 - DNS
80 - HTTP
443 - HTTPS
3389 - RDP

Stealth Scan (Half Open Scan):

root@kali~# namp -sS <IP address of the target>

TCP Connect Scan (Full Open Scan):
root@kali~# nmap -sT <IP address of the target>

Operating System Detection Scan:
root@kali~# nmap -O <IP Address of the target>

Software Version Detection Scan:
root@kali~#nmap -sV <IP Address of the target>

Fin Scan:
root@kali~#nmap -sF <IP Address of the target>

Null Scan:
root@kali~# nmap -sN <IP address of the target>

Filtered : this means the scan is unable to identify if the port is open or closed!
Open|Filtered : the port maybe open but i'm not sure
Closed|Filtered: the port maybe closed but i'm not sure

Why scan only 1000 ports?

nmap in general will only scan most important 1000 ports on the list (default port scan list inbuilt in nmap)

---

what if i need to scan all the ports(65,535)?

All port scan:
root@kali~# nmap -p- <type of scan you want to perform> <IP Address of the target>

---

why only show TCP ports? i need to scan UDP ports too, but how?

UDP Scan:
root@kali~# nmap -sU <IP address of the target>

---

i don't want to scan all the 65,535 ports and also i don't want to scan the most important 1000 default ports. but i want just want to scan a few ports i like, how to do that?

Specific port scan:
root@kali~# nmap -p 21,22,80,8080 <Target IP address>