1. Scan each port

- nmap -p- IP

1. UDP are fast compare to TCP
2. Netdiscover -i eth0(Your Network name)

-This command to find device to connnect your same network

1. Ignore any ip addrees for scan

- nmap -sn IP -exclude IP

1. -sn flag are use only system are open or close only no other information are provide
2. Bypass firewall using -PR flag.
3. Find Domain name using IP :- nmap -R IP

**Find own network connect device IP address**

1. find the range of own network

- netdiscover => get range of IP

- id addr -> it get range of IP like 192.168.1.1/25

1. Check device up

- nmap -sn IP-range like (nmap -sn 192.168.1.1/25);