Network Scanning with NMAP and Zenmap

Download Zenmap:

Open Chrome → Search "zenmap download" → Click on the first link → Then click on "zenmap download page" → Then click on Windows → Click "nmap-7.93-setup.exe" → Then download the file → Install Zenmap.

Scanning with Zenmap:

- Open Zenmap application → Give the target IP "50.50.48.13" → Select the profile "Ping Scan" → Then it will show the command → `nmap -sn -v 50.50.48.13` [target IP].
- Click on Scan.

Output:

- Host is up (0.00106 latency).
- MAC Address: D8:5E:D3:DE:0F:FE (Giga-byte Technology).
- Nmap Done: 1 IP address (1 host up) scanned in 0.42 second.

Scan with NMAP in Kali:

Open terminal in Kali Linux,

- **#nmap -sn <target IP> for scan (ping).**
- **#nmap -Pn <target IP> → Port scanning without host discovery.**

 # nmap -Pn -v <target IP> verbose scan.

 # nmap -Pn -ON <target IP> (Output Generate)

 # nmap -p sS -v -oX scan.xml <target IP>

 # nmap -p 22 <target IP>

 # nmap -p -sS -v <target IP>

 # nmap -A -v <target IP> Aggressive scan.

 # nmap -T1 -A -v -f <target IP>

 # nmap -p telnet <target IP>

 # nmap -r <IP> sequential port scan.

List Scan

 # nmap <IP> -sL view range of IP.

 # nmap <IP> -sV --version-intensity 6

 # nmap -f <IP>

 # nmap –mtu 64 <IP>

 # nmap -sI <IP> zombie scanning

 # nmap -sI 52215 <IP>