**Inverse Scan to bypass Firewall:**

If there no ping there's no reachability

If open no ack , if close get ack from RST

GIT: updating commands

New target 192.168.10.198

Ping 192.168.10.198

ttl=128/126 → windows

ttl=64 → linux

-sX -xmacs

-sM -maimon

nmap.org

**Scan behind Firewall:**

Packet fragmentation scan

**Decoy scan** : block kore dile scan korte parbo na , tai random ip diye scan kora jate net admin bujhte na pare.

Nmap 192.162.10.198 -D RND:10

**Network Enumeration:**

Information gathering

Network scanning

Enumeration

Target er sathe connected hoye more info gather kora, actively query korar process

Hostname, username. Group, ip and routing table, etc

SMTP Enumeration:

Ki ki user oi server e exist kore













