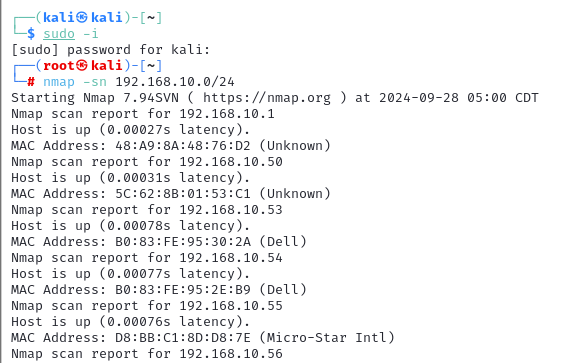
Date: 28th September,2024

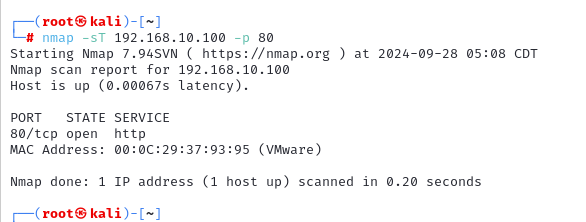
Mentor: Bappi Sir

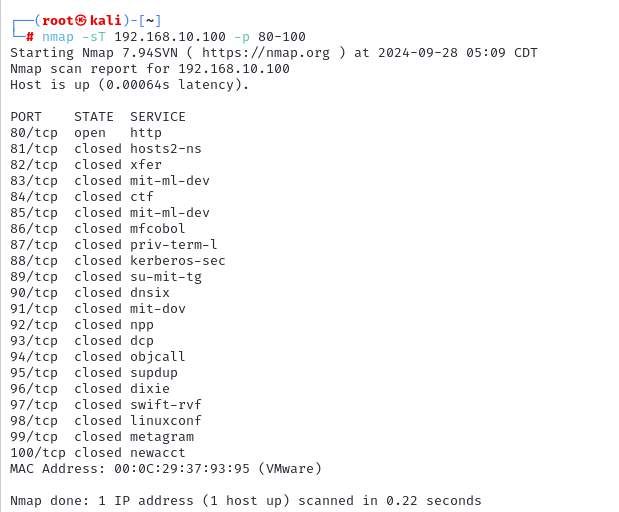
Nmap -sn -192.168.10.0/24 to check available ip



Target 192.168.10.100 – metasploitable-2

Sscanning techniques: **TCP scan**





**All: nmap -sT 192.168.10.100 -p-**

**nmap -sT 192.168.10.10 0-65535**

**UDP:**

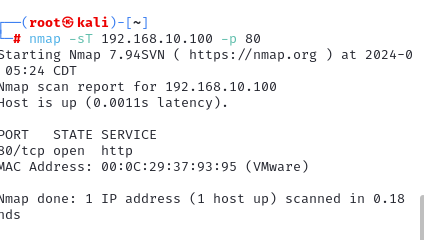
nmap -sU 192.168.10.100

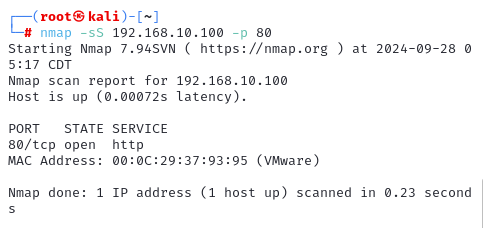
**Sync Scan:**

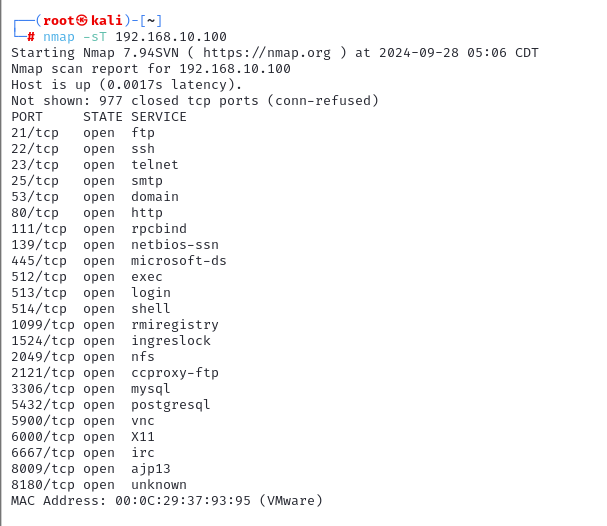
nmap -sS 192.168.10.100

Syn → ack←

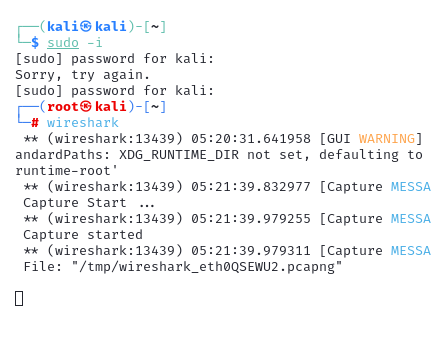
RST→

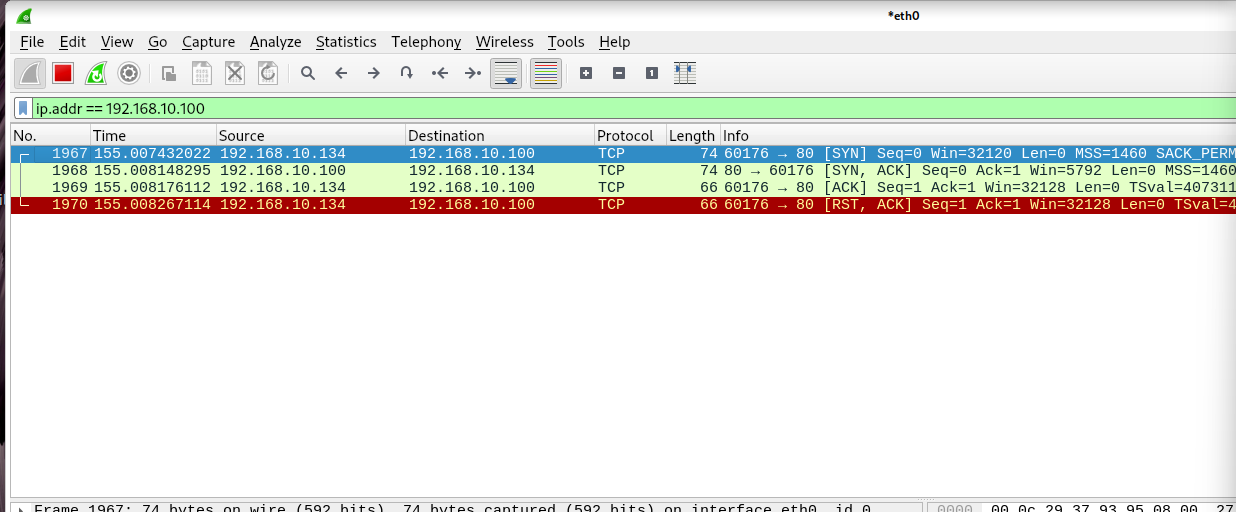




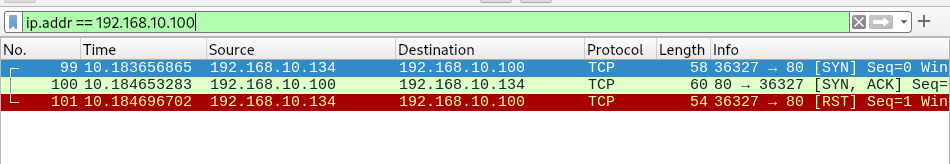


**Difference in backend: using wireshark**

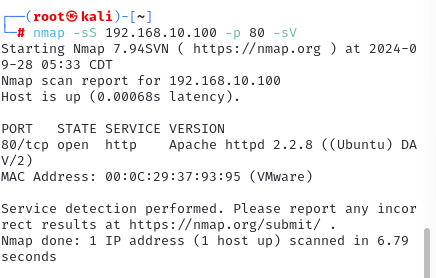




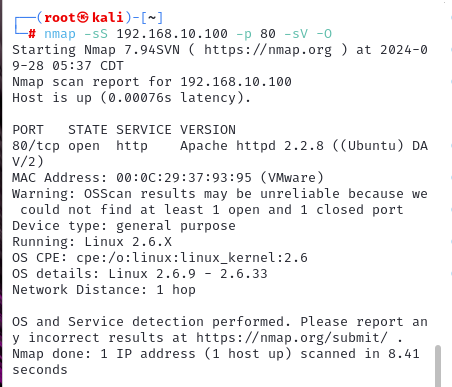
Sync scan:



Service version: nmap -sS 192.168.10.100 -p 80 –sV



Version theke security gap ber kora

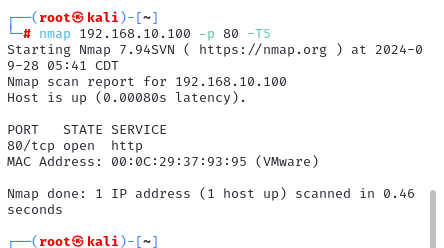


**Nmap scan speed:**

Reducing scan speed to prevent get blocked

Min T0 MAX T5

nmap -T0 default T4



**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

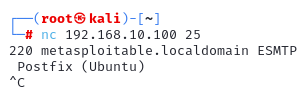
Target er sathe connected hoye more info gather kora, actively query korar process

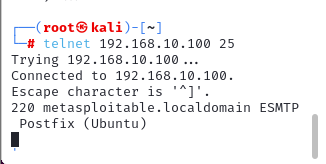
Hostname, username. Group, ip and routing table, etc

SMTP Enumeration:

Ki ki user oi server e exist kore

Apt-get install netcat-traditional





Smtp cmds: vrfy root

Vrfy test

test.com

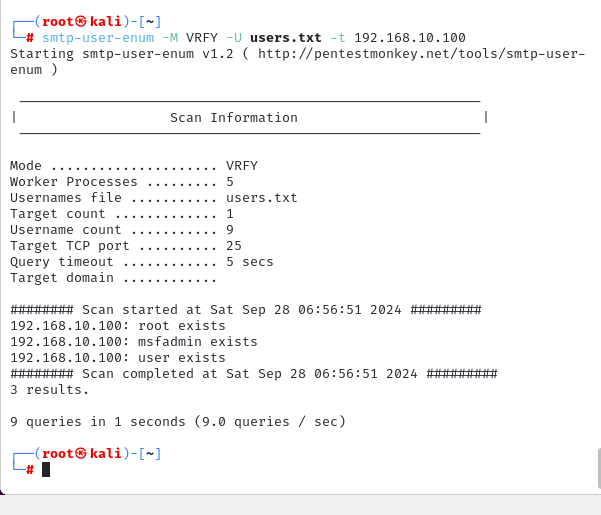
hunter.io =  email search vrfy



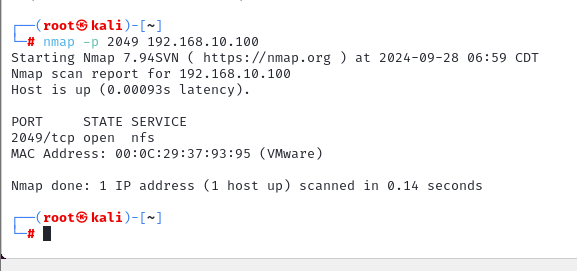
To save= ctrl+x

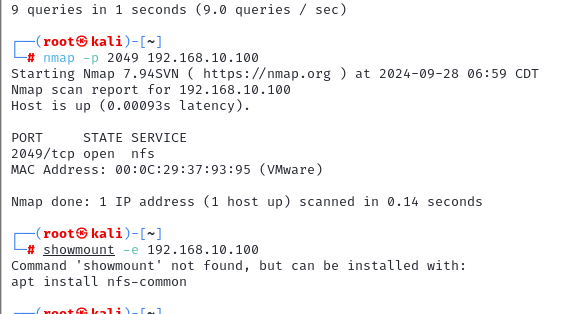
Then press y

Then press ENTER



Nfs for linux file sharing protocol.





Apt-get update

Apt install nfs-common

Showmount -e 192.168.10.100

