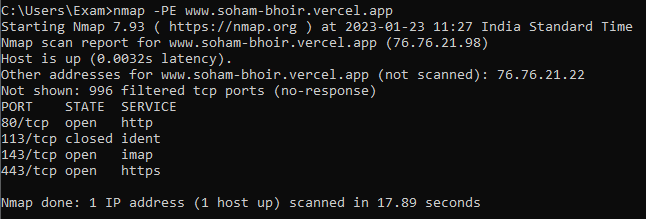
Nmap commands for different types of scanning

For ICMP sweep:

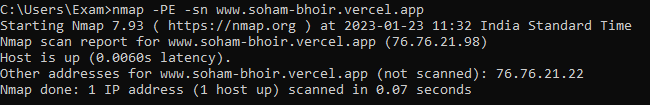
1)Nmap -PE target IP

Output: 

For shortand report:

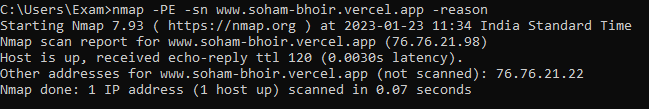
2)Nmap -PE -sn  target IP

Output:



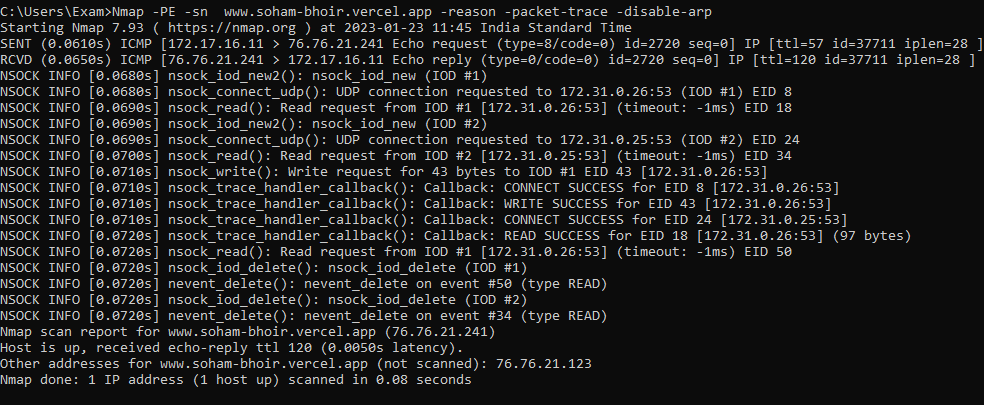
For reason of host up:

3)Nmap -PE -sn  target IP –reason



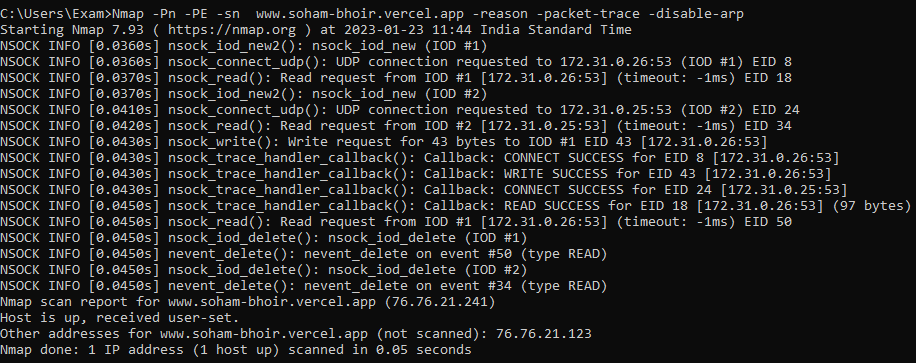
For packet tracing and arp disable

4)Nmap -PE -sn  target IP –reason –packet-trace –disable-arp



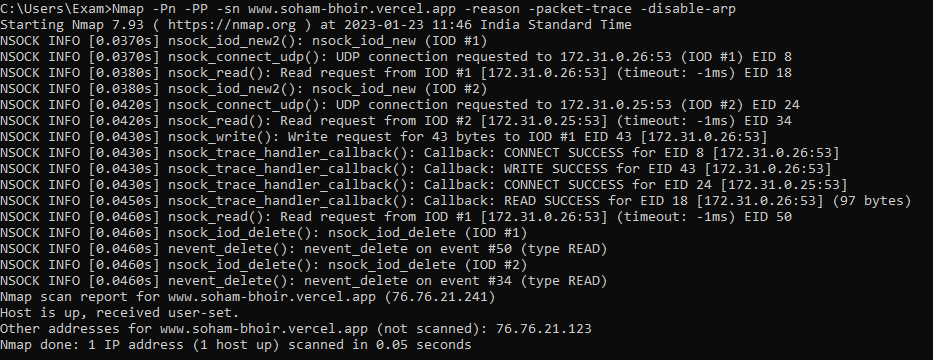
When the host is untraceable

5)Nmap -Pn -PE -sn  target IP –reason –packet-trace –disable-arp



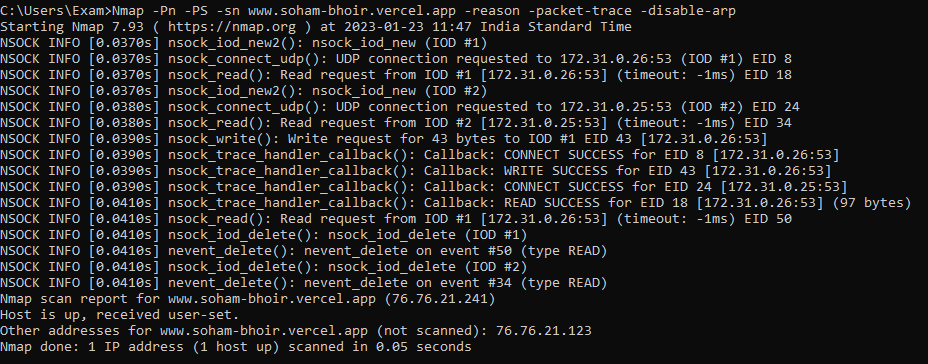
Non ECHO icmp sweep:

6) Nmap -Pn -PP -sn  target IP –reason –packet-trace –disable-arp

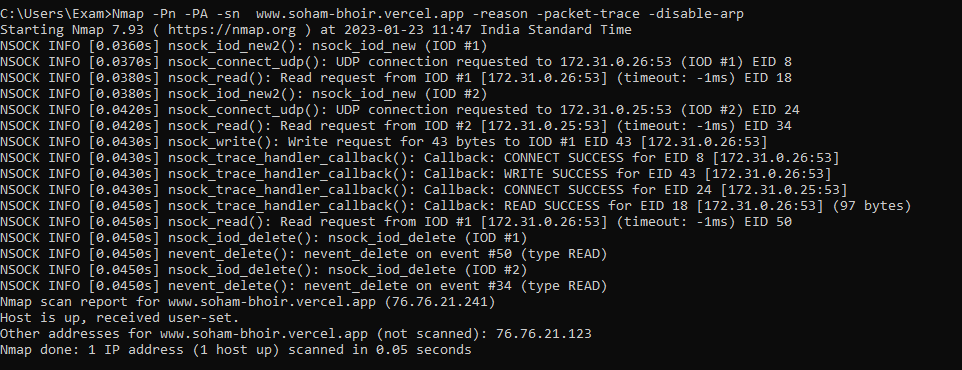


For TCP sweep

7)Nmap -Pn -PS -sn  target IP –reason –packet-trace –disable-arp

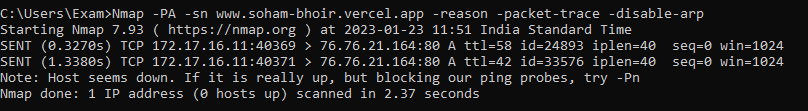


8)Nmap -Pn -PA -sn  target IP –reason –packet-trace –disable-arp

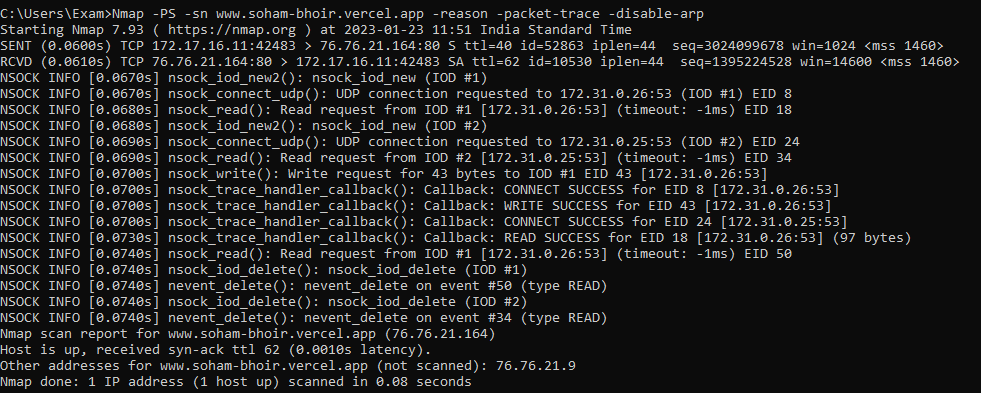


After putting off windows defender firewall (check how to put off windows firewall)

9) Nmap -PA -sn  target IP –reason –packet-trace –disable-arp

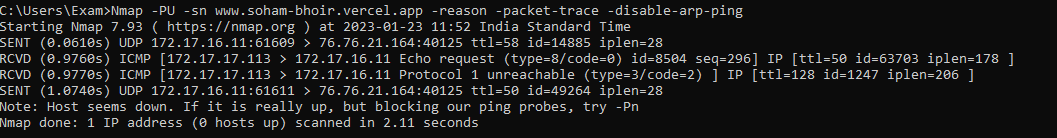


 10) Nmap -PS -sn  target IP –reason –packet-trace –disable-arp



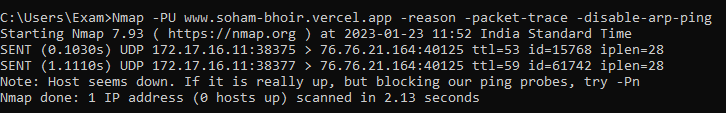
For UDP sweep

11)Nmap -PU -sn  target IP –reason –packet-trace –disable-arp-ping



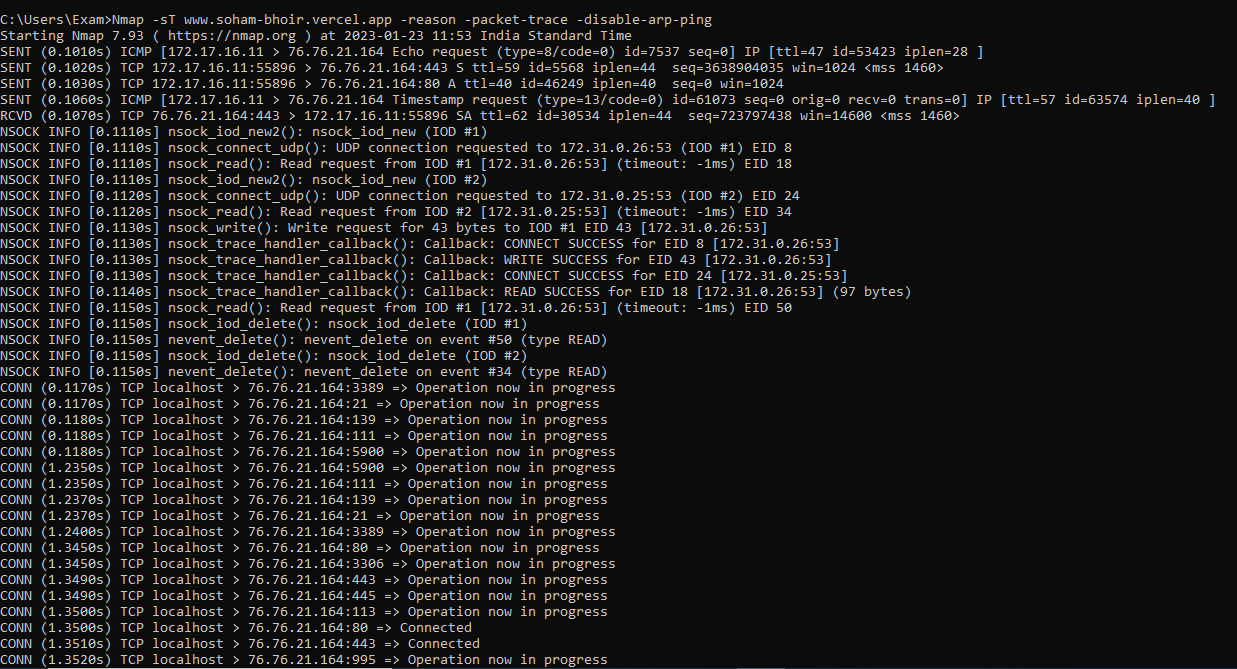
Removing sn then multiport to multiport scanning is done

12) Nmap -PU   target IP –reason –packet-trace –disable-arp-ping



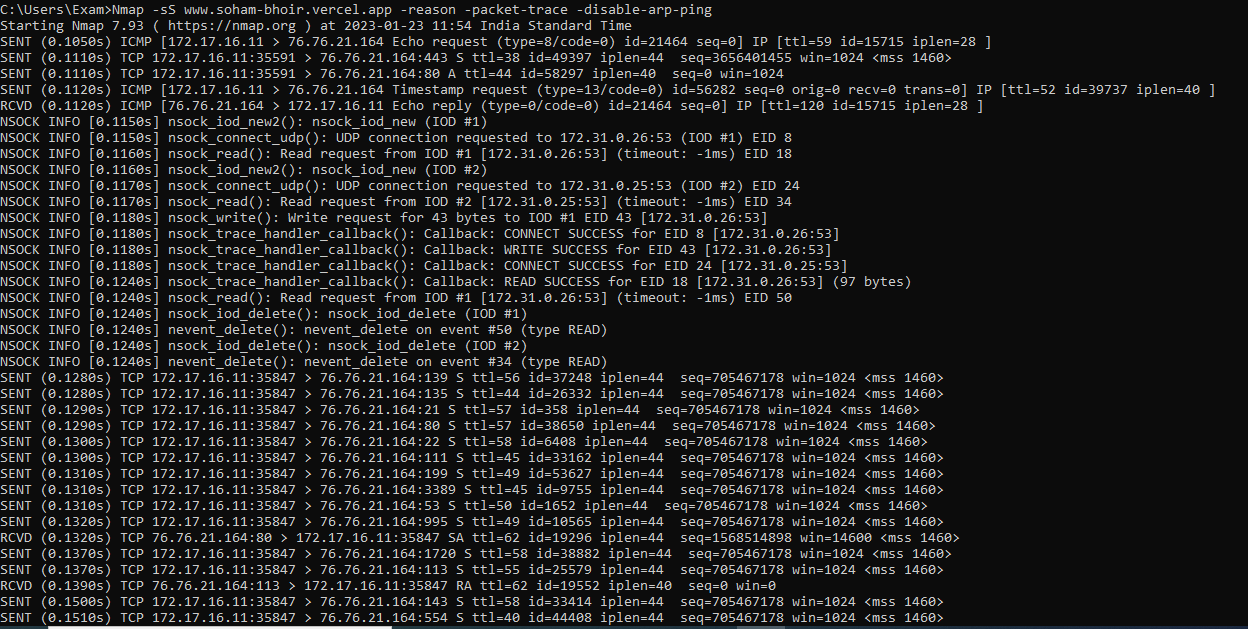
For TCP connect scan

13)Nmap -sT target ip –reason –pracket-trace –disable-arp-ping



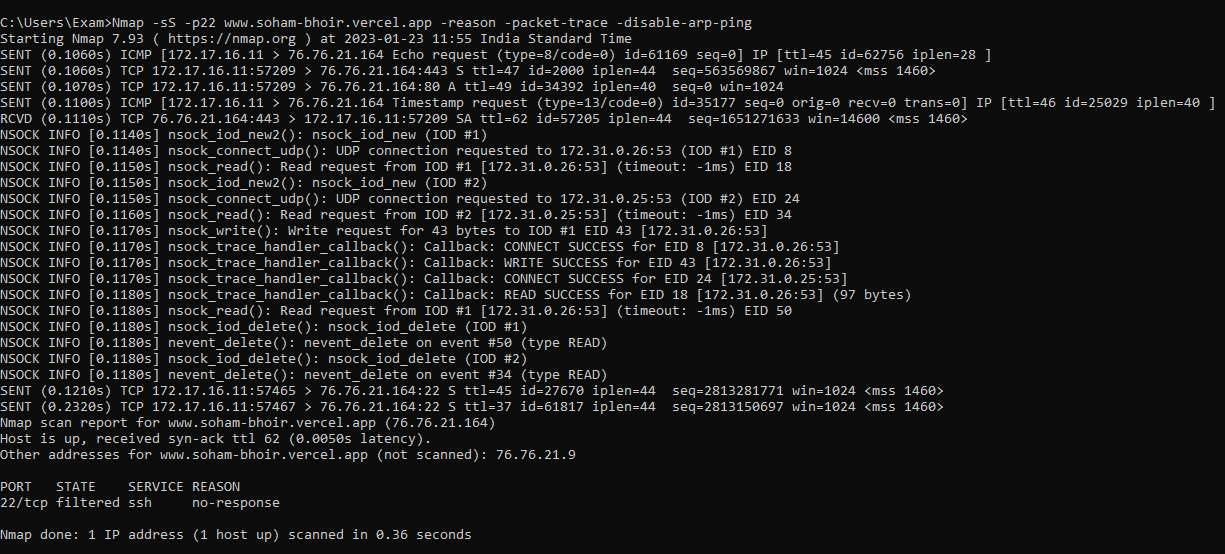
TCP stealth scan

14) Nmap -sS target ip –reason –pracket-trace –disable-arp-ping



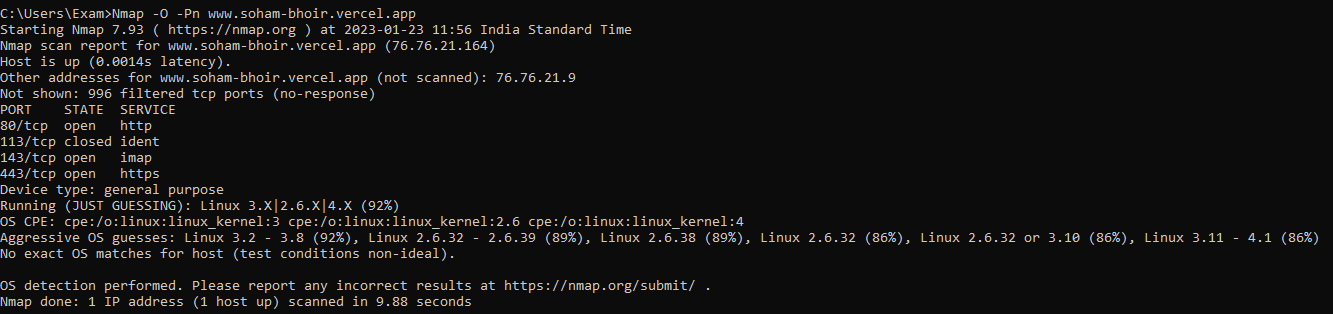
For scanning a specific port using TCP connect scan

15)Nmap -sS -p22 target ip –reason –pracket-trace –disable-arp-ping

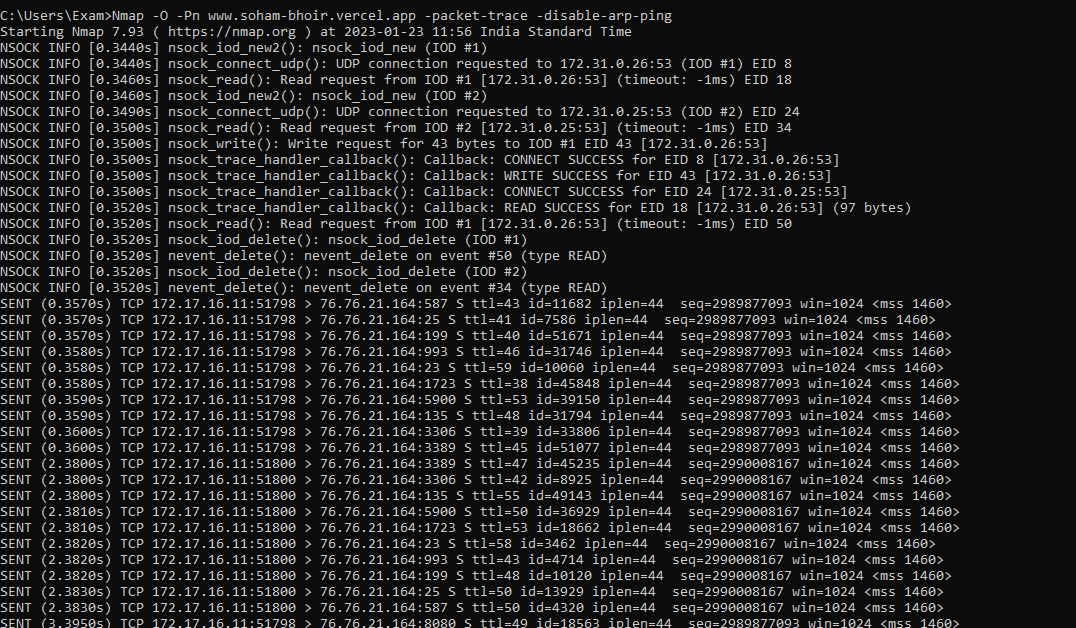


Os detection

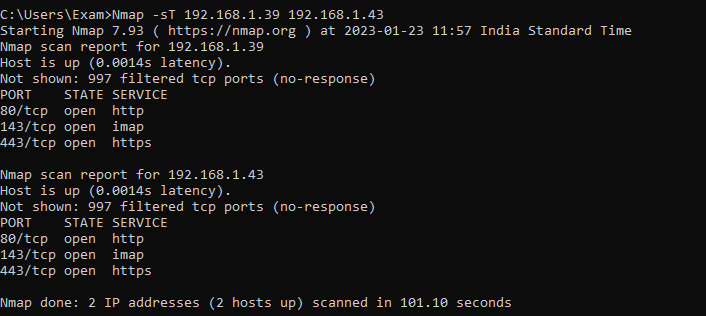
16)Nmap -O -Pn target IP



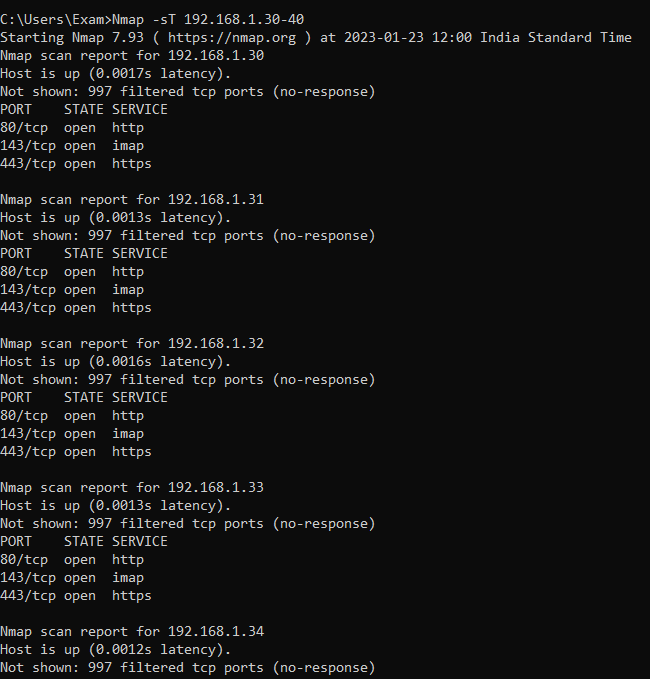
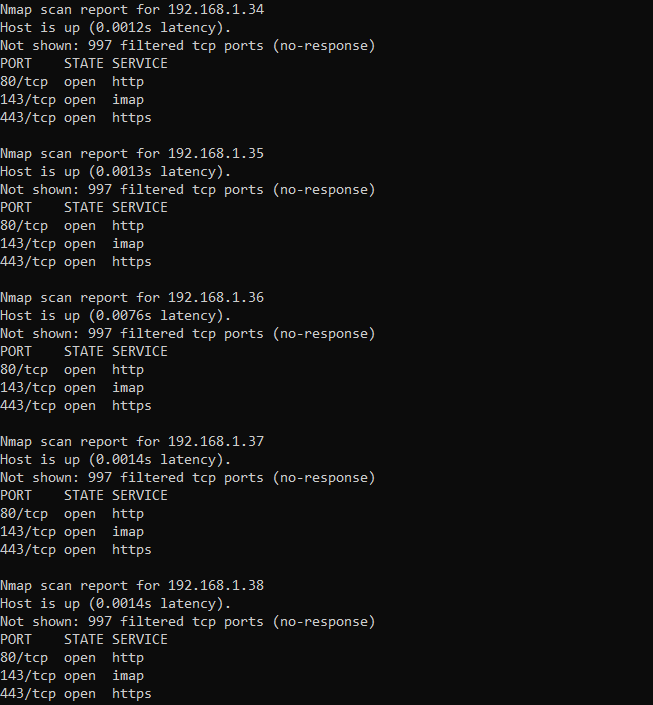
17) Nmap -O -Pn target IP –packet-trace –disable-arp-ping

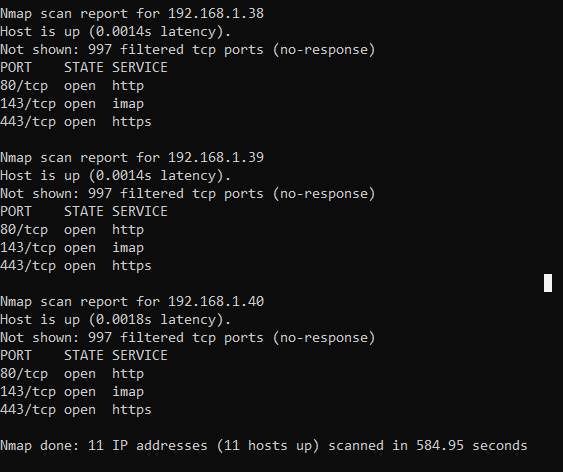


18) Nmap -sT 192.168.1.39 192.168.1.43

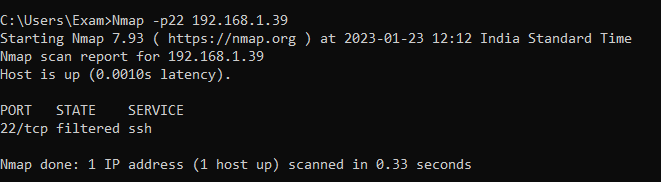


19) Nmap -sT 192.168.1.30-40

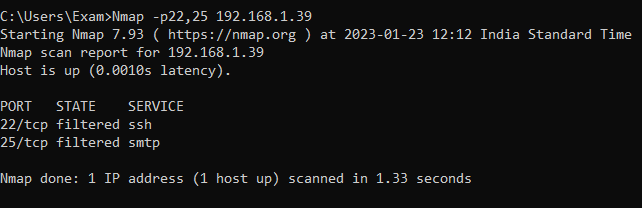
 



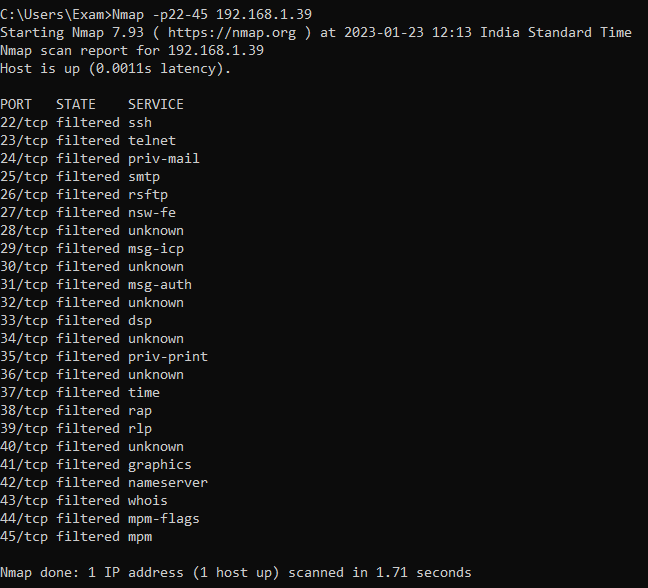
20)Nmap -p22 192.168.1.39



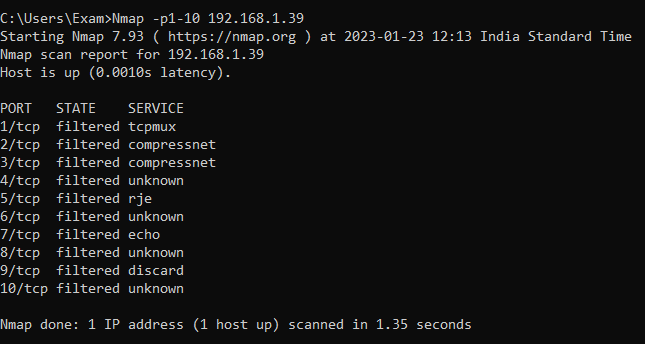
21)Nmap -p22,25 192.168.1.39



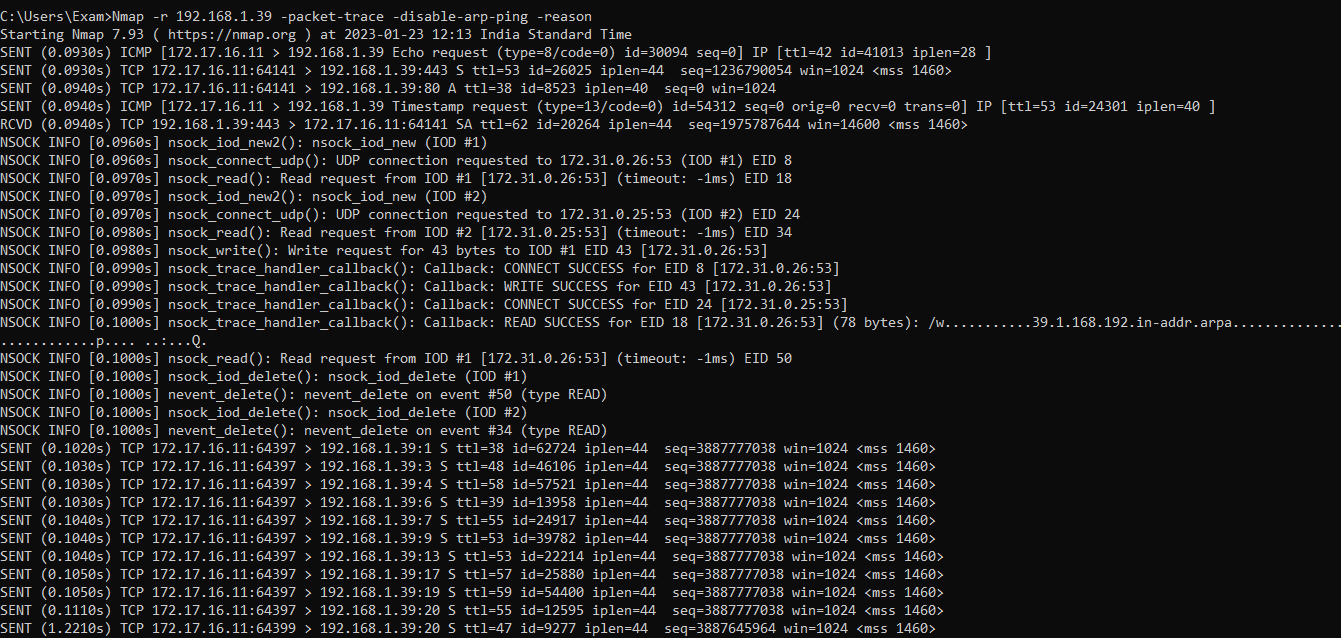
22)Nmap -p22-45 192.168.1.39



23)Nmap -p1-10 192.168.1.39



24)Nmap -r 192.168.1.39 –packet-trace –disable-arp-ping –reason



For version detection

25) Nmap -sV 192.168.1.39 – version detection

26) Nmap -A target ip os and version detection