Name :Sushant Bagul Reg ID: 221070011

TY CE:A

CN LAB EXPERIMENT 6

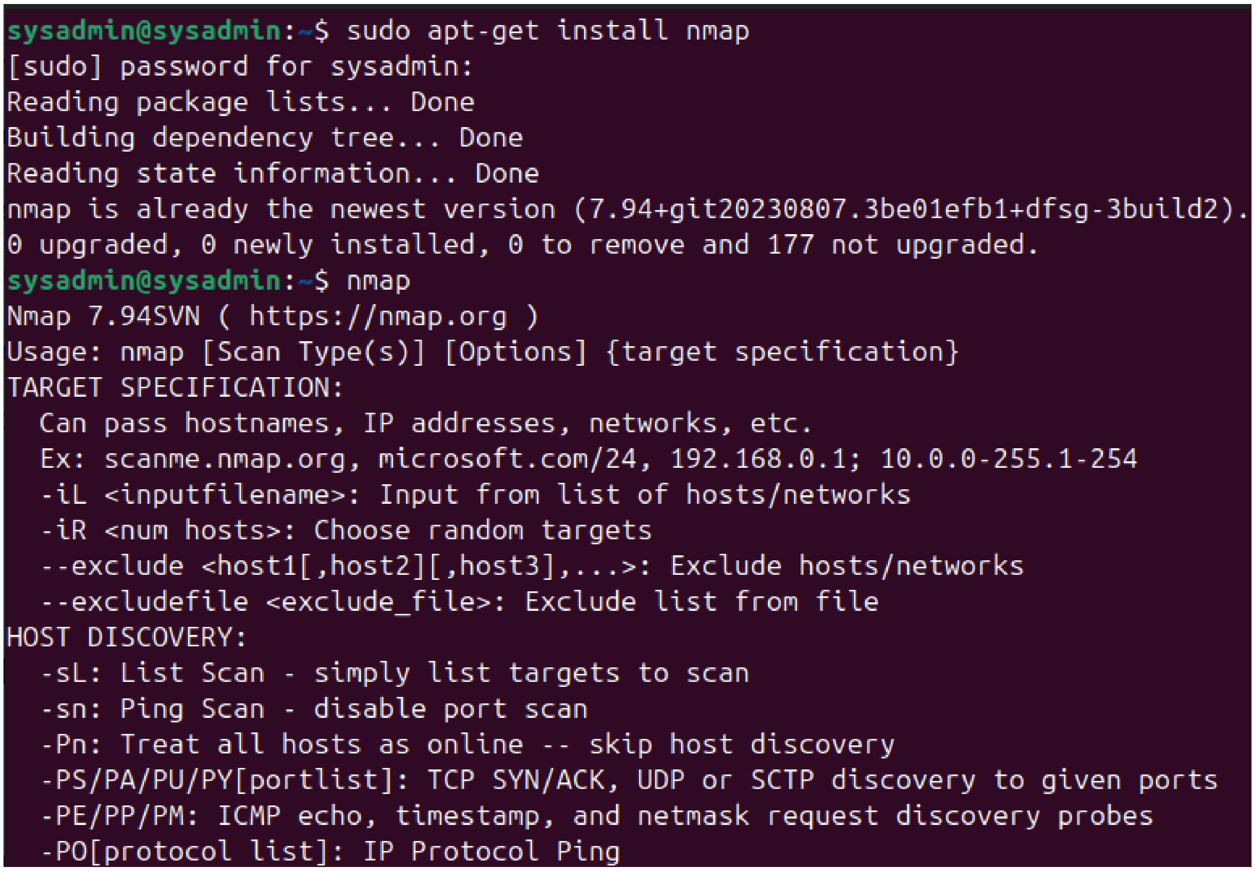
Aim: Perform network discovery using discovery tools (eg. Nmap, mrtg)

Theory:

Nmap (Network Mapper) is a powerful tool used by network administrators for network discovery and security auditing. It&#39;s capable of identifying devices on a network and their available services, operating system versions, and various other attributes. Nmap operates by sending specially crafted packets to target hosts and then analyzing the responses. It’s an essential tool for network administrators, cybersecurity professionals, and ethical hackers to understand and test the security of networks and systems they have permission to access.

Commands:

Installation:

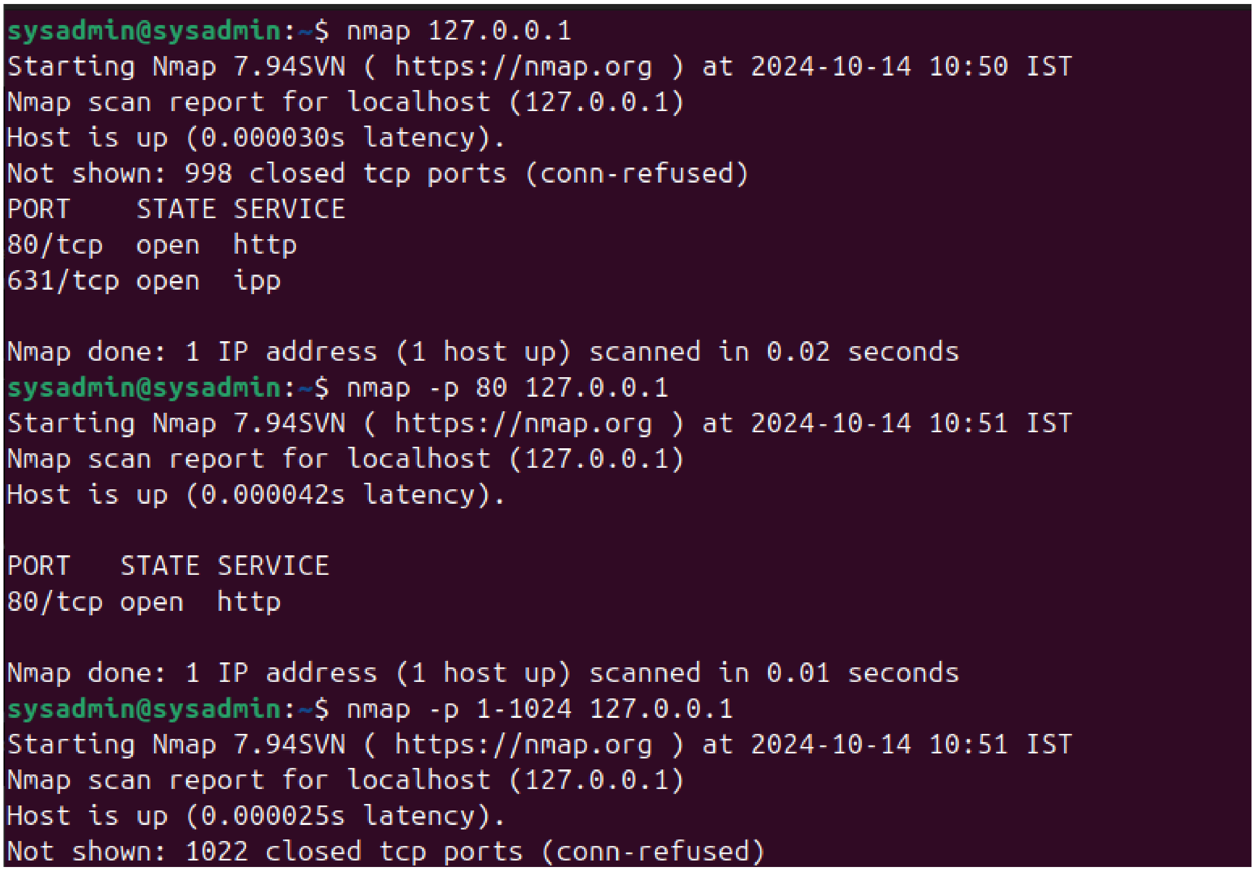


```
sysadmin@sysadmin:~$ sudo apt-get install nmap
[sudo] password for sysadmin:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
nmap is already the newest version (7.94+git20230807.3be01efb1+dfsg-3build2).
0 upgraded, 0 newly installed, 0 to remove and 177 not upgraded.
sysadmin@sysadmin:~$ nmap
Nmap 7.94SVN ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
```

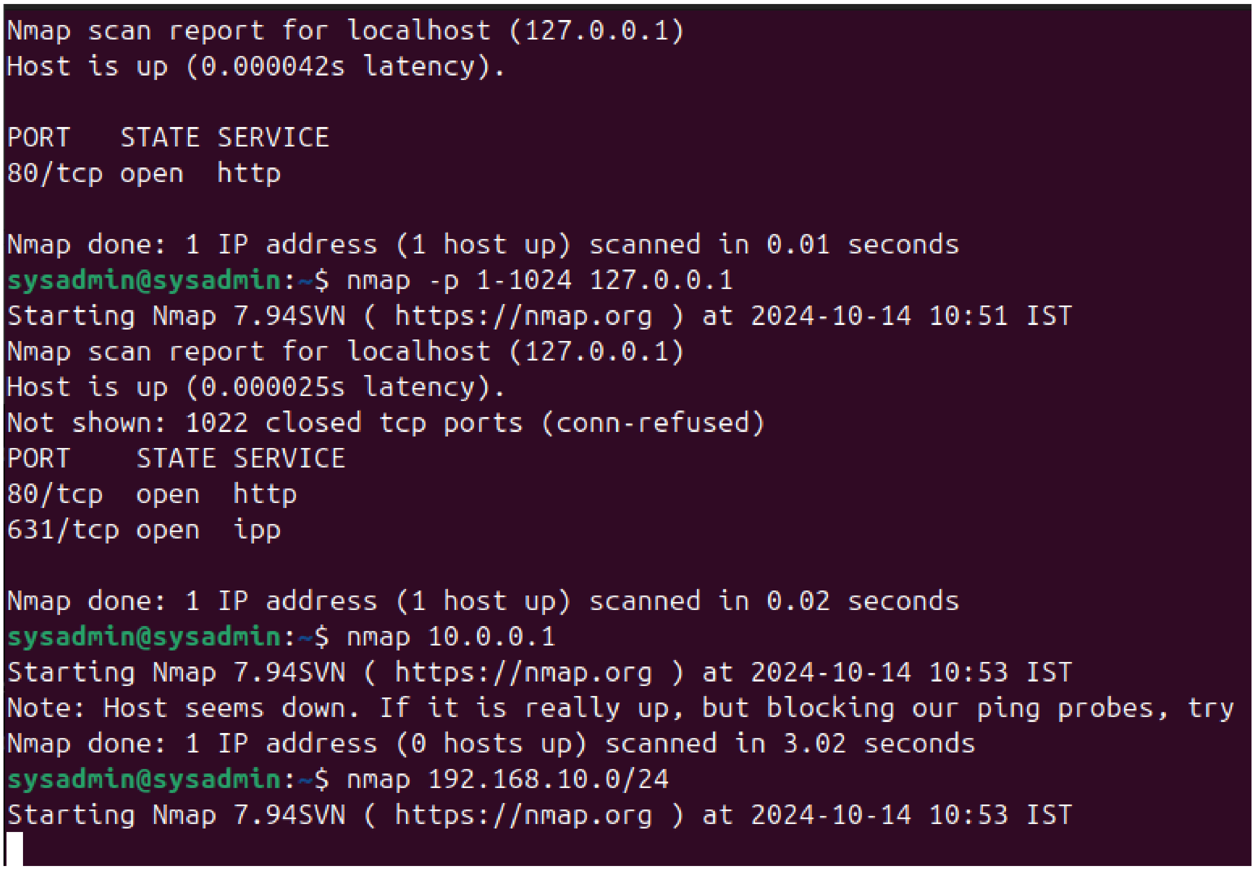
Name :Sushant Bagul Reg ID: 221070011

TY CE:A

1. To scan the ports.



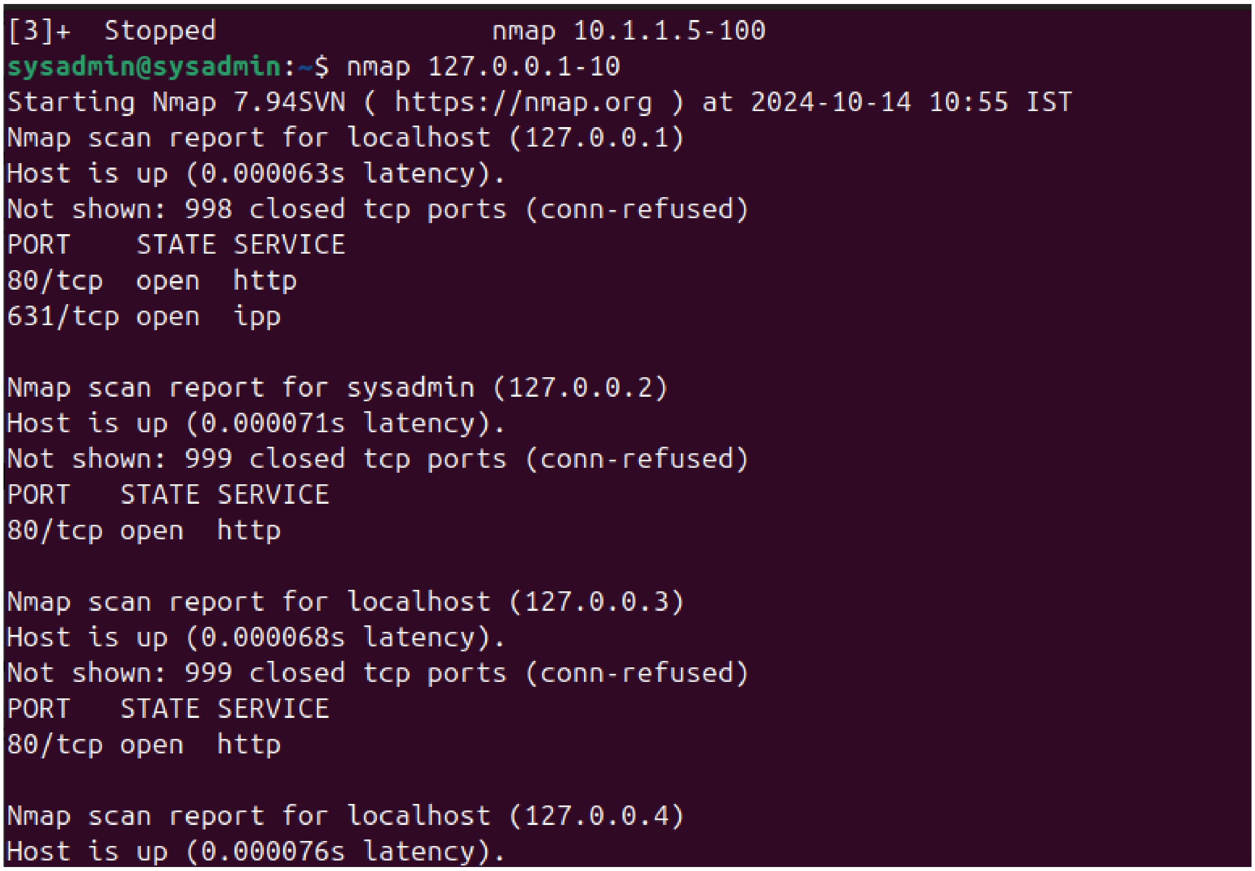
```
sysadmin@sysadmin:~$ nmap 127.0.0.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-14 10:50 IST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000030s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT     STATE SERVICE
80/tcp   open  http
631/tcp open  ipp

Nmap done: 1 IP address (1 host up) scanned in 0.02 seconds
sysadmin@sysadmin:~$ nmap -p 80 127.0.0.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-14 10:51 IST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000042s latency).

PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.01 seconds
sysadmin@sysadmin:~$ nmap -p 1-1024 127.0.0.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-14 10:51 IST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000025s latency).
Not shown: 1022 closed tcp ports (conn-refused)
```



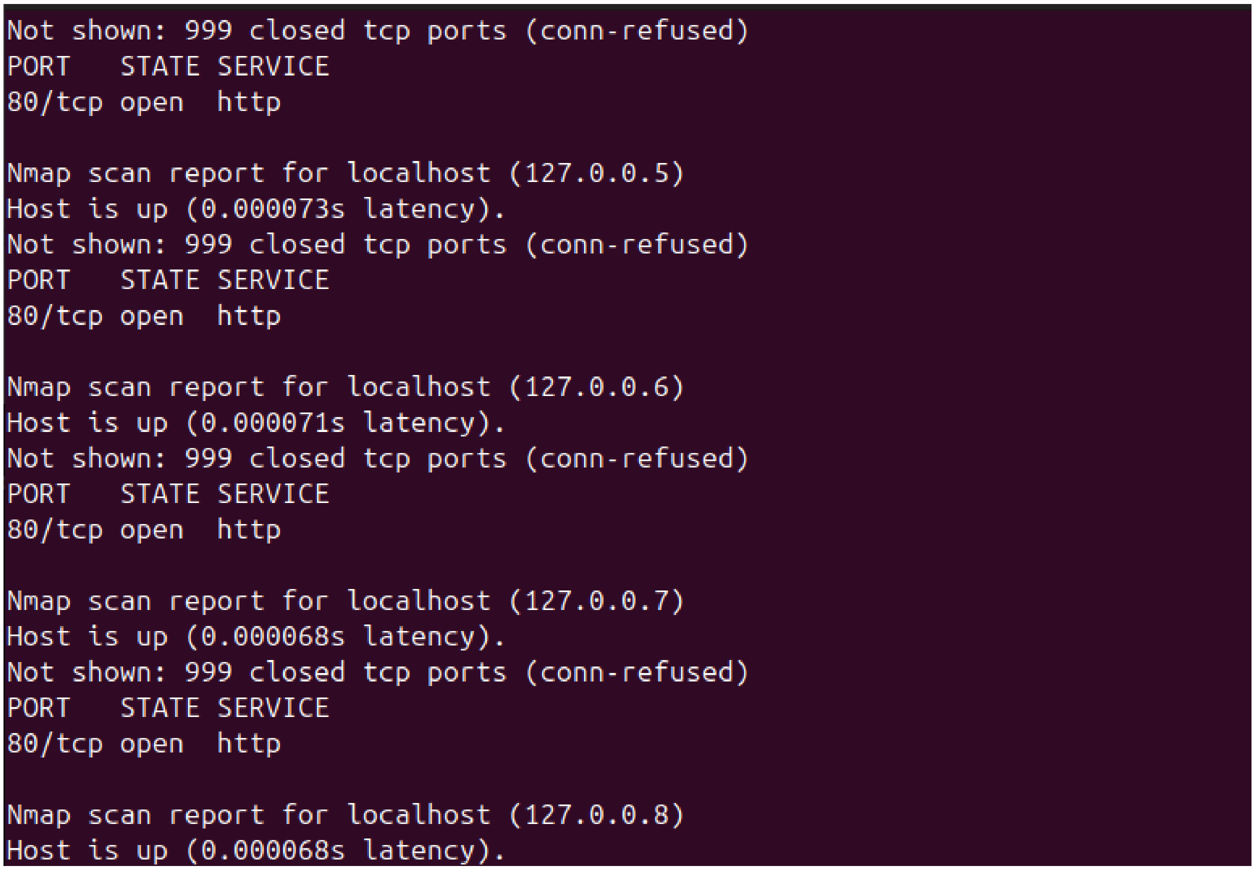
```
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000042s latency).

PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.01 seconds
sysadmin@sysadmin:~$ nmap -p 1-1024 127.0.0.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-14 10:51 IST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000025s latency).
Not shown: 1022 closed tcp ports (conn-refused)
PORT    STATE SERVICE
80/tcp  open  http
631/tcp open  ipp

Nmap done: 1 IP address (1 host up) scanned in 0.02 seconds
sysadmin@sysadmin:~$ nmap 10.0.0.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-14 10:53 IST
Note: Host seems down. If it is really up, but blocking our ping probes, try
Nmap done: 1 IP address (0 hosts up) scanned in 3.02 seconds
sysadmin@sysadmin:~$ nmap 192.168.10.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-14 10:53 IST
```

Name :Sushant Bagul Reg ID: 221070011
TY CE:A

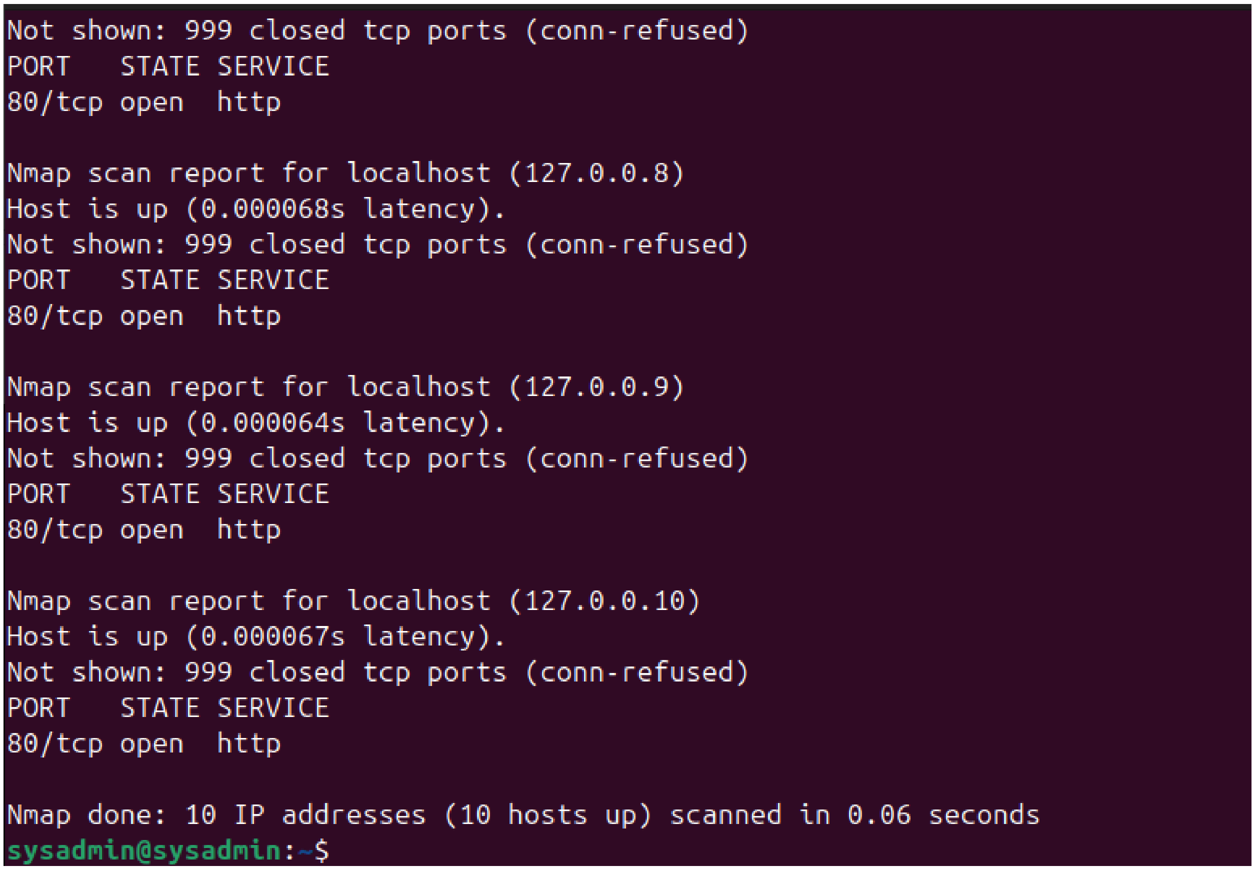
2.To scan multiple addresses



```
[3]+  Stopped                 nmap 10.1.1.5-100
sysadmin@sysadmin:~$ nmap 127.0.0.1-10
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-14 10:55 IST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000063s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT    STATE SERVICE
80/tcp  open  http
631/tcp open  ipp

Nmap scan report for sysadmin (127.0.0.2)
Host is up (0.000071s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE
80/tcp open  http

Nmap scan report for localhost (127.0.0.3)
Host is up (0.000068s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE
80/tcp open  http

Nmap scan report for localhost (127.0.0.4)
Host is up (0.000076s latency).
```

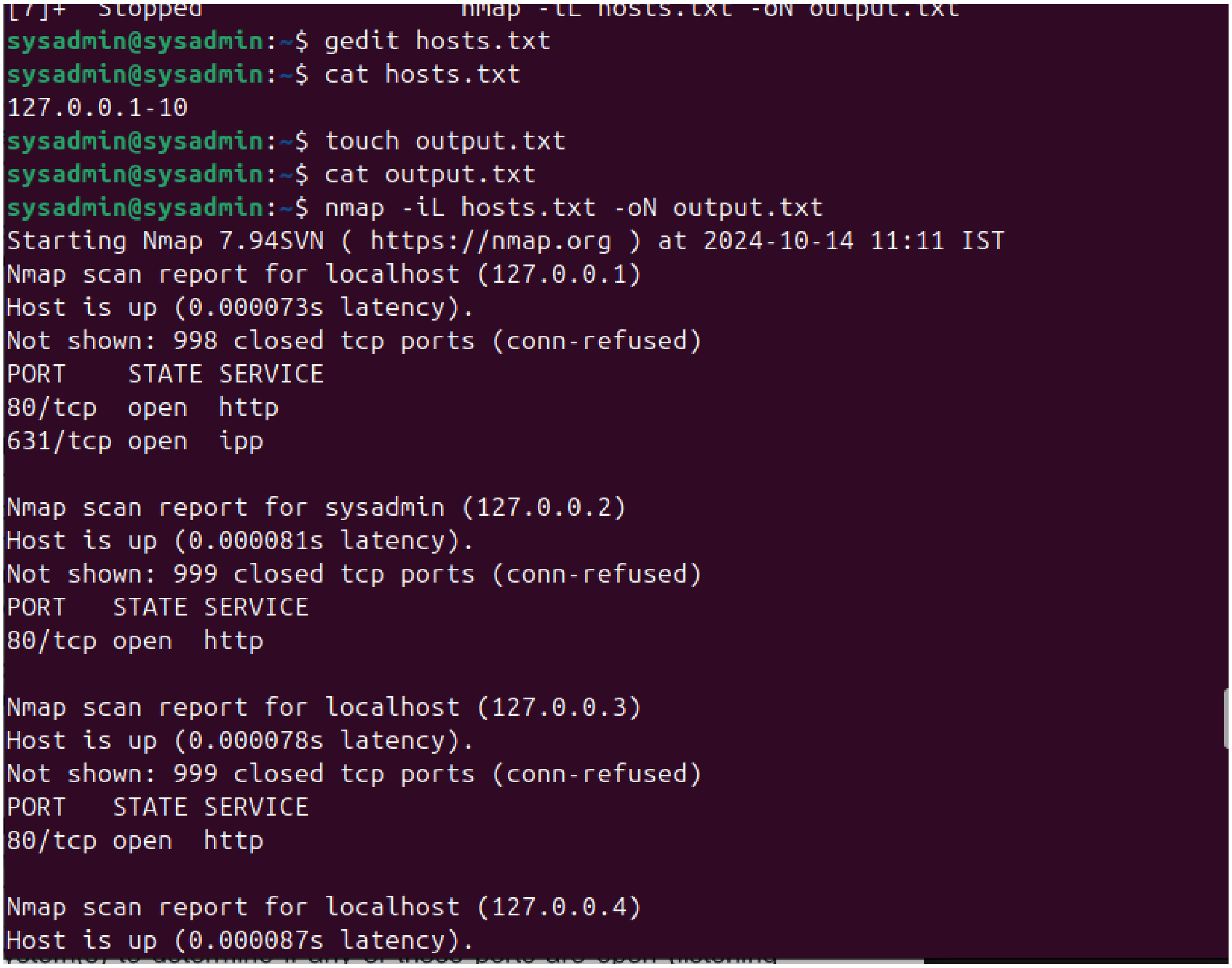


```
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE
80/tcp open  http

Nmap scan report for localhost (127.0.0.5)
Host is up (0.000073s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE
80/tcp open  http

Nmap scan report for localhost (127.0.0.6)
Host is up (0.000071s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE
80/tcp open  http

Nmap scan report for localhost (127.0.0.7)
Host is up (0.000068s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE
80/tcp open  http

Nmap scan report for localhost (127.0.0.8)
Host is up (0.000068s latency).
```

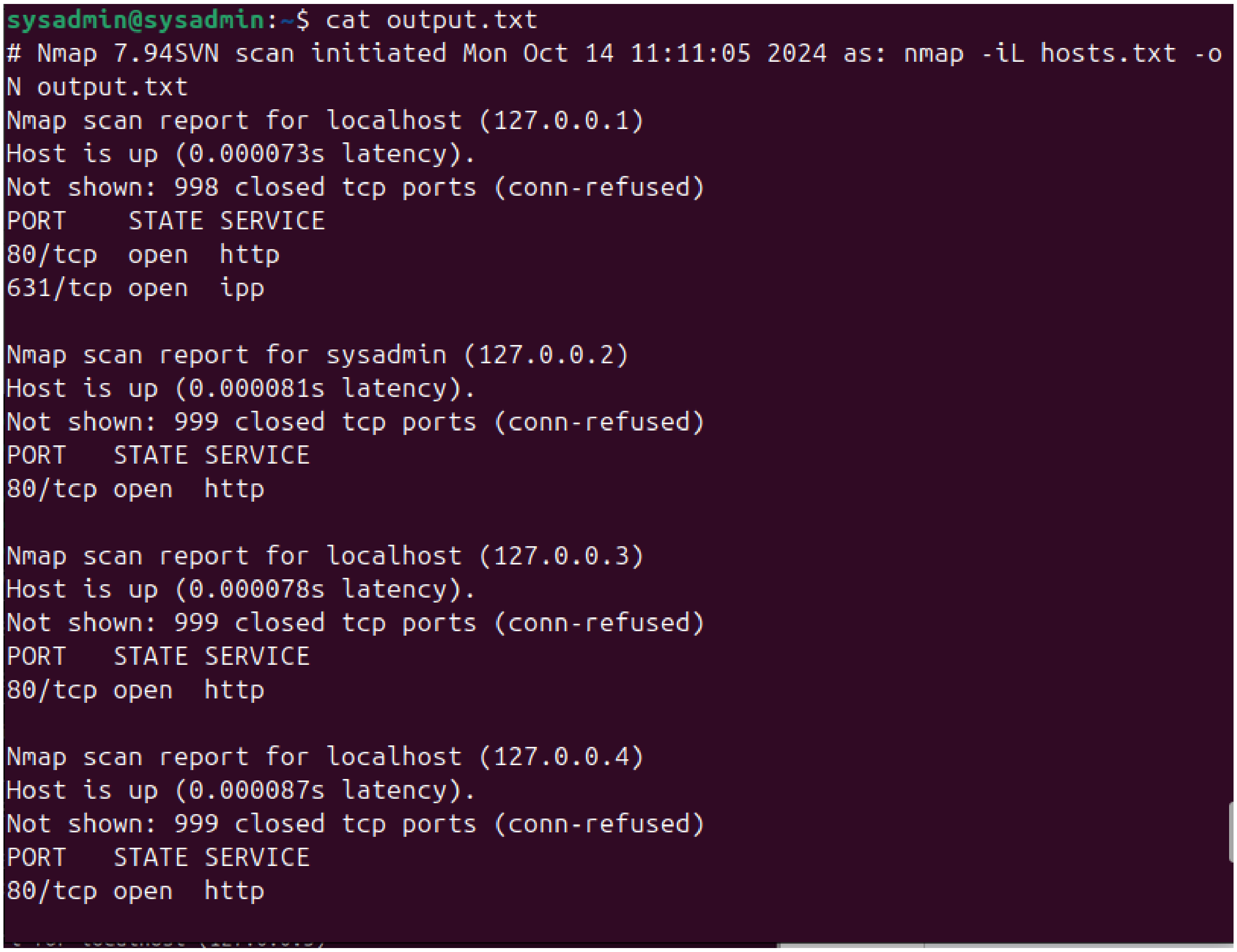


```
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE
80/tcp open  http

Nmap scan report for localhost (127.0.0.8)
Host is up (0.000068s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE
80/tcp open  http

Nmap scan report for localhost (127.0.0.9)
Host is up (0.000064s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE
80/tcp open  http

Nmap scan report for localhost (127.0.0.10)
Host is up (0.000067s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE
80/tcp open  http

Nmap done: 10 IP addresses (10 hosts up) scanned in 0.06 seconds
sysadmin@sysadmin:~$
```

3.Scan hosts and IP addresses reading from a text file and save your NMAP scan results to a file.

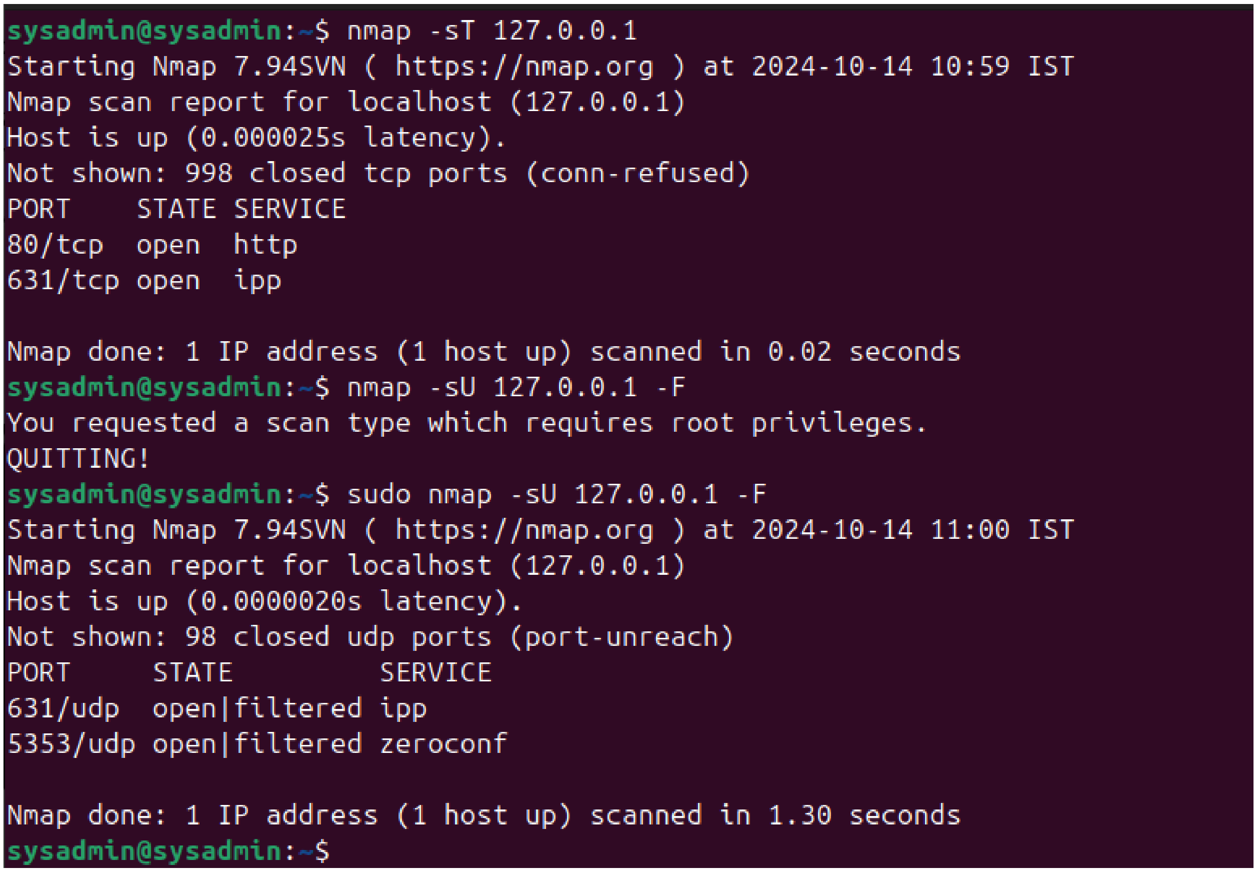


```
[7]+  Stopped                 nmap -iL hosts.txt -oN output.txt
sysadmin@sysadmin:~$ gedit hosts.txt
sysadmin@sysadmin:~$ cat hosts.txt
127.0.0.1-10
sysadmin@sysadmin:~$ touch output.txt
sysadmin@sysadmin:~$ cat output.txt
sysadmin@sysadmin:~$ nmap -iL hosts.txt -oN output.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-14 11:11 IST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000073s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT    STATE SERVICE
80/tcp  open  http
631/tcp open  ipp

Nmap scan report for sysadmin (127.0.0.2)
Host is up (0.000081s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE
80/tcp open  http

Nmap scan report for localhost (127.0.0.3)
Host is up (0.000078s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE
80/tcp open  http

Nmap scan report for localhost (127.0.0.4)
Host is up (0.000087s latency).
```



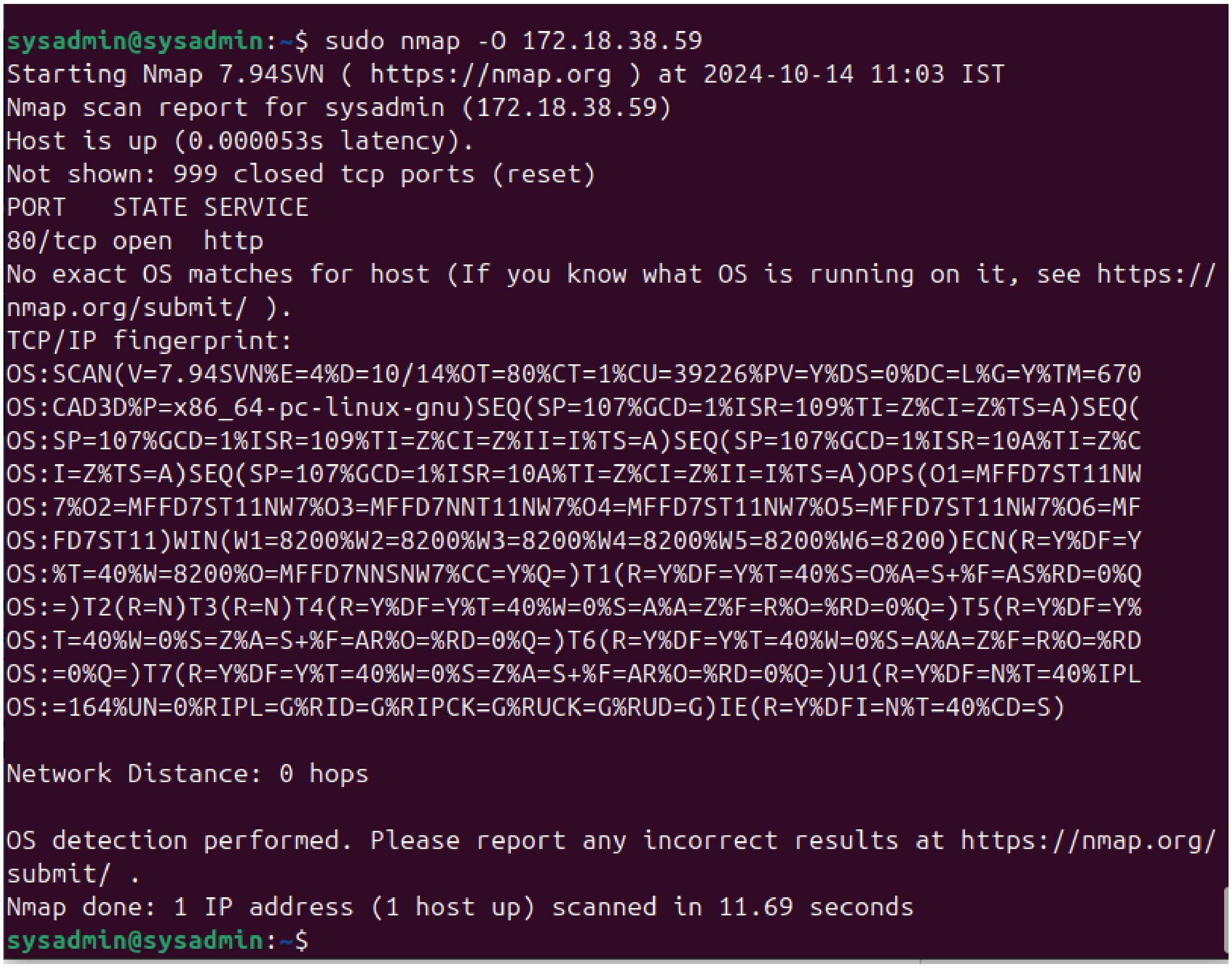
```
sysadmin@sysadmin:~$ cat output.txt
# Nmap 7.94SVN scan initiated Mon Oct 14 11:11:05 2024 as: nmap -iL hosts.txt -o
N output.txt
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000073s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT    STATE SERVICE
80/tcp  open  http
631/tcp open  ipp

Nmap scan report for sysadmin (127.0.0.2)
Host is up (0.000081s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE
80/tcp open  http

Nmap scan report for localhost (127.0.0.3)
Host is up (0.000078s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE
80/tcp open  http

Nmap scan report for localhost (127.0.0.4)
Host is up (0.000087s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE
80/tcp open  http
```

4.Scan using TCP or UDP protocols.



```
sysadmin@sysadmin:~$ nmap -sT 127.0.0.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-14 10:59 IST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000025s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT    STATE SERVICE
80/tcp  open  http
631/tcp open  ipp

Nmap done: 1 IP address (1 host up) scanned in 0.02 seconds
sysadmin@sysadmin:~$ nmap -sU 127.0.0.1 -F
You requested a scan type which requires root privileges.
QUITTING!
sysadmin@sysadmin:~$ sudo nmap -sU 127.0.0.1 -F
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-14 11:00 IST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000020s latency).
Not shown: 98 closed udp ports (port-unreach)
PORT     STATE         SERVICE
631/udp  open|filtered ipp
5353/udp open|filtered zeroconf

Nmap done: 1 IP address (1 host up) scanned in 1.30 seconds
sysadmin@sysadmin:~$
```

5.Guess the O.S. running on the hosts.



```
sysadmin@sysadmin:~$ sudo nmap -O 172.18.38.59
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-14 11:03 IST
Nmap scan report for sysadmin (172.18.38.59)
Host is up (0.000053s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
80/tcp open  http
No exact OS matches for host (If you know what OS is running on it, see https://
nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=10/14%OT=80%CT=1%CU=39226%PV=Y%DS=0%DC=L%G=Y%TM=670
OS:CAD3D%P=x86_64-pc-linux-gnu)SEQ(SP=107%GCD=1%ISR=109%TI=Z%CI=Z%TS=A)SEQ(
OS:SP=107%GCD=1%ISR=109%TI=Z%CI=Z%II=I%TS=A)SEQ(SP=107%GCD=1%ISR=10A%TI=Z%C
OS:I=Z%TS=A)SEQ(SP=107%GCD=1%ISR=10A%TI=Z%CI=Z%II=I%TS=A)OPS(O1=MFFD7ST11NW
OS:7%O2=MFFD7ST11NW7%O3=MFFD7NNT11NW7%O4=MFFD7ST11NW7%O5=MFFD7ST11NW7%O6=MF
OS:FD7ST11)WIN(W1=8200%W2=8200%W3=8200%W4=8200%W5=8200%W6=8200)ECN(R=Y%DF=Y
OS:%T=40%W=8200%O=MFFD7NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q
OS:=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%
OS:T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD
OS:=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL
OS:=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/
submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.69 seconds
sysadmin@sysadmin:~$
```

Conclusion:

Nmap’s versatility makes it an essential tool for network security. Its range of commands can accommodate simple network scans to complex security audits. By mastering these basic commands, network administrators can effectively monitor and secure their networks.

Nmap allows you to discover live devices, open ports, and services running on a network, providing valuable information for identifying potential security vulnerabilities..