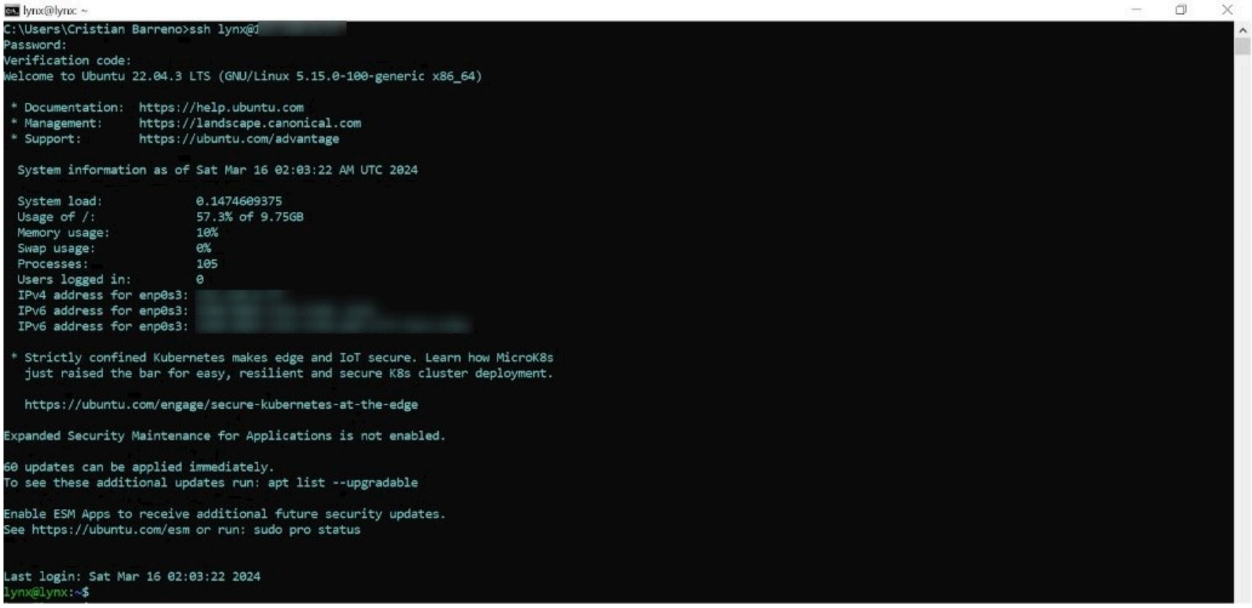
Name: Cristian Barreno

Network Mapper (NMAP)

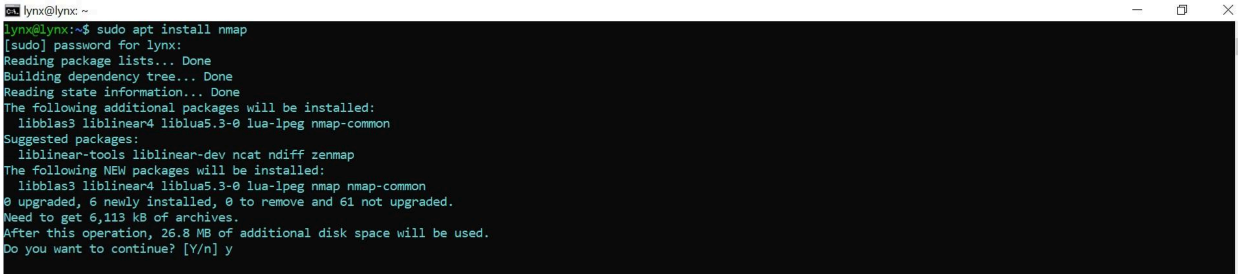
EXERCISE 1 – installing and using NMAP

Task 1 - Installation

sudo apt install nmap -y
Using the Advanced Package Tool install the nmap application.



```
C:\Users\Cristian Barreno>ssh lynx@1[redacted]
Password:
Verification code:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-100-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Sat Mar 16 02:03:22 AM UTC 2024

  System load:            0.1474609375
  Usage of /:             57.3% of 9.75GB
  Memory usage:           10%
  Swap usage:             0%
  Processes:              105
  Users logged in:        0
  IPv4 address for enp0s3: [redacted]
  IPv6 address for enp0s3: [redacted]
  IPv6 address for enp0s3: [redacted]

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

60 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


Last login: Sat Mar 16 02:03:22 2024
lynx@lynx:~$
```



```
lynx@lynx:~$ sudo apt install nmap
[sudo] password for lynx:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libblas3 liblinear4 liblua5.3-0 lua-lpeg nmap-common
Suggested packages:
  liblinear-tools liblinear-dev ncat ndiff zenmap
The following NEW packages will be installed:
  libblas3 liblinear4 liblua5.3-0 lua-lpeg nmap nmap-common
0 upgraded, 6 newly installed, 0 to remove and 61 not upgraded.
Need to get 6,113 kB of archives.
After this operation, 26.8 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
```

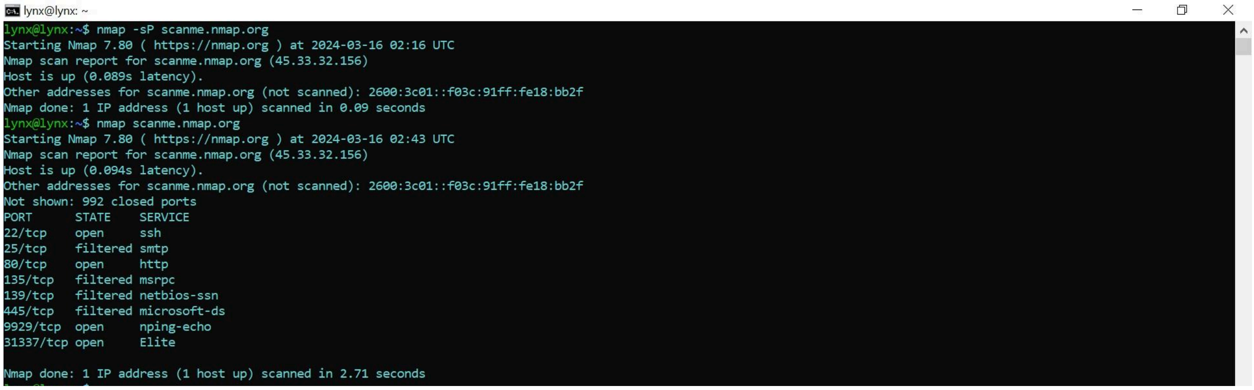
Task 2 – Basic Single Target Usage

Using the following link:
https://www.freecodecamp.org/news/what-is-nmap-and-how-to-use-it-a-tutorial-for-the-greatest-scanning-tool-of-all-time/

Via the CLI in your Ubuntu Server you will be conducting internet scans vs a single host.

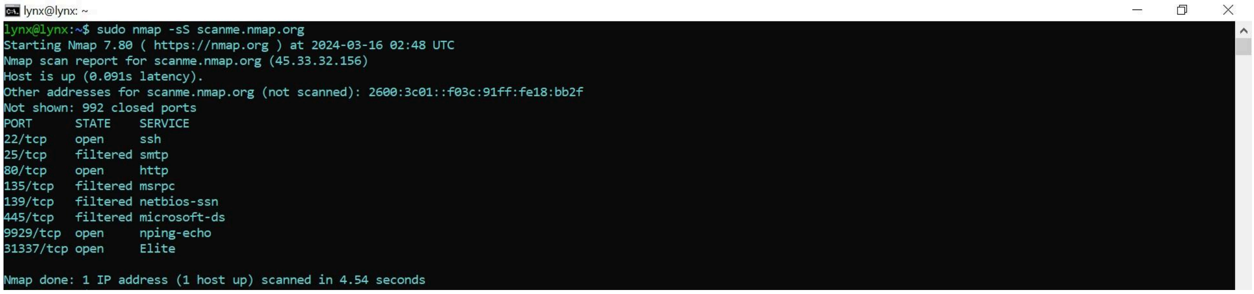
Read step by step the above website tutorial and conduct the specific simple scanning listed below via nmap against **scanme.nmap.org**

1. **Basic Scan**



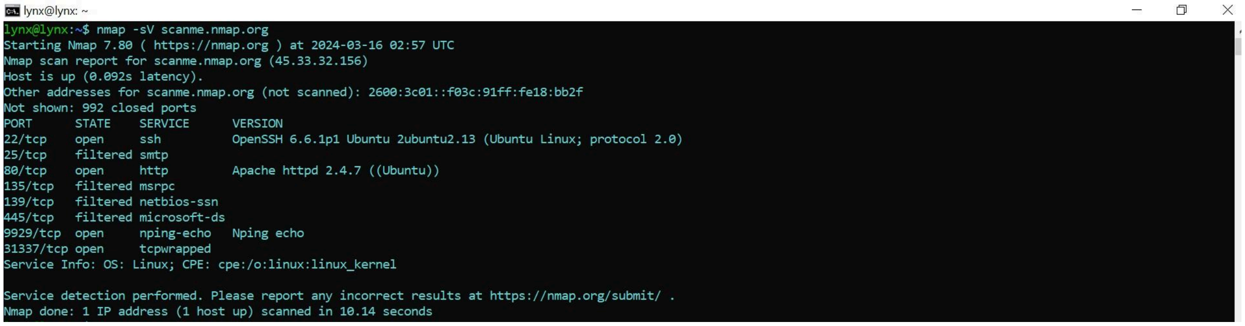
```
lynx@lynx:~$ nmap -sP scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2024-03-16 02:16 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.089s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds
lynx@lynx:~$ nmap scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2024-03-16 02:43 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.094s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 992 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
25/tcp    filtered smtp
80/tcp    open     http
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
9929/tcp  open     nping-echo
31337/tcp open     Elite

Nmap done: 1 IP address (1 host up) scanned in 2.71 seconds
```

2. **Stealth scan**



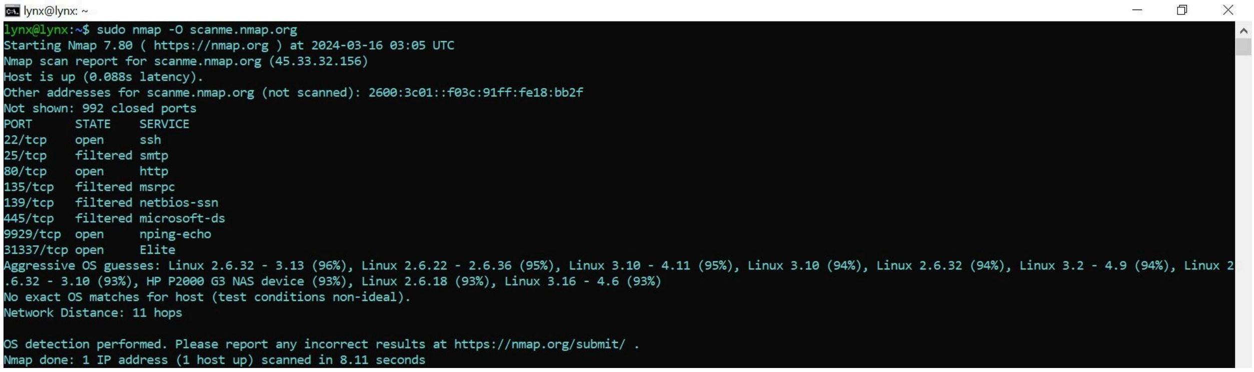
```
lynx@lynx:~$ sudo nmap -sS scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2024-03-16 02:48 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.091s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 992 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
25/tcp    filtered smtp
80/tcp    open     http
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
9929/tcp  open     nping-echo
31337/tcp open     Elite

Nmap done: 1 IP address (1 host up) scanned in 4.54 seconds
```

3. **Version ScanPort Scanning**



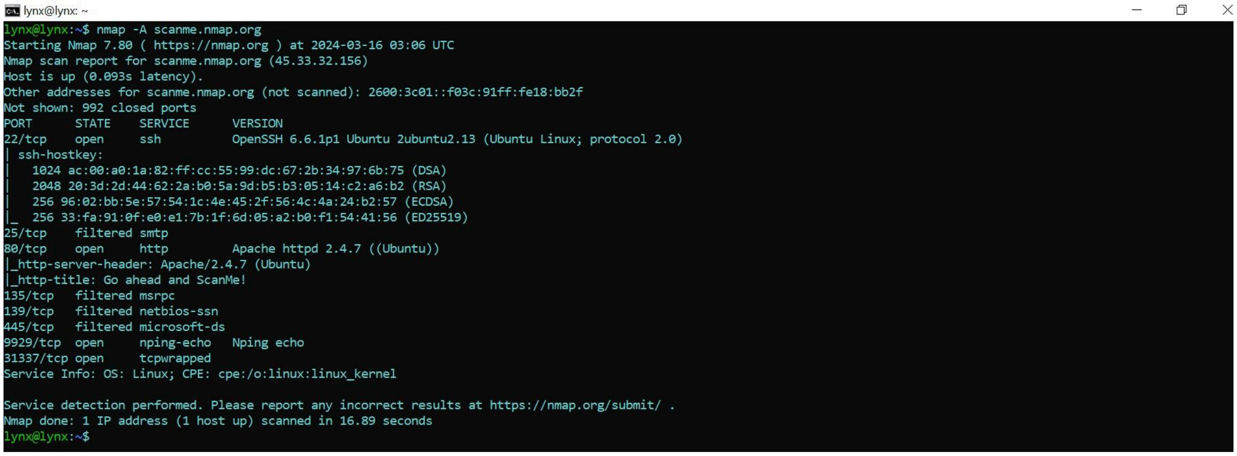
```
lynx@lynx:~$ nmap -sV scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2024-03-16 02:57 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.092s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 992 closed ports
PORT      STATE    SERVICE      VERSION
22/tcp    open     ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
25/tcp    filtered smtp
80/tcp    open     http         Apache httpd 2.4.7 ((Ubuntu))
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
9929/tcp  open     nping-echo   Nping echo
31337/tcp open     tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.14 seconds
```

4. **OS Scan**



```
lynx@lynx:~$ sudo nmap -O scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2024-03-16 03:05 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.088s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 992 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
25/tcp    filtered smtp
80/tcp    open     http
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
9929/tcp  open     nping-echo
31337/tcp open     Elite
Aggressive OS guesses: Linux 2.6.32 - 3.13 (96%), Linux 2.6.22 - 2.6.36 (95%), Linux 3.10 - 4.11 (95%), Linux 3.10 (94%), Linux 2.6.32 (94%), Linux 3.2 - 4.9 (94%), Linux 2
.6.32 - 3.10 (93%), HP P2000 G3 NAS device (93%), Linux 2.6.18 (93%), Linux 3.16 - 4.6 (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 11 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.11 seconds
```

5. **Aggressive Scan**



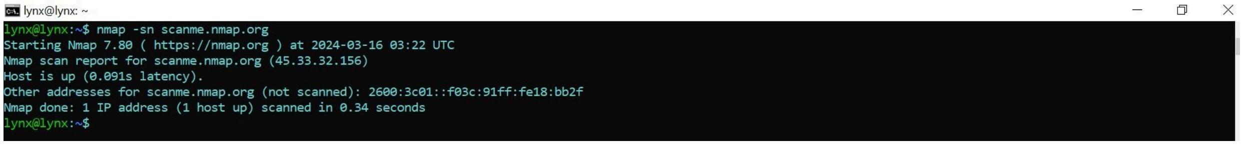
```
lynx@lynx:~$ nmap -A scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2024-03-16 03:06 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.093s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 992 closed ports
PORT      STATE    SERVICE      VERSION
22/tcp    open     ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)
|   2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)
|   256 96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (ECDSA)
|_  256 33:fa:91:0f:e0:e1:7b:1f:6d:05:a2:b0:f1:54:41:56 (ED25519)
25/tcp    filtered smtp
80/tcp    open     http         Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Go ahead and ScanMe!
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
9929/tcp  open     nping-echo   Nping echo
31337/tcp open     tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.89 seconds
lynx@lynx:~$
```

Task 3 – Discovery Scans

Nmap, the Network Mapper, can conduct discovery scans in a local network using various techniques to identify live hosts, open ports, and services running on those ports.
These scans are essential for network administrators to understand the topology of their network, the hosts on their network, and identify potential security vulnerabilities.

1. **ICMP Echo (Ping) Scan:**

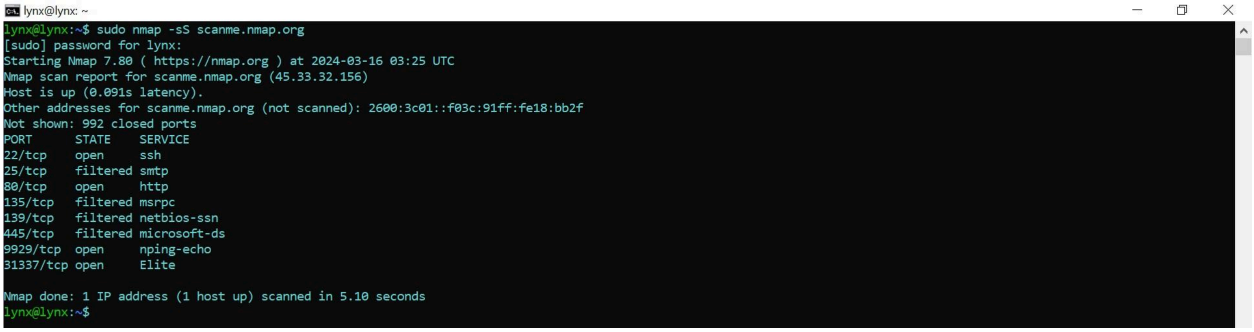
Nmap sends ICMP echo requests (ping) to the target hosts to check if they are online and responsive.
This scan is performed using the -sn or --ping option.



```
lynx@lynx:~$ nmap -sn scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2024-03-16 03:22 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.091s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Nmap done: 1 IP address (1 host up) scanned in 0.34 seconds
lynx@lynx:~$
```

2. TCP SYN Scan:

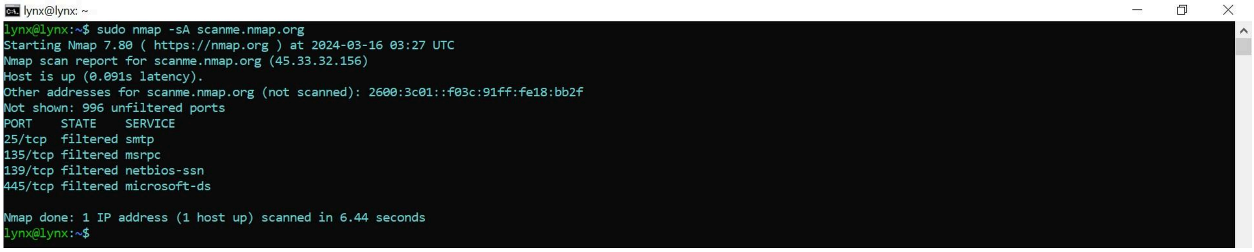
Nmap sends TCP SYN packets to the target hosts and analyzes their responses to determine if the ports are open, closed, or filtered.
This scan is performed using the -sS option.



```
lynx@lynx:~$ sudo nmap -sS scanme.nmap.org
[sudo] password for lynx:
Starting Nmap 7.80 ( https://nmap.org ) at 2024-03-16 03:25 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.091s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 992 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
25/tcp    filtered smtp
80/tcp    open     http
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
9929/tcp  open     nping-echo
31337/tcp open     Elite

Nmap done: 1 IP address (1 host up) scanned in 5.10 seconds
lynx@lynx:~$
```

3. TCP ACK Scan:

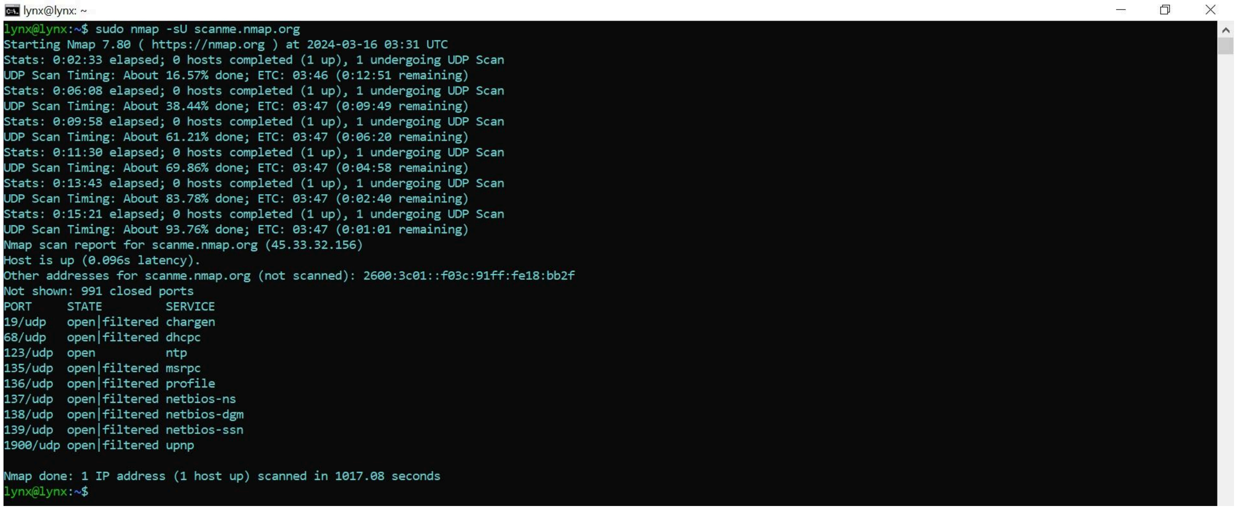
Nmap sends TCP ACK packets to the target hosts to determine if the ports are filtered by firewalls.
This scan is performed using the -sA option.



```
lynx@lynx:~$ sudo nmap -sA scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2024-03-16 03:27 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.091s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 996 unfiltered ports
PORT    STATE    SERVICE
25/tcp  filtered smtp
135/tcp filtered msrpc
139/tcp filtered netbios-ssn
445/tcp filtered microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 6.44 seconds
lynx@lynx:~$
```

4. UDP Scan:

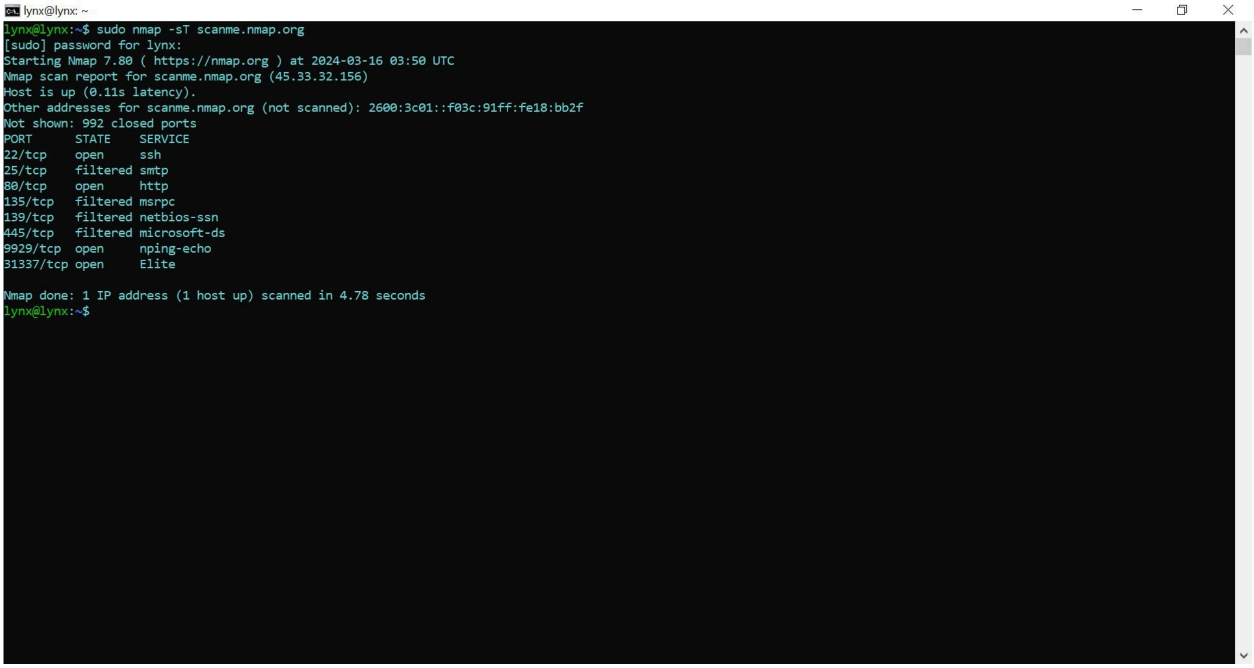
Nmap sends UDP packets to the target hosts to identify open UDP ports.
This scan is performed using the -sU option.



```
lynx@lynx:~$ sudo nmap -sU scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2024-03-16 03:31 UTC
Stats: 0:02:33 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 16.57% done; ETC: 03:46 (0:12:51 remaining)
Stats: 0:06:08 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 38.44% done; ETC: 03:47 (0:09:49 remaining)
Stats: 0:09:58 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 61.21% done; ETC: 03:47 (0:06:20 remaining)
Stats: 0:11:30 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 69.86% done; ETC: 03:47 (0:04:58 remaining)
Stats: 0:13:43 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 83.78% done; ETC: 03:47 (0:02:40 remaining)
Stats: 0:15:21 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 93.76% done; ETC: 03:47 (0:01:01 remaining)
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.096s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 991 closed ports
PORT     STATE         SERVICE
19/udp   open|filtered chargen
68/udp   open|filtered dhcpc
123/udp  open          ntp
135/udp  open|filtered msrpc
136/udp  open|filtered profile
137/udp  open|filtered netbios-ns
138/udp  open|filtered netbios-dgm
139/udp  open|filtered netbios-ssn
1900/udp open|filtered upnp

Nmap done: 1 IP address (1 host up) scanned in 1017.08 seconds
lynx@lynx:~$
```

5. TCP Connect Scan:

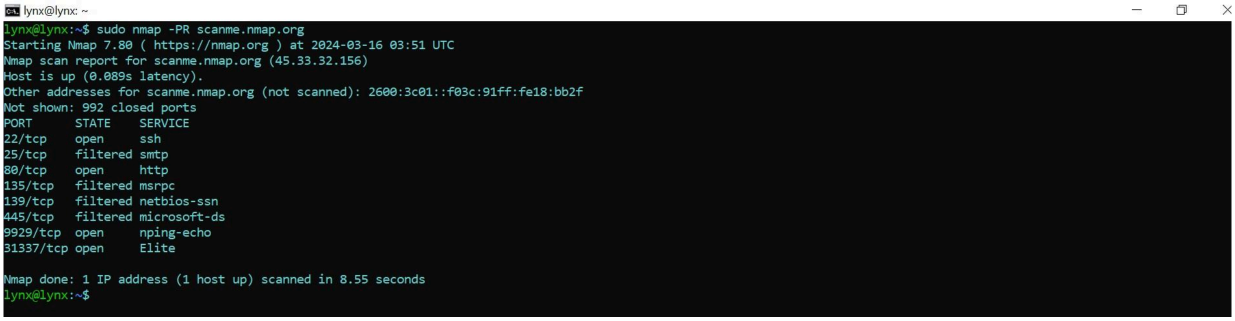
Nmap attempts to establish a full TCP connection with the target hosts to determine if the ports are open.
This scan is performed using the -sT option.



```
lynx@lynx:~$ sudo nmap -sT scanme.nmap.org
[sudo] password for lynx:
Starting Nmap 7.80 ( https://nmap.org ) at 2024-03-16 03:50 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.11s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 992 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
25/tcp    filtered smtp
80/tcp    open     http
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
9929/tcp  open     nping-echo
31337/tcp open     Elite

Nmap done: 1 IP address (1 host up) scanned in 4.78 seconds
lynx@lynx:~$
```

6. ARP Scan:

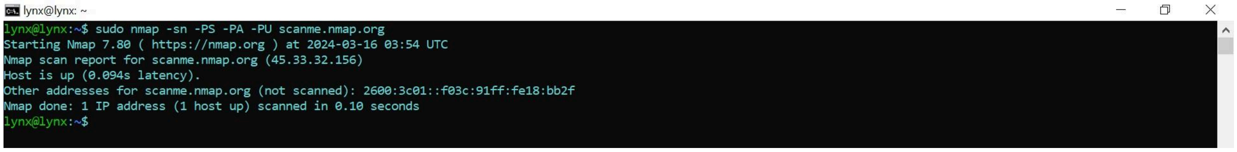
Nmap uses ARP requests to discover hosts on the local network without sending packets to each individual IP address.
This scan is performed using the -PR option.



```
lynx@lynx:~$ sudo nmap -PR scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2024-03-16 03:51 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.089s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 992 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
25/tcp    filtered smtp
80/tcp    open     http
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
9929/tcp  open     nping-echo
31337/tcp open     Elite

Nmap done: 1 IP address (1 host up) scanned in 8.55 seconds
lynx@lynx:~$
```

7. Host Discovery:

Nmap combines various discovery techniques, such as ARP scanning, ICMP ping, and TCP ping, to identify live hosts in the network.
This scan is performed using the -sn or --ping option along with other scan types.



```
lynx@lynx:~$ sudo nmap -sn -PS -PA -PU scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2024-03-16 03:54 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.094s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
lynx@lynx:~$
```