NMAP Scans

Written by Tyler Weiss

Assignment

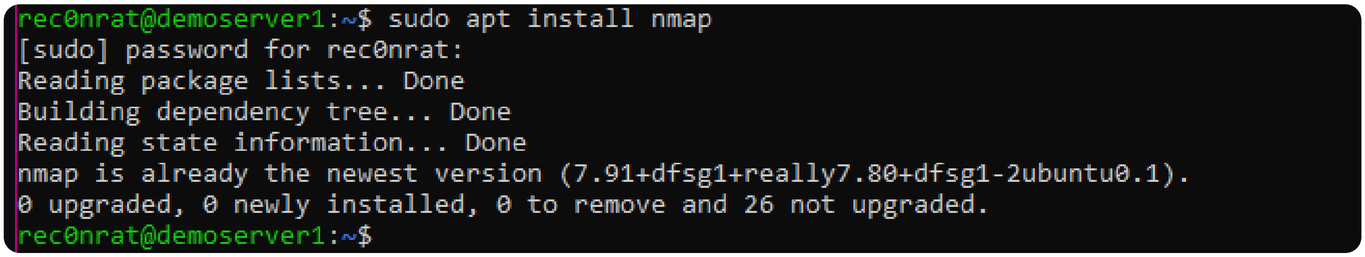
Perform the different namp scans against 'scanme.nmap.org' and your home network. Briefly explain each scan and it's results.

Exercise 1

Task 1 - Install

Install nmap the Linux server using the following command:

```
sudo apt install nmap
```



```
rec0nrat@demoserver1:~$ sudo apt install nmap
[sudo] password for rec0nrat:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
nmap is already the newest version (7.91+dfsg1+really7.80+dfsg1-2ubuntu0.1).
0 upgraded, 0 newly installed, 0 to remove and 26 not upgraded.
rec0nrat@demoserver1:~$
```

Task 2 - Basic Single-Target Use

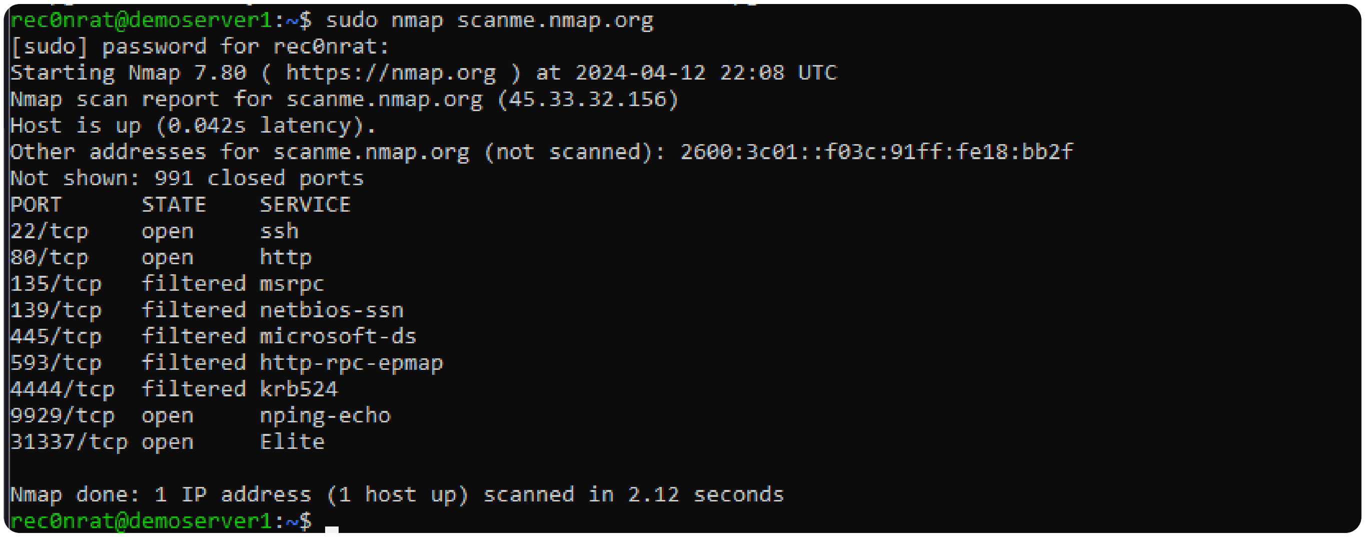
Using the following link:
https://www.freecodecamp.org/news/what-is-nmap-and-how-to-use-it-a-tutorial-for-the-greatest-

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

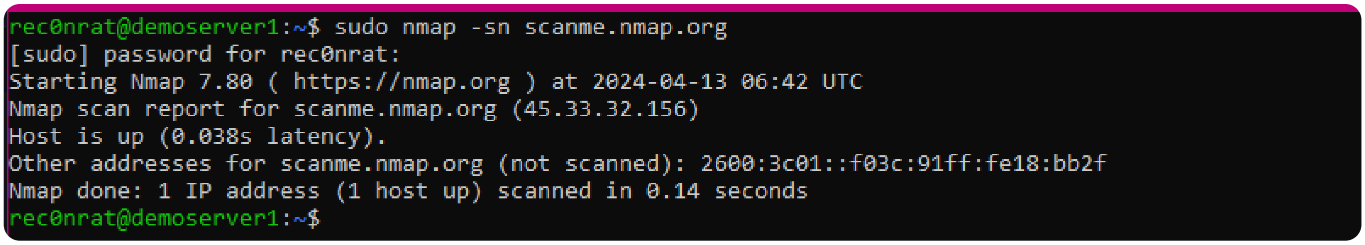
1. Basic Scan
2. Stealth Scan
3. Version Scan
4. Port Scan
5. OS Scan
6. Aggressive Scan
   Make sure the target of your scans are scanme.nmap.org

Basic Scan

Using no options and a single target or range of targets will perform a SYN scan of the top 1000 well-known ports. Using the '-sn' or '-sp' performs a default ping scan for host discovery, without scanning any ports, and reports if the host is up.



```
rec0nrat@demoserver1:~$ sudo nmap scanme.nmap.org
[sudo] password for rec0nrat:
Starting Nmap 7.80 ( https://nmap.org ) at 2024-04-12 22:08 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.042s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 991 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
80/tcp    open     http
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
593/tcp   filtered http-rpc-epmap
4444/tcp  filtered krb524
9929/tcp  open     nping-echo
31337/tcp open     Elite

Nmap done: 1 IP address (1 host up) scanned in 2.12 seconds
rec0nrat@demoserver1:~$
```

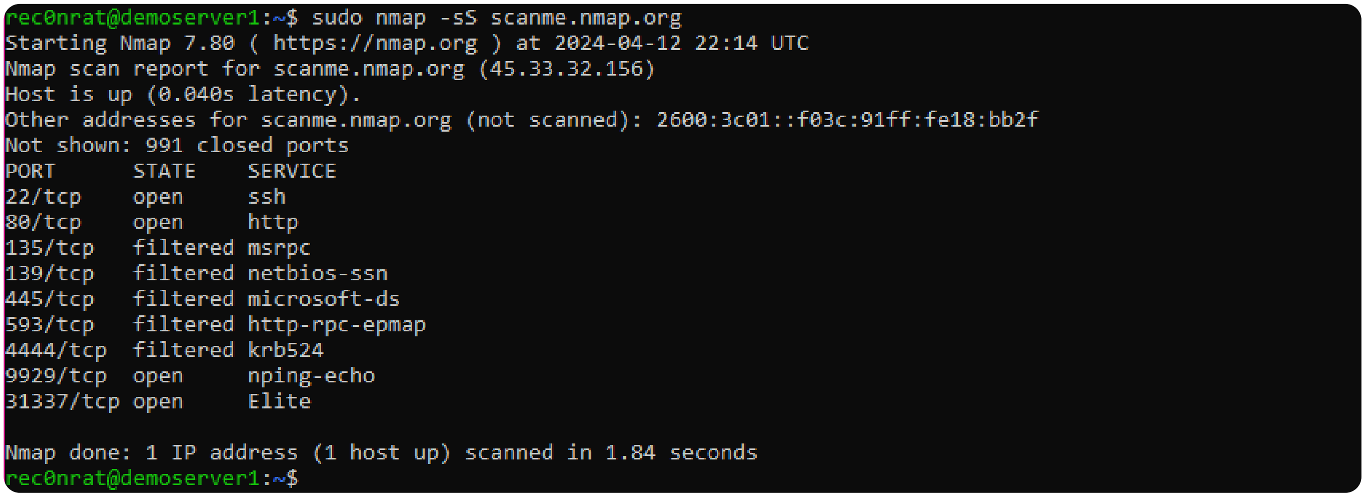


```
rec0nrat@demoserver1:~$ sudo nmap -sn scanme.nmap.org
[sudo] password for rec0nrat:
Starting Nmap 7.80 ( https://nmap.org ) at 2024-04-13 06:42 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.038s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds
rec0nrat@demoserver1:~$
```

The results of the first scan show all TCP ports that replied, their current state and associated service. The second scan results show the associated IPv4 and IPv6 addresses of 'scanme.nmap.org' along with the 'Host is up' status.

Stealth Scan

By using the '-sS' we can perform a SYN or Stealth scan. This will scan a host's ports and if a SYN\ACK is returned reports that the port is open. The Stealth scan does not complete the 3-way-handshake.

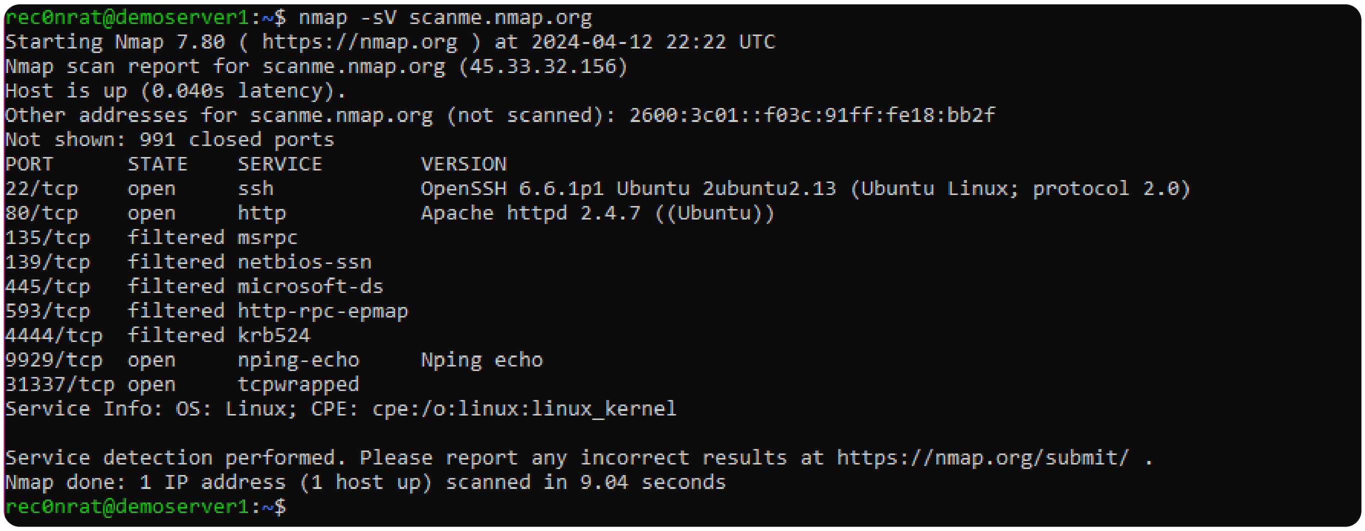


```
rec0nrat@demoserver1:~$ sudo nmap -sS scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2024-04-12 22:14 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.040s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 991 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
80/tcp    open     http
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
593/tcp   filtered http-rpc-epmap
4444/tcp  filtered krb524
9929/tcp  open     nping-echo
31337/tcp open     Elite

Nmap done: 1 IP address (1 host up) scanned in 1.84 seconds
rec0nrat@demoserver1:~$
```

The results of the SYN scan are the same as the default nmap scan because it is the same scan.

Version Scan

A Version scan will attempt to identify service and versions running on particular ports. It is not completely accurate but it will make the best guess based in the information it receives. CVEs can be discovered based off service versions. To perform a Version scan use the '-sV' option.

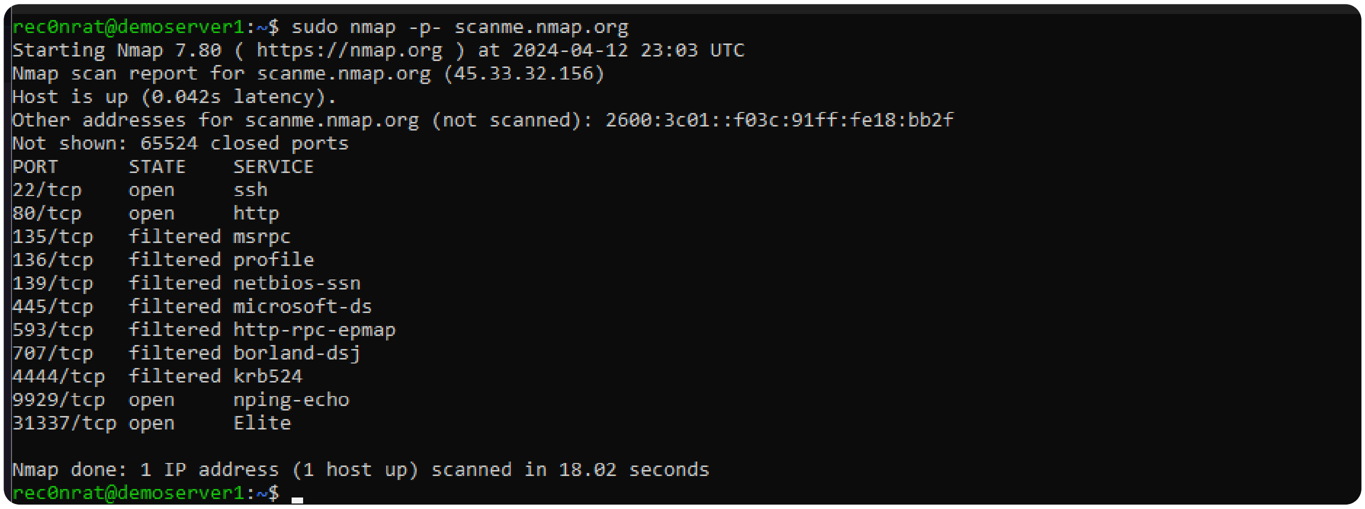


```
rec0nrat@demoserver1:~$ nmap -sV scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2024-04-12 22:22 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.040s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 991 closed ports
PORT      STATE    SERVICE        VERSION
22/tcp    open     ssh            OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
80/tcp    open     http           Apache httpd 2.4.7 ((Ubuntu))
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
593/tcp   filtered http-rpc-epmap
4444/tcp  filtered krb524
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 9.04 seconds
rec0nrat@demoserver1:~$
```

The Version scan produces the same output as the previous ones but also adds a version column. Nmap sends specialized, protocol specific, packets to different ports in order to determine services and versions. The above results show that openssh 6.6.1p1, apache httpd 2.4.7, and nping echo are running on the target system.

Port Scan

Most of the discovery scans performed by nmap scan ports but to be more specific you can use the '-p' option followed by a port range or list. By default namp only scans TCP ports. You can specify port UDP or TCP by using either 'T:<PORTS>' or 'U:<PORTS>'. You can also use '-p-' for all ports, '-sU' for UDP ports or '--top-ports' followed by the number of ports.

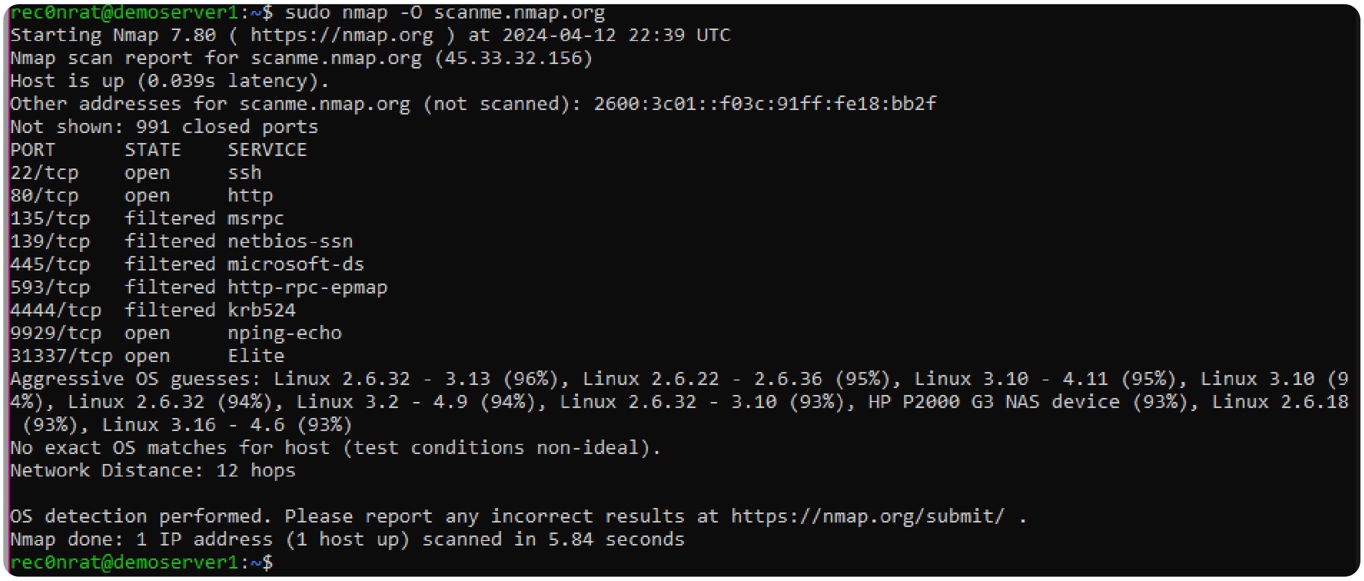


```
rec0nrat@demoserver1:~$ sudo nmap -p- scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2024-04-12 23:03 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.042s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 65524 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
80/tcp    open     http
135/tcp   filtered msrpc
136/tcp   filtered profile
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
593/tcp   filtered http-rpc-epmap
707/tcp   filtered borland-dsj
4444/tcp  filtered krb524
9929/tcp  open     nping-echo
31337/tcp open     Elite

Nmap done: 1 IP address (1 host up) scanned in 18.02 seconds
rec0nrat@demoserver1:~$ 
```

This Port scan, tough not displayed, checked all 65535 ports over TCP. The result is the same as before because no other ports are open.

OS Scan

OS scans can use TCP/IP fingerprinting to resolve a host's OS and uptime. The scan results will display the percent of accuracy of the OS discovery. An OS scan can be performed using the '-O' option.

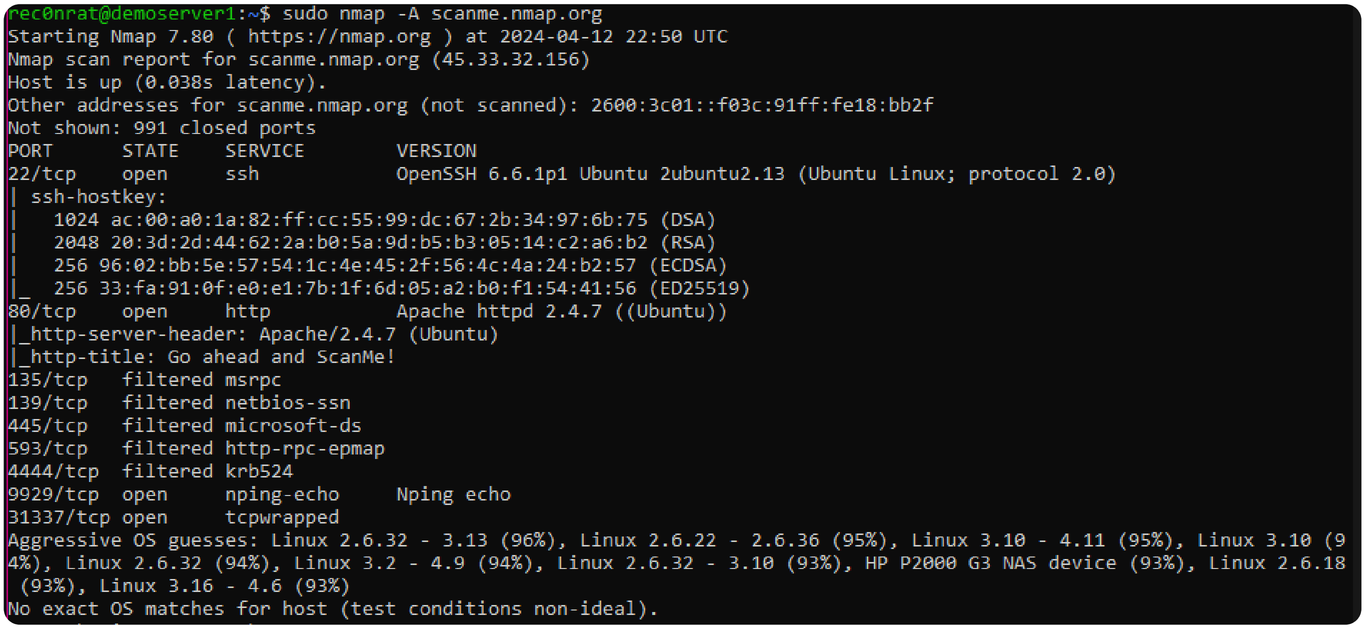


```
rec0nrat@demoserver1:~$ sudo nmap -O scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2024-04-12 22:39 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.039s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 991 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
80/tcp    open     http
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
593/tcp   filtered http-rpc-epmap
4444/tcp  filtered krb524
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 (9
4%), 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: 12 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 5.84 seconds
rec0nrat@demoserver1:~$
```

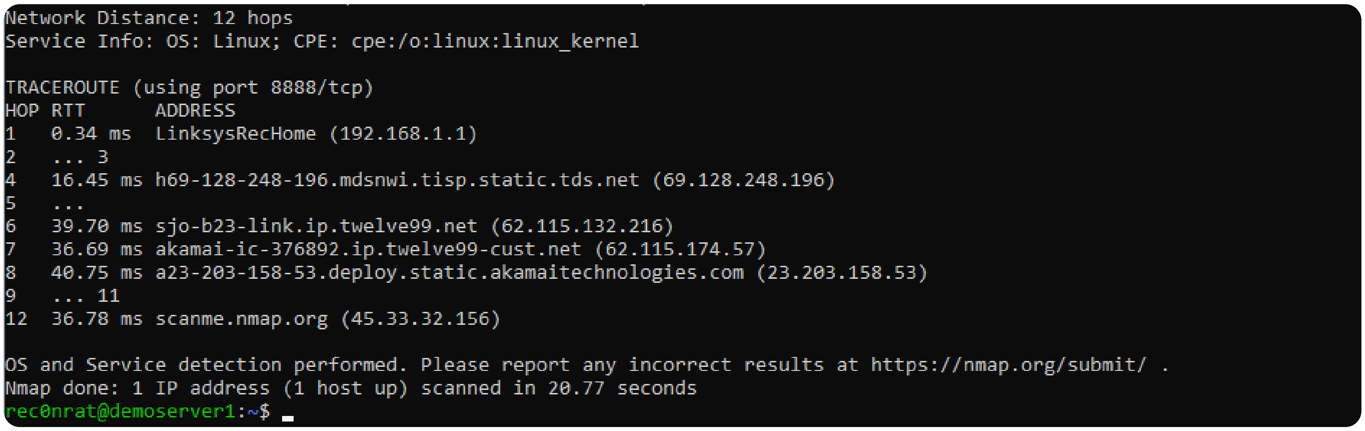
The scan results are the as the basic TCP SYN scan except that nmap also sent specialized packets to discern the OS. Below the port scan results are the potential OS versions and the percent of reliability of these guesses.

Aggressive Scan

The Aggressive scan performs OS detection, version detection, script scanning, and traceroute. It is extremely noisy but provides better results. An Aggressive scan can be performed using the '-A' option.



```
rec0nrat@demoserver1:~$ sudo nmap -A scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2024-04-12 22:50 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.038s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 991 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)
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
593/tcp   filtered http-rpc-epmap
4444/tcp  filtered krb524
9929/tcp  open     nping-echo     Nping echo
31337/tcp open     tcpwrapped
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 (9
4%), 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: 12 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 8888/tcp)
HOP RTT      ADDRESS
1   0.34 ms  LinksysRecHome (192.168.1.1)
2   ... 3
4   16.45 ms h69-128-248-196.mdsnwi.tisp.static.tds.net (69.128.248.196)
5   ...
6   39.70 ms sjo-b23-link.ip.twelve99.net (62.115.132.216)
7   36.69 ms akamai-ic-376892.ip.twelve99-cust.net (62.115.174.57)
8   40.75 ms a23-203-158-53.deploy.static.akamaitechnologies.com (23.203.158.53)
9   ... 11
12  36.78 ms scanme.nmap.org (45.33.32.156)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.77 seconds
rec0nrat@demoserver1:~$
```

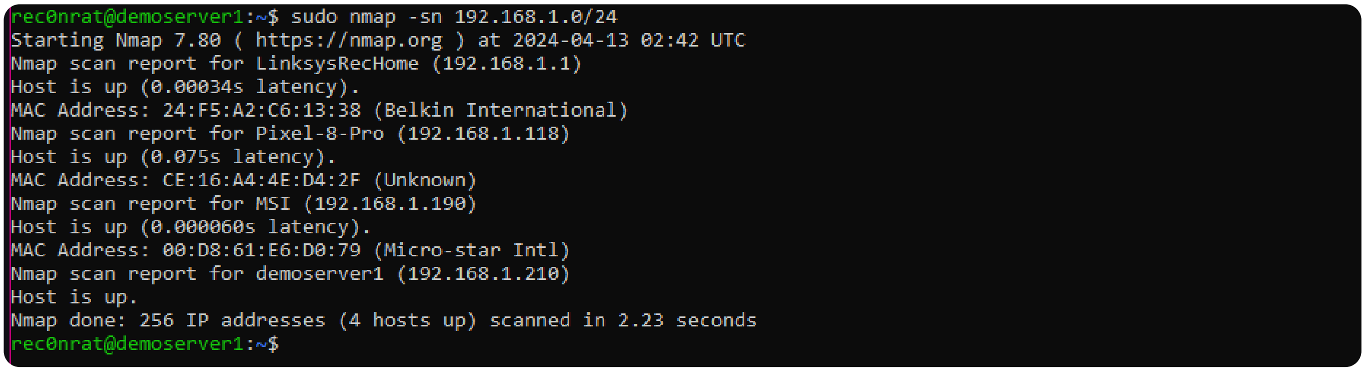
The Aggressive scan also used a basic SYN scan for the ports but has yielded slightly more information. An SSH host key, http header, OS version, and traceroute results were produced using this scan.

Task 3 - Discovery Scans

Conduct a discovery scan of your host network and note the outcome.

ICMP Echo (Ping) Scan

A Ping scan or performs host discovery when used with a range of IP address. By using the network ID with CIDR notation a the entire network range will be scanned for replies from ICMP echo requests. The '-sn' flag can be used to perform a Ping scan.

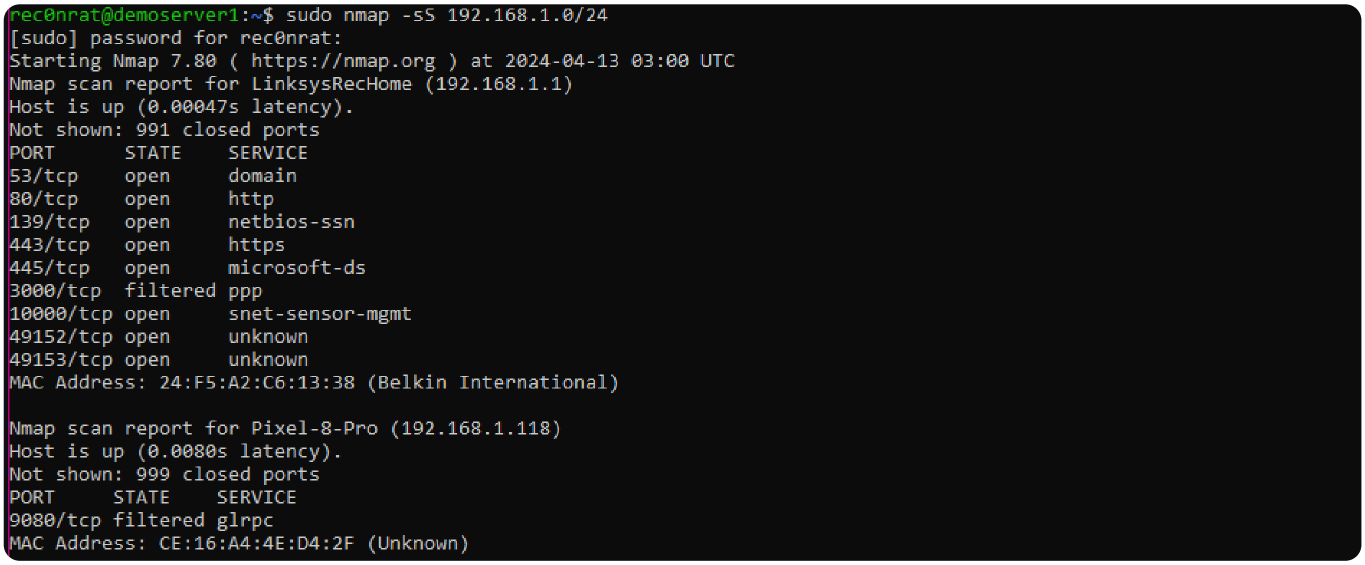


```
rec0nrat@demoserver1:~$ sudo nmap -sn 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2024-04-13 02:42 UTC
Nmap scan report for LinksysRecHome (192.168.1.1)
Host is up (0.00034s latency).
MAC Address: 24:F5:A2:C6:13:38 (Belkin International)
Nmap scan report for Pixel-8-Pro (192.168.1.118)
Host is up (0.075s latency).
MAC Address: CE:16:A4:4E:D4:2F (Unknown)
Nmap scan report for MSI (192.168.1.190)
Host is up (0.000060s latency).
MAC Address: 00:D8:61:E6:D0:79 (Micro-star Intl)
Nmap scan report for demoserver1 (192.168.1.210)
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.23 seconds
rec0nrat@demoserver1:~$
```

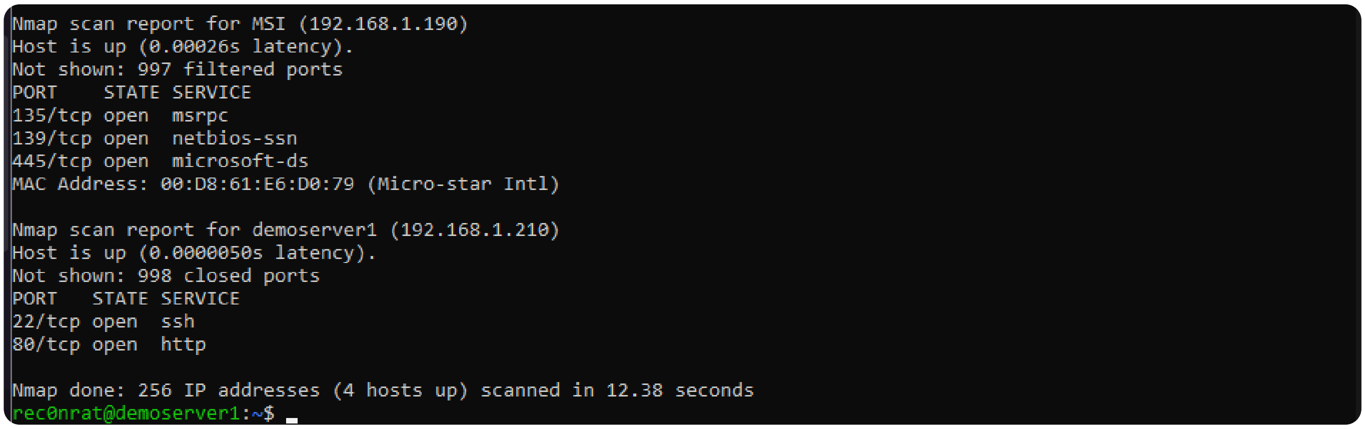
The results of the standard Ping scan show that 4 hosts are up and retrieves their IPv4, IPv6, MAC address and host name. Remember that a Ping scan does not send packets to verify open ports.

TCP SYN Scan

As described earlier, a SYN or Stealth scan will send wait for a SYN/ACK response to determine open ports. When using a network range the scan will discover open ports on hosts that respond.



```
rec0nrat@demoserver1:~$ sudo nmap -sS 192.168.1.0/24
[sudo] password for rec0nrat:
Starting Nmap 7.80 ( https://nmap.org ) at 2024-04-13 03:00 UTC
Nmap scan report for LinksysRecHome (192.168.1.1)
Host is up (0.00047s latency).
Not shown: 991 closed ports
PORT      STATE    SERVICE
53/tcp    open     domain
80/tcp    open     http
139/tcp   open     netbios-ssn
443/tcp   open     https
445/tcp   open     microsoft-ds
3000/tcp  filtered ppp
10000/tcp open     snet-sensor-mgmt
49152/tcp open     unknown
49153/tcp open     unknown
MAC Address: 24:F5:A2:C6:13:38 (Belkin International)

Nmap scan report for Pixel-8-Pro (192.168.1.118)
Host is up (0.0080s latency).
Not shown: 999 closed ports
PORT     STATE    SERVICE
9080/tcp filtered glrpc
MAC Address: CE:16:A4:4E:D4:2F (Unknown)
```

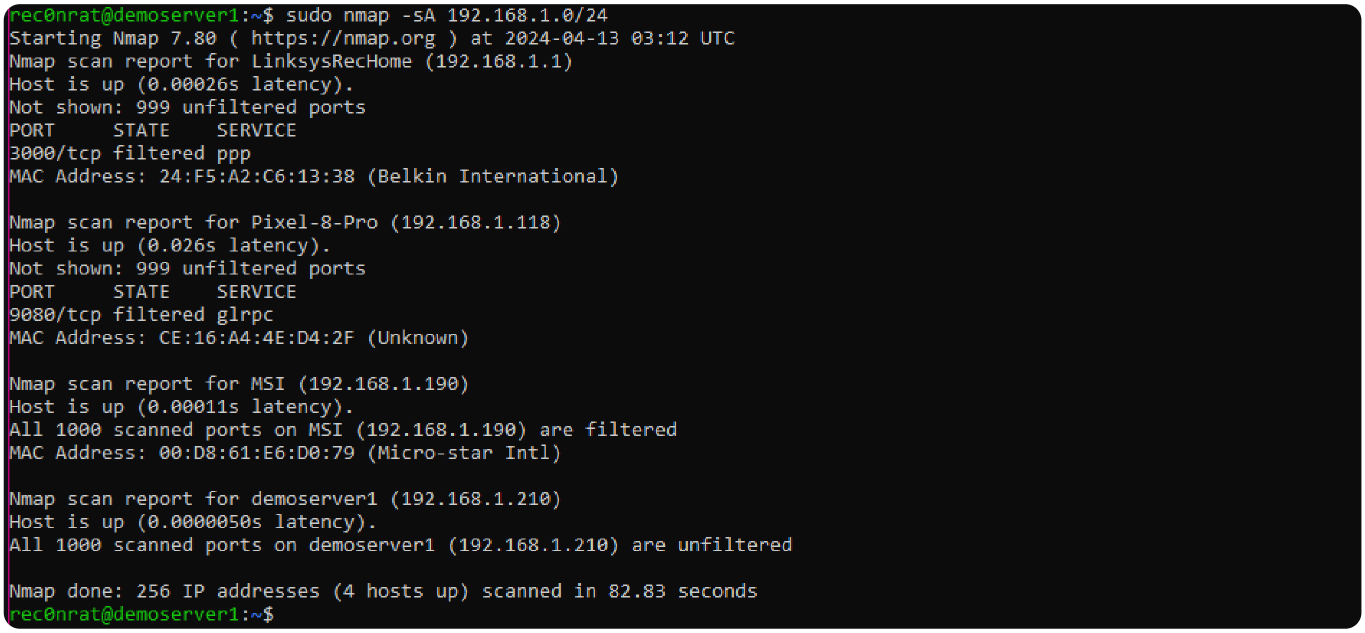


```
Nmap scan report for MSI (192.168.1.190)
Host is up (0.00026s latency).
Not shown: 997 filtered ports
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:D8:61:E6:D0:79 (Micro-star Intl)

Nmap scan report for demoserver1 (192.168.1.210)
Host is up (0.0000050s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 256 IP addresses (4 hosts up) scanned in 12.38 seconds
rec0nrat@demoserver1:~$ _
```

The standard SYN or Stealth scan produces the same results as the Ping scan except the port, state and service is displayed under each host. A host is considered 'up' if nmap is receiving any type of reply to it's SYN packets.

TCP ACK Scan

The ACK scan is different from the previous scans because it does not show open ports. It is used to map firewall rules. If a RST response is received a port is unfiltered and if no response or an ICMP unreachable error is received then the port is filtered. The '-sA' flag can be used to perform an ACK scan.

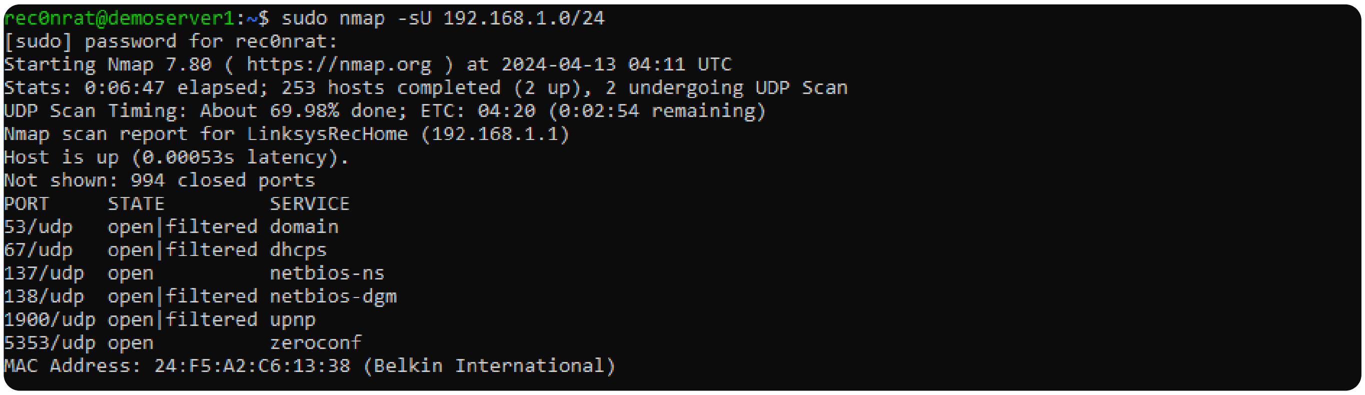


```
rec0nrat@demoserver1:~$ sudo nmap -sA 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2024-04-13 03:12 UTC
Nmap scan report for LinksysRecHome (192.168.1.1)
Host is up (0.00026s latency).
Not shown: 999 unfiltered ports
PORT     STATE    SERVICE
3000/tcp filtered ppp
MAC Address: 24:F5:A2:C6:13:38 (Belkin International)

Nmap scan report for Pixel-8-Pro (192.168.1.118)
Host is up (0.026s latency).
Not shown: 999 unfiltered ports
PORT     STATE    SERVICE
9080/tcp filtered glrpc
MAC Address: CE:16:A4:4E:D4:2F (Unknown)

Nmap scan report for MSI (192.168.1.190)
Host is up (0.00011s latency).
All 1000 scanned ports on MSI (192.168.1.190) are filtered
MAC Address: 00:D8:61:E6:D0:79 (Micro-star Intl)

Nmap scan report for demoserver1 (192.168.1.210)
Host is up (0.0000050s latency).
All 1000 scanned ports on demoserver1 (192.168.1.210) are unfiltered

Nmap done: 256 IP addresses (4 hosts up) scanned in 82.83 seconds
rec0nrat@demoserver1:~$
```

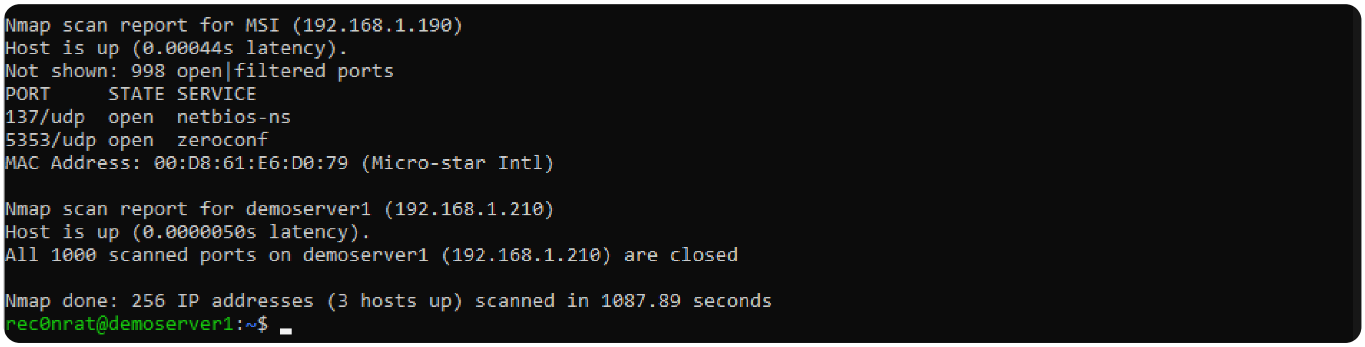
Notice that the ACK scan does not produce the same output as a SYN scan because the response to the ACK packets responses do not provide the information necessary to derive a state other than filtered or unfiltered. The results show that 2 ports are filtered out of 4 hosts.

UDP Scan

A UDP scan will send UDP packets, usually empty, and if a port responds then it is open. It is common to receive no response from open ports using UDP and thus no response is considered 'open|filtered'. If an ICMP unreachable response is received the port is closed. In order to determine 'open|filtered' are actually open nmap would need to send the proper service probes. The Service scan employs these service probes and thus using '-sV', with the UDP flag '-sU', would help resolve open ports.



```
rec0nrat@demoserver1:~$ sudo nmap -sU 192.168.1.0/24
[sudo] password for rec0nrat:
Starting Nmap 7.80 ( https://nmap.org ) at 2024-04-13 04:11 UTC
Stats: 0:06:47 elapsed; 253 hosts completed (2 up), 2 undergoing UDP Scan
UDP Scan Timing: About 69.98% done; ETC: 04:20 (0:02:54 remaining)
Nmap scan report for LinksysRecHome (192.168.1.1)
Host is up (0.00053s latency).
Not shown: 994 closed ports
PORT     STATE         SERVICE
53/udp   open|filtered domain
67/udp   open|filtered dhcps
137/udp  open          netbios-ns
138/udp  open|filtered netbios-dgm
1900/udp open|filtered upnp
5353/udp open          zeroconf
MAC Address: 24:F5:A2:C6:13:38 (Belkin International)
```

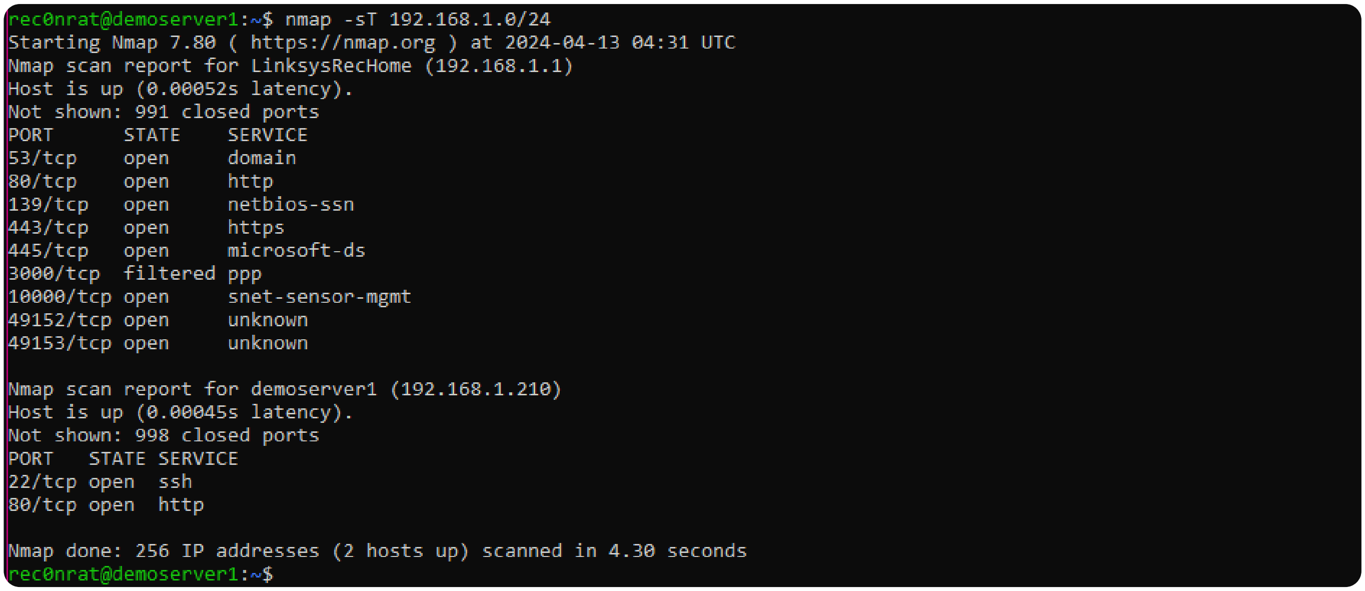


```
Nmap scan report for MSI (192.168.1.190)
Host is up (0.00044s latency).
Not shown: 998 open|filtered ports
PORT     STATE SERVICE
137/udp  open  netbios-ns
5353/udp open  zeroconf
MAC Address: 00:D8:61:E6:D0:79 (Micro-star Intl)

Nmap scan report for demoserver1 (192.168.1.210)
Host is up (0.0000050s latency).
All 1000 scanned ports on demoserver1 (192.168.1.210) are closed

Nmap done: 256 IP addresses (3 hosts up) scanned in 1087.89 seconds
rec0nrat@demoserver1:~$ 
```

The UDP scan results show the port, state and service of 3 hosts on the network. The 4th host may not be present because of the lack of information that UDP packet responses produce. UDP scan also takes a much longer time to complete than TCP oriented scans.

TCP Connect Scan

TCP scan completes a full 3-way-handshake over each port to determine if it is open. This behavior causes this scan to be loud and will set off IDS/IPS or be logged. SYN scans are a better choice achieving the same result. The only time a TCP scan is preferred when scanning IPv6 networks or when you don't have permission to create raw packets. The '-sT' can be used to perform a TCP scan.

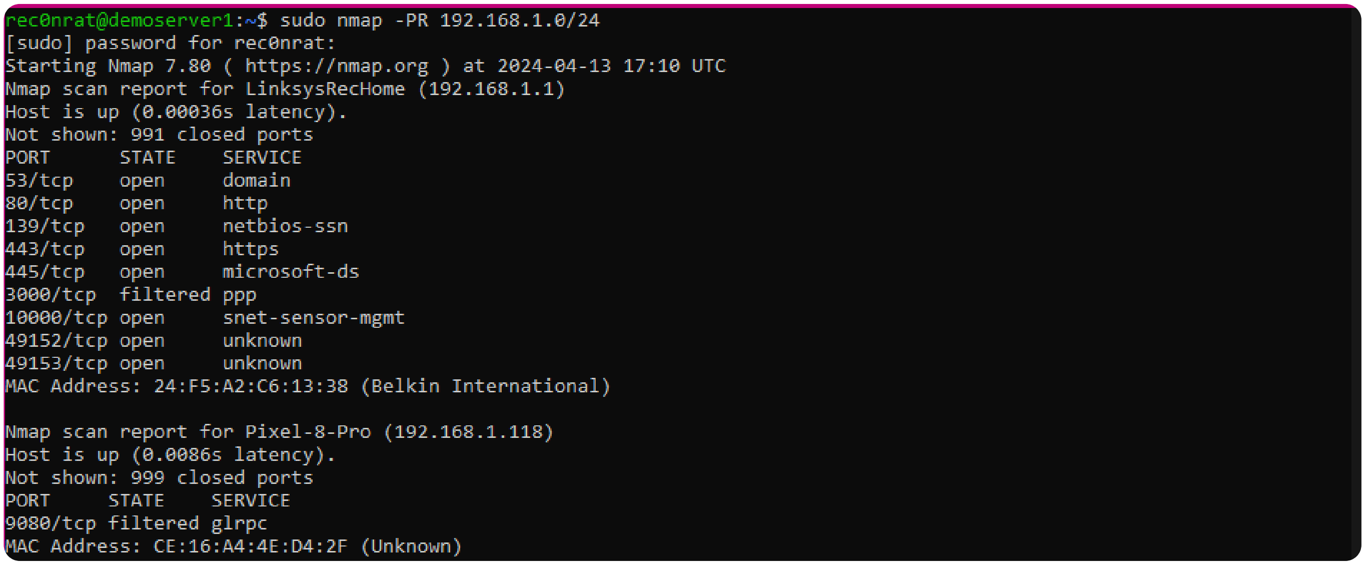


```
rec0nrat@demoserver1:~$ nmap -sT 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2024-04-13 04:31 UTC
Nmap scan report for LinksysRecHome (192.168.1.1)
Host is up (0.00052s latency).
Not shown: 991 closed ports
PORT      STATE    SERVICE
53/tcp    open     domain
80/tcp    open     http
139/tcp   open     netbios-ssn
443/tcp   open     https
445/tcp   open     microsoft-ds
3000/tcp  filtered ppp
10000/tcp open     snet-sensor-mgmt
49152/tcp open     unknown
49153/tcp open     unknown

Nmap scan report for demoserver1 (192.168.1.210)
Host is up (0.00045s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 256 IP addresses (2 hosts up) scanned in 4.30 seconds
rec0nrat@demoserver1:~$
```

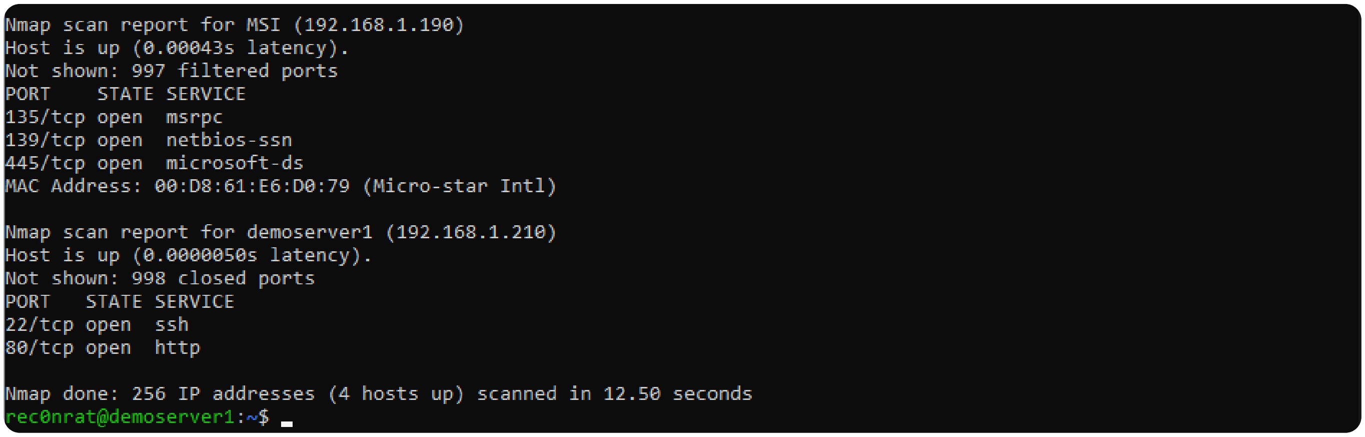
The TCP connect scan results are a slightly different than the SYN scan, showing only ports where a full 3-way-handshake was completed. Notice that 2 other hosts are not present because the full TCP connection was not completed for one reason or another on any ports. Also notice that sudo was not used in this command thus the program may not have the proper permission to send the packets that necessary to discover the the other 2 hosts. This was done because simulate an actual situation where a TCP connect scan would be used.

ARP Scan

ARP scan uses ARP requests to discover hosts on the network. This scan is used on LANs yields better results than a standard ping scan because although ICMP ping requests may be blocked, ARP requests are probably not. The '-PR' flag can be used to perform an ARP scan.



```
rec0nrat@demoserver1:~$ sudo nmap -PR 192.168.1.0/24
[sudo] password for rec0nrat:
Starting Nmap 7.80 ( https://nmap.org ) at 2024-04-13 17:10 UTC
Nmap scan report for LinksysRecHome (192.168.1.1)
Host is up (0.00036s latency).
Not shown: 991 closed ports
PORT      STATE    SERVICE
53/tcp    open     domain
80/tcp    open     http
139/tcp   open     netbios-ssn
443/tcp   open     https
445/tcp   open     microsoft-ds
3000/tcp  filtered ppp
10000/tcp open     snet-sensor-mgmt
49152/tcp open     unknown
49153/tcp open     unknown
MAC Address: 24:F5:A2:C6:13:38 (Belkin International)

Nmap scan report for Pixel-8-Pro (192.168.1.118)
Host is up (0.0086s latency).
Not shown: 999 closed ports
PORT     STATE    SERVICE
9080/tcp filtered glrpc
MAC Address: CE:16:A4:4E:D4:2F (Unknown)
```

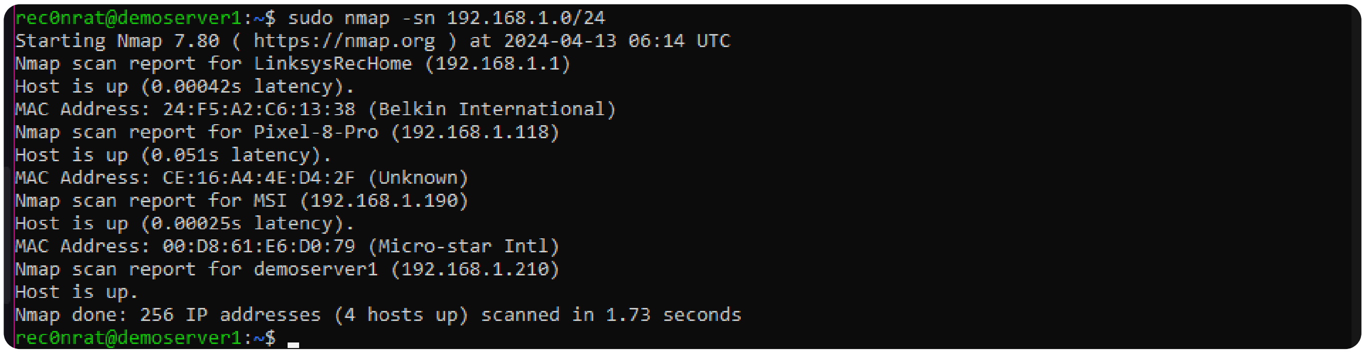


```
Nmap scan report for MSI (192.168.1.190)
Host is up (0.00043s latency).
Not shown: 997 filtered ports
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:D8:61:E6:D0:79 (Micro-star Intl)

Nmap scan report for demoserver1 (192.168.1.210)
Host is up (0.0000050s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 256 IP addresses (4 hosts up) scanned in 12.50 seconds
rec0nrat@demoserver1:~$ 
```

The ARP scan produces that same results as the SYN scan except that ARP requests were used to derive this information instead. Using ARP request may allow nmap scans to bypass certain firewall rules.

Host Discovery

Host Discovery is performed using a ping scan. there are many ping scan options including TCP, ACK, UDP, ICMP echo, Protocol and so on. Ping scan options are use the '-P' flag. The '-sn' flag specifies that port discovery be disabled and by default sends ICMP echo request, TCP SYN to port 443, TCP ACK to port 80, and an ICMP timestamp request. The nmap command 'sudo nmap -sn 192.168.1.0/24' could also be represented as 'sudo nmap -sn -PE -PS443 -PA80 -PP 192.168.1.0/24'. For more information of the different ping flags refer to https://nmap.org/book/man-host-discovery.html.



```
rec0nrat@demoserver1:~$ sudo nmap -sn 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2024-04-13 06:14 UTC
Nmap scan report for LinksysRecHome (192.168.1.1)
Host is up (0.00042s latency).
MAC Address: 24:F5:A2:C6:13:38 (Belkin International)
Nmap scan report for Pixel-8-Pro (192.168.1.118)
Host is up (0.051s latency).
MAC Address: CE:16:A4:4E:D4:2F (Unknown)
Nmap scan report for MSI (192.168.1.190)
Host is up (0.00025s latency).
MAC Address: 00:D8:61:E6:D0:79 (Micro-star Intl)
Nmap scan report for demoserver1 (192.168.1.210)
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 1.73 seconds
rec0nrat@demoserver1:~$
```

The Host Discovery scan is the exact same as the Ping scan. The description above explains in-depth the what the scan is doing and gives a reference for other options that may be introduced to this type of scan.