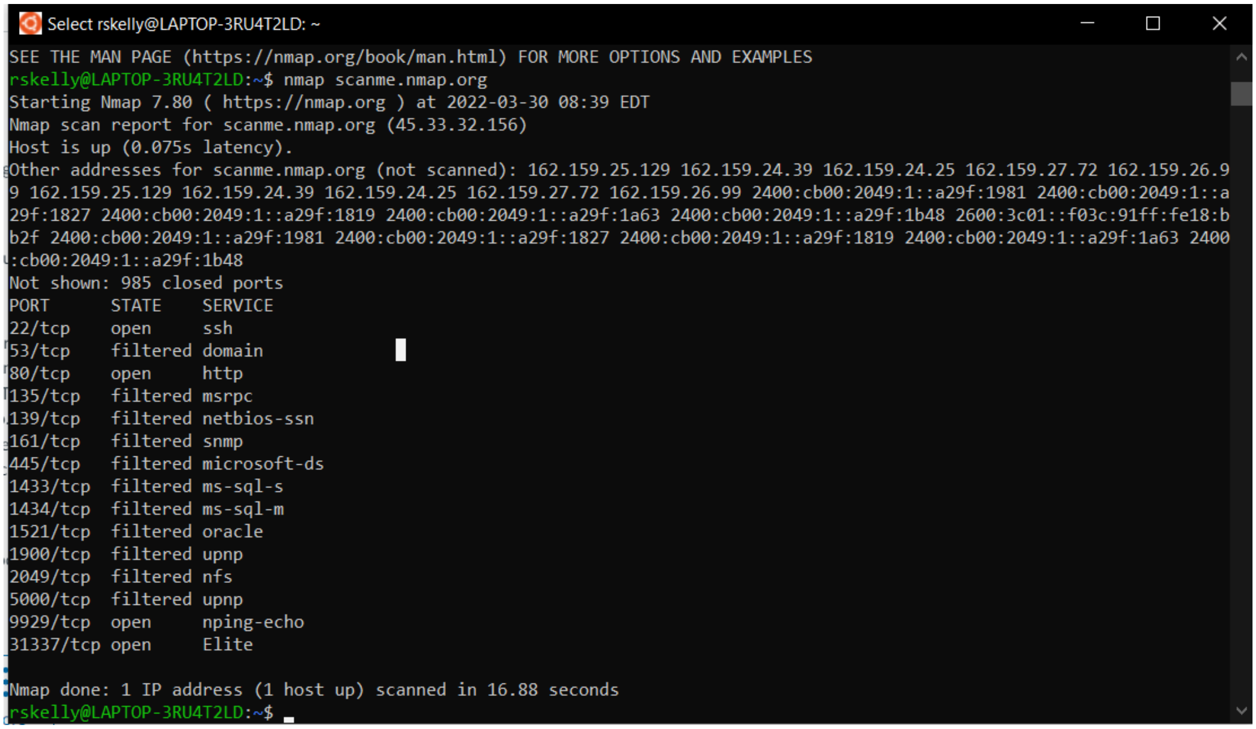
Ryan J. Skelly Lab 4 - CS527 3/30/22

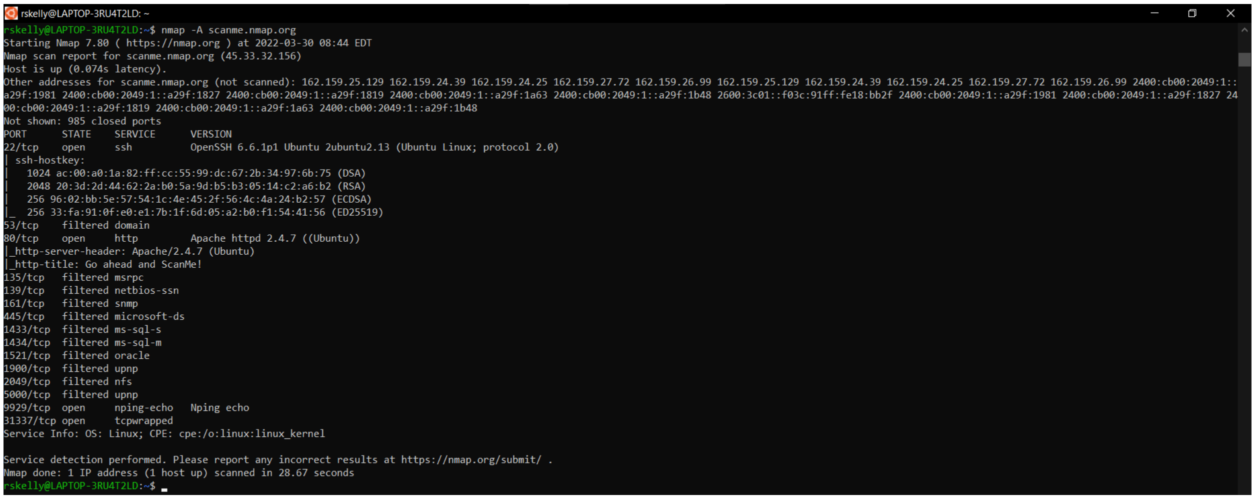
2.)



```
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
rskelly@LAPTOP-3RU4T2LD:~$ nmap scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2022-03-30 08:39 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.075s latency).
Other addresses for scanme.nmap.org (not scanned): 162.159.25.129 162.159.24.39 162.159.24.25 162.159.27.72 162.159.26.9
9 162.159.25.129 162.159.24.39 162.159.24.25 162.159.27.72 162.159.26.99 2400:cb00:2049:1::a29f:1981 2400:cb00:2049:1::a
29f:1827 2400:cb00:2049:1::a29f:1819 2400:cb00:2049:1::a29f:1a63 2400:cb00:2049:1::a29f:1b48 2600:3c01::f03c:91ff:fe18:b
b2f 2400:cb00:2049:1::a29f:1981 2400:cb00:2049:1::a29f:1827 2400:cb00:2049:1::a29f:1819 2400:cb00:2049:1::a29f:1a63 2400
:cb00:2049:1::a29f:1b48
Not shown: 985 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
53/tcp    filtered domain
80/tcp    open     http
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
161/tcp   filtered snmp
445/tcp   filtered microsoft-ds
1433/tcp  filtered ms-sql-s
1434/tcp  filtered ms-sql-m
1521/tcp  filtered oracle
1900/tcp  filtered upnp
2049/tcp  filtered nfs
5000/tcp  filtered upnp
9929/tcp  open     nping-echo
31337/tcp open     Elite

Nmap done: 1 IP address (1 host up) scanned in 16.88 seconds
rskelly@LAPTOP-3RU4T2LD:~$ _
```

The URL being used to ping is special to the nmap software, as it searches and maps all other devices/addresses in the /24 subnet(or every device locally scoped). This is done based on our own device's IPv4 and v6 addresses. It finds more than what is locally scoped but only provides information about those that are locally scoped.

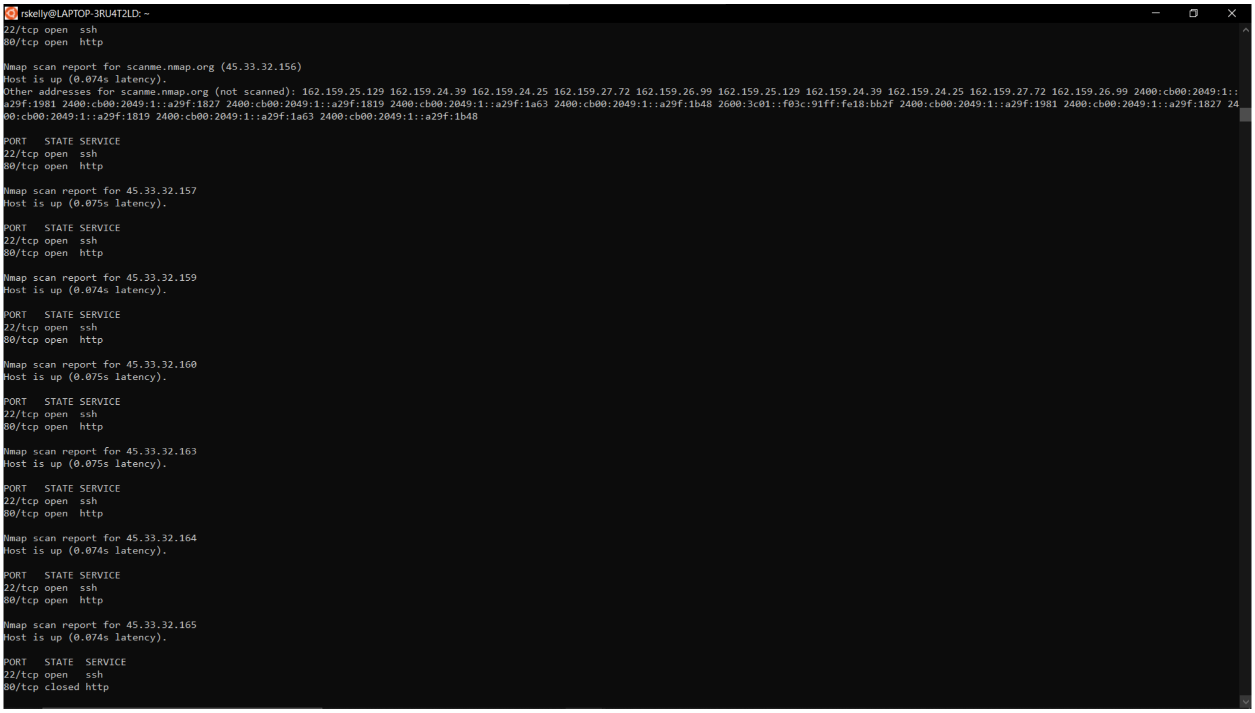
3.)



```
rskelly@LAPTOP-3RU4T2LD:~$ nmap -A scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2022-03-30 08:44 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.074s latency).
Other addresses for scanme.nmap.org (not scanned): 162.159.25.129 162.159.24.39 162.159.24.25 162.159.27.72 162.159.26.99 162.159.25.129 162.159.24.39 162.159.24.25 162.159.27.72 162.159.26.99 2400:cb00:2049:1::
a29f:1981 2400:cb00:2049:1::a29f:1827 2400:cb00:2049:1::a29f:1819 2400:cb00:2049:1::a29f:1a63 2400:cb00:2049:1::a29f:1b48 2600:3c01::f03c:91ff:fe18:bb2f 2400:cb00:2049:1::a29f:1981 2400:cb00:2049:1::a29f:1827 24
00:cb00:2049:1::a29f:1819 2400:cb00:2049:1::a29f:1a63 2400:cb00:2049:1::a29f:1b48
Not shown: 985 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)
53/tcp    filtered domain
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
161/tcp   filtered snmp
445/tcp   filtered microsoft-ds
1433/tcp  filtered ms-sql-s
1434/tcp  filtered ms-sql-m
1521/tcp  filtered oracle
1900/tcp  filtered upnp
2049/tcp  filtered nfs
5000/tcp  filtered upnp
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 28.67 seconds
rskelly@LAPTOP-3RU4T2LD:~$ _
```

The A flag enables the nmap software to provide version information based on the device on the other end of the port. The A flag also allows the nmap command to display currently displayed DNS lookups on the specified network.

4.)

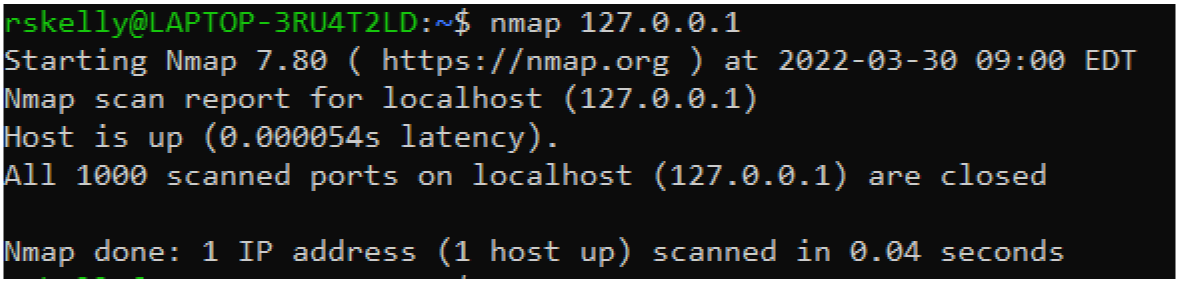


rskelly@LAPTOP-3RU4T2LD: ~

```
22/tcp open  ssh
80/tcp open  http

Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.074s latency).
Other addresses for scanme.nmap.org (not scanned): 162.159.25.129 162.159.24.39 162.159.24.25 162.159.27.72 162.159.26.99 162.159.25.129 162.159.24.39 162.159.24.25 162.159.27.72 162.159.26.99 2400:cb00:2049:1::
a29f:1981 2400:cb00:2049:1::a29f:1827 2400:cb00:2049:1::a29f:1819 2400:cb00:2049:1::a29f:1a63 2400:cb00:2049:1::a29f:1b48 2600:3c01::f03c:91ff:fe18:bb2f 2400:cb00:2049:1::a29f:1981 2400:cb00:2049:1::a29f:1827 24
00:cb00:2049:1::a29f:1819 2400:cb00:2049:1::a29f:1a63 2400:cb00:2049:1::a29f:1b48

PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap scan report for 45.33.32.157
Host is up (0.075s latency).

PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap scan report for 45.33.32.159
Host is up (0.074s latency).

PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap scan report for 45.33.32.160
Host is up (0.075s latency).

PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap scan report for 45.33.32.163
Host is up (0.075s latency).

PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap scan report for 45.33.32.164
Host is up (0.074s latency).

PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap scan report for 45.33.32.165
Host is up (0.074s latency).

PORT   STATE  SERVICE
22/tcp open   ssh
80/tcp closed http
```

The P flag allows you to specify which ports you'd like to probe on, this is much more concise than the All ports as in the previous commands. It also gives all hosts on the ports, which can be useful for locating other devices that could be important to protect/attack.

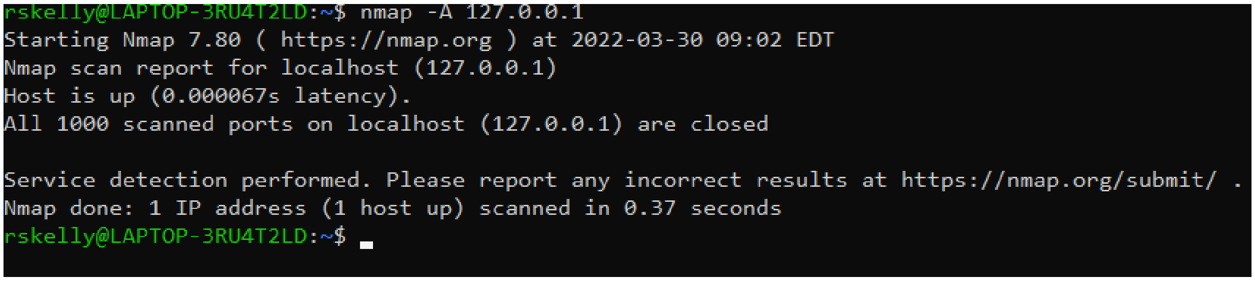
5.)



```
rskelly@LAPTOP-3RU4T2LD:~$ nmap 127.0.0.1
Starting Nmap 7.80 ( https://nmap.org ) at 2022-03-30 09:00 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000054s latency).
All 1000 scanned ports on localhost (127.0.0.1) are closed

Nmap done: 1 IP address (1 host up) scanned in 0.04 seconds
```

For this command, the IPv4 loopback addr for the device was provided to probe. This resulted in my devices ports being scanned and only my device, because there wasnt anywhere to traverse to, no other information was provided.

6.)



```
rskelly@LAPTOP-3RU4T2LD:~$ nmap -A 127.0.0.1
Starting Nmap 7.80 ( https://nmap.org ) at 2022-03-30 09:02 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000067s latency).
All 1000 scanned ports on localhost (127.0.0.1) are closed

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.37 seconds
rskelly@LAPTOP-3RU4T2LD:~$ 
```

This command did the same thing as question 2, however since its probing packet didn't go anywhere, there wasn't any returned information.