Section 1 What Did You Do? :

The first activity centers around analyzing your personal network using NMAP. NMAP is an open source(free for public use and manipulation) network scanning tool that is used to get a picture of a network. This includes discovering hosts, services, detecting operating systems, identifying open ports, and collecting network device information. It does so by initially checking a network for hosts and services, and then sending information to what was found and seeing which hosts or services respond. NMAP then interprets the response and uses it to create the network map. This map includes information about what is occupying each port, including what is using the port. It also includes firewall and other security information. I have ran similar scans in the past but not specifically NMAP. This is an extremely useful tool for any individual or household and a must for any business or organization as it identifies potential threats and vulnerabilities. Like any useful network protection tool there is also the potential for the tool to be used for malicious purposes, that can lead to potentially severe legal consequences. NMAP does not do anything to protect any potential vulnerabilities found, but it is a tremendous jumping off point to start to understand the layout of a network and any weaknesses associated with it.

In order to execute the NMAP induced network mapping, the first step of the process was to download NMAP onto my Windows device. I went to Google and entered NMAP to find the product website as well as do a little initial research to further understand exactly how NMAP would map the network. After doing my initial research I proceeded to the product site (nmap.org) and found the download tab. I scrolled down to find the Windows version and downloaded NMAP version 7.94. Once NMAP's setup file was downloaded I opened the installation file and installed NMAP with all base recommended settings. After installation was complete I opened the program labeled Zenmap and found that, as opposed to my assumption, that initiating network mapping execution was not self explanatory. NMAP's website (nmap.org) has an extremely helpful 18 chapter guide, that ranges from basic instructions on functionality to details on how NMAP functions. I read some of the provided documentation on NMAP.org and was able to find a guide that provided some guide rails on executing Zenmap. The first step of executing Zenmap, after opening the program, was to set the target to 'scanme.nmap.org'. I noticed that as I was entering 'scanme.nmap.org' into the target field it was also filling in automatically to the command field. After that I had to confirm the profile which was already set to 'Intense Scan' which was the recommended profile from the instructions, and I wanted to get the most detailed scan possible. I did notice that the profile did not flow into command like target did. Once target and profile were all set I was able to hit scan and start the execution process. Zenmap took no more than 90 seconds to complete and my results were available. I took screenshots of the results. Additionally while finding instructions on how to use the Zenmap interface I also stumbled upon some instructions that shared how to execute NMAP directly in the windows command terminal. That made me curious to see if doing it via the terminal would produce any different results. I assumed it would produce the same results, especially considering Zenmap seems to run the same command. Nevertheless I did it anyway. In order to execute the mapping this way, the first step was to open the command prompt. Then I had to ensure that NMAP was housed underneath the current directory in the prompt. Finally I ran the following code, ' -T4 -A -v scanme.map.org', which was the same command run by Zenmap.

The results were available in under 2 minutes and I took screenshots of the results. It turned out upon inspection that both methods of mapping produced the same results. Since the Zenmap generated results were a tad more user friendly I decided to use those for the analysis portion. In order to conduct the analysis I examined each tab separately. The tab that I conducted the most analysis on was Ports/Hosts tab. While I understood a majority of the information provided on the Ports/Hosts tab there were some port numbers and service names that I had to use some of the documentation on nmap.org and do some other research to better understand the results.

Section 2 What were the results? :

Note See Appendix for Screenshots of Zenmap and Command Prompt Results

The NMAP network scanned a total of 1000 TCP ports and found that out of the 1000 ports scanned, 992 of them were closed, 4 were filtered and 4 were open. Closed ports indicate that the port is 'not listening' currently (meaning the port is not looking for connections) however these ports could potentially open in the future if services are activated. Filtered ports indicate that those ports are being blocked from some sort of protection service, most likely a firewall, and it is not giving NMAP a reading. Finally open ports indicate that the port is actively looking for connections. Looking closer at the ports that are filtered. The first filtered port was number 25 and the service was smtp. SMTP stands for Simple Mail Transfer Protocol and is used to send email. The second filtered port was number 135 and the service is msrpc. MSRPC stands for Microsoft Remote Procedure Call which allows different machines to communicate. A good example of a standard use of this would be a connection with a printer. The third filtered port was port number 139 and the protocol was netbios-ssn. Netbios is similar to RPC in that it is another protocol used for communication between different machines on a Local Area Network(LAN). The final filtered port was port number 445 and the protocol was Microsoft-ds, which can be used on windows networks to share resources and even remotely execute commands. Now to look at the open ports. The first open port was port number 22 and the protocol was ssh. SSH stands for Secure Shell and it is used to create a secure connection with a server even on insecure networks. The reason for this is because Secure Shell creates an encryption between the two parties. It is set to open by default, so it is expected (if default settings are still in place) that port 22 would be open for SSH use. The second open port was port number 80 and the protocol was HTTP. This port is used to connect to web sites or any sort of web browsing. Similar to 22 this port is generally open by default. The third open port was number 9929 and the protocol was nping echo. This port from my research and analysis seems to be used by nmap to map the network, and is expected to be open during this mapping exercise. The final open port was 31337 and the protocol was tcpwrapped. From my research this indicates that the port has a real service available but the current host is not on the list of approved hosts for sed port. Since the network scanned was my personal home network it has a relatively small attack surface compared to an organization, however there are still plenty of places for attackers to find ways in. The biggest of which generally involve port 80, which is the port that is generally used to communicate with the internet. The other ports can be hacked yes, however they are not as open to human error as port 80 can be. There is potential to be attacked via a website you visit using port 80. Devices that connect to the internet through your network also create a much larger attack surface, including the router and any sort of mobile,

streaming, gaming, home or internet connecting devices. Every single one of these devices that connect to the network bring their own list of potential vulnerabilities and avenues for attack. Not only do the devices themselves open the network up for attack but also any applications or features used by the devices open the network up for attack. For example, if you look at a mobile device that is connected to a network. Not only is there potential for hackers to use your mobile device directly to gain access to your network they can also get to your network by hacking an app that you may have on your phone and use. This applies across the board on all devices that connect to the network. Something as seemingly harmless as a Roku can be used to attack. Additionally some of these devices feature bluetooth capability that can relatively easily be hacked by attackers if they are within a close vicinity of the device. Some of these devices or apps may also use the cloud to store data for backups or non-local access. Cloud saving is another opportunity for hackers to potentially reach the network. These devices, their apps, and features all increase the network attack surface nearly tenfold even for a personal network, this would be exponentially greater for an organization. It is important to view all devices that may connect to a port as a link in a chain, while they may not show directly on the network map they are connected to the network and therefore could be used against it.
The last part of the results is the topography. My network has 19 levels all seemingly related to my internet provider comcast.

Section 3 What did you learn? :

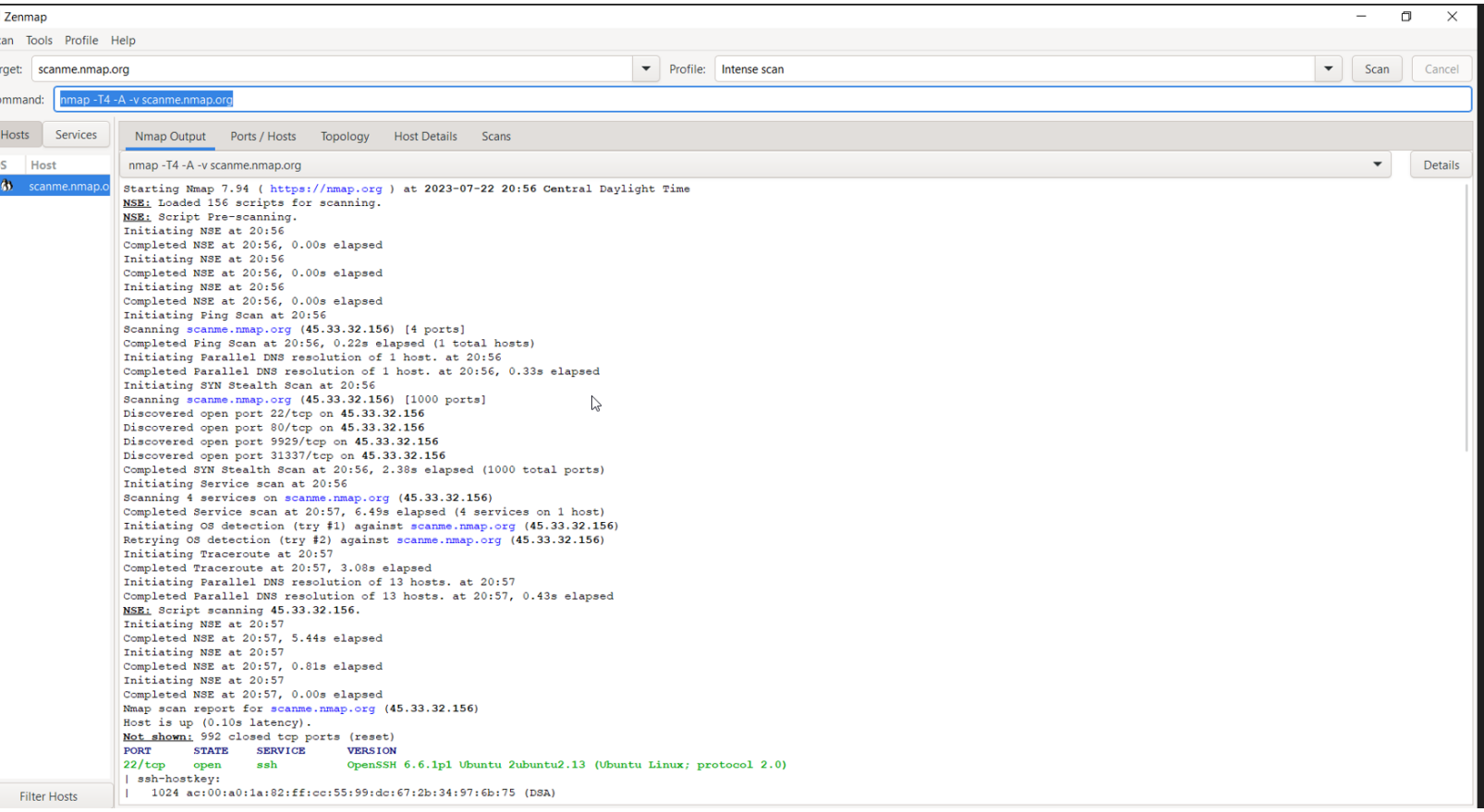
This whole experiment reinforced a lot of what I believe already. It was really nice to be able to run a scan like this again, as I had just moved to a new house with a new already existing network and I had not had a chance to look at the network details yet. One of my biggest takeaways from running a scan this time around is that even a personal network can easily have hundreds of potential vulnerabilities that extend far beyond the ports and protocols themselves. You always have to be mindful of what devices are connected to the network and what features and applications they may have. While I may have a relatively small attack surface, especially when compared to some organizations, I think it is fairly clear that the attack surface will only grow as everything in our lives becomes internet integrated. When I think of my company's attack surface, a retailer with both stores and digital businesses, it is no wonder that there is a large security team. I would be very interested in seeing the results of a NMAP execution on my company's networking, especially the topography. Since there are multiple stores, corporate departments, systems and you have to worry about employee's personal devices too I am really curious to see what shape the network would take. I am assuming that there would be multiple levels broken up by store or by business function. Additionally you have to train thousands of employees on proper security practices and develop your security to protect against their negligence and any potential intentional malfeasance conducted by employees. Having so many employees equally increases physical security risks. In terms of my personal network, the mapping further supports the importance of physical security. Gaining physical access is one of the easiest ways for hackers to attack, so it is always important to keep all devices that connect to the network, including the router itself, secured both physically and with passwords or passcodes. It is invaluable to have secure logins for devices, including

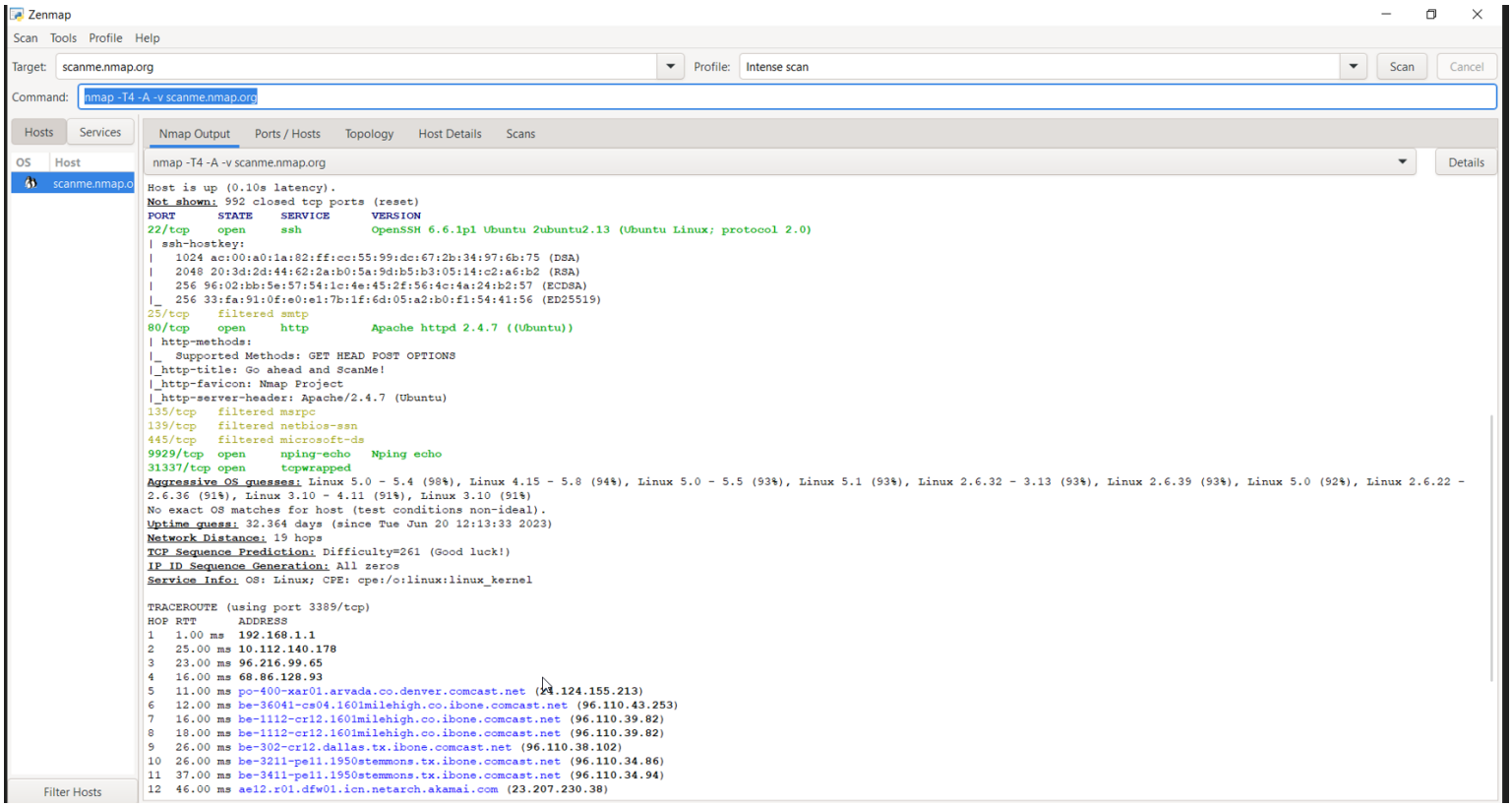
those devices with bluetooth capabilities(and to even turn off bluetooth capabilities when not actively using it).

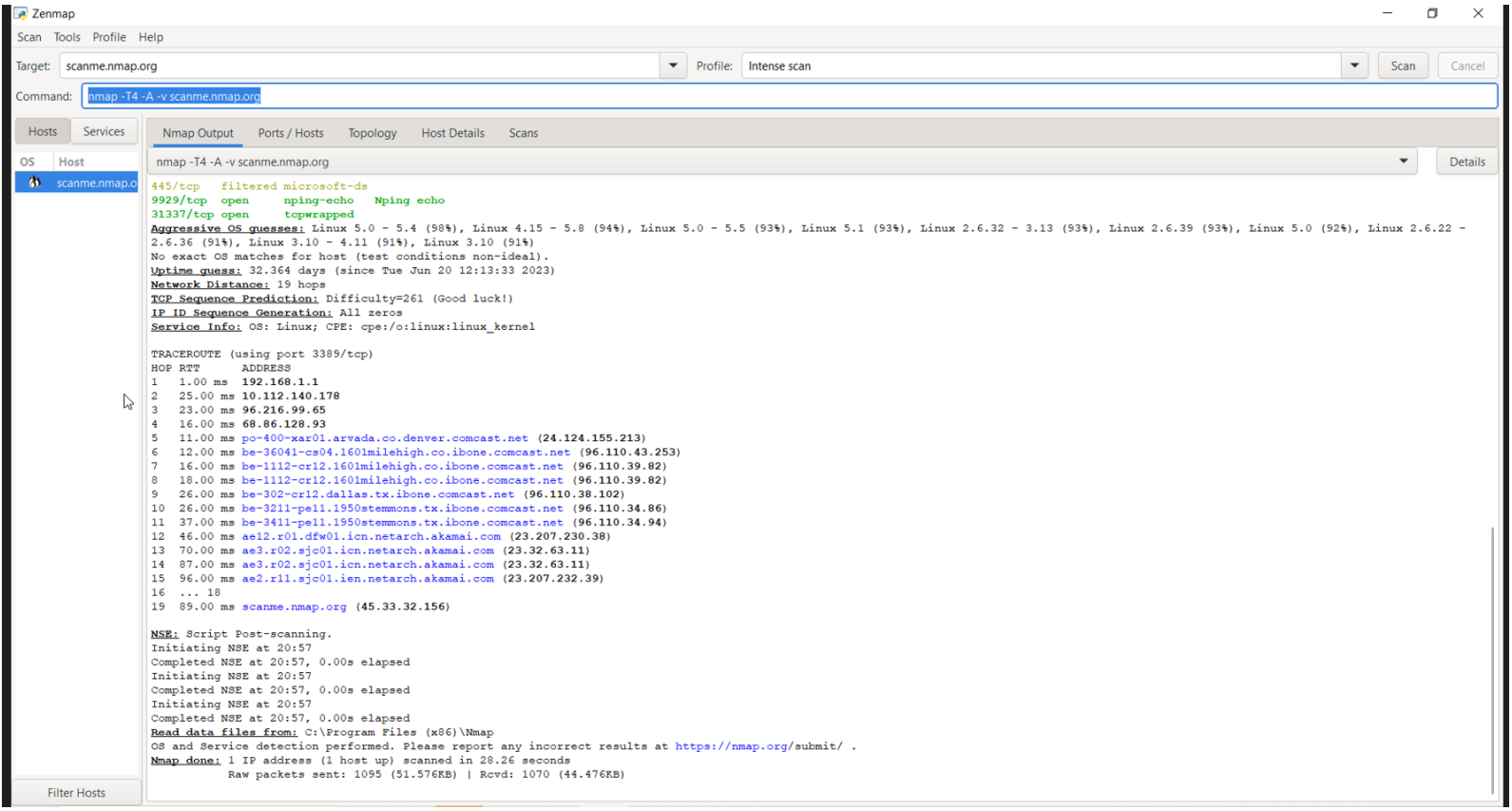
Outside of physical access one of the biggest vulnerabilities of my network are the 992 closed ports. While these ports are not listening for any data or connections they are still not necessarily secured. These ports can be turned on at any time, by their associated service and protocol. It would be wise for me to keep periodically monitoring these ports(and all ports for that matter) to determine if any action is needed on these ports. Ideally these ports would be filtered with some sort of firewall however since my landlord is the name on the account with the internet service provider I am not sure the legality of filtering those ports since I am not the account holder. So I believe the most diligent thing I can do is to periodically check and react to any changes. All of the open ports appear to be standard / default settings so again the approach here will be vigilant monitoring, especially for network connected items using port 80 to connect to the web. It would be foolish to not periodically check port status even if all ports were showing as filtered, as network security is an ongoing process and just because something was previously secured does not mean that it will stay that way going forward. I think that is the biggest and most important tactic I can take, to be diligent about monitoring my personal network. This includes monitoring web traffic (via port 80) and any devices on the network, creating strong passwords for any device that will allow it, keeping all systems and devices up to date and monitoring the news cycle for any big hacks. It will also be important to use other network security software in congruence with network mapping, as just identifying issues does not actually fix any vulnerabilities or breaches.

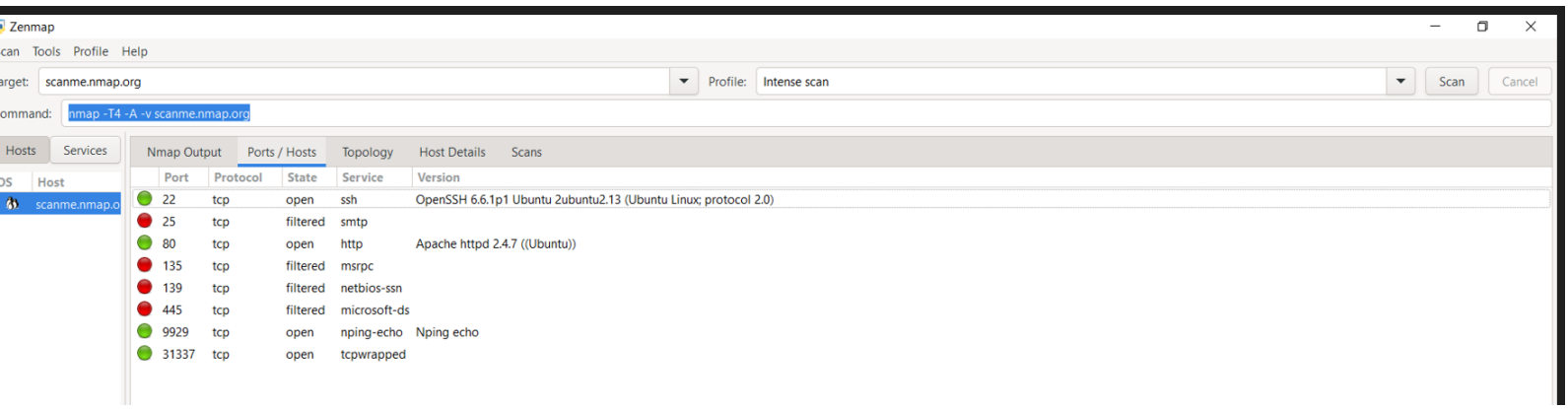
Overall this assignment was a good reminder that a network's attack surface is much deeper than the screenshot a scan can provide. It was also a good reinforcement of something I truly believe regarding network security(and life in general for that matter) and that is that you are only as secure or as strong as your weakest link. Meaning you can have the most state of the art security system but if you are allowing an insecure application or website to use your network to connect to the web, you are opening yourself up to those same vulnerabilities. Which is exactly why you must stay vigilant either as an individual or an organization. I would be extremely interested in seeing what a large organization's map would look like, compared to my relatively small network. However for both organizations and individuals attack surfaces will continue to grow as more and more products incorporate network capabilities, and it will be paramount to continue to stay vigilant and in the know with new hacking trends and potential vulnerabilities.

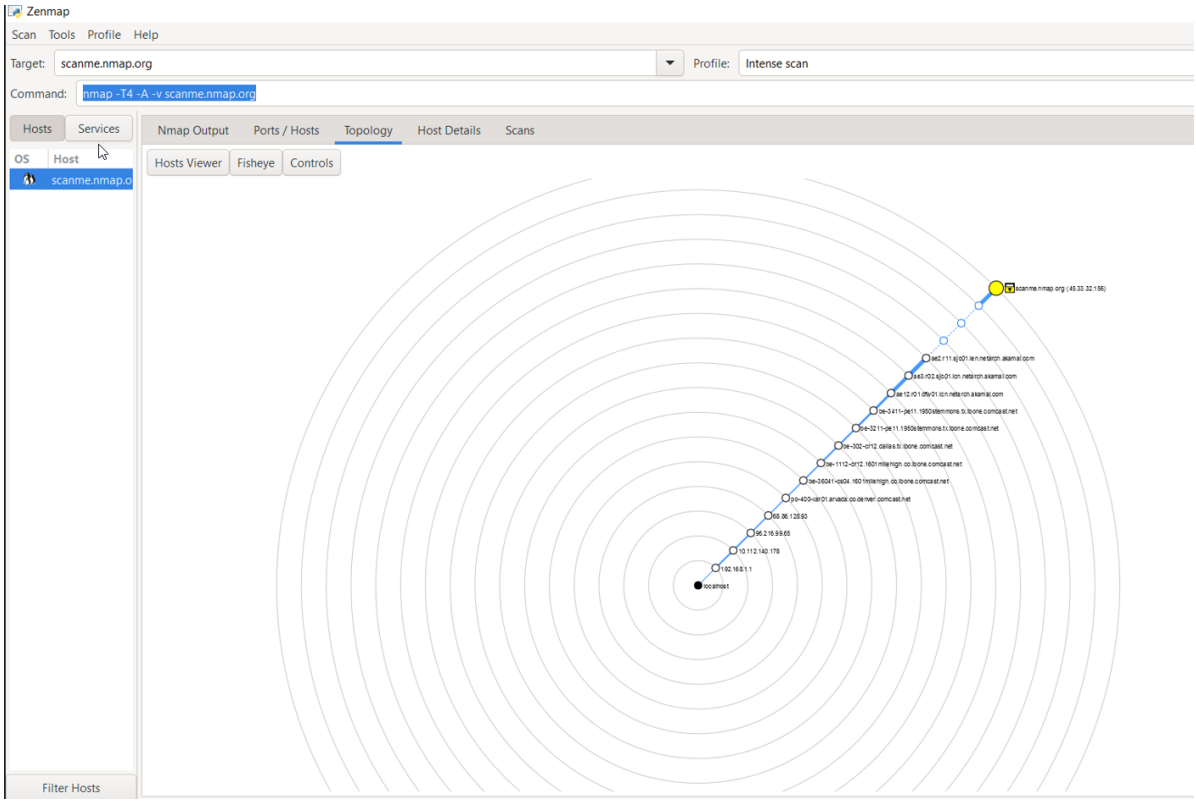
Appendix:

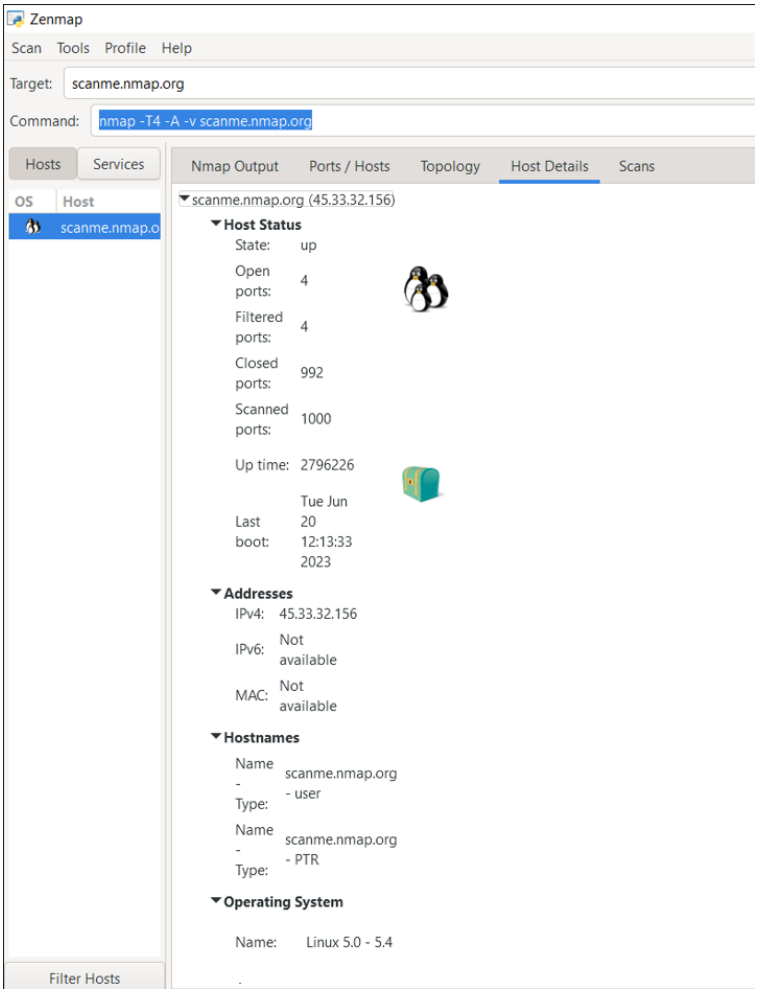

Zenmap
Tools Profile Help
scanme.nmap.org
Profile: Intense scan
Scan
Cancel
nmap -T4 -A -v scanme.nmap.org
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
Host
scanme.nmap.o
nmap -T4 -A -v scanme.nmap.org
Details
Starting Nmap 7.94 (https://nmap.org) at 2023-07-22 20:56 Central Daylight Time
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 20:56
Completed NSE at 20:56, 0.00s elapsed
Initiating NSE at 20:56
Completed NSE at 20:56, 0.00s elapsed
Initiating NSE at 20:56
Completed NSE at 20:56, 0.00s elapsed
Initiating Ping Scan at 20:56
Scanning scanme.nmap.org (45.33.32.156) [4 ports]
Completed Ping Scan at 20:56, 0.22s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 20:56
Completed Parallel DNS resolution of 1 host. at 20:56, 0.33s elapsed
Initiating SYN Stealth Scan at 20:56
Scanning scanme.nmap.org (45.33.32.156) [1000 ports]
Discovered open port 22/tcp on 45.33.32.156
Discovered open port 80/tcp on 45.33.32.156
Discovered open port 9929/tcp on 45.33.32.156
Discovered open port 31337/tcp on 45.33.32.156
Completed SYN Stealth Scan at 20:56, 2.38s elapsed (1000 total ports)
Initiating Service scan at 20:56
Scanning 4 services on scanme.nmap.org (45.33.32.156)
Completed Service scan at 20:57, 6.49s elapsed (4 services on 1 host)
Initiating OS detection (try #1) against scanme.nmap.org (45.33.32.156)
Retrying OS detection (try #2) against scanme.nmap.org (45.33.32.156)
Initiating Traceroute at 20:57
Completed Traceroute at 20:57, 3.08s elapsed
Initiating Parallel DNS resolution of 13 hosts. at 20:57
Completed Parallel DNS resolution of 13 hosts. at 20:57, 0.43s elapsed
NSE: Script scanning 45.33.32.156.
Initiating NSE at 20:57
Completed NSE at 20:57, 5.44s elapsed
Initiating NSE at 20:57
Completed NSE at 20:57, 0.81s elapsed
Initiating NSE at 20:57
Completed NSE at 20:57, 0.00s elapsed
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.10s latency).
Not shown: 992 closed tcp ports (reset)
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)
Filter Hosts

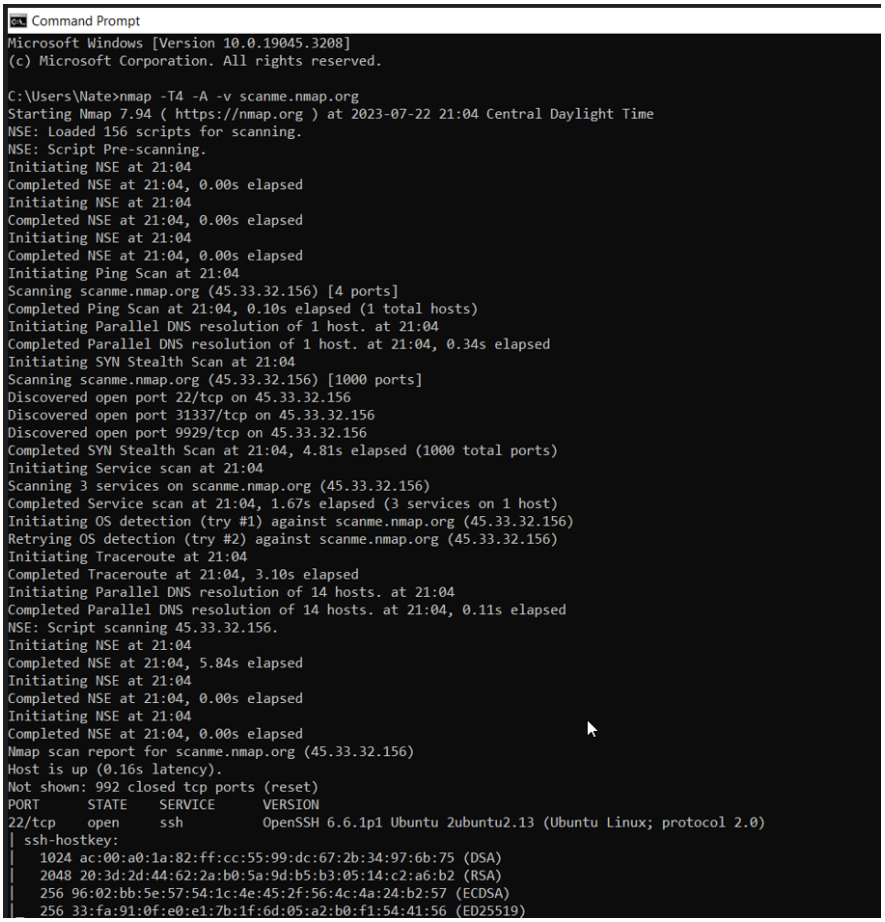

Zenmap
Scan Tools Profile Help
Target: scanme.nmap.org
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v scanme.nmap.org
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
OS Host
scanme.nmap.o
nmap -T4 -A -v scanme.nmap.org
Details
Host is up (0.10s latency).
Not shown: 992 closed tcp ports (reset)
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-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-title: Go ahead and ScanMe!
|_http-favicon: Nmap Project
|_http-server-header: Apache/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
Aggressive OS guesses: Linux 5.0 - 5.4 (98%), Linux 4.15 - 5.8 (94%), Linux 5.0 - 5.5 (93%), Linux 5.1 (93%), Linux 2.6.32 - 3.13 (93%), Linux 2.6.39 (93%), Linux 5.0 (92%), Linux 2.6.22 - 2.6.36 (91%), Linux 3.10 - 4.11 (91%), Linux 3.10 (91%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 32.364 days (since Tue Jun 20 12:13:33 2023)
Network Distance: 19 hops
TCP Sequence Prediction: Difficulty=261 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
TRACEROUTE (using port 3389/tcp)
HOP RTT ADDRESS
1 1.00 ms 192.168.1.1
2 25.00 ms 10.112.140.178
3 23.00 ms 96.216.99.65
4 16.00 ms 68.86.128.93
5 11.00 ms po-400-xar01.arvada.co.denver.comcast.net (24.124.155.213)
6 12.00 ms be-36041-cs04.1601milehigh.co.ibone.comcast.net (96.110.43.253)
7 16.00 ms be-1112-cr12.1601milehigh.co.ibone.comcast.net (96.110.39.82)
8 18.00 ms be-1112-cr12.1601milehigh.co.ibone.comcast.net (96.110.39.82)
9 26.00 ms be-302-cr12.dallas.tx.ibone.comcast.net (96.110.38.102)
10 26.00 ms be-3211-pe11.1950stemmons.tx.ibone.comcast.net (96.110.34.86)
11 37.00 ms be-3411-pe11.1950stemmons.tx.ibone.comcast.net (96.110.34.94)
12 46.00 ms ae12.r01.dfw01.icn.netarch.akamai.com (23.207.230.38)
Filter Hosts

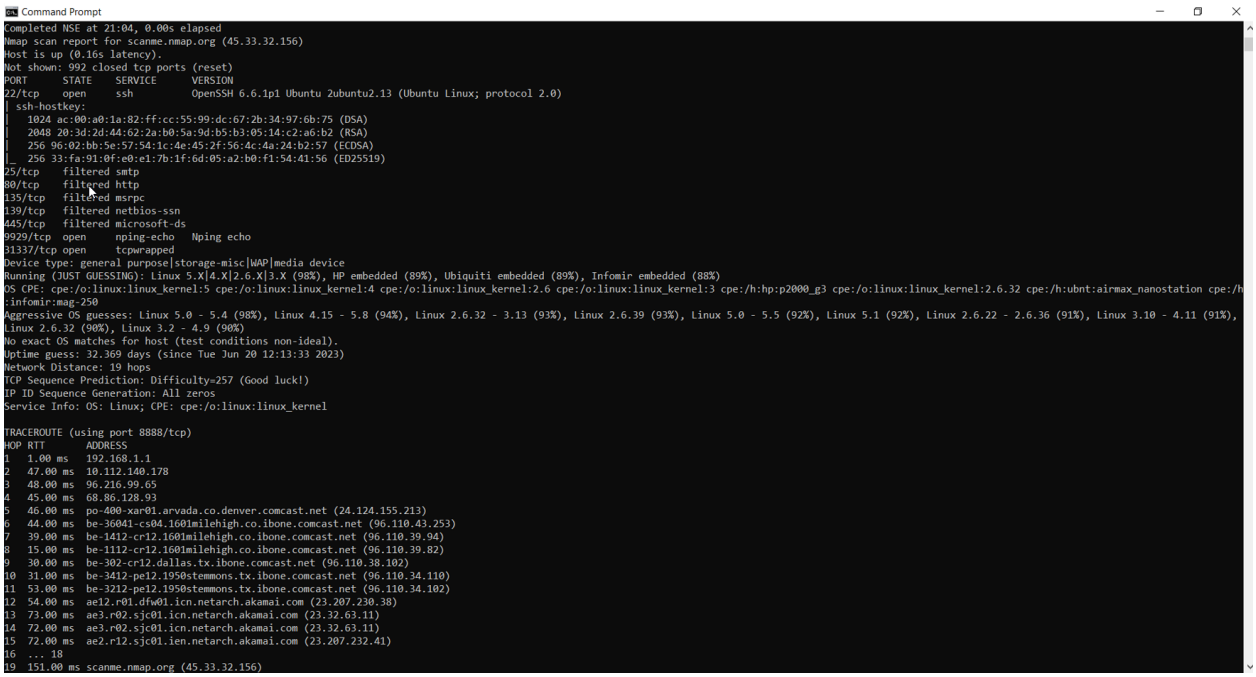

Zenmap
Scan Tools Profile Help
Target: scanme.nmap.org
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v scanme.nmap.org
Hosts
Services
OS
Host
scanme.nmap.o
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -T4 -A -v scanme.nmap.org
Details
445/tcp filtered microsoft-ds
9929/tcp open nping-echo Nping echo
31337/tcp open tcpwrapped
Aggressive OS guesses: Linux 5.0 - 5.4 (98%), Linux 4.15 - 5.8 (94%), Linux 5.0 - 5.5 (93%), Linux 5.1 (93%), Linux 2.6.32 - 3.13 (93%), Linux 2.6.39 (93%), Linux 5.0 (92%), Linux 2.6.22 - 2.6.36 (91%), Linux 3.10 - 4.11 (91%), Linux 3.10 (91%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 32.364 days (since Tue Jun 20 12:13:33 2023)
Network Distance: 19 hops
TCP Sequence Prediction: Difficulty=261 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
TRACEROUTE (using port 3389/tcp)
HOP RTT ADDRESS
1 1.00 ms 192.168.1.1
2 25.00 ms 10.112.140.178
3 23.00 ms 96.216.99.65
4 16.00 ms 68.86.128.93
5 11.00 ms po-400-xar01.arvada.co.denver.comcast.net (24.124.155.213)
6 12.00 ms be-36041-cs04.1601milehigh.co.ibone.comcast.net (96.110.43.253)
7 16.00 ms be-1112-cr12.1601milehigh.co.ibone.comcast.net (96.110.39.82)
8 18.00 ms be-1112-cr12.1601milehigh.co.ibone.comcast.net (96.110.39.82)
9 26.00 ms be-302-cr12.dallas.tx.ibone.comcast.net (96.110.38.102)
10 26.00 ms be-3211-pe11.1950stemmons.tx.ibone.comcast.net (96.110.34.86)
11 37.00 ms be-3411-pe11.1950stemmons.tx.ibone.comcast.net (96.110.34.94)
12 46.00 ms ae12.r01.dfw01.icn.netarch.akamai.com (23.207.230.38)
13 70.00 ms ae3.r02.sjc01.icn.netarch.akamai.com (23.32.63.11)
14 87.00 ms ae3.r02.sjc01.icn.netarch.akamai.com (23.32.63.11)
15 96.00 ms ae2.r11.sjc01.ien.netarch.akamai.com (23.207.232.39)
16 ... 18
19 89.00 ms scanme.nmap.org (45.33.32.156)
NSE: Script Post-scanning.
Initiating NSE at 20:57
Completed NSE at 20:57, 0.00s elapsed
Initiating NSE at 20:57
Completed NSE at 20:57, 0.00s elapsed
Initiating NSE at 20:57
Completed NSE at 20:57, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
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 28.26 seconds
Raw packets sent: 1095 (51.576KB) | Rcvd: 1070 (44.476KB)
Filter Hosts

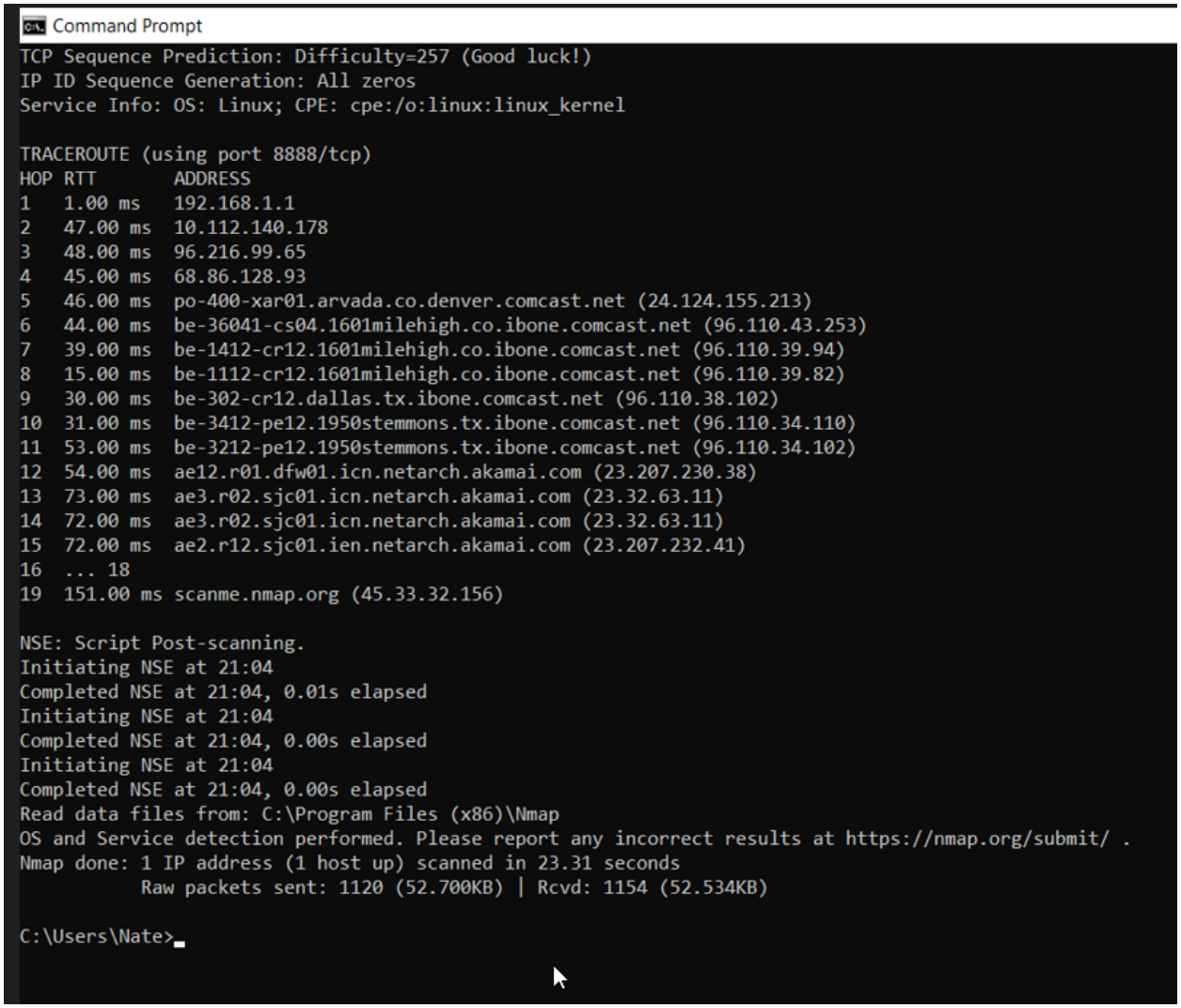

Zenmap
can Tools Profile Help
arget: scanme.nmap.org
Profile: Intense scan
Scan
Cancel
ommand: nmap -T4 -A -v scanme.nmap.org
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
Port Protocol State Service Version
22 tcp open ssh OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 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


Zenmap
Scan Tools Profile Help
Target: scanme.nmap.org
Profile: Intense scan
Command: nmap -T4 -A -v scanme.nmap.org
Hosts Services
OS Host
scanme.nmap.o
Nmap Output Ports / Hosts Topology Host Details Scans
Hosts Viewer Fisheye Controls
scanme.nmap.org (45.33.32.156)
192.168.1.1
10.112.140.178
96.2.16.9.65
68.86.128.93
localhost
Filter Hosts


Zenmap
Scan Tools Profile Help
Target: scanme.nmap.org
Command: nmap -T4 -A -v scanme.nmap.org
Hosts Services
OS Host
scanme.nmap.o
Nmap Output Ports / Hosts Topology Host Details Scans
scanme.nmap.org (45.33.32.156)
Host Status
State: up
Open ports: 4
Filtered ports: 4
Closed ports: 992
Scanned ports: 1000
Up time: 2796226
Last boot: Tue Jun 20 12:13:33 2023
Addresses
IPv4: 45.33.32.156
IPv6: Not available
MAC: Not available
Hostnames
Name - Type: scanme.nmap.org - user
Name - Type: scanme.nmap.org - PTR
Operating System
Name: Linux 5.0 - 5.4
Filter Hosts


Command Prompt
Microsoft Windows [Version 10.0.19045.3208]
(c) Microsoft Corporation. All rights reserved.
C:\Users\Nate>nmap -T4 -A -v scanme.nmap.org
Starting Nmap 7.94 (https://nmap.org) at 2023-07-22 21:04 Central Daylight Time
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 21:04
Completed NSE at 21:04, 0.00s elapsed
Initiating NSE at 21:04
Completed NSE at 21:04, 0.00s elapsed
Initiating NSE at 21:04
Completed NSE at 21:04, 0.00s elapsed
Initiating Ping Scan at 21:04
Scanning scanme.nmap.org (45.33.32.156) [4 ports]
Completed Ping Scan at 21:04, 0.10s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 21:04
Completed Parallel DNS resolution of 1 host. at 21:04, 0.34s elapsed
Initiating SYN Stealth Scan at 21:04
Scanning scanme.nmap.org (45.33.32.156) [1000 ports]
Discovered open port 22/tcp on 45.33.32.156
Discovered open port 31337/tcp on 45.33.32.156
Discovered open port 9929/tcp on 45.33.32.156
Completed SYN Stealth Scan at 21:04, 4.81s elapsed (1000 total ports)
Initiating Service scan at 21:04
Scanning 3 services on scanme.nmap.org (45.33.32.156)
Completed Service scan at 21:04, 1.67s elapsed (3 services on 1 host)
Initiating OS detection (try #1) against scanme.nmap.org (45.33.32.156)
Retrying OS detection (try #2) against scanme.nmap.org (45.33.32.156)
Initiating Traceroute at 21:04
Completed Traceroute at 21:04, 3.10s elapsed
Initiating Parallel DNS resolution of 14 hosts. at 21:04
Completed Parallel DNS resolution of 14 hosts. at 21:04, 0.11s elapsed
NSE: Script scanning 45.33.32.156.
Initiating NSE at 21:04
Completed NSE at 21:04, 5.84s elapsed
Initiating NSE at 21:04
Completed NSE at 21:04, 0.00s elapsed
Initiating NSE at 21:04
Completed NSE at 21:04, 0.00s elapsed
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.16s latency).
Not shown: 992 closed tcp ports (reset)
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)


Command Prompt
Completed NSE at 21:04, 0.00s elapsed
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.16s latency).
Not shown: 992 closed tcp ports (reset)
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 filtered http
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
Device type: general purpose|storage-misc|WAP|media device
Running (JUST GUESSING): Linux 5.X|4.X|2.6.X|3.X (98%), HP embedded (89%), Ubiquiti embedded (89%), Infomir embedded (88%)
OS CPE: cpe:/o:linux:linux_kernel:5 cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3 cpe:/h:hp:p2000_g3 cpe:/o:linux:linux_kernel:2.6.32 cpe:/h:ubnt:airmax_nanostation cpe:/h
:infomir:mag-250
Aggressive OS guesses: Linux 5.0 - 5.4 (98%), Linux 4.15 - 5.8 (94%), Linux 2.6.32 - 3.13 (93%), Linux 2.6.39 (93%), Linux 5.0 - 5.5 (92%), Linux 5.1 (92%), Linux 2.6.22 - 2.6.36 (91%), Linux 3.10 - 4.11 (91%),
Linux 2.6.32 (90%), Linux 3.2 - 4.9 (90%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 32.369 days (since Tue Jun 20 12:13:33 2023)
Network Distance: 19 hops
TCP Sequence Prediction: Difficulty=257 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
TRACEROUTE (using port 8888/tcp)
HOP RTT ADDRESS
1 1.00 ms 192.168.1.1
2 47.00 ms 10.112.140.178
3 48.00 ms 96.216.99.65
4 45.00 ms 68.86.128.93
5 46.00 ms po-400-xar01.arvada.co.denver.comcast.net (24.124.155.213)
6 44.00 ms be-36041-cs04.1601milehigh.co.ibone.comcast.net (96.110.43.253)
7 39.00 ms be-1412-cr12.1601milehigh.co.ibone.comcast.net (96.110.39.94)
8 15.00 ms be-1112-cr12.1601milehigh.co.ibone.comcast.net (96.110.39.82)
9 30.00 ms be-302-cr12.dallas.tx.ibone.comcast.net (96.110.38.102)
10 31.00 ms be-3412-pe12.1950stemmons.tx.ibone.comcast.net (96.110.34.110)
11 53.00 ms be-3212-pe12.1950stemmons.tx.ibone.comcast.net (96.110.34.102)
12 54.00 ms ae12.r01.dfw01.icn.netarch.akamai.com (23.207.230.38)
13 73.00 ms ae3.r02.sjc01.icn.netarch.akamai.com (23.32.63.11)
14 72.00 ms ae3.r02.sjc01.icn.netarch.akamai.com (23.32.63.11)
15 72.00 ms ae2.r12.sjc01.ien.netarch.akamai.com (23.207.232.41)
16 ... 18
19 151.00 ms scanme.nmap.org (45.33.32.156)


Command Prompt
TCP Sequence Prediction: Difficulty=257 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
TRACEROUTE (using port 8888/tcp)
HOP RTT ADDRESS
1 1.00 ms 192.168.1.1
2 47.00 ms 10.112.140.178
3 48.00 ms 96.216.99.65
4 45.00 ms 68.86.128.93
5 46.00 ms po-400-xar01.arvada.co.denver.comcast.net (24.124.155.213)
6 44.00 ms be-36041-cs04.1601milehigh.co.ibone.comcast.net (96.110.43.253)
7 39.00 ms be-1412-cr12.1601milehigh.co.ibone.comcast.net (96.110.39.94)
8 15.00 ms be-1112-cr12.1601milehigh.co.ibone.comcast.net (96.110.39.82)
9 30.00 ms be-302-cr12.dallas.tx.ibone.comcast.net (96.110.38.102)
10 31.00 ms be-3412-pe12.1950stemmons.tx.ibone.comcast.net (96.110.34.110)
11 53.00 ms be-3212-pe12.1950stemmons.tx.ibone.comcast.net (96.110.34.102)
12 54.00 ms ae12.r01.dfw01.icn.netarch.akamai.com (23.207.230.38)
13 73.00 ms ae3.r02.sjc01.icn.netarch.akamai.com (23.32.63.11)
14 72.00 ms ae3.r02.sjc01.icn.netarch.akamai.com (23.32.63.11)
15 72.00 ms ae2.r12.sjc01.ien.netarch.akamai.com (23.207.232.41)
16 ... 18
19 151.00 ms scanme.nmap.org (45.33.32.156)
NSE: Script Post-scanning.
Initiating NSE at 21:04
Completed NSE at 21:04, 0.01s elapsed
Initiating NSE at 21:04
Completed NSE at 21:04, 0.00s elapsed
Initiating NSE at 21:04
Completed NSE at 21:04, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
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 23.31 seconds
Raw packets sent: 1120 (52.700KB) | Rcvd: 1154 (52.534KB)
C:\Users\Nate>