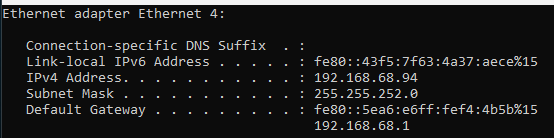
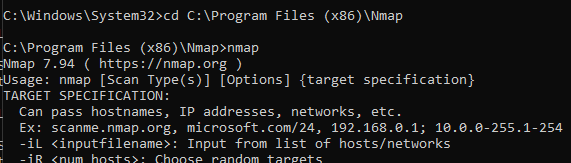
**Question 1: what did you do?**

I had no experience with NMAP prior to this assignment. The first thing I did was I went to nmap.org to download and install the application. What helped was going to YouTube.com and searching for a video on installation and scanning Windows machines with NMAP. Adrian Mikeliunas’ YouTube video was very helpful in this. For this session, I used my computer in the study room which was on an ethernet connection.

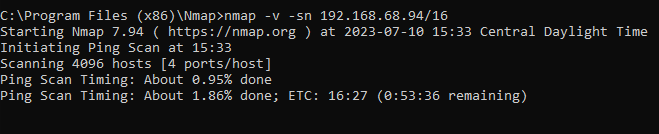
I had to first find my IP address by running IPConfig /all command for my machine to get the IPv4 address that I will use in my scan.



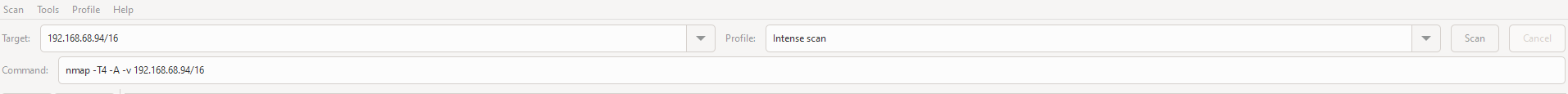
Next, I opened command prompt as administrator, navigated to the NMAP folder and evaluated a few commands to see if it worked.



I then ran the scan, and I was informed that it would take about 54 minutes.



However, I found something better! NMAP has a zenmap application that does most of the heavy lifting. I opened up zenmap (while the command prompt NMAP command was running) and added the target IP to scan with the profile set to “Intense scan.”



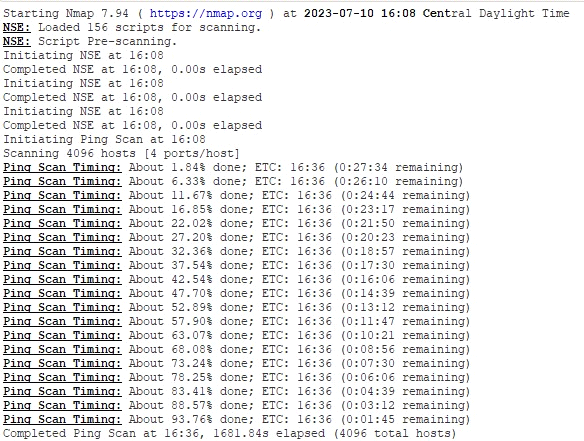
This application above is what I will be using for the results moving forward. The command prompt scans were similar but less robust results-wise.

Once the results were done I realized I needed to research what each scan meant, what they did and their importance. I will include the references/citations during the results portion.

**Question 2: What were the results?**

There were multiple scans, so this part is lengthy. I will touch each part briefly with the results of each scan. I will use the results from the zenmap scan since it nicely presented the data.

There were five ping scans that produced the same results shown below:



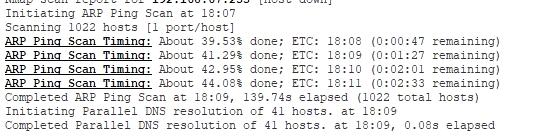
As it turns out, there were several ping scan timings that ran from 50 to 30 minutes with each session. NSE script was already loaded with Zenmap, and I made no modification to it.

The ping scan timing results all displayed the same report for each host scanned as shown by the snippet below:



My hypothesis is the reason it reported “host down” for each IP address was simply because there were no active host tied to the IP address or there is no response from the host. NMAP designates a non-responsive host as “down.”

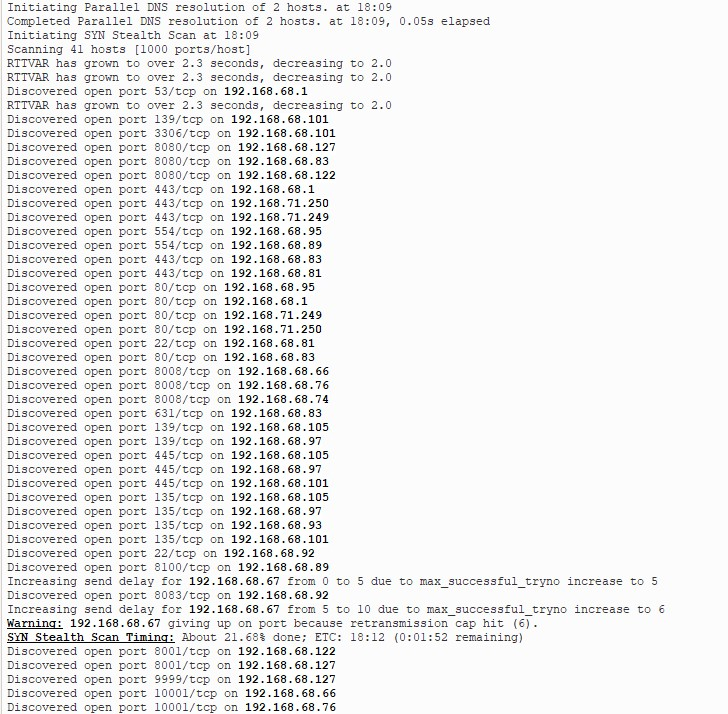
ARP Ping scan timing/Parallel DNS resolution:



An ARP ping scan is used to detect if hosts are online. While it is the most effective way of detecting hosts in LAN networks, NMAP also performs reverse-DNS resolution for every IP which responds to host discovery probes (NMAP). These scans yielded a result of 41 hosts.

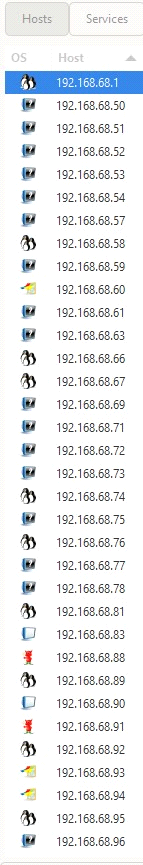
This is about the estimate I had for active devices in my home. With Internet of Things devices in my house, I believe I have over 70 but not all are turned on or were active at the time of the scan. This means I have a wider attack surface when all my devices are active. However, such things as Bluetooth and some IoT devices are not turned on 100% of the time so it lessens the exposure to threat actors. At the time of the scan, my laptop was the only computer on and activity at this time was not peak. I did locate my mobile phone IP address (192.168.68.52), so it was captured in the results. This means my Wi-Fi devices were also being captured in the scans. It tells me that any device that connects to the network, IoT or mobile phone will open the possibility of exploitation and compromise to my network.

The results above were used in the next scans which were the SYN Stealth Scan, and scans thereafter. A SYN scan determines the state of a communications port without establishing a full connection (Hanna, 2021). This is a tactic a malicious hacker can use to perform a denial-of-service (DoS) attack (Tech).



There were five SYN scans that were performed. Each host in the list showed several open ports. There were familiar ports like 443 (HTTPS) and 22 (SSH) but many I could not identify. Port 8080 is used for web servers, 139 is NetBIOS session service, 3306 is MySQL protocol, 554 is Real Time Streaming Protocol for Windows media services, 631 is Internet Printing Protocol, 135 is RPC Endpoint Mapper service, 8100 is the default port used by all detection servers to communicate with the enforce server, 9999 and 10001 are a Datagram protocols.

Zenmap was visually superior to the command prompt results. A full listing of the host IP shown in the Zenmap interface as depicted below:



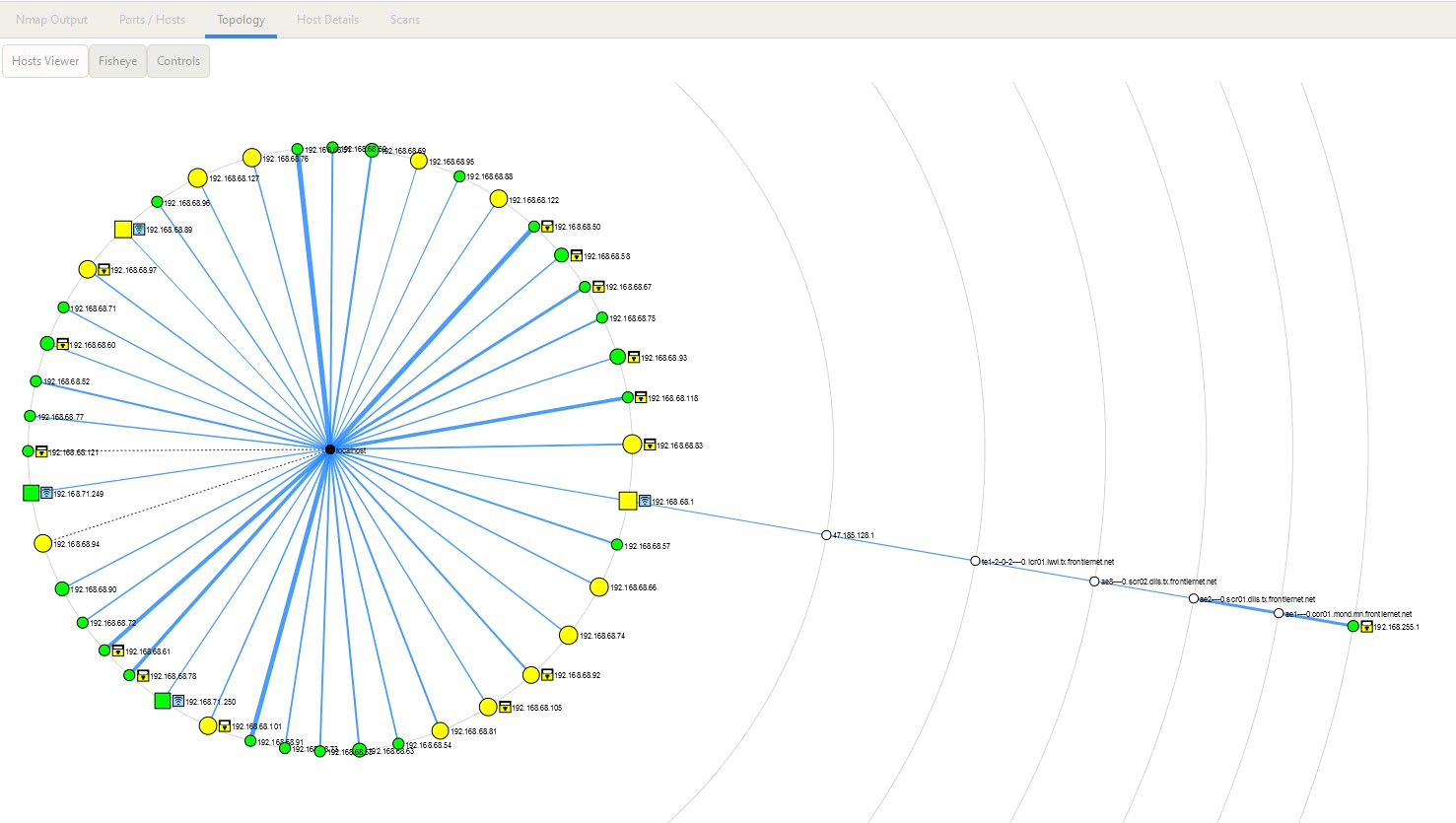
I had to do a bit of research on what each meant. The hosts come with symbols that show the OS. This hints what is a router, switch, computer, or some other device. NMAP provided a reference in their online reference book (NMAP):



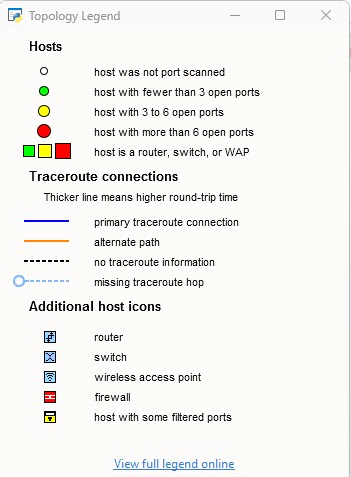
Here I had to take the IP address information and identify what device was tied to the IP address. The way I did this was take the router listing and match it with the devices. The results are follows:

|  |  |
| --- | --- |
| Device | Host IP |
| Router | 192.168.68.1 |
| Samsung Media room TV 1 | 192.168.68.50 |
| Wyze Living Room Camera | 192.168.68.51 |
| My S10 phone | 192.168.68.52 |
| Wyze Garage Camera | 192.168.68 53 |
| Wyze Front Lawn Camera | 192.168.68.54 |
| Wife's S10 phone | 192.168.68.57 |
| Roku Express | 192.168.68.58 |
| Wyze Pan Camera | 192.168.68.59 |
| Wife's laptop | 192.168.68.60 |
| Media Laptop | 192.168.68.61 |
| Kasa IoT | 192.168.68.63 |
| Google Home mini | 192.168.68.66 |
| Android phone | 192.168.68.67 |
| Kasa IoT | 192.168.68.69 |
| Roborock vacuum | 192.168.68.71 |
| Wyze Study Camera | 192.168.68.72 |
| Wyze Driveway camera | 192.168.68.73 |
| Google Home mini | 192.168.68.74 |
| Wife S23 phone | 192.168.68.75 |
| Google Home mini | 192.168.68.76 |
| Wyze Upstairs Hall cam | 192.168.68.77 |
| Samsung TV Living | 192.168.68.78 |
| Amazon Tablet | 192.168.68.81 |
| Wife’s Android tablet | 192.168.68.83 |
| Playstation 5 | 192.168.68.88 |
| Samsung Main Bedroom | 192.168.68.89 |
| Roku Ultra | 192.168.68.90 |
| Playstation 5 | 192.168.68.91 |
| Lutron IoT | 192.168.68.92 |
| Media Laptop | 192.168.68.93 |
| My laptop | 192.168.68.94 |
| HD Home run | 192.168.68.95 |
| Playstation 4 | 192.168.68.96 |
| NUC media server | 192.168.68.97 |
| Daughter's laptop | 192.168.68.101 |
| Media laptop | 192.168.68.105 |
| Nintendo Switch | 192.168.68.118 |
| Wyze Study Camera | 192.168.68.121 |
| Samsung TV bedroom | 192.168.68.122 |
| Google Chrome stick | 192.168.68.127 |
| Deco Satellite 1 | 192.168.71.249 |
| Deco Satellite 2 | 192.168.71.250 |

What was a very interesting visual in Zenmap was the topology of my home network based on the scan results:



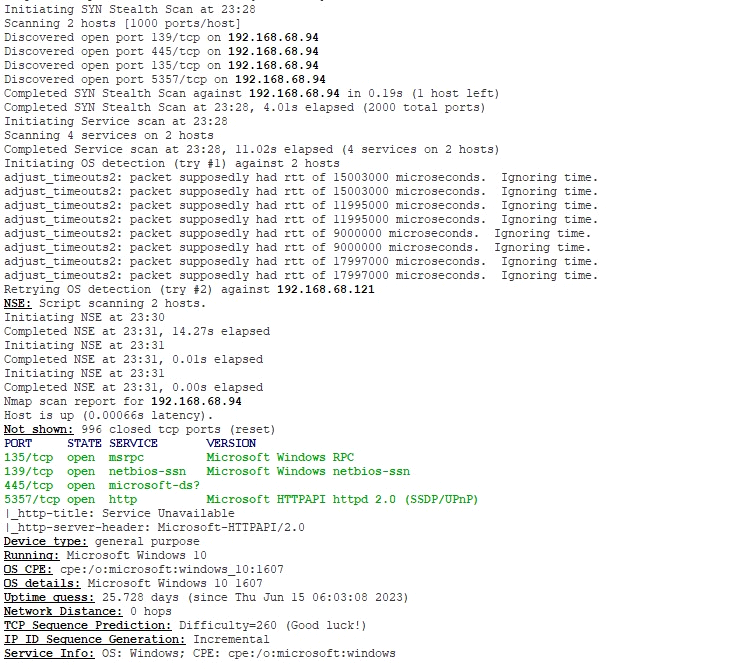
The legend helped with identifying what was what:



Referring to the topology, I had a lot of hosts with 3 to 6 open ports, but none had more than six ports open. There is no firewall on the edge so that explains why there was none shown in the topology. As expected, there are three wireless access points that represent my mesh router system. There are four switches symbolized by the squares which is also expected since I have one in the main room, the media room and two in the study area. There were a lot of filtered ports which means NMAP could not tell if it was open or not so it could mean it was the computers with windows firewall built in.

This result tells me that I still have many open ports that are susceptible exploits through security vulnerabilities or malicious services.

Host 192.168.68.94 resulted in detected services:



This was the laptop computer I ran the scan on. It was the only active computer (turned on) at the point of the scan, so this makes sense to me. What was very interesting is that NMAP was able to detect what Windows I was running, including OS details, and uptime. It looks like TCP Sequence prediction is 260. This score means the difficulty is very high for blind TCP spoofing attacks. It turns out this is the case for any system that has existed in the past 10 years or so.

**Question 3: what did you learn?**

This exercise was challenging since I had never done one before. It gave me a good idea of my attack surface at present for my home network and the exposure I have regarding hosts with open ports. I am glad that the NMAP scan showed I do not have hosts with more than six open ports but that could be inconclusive due to filtered hosts. It was interesting to learn that these scans are like what hackers do to gain access to networks! I thought that was cool to bridge that understanding. This exercise was great in developing a very basic idea of how hackers access networks and what could be done to limit the attack surface.

I am a bit curious on how a business network would look like, but the opportunity just did not seem possible for me at this time. It has given me insight into what a home network looks like and tells me that the best solution to limiting my attack surface is to keep things turned off! My guess is that this explains why some organizations implemented practices like turning off ports on company devices, limiting the hot ports in offices and even perform mac filtering. This limits the attack surface that malicious threats can exploit.

For my home network, the other option I might want to consider is setting up a network layer firewall on my home network. This added layer of protection might prevent malicious software or unnecessary network traffic. I would have to learn a bit on how to configure it but something I am considering now. Overall, this was a great experience and opened my eyes to my network’s exposure.

Citations

(n.d.). Attack Surface Definition. Tech Target. Retrieved July 12, 2023, from

<https://www.techtarget.com/whatis/definition/attack-surface>

Cybersecurity & Infrastructure Security Agency (2021, February 1). Home Network Security. CISA.gov.

Retrieved July 12, 2023, from <https://www.cisa.gov/news-events/news/home-network-security>

Hanna, K. T. (2021, July 22). *What is SYN scanning and how does it work?*. Networking.

Retrieved July 12, 2023, from <https://www.techtarget.com/searchnetworking/definition/SYN-scanning#:~:text=SYN%20scanning%20is%20a%20tactic,known%20as%20half%2Dopen%20scanning>.

*Usage and examples: NMAP network scanning*. Usage and Examples | Nmap Network Scanning. (n.d.). Retrieved July 12, 2023, from <https://nmap.org/book/nseusage.html#:~:text=NSE%20scripts%20define%20a%20list,safe%20%2C%20version%20%2C%20and%20vuln%20>.

Mikeliunas, Adrian (2021, July). Nmap installation in Windows and test run 2021. YouTube.com. Retrieved July 11, 2023, from <https://www.youtube.com/watch?v=_cx0GvdUw5k>

Trend Micro (2019, March 30). The IoT Attack Surface: Threats and Security Solutions. Trendmicro.com.

Retrieved July 12, 2023, from <https://www.trendmicro.com/vinfo/fr/security/news/internet-of-things/the-iot-attack-surface-threats-and-security-solutions>