

Research Report 1 - NMAP

Question 1: What did you do?

For the initial portion of this research report, I set out to gain familiarity with the NMAP program. The premise of how it functioned in the way it maps out the network it is connected to and then all the connections. While the goal of this exercise was to map a medium to large network, such as that of the large company I work for, I was unable to gain permission from IT and Security to conduct such a scan there. The potential risks to the company and members, due to my company being in financial services industry, are too great to justify permission which I fully respect. Due to this, I conducted the exercise on my home network which will have far less connections but can still be investigated nonetheless to gain valuable insights.

To begin, I used my command prompt to first determine my IPv4 address using the command of "ipconfig/all". This resulted in 192.168.1.229, subnet mask of 255.255.255.0 and default gateway of 192.168.1.1. From the course support readings, specifically "An Introduction to Computer Networks" by Peter L Dordal, I became aware that IPv4 addresses can indicate what type of setup a network has. Most loopback addresses begin with 127. Private IP addresses on the other hand usually begin with 172, 192 or 10. Private IP addresses are intended for site internal use. My IP address of 192 is an example which is most commonly allocated by DHCP servers while addresses beginning with 10 could indicate a connection via a VPN. I also learned that my laptop is an example of a multihomed host as it has both an ethernet interface and a Wi-Fi interface. These can be used simultaneously and be assigned different IP addresses. As I usually only connect via Wi-Fi, this is all the NMAP scans picked up. All of this helped me to gather the basic information and understanding for planning and running useful NMAP scans.

As I completed my NMAP scans, I read more of the support readings and NMAP reference information online to gather a better understanding for what each scan sought to achieve and how the information gathered would help build a strategy towards reducing my attack surface and plan a proactive approach towards network security. My background is not in IT so I found the results and knowledge gained to be very enlightening. Separately I also found reaching out to IT security colleagues in my organization to be even more rewarding as they shared real world examples of situations and remedies put in place to protect users.

Question 2: What were the results?

Researching NMAP taught me the program has many command line options I could utilize in my network research. Nmap offers a variety of scanning techniques and options that can be tailored to specific objectives and network environments. I decided to do a number of commonly used scans. The choice of the "best" scan type seems to depend entirely on the purpose of the scan, the target network, and the desired level of detail. While using the tool, I also discovered I could enter the scan options through two methods – the command line interface or within the NMAP tool itself. For the results displayed in the NMAP program, I could not find a method to print these via PDF. I did however take screenshots and include all scan results in this report.

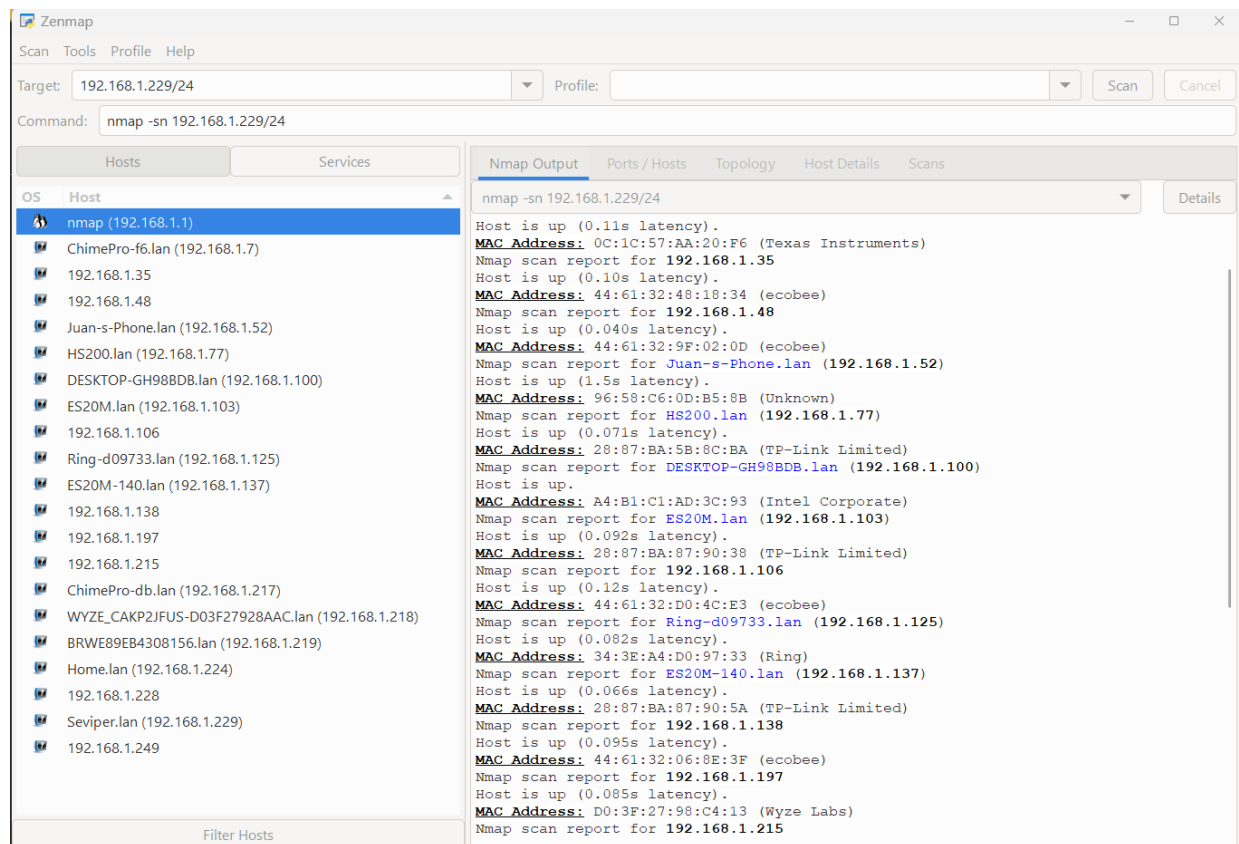
While I had not been able to gain company permission to scan their network, I was able to find time during this past week with a member of the security team to explain in more detail how they categorize an attack surface. Regardless of company or network size, cybersecurity pays high attention to their attack surface as this includes all potential points of vulnerabilities or access an attacker can exploit to compromise a system. In short, it represents the various methods in which an attacker can gain

Research Report 1 - NMAP

authorized access to things such as PII (Personal Identifiable Information), manipulate data on company systems or intentionally disrupt normal process flows for the system. This attack surface – either for a home network or large enterprise – represents all hardware from laptops to routers and servers, software, user interfaces, APIs, web applications, databases and even operating systems. Each time the system grows with new devices, software updates, poor security configuration, a new entry point for attackers can potentially become available thus growing your attack surface.

I felt the first approach I should perform on my home network was to run a Host Discovery scan to see how many active devices were on my home network. This felt to me as a great first step in determining a basic view. To do this, I entered “Nmap -sn 192.168.100.0/24”. The scan found 256 IP addresses (21 hosts up) scanned in 17.68 seconds.

This scan type is used to discover live hosts on a network without performing any port scanning. It sends ICMP echo requests (ping) and/or ARP requests to identify active hosts. The host discovery scan is useful for network reconnaissance, determining the reachability of hosts, and creating a target list for subsequent scans.

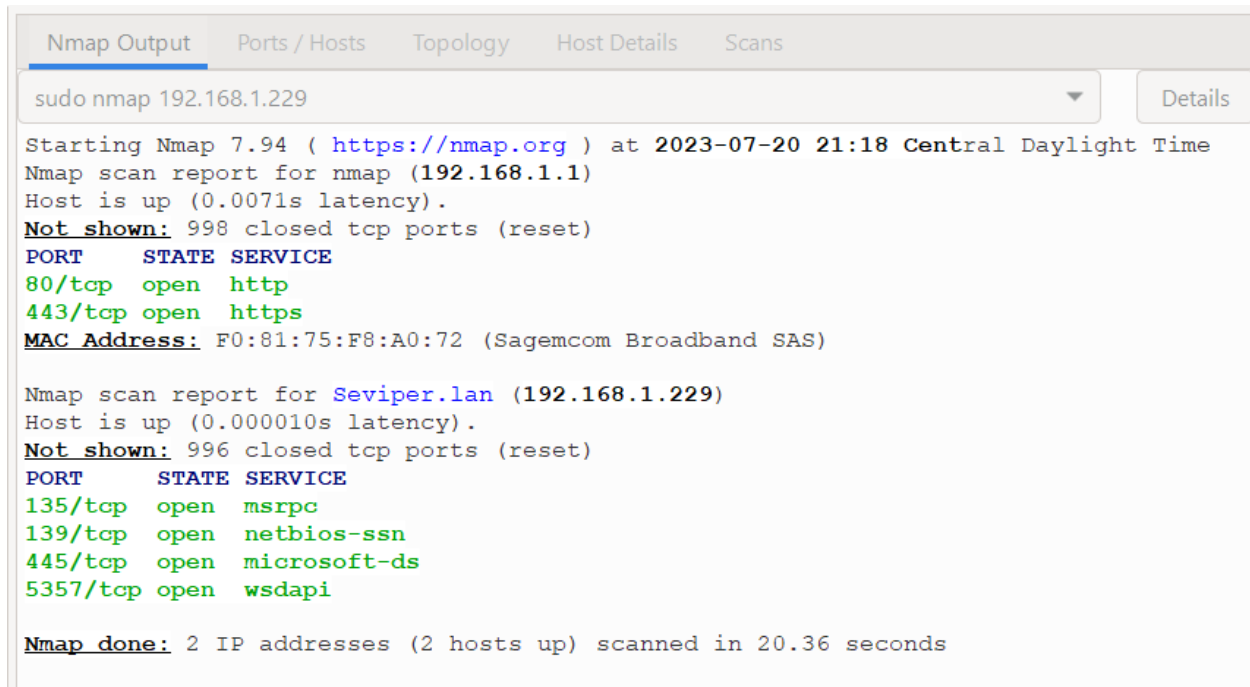


Within the Ports/Hosts tab in the NMAP program, it identified two items with an open state.

Nmap Output					
Ports / Hosts					
Port	Protocol	State	Service	Version	
80	tcp	open	http		
443	tcp	open	https		

Research Report 1 - NMAP

For the second scan I chose to perform a Port Scan to view how many ports were closed vs open for my network. I learned that Nmap can scan for open ports on target systems, providing information about which services and protocols are running. By identifying open ports, users on home networks or organizations can implement appropriate access control measures and ensure only necessary services are exposed.



The screenshot shows a web interface with tabs for 'Nmap Output', 'Ports / Hosts', 'Topology', 'Host Details', and 'Scans'. The 'Nmap Output' tab is selected, displaying the command 'sudo nmap 192.168.1.229' in a search bar. Below the command, the output of the Nmap scan is shown, including the start time, scan report for 192.168.1.1, host status, and open ports for both 192.168.1.1 and 192.168.1.229. The output is color-coded: green for open ports and red for closed ports.

```
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-20 21:18 Central Daylight Time
Nmap scan report for nmap (192.168.1.1)
Host is up (0.0071s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
MAC Address: F0:81:75:F8:A0:72 (Sagemcom Broadband SAS)

Nmap scan report for Seviper.lan (192.168.1.229)
Host is up (0.000010s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp  open  wsapi

Nmap done: 2 IP addresses (2 hosts up) scanned in 20.36 seconds
```

For more detail, I was interested in checking the ports listed as open. To do this, I selected each port individually, for example: “-p 80,443, 192.168.1.229”. At this same time, I ran into my first instance of NMAP stating the host was down and the scan request failed repeatedly. After doing some research online and asking a few peers, a possible simple solution was to simply begin the command with “sudo”.

I reviewed both Port 80 and 443 first. I found it interesting how these are open for the router address ending in .1.1 however for my laptop specifically they are closed.

Research Report 1 - NMAP

```
sudo -p 80,443 nmap 192.168.1.229
```

Details

```
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-20 21:23 Central Daylight Time
Nmap scan report for nmap (192.168.1.1)
Host is up (0.012s latency).

PORT      STATE SERVICE
80/tcp    open  http
443/tcp    open  https
MAC Address: F0:81:75:F8:A0:72 (Sagemcom Broadband SAS)

Nmap scan report for Seviper.lan (192.168.1.229)
Host is up (0.00088s latency).

PORT      STATE SERVICE
80/tcp    closed http
443/tcp    closed https

Nmap done: 2 IP addresses (2 hosts up) scanned in 19.48 seconds
```

Next, I reviewed Ports 135, 139, 445 and 5357. Port 135 indicated msrpc which I researched to determine this represent Microsoft's Remote Procedure call that allows client/server software communication. Port 139 was revealed to be NetBIOS Sessions Service which offers an API for communication between applications on a LAN and surprise to this, this predates TCP/IP. Port 445 indicated Microsoft Direct SMB which is used for file sharing. Seeing open ports like this was concerning to a network beginner such as myself but further research revealed this is typical for Windows and usually the set firewall blocks all attempts to use these points of access from the outside. One article I read indicated if someone had a second computer and ran NMAP outside of the LAN, none of these ports would be visible and thus show as closed. I did not have a second laptop to compare this information but thought that would be an interesting scan to complete.

```
sudo -p 135,139,445,5357 nmap 192.168.1.229
```

Details

```
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-20 21:25 Central Daylight Time
Nmap scan report for nmap (192.168.1.1)
Host is up (0.0049s latency).

PORT      STATE SERVICE
135/tcp    closed msrpc
139/tcp    closed netbios-ssn
445/tcp    closed microsoft-ds
5357/tcp    closed wsdapi
MAC Address: F0:81:75:F8:A0:72 (Sagemcom Broadband SAS)

Nmap scan report for Seviper.lan (192.168.1.229)
Host is up (0.0017s latency).

PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
5357/tcp    open  wsdapi

Nmap done: 2 IP addresses (2 hosts up) scanned in 19.42 seconds
```

Research Report 1 - NMAP

Third, I attempted a Services and Version scan (-sV) to hopefully get version information on services running on the target hosts. This comprehensive scan showed both pieces of information, service and version, for all of the open ports just identified in the port scan. Comprehensive scans, like Version detection, combines multiple scan techniques to provide a comprehensive assessment of target systems. Other examples are SYN scanning (-sS) and aggressive scanning options (-A). The SYN scan is useful for general port scanning and detecting firewall rules. The aggressive option also enables additional scripts and advanced techniques to gather more information about the target, such as operating system detection, service enumeration, and vulnerability scanning. This scan is useful for thorough network assessments and security audits so I decided to try this as well.

Shown first is the version scan which simply detailed the services running on the open ports I already discovered previously. This is followed by the aggressive scan which took longer to run but gained more details for the OS, network, MAC address, etc.

```
sudo -sV nmap 192.168.1.229

Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-20 21:31 Central Daylight Time
Nmap scan report for nmap (192.168.1.1)
Host is up (0.0092s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE  VERSION
80/tcp    open  http     lighttpd
443/tcp   open  ssl/http lighttpd
MAC Address: F0:81:75:F8:A0:72 (Sagemcom Broadband SAS)

Nmap scan report for Seviper.lan (192.168.1.229)
Host is up (0.000032s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE  VERSION
135/tcp   open  msrpc    Microsoft Windows RPC
139/tcp   open  netbios-ssn Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
5357/tcp  open  http     Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 2 IP addresses (2 hosts up) scanned in 45.06 seconds
```

Research Report 1 - NMAP

Nmap OutputPorts / HostsTopologyHost DetailsScans

sudo -A nmap 192.168.1.229

Details

Starting Nmap 7.94 (<https://nmap.org>) at 2023-07-22 20:52 Central Daylight Time
Nmap scan report for nmap (192.168.1.1)
Host is up (0.020s latency).
Not shown: 998 closed tcp ports (reset)

PORT	STATE	SERVICE	VERSION
80/tcp	open	http	lighttpd

|_http-title: Site doesn't have a title.
443/tcp open ssl/http lighttpd
| ssl-cert: Subject: commonName=self-signedKey/organizationName=Sagemcom Ca/
countryName=FR
| Not valid before: 2011-10-14T12:32:29
|_Not valid after: 2111-09-20T12:32:29
|_tls-alpn:
|_ http/1.0
|_ http/1.1
|_ssl-date: TLS randomness does not represent time
|_http-title: Site doesn't have a title (text/html).
MAC Address: F0:81:75:F8:A0:72 (Sagemcom Broadband SAS)
No exact OS matches for host (If you know what OS is running on it, see <https://nmap.org/submit/>).
TCP/IP fingerprint:
OS:SCAN(V=7.94%E=4%D=7/22%OT=80%CT=1%CU=42508%PV=Y%DS=1%DC=D%G=Y%M=F08175%T
OS:M=64BC87F6%P=i686-pc-windows-windows) SEQ(II=I) SEQ(SP=F7%GCD=1%ISR=106%TI
OS:=Z%II=I%TS=U) SEQ(SP=F8%GCD=1%ISR=106%TI=Z%II=I%TS=U) OPS(O1=%O2=%O3=%O4=%
OS:O5=%O6=) OPS(O1=%O2=%O3=%O4=%O5=%O6=M5B4NNS) OPS(O1=M5B4NNSNW7%O2=M5B4NNSN
OS:W7%O3=M5B4NNSNW7%O4=M5B4NNSNW7%O5=M5B4NNSNW7%O6=M5B4NNS) WIN(W1=7210%W2=7210
OS:%W3=7210%W4=7210%W5=7210%W6=7210) ECN(R=Y%DF=Y%T=40%W=7210%O=%CC=N%Q=) ECN
OS:(R=Y%DF=Y%T=40%W=7210%O=M5B4NNSNW7%CC=N%Q=) T1(R=Y%DF=Y%T=40%S=O%A=O%F=A%
OS:RD=0%Q=) T1(R=Y%DF=Y%T=40%S=O%A=O%F=AS%RD=0%Q=) T1(R=Y%DF=Y%T=40%S=O%A=S+
OS:F=AS%RD=0%Q=) T2(R=N) T3(R=N) T4(R=N) T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%
OS:RD=0%Q=) T6(R=N) T7(R=N) U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G
OS:%RUCK=G%RUD=G) IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 1 hop

TRACEROUTE
HOP RTT ADDRESS
1 20.35 ms 192.168.1.1

Nmap scan report for Sevipier.lan (192.168.1.229)
Host is up (0.00052s latency).
Not shown: 996 closed tcp ports (reset)

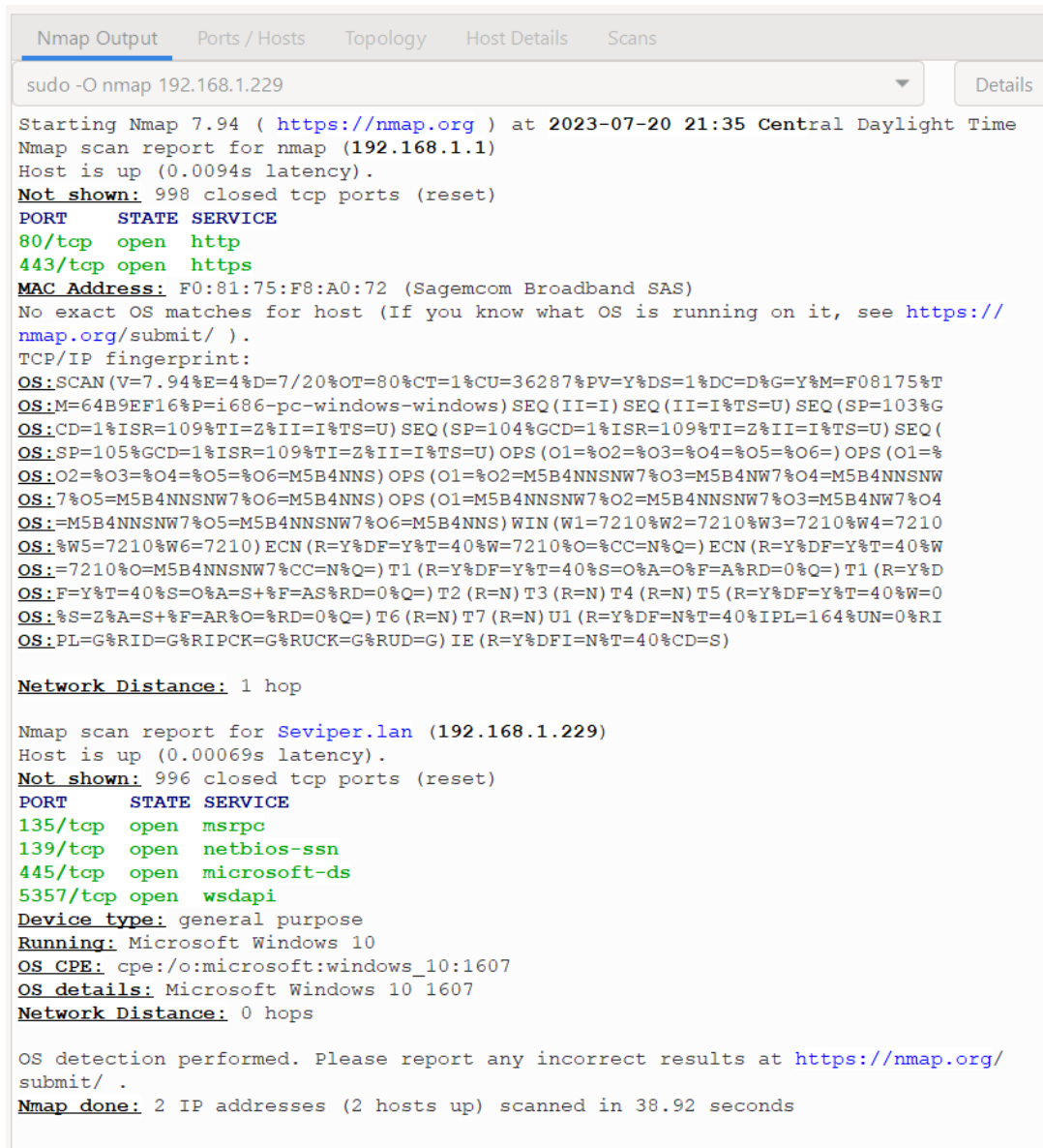
PORT	STATE	SERVICE	VERSION
135/tcp	open	msrpc	Microsoft Windows RPC
139/tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
445/tcp	open	microsoft-ds?	
5357/tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

|_http-title: Service Unavailable
|_http-server-header: Microsoft-HTTPAPI/2.0
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10:1607
OS details: Microsoft Windows 10 1607
Network Distance: 0 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
| 3:1:1:
|_ Message signing enabled but not required
| smb2-time:
| date: 2023-07-23T01:53:07
|_ start_date: N/A

Research Report 1 - NMAP

I then ran a specific OS (-O) scan to determine the operating system the target host is running and to see how this compared with the aggressive scan results. As I expected, this information matched.



```
Nmap Output  Ports / Hosts  Topology  Host Details  Scans
sudo -O nmap 192.168.1.229  Details

Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-20 21:35 Central Daylight Time
Nmap scan report for nmap (192.168.1.1)
Host is up (0.0094s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
MAC Address: F0:81:75:F8:A0:72 (Sagemcom Broadband SAS)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94%E=4%D=7/20%OT=80%CT=1%CU=36287%PV=Y%DS=1%DC=D%G=Y%M=F08175%T
OS:M=64B9EF16%P=i686-pc-windows-windows) SEQ(II=I) SEQ(II=I%TS=U) SEQ(SP=103%G
OS:CD=1%ISR=109%TI=Z%II=I%TS=U) SEQ(SP=104%GCD=1%ISR=109%TI=Z%II=I%TS=U) SEQ(
OS:SP=105%GCD=1%ISR=109%TI=Z%II=I%TS=U) OPS(O1=%O2=%O3=%O4=%O5=%O6=) OPS(O1=%
OS:O2=%O3=%O4=%O5=%O6=M5B4NNS) OPS(O1=%O2=M5B4NNSNW7%O3=M5B4NW7%O4=M5B4NNSNW
OS:7%O5=M5B4NNSNW7%O6=M5B4NNS) OPS(O1=M5B4NNSNW7%O2=M5B4NNSNW7%O3=M5B4NW7%O4
OS:=M5B4NNSNW7%O5=M5B4NNSNW7%O6=M5B4NNS) WIN(W1=7210%W2=7210%W3=7210%W4=7210
OS:%W5=7210%W6=7210) ECN(R=Y%DF=Y%T=40%W=7210%O=%CC=N%Q=) ECN(R=Y%DF=Y%T=40%W
OS:=7210%O=M5B4NNSNW7%CC=N%Q=) T1(R=Y%DF=Y%T=40%S=O%A=O%F=A%RD=0%Q=) T1(R=Y%D
OS:F=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=) T2(R=N) T3(R=N) T4(R=N) T5(R=Y%DF=Y%T=40%W=0
OS:%S=Z%A=S+%F=AR%O=%RD=0%Q=) T6(R=N) T7(R=N) U1(R=Y%DF=N%T=40%IPL=164%UN=0%RI
OS:PL=G%RID=G%RIPCK=G%RUCK=G%RUD=G) IE(R=Y%DFI=N%T=40%CD=S)

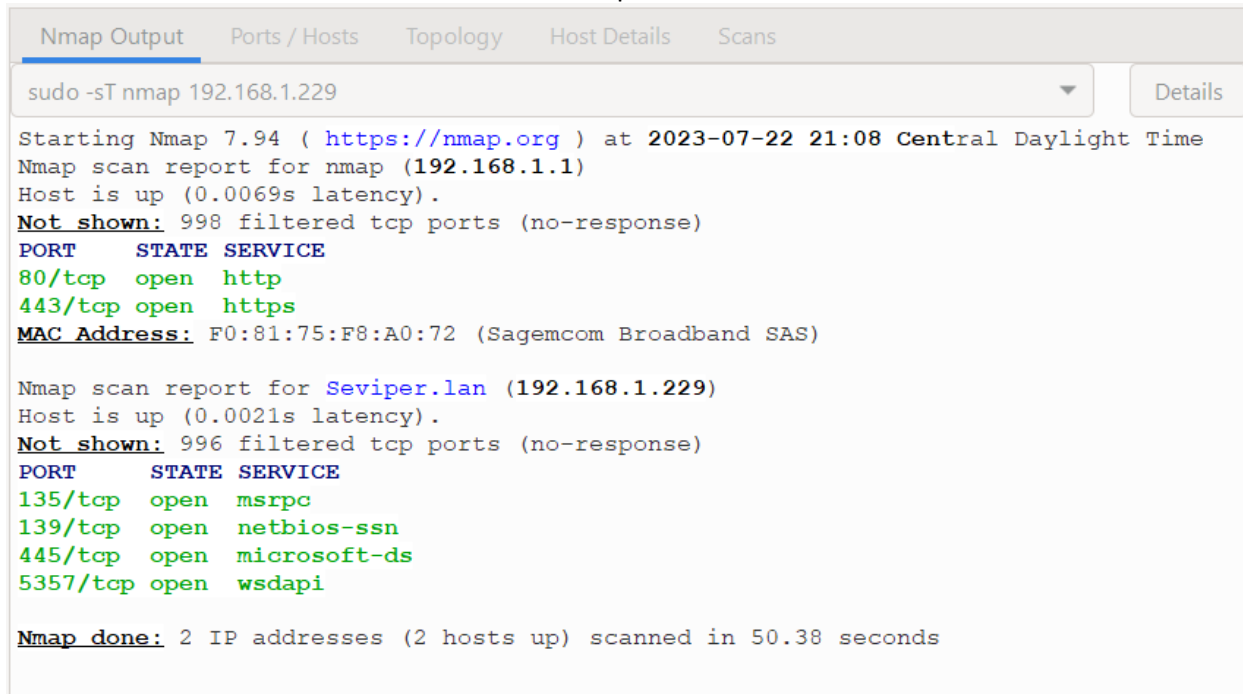
Network Distance: 1 hop

Nmap scan report for Seviper.lan (192.168.1.229)
Host is up (0.00069s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp  open  wsddapi
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10:1607
OS details: Microsoft Windows 10 1607
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 2 IP addresses (2 hosts up) scanned in 38.92 seconds
```

After running the previous scan, I came across the TCP connect scan (-sT). This is the default and most basic scan type apparently available in Nmap. It establishes a full TCP connection with each target port to check its state. It is reliable and useful for general port scanning and determining if a service is available on a particular port. Perhaps I could have reordered my scans knowing this but is valuable to know should I perform this exercise on another network.

Research Report 1 - NMAP

A screenshot of a terminal window showing Nmap scan results. The window has tabs for 'Nmap Output', 'Ports / Hosts', 'Topology', 'Host Details', and 'Scans'. The 'Nmap Output' tab is active, displaying the command 'sudo -sT nmap 192.168.1.229' and its output. The output shows two scan reports: one for '192.168.1.1' and another for 'Seviper.lan (192.168.1.229)'. Both reports list open ports and services, with the first report showing ports 80 and 443, and the second showing ports 135, 139, 445, and 5357. The scan for 'Seviper.lan' also lists the MAC address 'F0:81:75:F8:A0:72'.

```
sudo -sT nmap 192.168.1.229

Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-22 21:08 Central Daylight Time
Nmap scan report for nmap (192.168.1.1)
Host is up (0.0069s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp    open  https
MAC Address: F0:81:75:F8:A0:72 (Sagemcom Broadband SAS)

Nmap scan report for Seviper.lan (192.168.1.229)
Host is up (0.0021s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
5357/tcp   open  wsdapi

Nmap done: 2 IP addresses (2 hosts up) scanned in 50.38 seconds
```

Continuing along this path, I felt the need to run a UDP scan (-sU). UDP scan types are used to identify open UDP ports and the associated services. UDP does not have a handshake mechanism like TCP, so the scan relies on analyzing the response from target ports. Since UDP is connectionless, this scan can be slower and more challenging to perform accurately. UDP scans are useful for identifying potential vulnerabilities in services running over UDP, such as DNS, DHCP, and SNMP. This scan, while sounding very helpful to complete never actually seemed to finish. I tried to run it multiple times with no output.

Finally, I ran a Script Scanning (-sC) scan. I learned that Nmap's scripting engine, NSE, allows the execution of pre-defined scripts and this is due to the ability to automate various network-related tasks. Script scanning enables the use of scripts for specific purposes, such as vulnerability detection, service enumeration, and information gathering. Not only does Nmap contain an expansive library of scripts, it also surprisingly allows users to create custom scripts to suit their specific needs. I attempted a more thorough script tyle scan to sniff out any UPNP devices and this is the second image.

Research Report 1 - NMAP

```
Nmap Output  Ports / Hosts  Topology  Host Details  Scans
sudo -sC nmap 192.168.1.229  Details

Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-22 21:10 Central Daylight Time
Nmap scan report for nmap (192.168.1.1)
Host is up (0.015s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
|_ http-title: Site doesn't have a title.
443/tcp   open  https
|_ ssl-cert: Subject: commonName=self-signedKey/organizationName=Sagemcom Ca/
countryName=FR
|_ Not valid before: 2011-10-14T12:32:29
|_ Not valid after: 2111-09-20T12:32:29
|_ tls-alpn:
|   http/1.0
|_ http/1.1
|_ ssl-date: TLS randomness does not represent time
|_ http-title: Site doesn't have a title (text/html).
MAC Address: F0:81:75:F8:A0:72 (Sagemcom Broadband SAS)

Nmap scan report for Seviper.lan (192.168.1.229)
Host is up (0.000058s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp  open  wsdapi

Host script results:
| smb2-time:
|   date: 2023-07-23T02:11:32
|_ start_date: N/A
|_ clock-skew: -1s
| smb2-security-mode:
|   3:1:1:
|_ Message signing enabled but not required

Nmap done: 2 IP addresses (2 hosts up) scanned in 51.60 seconds
```

```
Nmap Output  Ports / Hosts  Topology  Host Details  Scans
sudo -sV -T4 --script broadcast-upnp-info nmap 192.168.1.1  Details

Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-22 21:24 Central Daylight Time
Pre-scan script results:
| broadcast-upnp-info:
|   239.255.255.250
|   Server: Ubuntu/xenial UPnP/1.1 MiniUPnPd/2.1
|   Location: http://192.168.1.1:35040/rootDesc.xml
|   Webserver: Ubuntu/xenial UPnP/1.1 MiniUPnPd/2.1
|   Name: SAC2V2S
|   Manufacturer: Sagemcom
|   Model Descr: Charter SCP Router
|   Model Name: SAC2V2S
|   Model Version: 3
|   Name: WANDevice
|   Manufacturer: MiniUPnP
|   Model Descr: WAN Device
|   Model Name: WAN Device
|   Model Version: 20230426
|   Name: WANConnectionDevice
|   Manufacturer: MiniUPnP
|   Model Descr: MiniUPnP daemon
|   Model Name: MiniUPnPd
|_ Model Version: 20230426

Nmap scan report for nmap (192.168.1.1)
Host is up (0.039s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http    lighttpd
443/tcp   open  ssl/http lighttpd
MAC Address: F0:81:75:F8:A0:72 (Sagemcom Broadband SAS)

Nmap scan report for 192.168.1.1
Host is up (0.0087s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http    lighttpd
443/tcp   open  ssl/http lighttpd
MAC Address: F0:81:75:F8:A0:72 (Sagemcom Broadband SAS)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 2 IP addresses (2 hosts up) scanned in 68.18 seconds
```

Research Report 1 - NMAP

Overall, I found that by using Nmap, users can gain valuable insights and information about network infrastructure and security. Understanding what items could be impacted by a security attack, also referred to as your attack surface, is crucial. Attacks can originate in any of the network LAN/WAN types but also Bluetooth, IoT and even cloud components/systems. The IoT device type, for example an object with an embedded sensor, have the simplest password to break. Attackers gain access to any IoT device by exploiting this vulnerability through methods like operating system oversights, unpatched vulnerabilities or even a simple bug. In short, the capabilities of Nmap enhance user's understanding of network infrastructure, assess security risks, and aide to implement appropriate security measures to protect systems from potential threats.

Question 3: What did you learn?

First thing I have learned by working on this research report is that by understanding the attack surface, home network owners and organizations alike can enhance their security posture by taking precautions and implementing measures such as regular software updates, robust access controls, network segmentation, intrusion detection systems, firewalls and overall security awareness training. Gaining insight where a system can be vulnerable is essential in order to take the proper precautions to protect it. By leveraging the capabilities of tools like Nmap, users can enhance their understanding of network infrastructure, assess security risks, and implement appropriate security measures to protect their systems from potential threats. Nmap provides a comprehensive view of network infrastructure, helping users understand the relationships between hosts, subnets, and routers. Nmap can be utilized to diagnose network connectivity problems, identify network bottlenecks, and troubleshoot network issues by examining the reachability and responsiveness of hosts and services. Nmap can also assist in compliance audits by providing information about network assets, open ports, and software versions. This data aids in critical in meeting regulatory requirements and ensuring adherence to security standards. Personally, I would love to take more time and find a way to see how items such as my cell phone can be vulnerable and scan that device somehow and review the data collected.

Next most important understanding I gained is that digital networks, and cybersecurity as a whole, involves a number of crucial aspects. A few examples are as follows. When speaking with my security colleagues, Network Architecture plays a huge role. Having knowledge of all the network's components, switches, firewalls, servers and endpoints. The interconnections and process flow of data within the network is what a home network user or a security team in an organization use to help find vulnerabilities and design security measures. Second most important, as I just mentioned above, is the attack surface or as my organization refers to it, Threat Landscape. A few other important items are a proper risk assessment, security policies and procedures, incident response plans and implementing continuous monitoring tools.

Last, I feel a level of security awareness training is a must. Not surprisingly, we as humans are the weakest link in cybersecurity. Keeping myself, or members of an organization which share usage of a system, aware of common threats, social engineering techniques and general best practices in creating strong passwords, avoiding phishing scams and browsing safely helps reduce successful attacks. It sounds repetitive but by understanding these aspects, an organization can develop a proactive approach to enhance their ability to defend against a wide range of threats and protect their digital networks effectively.