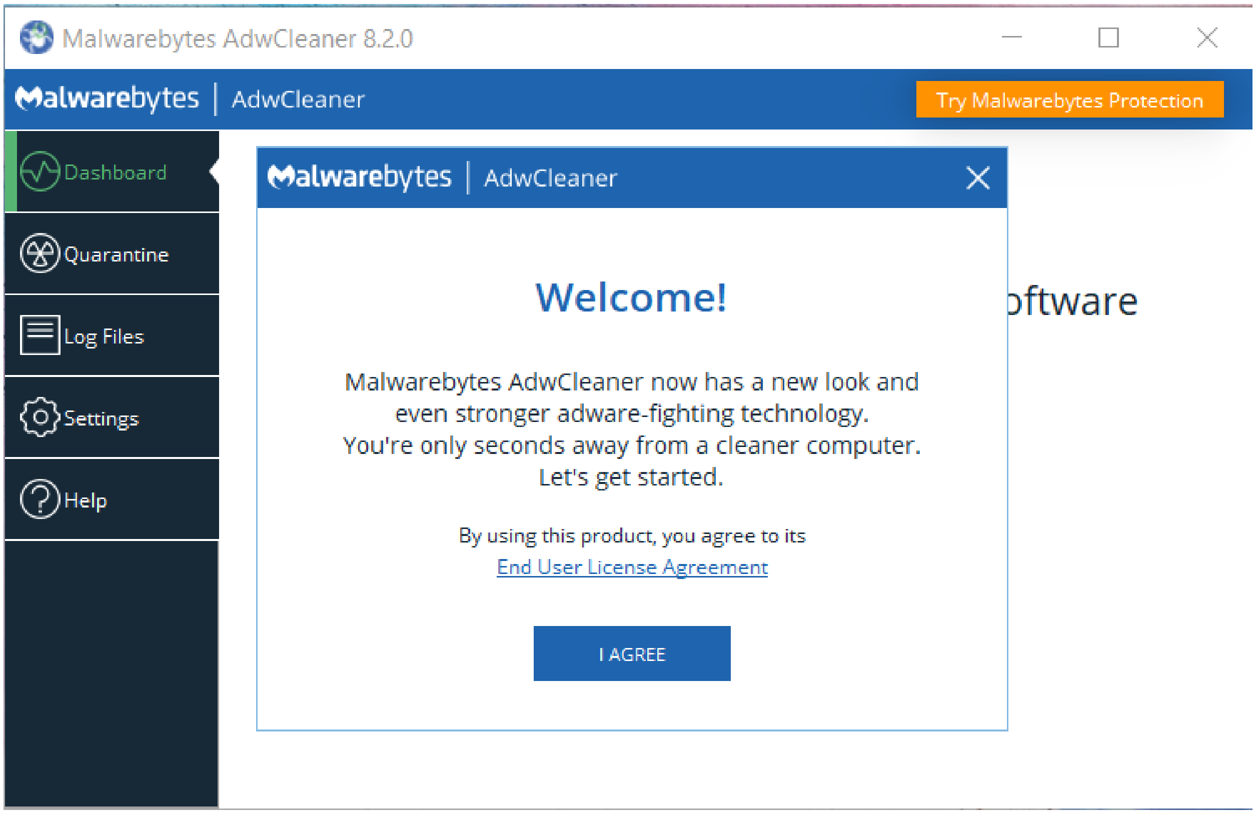
Lab 3 (Final Part1)
Report

By: Sneha Shukla

Task 1: Clean your computer from adware and spyware.

Result: The computer was cleaned using MalwareBytes AdwCleaner. The figures below are evidence of the task done.

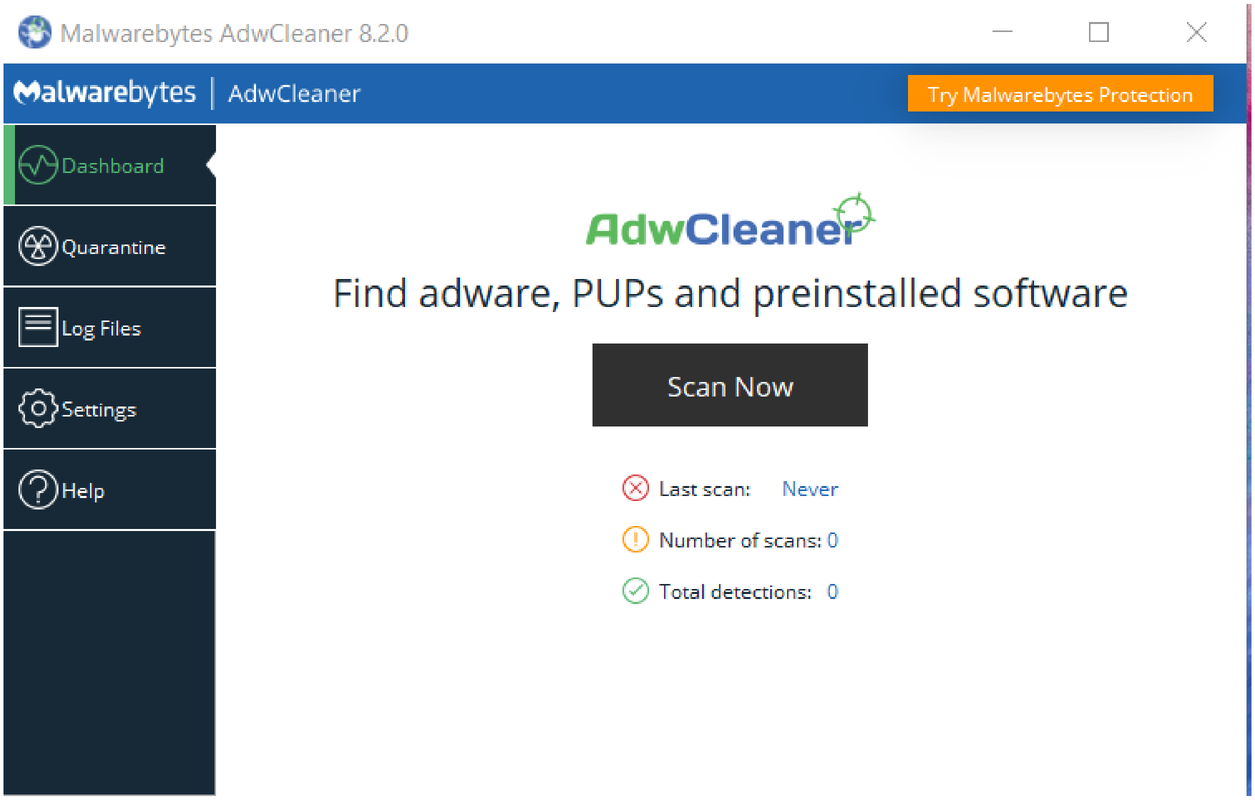

Malwarebytes AdwCleaner 8.2.0
Malwarebytes | AdwCleaner
Try Malwarebytes Protection
Dashboard
Quarantine
Log Files
Settings
Help
Malwarebytes | AdwCleaner
oftware
I AGREE

Welcome!

Malwarebytes AdwCleaner now has a new look and even stronger adware-fighting technology. You're only seconds away from a cleaner computer. Let's get started.

By using this product, you agree to its End User License Agreement

Figure 1: Installed the Malwarebytes AdwCleaner application on the computer.


Malwarebytes AdwCleaner 8.2.0
Malwarebytes | AdwCleaner
Try Malwarebytes Protection
Dashboard
Quarantine
Log Files
Settings
Help
AdwCleaner
Scan Now

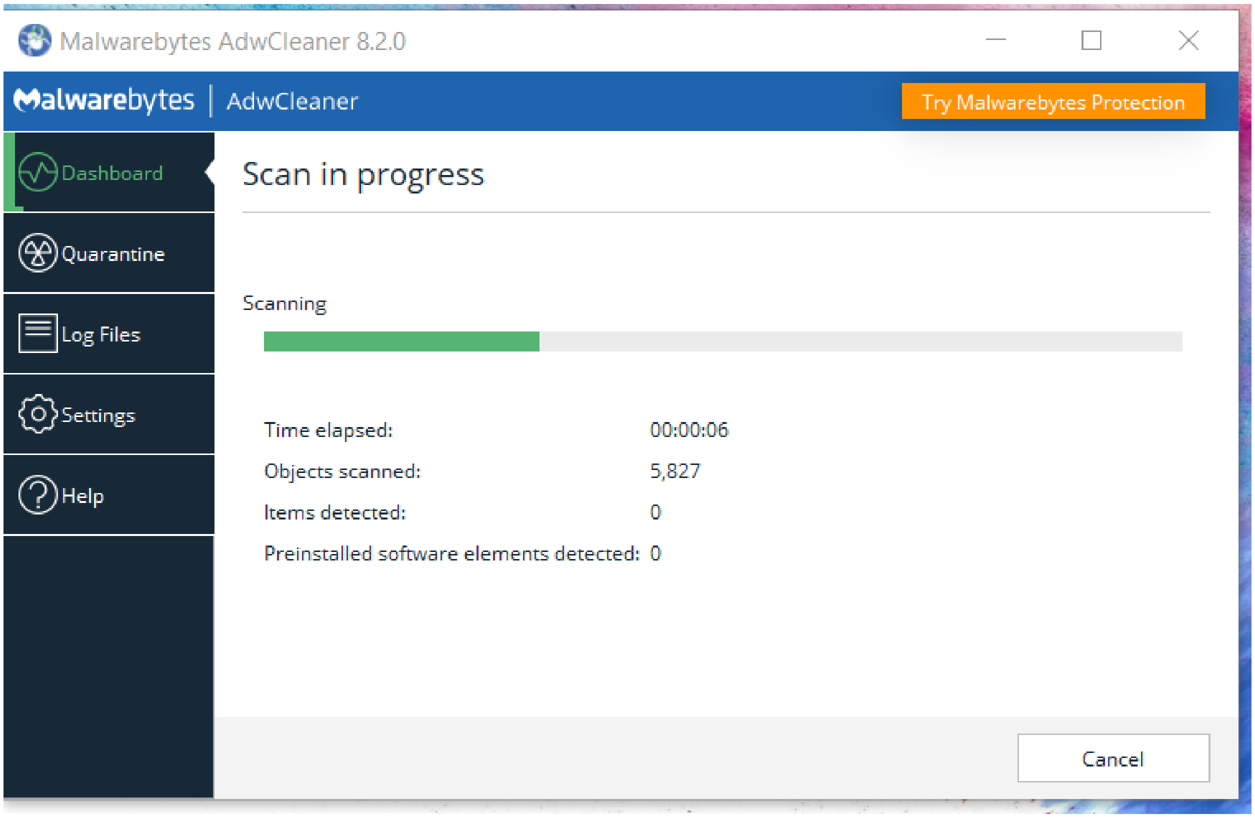
Find adware, PUPs and preinstalled software

Last scan: Never

Number of scans: 0

Total detections: 0

Figure 2: Successfully installed and ready to scan and clean the computer.

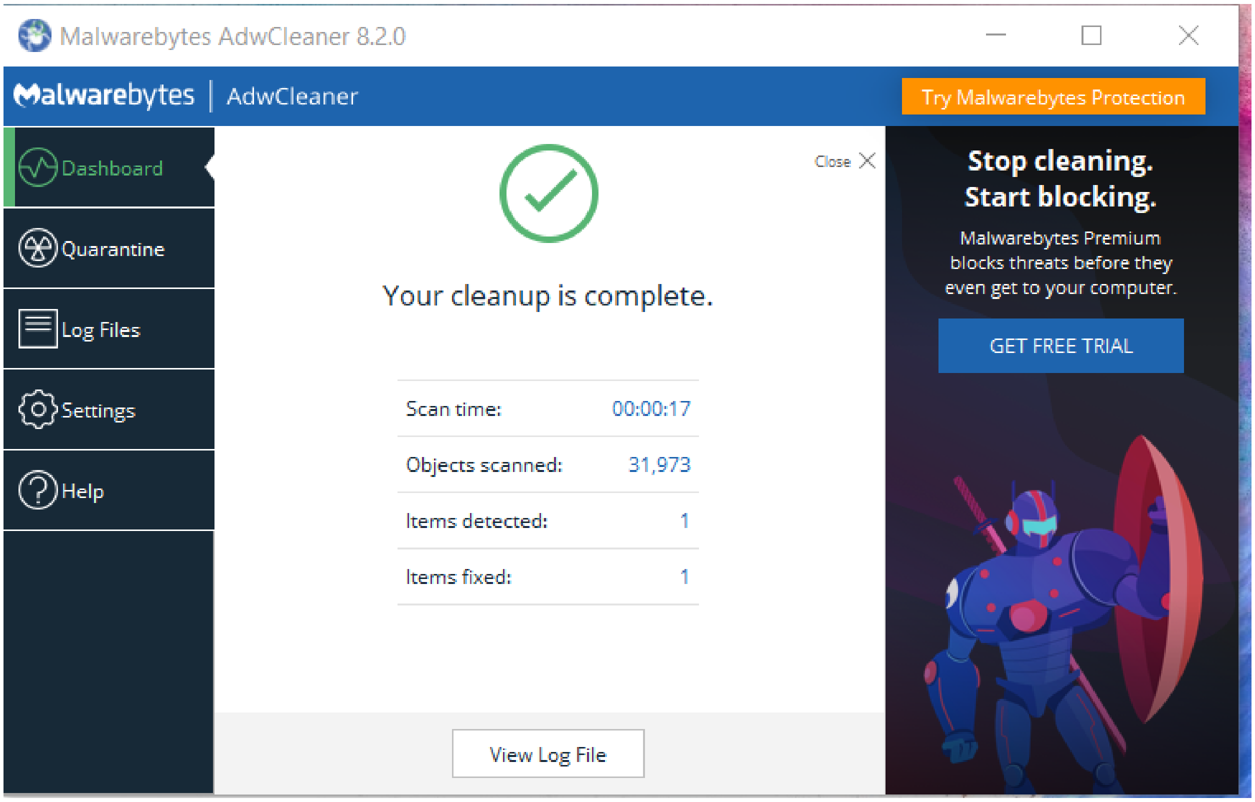

Malwarebytes AdwCleaner 8.2.0
Malwarebytes | AdwCleaner
Try Malwarebytes Protection
Dashboard
Quarantine
Log Files
Settings
Help
Cancel

Scan in progress

Scanning

Time elapsed: 00:00:06
Objects scanned: 5,827
Items detected: 0
Preinstalled software elements detected: 0

Figure 3: Scanning in Progress


Malwarebytes AdwCleaner 8.2.0
Malwarebytes | AdwCleaner
Try Malwarebytes Protection
Dashboard
Quarantine
Log Files
Settings
Help
Close
Stop cleaning.
Start blocking.
Malwarebytes Premium blocks threats before they even get to your computer.
GET FREE TRIAL
View Log File

Your cleanup is complete.

Scan time: 00:00:17

Objects scanned: 31,973

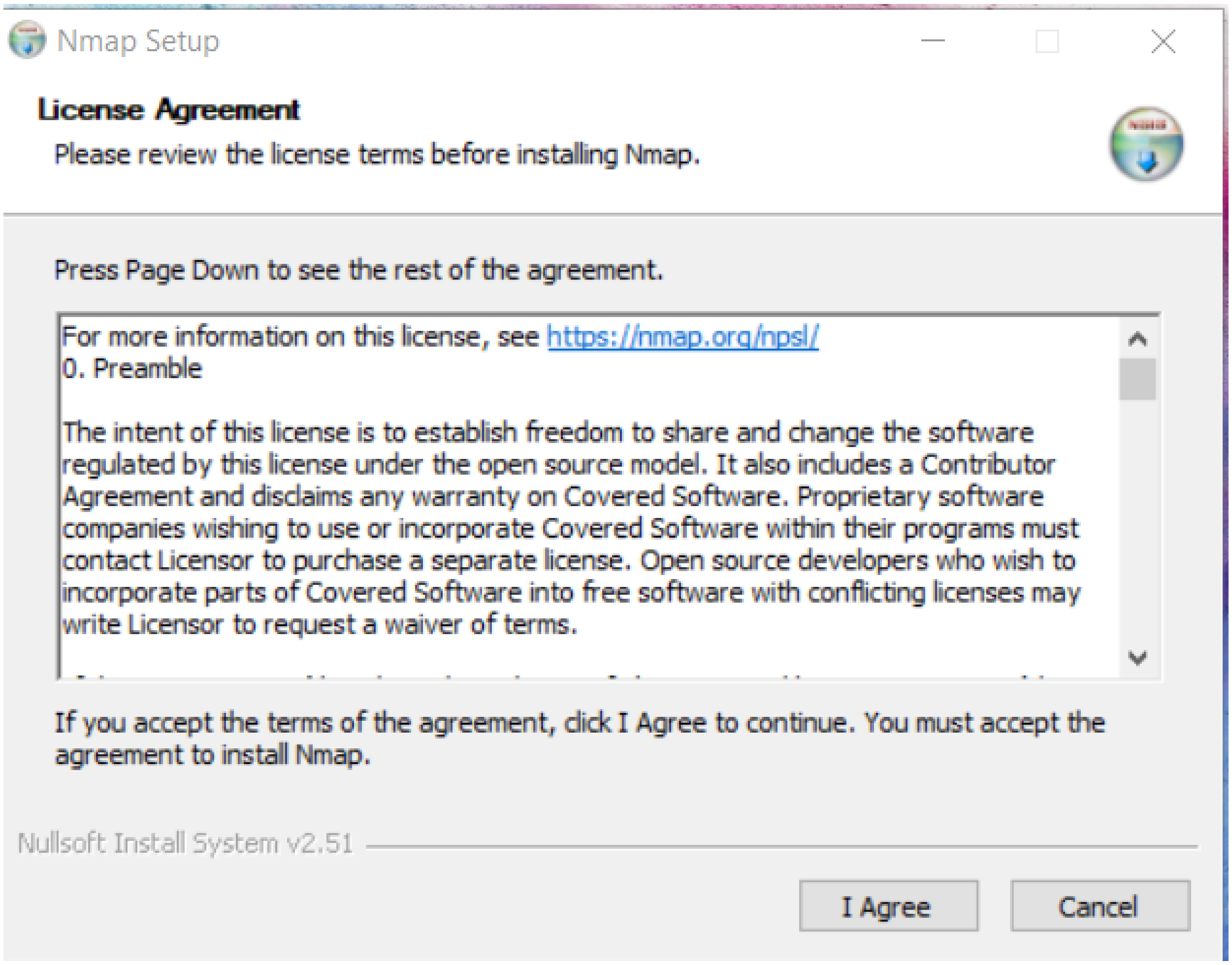
Items detected: 1

Items fixed: 1

Figure 4: Cleanup completed.

Task 2: Install Nmap.

Result: Nmap, short for Network Mapper, is a free, open-source tool for vulnerability scanning and network discovery. Network administrators use Nmap to identify what devices are running on their systems, discovering hosts that are available and the services they offer, finding open ports and detecting security risks.
Below figures are proof for its installation.



License Agreement

Please review the license terms before installing Nmap.

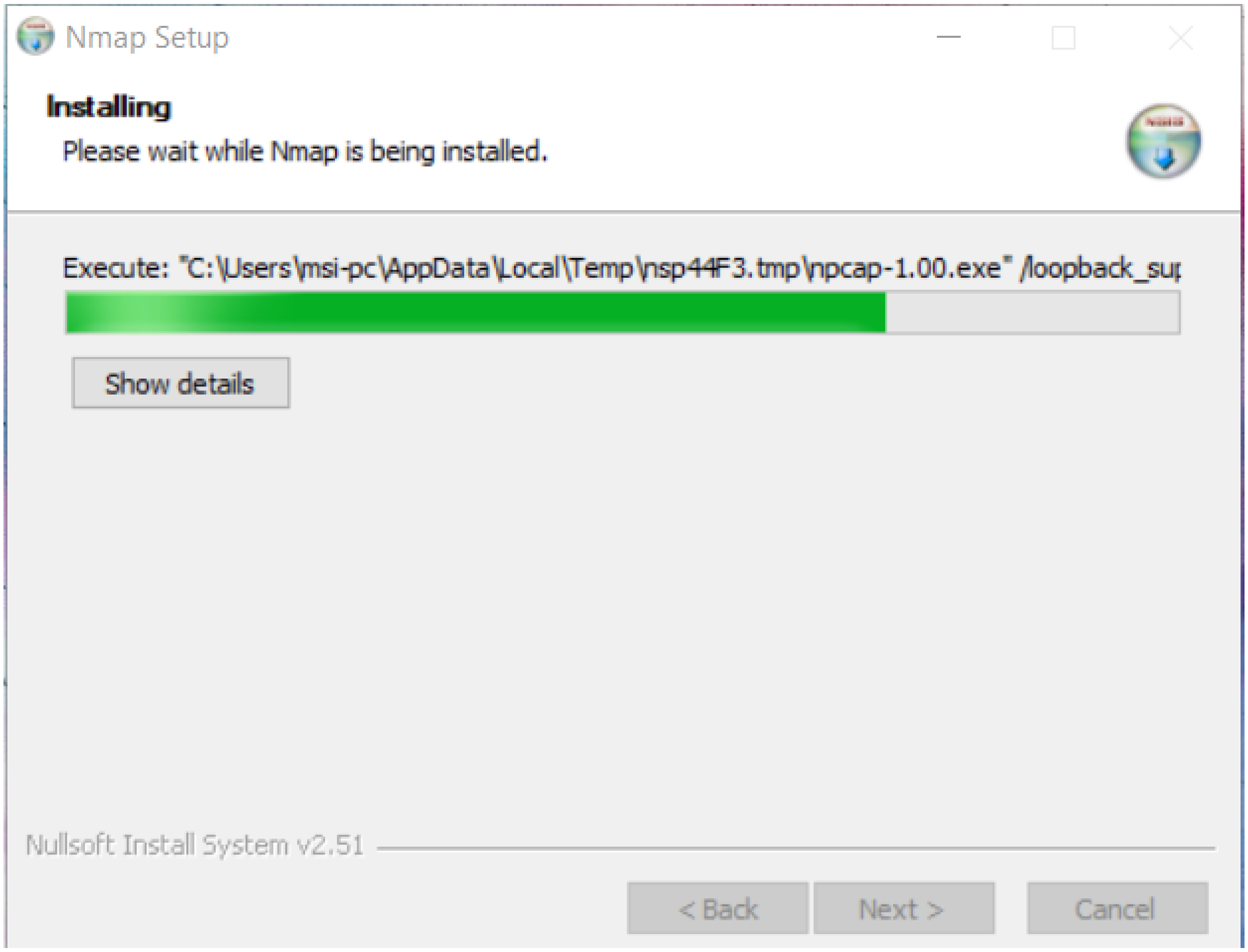
Press Page Down to see the rest of the agreement.

For more information on this license, see https://nmap.org/npsl/
0. Preamble

The intent of this license is to establish freedom to share and change the software regulated by this license under the open source model. It also includes a Contributor Agreement and disclaims any warranty on Covered Software. Proprietary software companies wishing to use or incorporate Covered Software within their programs must contact Licensor to purchase a separate license. Open source developers who wish to incorporate parts of Covered Software into free software with conflicting licenses may write Licensor to request a waiver of terms.

If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install Nmap.

Figure 5: Installation of Nmap in the computer.

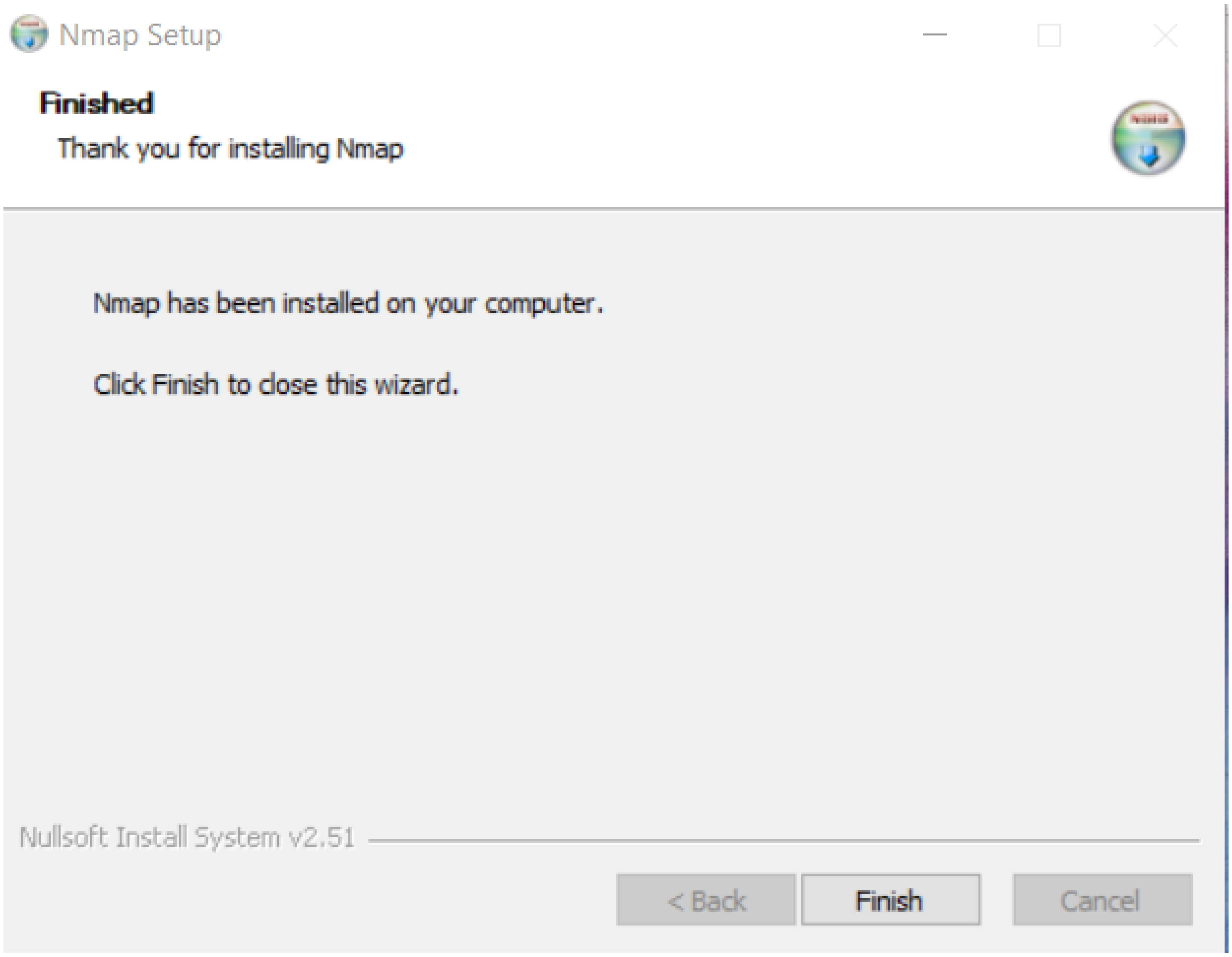


Installing

Please wait while Nmap is being installed.

Execute: "C:\Users\msi-pc\AppData\Local\Temp\nsp44F3.tmp\npcap-1.00.exe" /loopback_sup

Figure 6: Installing



Nmap Setup

Finished

Thank you for installing Nmap

Nmap has been installed on your computer.

Click Finish to close this wizard.

Figure 7: Installation Complete.

Task 3: Learn the command syntax and functionality of Nmap.

Result: Learnt the command syntax and functionality of Nmap and here’s the quick summary.

Basic Scanning Commands of Nmap:

Goal	Command	Example
Scan a Single Target	nmap [target]	nmap 192.168.0.1
Scan Multiple Targets	nmap [target1, target2, etc	nmap 192.168.0.1 192.168.0.2
Scan a Range of Hosts	nmap [range of ip addresses]	nmap 192.168.0.1-10
Scan an Entire Subnet	nmap [ip address/cdir]	nmap 192.168.0.1/24
Scan Random Hosts	nmap -iR [number]	nmap -iR 0
Excluding Targets from a Scan	nmap [targets] – exclude [targets]	nmap 192.168.0.1/24 –exclude 192.168.0.100, 192.168.0.200
Excluding Targets Using a List	nmap [targets] – excludefile [list.txt]	nmap 192.168.0.1/24 –excludefile notargets.txt
Perform an Aggressive Scan	nmap -A [target]	nmap -A 192.168.0.1
Scan an IPv6 Target	nmap -6 [target]	nmap -6 1aff:3c21:47b1:0000:0000:0000:0000:2afe

Functionalities of Nmap:

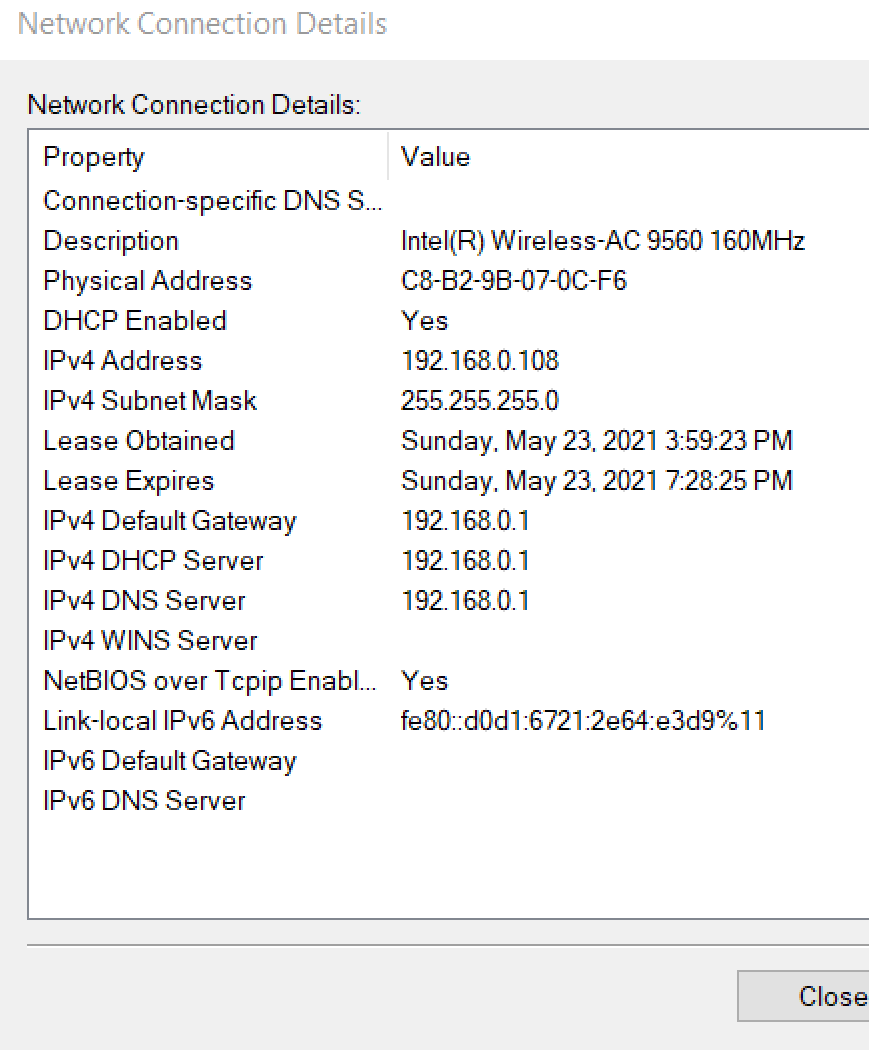
- Host discovery
- Scan techniques
- Port specification and scan order
- Service or version detection
- Script scan
- OS detection
- Timing and performance
- Evasion and spoofing
- Output
- Target specification

Task 4: Determine your IP address.

Result: IP Address has been determined in many ways. I have chosen this way:

Step 1: Clicked on Control Panel.
Step 2: Clicked on Network and Internet.
Step 3: Clicked on “View network status and tasks” under Network and Sharing Centre
Step 4: Clicked on my Connections and then saw the details.

The following figure is evidence of the task done.



Network Connection Details

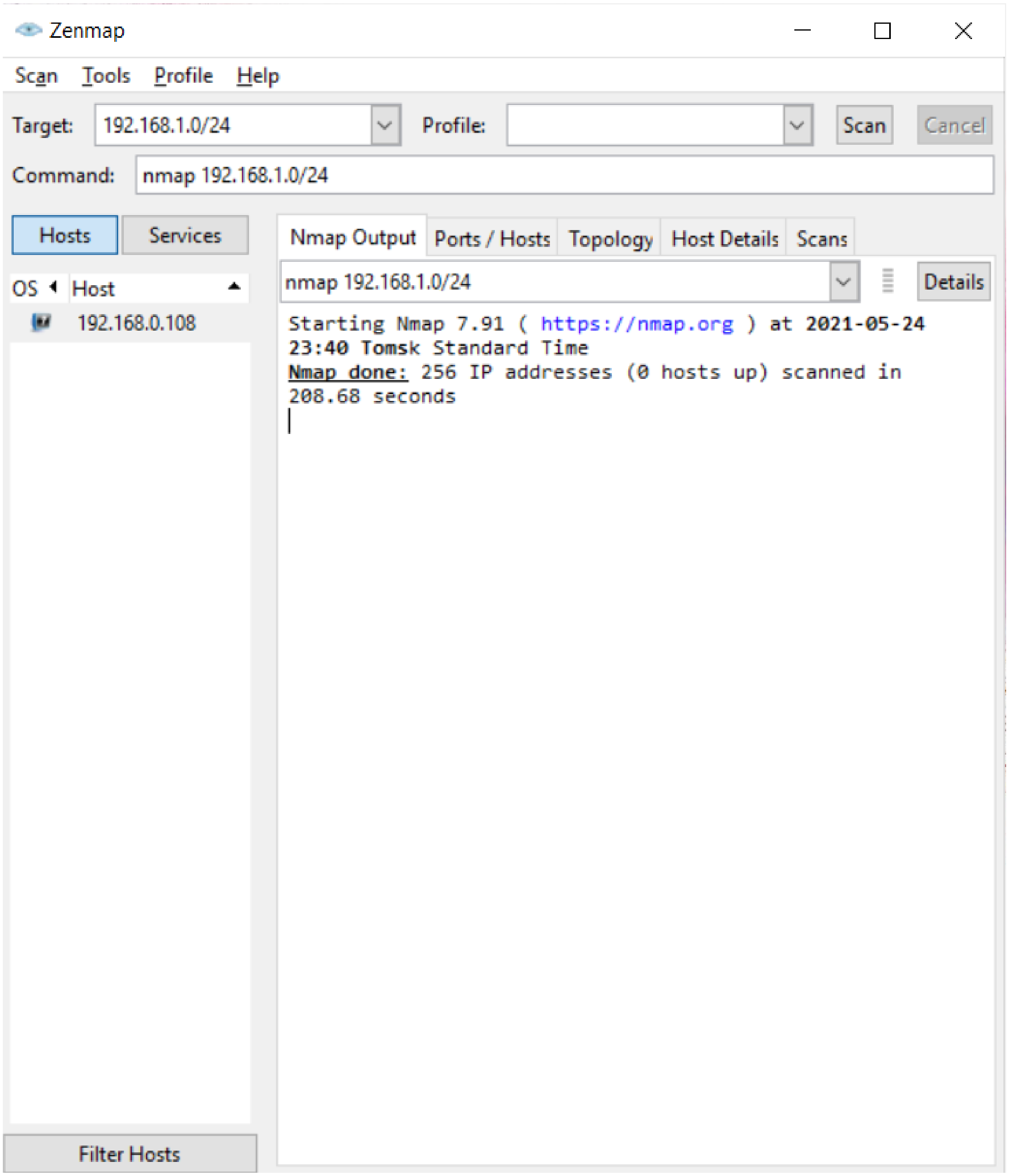
Network Connection Details:

Property	Value
Connection-specific DNS S...	
Description	Intel(R) Wireless-AC 9560 160MHz
Physical Address	C8-B2-9B-07-0C-F6
DHCP Enabled	Yes
IPv4 Address	192.168.0.108
IPv4 Subnet Mask	255.255.255.0
Lease Obtained	Sunday, May 23, 2021 3:59:23 PM
Lease Expires	Sunday, May 23, 2021 7:28:25 PM
IPv4 Default Gateway	192.168.0.1
IPv4 DHCP Server	192.168.0.1
IPv4 DNS Server	192.168.0.1
IPv4 WINS Server	
NetBIOS over Tcpip Enabl...	Yes
Link-local IPv6 Address	fe80::d0d1:6721:2e64:e3d9%11
IPv6 Default Gateway	
IPv6 DNS Server	

Figure 8: My IP Address.

Task 5: Perform a clean scan of your subnet without attracting attention. Use the appropriate setting when scanning and 24 bit width.

Result: A subnet, or subnetwork, is a network inside a network. Subnets make networks more efficient. Through subnetting, network traffic can travel a shorter distance without passing through unnecessary routers to reach its destination.



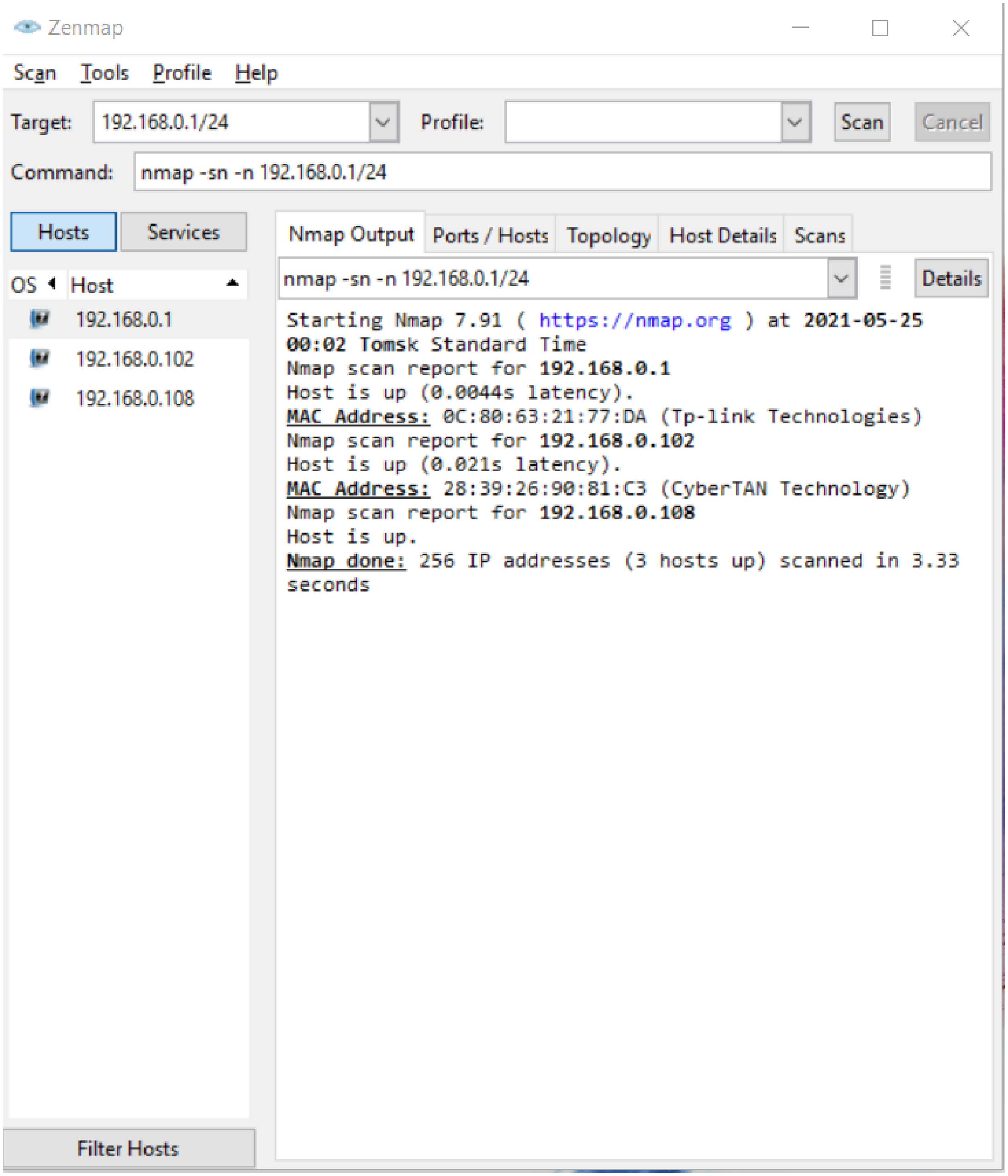
```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-24
23:40 Tomsk Standard Time
Nmap done: 256 IP addresses (0 hosts up) scanned in
208.68 seconds
```

Figure 9: Scan of my subnet.

Task 6: Perform an ARP scan of your subnet using 24 bits. Analyze the scan and draw conclusions.

Result: ARP scanning is a process used to identify other active hosts on a local network, and they're surprisingly easy to perform. Every aspiring hacker needs to have a solid understanding of fundamental networking protocols, and ARP is near the top of the list. Without ARP, LANs would cease to function, and you need to feel comfortable checking the contents of your ARP cache as well as understand how to perform ARP scanning.

ARP is a very important networking protocol that binds layer two addresses to layer three addresses. With IPv4, ARP (Address Resolution Protocol) makes one to one links between MAC addresses and IP addresses. But ARP is frequently used by hackers to poke around and feel out local network topologies. Most often, the process of using an ARP scan falls under the reconnaissance umbrella, too. But before we look at different methods to perform ARP scans, you need to know how ARP operates on a technical level.



Target: 192.168.0.1/24

Command: nmap -sn -n 192.168.0.1/24

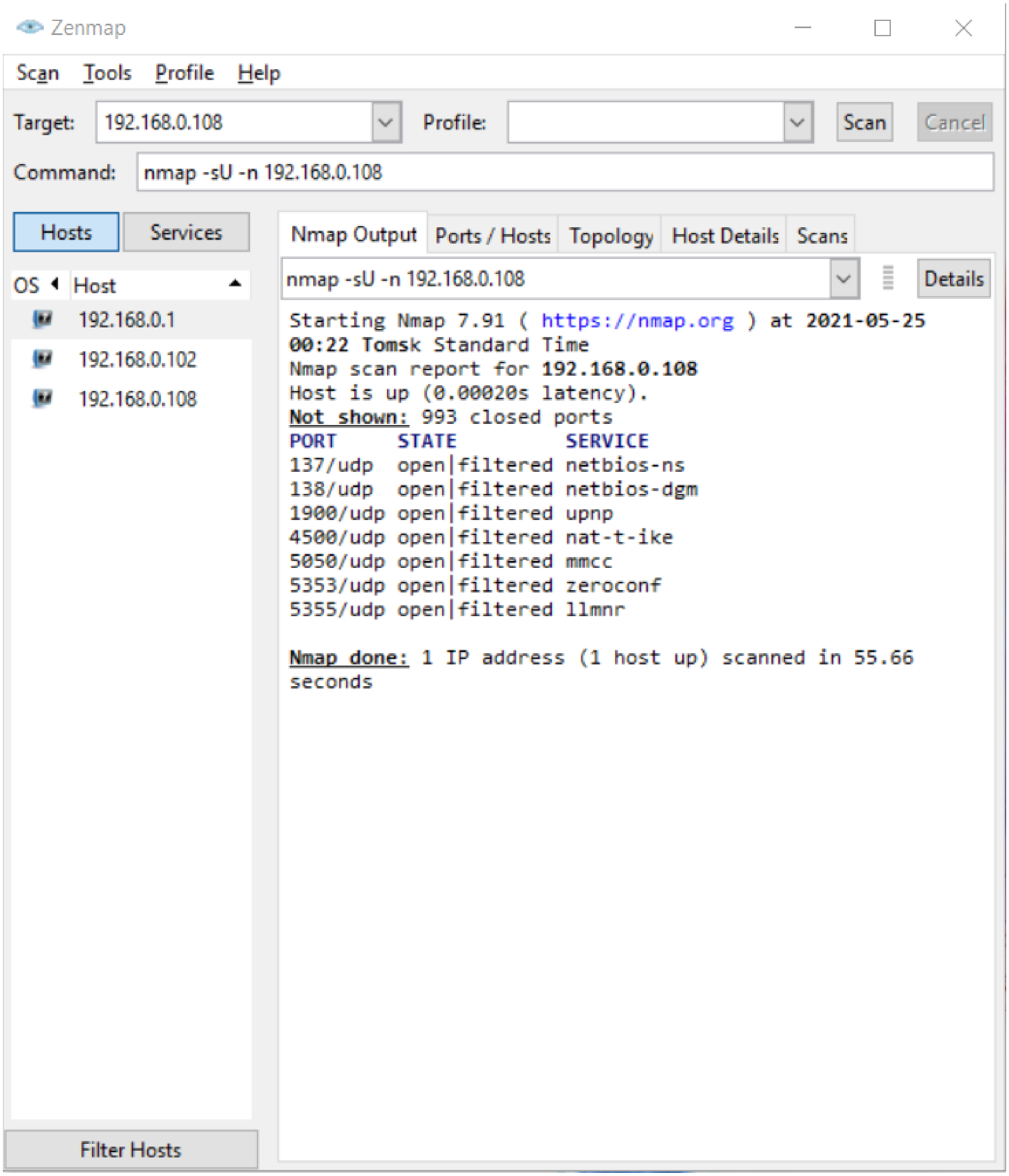
192.168.0.1
192.168.0.102
192.168.0.108

```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-25
00:02 Tomsk Standard Time
Nmap scan report for 192.168.0.1
Host is up (0.0044s latency).
MAC Address: 0C:80:63:21:77:DA (Tp-link Technologies)
Nmap scan report for 192.168.0.102
Host is up (0.021s latency).
MAC Address: 28:39:26:90:81:C3 (CyberTAN Technology)
Nmap scan report for 192.168.0.108
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 3.33
seconds
```

Figure 10: ARP Scan

Task 7: Select any host from the results in step 4 or 5 and perform a UDP scan on the default port. Compare the current results with those obtained in step 4 or 5.

Result: As we all know, TCP is a connection-oriented protocol that establishes a connection to the remote host via a 3-way handshake, kinda like a formal introduction. UDP, on the other hand, is a connectionless protocol and less formal. In this sense, a UDP connection is a meaningless term since a client can send packets to a UDP service without first establishing a connection. This means UDP is more difficult to probe than TCP. Basically, you can throw out a bunch of packets and hope something sticks or in this case, what is returned.



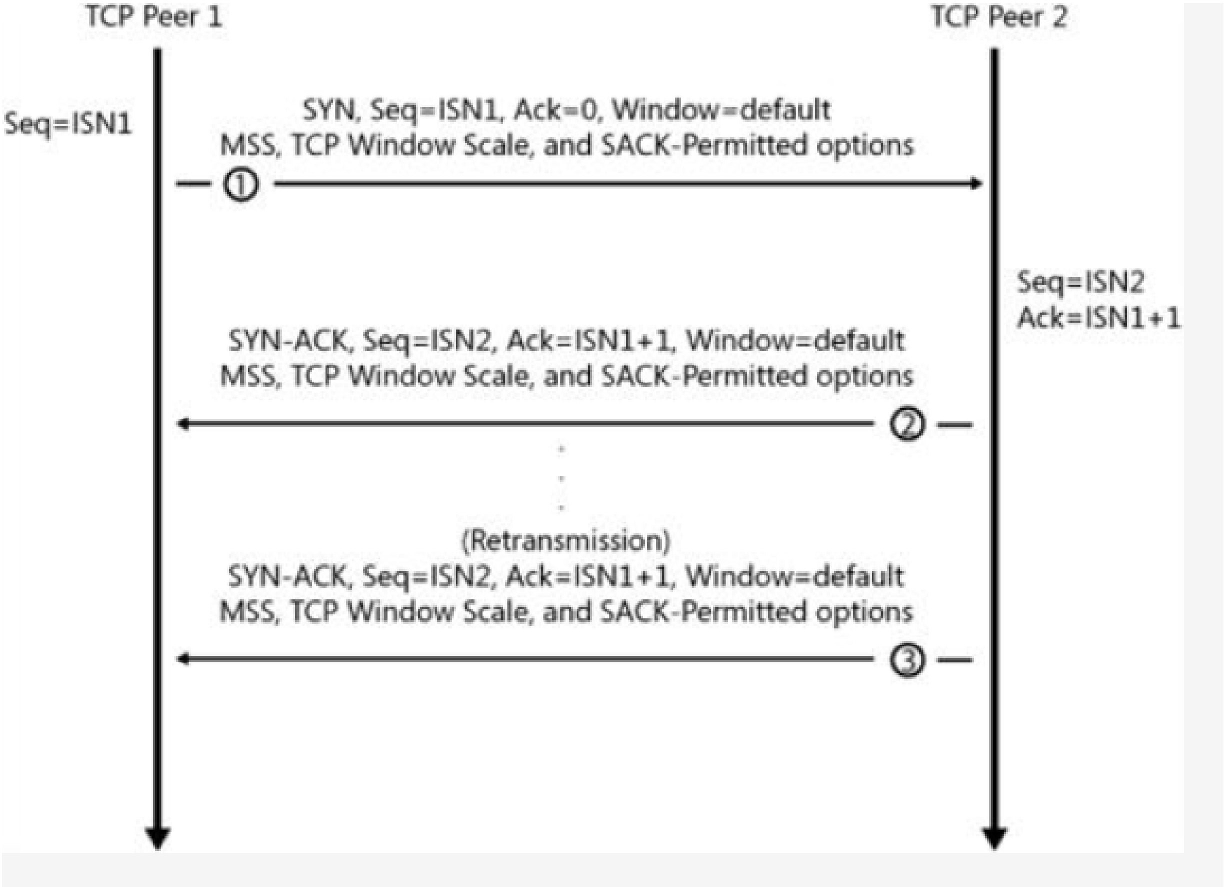
Command: nmap -sU -n 192.168.0.108

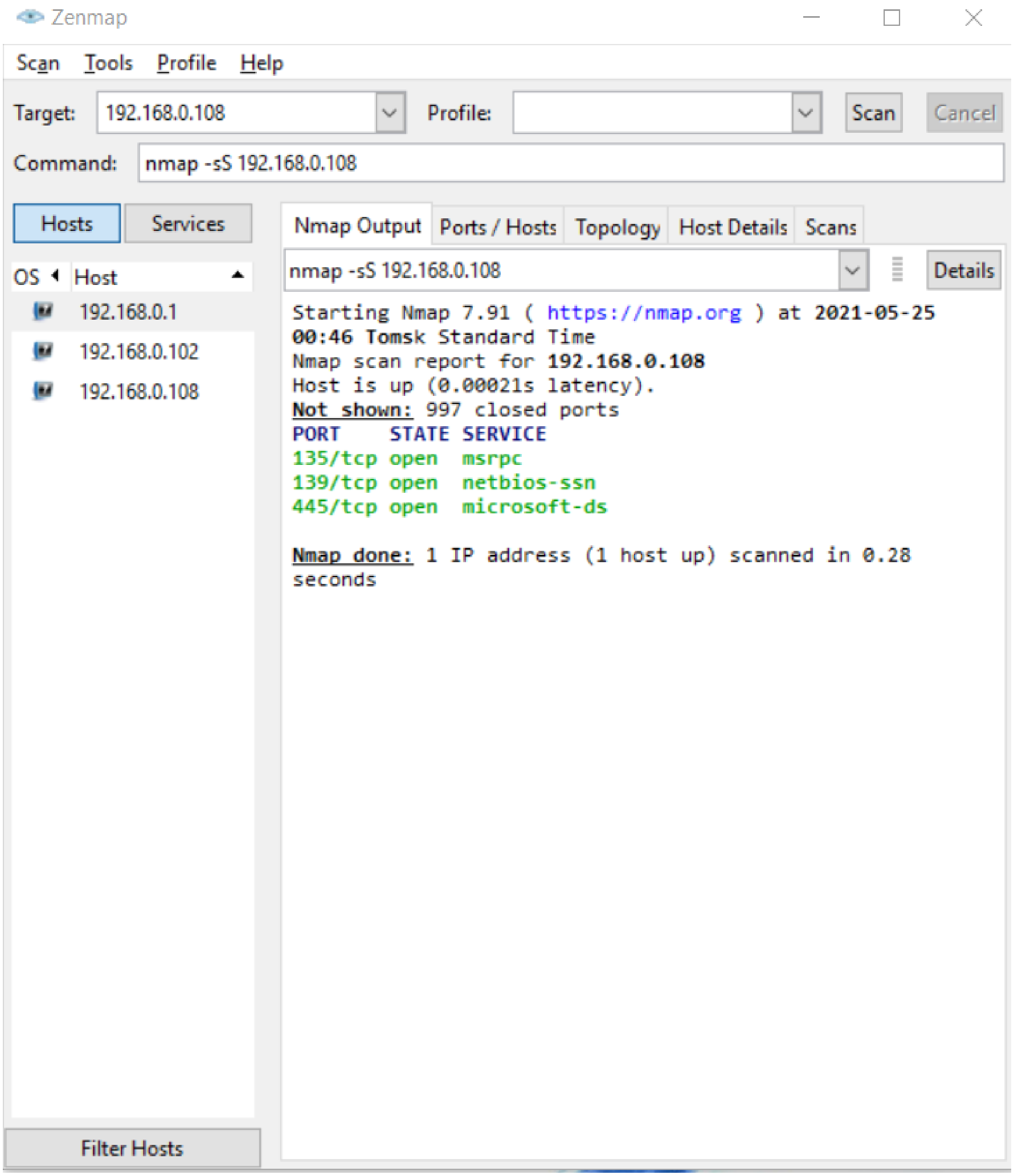
```
nmap -sU -n 192.168.0.108

Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-25
00:22 Tomsk Standard Time
Nmap scan report for 192.168.0.108
Host is up (0.00020s latency).
Not shown: 993 closed ports
PORT     STATE         SERVICE
137/udp  open|filtered netbios-ns
138/udp  open|filtered netbios-dgm
1900/udp open|filtered upnp
4500/udp open|filtered nat-t-ike
5050/udp open|filtered mmcc
5353/udp open|filtered zeroconf
5355/udp open|filtered llmnr

Nmap done: 1 IP address (1 host up) scanned in 55.66
seconds
```

Figure 11: UDP Scan

Task 8: Scan your network using half-open connections. Compare with the result from step 4.

Result: A TCP half-open connection, shown in figure below, is a TCP connection that has not completed the connection establishment process. A SYN segment has been received and a SYN-ACK has been sent, but the final ACK has not been received. Until the final ACK is received, data cannot be sent on the connection.


TCP Peer 1
TCP Peer 2
Seq=ISN1
SYN, Seq=ISN1, Ack=0, Window=default
MSS, TCP Window Scale, and SACK-Permitted options
①
Seq=ISN2
Ack=ISN1+1
SYN-ACK, Seq=ISN2, Ack=ISN1+1, Window=default
MSS, TCP Window Scale, and SACK-Permitted options
②
(Retransmission)
SYN-ACK, Seq=ISN2, Ack=ISN1+1, Window=default
MSS, TCP Window Scale, and SACK-Permitted options
③



```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-25
00:46 Tomsk Standard Time
Nmap scan report for 192.168.0.108
Host is up (0.00021s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 0.28
seconds
```

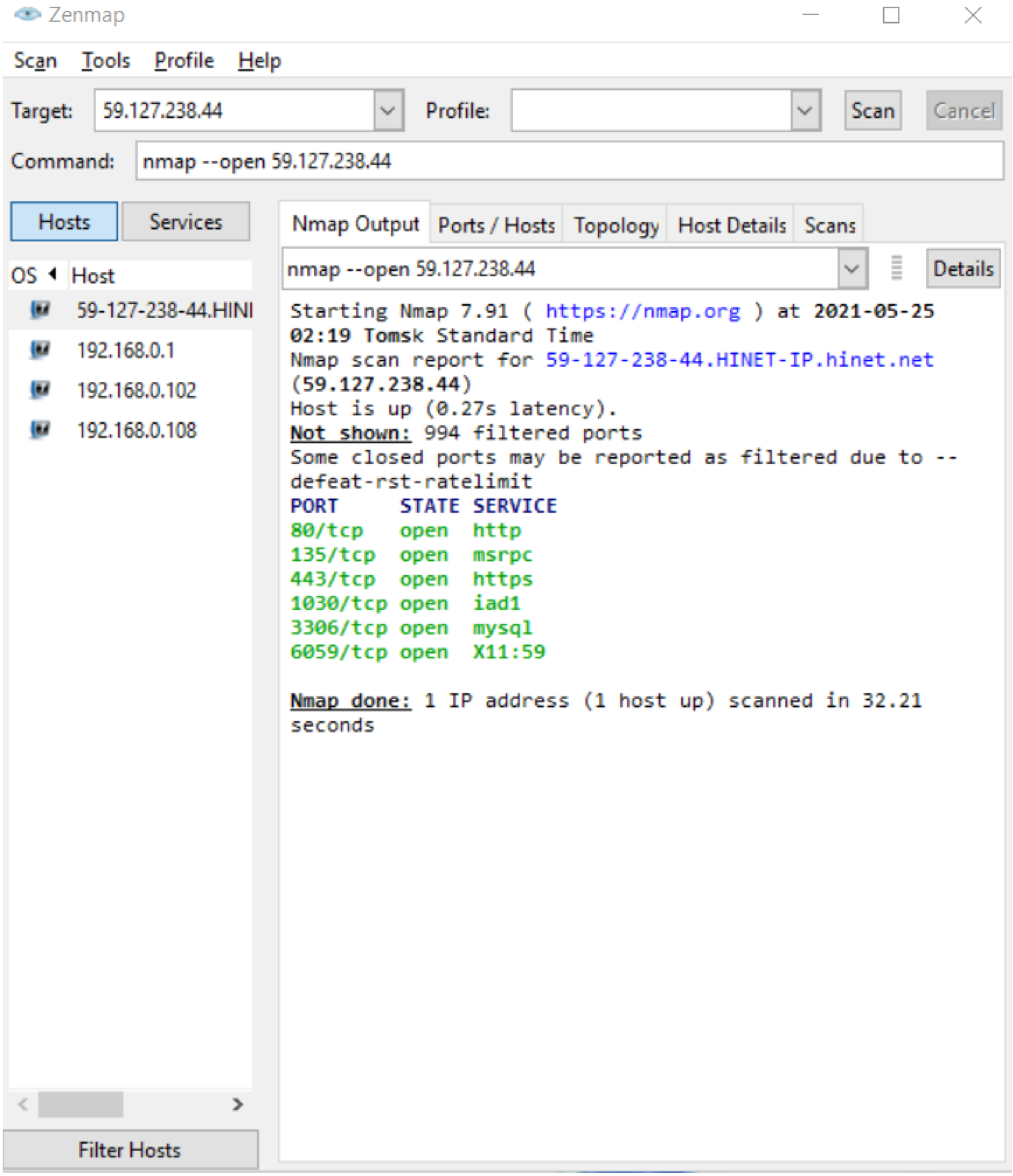
Figure 12: Scanned my network using half-open connection.

Task 9: Select the target host from the commands offered for research (Appendix B).

Result: Chosen target host: 59.127.238.44

Task 10: Scan the target host's open ports:

Result: Following figure below shows the open ports of target host - 59.127.238.44



```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-25
02:19 Tomsk Standard Time
Nmap scan report for 59-127-238-44.HINET-IP.hinet.net
(59.127.238.44)
Host is up (0.27s latency).
Not shown: 994 filtered ports
Some closed ports may be reported as filtered due to --
defeat-rst-ratelimit
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
443/tcp   open  https
1030/tcp  open  iad1
3306/tcp  open  mysql
6059/tcp  open  X11:59

Nmap done: 1 IP address (1 host up) scanned in 32.21
seconds
```

Figure 13: Scanned the target host’s open ports.

Task 10.1: What ports were discovered and what services / services are they responsible for?

Result:

Service Name	Port Number
http	80
msrpc	135
https	443
iad1	1030
mysql	3306
X11:59	6059

Task 10.2: Use the literature or the Internet and determine which services / services from the detected vulnerabilities?

Result:

Service Name: http

Port 80 is used by the HyperText Transport Protocol (HTTP). HTTP is the protocol websites and web browsers use to communicate with each other. Port 80 is a frequent target for attacks.

Vulnerabilities of port HTTP:

Privacy issues:

- Personal information about clients can be revealed in HTTP server logs.
- Servers that reveal their software and version information allow attackers to target specific servers with known vulnerabilities.
- Private data submitted by clients in an HTTP GET method will be exposed in client browser history logs, proxy logs, and server logs. The HTTP POST method is preferred over HTTP GET.

Attacks on the server filesystem:

- Attackers have modified HTTP requests for files by using “..” in paths. On Windows and Unix machines “..” refers to the parent directory. Attackers would create requests like www.victim.com/../../../etc/shadow/ to trick the server into revealing a security relevant file. Current servers protect against this by filtering out “..” from requests and by running the server as a process without permissions to read most system files.
- Another attack is to send a request to the browser for one of its configuration files. This gives an attacker more information about the server to conduct an attack against it.

SQL Piggybacking:

- An attacker embeds SQL commands in input fields requested by a server. The server uses the input fields to build database queries. If the server does not validate the attacker's input, the attacker's SQL commands will be embedded in the queries the server builds to send to the database. This may cause the database to reveal information unintentionally or to perform some action.

Attacking state maintenance:

- In many cases clients are responsible for maintaining state information of an HTTP session. This is done through cookies, URL fields, or hidden form elements that are exchanged between client and server during an HTTP session.
- The client is able to manipulate these states and possibly cause the server to operate incorrectly.
- Example: If a server supports multiple clients and tracks their sessions using a userid stored in a cookie. The client may be able to change the userid to that of another user and get information for the other user's session.
- A hypothetical online merchant lets clients select items in an electronic shopping cart. The merchant's web application tracks what is already in the shopping cart by storing the items and their prices in a cookie that is exchanged between the client and the server. A client that manipulates an item's price in the cookie could trick the server into giving the client a discount.

Service Name: msrpc

Microsoft''s "DCOM (Distributed Component Object Model) Service Control Manager " running on the user''s computer utilizes the port 135. Port 135 exposes where DCOM services can be found on a machine. Hacker tools such as "epdump" (Endpoint Dump) can immediately identify every DCOM-related server/service running on the user's hosting computer and match them up with known exploits against those services. Therefore, port 135 should not be exposed to the internet and must be blocked.

Service Name: mysql

In general, port 3306 shouldn’t be opened since it could make the server vulnerable to attack. If the user needs to connect to the database remotely, there are many other secure options, instead of opening the port 3306.

One of the secure options includes using an SSH tunnel. On the other hand, if it is required to open port 3306, the user has to ensure to restrict the IP addresses which can access it so that the connection can’t be accessed by untrusted hosts. Even though MySQL's default port is 3306, it doesn’t necessarily mean that MySQL service will always use that port.

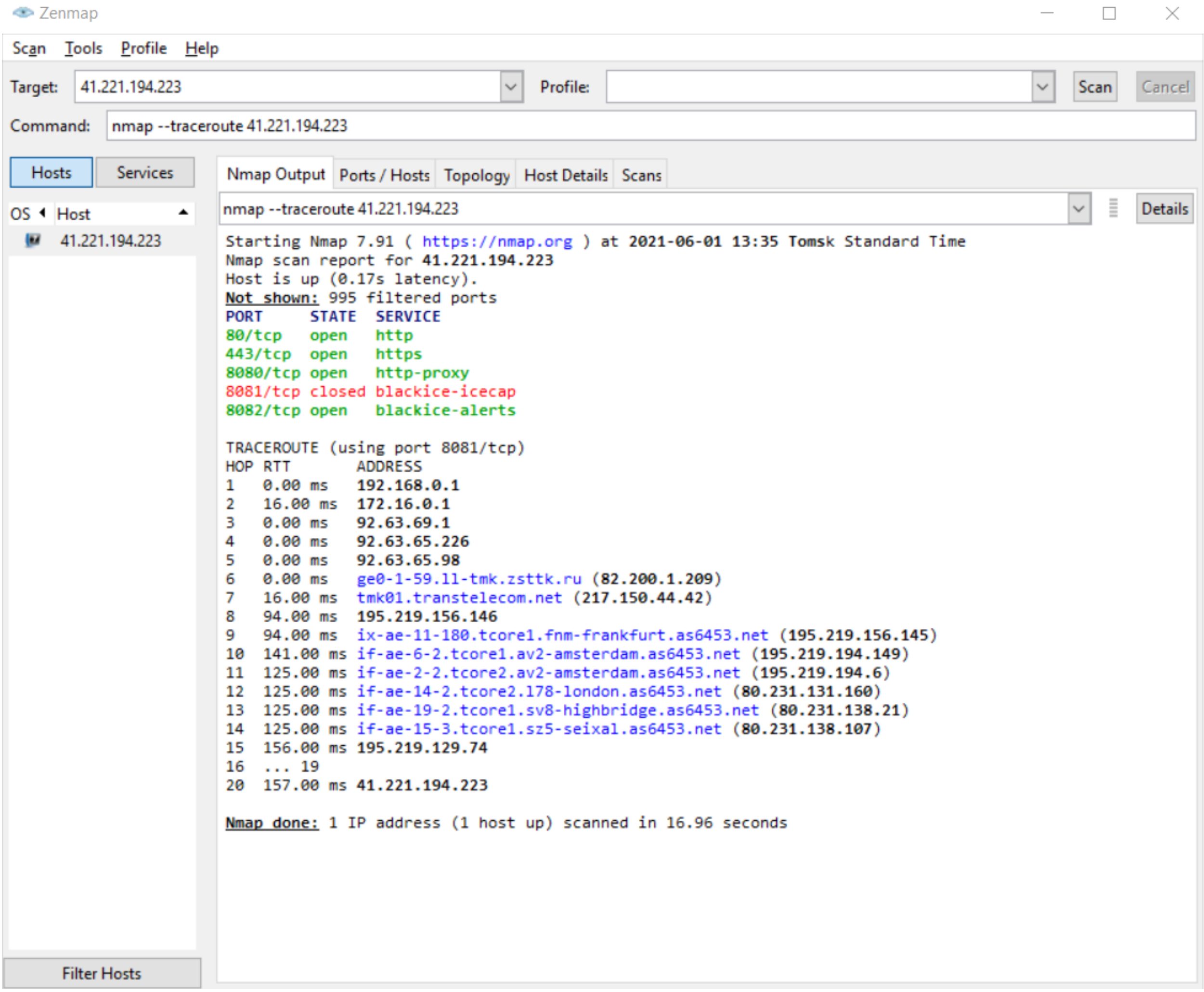
If the user wants to verify the port or see if MySQL is using a different port, it can be done by running a short SQL query.

```
SHOW VARIABLES WHERE Variable_name = 'port';
```

Task 10.3: Track the path to the target host.

Result: Traceroute is a network diagnostic tool used to track in real-time the pathway taken by a packet on an IP network from source to destination, reporting the IP addresses of all the routers it pinged in between. Traceroute also records the time taken for each hop the packet makes during its route to the destination.

Traceroute most commonly uses Internet Control Message Protocol (ICMP) echo packets with variable time to live (TTL) values. The response time of each hop is calculated. To guarantee accuracy, each hop is queried multiple times (usually three times) to better measure the response of that particular hop. Traceroute uses ICMP messages and TTL fields in the IP address header to function. Traceroute tools are typically included as a utility by operating systems such as Windows and Unix. Traceroute utilities based on TCP are also available.



Target: 41.221.194.223

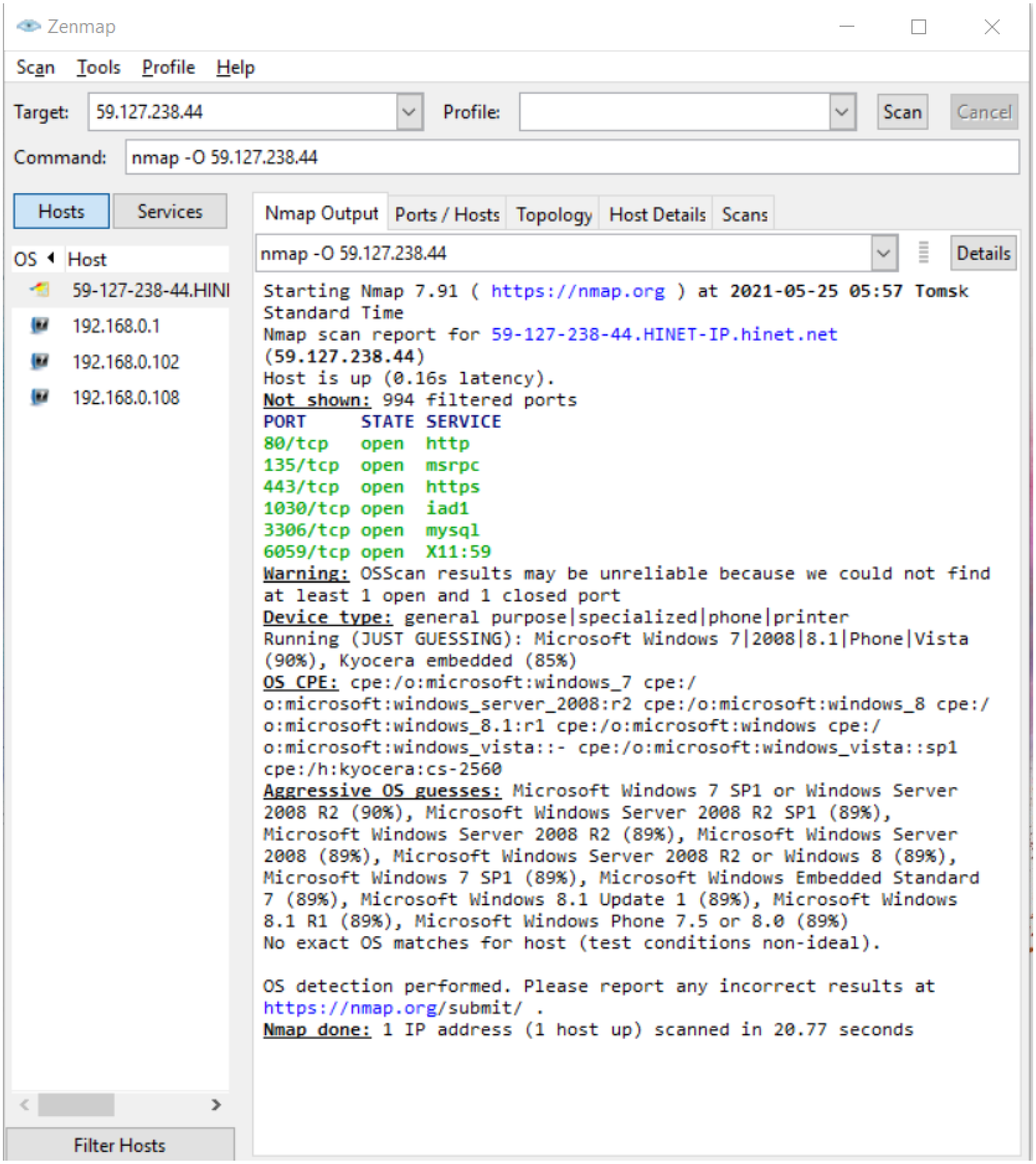
Command: nmap --traceroute 41.221.194.223

```
nmap --traceroute 41.221.194.223

Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-01 13:35 Tomsk Standard Time
Nmap scan report for 41.221.194.223
Host is up (0.17s latency).
Not shown: 995 filtered ports
PORT     STATE  SERVICE
80/tcp   open   http
443/tcp  open   https
8080/tcp open   http-proxy
8081/tcp closed blackice-icecap
8082/tcp open   blackice-alerts

TRACEROUTE (using port 8081/tcp)
HOP RTT       ADDRESS
1   0.00 ms   192.168.0.1
2   16.00 ms  172.16.0.1
3   0.00 ms   92.63.69.1
4   0.00 ms   92.63.65.226
5   0.00 ms   92.63.65.98
6   0.00 ms   ge0-1-59.11-tmk.zsttk.ru (82.200.1.209)
7   16.00 ms  tmk01.transtelecom.net (217.150.44.42)
8   94.00 ms  195.219.156.146
9   94.00 ms  ix-ae-11-180.tcore1.fnm-frankfurt.as6453.net (195.219.156.145)
10  141.00 ms if-ae-6-2.tcore1.av2-amsterdam.as6453.net (195.219.194.149)
11  125.00 ms if-ae-2-2.tcore2.av2-amsterdam.as6453.net (195.219.194.6)
12  125.00 ms if-ae-14-2.tcore2.178-london.as6453.net (80.231.131.160)
13  125.00 ms if-ae-19-2.tcore1.sv8-highbridge.as6453.net (80.231.138.21)
14  125.00 ms if-ae-15-3.tcore1.sz5-seixal.as6453.net (80.231.138.107)
15  156.00 ms 195.219.129.74
16  ... 19
20  157.00 ms 41.221.194.223

Nmap done: 1 IP address (1 host up) scanned in 16.96 seconds
```

Figure 14: Since, the target host-59.127.238.44 seems down, so I have traced the host, 41.221.194.223

Task 10.4: Determine the operating system of the target host. If resisted, enter the appropriate value with 50 attempts. Comment on the result.

Result: The figure below shows the OS of the target host.

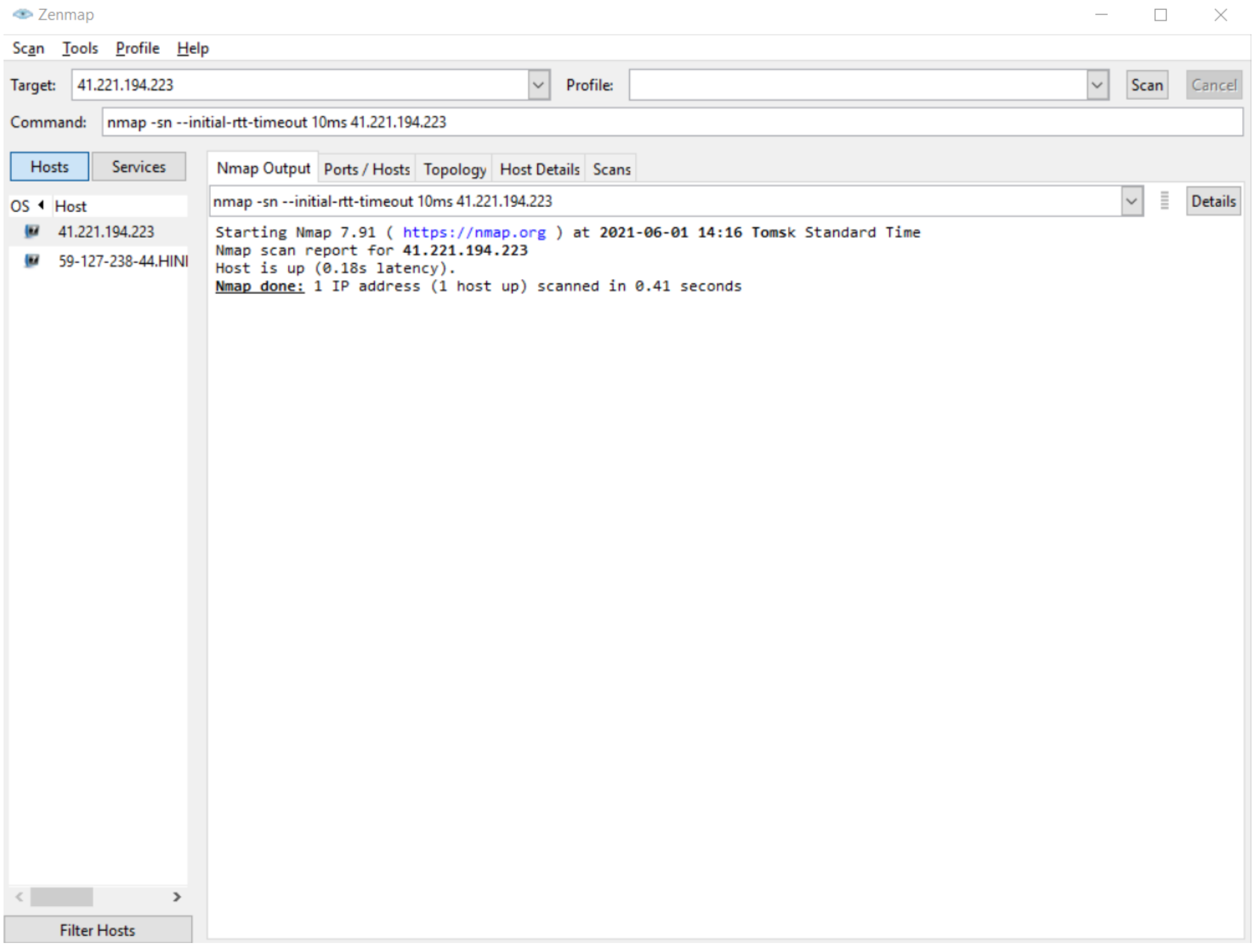


```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-25 05:57 Tomsk
Standard Time
Nmap scan report for 59-127-238-44.HINET-IP.hinet.net
(59.127.238.44)
Host is up (0.16s latency).
Not shown: 994 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
443/tcp   open  https
1030/tcp open  iad1
3306/tcp open  mysql
6059/tcp open  X11:59
Warning: OSScan results may be unreliable because we could not find
at least 1 open and 1 closed port
Device type: general purpose|specialized|phone|printer
Running (JUST GUESSING): Microsoft Windows 7|2008|8.1|Phone|Vista
(90%), Kyocera embedded (85%)
OS CPE: cpe:/o:microsoft:windows_7 cpe:/
o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8 cpe:/
o:microsoft:windows_8.1:r1 cpe:/o:microsoft:windows cpe:/
o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1
cpe:/h:kyocera:cs-2560
Aggressive OS guesses: Microsoft Windows 7 SP1 or Windows Server
2008 R2 (90%), Microsoft Windows Server 2008 R2 SP1 (89%),
Microsoft Windows Server 2008 R2 (89%), Microsoft Windows Server
2008 (89%), Microsoft Windows Server 2008 R2 or Windows 8 (89%),
Microsoft Windows 7 SP1 (89%), Microsoft Windows Embedded Standard
7 (89%), Microsoft Windows 8.1 Update 1 (89%), Microsoft Windows
8.1 R1 (89%), Microsoft Windows Phone 7.5 or 8.0 (89%)
No exact OS matches for host (test conditions non-ideal).

OS 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
```

Figure 15: Operating System of target host - 59.127.238.44

5. Ping to the target computer, adjusting the request response timeout.

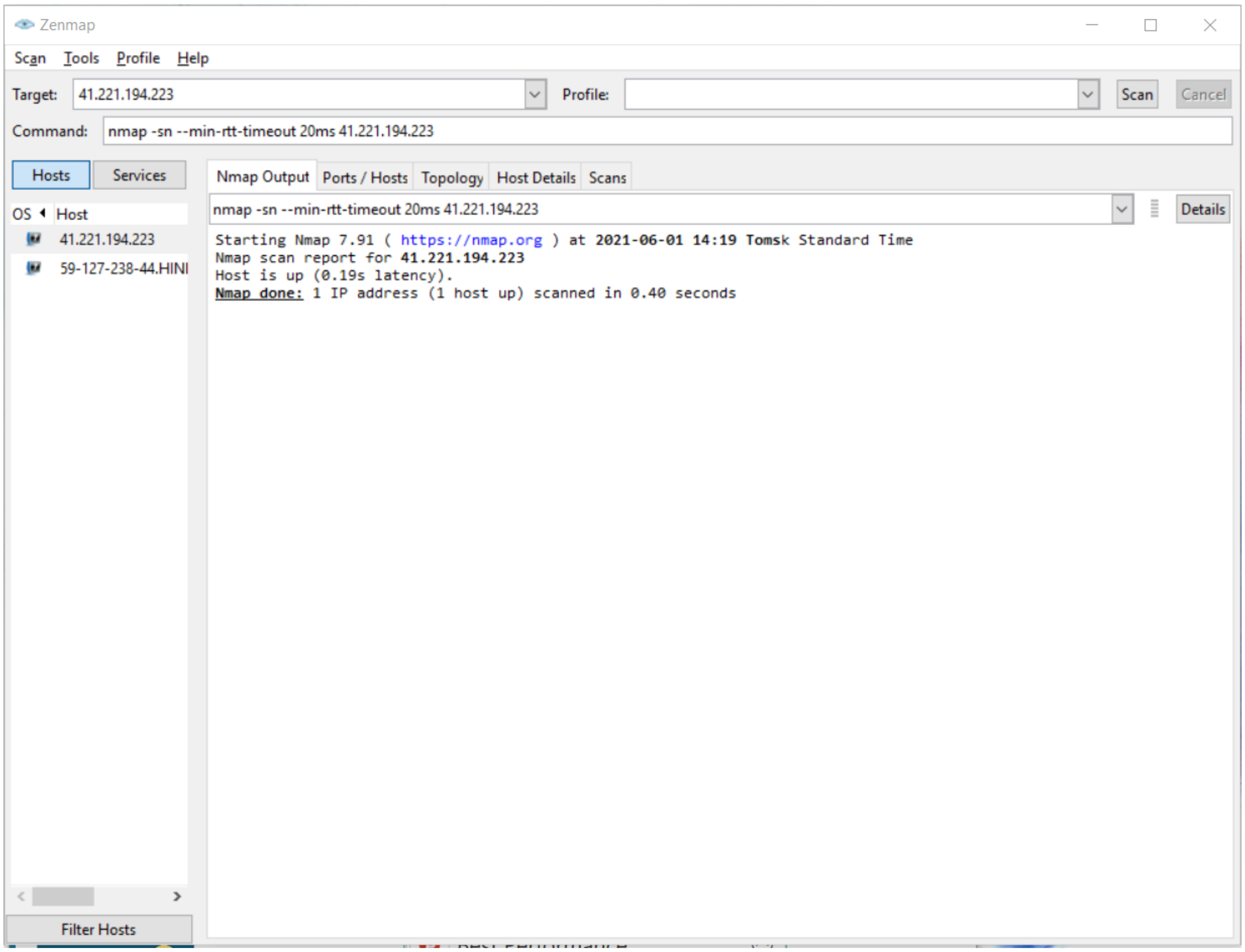
Result:



Command: nmap -sn --initial-rtt-timeout 10ms 41.221.194.223

```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-01 14:16 Tomsk Standard Time
Nmap scan report for 41.221.194.223
Host is up (0.18s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.41 seconds
```

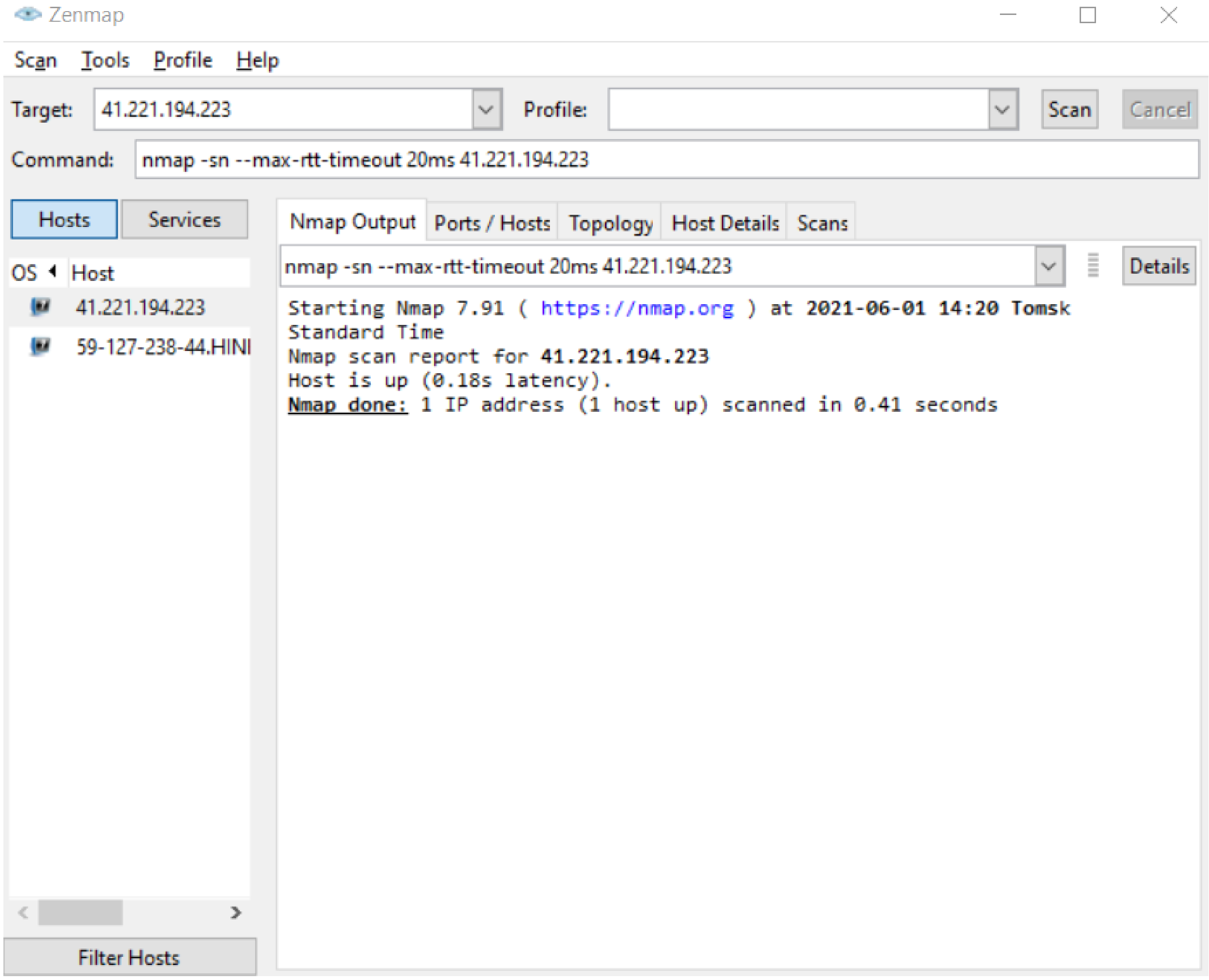
Figure 16: Ping to target computer- 41.221.194.223 and adjusted the request response timeout by using initial-rtt-timeout <time>



Command: nmap -sn --min-rtt-timeout 20ms 41.221.194.223

```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-01 14:19 Tomsk Standard Time
Nmap scan report for 41.221.194.223
Host is up (0.19s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.40 seconds
```

Figure 17: Ping to target computer- 41.221.194.223 and adjusted the request response timeout by using min-rtt-timeout <time>



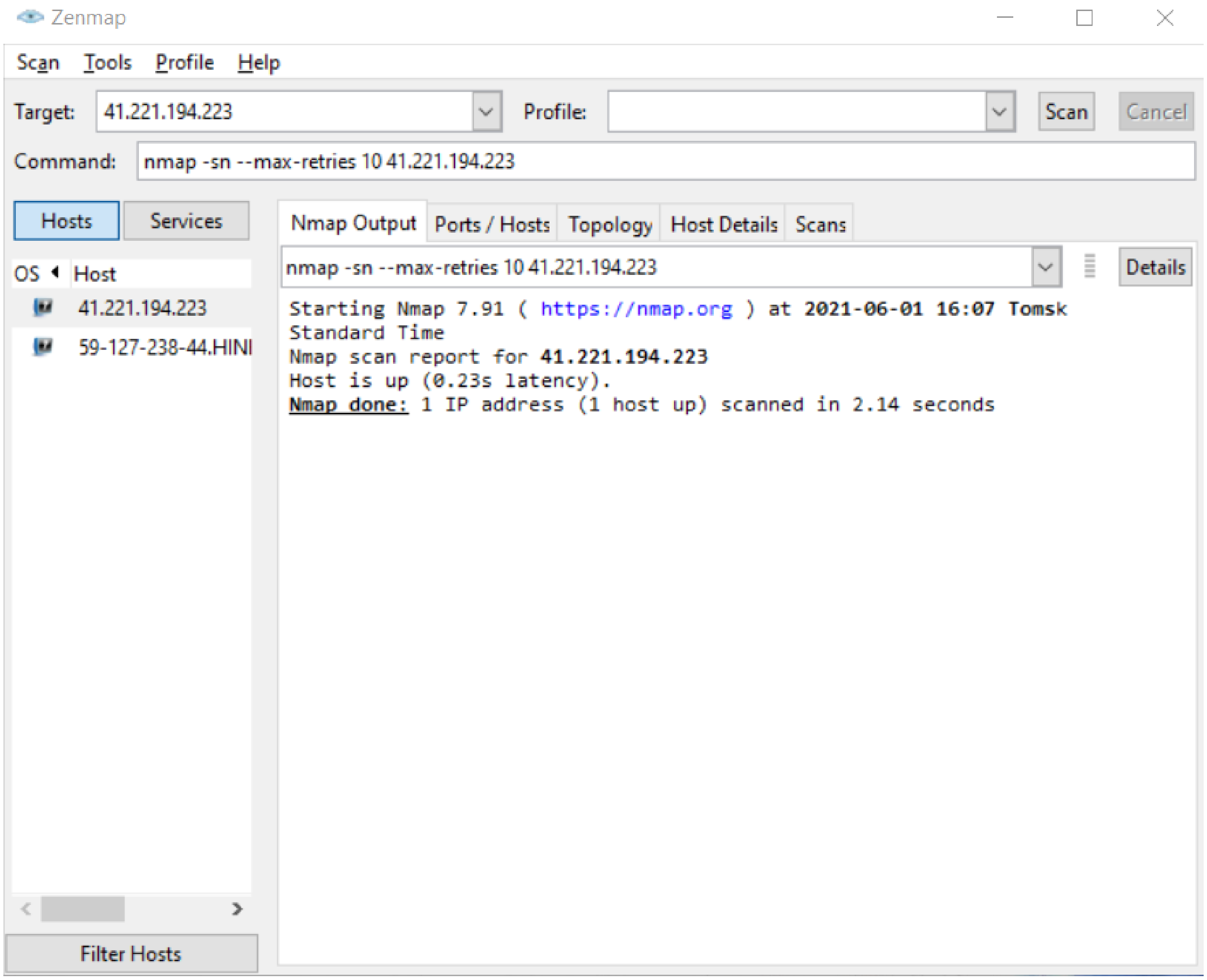
Command: nmap -sn --max-rtt-timeout 20ms 41.221.194.223

```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-01 14:20 Tomsk
Standard Time
Nmap scan report for 41.221.194.223
Host is up (0.18s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.41 seconds
```

Figure 18: Ping to target computer- 41.221.194.223 and adjusted the request response timeout by using max-rtt-timeout <time>

Task 10.6. Ping the target computer and set the maximum number of request retransmissions.

Result:



Target: 41.221.194.223

Command: nmap -sn --max-retries 10 41.221.194.223

41.221.194.223
59-127-238-44.HINI

```
nmap -sn --max-retries 10 41.221.194.223
```

```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-01 16:07 Tomsk
Standard Time
Nmap scan report for 41.221.194.223
Host is up (0.23s latency).
Nmap done: 1 IP address (1 host up) scanned in 2.14 seconds
```

Figure 19: Ping to target computer- 41.221.194.223 and set the maximum number of request retransmissions.

Task 10.7: Implement a time control option when scanning the target host. Adjust the delay between requests. Comment on the result.

Result: Nmap timing has built with this ability to scan the target set faster or slower scanning speed than the normal or default speed. There are a number of different settings that can be selected based on timing templates. Timing template in the nmap is defined by –T<0-5> having -T0 as the slowest and –T5 as the fastest. By default, all nmap scans run on –T3 timing template. Timing template in Nmap is used to optimize and improve the quality and performance of the scan to get desired results.So Nmap offers a simpler approach, with six timing templates. You can specify them with the -T option and their number (0–5) or their name. The template names are paranoid (0), sneaky (1), polite (2), normal (3), aggressive (4), and insane (5).

-T0 Paranoid

This Type of scan is used for slower network scan than the normal speed in these situations, and detection risks must be minimized. This is a serial scan that will pause for 5 minutes; however, the *max_delay* setting of second is ignored, and *scan_delay* is set to a higher value than the normal value.

–T1 **sneaky**

The ***–T1 or –timing sneaky*** scan is a little bit faster than the paranoid (-T0) scan, it happens by reducing the scan time needed. This scan uses serial process to find the open port of target

-T2 Polite

The ***T2 or -timing polite*** scan is a build in velocity again over the T0 what's more T1 scan and is the last scanning template to utilize the serial scanning method. The *scan_delay* for this scan is situated at 400 milliseconds, making this the first template to make utilization of the *max_scan* delay, a value that is still set to the default estimation of 1 second. With this format chosen Nmap will start checking targets utilizing the scan_delay of 400 milliseconds yet has the capability to dynamically alter the postponement up to a most extreme of 1 second. By analyzing the time needed to finish the respectful sweep of the same 100 ports, general examining time has been decreased to only 544 seconds or only 9 minutes.

T3 Normal

The ***T3 or -timing normal*** scan is the default check for Nmap, implying that on the off chance that no timing layout or manual timing choices are set, the settings in this template will be utilized for the scan. This template is the first to utilize the parallel handling method, sending different probes out all the while, expanding the general speed. This output has a *scan_delay* of 0 seconds that can develop to a *max_scan_delay* that can develop to 1 second, meaning the output will happen as fast as would be prudent yet following 1 second the current port scan will be complete and the following port will be filtered. The normal scan will finish the scan of chosen ports on the target machine in 547 seconds, really slower than the amiable output for this situation, however this is not ordinarily the case.

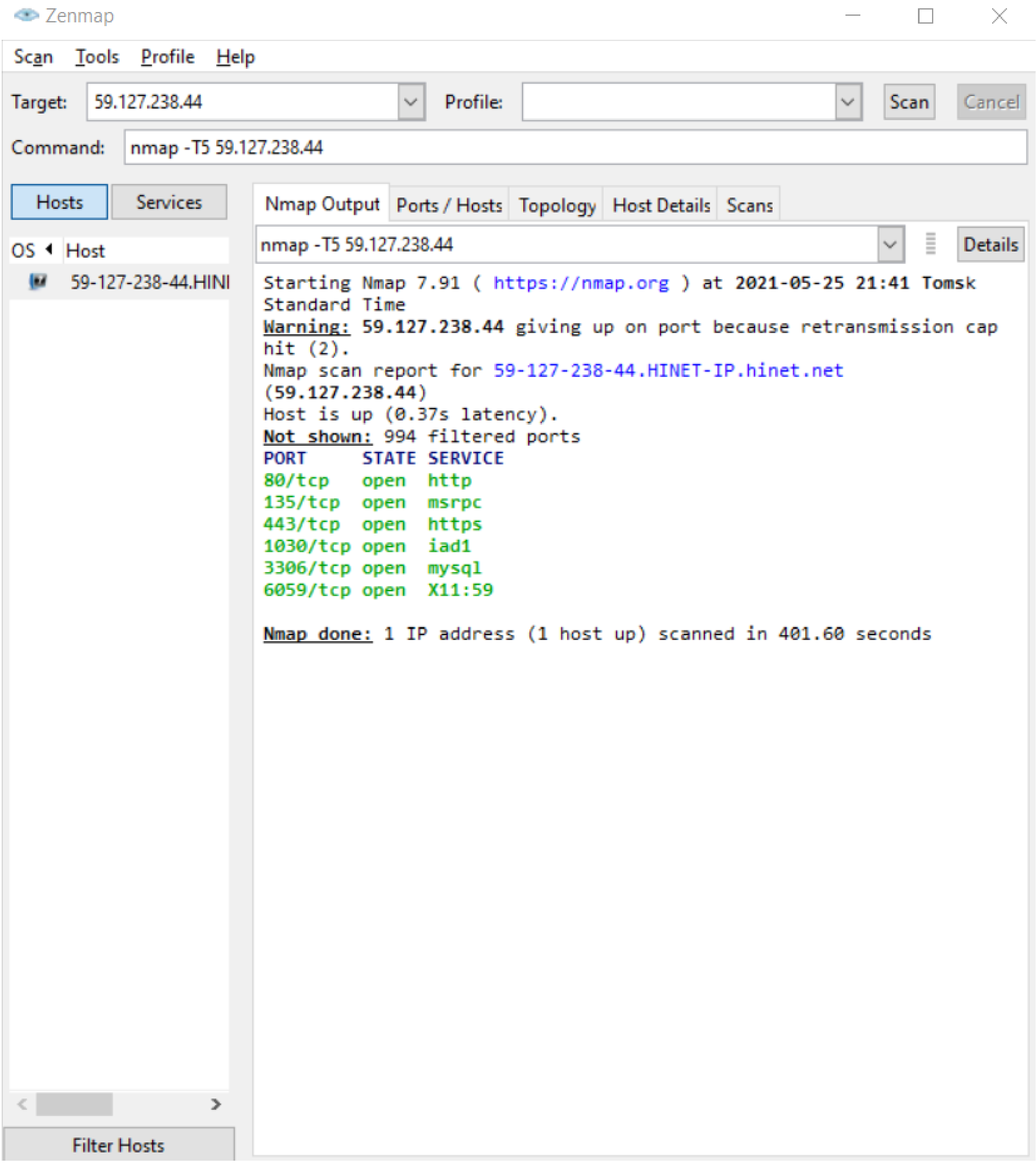
T4 Aggressive

The ***T4 or -timing aggressive*** layout additionally runs its filtering in parallel expanding speed. The *scan_delay* for this template is situated at 0 seconds and can develop to a *max_scan_delay* of 10 milliseconds. Scan with a *max_scan_delay* of short of what 1 second is inclined to slips as some target Operating Systems have settings that oblige a base postpone between test reactions of 1 second. This scan finished the port scan of the metasploit virtual machine in only 477 seconds or simply under 8 minutes.

-T5 **Insane**

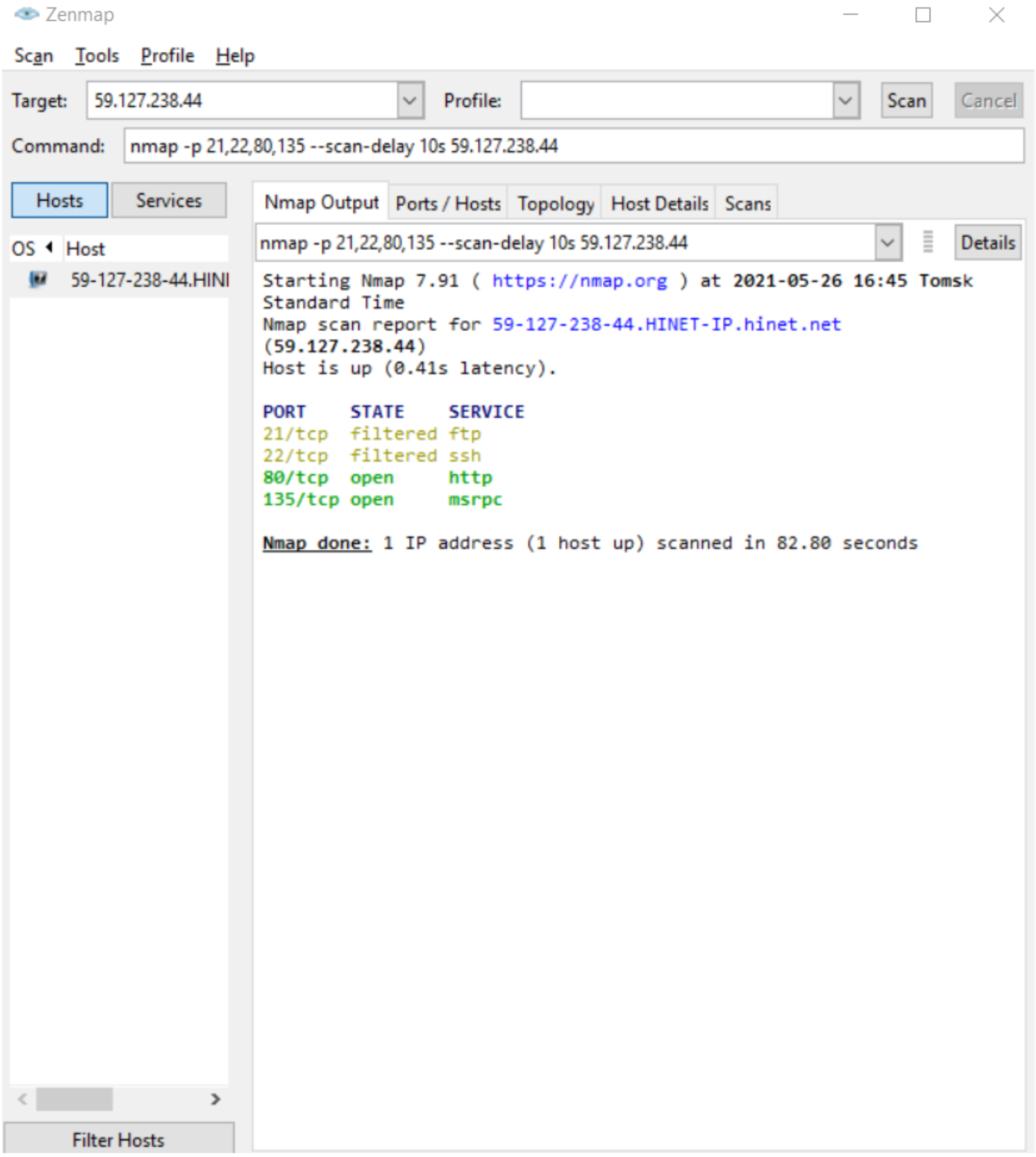
The ***T5 or -timing insane*** timing format is the quickest of the inherent timing template. This template utilizes the parallel scanning strategy with a *scan_delay* of 0 seconds and a *max_scan_delay* of 5 milliseconds. As expressed with the aggressive scan, this scan can result in mistakes focused around target machine Operating System and settings. This scan, the quickest, finished in simply under 22 seconds; be that as it may, the results are a considerable amount not quite the same as the majority of the scan to this point

You can slow down or speed up scans by specifying the amount of time that Nmap will wait between probes. Scans are often slowed down in order to avoid detection. You need to specify the number of seconds Nmap will wait between each probe it sends to a given host. The flag used is **--scan-delay**.



```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-25 21:41 Tomsk
Standard Time
Warning: 59.127.238.44 giving up on port because retransmission cap
hit (2).
Nmap scan report for 59-127-238-44.HINET-IP.hinet.net
(59.127.238.44)
Host is up (0.37s latency).
Not shown: 994 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
443/tcp  open  https
1030/tcp open  iad1
3306/tcp open  mysql
6059/tcp open  X11:59

Nmap done: 1 IP address (1 host up) scanned in 401.60 seconds
```

Figure 20: Shows the results for -T5 timing template

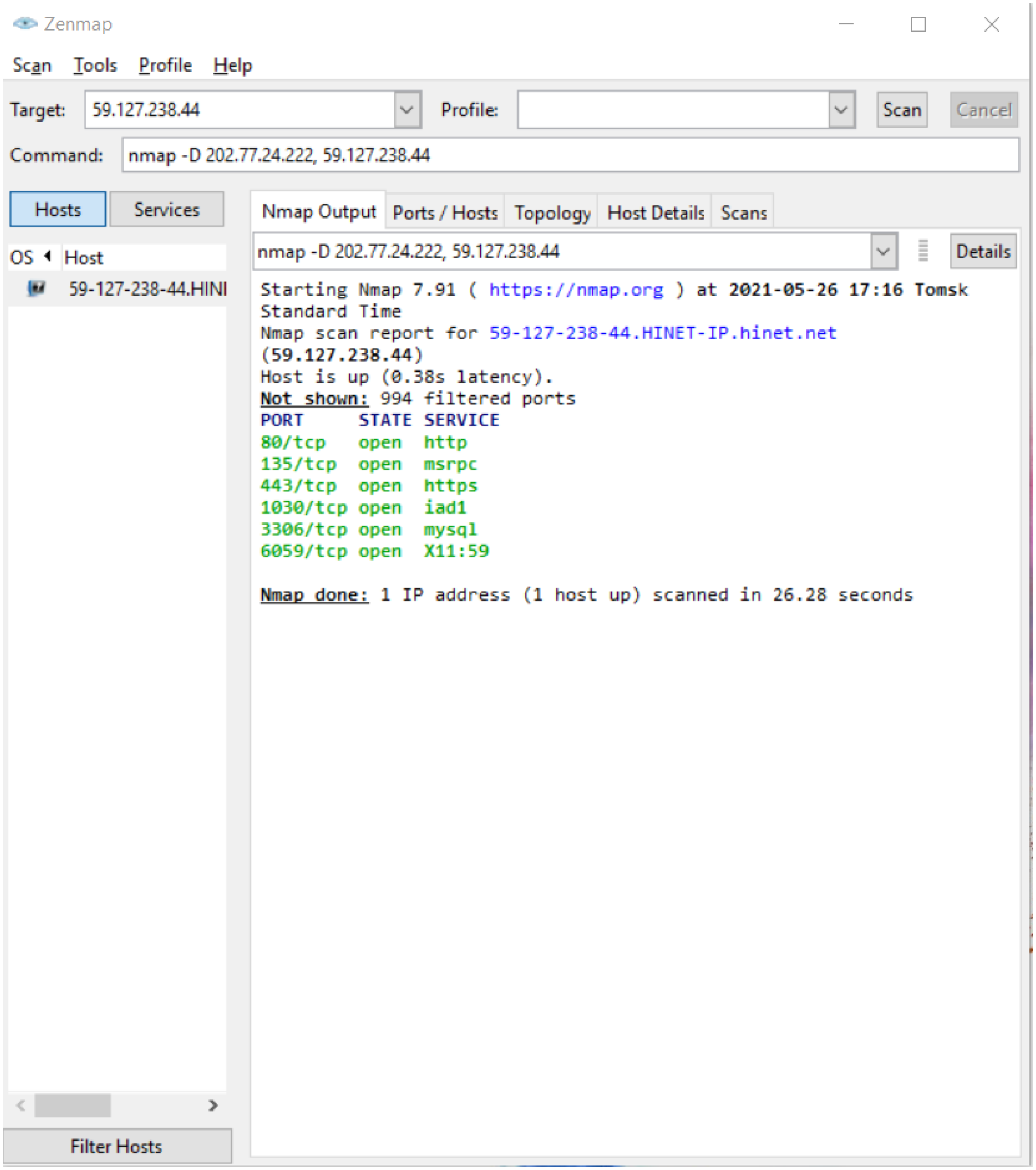


```
nmap -p 21,22,80,135 --scan-delay 10s 59.127.238.44
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-26 16:45 Tomsk
Standard Time
Nmap scan report for 59-127-238-44.HINET-IP.hinet.net
(59.127.238.44)
Host is up (0.41s latency).

PORT    STATE    SERVICE
21/tcp  filtered ftp
22/tcp  filtered ssh
80/tcp  open     http
135/tcp open     msrpc

Nmap done: 1 IP address (1 host up) scanned in 82.80 seconds
```

Figure 21: Adjusting the delay between requests. As you can see from the output above, we've scanned 4 ports on the target host, with the 10 seconds wait time between requests. Note that this has slowed down the scan considerably (the scanning process for only 4 ports took 82.80 seconds).

Task 10.8: Perform a disguise scan of the target host using bogus hosts. Select any of the provided hosts in Appendix B.

Result:



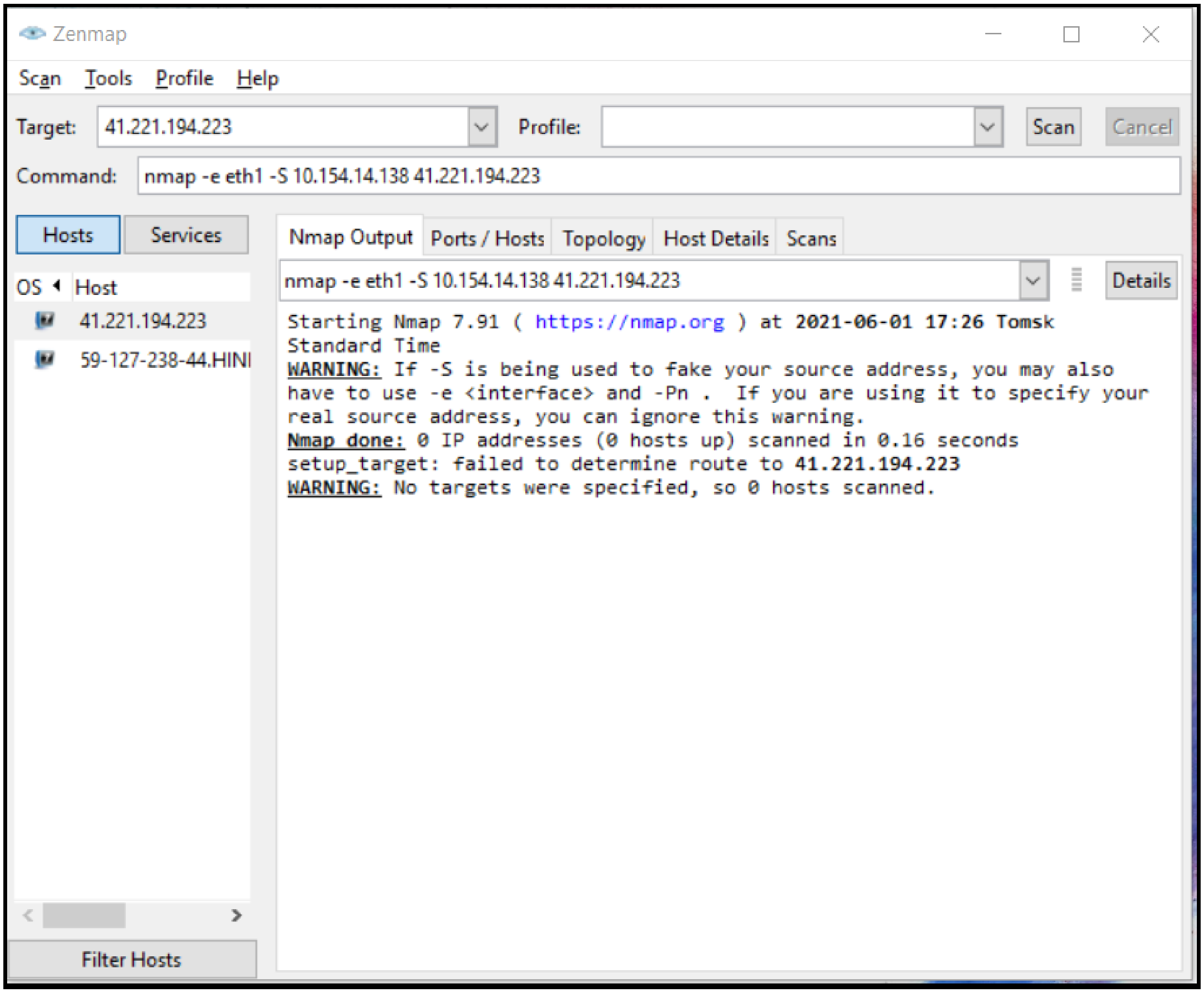
Target: 59.127.238.44

Command: nmap -D 202.77.24.222, 59.127.238.44

```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-26 17:16 Tomsk
Standard Time
Nmap scan report for 59-127-238-44.HINET-IP.hinet.net
(59.127.238.44)
Host is up (0.38s latency).
Not shown: 994 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
443/tcp  open  https
1030/tcp open  iad1
3306/tcp open  mysql
6059/tcp open  X11:59

Nmap done: 1 IP address (1 host up) scanned in 26.28 seconds
```

Task 10.9: Scan the target host with spoofing the original address.

Result:



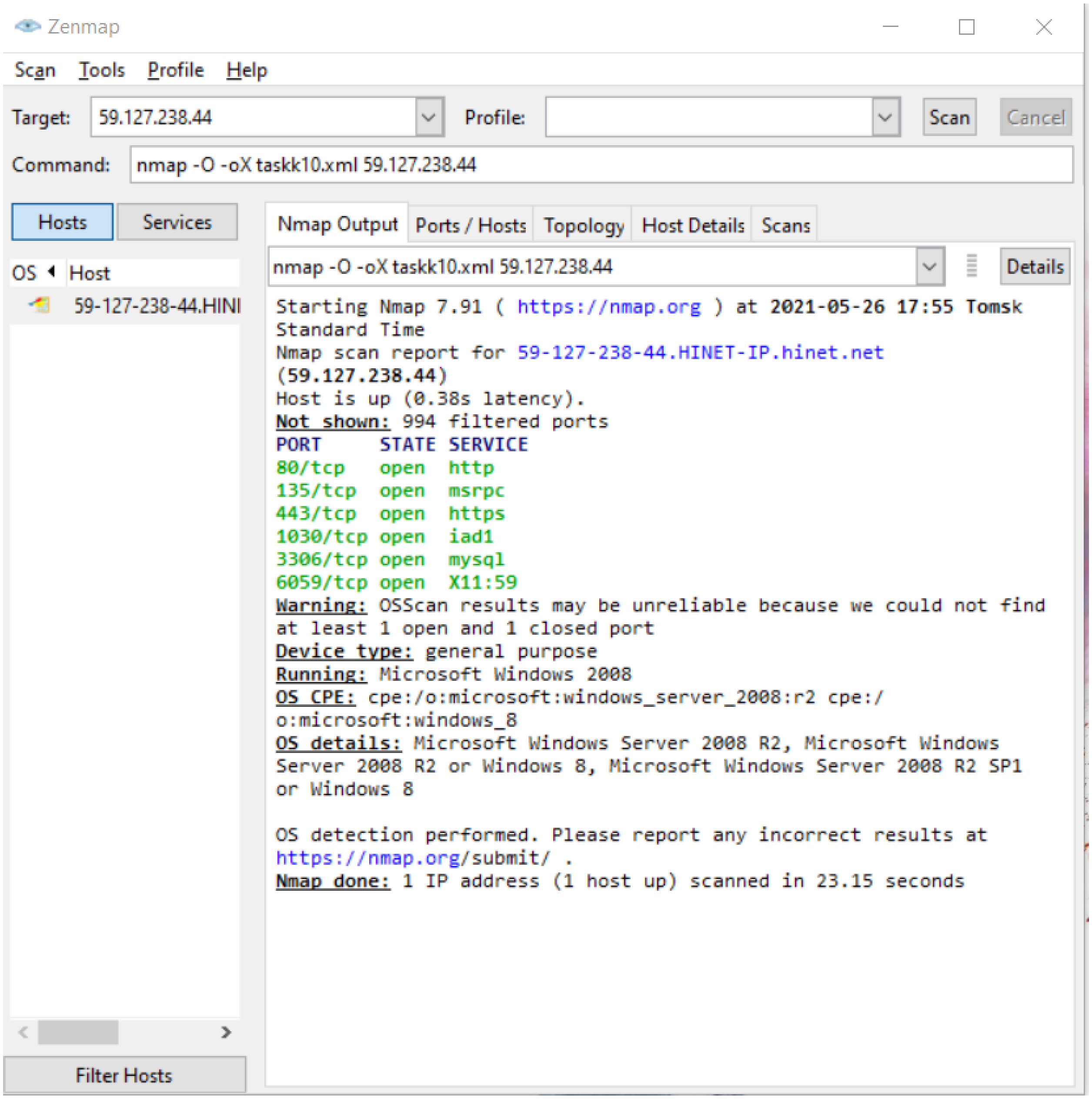
Command: nmap -e eth1 -S 10.154.14.138 41.221.194.223

```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-01 17:26 Tomsk
Standard Time
WARNING: If -S is being used to fake your source address, you may also
have to use -e <interface> and -Pn .  If you are using it to specify your
real source address, you can ignore this warning.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.16 seconds
setup_target: failed to determine route to 41.221.194.223
WARNING: No targets were specified, so 0 hosts scanned.
```

Figure 23: Tried scanning the target host- 41.221.194.223 by spoofing the original address but couldn’t succeed.

Task 10.10: Output the scan results at any of the steps (3-9) in XML format.

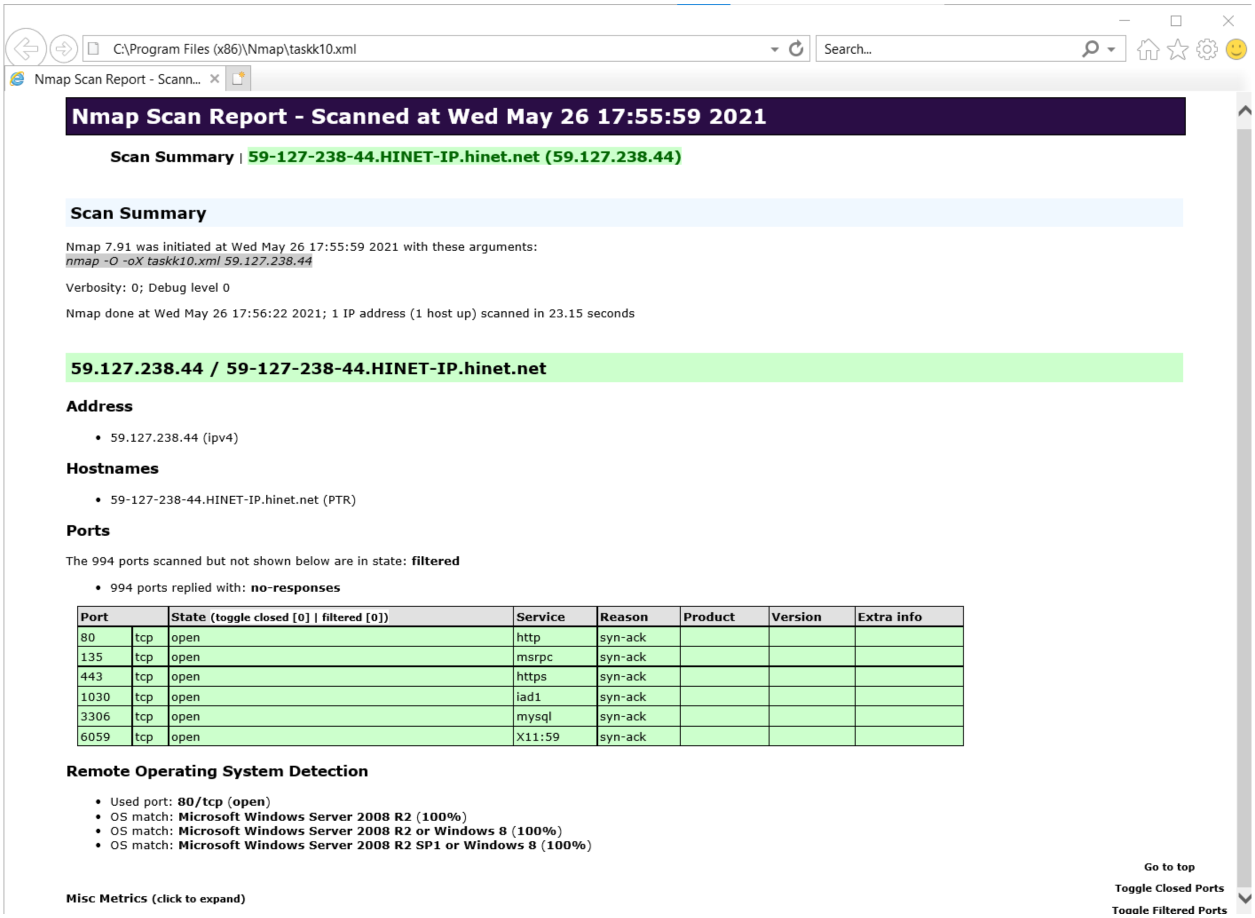
Result: I have repeated the task 10.3 of finding the operating system and output the scan results in XML formal.



```
nmap -O -oX taskk10.xml 59.127.238.44
```

```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-26 17:55 Tomsk
Standard Time
Nmap scan report for 59-127-238-44.HINET-IP.hinet.net
(59.127.238.44)
Host is up (0.38s latency).
Not shown: 994 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
443/tcp  open  https
1030/tcp open  iad1
3306/tcp open  mysql
6059/tcp open  X11:59
Warning: OSScan results may be unreliable because we could not find
at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows 2008
OS CPE: cpe:/o:microsoft:windows_server_2008:r2 cpe:/
o:microsoft:windows_8
OS details: Microsoft Windows Server 2008 R2, Microsoft Windows
Server 2008 R2 or Windows 8, Microsoft Windows Server 2008 R2 SP1
or Windows 8

OS detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.15 seconds
```

Figure 24: Shows the command for saving the scan results to file task10.xml


C:\Program Files (x86)\Nmap\taskk10.xml
Search...
Nmap Scan Report - Scann...

Nmap Scan Report - Scanned at Wed May 26 17:55:59 2021

Scan Summary | **59-127-238-44.HINET-IP.hinet.net (59.127.238.44)**

Scan Summary

Nmap 7.91 was initiated at Wed May 26 17:55:59 2021 with these arguments:
nmap -O -oX taskk10.xml 59.127.238.44

Verbosity: 0; Debug level 0

Nmap done at Wed May 26 17:56:22 2021; 1 IP address (1 host up) scanned in 23.15 seconds

59.127.238.44 / 59-127-238-44.HINET-IP.hinet.net

Address

- 59.127.238.44 (ipv4)

Hostnames

- 59-127-238-44.HINET-IP.hinet.net (PTR)

Ports

The 994 ports scanned but not shown below are in state: **filtered**

- 994 ports replied with: **no-responses**

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
80	tcp	open	http	syn-ack			
135	tcp	open	msrpc	syn-ack			
443	tcp	open	https	syn-ack			
1030	tcp	open	iad1	syn-ack			
3306	tcp	open	mysql	syn-ack			
6059	tcp	open	X11:59	syn-ack			

Remote Operating System Detection

- Used port: **80/tcp** (**open**)
- OS match: **Microsoft Windows Server 2008 R2** (**100%**)
- OS match: **Microsoft Windows Server 2008 R2 or Windows 8** (**100%**)
- OS match: **Microsoft Windows Server 2008 R2 SP1 or Windows 8** (**100%**)

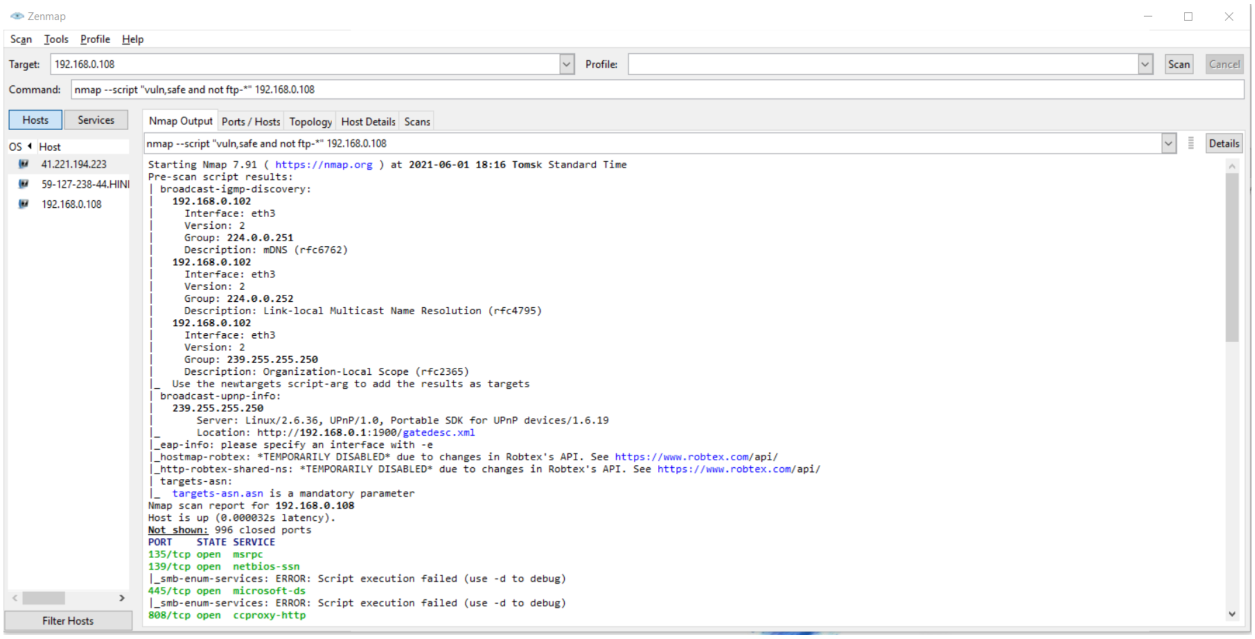
Go to top
Toggle Closed Ports
Toggle Filtered Ports

Misc Metrics (click to expand)

Figure 25: Shows the scan results saved in taskk10.xml in XML format

Task 10: With the help of the NSE engine, implement a script that combines 2-3 tasks that you have already done earlier and display the incoming and outgoing connections.

Result:



Target: 192.168.0.108

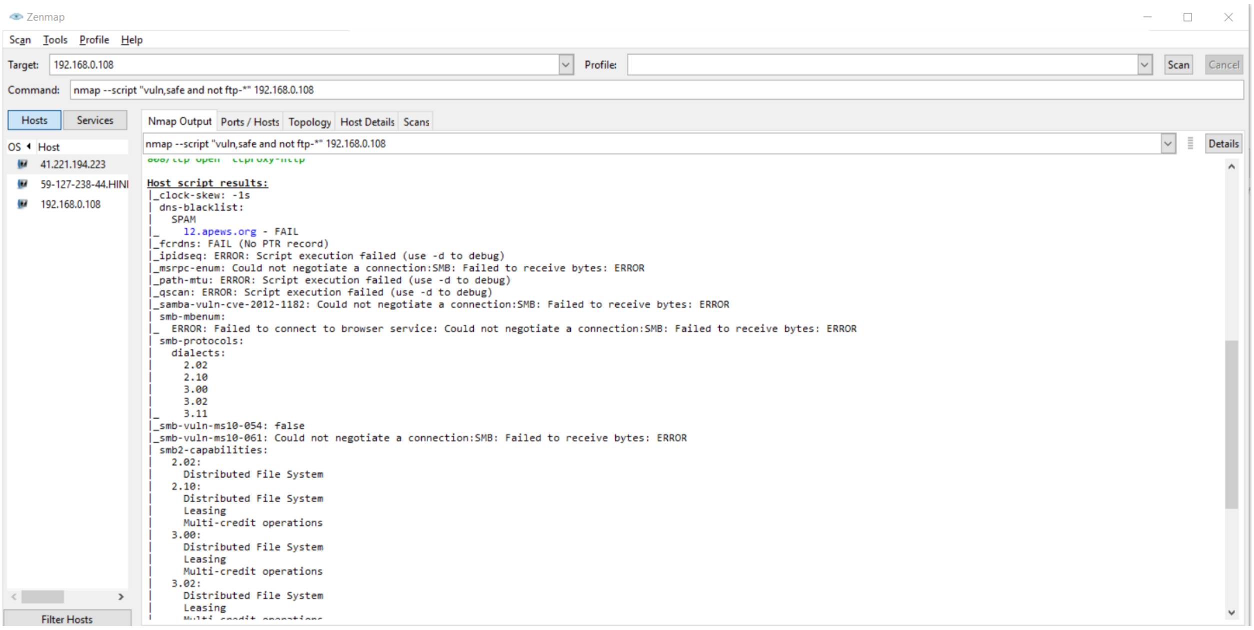
Profile:

Command: nmap --script "vuln,safe and not ftp-*" 192.168.0.108

OS Host
41.221.194.223
59-127-238-44.HINI
192.168.0.108

nmap --script "vuln,safe and not ftp-*" 192.168.0.108

```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-01 18:16 Tomsk Standard Time
Pre-scan script results:
| broadcast-igmp-discovery:
|   192.168.0.102
|     Interface: eth3
|     Version: 2
|     Group: 224.0.0.251
|     Description: mDNS (rfc6762)
|   192.168.0.102
|     Interface: eth3
|     Version: 2
|     Group: 224.0.0.252
|     Description: Link-local Multicast Name Resolution (rfc4795)
|   192.168.0.102
|     Interface: eth3
|     Version: 2
|     Group: 239.255.255.250
|     Description: Organization-Local Scope (rfc2365)
|_  Use the newtargets script-arg to add the results as targets
| broadcast-upnp-info:
|   239.255.255.250
|       Server: Linux/2.6.36, UPnP/1.0, Portable SDK for UPnP devices/1.6.19
|_      Location: http://192.168.0.1:1900/gatedesc.xml
|_eap-info: please specify an interface with -e
|_hostmap-robtex: *TEMPORARILY DISABLED* due to changes in Robtex's API. See https://www.robtex.com/api/
|_http-robtex-shared-ns: *TEMPORARILY DISABLED* due to changes in Robtex's API. See https://www.robtex.com/api/
| targets-asn:
|_  targets-asn.asn is a mandatory parameter
Nmap scan report for 192.168.0.108
Host is up (0.000032s latency).
Not shown: 996 closed ports
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
|_smb-enum-services: ERROR: Script execution failed (use -d to debug)
445/tcp open  microsoft-ds
|_smb-enum-services: ERROR: Script execution failed (use -d to debug)
808/tcp open  ccproxy-http
```



Target: 192.168.0.108

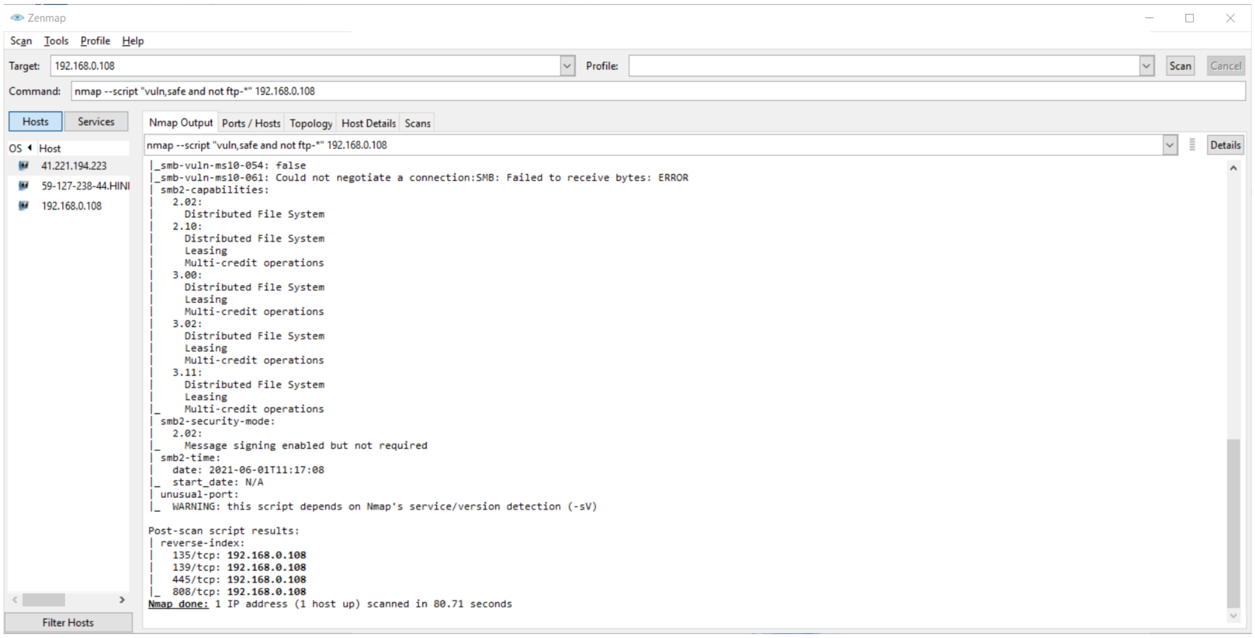
Profile:

Command: nmap --script "vuln,safe and not ftp-*" 192.168.0.108

OS Host
41.221.194.223
59-127-238-44.HINI
192.168.0.108

nmap --script "vuln,safe and not ftp-*" 192.168.0.108

```
808/tcp open  ccproxy-http

Host script results:
|_clock-skew: -1s
| dns-blacklist:
|   SPAM
|_    l2.apews.org - FAIL
|_fcrdns: FAIL (No PTR record)
|_ipidseq: ERROR: Script execution failed (use -d to debug)
|_msrpc-enum: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR
|_path-mtu: ERROR: Script execution failed (use -d to debug)
|_qscan: ERROR: Script execution failed (use -d to debug)
|_samba-vuln-cve-2012-1182: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR
| smb-mbenum:
|_  ERROR: Failed to connect to browser service: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR
| smb-protocols:
|   dialects:
|     2.02
|     2.10
|     3.00
|     3.02
|_    3.11
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR
| smb2-capabilities:
|   2.02:
|     Distributed File System
|   2.10:
|     Distributed File System
|     Leasing
|     Multi-credit operations
|   3.00:
|     Distributed File System
|     Leasing
|     Multi-credit operations
|   3.02:
|     Distributed File System
|     Leasing
|     Multi-credit operations
```



Target: 192.168.0.108

Command: nmap --script "vuln,safe and not ftp-*" 192.168.0.108

41.221.194.223
59-127-238-44.HINI
192.168.0.108

nmap --script "vuln,safe and not ftp-*" 192.168.0.108

```
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR
| smb2-capabilities:
|   2.02:
|     Distributed File System
|   2.10:
|     Distributed File System
|     Leasing
|     Multi-credit operations
|   3.00:
|     Distributed File System
|     Leasing
|     Multi-credit operations
|   3.02:
|     Distributed File System
|     Leasing
|     Multi-credit operations
|   3.11:
|     Distributed File System
|     Leasing
|_    Multi-credit operations
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2021-06-01T11:17:08
|_  start_date: N/A
| unusual-port:
|_  WARNING: this script depends on Nmap's service/version detection (-sV)

Post-scan script results:
| reverse-index:
|   135/tcp: 192.168.0.108
|   139/tcp: 192.168.0.108
|   445/tcp: 192.168.0.108
|_  808/tcp: 192.168.0.108
Nmap done: 1 IP address (1 host up) scanned in 80.71 seconds
```