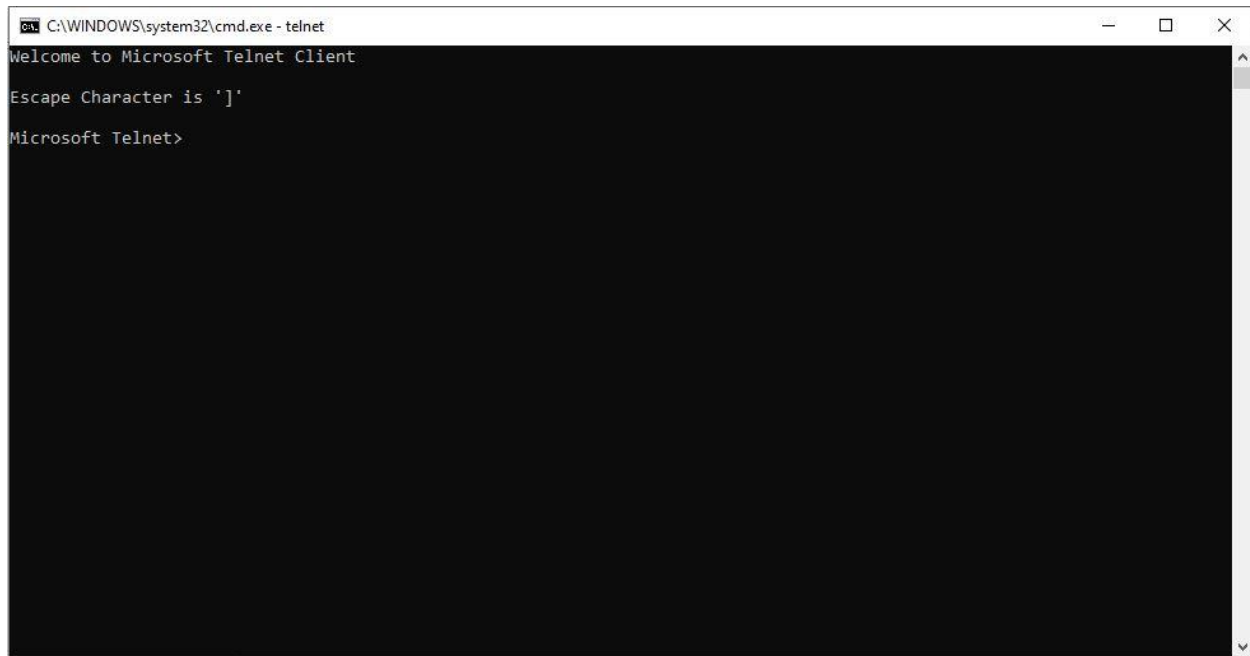


Name: Najmun Nahar

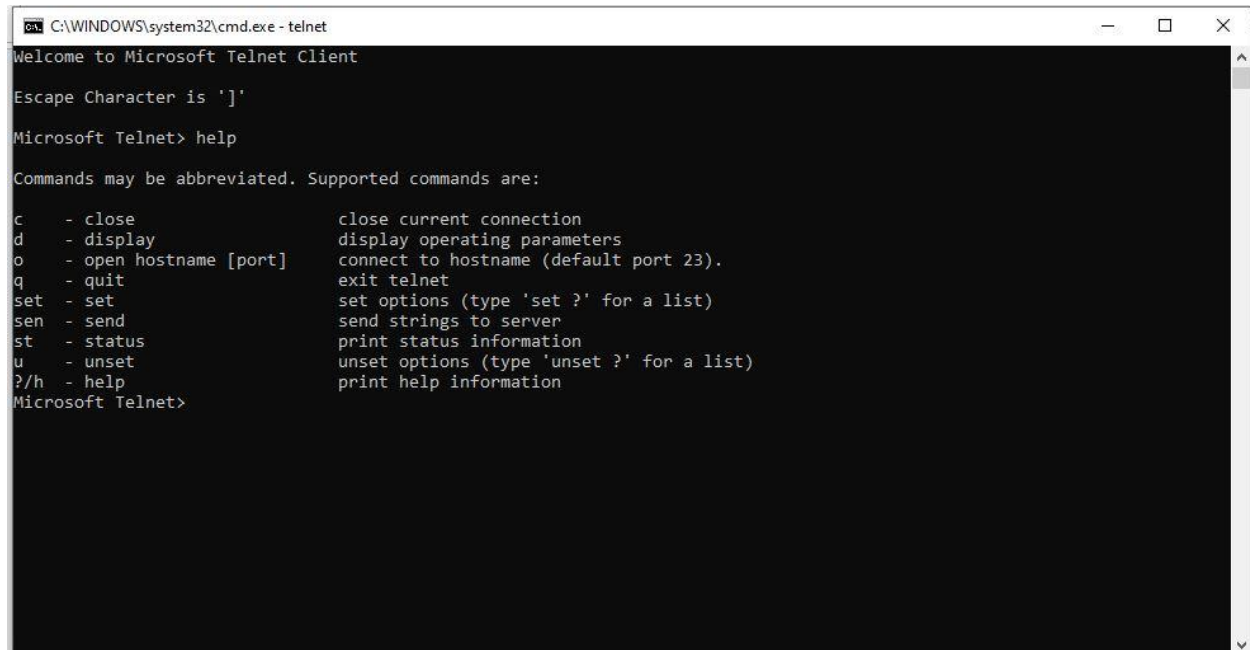
ID: 301160081

Lab-7

Telnet Enabled



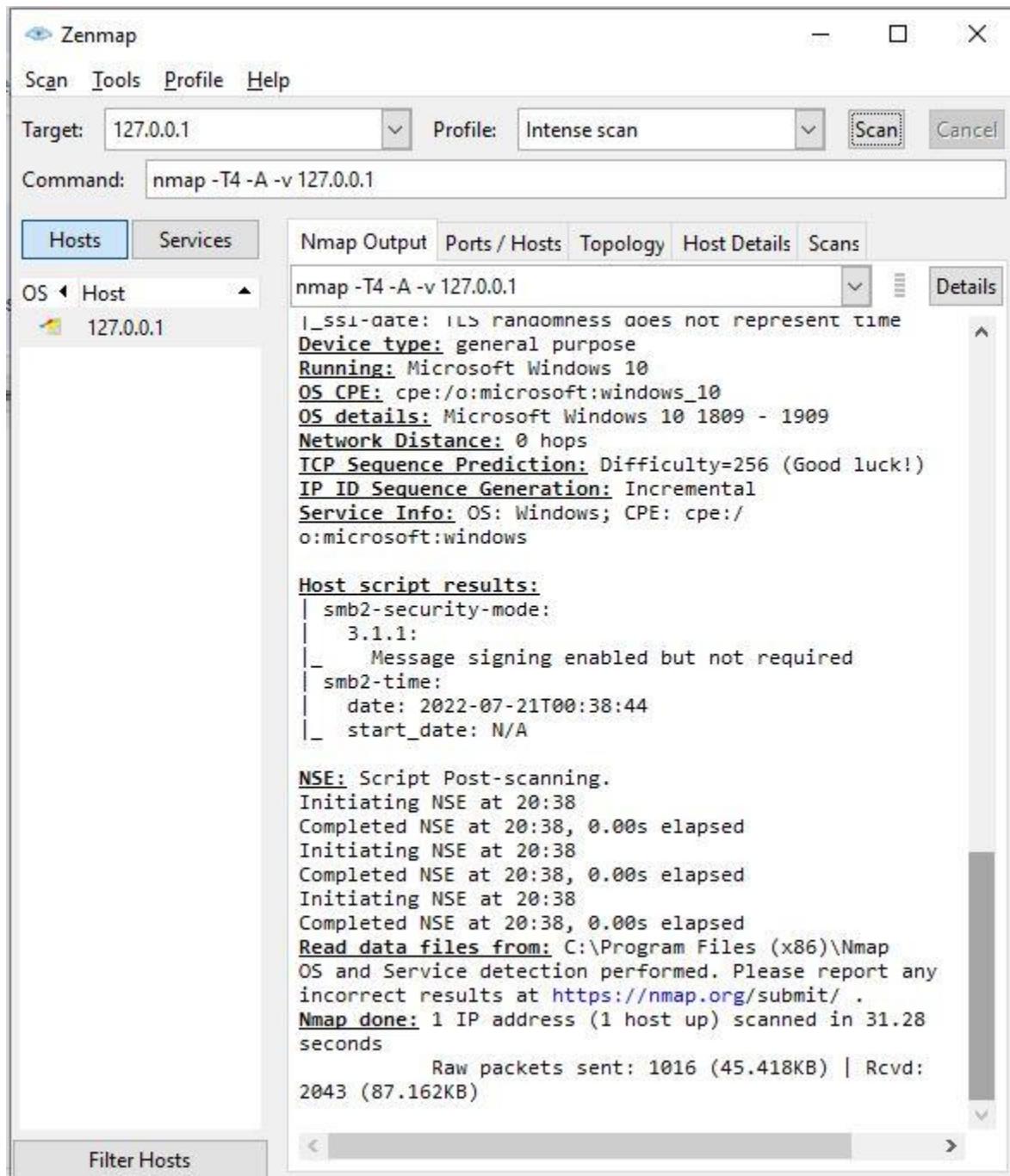
```
C:\WINDOWS\system32\cmd.exe - telnet
Welcome to Microsoft Telnet Client
Escape Character is ']'
Microsoft Telnet>
```



```
C:\WINDOWS\system32\cmd.exe - telnet
Welcome to Microsoft Telnet Client
Escape Character is ']'
Microsoft Telnet> help
Commands may be abbreviated. Supported commands are:
c  - close           close current connection
d  - display         display operating parameters
o  - open hostname [port] connect to hostname (default port 23).
q  - quit           exit telnet
set - set           set options (type 'set ?' for a list)
sen - send          send strings to server
st  - status        print status information
u  - unset          unset options (type 'unset ?' for a list)
?/h - help         print help information
Microsoft Telnet>
```

Zenmap GUI Testing

127.0.0.1 (Intense Scan)



192.168.1.0/24 Intense scan

Zenmap

Scan Tools Profile Help

Target: 192.168.1.0/24 Profile: Intense scan Scan Cancel

Command: nmap -T4 -A -v 192.168.1.0/24

Hosts Services

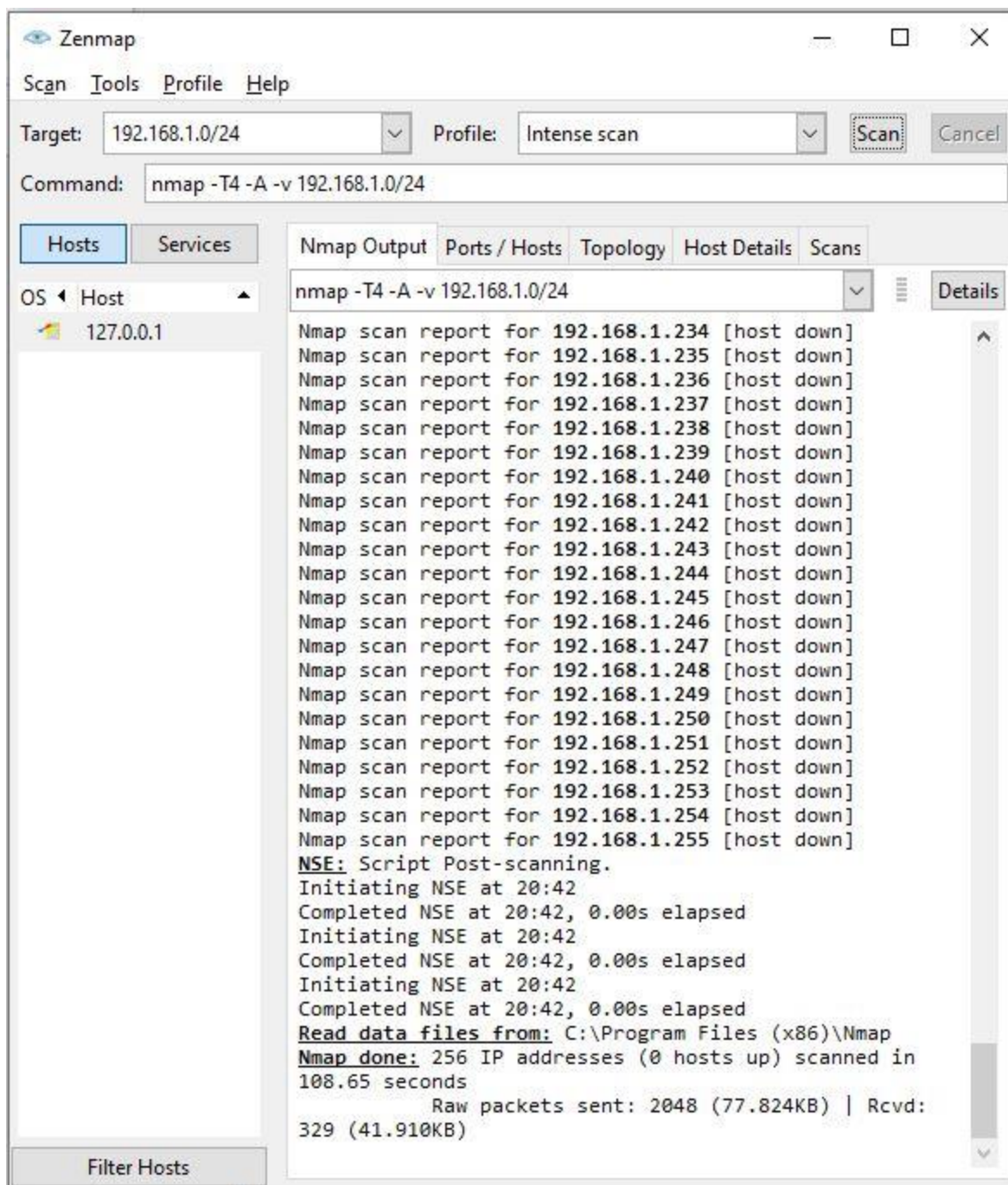
OS Host 127.0.0.1

Filter Hosts

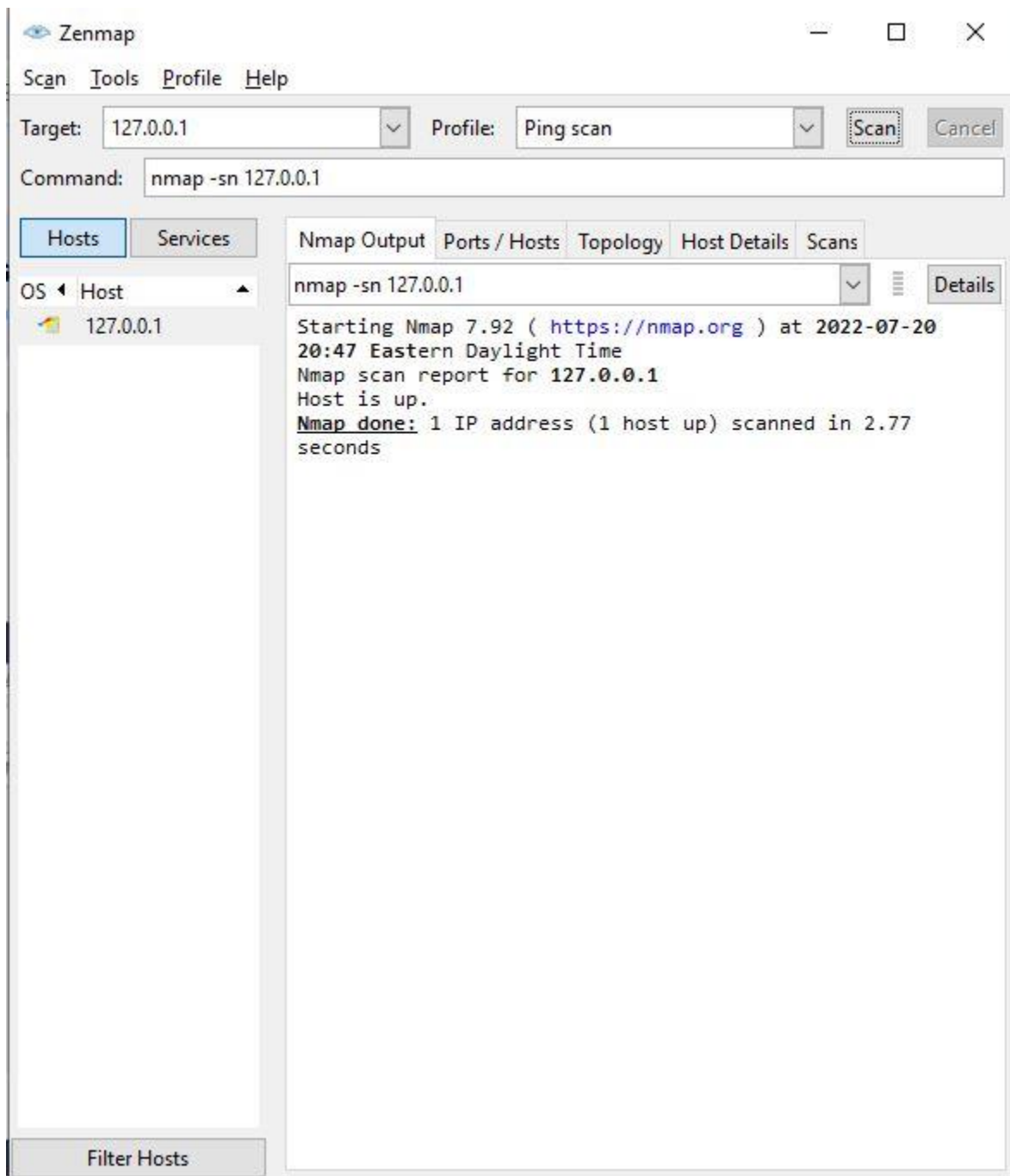
Nmap Output Ports / Hosts Topology Host Details Scans

nmap -T4 -A -v 192.168.1.0/24 Details

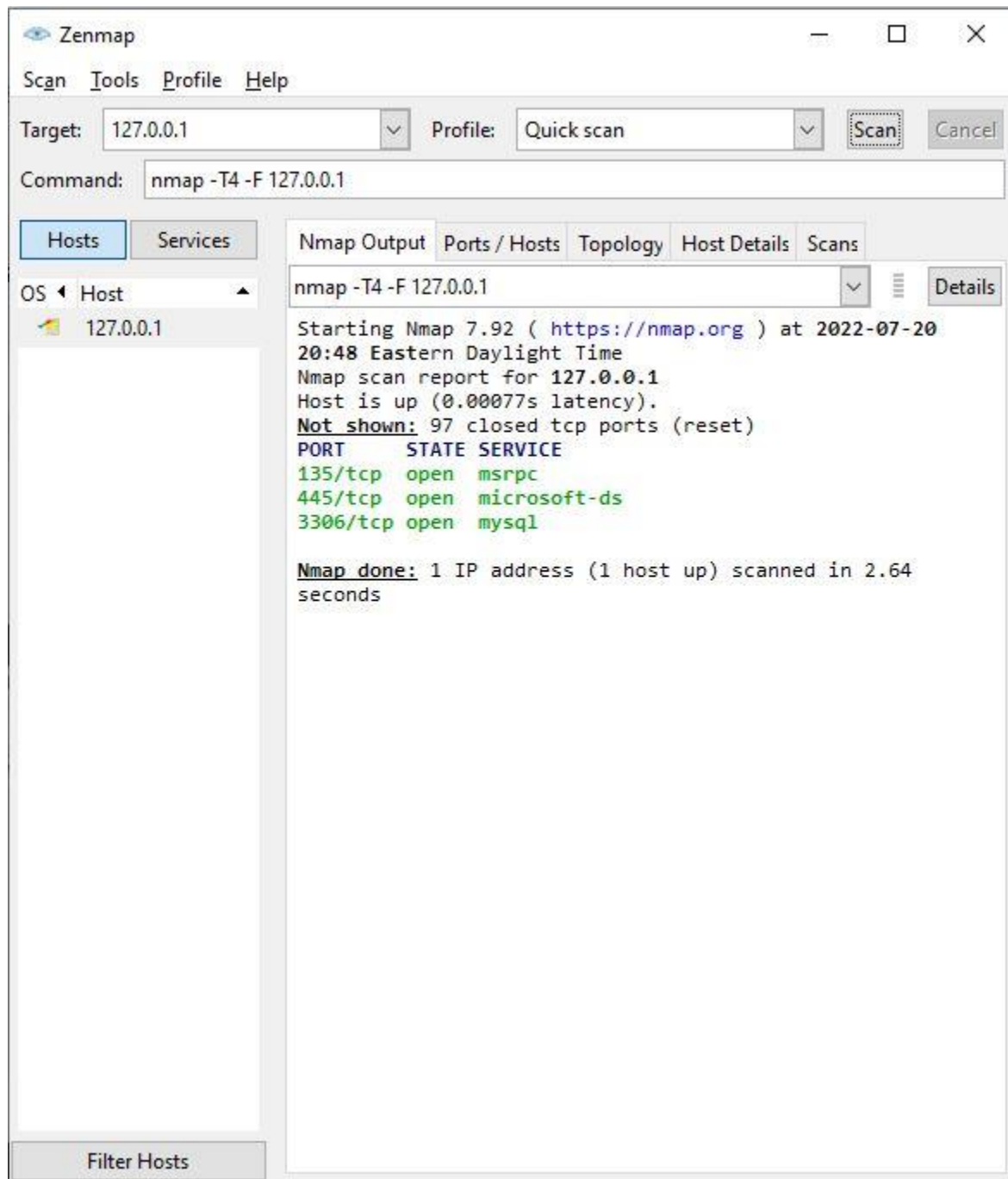
Starting Nmap 7.92 (<https://nmap.org>) at 2022-07-20 20:40 Eastern Daylight Time
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 20:41
Completed NSE at 20:41, 0.00s elapsed
Initiating NSE at 20:41
Completed NSE at 20:41, 0.00s elapsed
Initiating NSE at 20:41
Completed NSE at 20:41, 0.00s elapsed
Initiating Ping Scan at 20:41
Scanning 256 hosts [4 ports/host]
Ping Scan Timing: About 29.35% done; ETC: 20:42 (0:01:15 remaining)
Ping Scan Timing: About 57.57% done; ETC: 20:42 (0:00:45 remaining)
Completed Ping Scan at 20:42, 105.29s elapsed (256 total hosts)
Nmap scan report for 192.168.1.0 [host down]
Nmap scan report for 192.168.1.1 [host down]
Nmap scan report for 192.168.1.2 [host down]
Nmap scan report for 192.168.1.3 [host down]
Nmap scan report for 192.168.1.4 [host down]
Nmap scan report for 192.168.1.5 [host down]
Nmap scan report for 192.168.1.6 [host down]
Nmap scan report for 192.168.1.7 [host down]
Nmap scan report for 192.168.1.8 [host down]
Nmap scan report for 192.168.1.9 [host down]
Nmap scan report for 192.168.1.10 [host down]
Nmap scan report for 192.168.1.11 [host down]
Nmap scan report for 192.168.1.12 [host down]
Nmap scan report for 192.168.1.13 [host down]
Nmap scan report for 192.168.1.14 [host down]
Nmap scan report for 192.168.1.15 [host down]
Nmap scan report for 192.168.1.16 [host down]



127.0.0.1 Ping Scan



127.0.0.1 Quick Scan



Zenmap

Scan Tools Profile Help

Target: 127.0.0.1 Profile: Quick scan Scan Cancel

Command: nmap -T4 -F 127.0.0.1

Hosts Services

OS Host

127.0.0.1

Filter Hosts

Nmap Output Ports / Hosts Topology Host Details Scans

nmap -T4 -F 127.0.0.1 Details

Starting Nmap 7.92 (<https://nmap.org>) at 2022-07-20 20:48 Eastern Daylight Time
Nmap scan report for 127.0.0.1
Host is up (0.00077s latency).
Not shown: 97 closed tcp ports (reset)

PORT	STATE	SERVICE
135/tcp	open	msrpc
445/tcp	open	microsoft-ds
3306/tcp	open	mysql

Nmap done: 1 IP address (1 host up) scanned in 2.64 seconds

127.0.0.1 Regular Scan

The screenshot shows the Zenmap application window. At the top, there's a menu bar with 'Scan', 'Tools', 'Profile', and 'Help'. Below the menu, the 'Target' field is set to '127.0.0.1' and the 'Profile' is set to 'Regular scan'. There are 'Scan' and 'Cancel' buttons. The 'Command' field shows 'nmap 127.0.0.1'. On the left, there's a sidebar with 'Hosts' and 'Services' tabs. Under 'Hosts', there's a list with '127.0.0.1'. At the bottom left is a 'Filter Hosts' button. The main area has tabs for 'Nmap Output', 'Ports / Hosts', 'Topology', 'Host Details', and 'Scans'. The 'Nmap Output' tab is active, showing the scan results for '127.0.0.1'. The output text is as follows:

```
nmap 127.0.0.1

Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-20
20:49 Eastern Daylight Time
Nmap scan report for 127.0.0.1
Host is up (0.0012s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
445/tcp    open  microsoft-ds
3306/tcp   open  mysql

Nmap done: 1 IP address (1 host up) scanned in 2.62
seconds
```

Nmap centennialcollege.ca

The screenshot shows the Zenmap application window. At the top, there's a menu bar with 'Scan', 'Tools', 'Profile', and 'Help'. Below the menu, the 'Target' field is set to 'centennialcollege.ca' and the 'Profile' is 'Regular scan'. There are 'Scan' and 'Cancel' buttons. The 'Command' field shows 'nmap centennialcollege.ca'. On the left, there's a sidebar with 'Hosts' and 'Services' tabs. Under 'Hosts', there's a list with '127.0.0.1' and 'centennialcollege.c'. The main area has tabs for 'Nmap Output', 'Ports / Hosts', 'Topology', 'Host Details', and 'Scans'. The 'Nmap Output' tab is active, showing the scan results for 'centennialcollege.ca'. The output text is as follows:

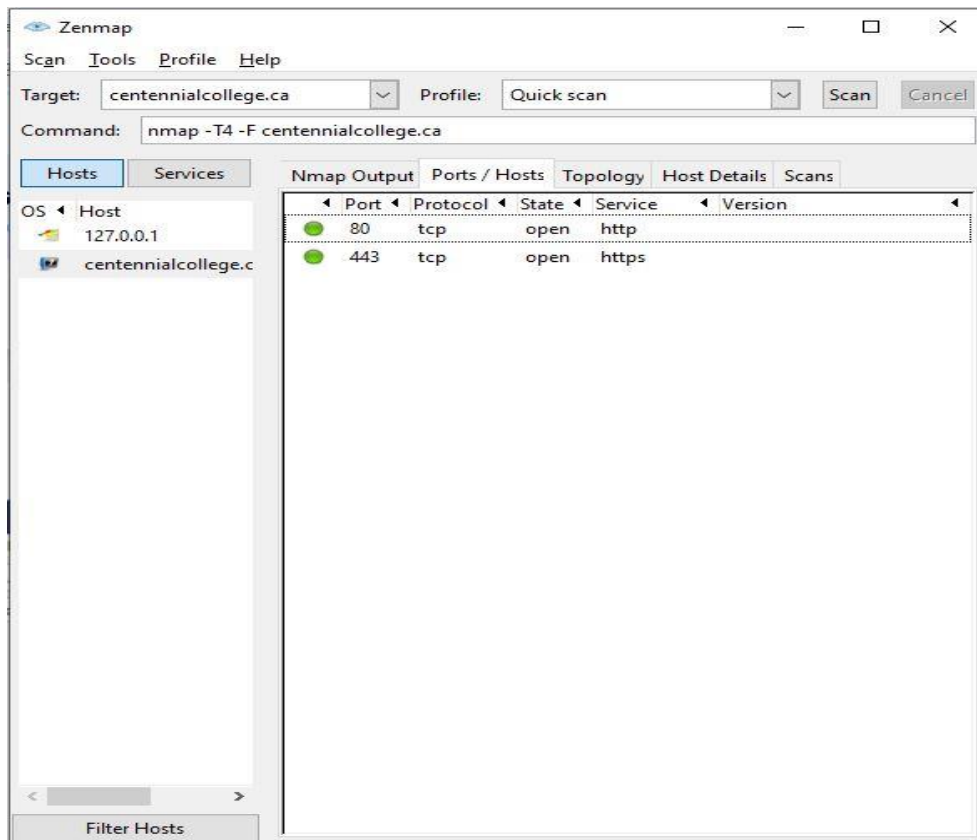
```
nmap centennialcollege.ca

Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-20
20:55 Eastern Daylight Time
Nmap scan report for centennialcollege.ca
(199.212.27.206)
Host is up (0.029s latency).
rDNS record for 199.212.27.206: www.centennialcollege.ca
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

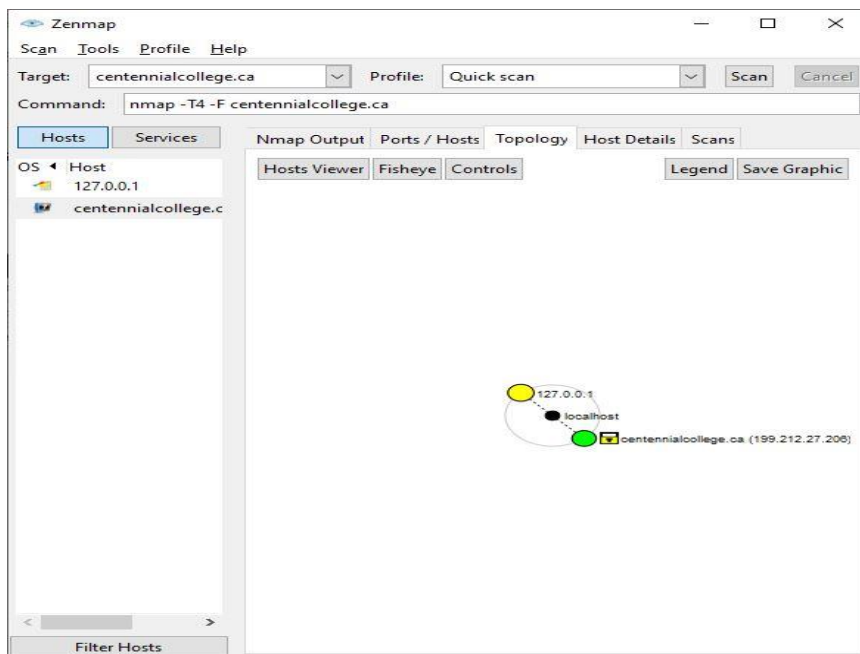
Nmap done: 1 IP address (1 host up) scanned in 7.57
seconds
```

At the bottom left, there's a 'Filter Hosts' button.

Ports/Hosts



Topology



Host Details

The screenshot shows the Zenmap application window. The title bar is "Zenmap" with standard window controls. The menu bar includes "Scan", "Tools", "Profile", and "Help". The "Target" field is set to "centennialcollege.ca" and the "Profile" is "Quick scan". The "Command" field shows "nmap -T4 -F centennialcollege.ca". The "Hosts" tab is selected in the left sidebar, showing a list of hosts: "127.0.0.1" and "centennialcollege.c". The "Host Details" tab is selected in the main panel, showing details for "centennialcollege.ca (199.212.27.206)".

Host Status

State:	up
Open ports:	2
Filtered ports:	98
Closed ports:	0
Scanned ports:	100
Up time:	Not available
Last boot:	Not available

Addresses

IPv4:	199.212.27.206
IPv6:	Not available
MAC:	Not available

Hostnames

Name - Type:	centennialcollege.ca - user
Name - Type:	www.centennialcollege.ca - PTR

Comments

Scans

The screenshot shows the Zenmap application window. At the top, there is a menu bar with 'Scan', 'Tools', 'Profile', and 'Help'. Below the menu bar, the 'Target' field is set to 'centennialcollege.ca' and the 'Profile' is set to 'Quick scan'. There are 'Scan' and 'Cancel' buttons. The 'Command' field shows 'nmap -T4 -F centennialcollege.ca'.

On the left side, there are two tabs: 'Hosts' and 'Services'. Under 'Hosts', there is a list of hosts: '127.0.0.1' and 'centennialcollege.c'. Below this list is a 'Filter Hosts' button.

The main area of the window is divided into several tabs: 'Nmap Output', 'Ports / Hosts', 'Topology', 'Host Details', and 'Scans'. The 'Scans' tab is currently selected. It displays a table with two columns: 'Status' and 'Command'.

Status	Command
Unsaved	nmap -T4 -A -v 127.0.0.1
Unsaved	nmap -T4 -A -v 192.168.1.0/24
Unsaved	nmap -sn 127.0.0.1
Unsaved	nmap -T4 -F 127.0.0.1
Unsaved	nmap 127.0.0.1
Unsaved	nmap centennialcollege.ca
Unsaved	nmap -T4 -F centennialcollege.ca

At the bottom of the window, there are three buttons: '+ Append Scan', '- Remove Scan', and 'X Cancel Scan'.

Method-2

Nmap command line- 127.0.0.1

```
C:\WINDOWS\system32\cmd.exe

C:\Users\Moon>nmap 127.0.0.1
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-20 21:00 Eastern Daylight Time
Nmap scan report for 127.0.0.1
Host is up (0.00092s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
445/tcp    open  microsoft-ds
3306/tcp   open  mysql

Nmap done: 1 IP address (1 host up) scanned in 3.23 seconds

C:\Users\Moon>
```

Nmap -sS 127.0.0.1

```
C:\WINDOWS\system32\cmd.exe

C:\Users\Moon>nmap -sS 127.0.0.1
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-20 21:05 Eastern Daylight Time
Nmap scan report for 127.0.0.1
Host is up (0.0011s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
445/tcp    open  microsoft-ds
3306/tcp   open  mysql

Nmap done: 1 IP address (1 host up) scanned in 3.41 seconds

C:\Users\Moon>
```

Nmap -sn 127.0.0.1

```
C:\WINDOWS\system32\cmd.exe

C:\Users\Moon>nmap -sn 127.0.0.1
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-20 21:06 Eastern Daylight Time
Nmap scan report for 127.0.0.1
Host is up.
Nmap done: 1 IP address (1 host up) scanned in 3.15 seconds

C:\Users\Moon>
```

Nmap -O 127.0.0.1

```
C:\WINDOWS\system32\cmd.exe

C:\Users\Moon>nmap -O 127.0.0.1
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-20 21:07 Eastern Daylight Time
Nmap scan report for 127.0.0.1
Host is up (0.00057s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
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=7.92%E=4%D=7/20%OT=135%CT=1%CU=37564%PV=N%DS=0%DC=L%G=Y%TM=62D8A6
OS:D2P=i686-pc-windows-windows)SEQ(SP=FA%GCD=1%ISR=FD%TI=I%CI=I%II=I%SS=5%
OS:TS=U)OPS(O1=MFFD7NW8NNNS%O2=MFFD7NW8NNNS%O3=MFFD7NW8%O4=MFFD7NW8NNNS%O5=MFF
OS:D7NW8NNNS%O6=MFFD7NNS)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FF70
OS: )ECN(R=Y%DF=Y%T=80%W=FFFF%O=MFFD7NW8NNNS%CC=N%Q=)T1(R=Y%DF=Y%T=80%S=0%A=S
OS: +%F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=Y%
OS: T=80%W=0%S=Z%A=0%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=0%F=R%O=%RD=
OS: 0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%
OS: S=A%A=0%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(
OS: R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=Z%RUCK=G%RUD=G)IE(R=Y%DFI=
OS: N%T=80%CD=Z)

Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.60 seconds

C:\Users\Moon>
```


Nmap -A 127.0.0.1

```
C:\WINDOWS\system32\cmd.exe

C:\Users\Moon>nmap -A 127.0.0.1
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-20 21:08 Eastern Daylight Time
Nmap scan report for 127.0.0.1
Host is up (0.00076s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc      Microsoft Windows RPC
445/tcp    open  microsoft-ds?
3306/tcp   open  mysql      MySQL 8.0.28
|_ mysql-info:
|_   Protocol: 10
|_   Version: 8.0.28
|_   Thread ID: 19
|_   Capabilities flags: 65535
|_   Some Capabilities: DontAllowDatabaseTableColumn, LongColumnFlag, Speaks41ProtocolOld, InteractiveClient, LongPassword, ConnectWithDatabase, SupportsTransactions, Sw
itchToSSLAfterHandshake, FoundRows, IgnoreSigpipes, Speaks41ProtocolNew, SupportsLoadDataLocal, Support41Auth, ODBCClient, IgnoreSpaceBeforeParenthesis, SupportsCompre
sion, SupportsMultipleStatements, SupportsMultipleResults, SupportsAuthPlugins
|_   Status: Autocommit
|_   Salt: J5o\x02:4A\x1F\x1Cmn9 \x0C \x10\x16\x1F8
|_   Auth Plugin Name: caching_sha2_password
|_   ssl-date: TLS randomness does not represent time
|_   ssl-cert: Subject: commonName=MySQL_Server_8.0.28_Auto_Generated_Server_Certificate
|_   Not valid before: 2022-03-08T04:22:34
|_   Not valid after: 2032-03-05T04:22:34
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1809 - 1909
Network Distance: 0 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_ smb2-time:
|_   date: 2022-07-21T01:08:37
|_   start_date: N/A
|_   smb2-security-mode:
|_     3.1.1:
|_       Message signing enabled but not required

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 36.80 seconds

C:\Users\Moon>
```

Nmap -F 127.0.0.1

```
C:\WINDOWS\system32\cmd.exe

C:\Users\Moon>nmap -F 127.0.0.1
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-20 21:10 Eastern Daylight Time
Nmap scan report for 127.0.0.1
Host is up (0.0012s latency).
Not shown: 97 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
445/tcp    open  microsoft-ds
3306/tcp   open  mysql

Nmap done: 1 IP address (1 host up) scanned in 2.93 seconds

C:\Users\Moon>
```

Nmap -v 127.0.0.1

```
C:\WINDOWS\system32\cmd.exe

C:\Users\Moon>nmap -v 127.0.0.1
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-20 21:11 Eastern Daylight Time
Initiating Parallel DNS resolution of 1 host. at 21:11
Completed Parallel DNS resolution of 1 host. at 21:11, 0.02s elapsed
Initiating SYN Stealth Scan at 21:11
Scanning 127.0.0.1 [1000 ports]
Discovered open port 445/tcp on 127.0.0.1
Discovered open port 135/tcp on 127.0.0.1
Discovered open port 3306/tcp on 127.0.0.1
Completed SYN Stealth Scan at 21:11, 0.12s elapsed (1000 total ports)
Nmap scan report for 127.0.0.1
Host is up (0.00079s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
445/tcp    open  microsoft-ds
3306/tcp   open  mysql

Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 2.86 seconds
Raw packets sent: 1000 (44.000KB) | Rcvd: 2003 (84.132KB)

C:\Users\Moon>
```

Nmap -oX scan Results.xml 127.0.0.1

```
C:\WINDOWS\system32\cmd.exe

C:\Users\Moon>nmap -v 127.0.0.1
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-20 21:11 Eastern Daylight Time
Initiating Parallel DNS resolution of 1 host. at 21:11
Completed Parallel DNS resolution of 1 host. at 21:11, 0.02s elapsed
Initiating SYN Stealth Scan at 21:11
Scanning 127.0.0.1 [1000 ports]
Discovered open port 445/tcp on 127.0.0.1
Discovered open port 135/tcp on 127.0.0.1
Discovered open port 3306/tcp on 127.0.0.1
Completed SYN Stealth Scan at 21:11, 0.12s elapsed (1000 total ports)
Nmap scan report for 127.0.0.1
Host is up (0.00079s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
445/tcp    open  microsoft-ds
3306/tcp   open  mysql

Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 2.86 seconds
Raw packets sent: 1000 (44.000KB) | Rcvd: 2003 (84.132KB)

C:\Users\Moon>nmap -oX Scan Results.xml 127.0.0.1
```

```
Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 2.86 seconds
Raw packets sent: 1000 (44.000KB) | Rcvd: 2003 (84.132KB)

C:\Users\Moon>nmap -oX Scan Results.xml 127.0.0.1
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-20 21:13 Eastern Daylight Time
Failed to resolve "Results.xml".
Nmap scan report for 127.0.0.1
Host is up (0.00051s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
445/tcp   open  microsoft-ds
3306/tcp  open  mysql

Nmap done: 1 IP address (1 host up) scanned in 2.95 seconds

C:\Users\Moon>
```