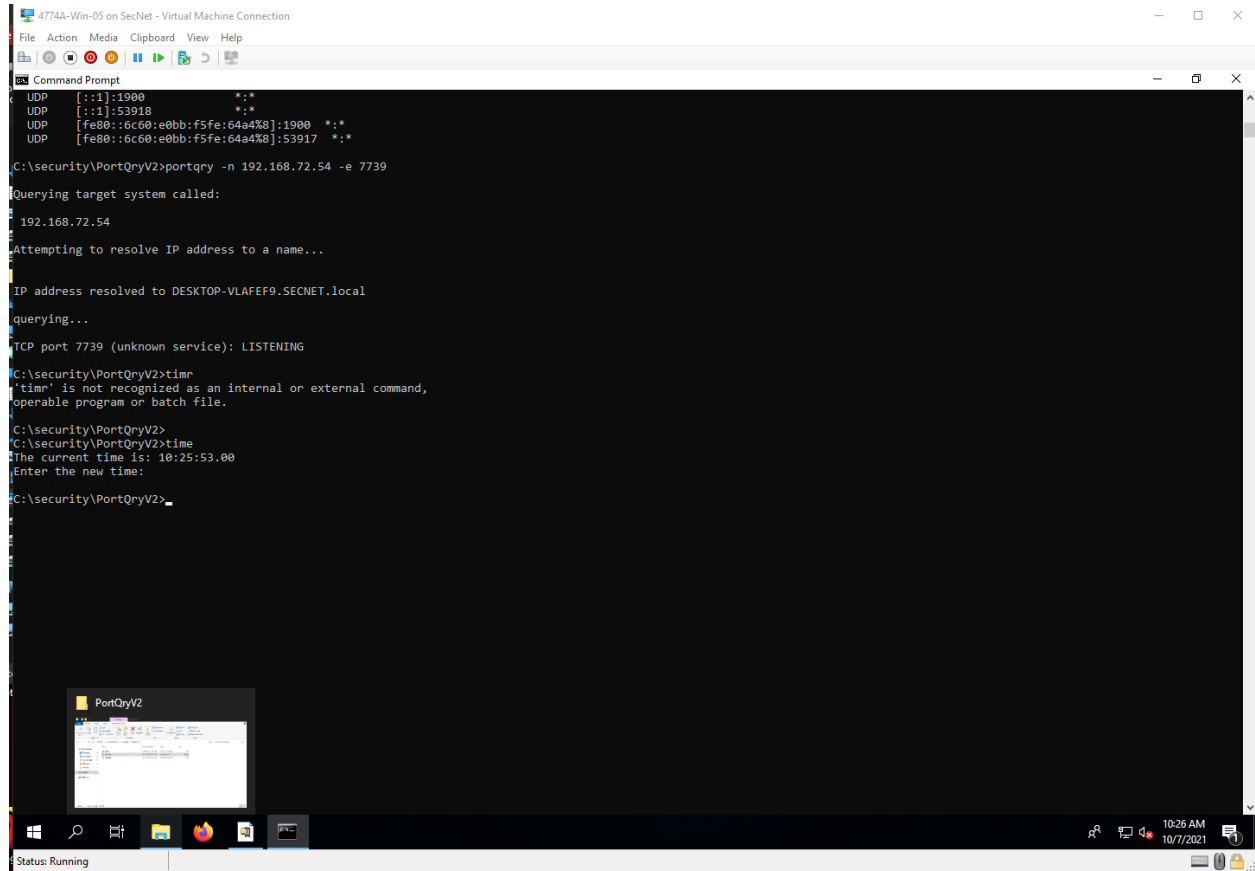


Screenshots

Step 34



```
4774A-Win-05 on SecNet - Virtual Machine Connection
File Action Media Clipboard View Help

C:\security\PortQryV2>portqry -n 192.168.72.54 -e 7739

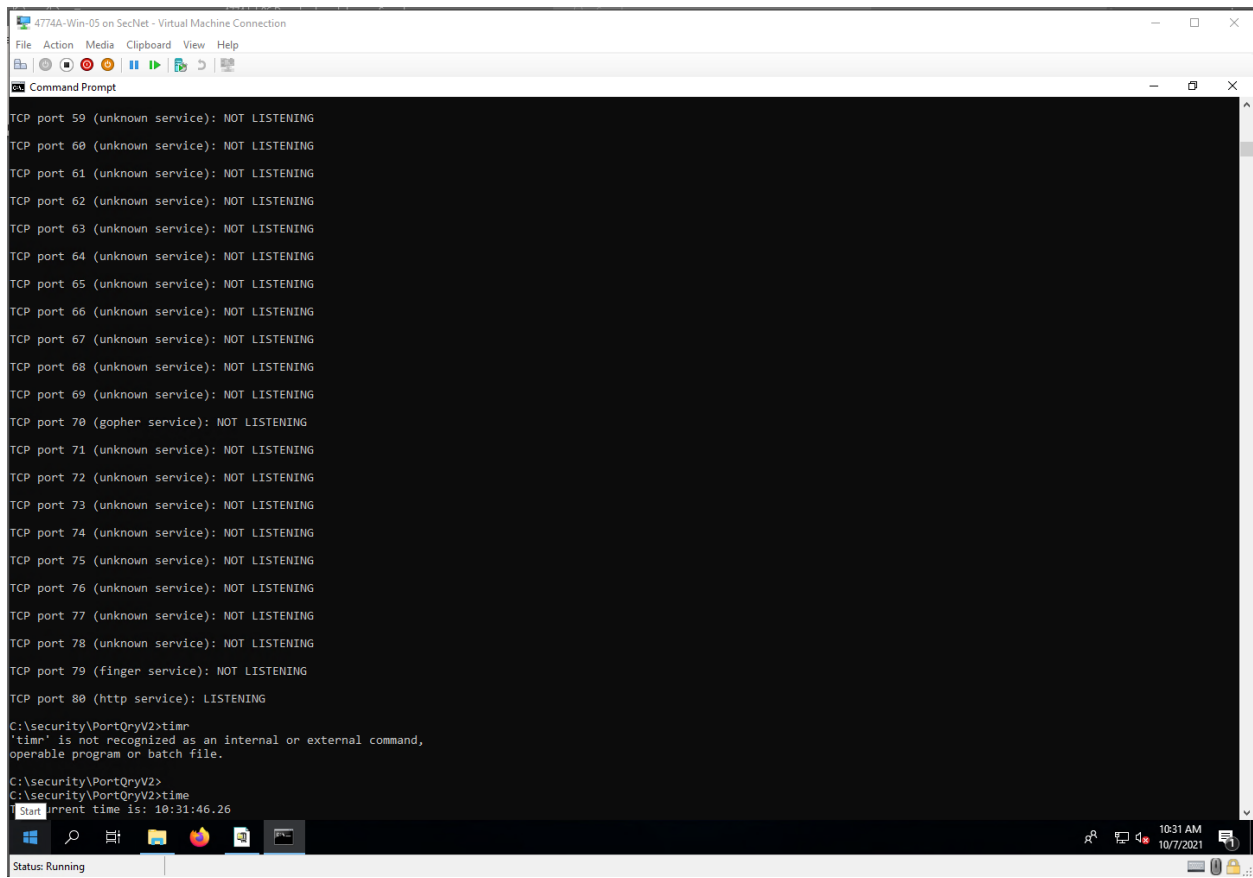
Querying target system called:
192.168.72.54
Attempting to resolve IP address to a name...
IP address resolved to DESKTOP-VLAFEF9.SECNET.local
querying...
TCP port 7739 (unknown service): LISTENING

C:\security\PortQryV2>timr
'timr' is not recognized as an internal or external command,
operable program or batch file.

C:\security\PortQryV2>time
The current time is: 10:25:53.00
Enter the new time:

C:\security\PortQryV2>
```

Step 39



```
4774A-Win-05 on SecNet - Virtual Machine Connection
File Action Media Clipboard View Help
Command Prompt

TCP port 59 (unknown service): NOT LISTENING
TCP port 60 (unknown service): NOT LISTENING
TCP port 61 (unknown service): NOT LISTENING
TCP port 62 (unknown service): NOT LISTENING
TCP port 63 (unknown service): NOT LISTENING
TCP port 64 (unknown service): NOT LISTENING
TCP port 65 (unknown service): NOT LISTENING
TCP port 66 (unknown service): NOT LISTENING
TCP port 67 (unknown service): NOT LISTENING
TCP port 68 (unknown service): NOT LISTENING
TCP port 69 (unknown service): NOT LISTENING
TCP port 70 (gopher service): NOT LISTENING
TCP port 71 (unknown service): NOT LISTENING
TCP port 72 (unknown service): NOT LISTENING
TCP port 73 (unknown service): NOT LISTENING
TCP port 74 (unknown service): NOT LISTENING
TCP port 75 (unknown service): NOT LISTENING
TCP port 76 (unknown service): NOT LISTENING
TCP port 77 (unknown service): NOT LISTENING
TCP port 78 (unknown service): NOT LISTENING
TCP port 79 (finger service): NOT LISTENING
TCP port 80 (http service): LISTENING

C:\security\PortQryV2>timr
'timr' is not recognized as an internal or external command,
operable program or batch file.

C:\security\PortQryV2>time
Start current time is: 10:31:46.26

Status: Running
```

Project Questions

1. My IP address is 192.168.72.54.
2. When I ran the “netstat -a”, approximately 40 ports were designated as listening.
3. Only port 80 was open when I scanned ports 1 through 80.
4. I was unaware of how many listening ports of generally open on a computer. Ports like 7739 and 5357

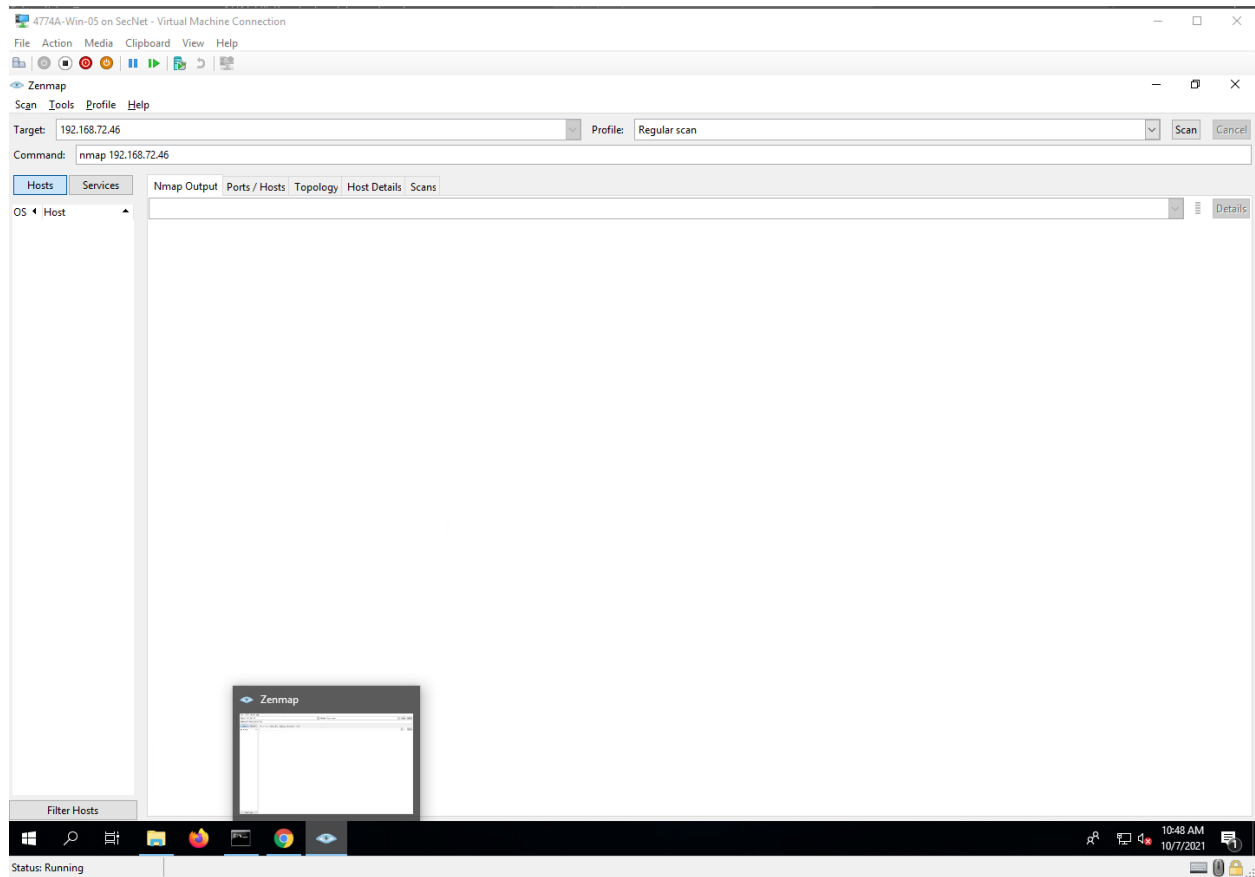
Thought Questions

1. There can be up to 65535 ports on a computer. Obviously, not all of these are used.
2. Any program that needs to connect or receive connections from others use a port. A port can only be used by one service at one time.
3. Yes, hackers do use ports to spread malware. Open ports are open access points to a machine.
4. To close ports that may already be open, you would have to disable the service that uses that port.

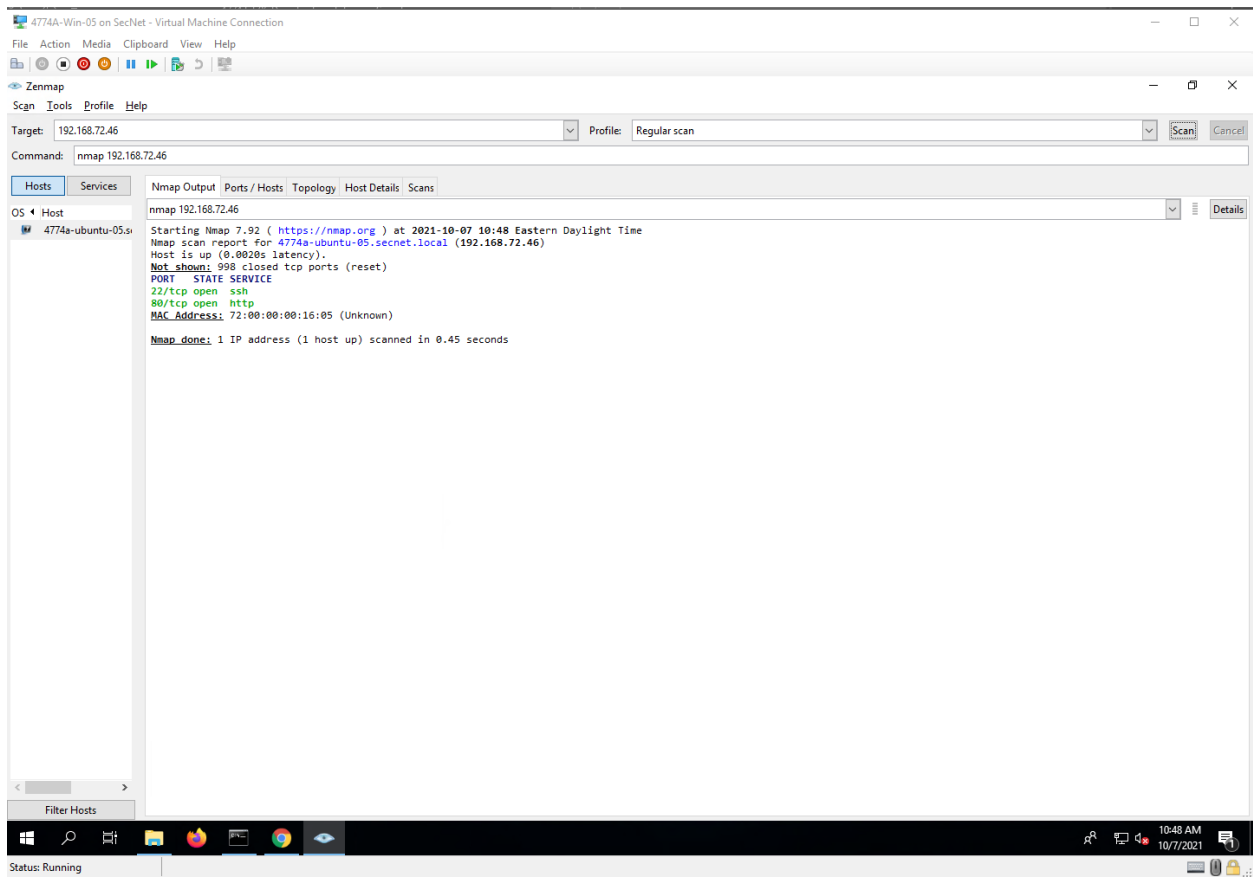
2 NMAP (ZENMAP)

Screenshots

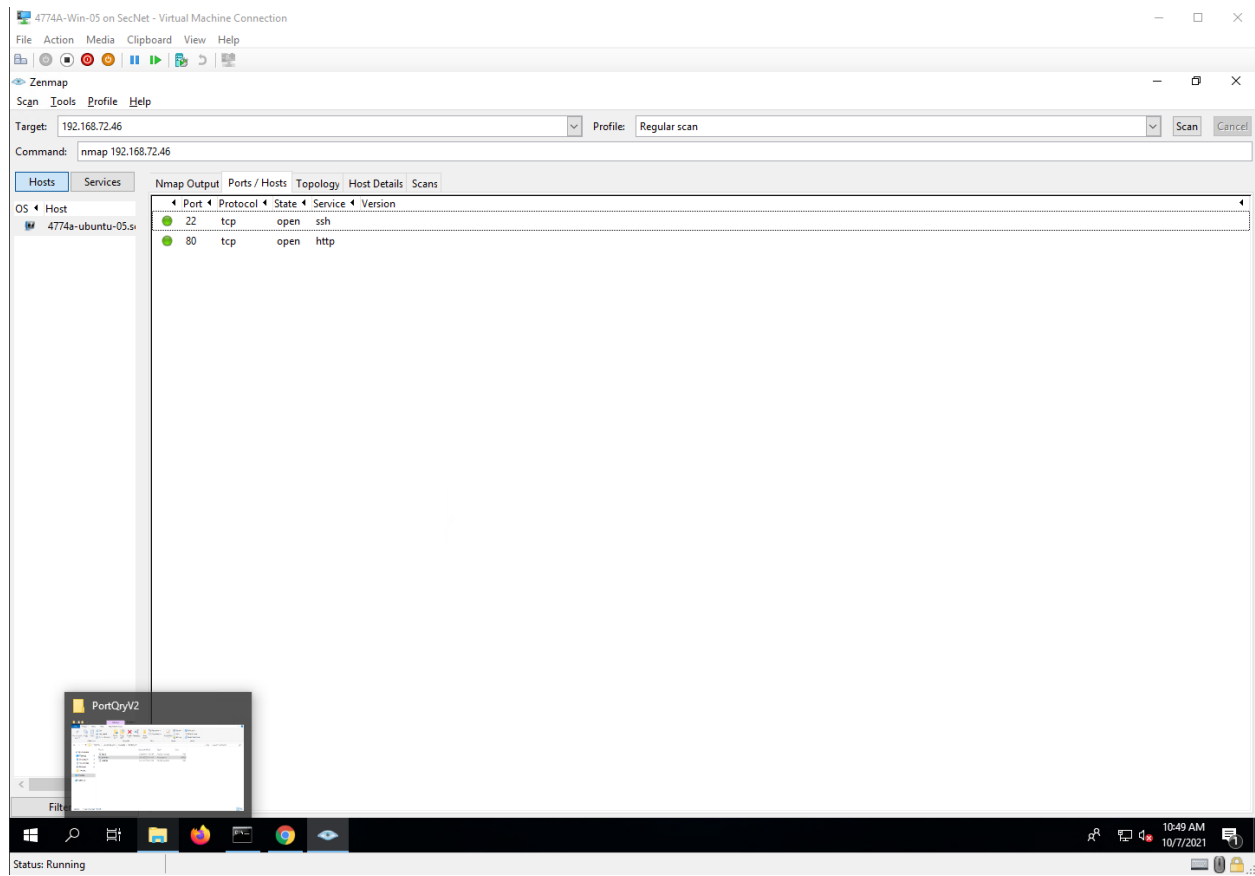
Step 12



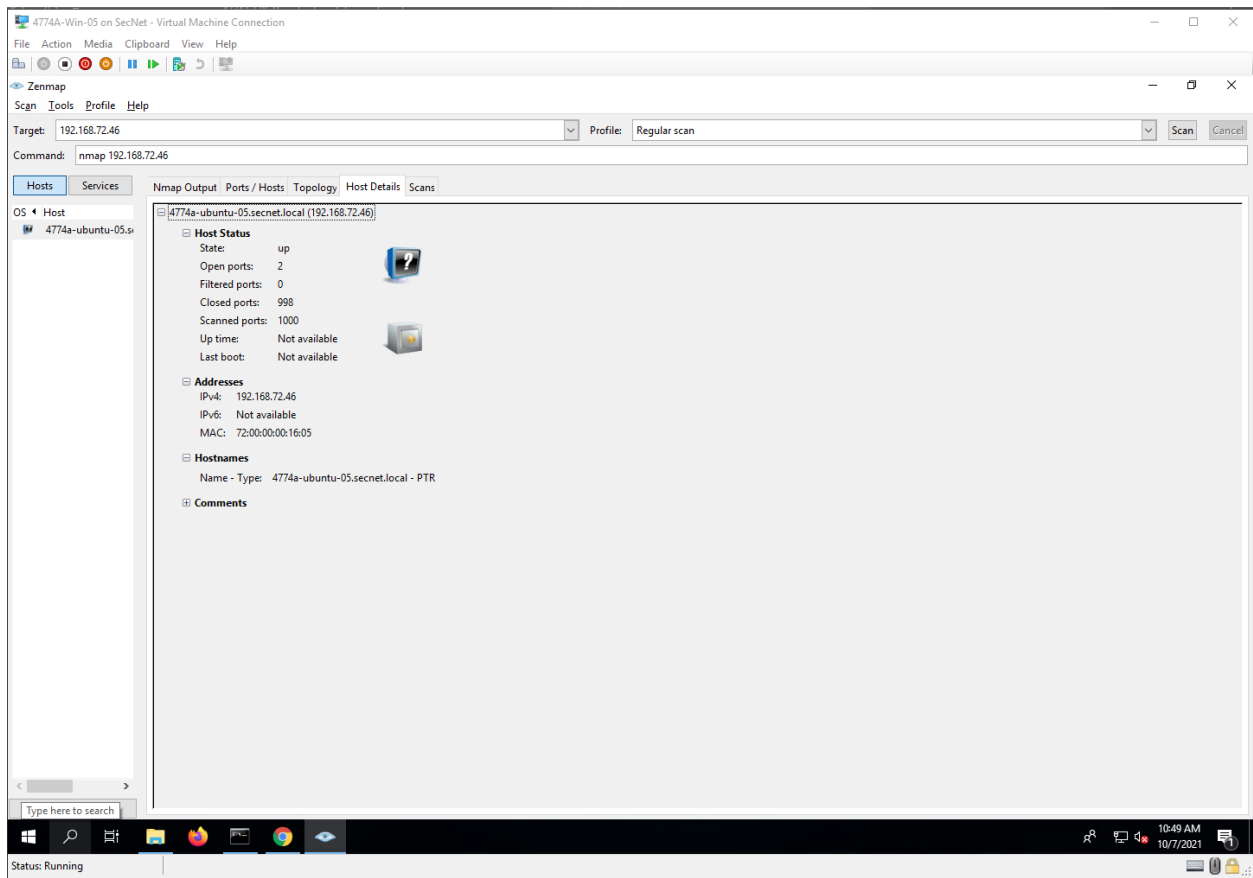
Step 16



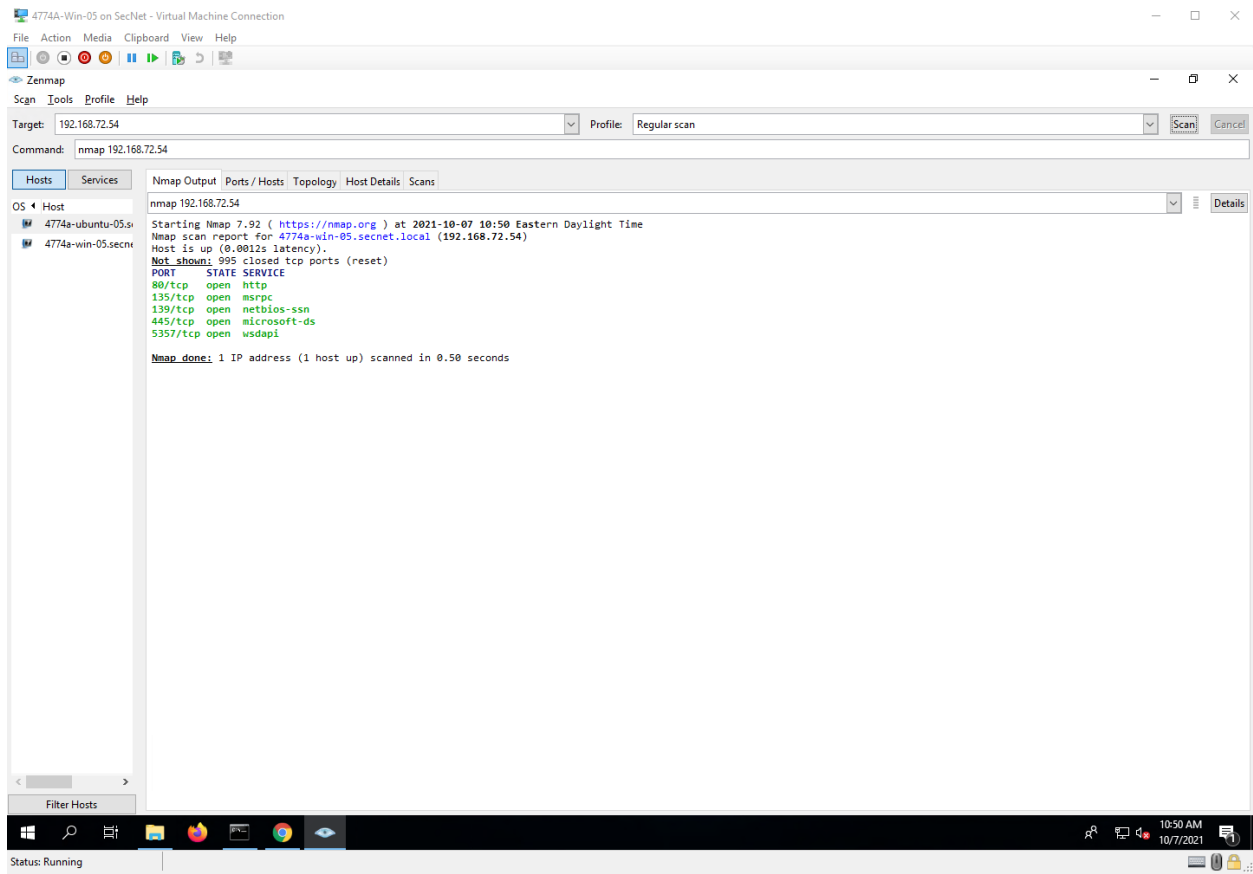
Step 18



Step 20



Step 22



Project Questions

1. The first IP address that I used was 192.168.72.46
2. The second IP address that I used was 192.168.72.54.
3. The first machine had 2 ports open. The second machine had 5 ports open.
4. The first scan took less than 1 second to complete

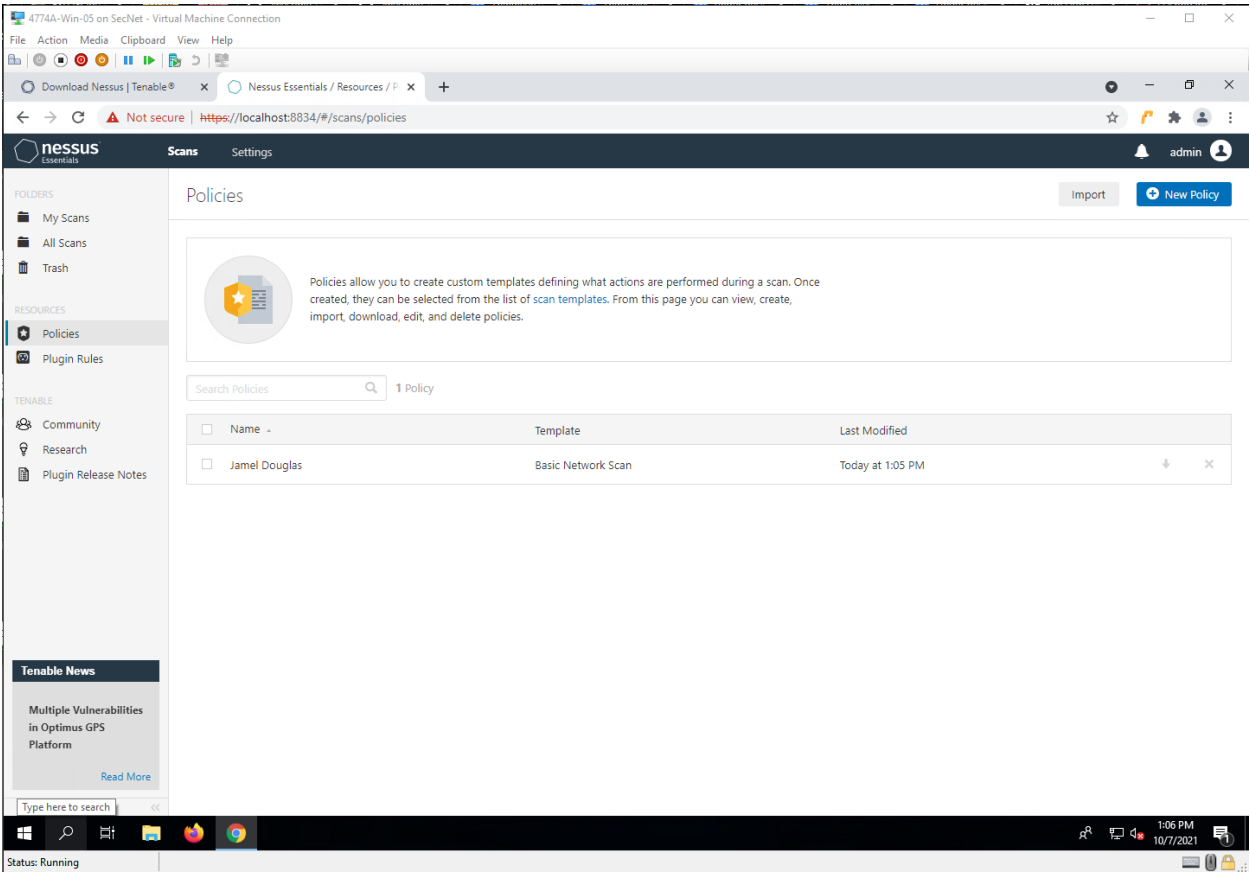
Thought Questions

1. A regular scan just looks to see if a port is open. An intense scan looks to see what service is open that port and a little more info about the service.
2. Sometimes NMAP won't be able to get the necessary information to determine the type of operating system.
3. Some ports will show up because certain ports are used for certain services. For example, port 80 is typically used for web servers.
4. I'm not sure if there is a way to protect against port scans. The only way to be safe about it is to make sure only the necessary ports are open

4 Nessus

Screenshots

Step 28



Step 37

The screenshot displays the Nessus Essentials web interface within a virtual machine window titled '4774A-Win-05 on SecNet - Virtual Machine Connection'. The browser address bar shows the URL `https://localhost:8834/#/scans/reports/9/hosts`. The interface features a left-hand navigation menu with sections for FOLDERS (My Scans, All Scans, Trash), RESOURCES (Policies, Plugin Rules), and TENABLE (Community, Research, Plugin Release Notes). The main content area is titled 'Jamel Douglas Scan' and includes a 'Back to My Scans' link. Below the title, there are tabs for 'Hosts' (1), 'Vulnerabilities' (5), and 'History' (1). A 'Filter' dropdown and a 'Search Hosts' input field are present. A table lists the hosts, with one entry for '192.168.72.54' showing 18 vulnerabilities (4%). To the right, the 'Scan Details' section provides information: Policy: Jamel Douglas, Status: Running (with a green status icon), Severity Base: CVSS v3.0, Scanner: Local Scanner, and Start: Today at 1:11 PM. Below this, a 'Vulnerabilities' section contains a donut chart and a legend for severity levels: Critical (red), High (orange), Medium (yellow), Low (green), and Info (blue). The donut chart is currently empty. At the bottom left, a 'Tenable News' sidebar is visible. The system tray at the bottom shows the status 'Running' and the time '1:13 PM 10/7/2021'.

4774A-Win-05 on SecNet - Virtual Machine Connection

File Action Media Clipboard View Help

Download Nessus | Tenable®

Nessus Essentials / Folders / View

Not secure | `https://localhost:8834/#/scans/reports/9/hosts`

nessus Essentials

Scans Settings

admin

FOLDERS

- My Scans
- All Scans
- Trash

RESOURCES

- Policies
- Plugin Rules

TENABLE

- Community
- Research
- Plugin Release Notes

Jamel Douglas Scan

Back to My Scans

Hosts 1 Vulnerabilities 5 History 1

Filter Search Hosts 1 Host

Host	Vulnerabilities	%
192.168.72.54	18	4%

Scan Details

Policy: Jamel Douglas

Status: Running

Severity Base: CVSS v3.0

Scanner: Local Scanner

Start: Today at 1:11 PM

Vulnerabilities

- Critical
- High
- Medium
- Low
- Info

Tenable News

Nessus Essentials / Folders / View Scan - Google Chrome

Nessus Essentials / Folders / View...

Tenable.io and Tenable.io WAS Achieve FedRAMP Auth... Read More

Status: Running

1:13 PM 10/7/2021

Step 39

4774A-Win-05 on SecNet - Virtual Machine Connection

File Action Media Clipboard View Help

Download Nessus | Tenable® x Nessus Essentials / Folders / View x +

Not secure | https://localhost:8834/#/scans/reports/9/hosts/2/vulnerabilities

nessus Essentials Scans Settings admin

FOLDERS

- My Scans
- All Scans
- Trash

RESOURCES

- Policies
- Plugin Rules

TENABLE

- Community
- Research
- Plugin Release Notes

Tenable News

Cybersecurity Awareness: Six Tips to Help Your Emp...
[Read More](#)

Jamel Douglas Scan / 192.168.72.54

[Back to Hosts](#) [Configure](#)

Vulnerabilities 12

Filter Search Vulnerabilities 12 Vulnerabilities

Sev	Name	Family	Count
MIXED	Apache Httpd (Multiple Issues)	Web Servers	4
MIXED	HTTP (Multiple Issues)	Web Servers	4
MEDIUM	SMB Signing not required	Misc.	1
INFO	DCE Services Enumeration	Windows	8
INFO	SMB (Multiple Issues)	Windows	6
INFO	Microsoft Windows (Multiple Issues)	Windows	2
INFO	Apache HTTP Server Version	Web Servers	1
INFO	Device Type	General	1
INFO	Host Fully Qualified Domain Name (FQDN) Resolution	General	1
INFO	Inconsistent Hostname and IP Address	Settings	1
INFO	OS Identification	General	1
INFO	OS Identification and Installed Software Enumeration over SSH v2 (U...	Misc.	1

Host Details

IP: 192.168.72.54
DNS: DESKTOP-VLA9EF9.SECNET.local
OS: Windows
Start: Today at 1:18 PM

Vulnerabilities

Legend: Critical (red), High (orange), Medium (yellow), Low (green), Info (blue)

Status: Running

1:23 PM 10/7/2021

Step 42

The screenshot displays the Nessus Essentials web interface within a virtual machine window titled "4774A-Win-05 on SecNet - Virtual Machine Connection". The browser address bar shows the URL <https://localhost:8834/#/scans/reports/11/hosts/2/vulnerabilities>. The interface is for a scan named "Jamel Douglas Scan 2 / 192.168.72.46".

Vulnerabilities Table:

Sev	Name	Family	Count
INFO	1 HTTP (Multiple Issues)	Web Servers	3
INFO	2 Apache HTTP Server (Multiple Issues)	Web Servers	2
INFO	2 SSH (Multiple Issues)	General	2
INFO	2 SSH (Multiple Issues)	Misc.	2
INFO	2 SSH (Multiple Issues)	Service detection	2
INFO	Nessus SYN scanner	Port scanners	2
INFO	Service Detection	Service detection	2
INFO	Backported Security Patch Detection (WWW)	General	1
INFO	Common Platform Enumeration (CPE)	General	1
INFO	Device Type	General	1
INFO	Ethernet MAC Addresses	General	1
INFO	Host Fully Qualified Domain Name (FQDN) Resoluti...	General	1

Host Details:

- IP: 192.168.72.46
- DNS: 4774a-ubuntu-05.secnct.local
- MAC: 72:00:00:00:16:05
- OS: Linux Kernel 4.4 on Ubuntu 16.04 (xenial)
- Start: Today at 1:16 PM
- End: Today at 1:20 PM
- Elapsed: 4 minutes
- KB: [Download](#)

Vulnerabilities Distribution:

- Critical (Red)
- High (Orange)
- Medium (Yellow)
- Low (Green)
- Info (Blue)

The donut chart shows that all 20 vulnerabilities are of "Info" severity, represented by the blue segment.

Project Questions

1. I had 2 critical results and 2 high-risk results. These are vulnerabilities from Apache versions 2.4.49 and before.
2. I had 2 medium risk results. One was for HTTP Trace/Track Methods and the other was for SMB signing not required.
3. The other IP addresses that I scanned was 192.168.72.46
4. No, I didn't find any high-risk weaknesses. Only information warnings.

Thought Questions

1. Yeah, running the scan was pretty easy. I was able to see what some of the vulnerabilities are, so that I can do some more research on them.
2. Tenable, the company that owns and maintains Nessus, is responsible for creating the plugins that are used with Nessus
3. There is an average of 50 vulnerabilities reported each day in 2020.
4. Everything is prone to a vulnerability if it is not kept up to date with modern security standards. It is said that Linux machines are less vulnerable to attacks, but I am not personally sure of that.