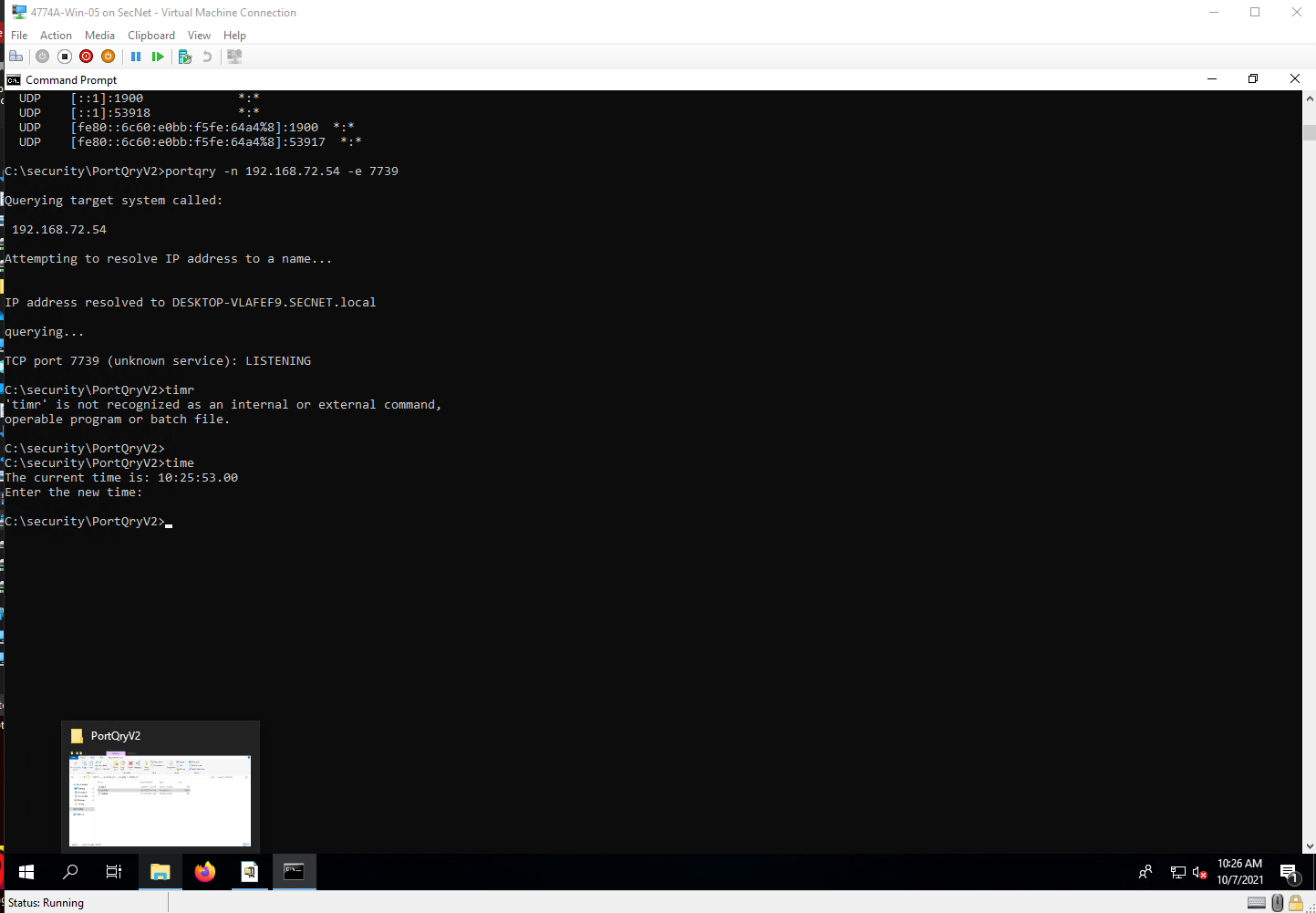
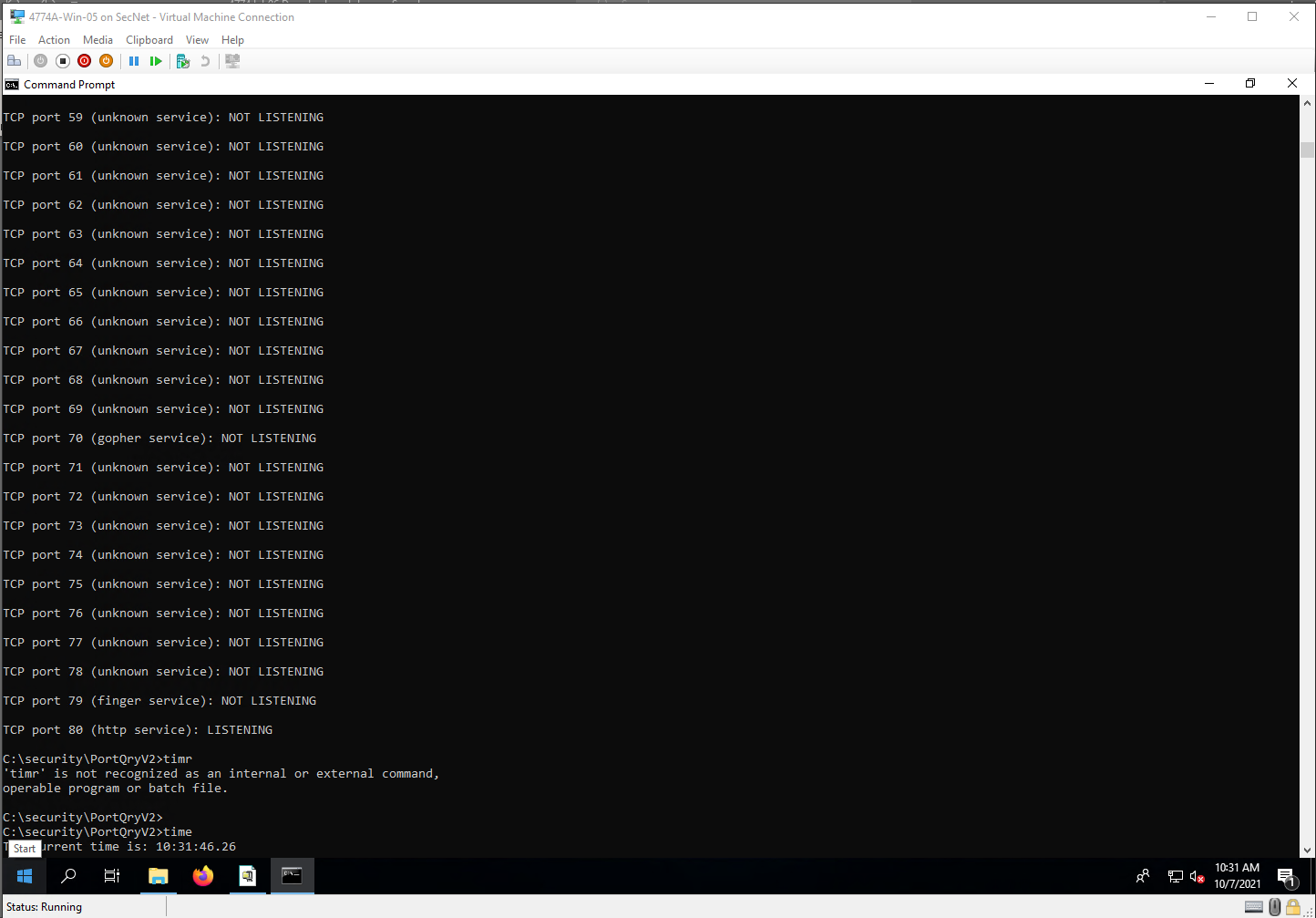
1 Portqry

Screenshots

Step 34



Step 39



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

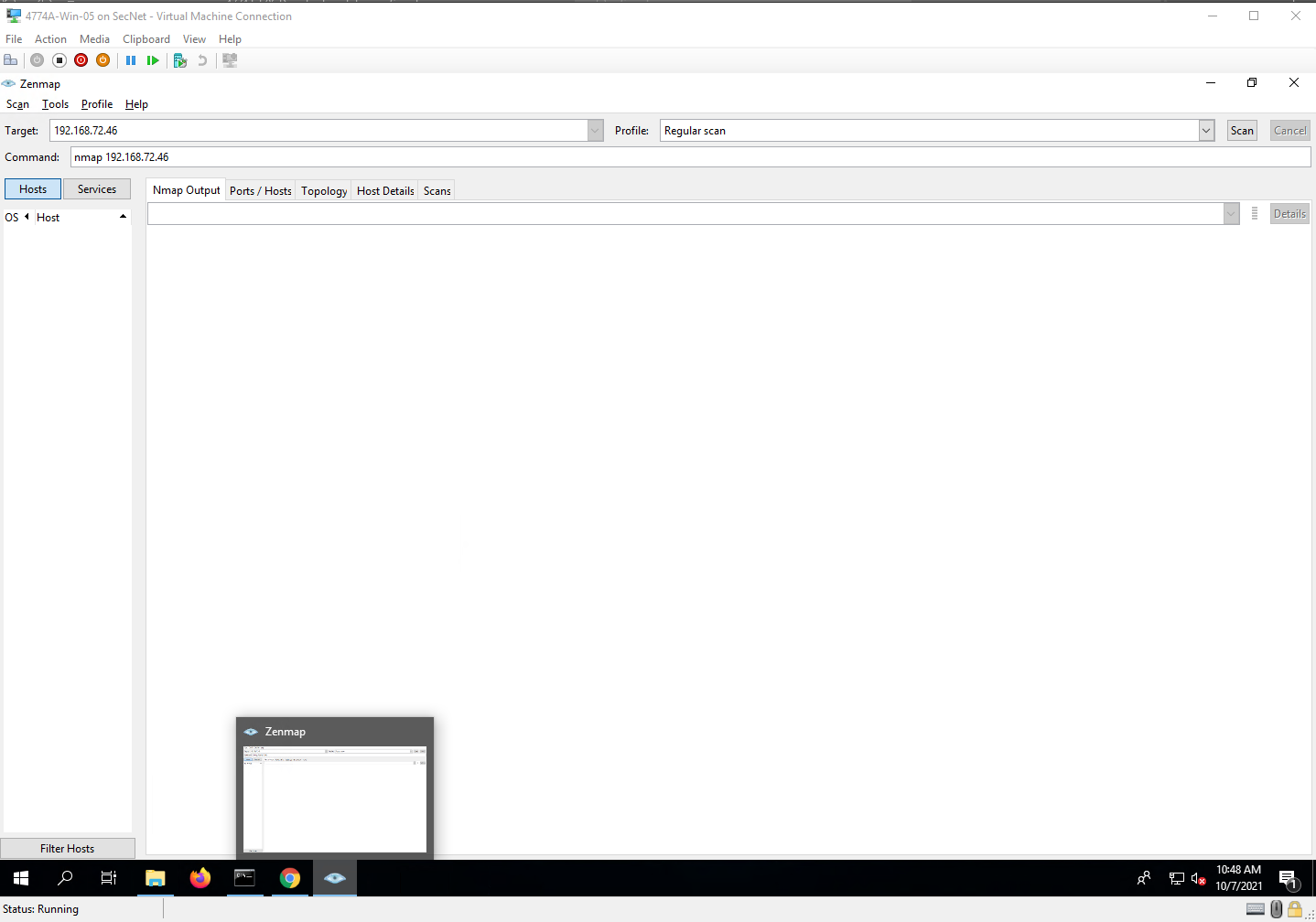
Thought Questions

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.

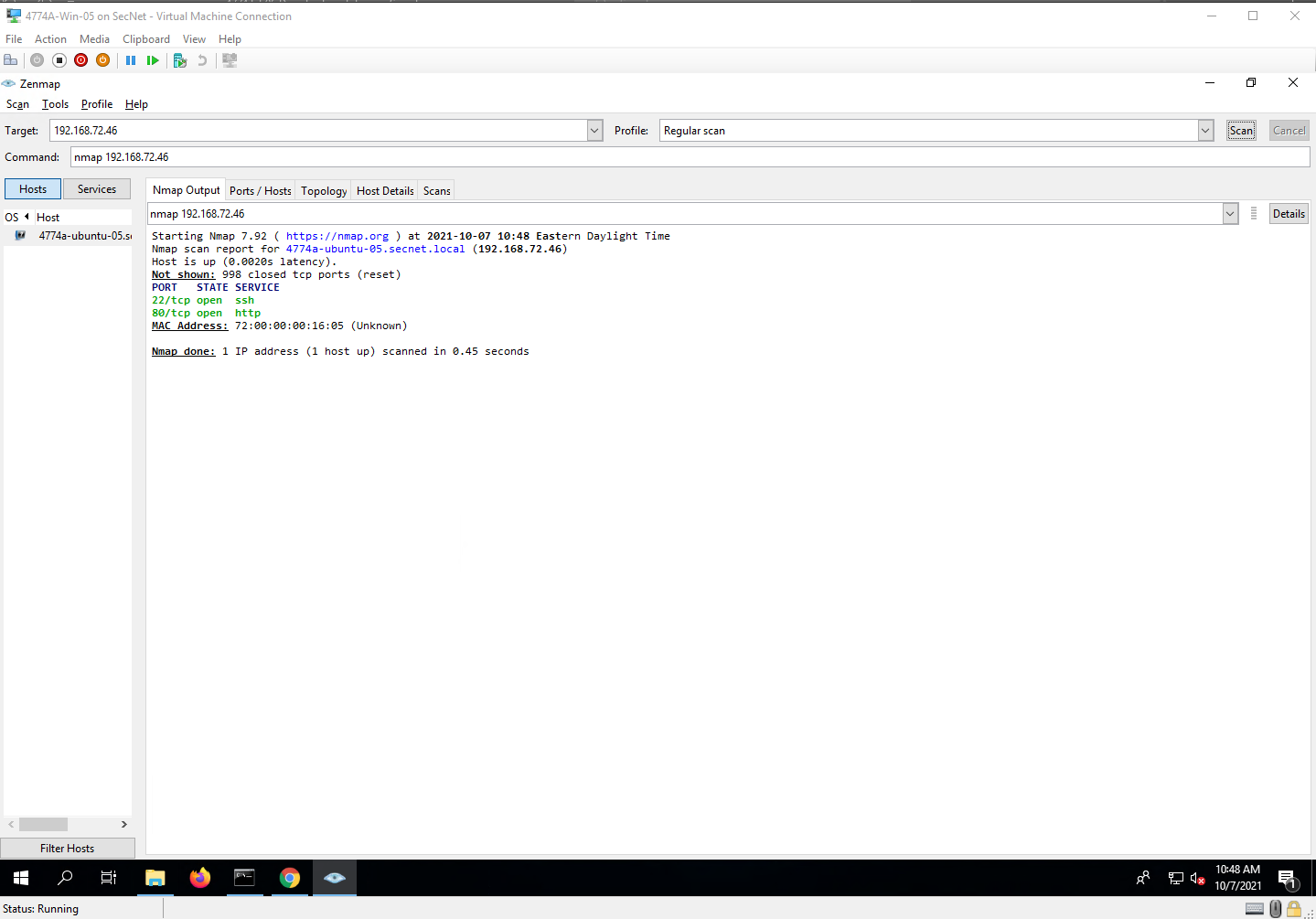
2 NMAP (ZENMAP)

Screenshots

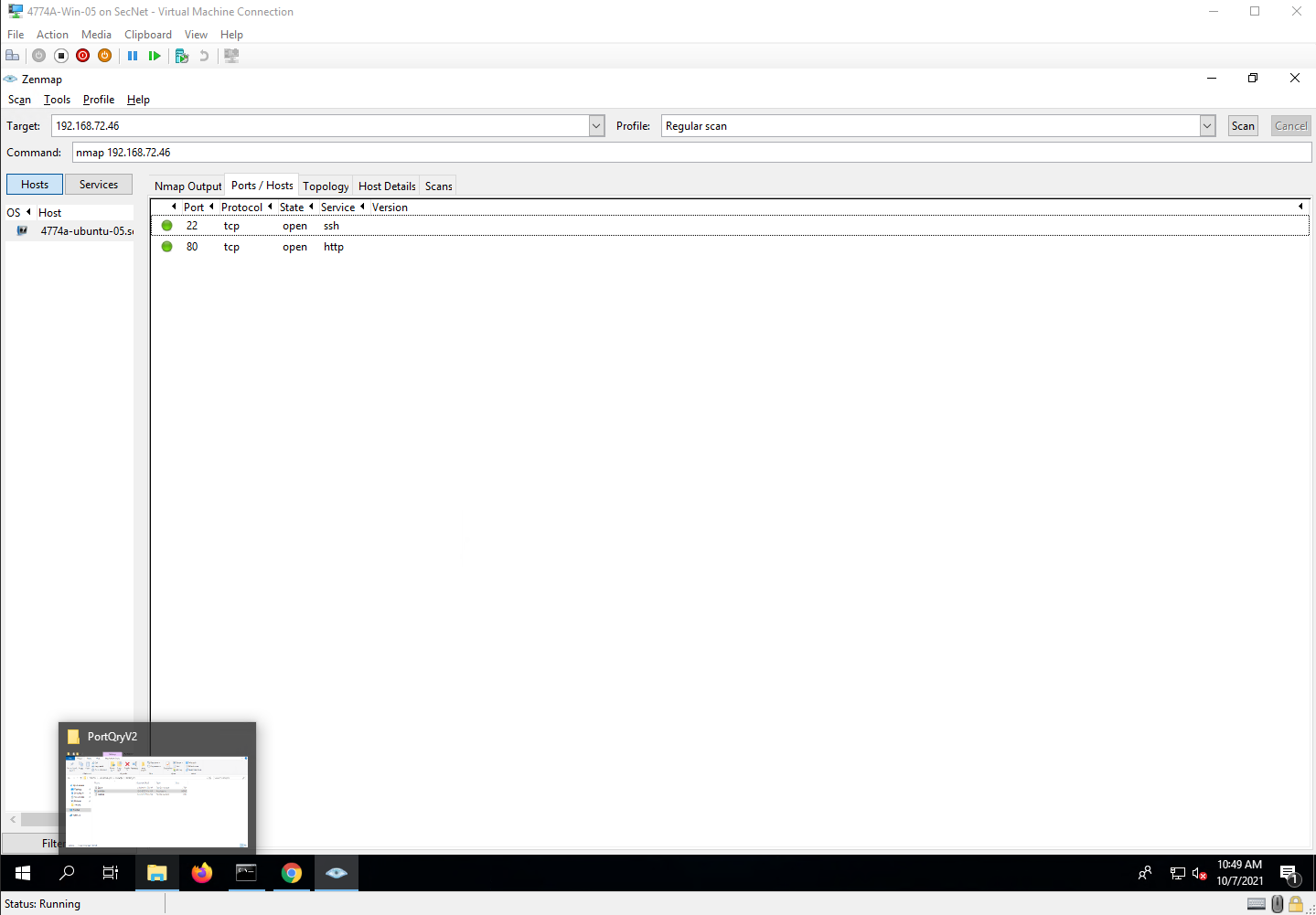
Step 12



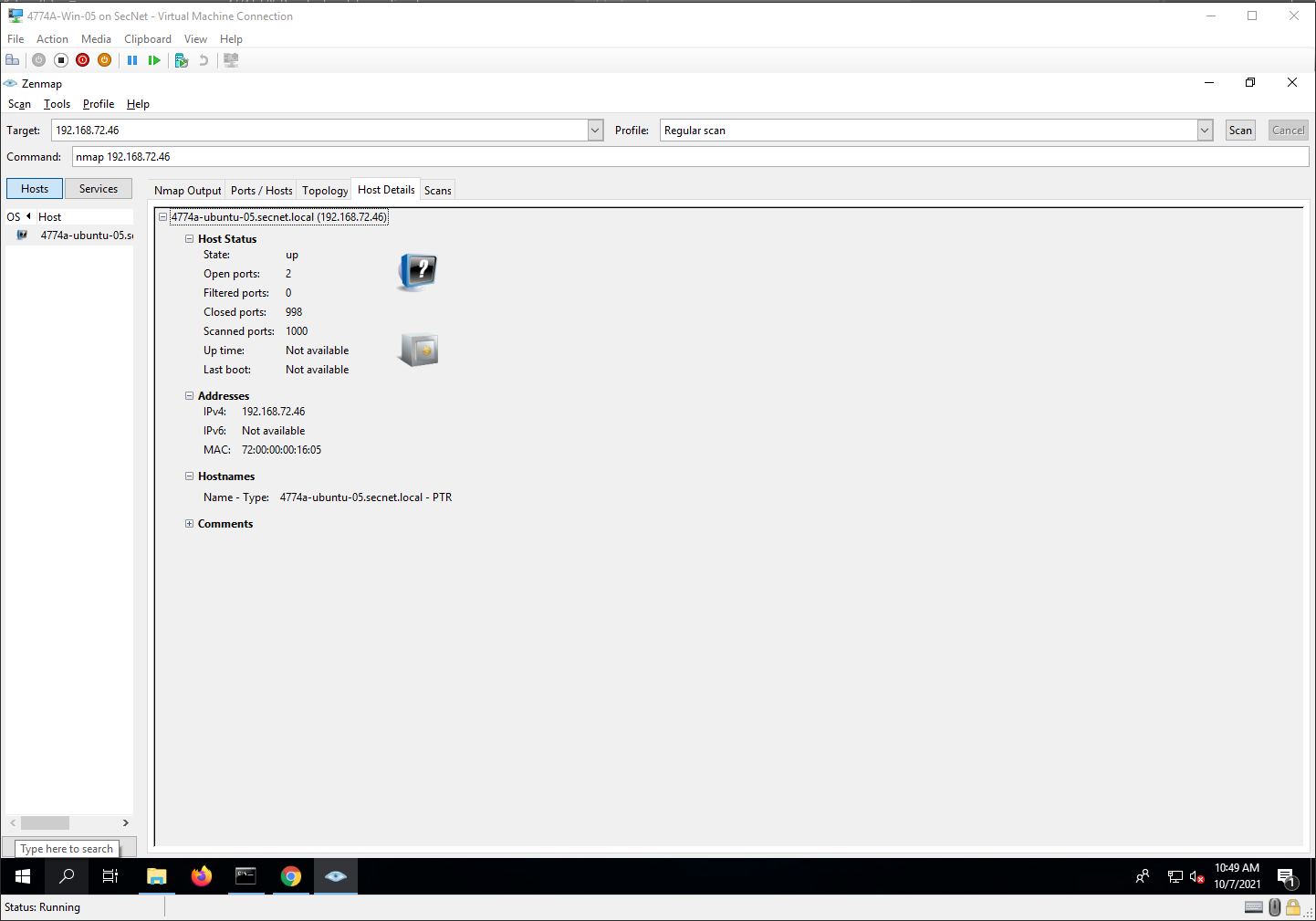
Step 16



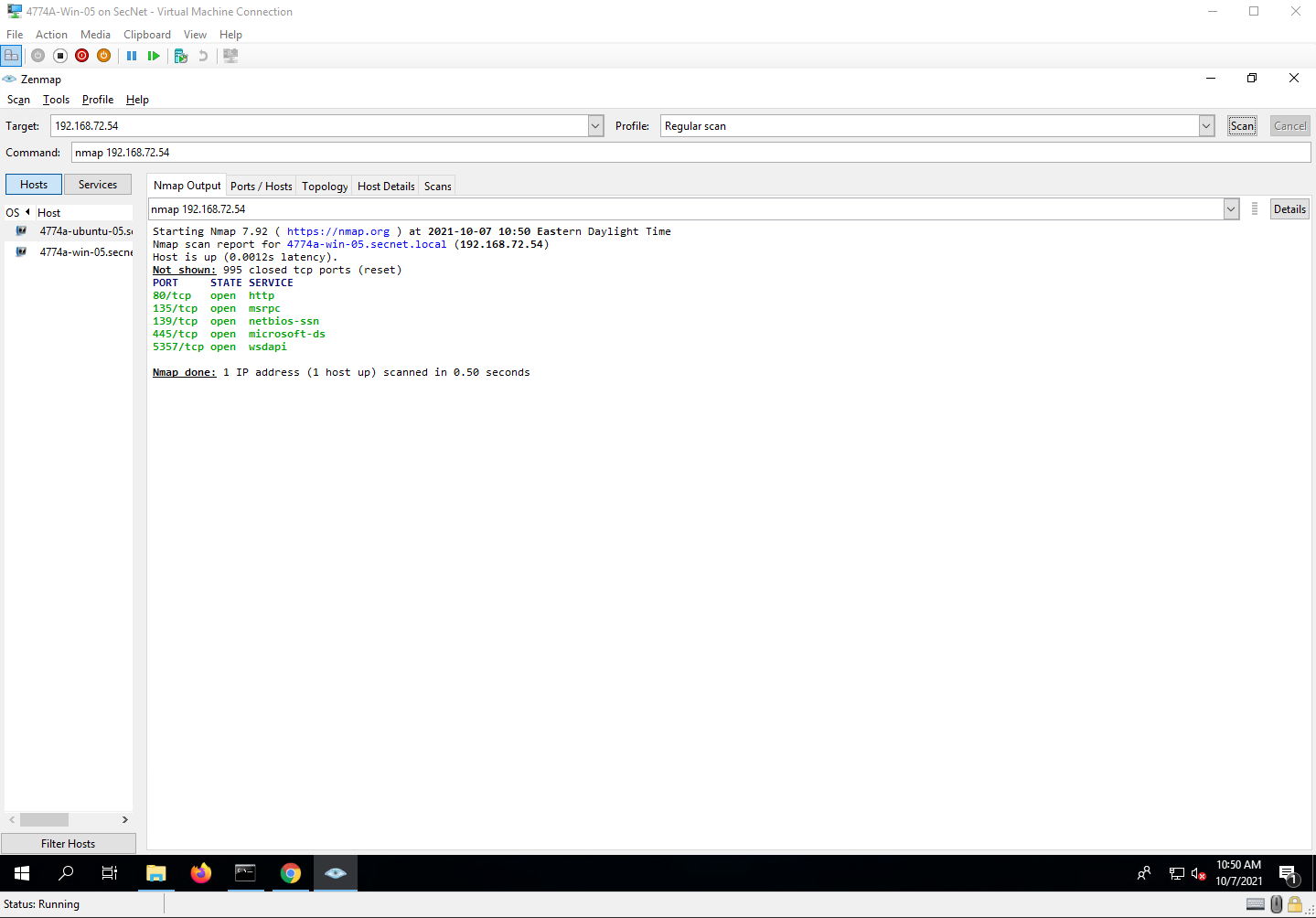
Step 18



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

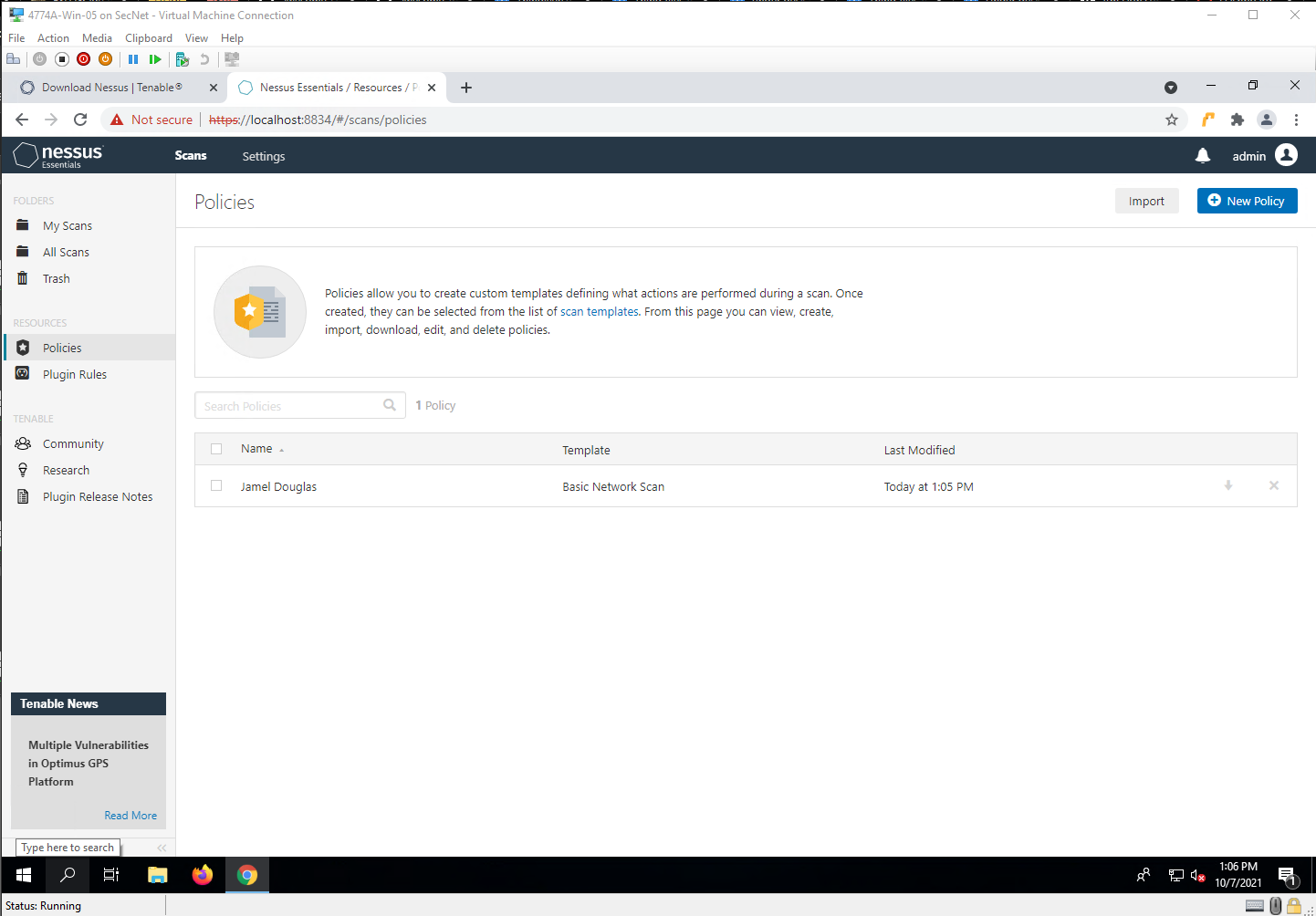
Thought Questions

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 webservers.
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

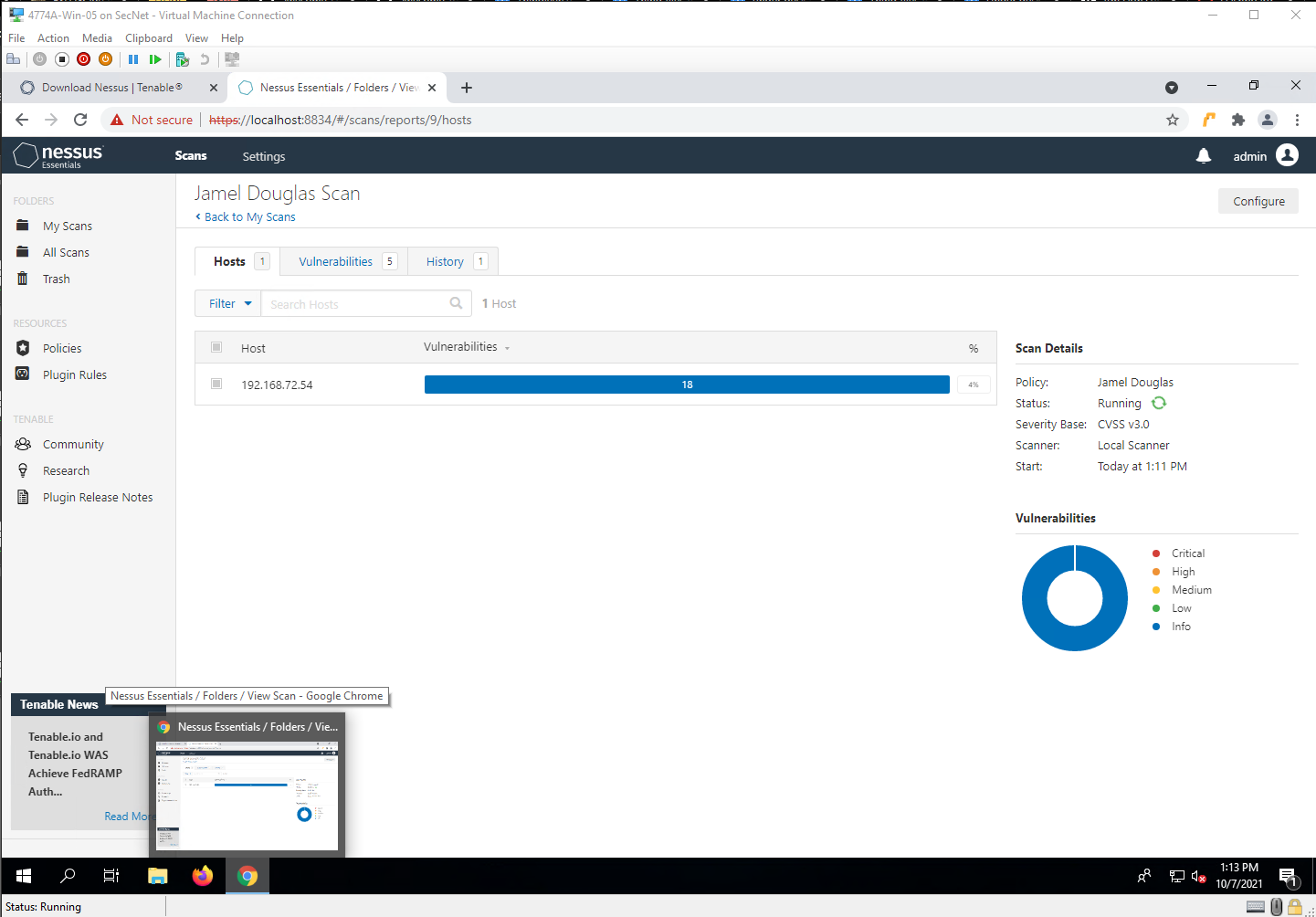
4 Nessus

Screenshots

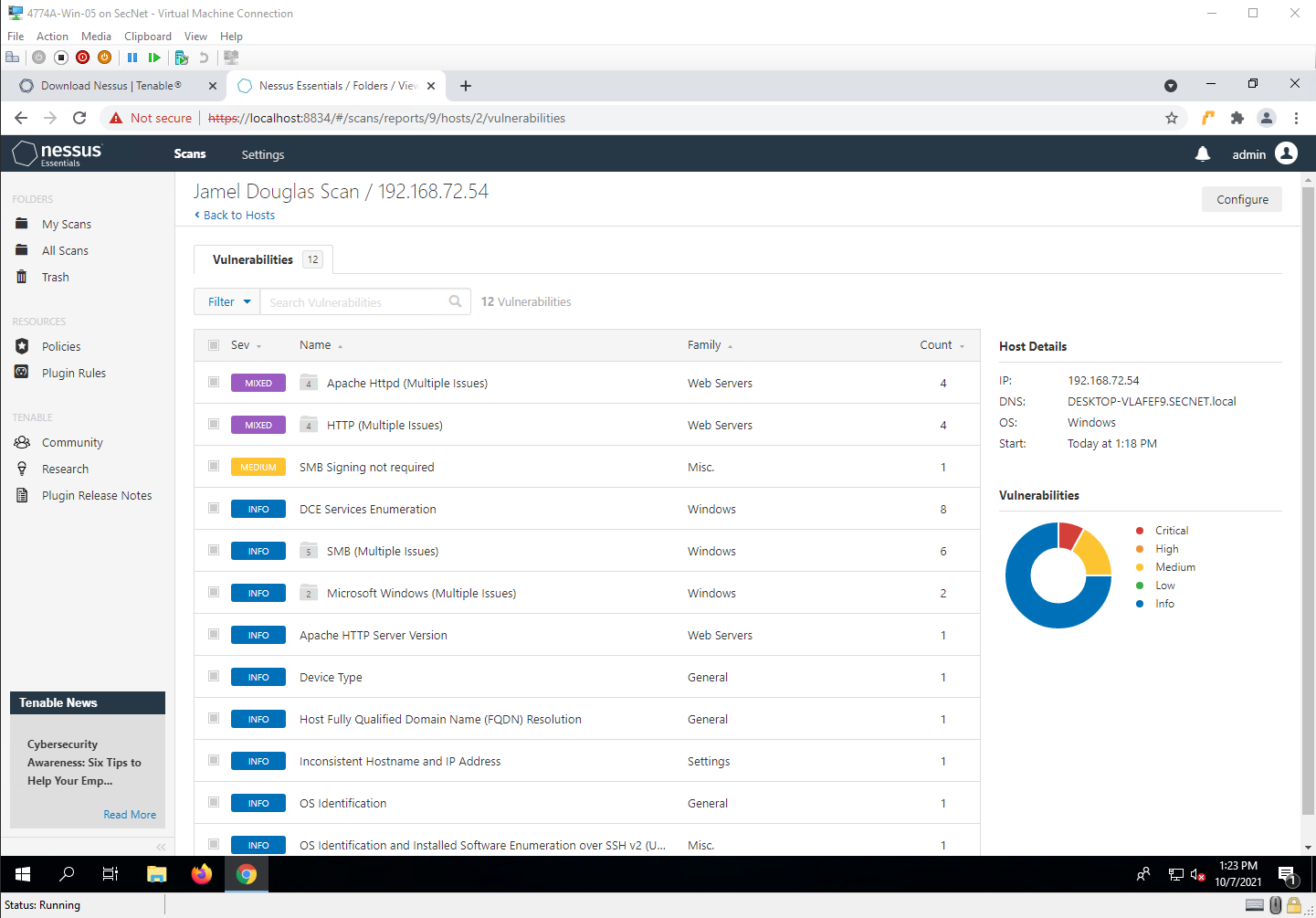
Step 28



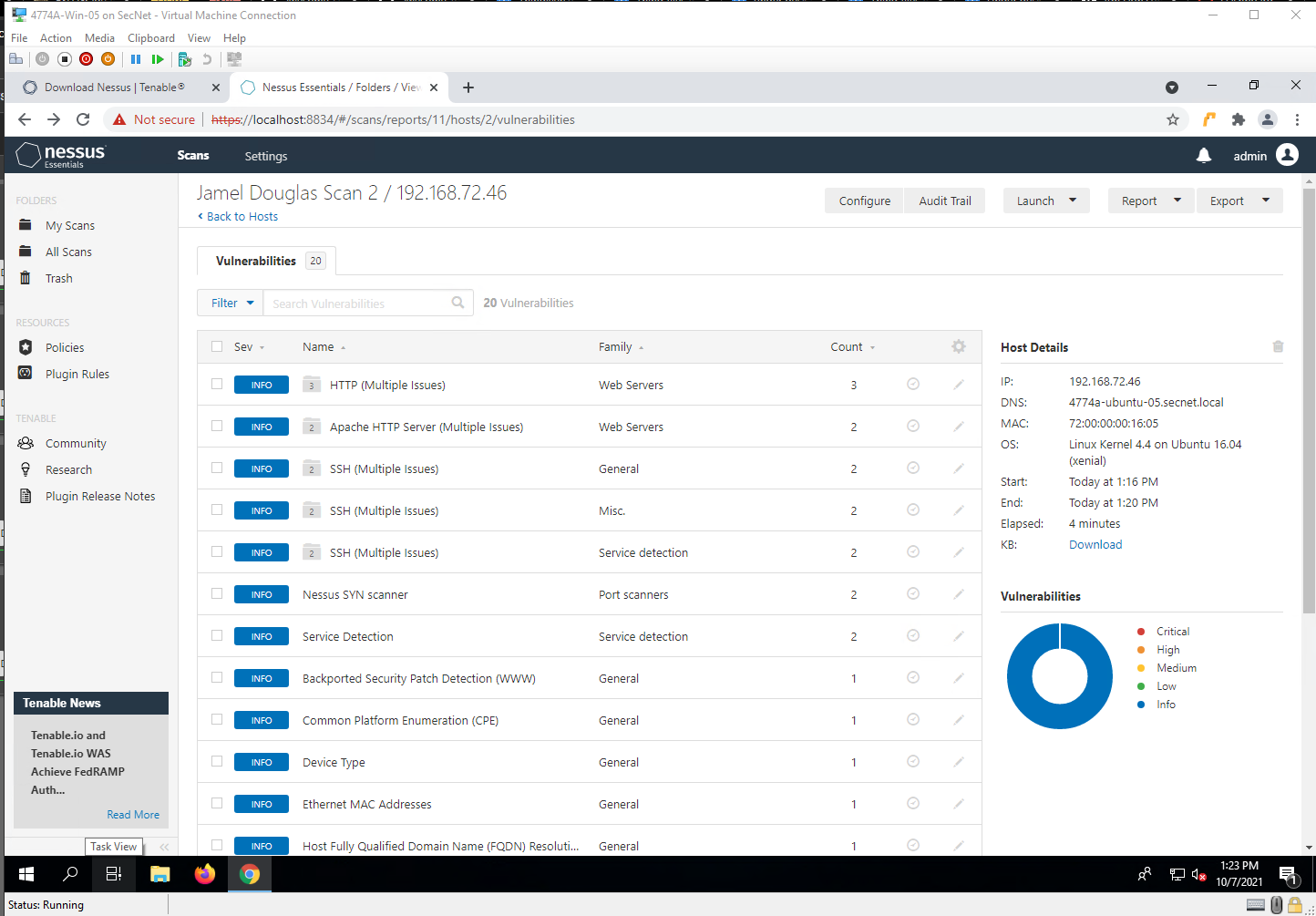
Step 37



Step 39



Step 42



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.