Name: Cristian Barreno

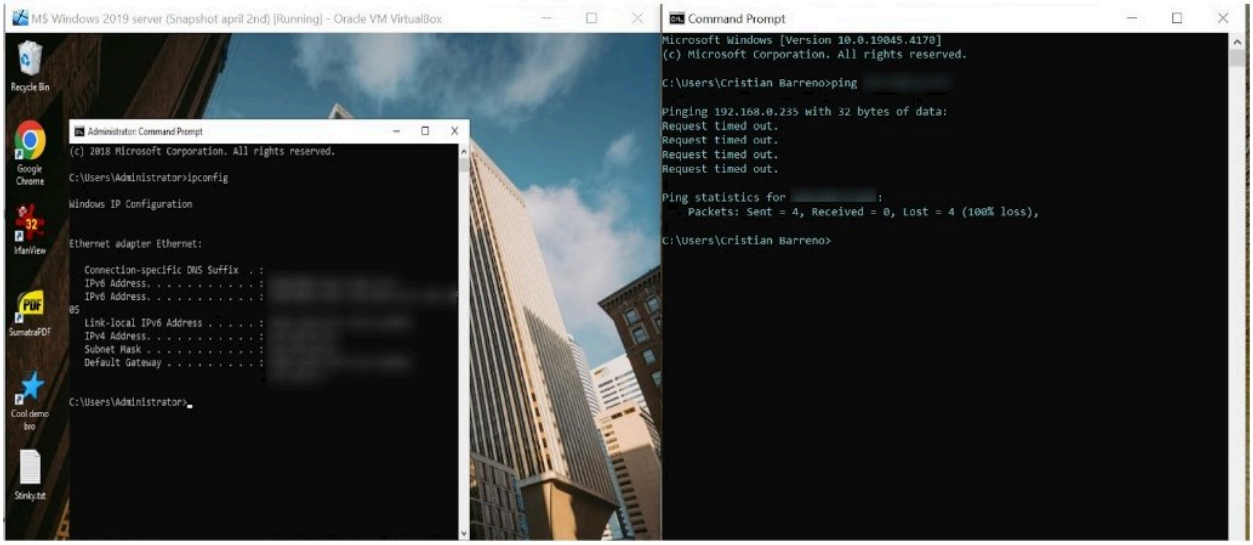
Incident Response exercises - Third group

Prerequisites

- Windows 2019 Server
- Linux Ubuntu 22.04 Server

Exercise 1 - Windows Server Firewall

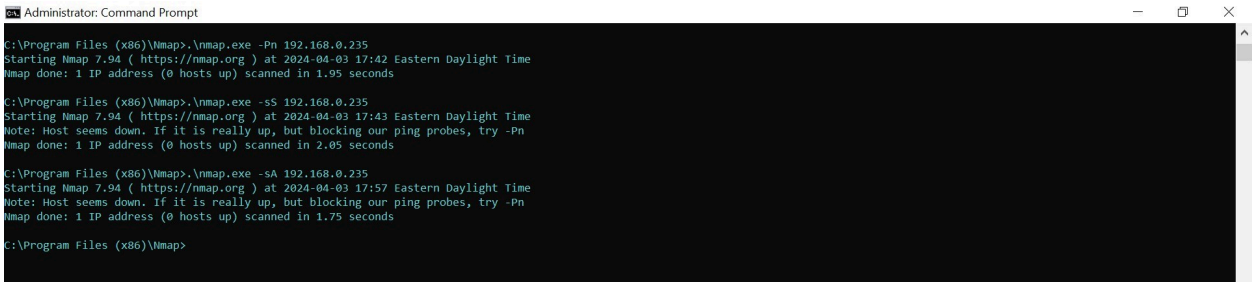
Task 1



On the right screen I ping my guest OS, and because ICMP is disabled, I'm not able to ping it. Turning off ICMP is a security measure, so threat actors don't perform reconnaissance on your network.

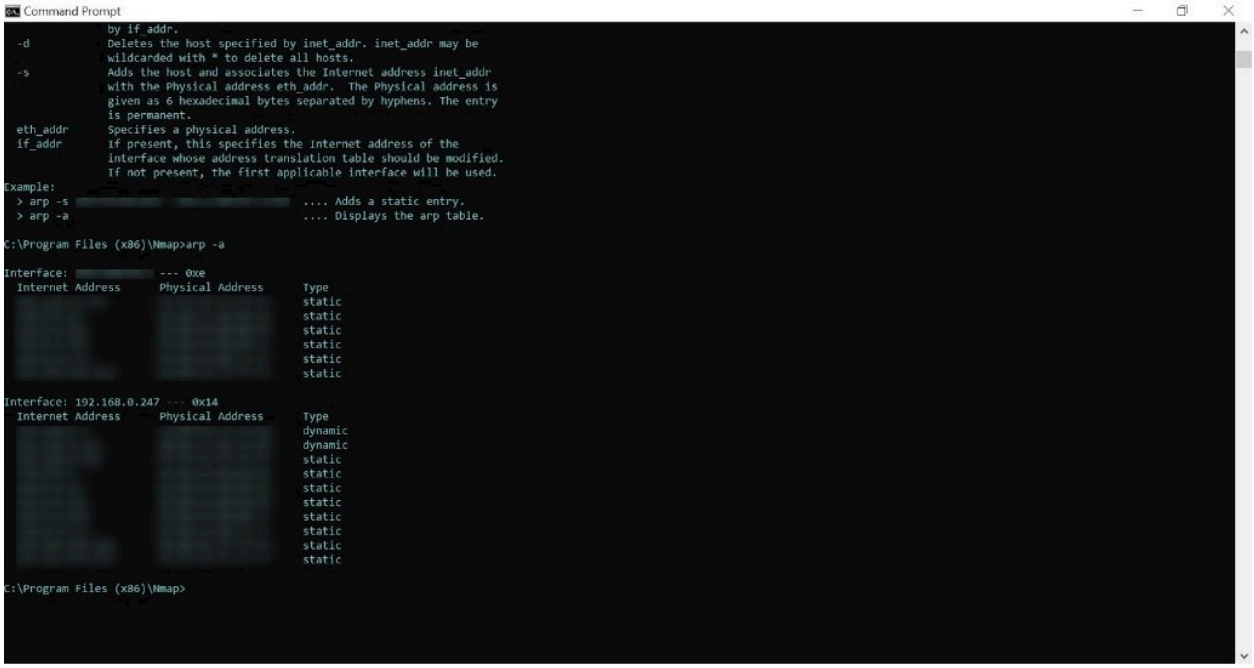
Task 2

1. **NMAP with 3 different options**



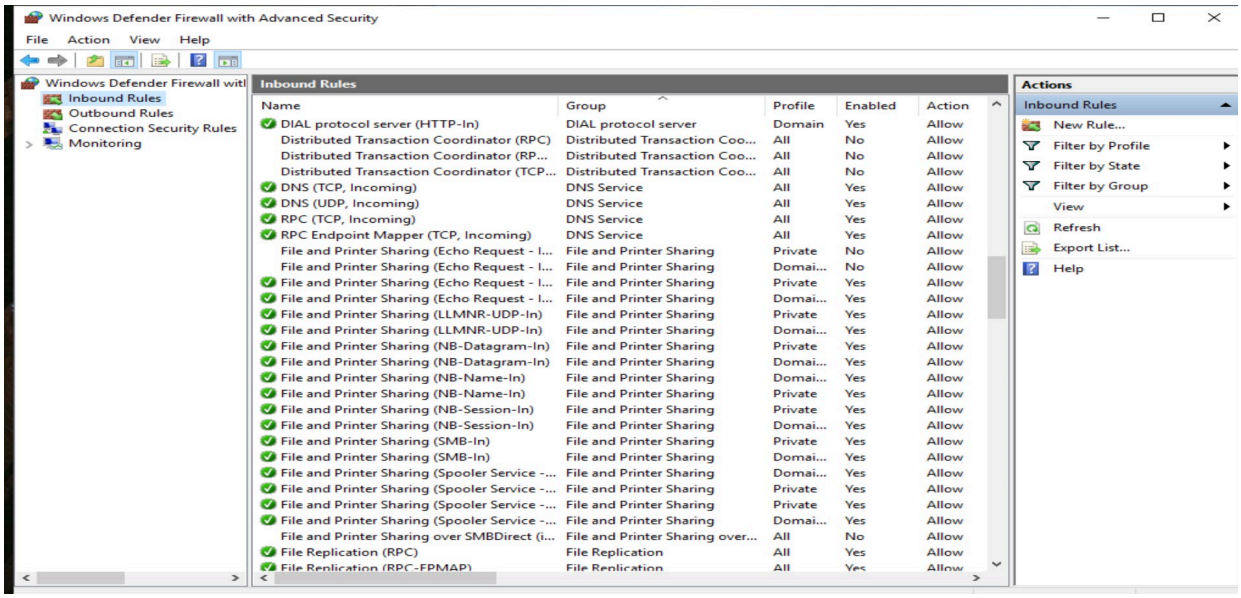
By trying nmap with 3 different flag (-sS, -Pn, -sA) we get a note: “Host seems down”

2. ARP and find your server

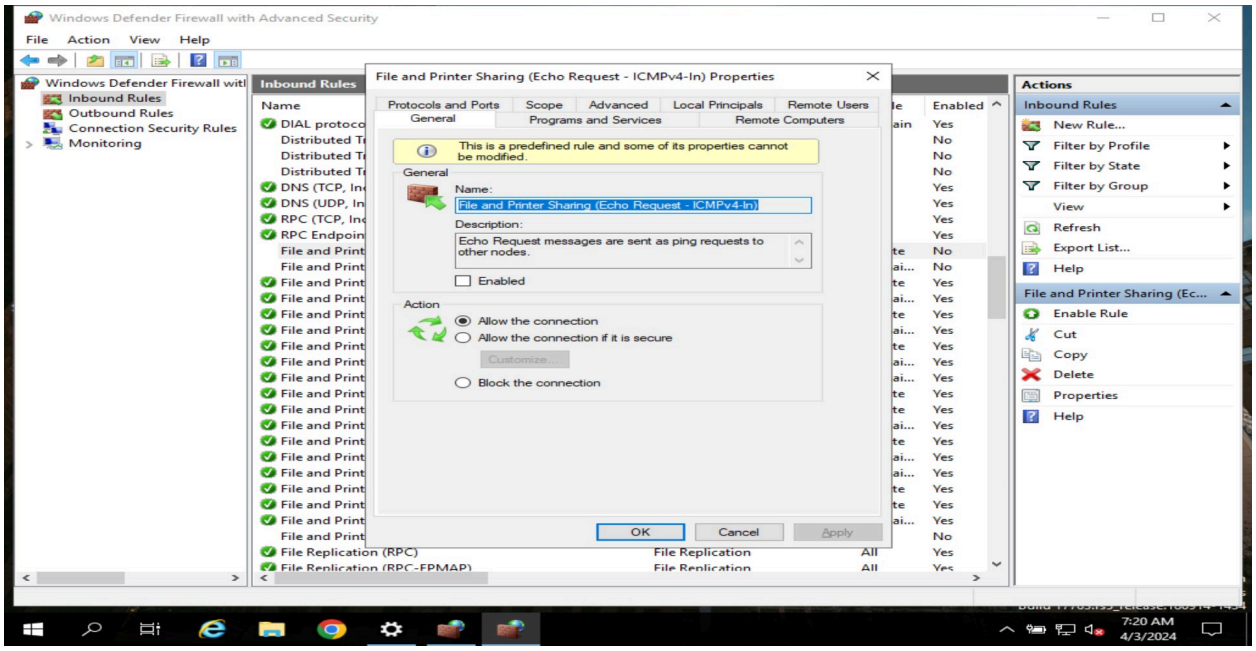


In the screenshot above I used arp -a , and it shows the Address Resolution Protocol table.

Task 3

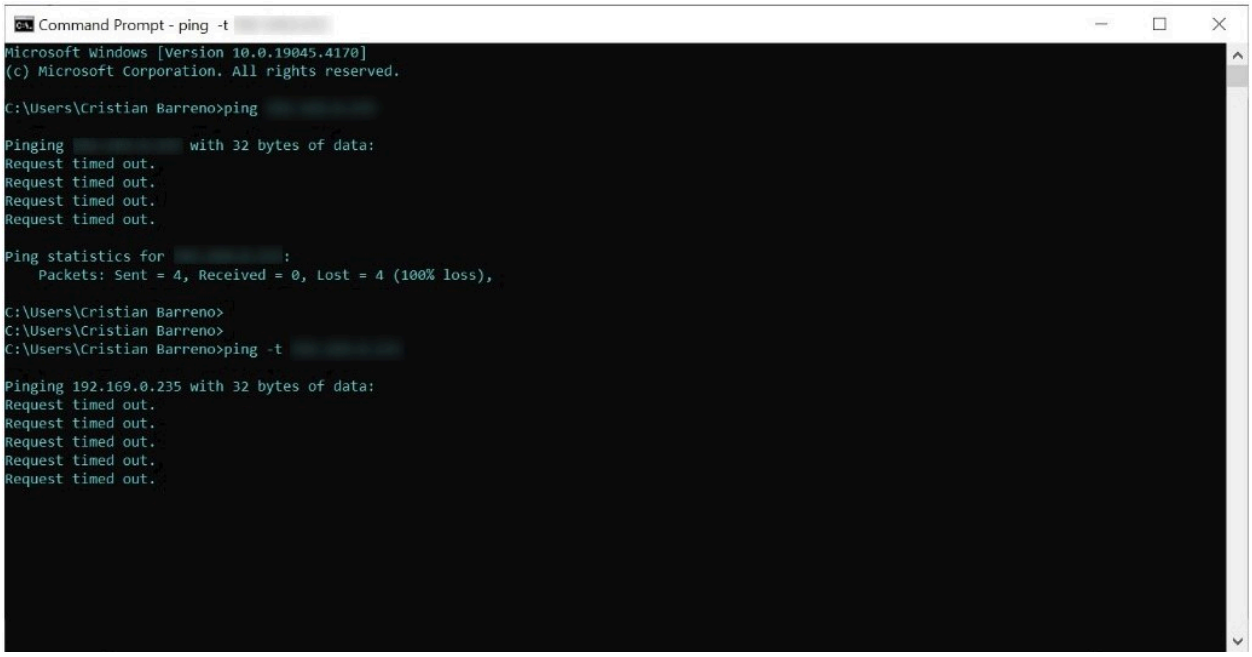


The screenshot above shows the inbound rules of the windows firewall.



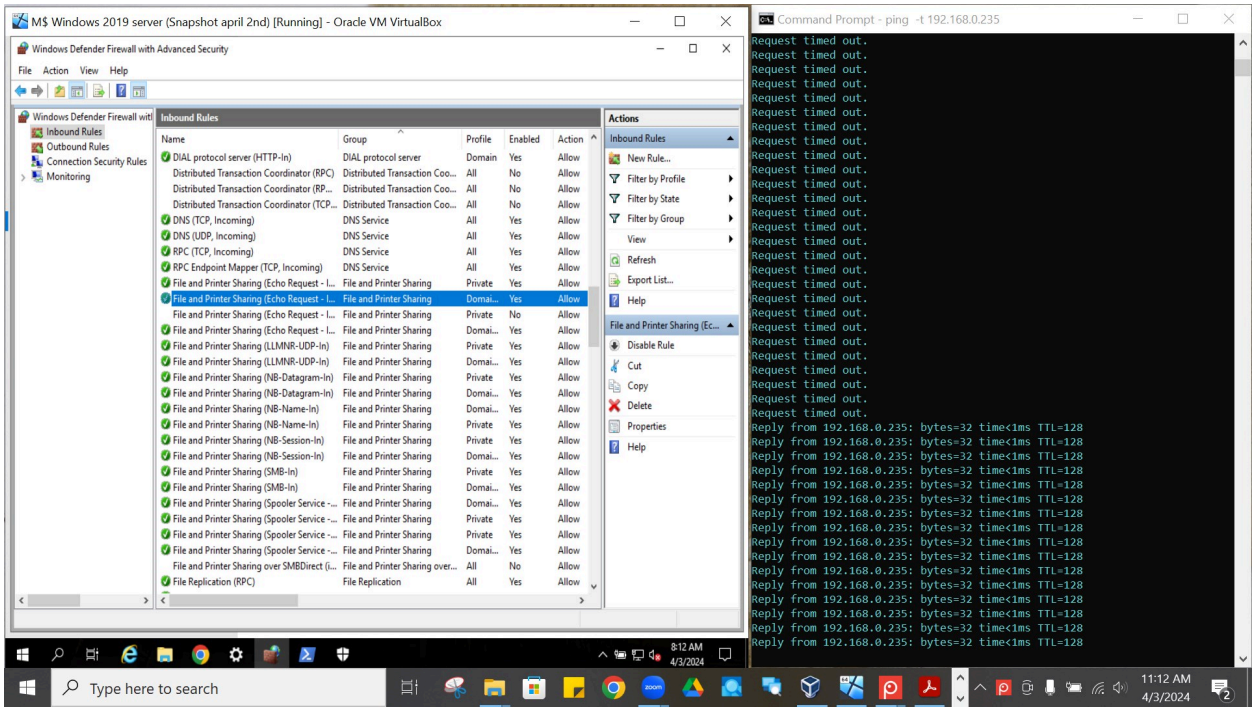
On the screenshot above I opened the firewall rule : “File and Printing Sharing (Echo Request -ICMPv3-In)”. The description tells us about the rule. This rule is not enabled.

Task 4



Ping with the option -t pings the specific host until stopped.

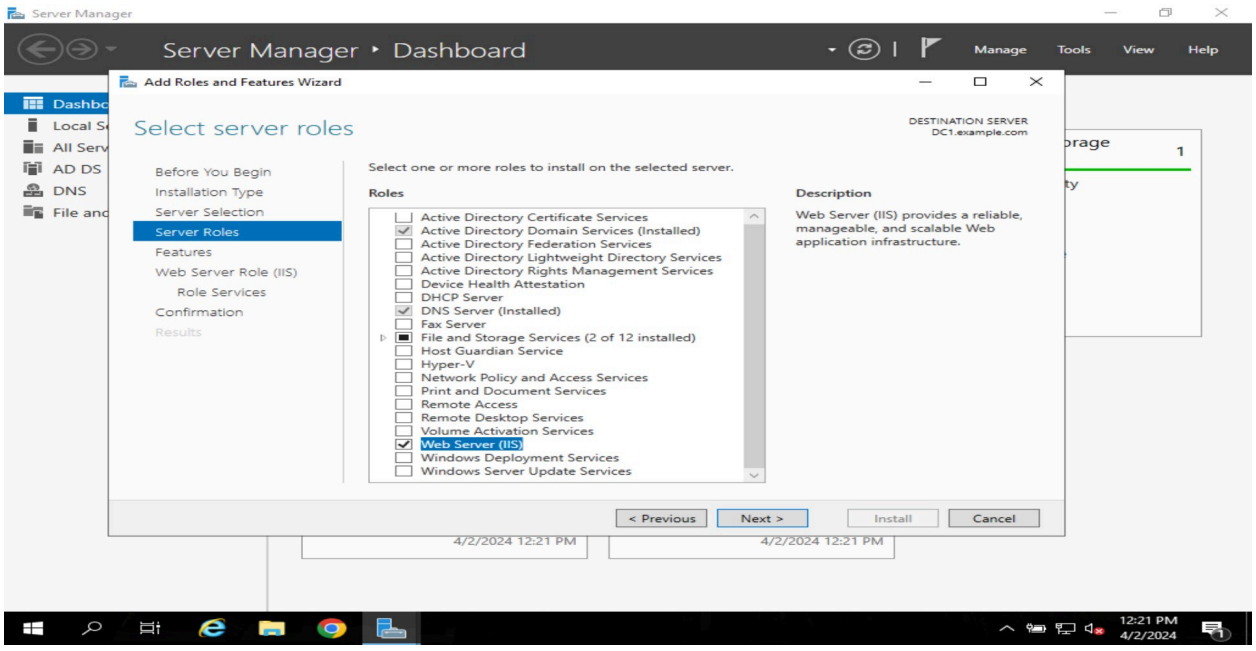
Task 5



In the screenshot above, I enabled the firewall rule, and right away on the command prompt window I can see the ICMP streaming working.

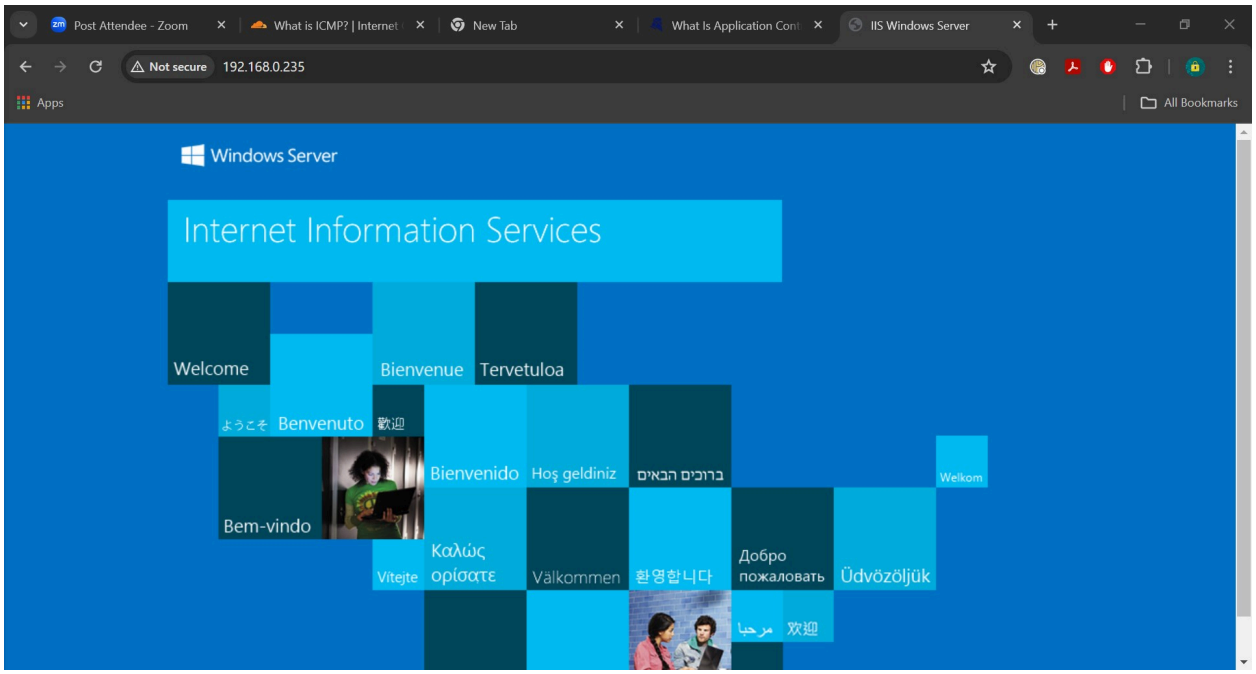
Exercise 2 - Windows Server Firewall - Internet Information Server

Task 1



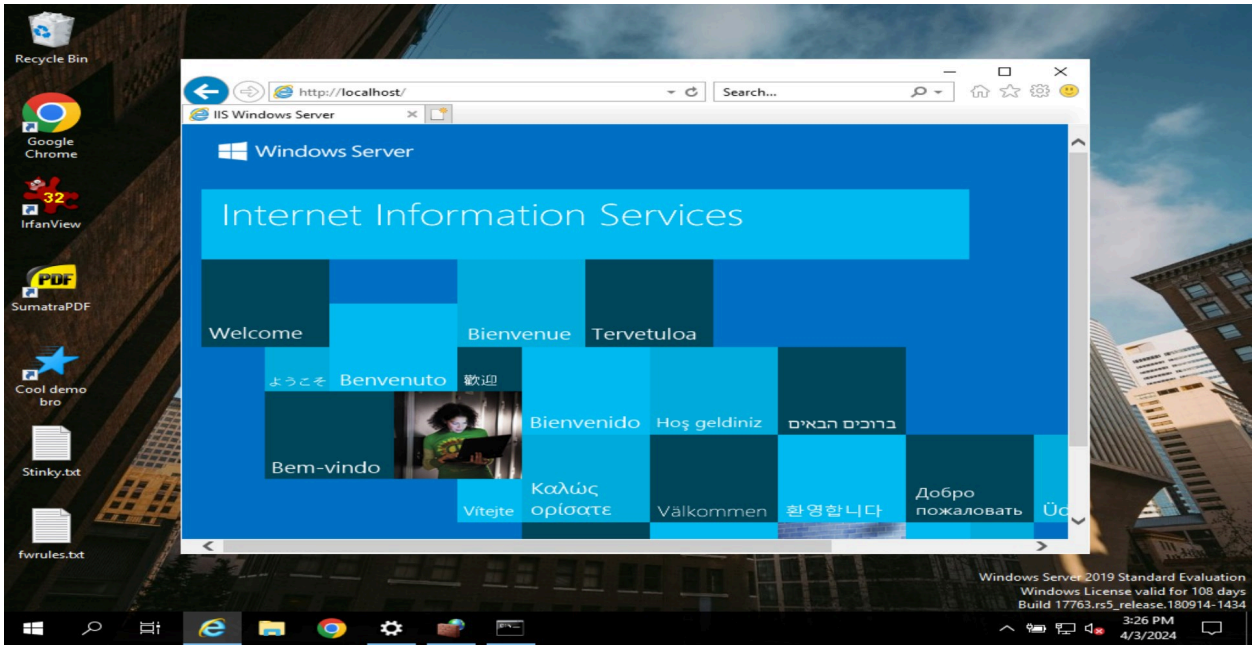
The screenshot above shows the process of installing Internet Information Server on Windows. ISS is a multi-purpose web server to deploying and managing web-based applications.

Task 2



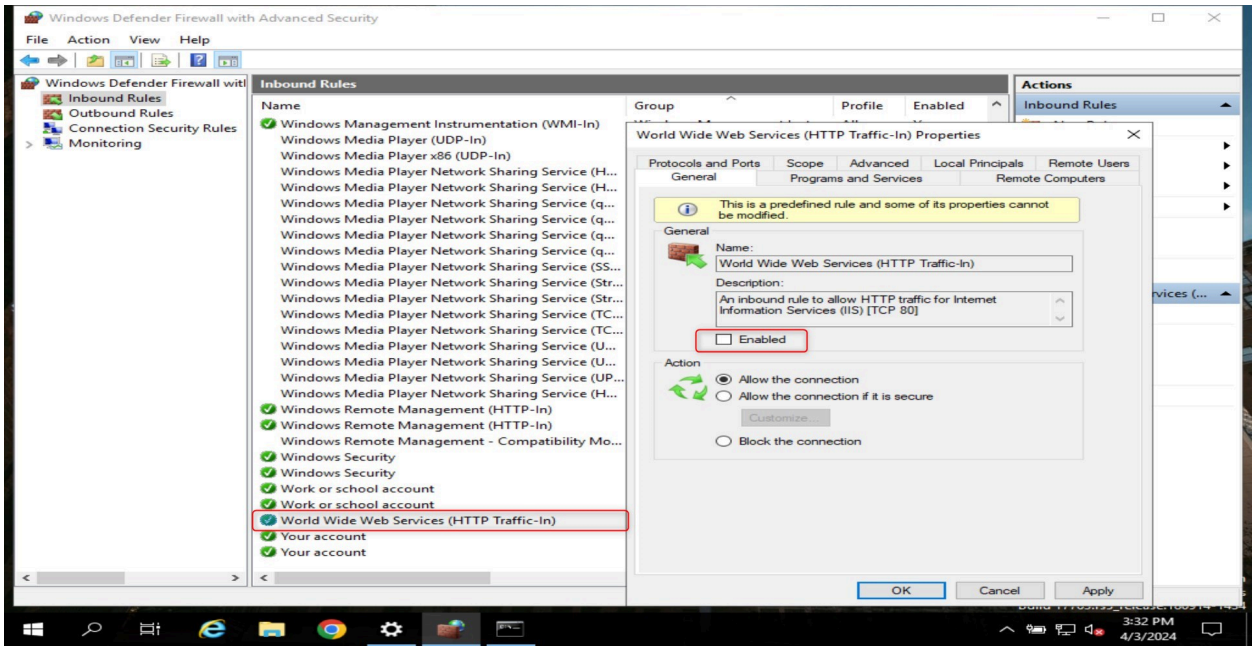
After it finished installing, open a web browser window on your host OS, and enter the IP address of your guest OS. press enter and you will get the web page.

Task 3



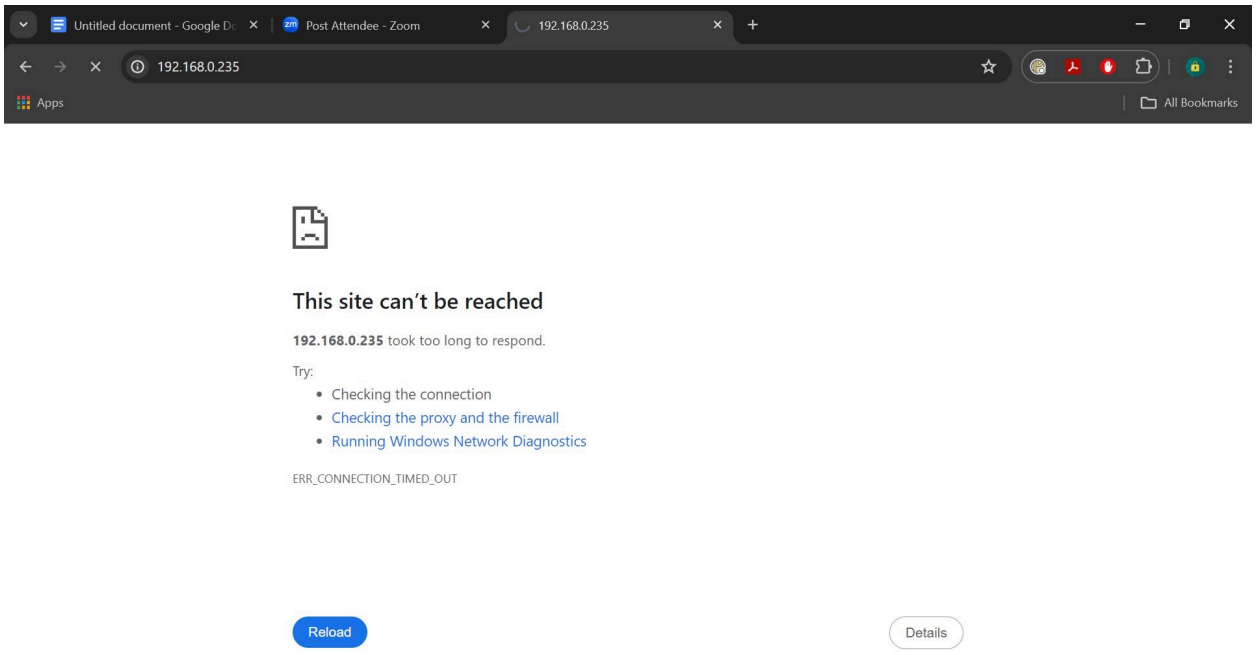
You can also open the Internet Information Server on your guest OS.

Task 4



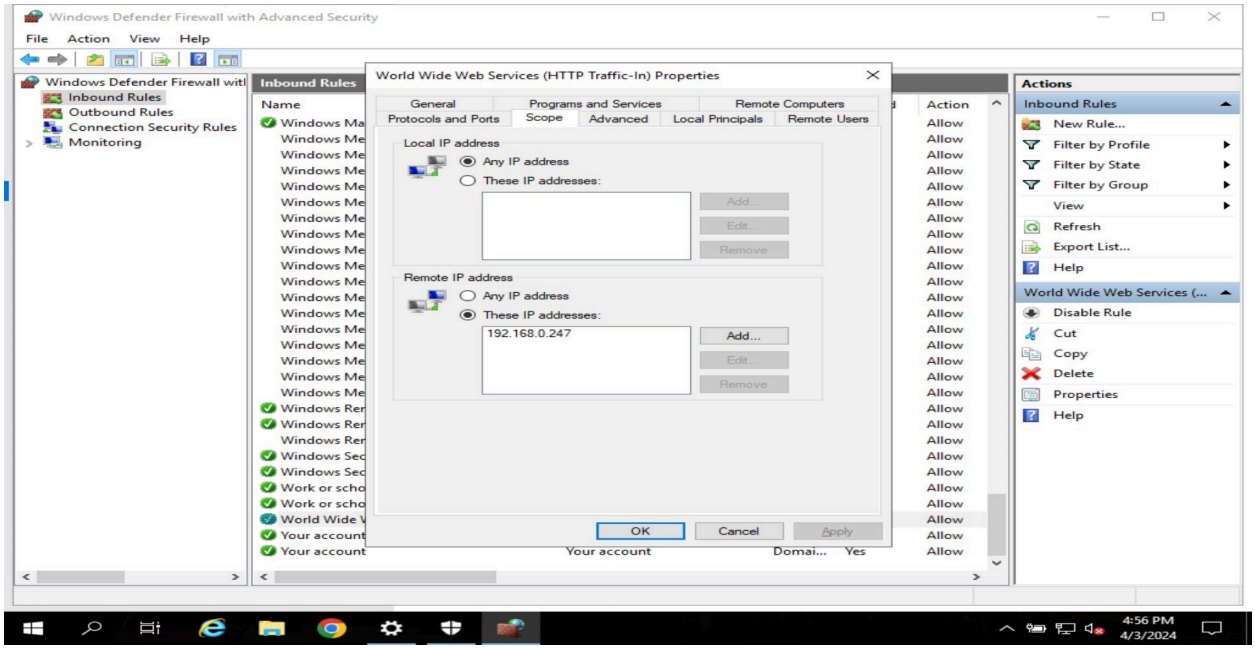
From the firewall inbound rules I'm able to control World Wide Web services, and disable it on my system.

Task 5



If I refresh the web page, I get a “This site cant be reached” message because we disabled WWW services.

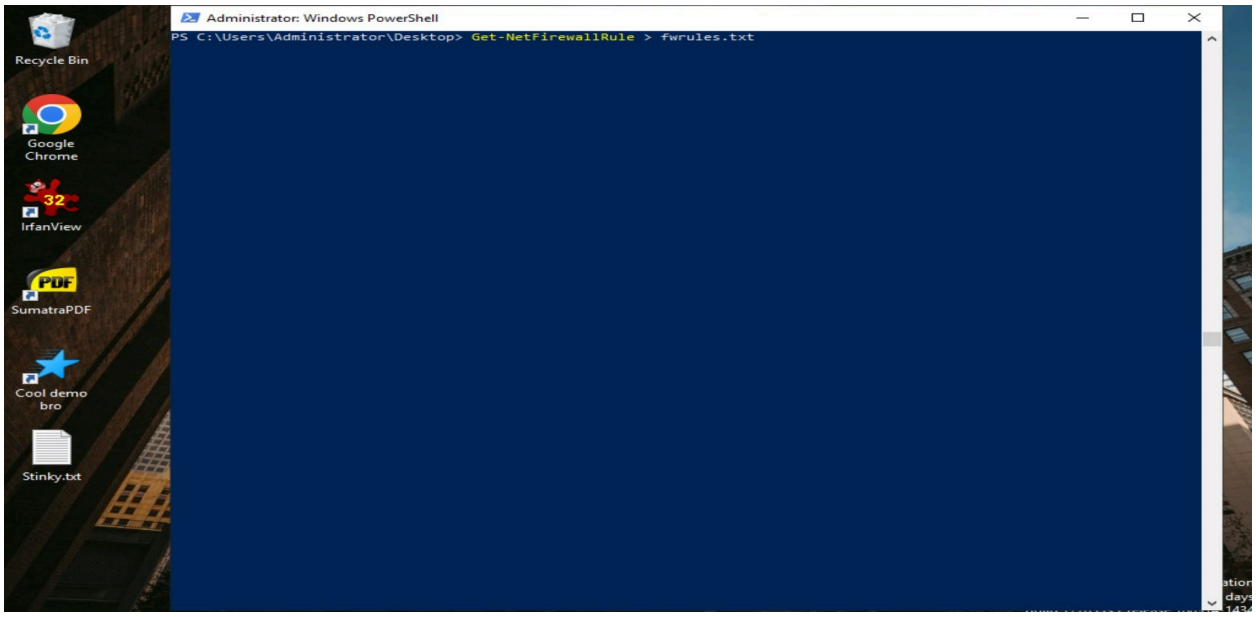
Task 6



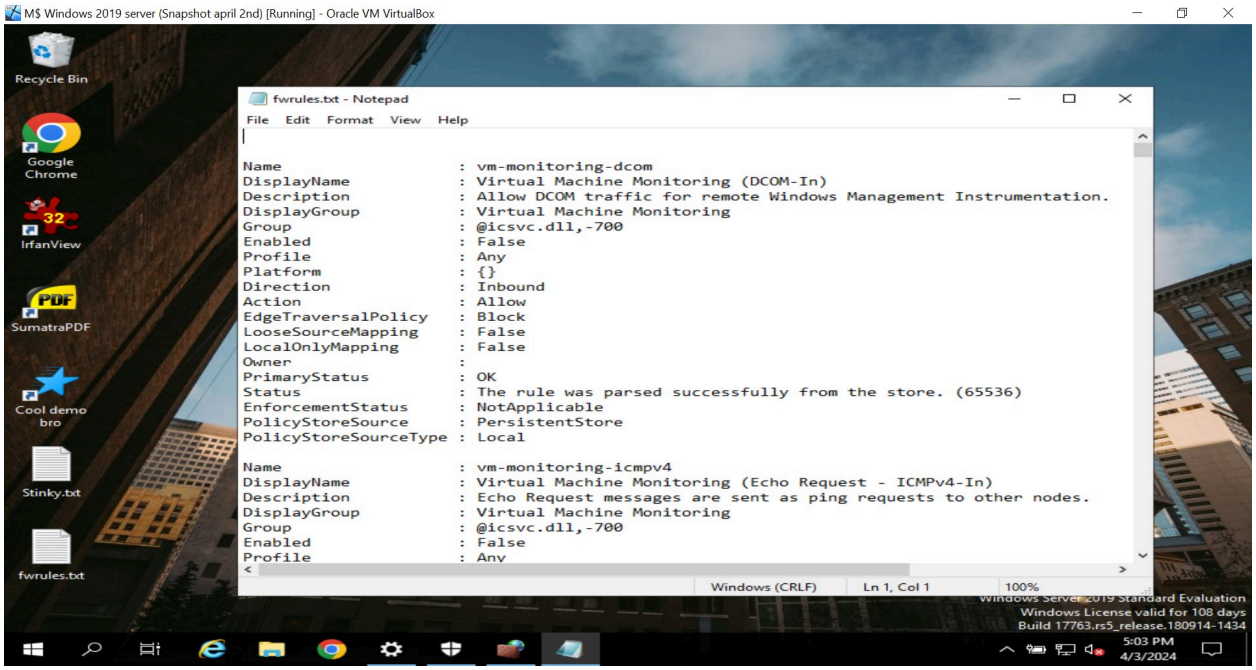
By inserting the Host IP address on the remote IP address section, and then trying to login from someone else's computer you won't be successful. Only your Host OS can access it.

Exercise 3

Task 1

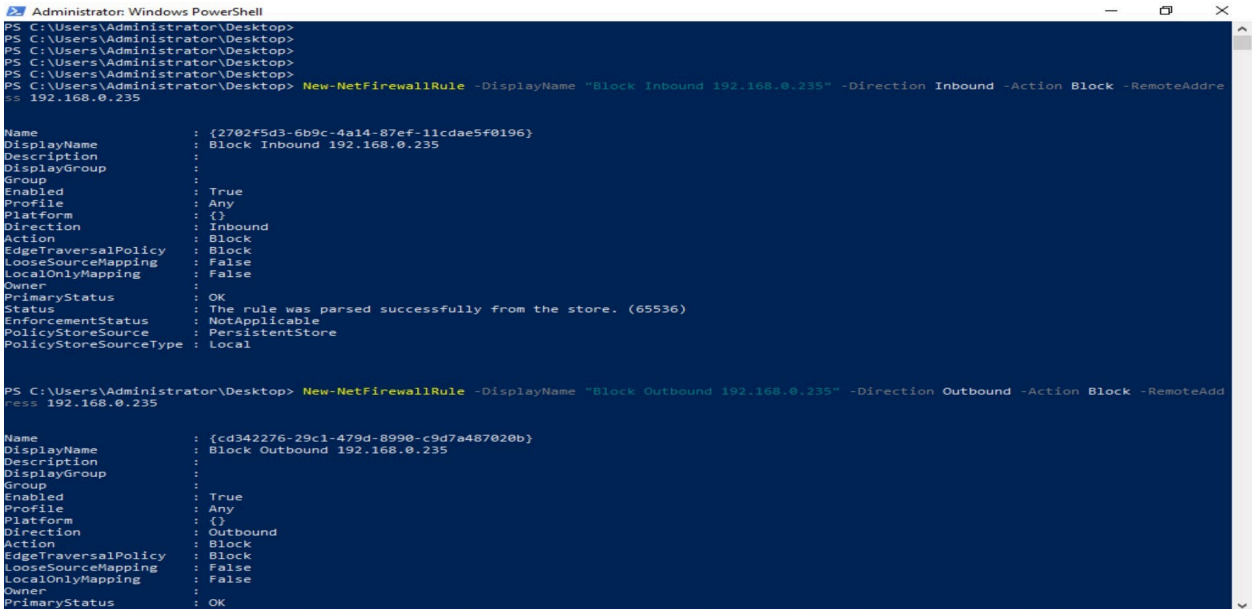


I redirected the output of Get-NetFirewallRule to a text file.



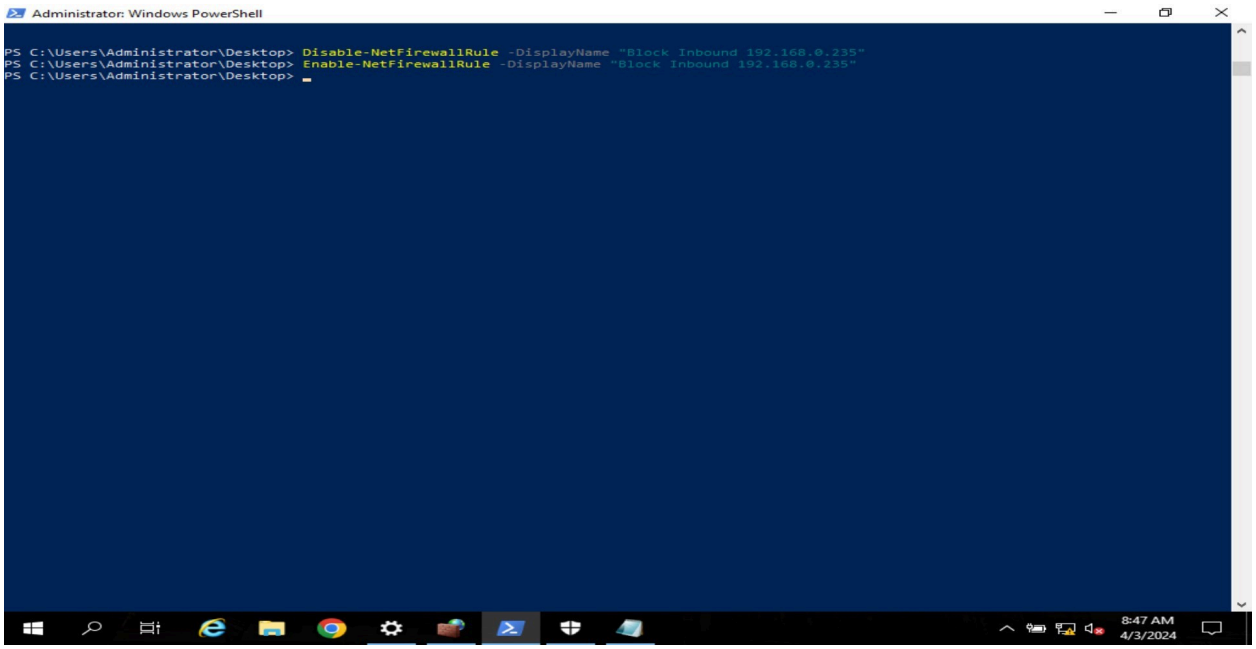
Get- NetFirewallRule is used to view existing firewall rules. In the screenshot above we can see the content of fwrules.txt

Task 2



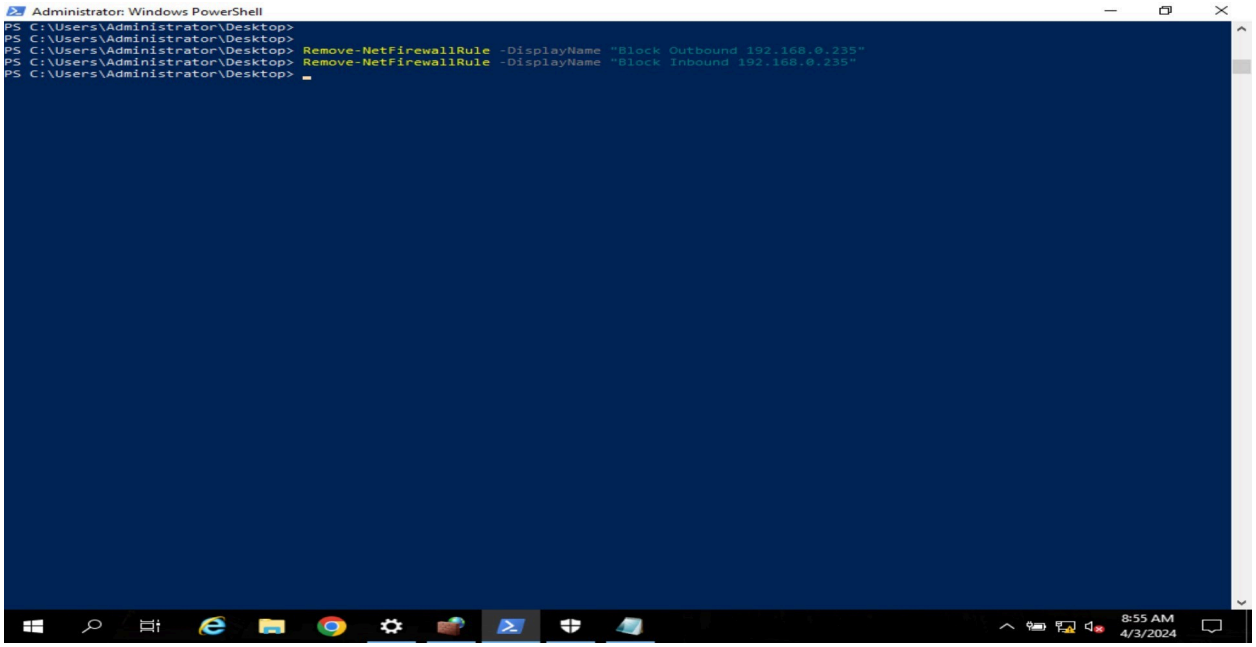
We can block inbound or outbound traffic from a specific IP address using powershell.

Task 3



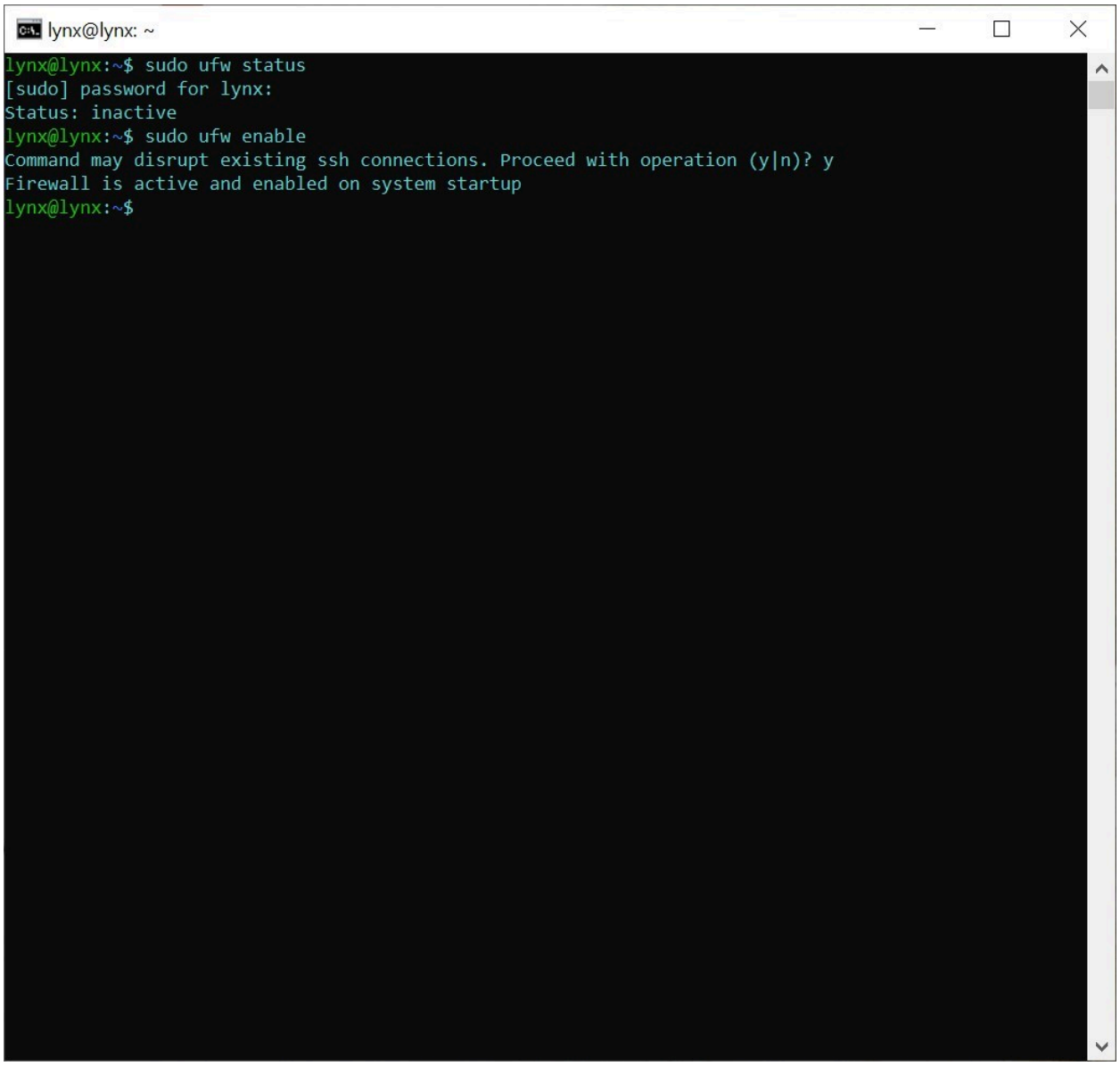
I'm also able to disable or enable firewall rules from powershell.

Task 4



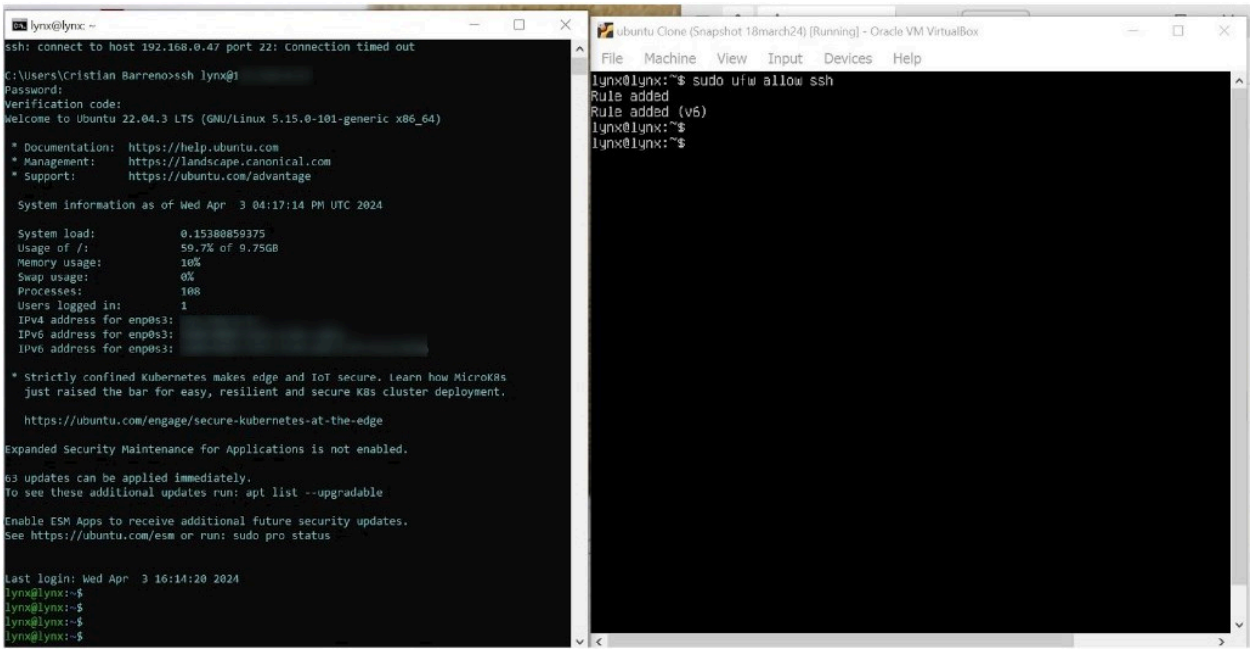
I'm also able to easily remove firewall rules from powershell.

Exercise 4
Task 1



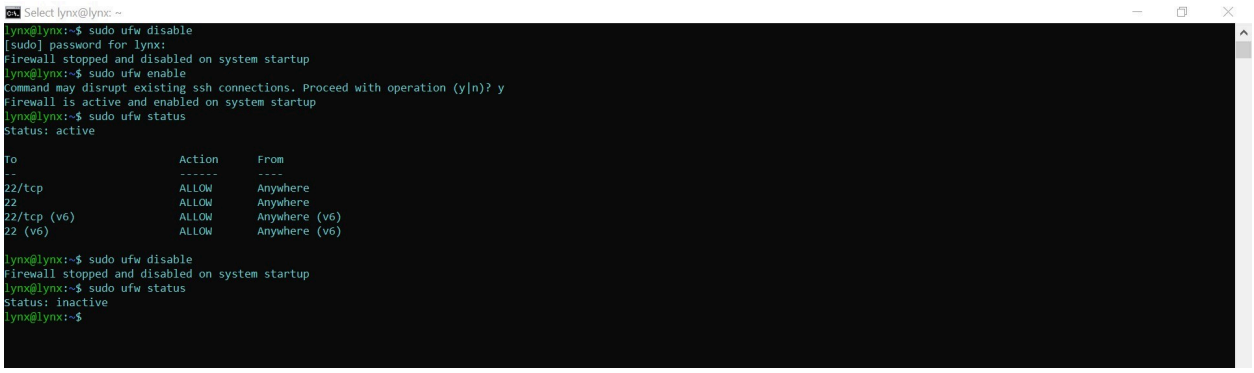
I entered sudo ufw status, and it shows inactive. We are able to enable it by entering sudo ufw enable. After we reconnect via ssh we are not able to connect because we didn't set up any access rules.

Task 2

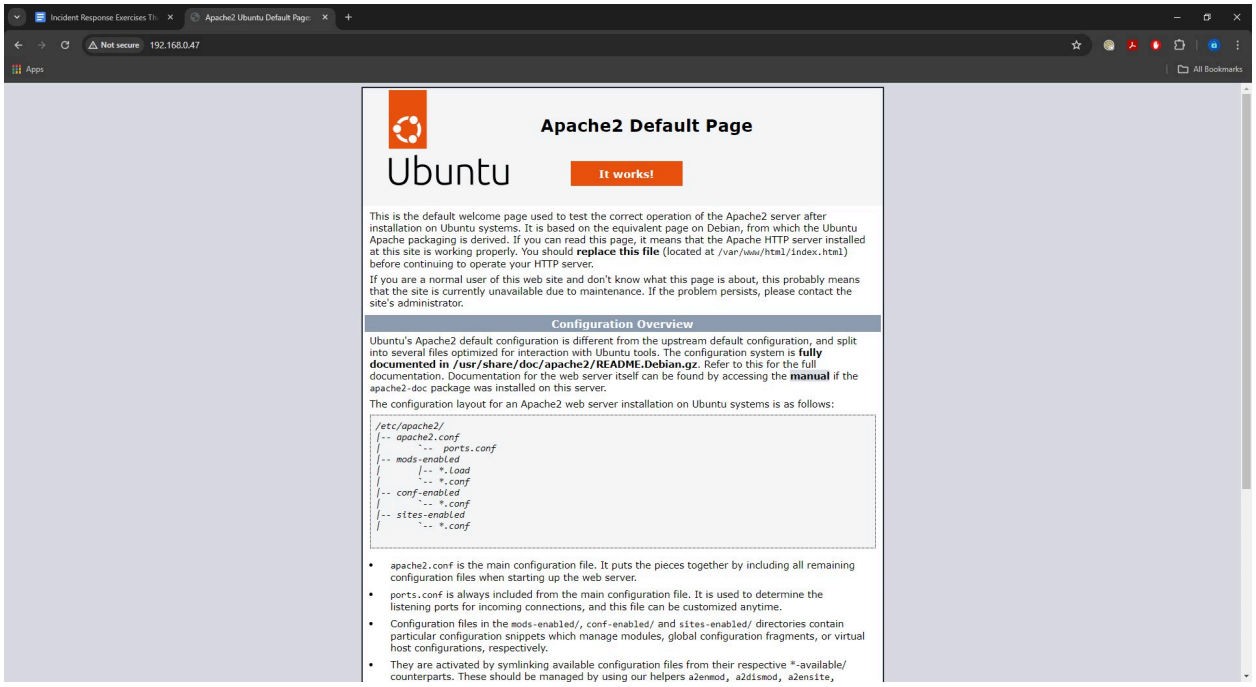


In the screenshot above I modified the ufw to allow ssh traffic. Once I left the ssh session, and tried to reconnect, I wasn't able to do it because we haven't set up a firewall rule.

Task 3



We can enable and disable the firewall with sudo ufw disable, and sudo ufw enable.



We can open a browser and turn on and off the firewall to see that it works.

Task 4

We can specify a rule to allow http traffic with sudo ufw allow http

Task 5

We can create a specific rule to allow http traffic only from a range of addresses by using sudo ufw allow <your network ID>/< CIDR> to any port 80

We can validate by looking at the apache web server. Also to show the ufw configuration we use:

Sudo ufw status