

Name: Cristian Barreno

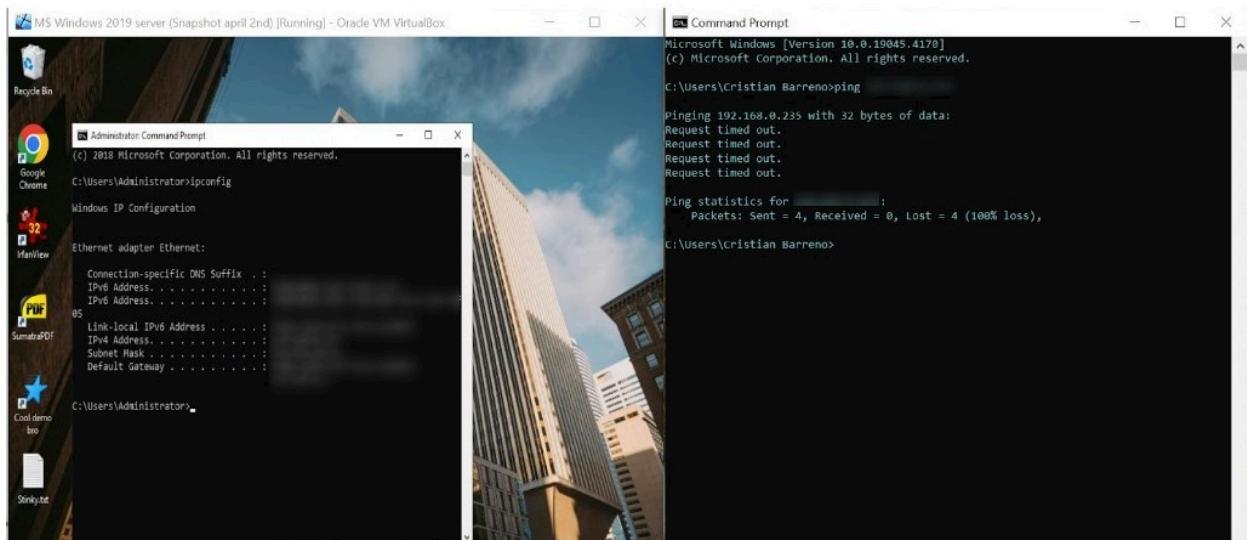
Incident Response exercises - Third group

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

```
C:\> Administrator: Command Prompt
C:\Program Files (x86)\Nmap>.\nmap.exe -Pn 192.168.0.235
Starting Nmap 7.94 ( https://nmap.org ) at 2024-04-03 17:42 Eastern Daylight Time
Nmap done: 1 IP address (0 hosts up) scanned in 1.95 seconds

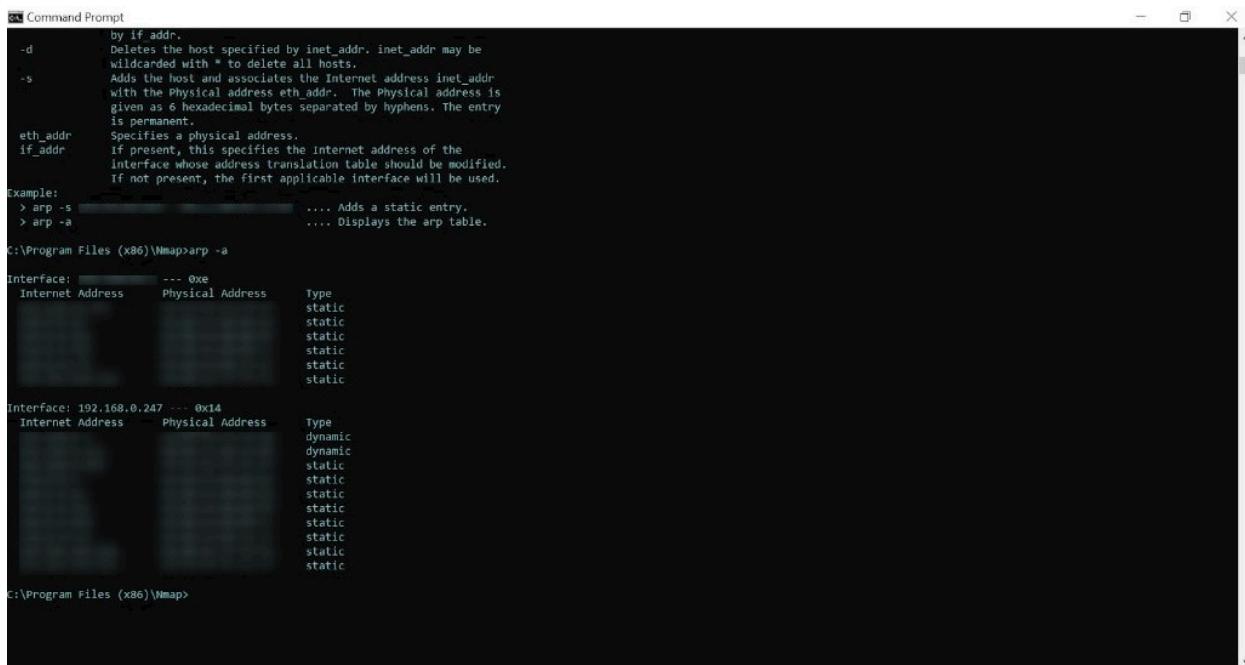
C:\Program Files (x86)\Nmap>.\nmap.exe -sS 192.168.0.235
Starting Nmap 7.94 ( https://nmap.org ) at 2024-04-03 17:43 Eastern Daylight Time
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 2.05 seconds

C:\Program Files (x86)\Nmap>.\nmap.exe -sA 192.168.0.235
Starting Nmap 7.94 ( https://nmap.org ) at 2024-04-03 17:57 Eastern Daylight Time
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 1.75 seconds

C:\Program Files (x86)\Nmap>
```

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

2. ARP and find your server



The screenshot shows a Windows Command Prompt window titled "Command Prompt". It displays the output of the "arp -a" command. The output lists two network interfaces: one with a static IP of 192.168.0.247 and another with a dynamic IP of 192.168.0.247. For each interface, it shows the Internet Address, Physical Address, and Type (static or dynamic). The "Type" column shows several entries for each interface, indicating multiple static entries for each.

```
by if addr.
-d Deletes the host specified by inet_addr. inet_addr may be
wildcarded with * to delete all hosts.
-s Adds the host and associates the Internet address inet_addr
with the Physical address eth_addr. The Physical address is
given as 6 hexadecimal bytes separated by hyphens. The entry
is permanent.
eth_addr Specifies a physical address.
if_addr If present, this specifies the internet address of the
interface whose address translation table should be modified.
If not present, the first applicable interface will be used.

Example:
> arp -s ..... Adds a static entry.
> arp -a ..... Displays the arp table.

C:\Program Files (x86)\Wmap>arp -a

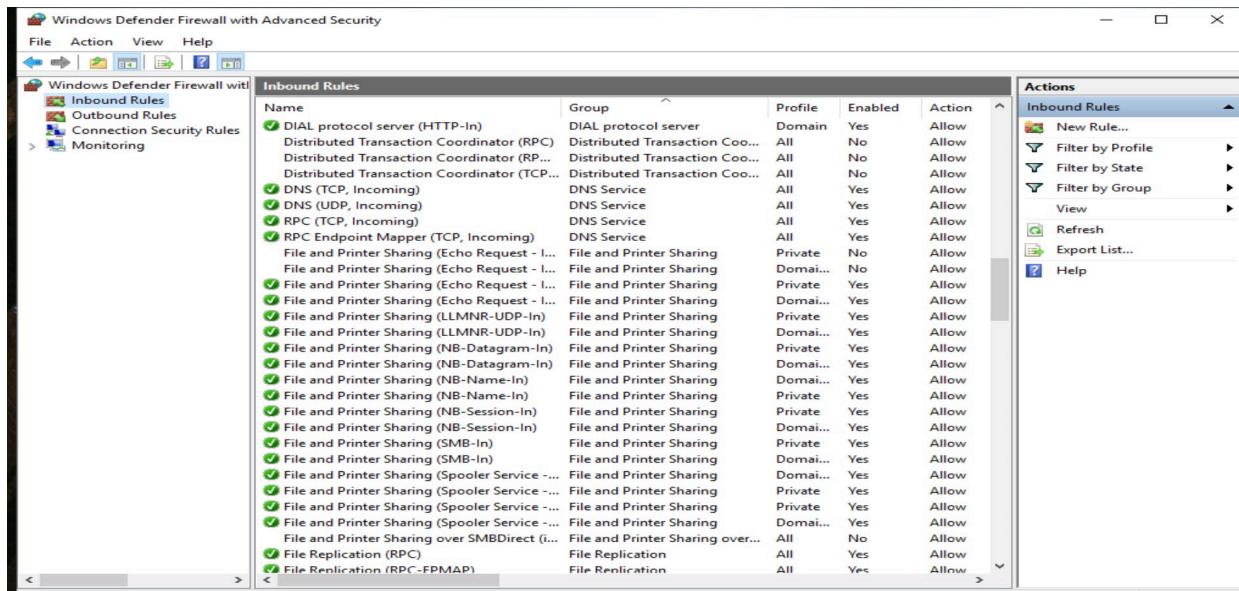
Interface: [REDACTED] --- 0xe
Internet Address Physical Address Type
[REDACTED] static
[REDACTED] static
[REDACTED] static
[REDACTED] static
[REDACTED] static
[REDACTED] static

Interface: 192.168.0.247 --- 0x14
Internet Address Physical Address Type
[REDACTED] dynamic
[REDACTED] dynamic
[REDACTED] static

C:\Program Files (x86)\Wmap>
```

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

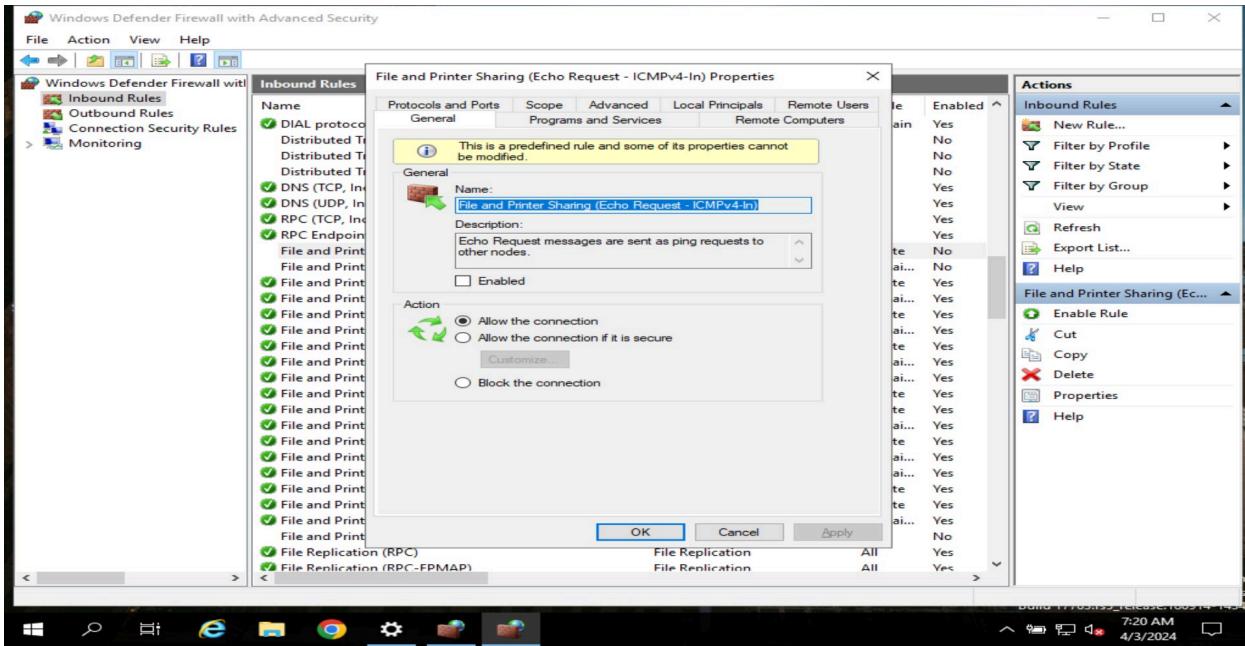
Task 3



The screenshot shows the Windows Defender Firewall with Advanced Security interface. The left navigation pane shows "Inbound Rules" selected. The main area displays a table of inbound rules. The columns are: Name, Group, Profile, Enabled, and Action. The "Enabled" column shows that most rules are set to "Allow". The "Actions" pane on the right provides options for managing rules, including "New Rule...", "Filter by Profile", "Filter by State", "Filter by Group", "View", "Refresh", "Export List...", and "Help".

Name	Group	Profile	Enabled	Action
DIAL protocol server (HTTP-In)	DIAL protocol server	Domain	Yes	Allow
Distributed Transaction Coordinator (RPC)	Distributed Transaction Coo...	All	No	Allow
Distributed Transaction Coordinator (RP...	Distributed Transaction Coo...	All	No	Allow
Distributed Transaction Coordinator (TCP...	Distributed Transaction Coo...	All	No	Allow
DNS (TCP, Incoming)	DNS Service	All	Yes	Allow
DNS (UDP, Incoming)	DNS Service	All	Yes	Allow
RPC (TCP, Incoming)	DNS Service	All	Yes	Allow
RPC Endpoint Mapper (TCP, Incoming)	DNS Service	All	Yes	Allow
File and Printer Sharing (Echo Request - I...	File and Printer Sharing	Private	No	Allow
File and Printer Sharing (Echo Request - I...	File and Printer Sharing	Domai...	No	Allow
File and Printer Sharing (Echo Request - I...	File and Printer Sharing	Private	Yes	Allow
File and Printer Sharing (Echo Request - I...	File and Printer Sharing	Domai...	Yes	Allow
File and Printer Sharing (LLMNR-UDP-In)	File and Printer Sharing	Private	Yes	Allow
File and Printer Sharing (LLMNR-UDP-In)	File and Printer Sharing	Domai...	Yes	Allow
File and Printer Sharing (NB-Datagram-In)	File and Printer Sharing	Private	Yes	Allow
File and Printer Sharing (NB-Name-In)	File and Printer Sharing	Domai...	Yes	Allow
File and Printer Sharing (NB-Name-In)	File and Printer Sharing	Private	Yes	Allow
File and Printer Sharing (NB-Session-In)	File and Printer Sharing	Private	Yes	Allow
File and Printer Sharing (NB-Session-In)	File and Printer Sharing	Domai...	Yes	Allow
File and Printer Sharing (SMB-In)	File and Printer Sharing	Private	Yes	Allow
File and Printer Sharing (SMB-In)	File and Printer Sharing	Domai...	Yes	Allow
File and Printer Sharing (Spooler Service - ...)	File and Printer Sharing	Domai...	Yes	Allow
File and Printer Sharing (Spooler Service - ...)	File and Printer Sharing	Private	Yes	Allow
File and Printer Sharing (Spooler Service - ...)	File and Printer Sharing	Domai...	Yes	Allow
File and Printer Sharing (Spooler Service - ...)	File and Printer Sharing	Domai...	Yes	Allow
File and Printer Sharing over SMBDirect (...	File and Printer Sharing over...	All	No	Allow
File Replication (RPC)	File Replication	All	Yes	Allow
File Replication (RPC-FPMAP)	File Replication	All	Yes	Allow

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

```
Administrator: Command Prompt - ping -t
Microsoft Windows [Version 10.0.19045.4170]
(c) Microsoft Corporation. All rights reserved.

C:\Users\cristian Barreno>ping

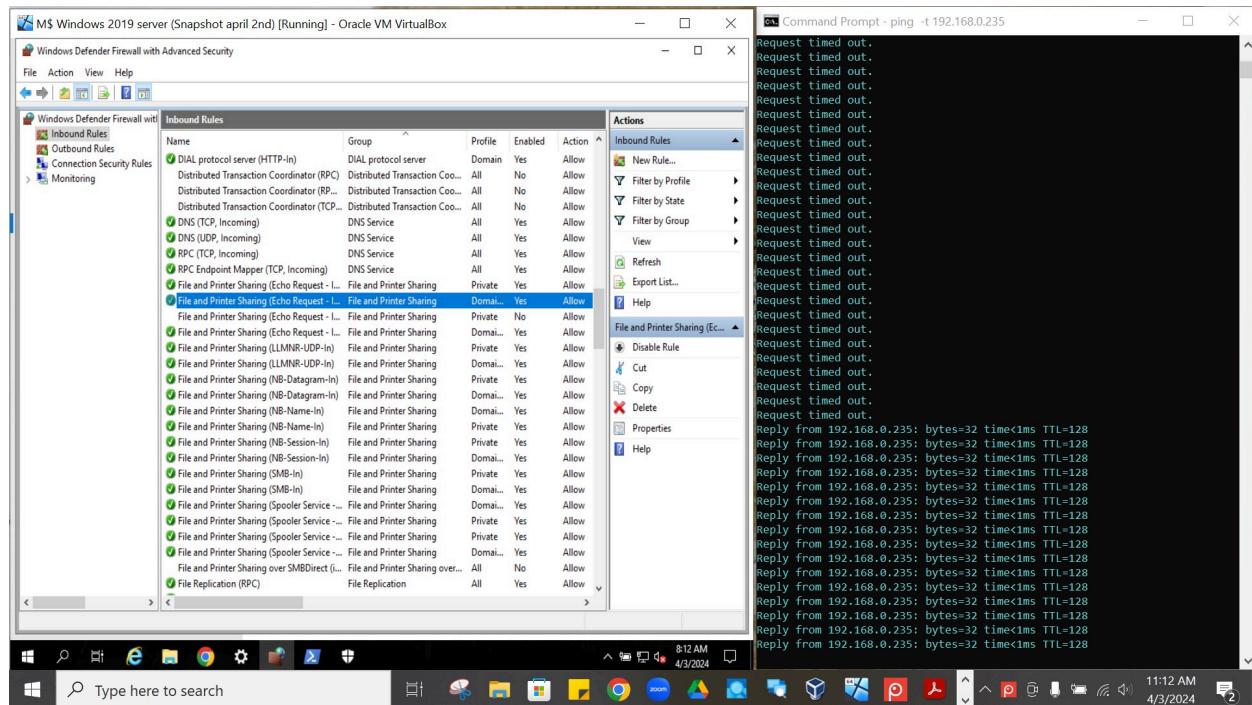
Pinging [REDACTED] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for [REDACTED]:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Users\cristian Barreno>
C:\Users\cristian Barreno>
C:\Users\cristian Barreno>ping -t [REDACTED]

Pinging 192.169.0.235 with 32 bytes of data:
Request timed out.
```

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

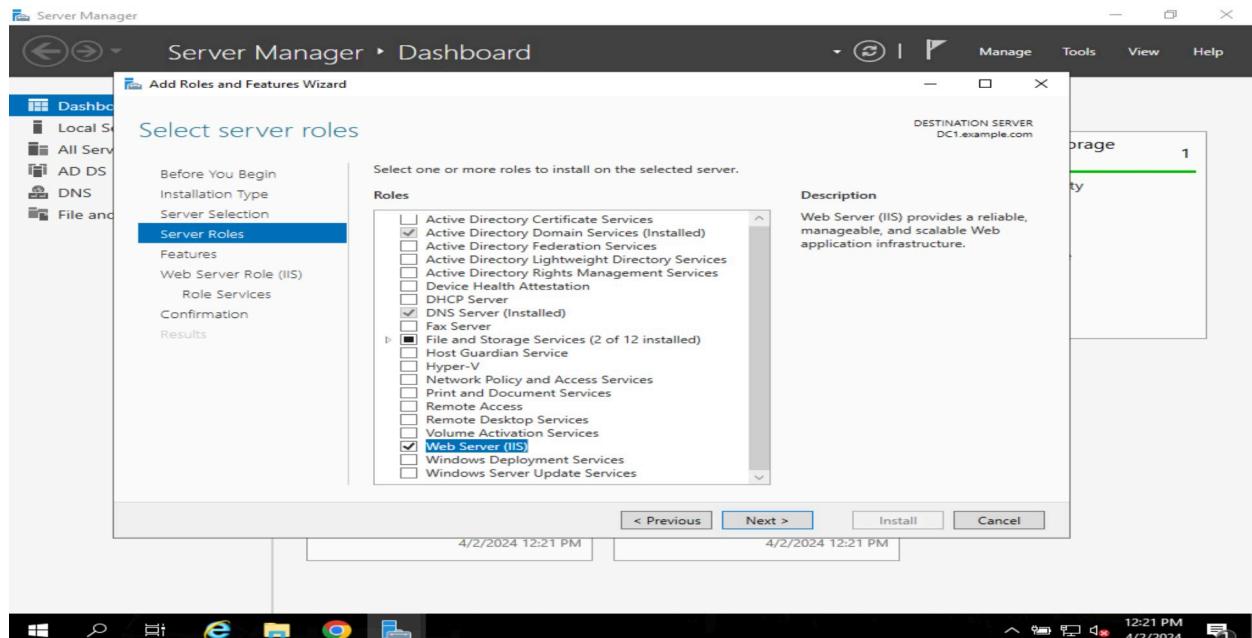
Task 5



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

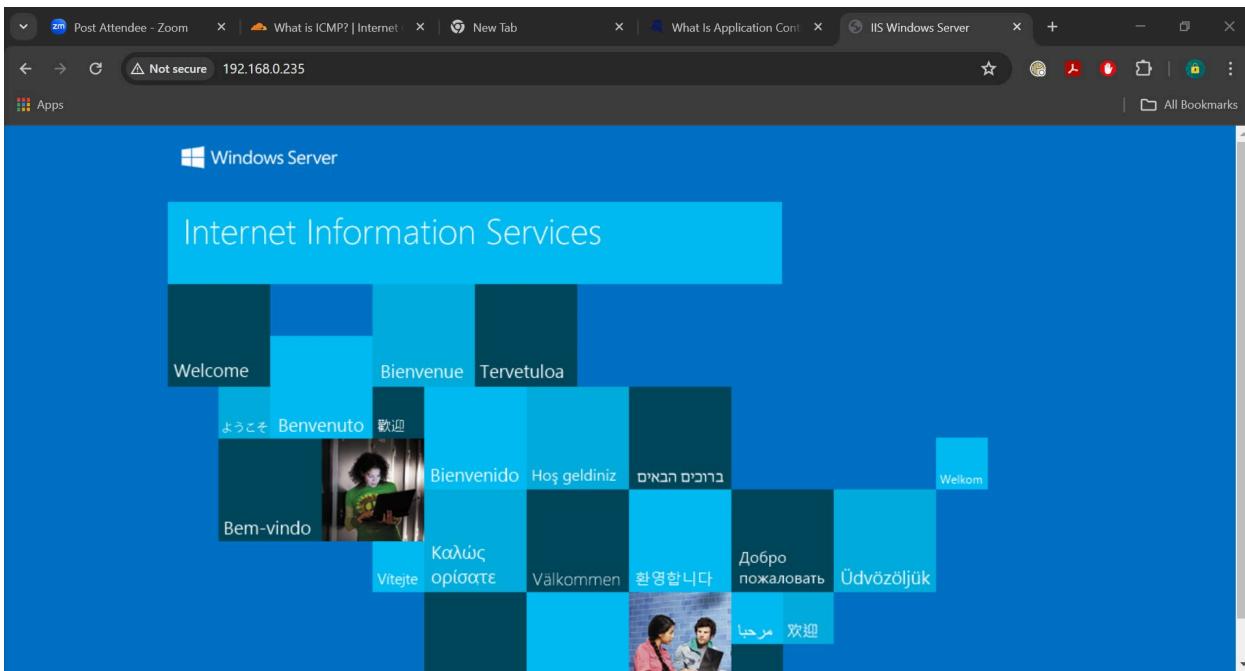
Exercise 2 - Windows Server Firewall - Internet Information Server

Task 1



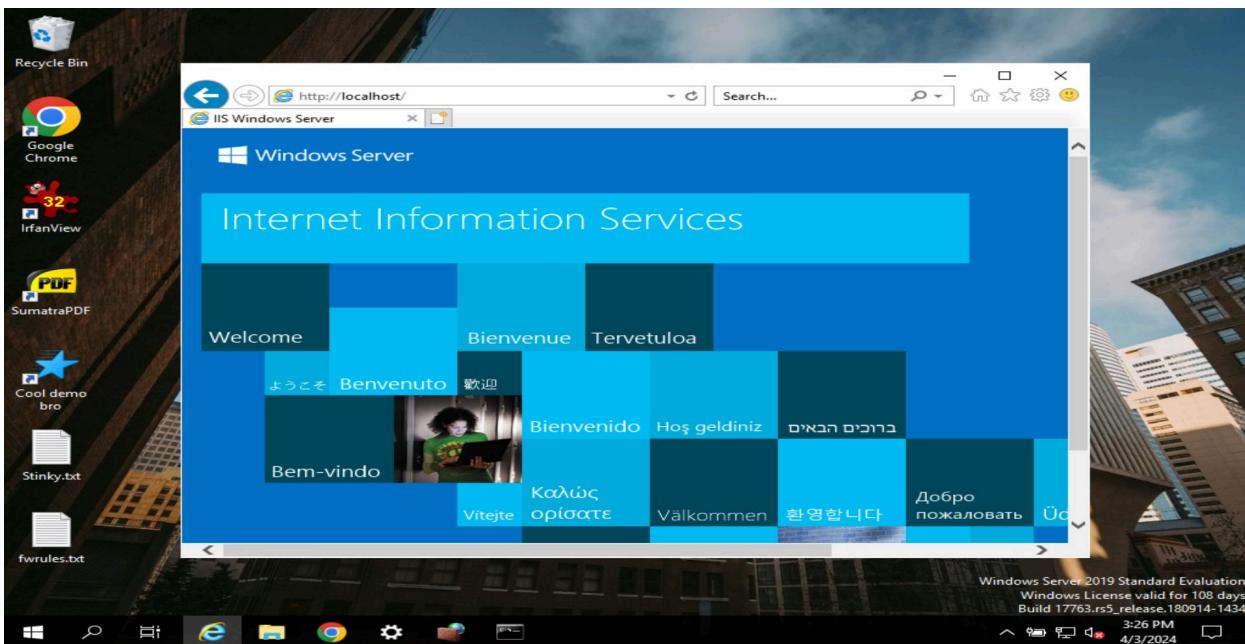
The screenshot above shows the process of installing Internet Information Server on Windows. IIS is a multi-purpose web server to deploying and managing web-based applications.

Task 2



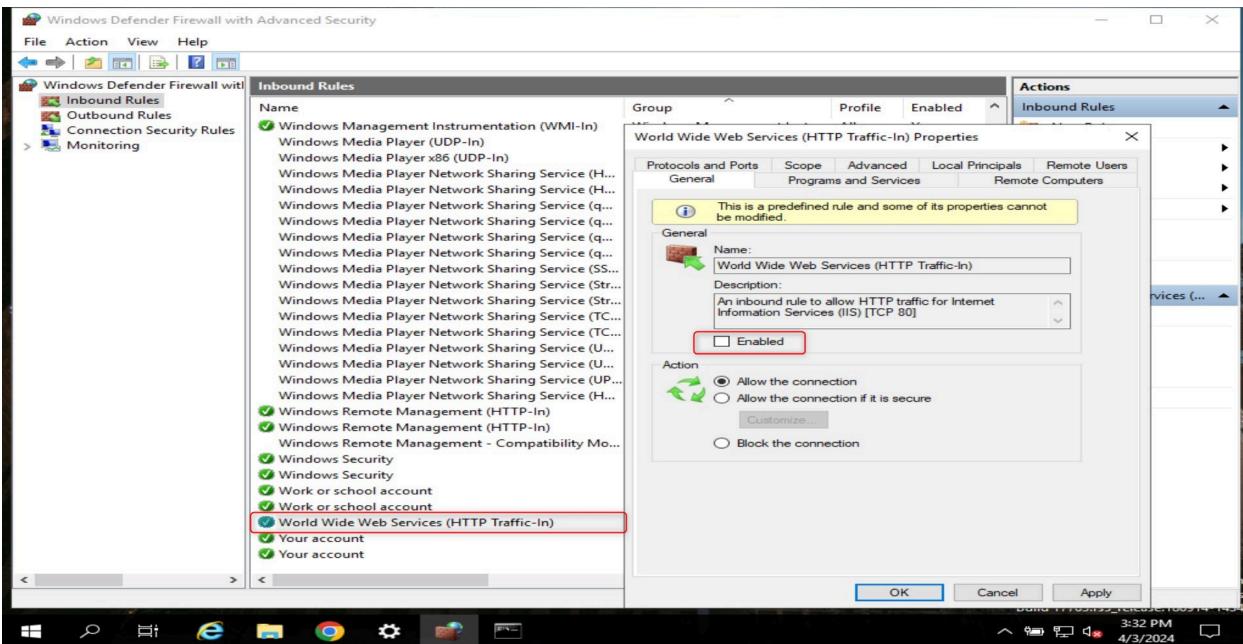
After it finished installing, open a web browser window on your host OS, and enter the IP address of your guest OS. press enter and you will get the web page.

Task 3



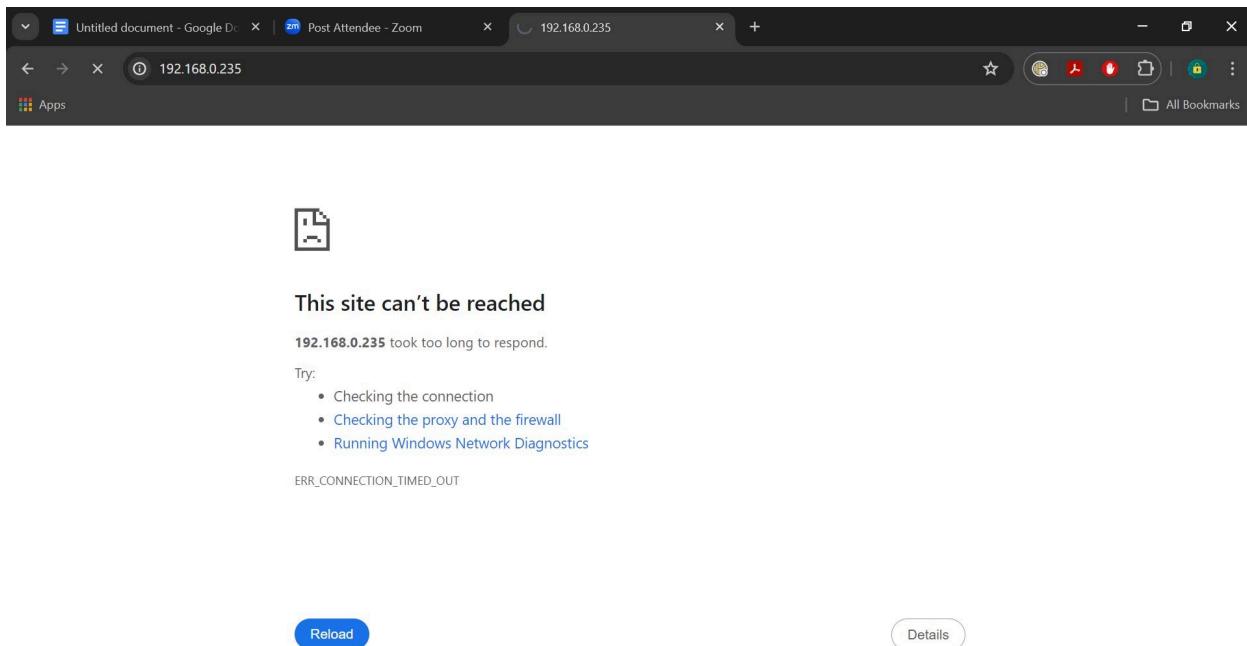
You can also open the Internet Information Server on your guest OS.

Task 4



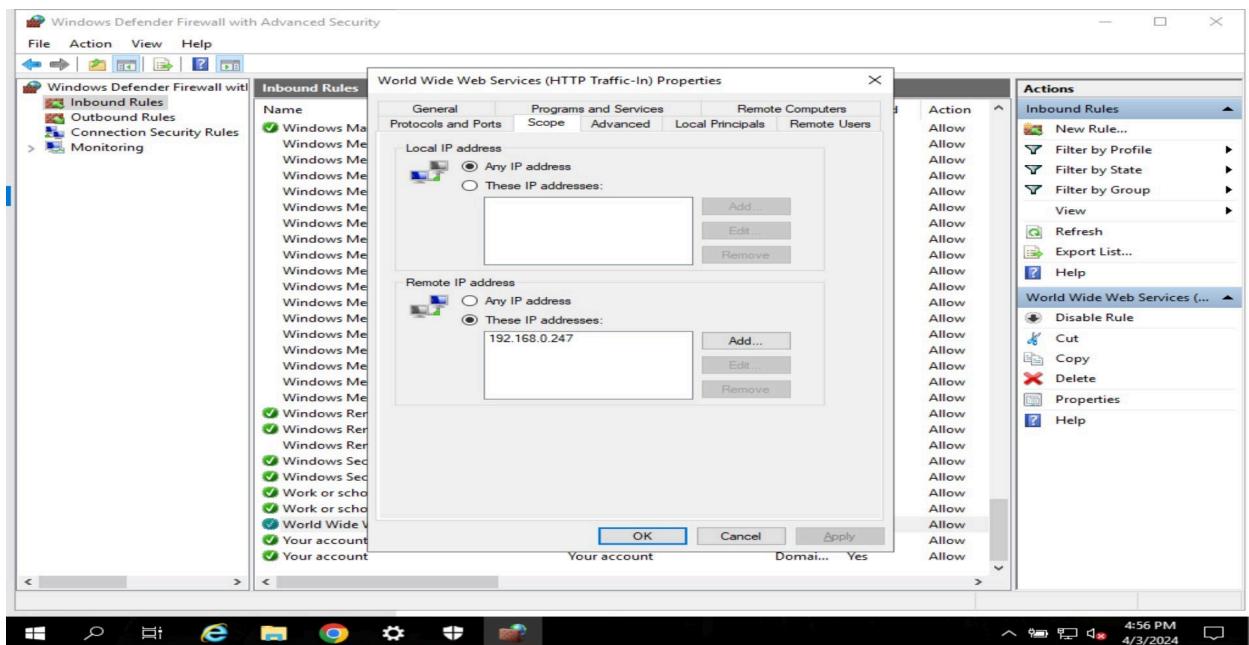
From the firewall inbound rules I'm able to control World Wide Web services, and disable it on my system.

Task 5



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

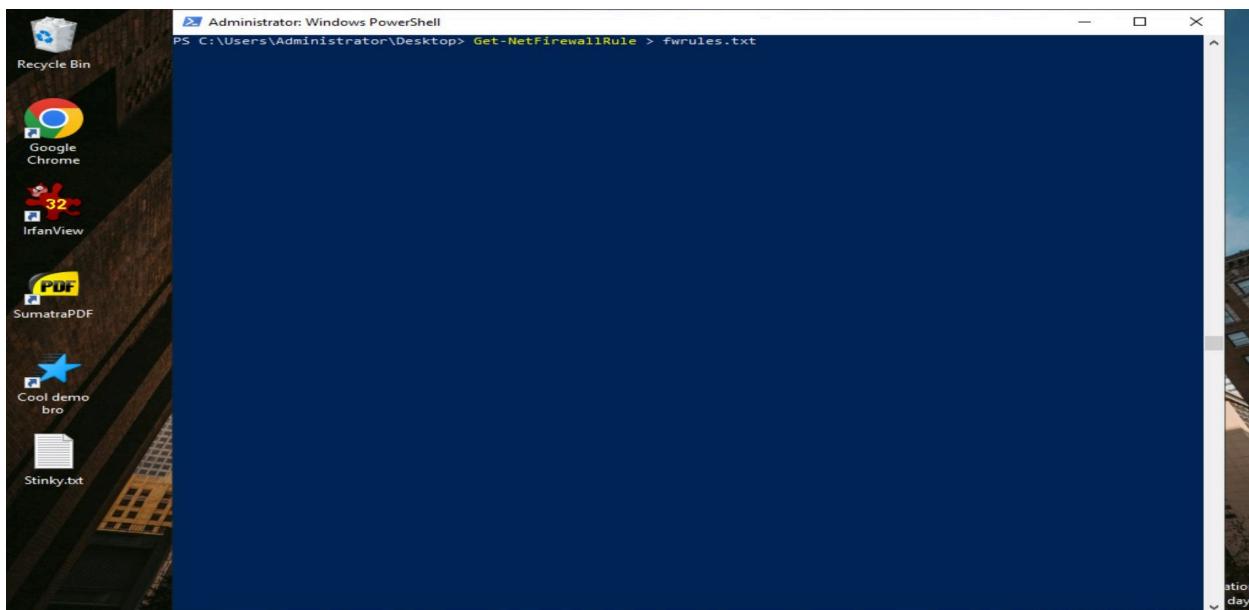
Task 6



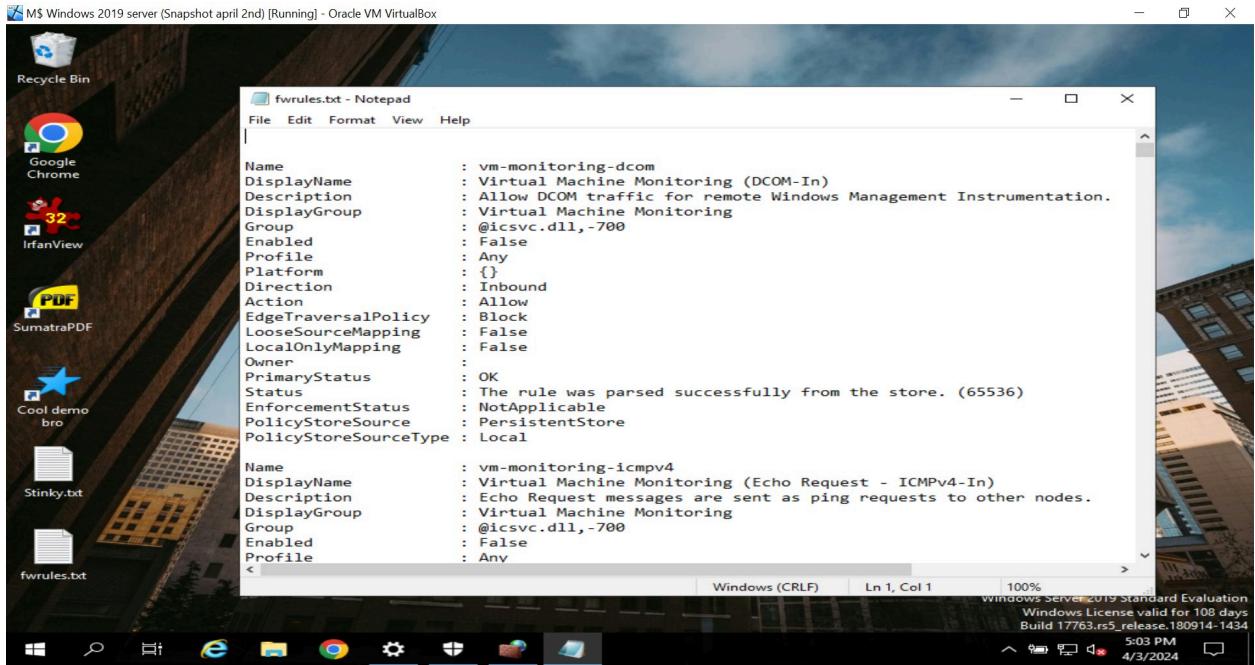
By inserting the Host IP address on the remote IP address section, and then trying to login from someone else's computer you won't be successful. Only your Host OS can access it.

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

```

PS C:\Users\Administrator\Desktop> New-NetFirewallRule -DisplayName "Block Inbound 192.168.0.235" -Direction Inbound -Action Block -RemoteAddress 192.168.0.235

Name : {2702f5d3-6b9c-4a14-87ef-11cdcae5f0196}
DisplayName : Block Inbound 192.168.0.235
Description :
DisplayGroup :
Group :
Enabled : True
Profile :
Platform :
Direction : Inbound
Action : Block
EdgeTraversalPolicy : Block
LooseSourceMapping : False
LocalOnlyMapping : False
Owner :
PrimaryStatus : OK
Status : The rule was parsed successfully from the store. (65536)
EnforcementStatus : NotApplicable
PolicyStoreSource : PersistentStore
PolicyStoreSourceType : Local

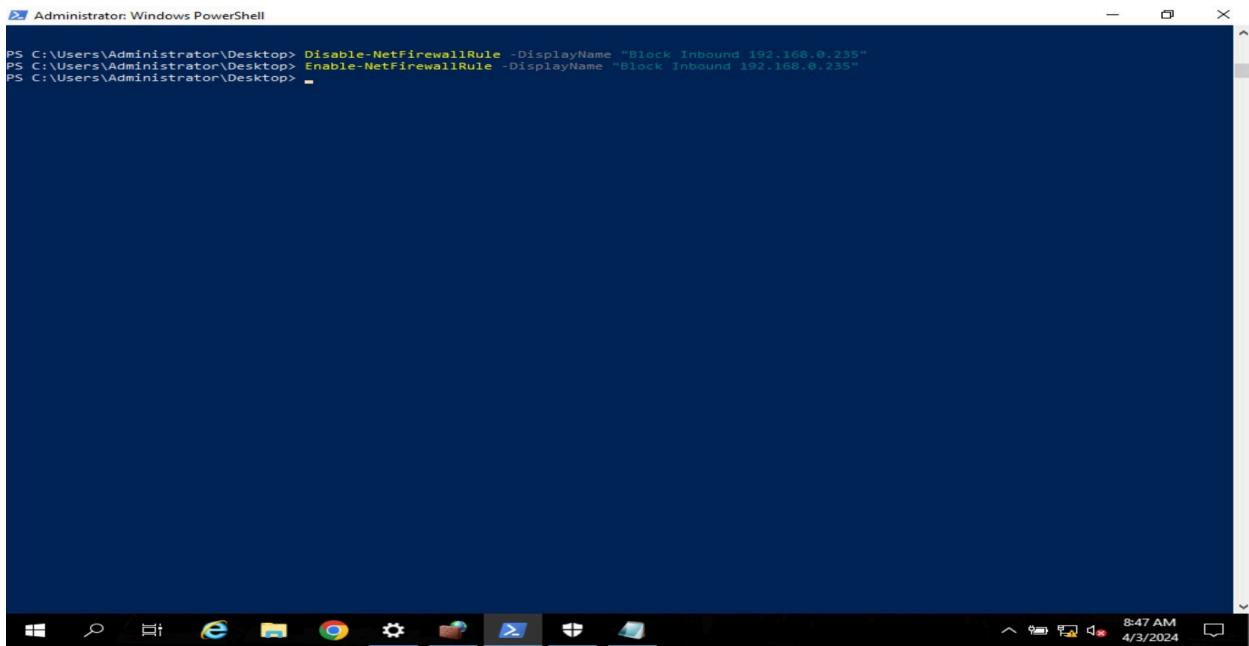
PS C:\Users\Administrator\Desktop> New-NetFirewallRule -DisplayName "Block Outbound 192.168.0.235" -Direction Outbound -Action Block -RemoteAddress 192.168.0.235

Name : {cd342276-29c1-479d-8990-c9d7a487020b}
DisplayName : Block Outbound 192.168.0.235
Description :
DisplayGroup :
Group :
Enabled : True
Profile :
Platform :
Direction : Outbound
Action : Block
EdgeTraversalPolicy : Block
LooseSourceMapping : False
LocalOnlyMapping : False
Owner :
PrimaryStatus : OK

```

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

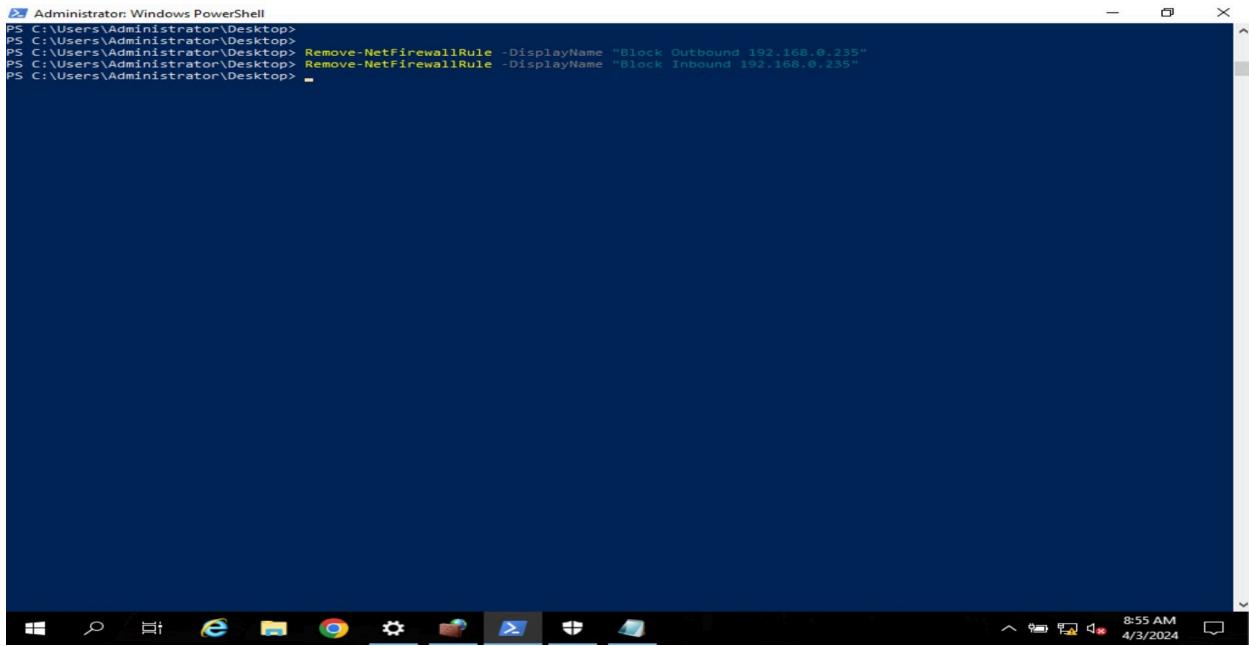
Task 3



```
Administrator: Windows PowerShell
PS C:\Users\Administrator\Desktop> Disable-NetFirewallRule -DisplayName "Block Inbound 192.168.0.235"
PS C:\Users\Administrator\Desktop> Enable-NetFirewallRule -DisplayName "Block Inbound 192.168.0.235"
PS C:\Users\Administrator\Desktop>
```

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

Task 4

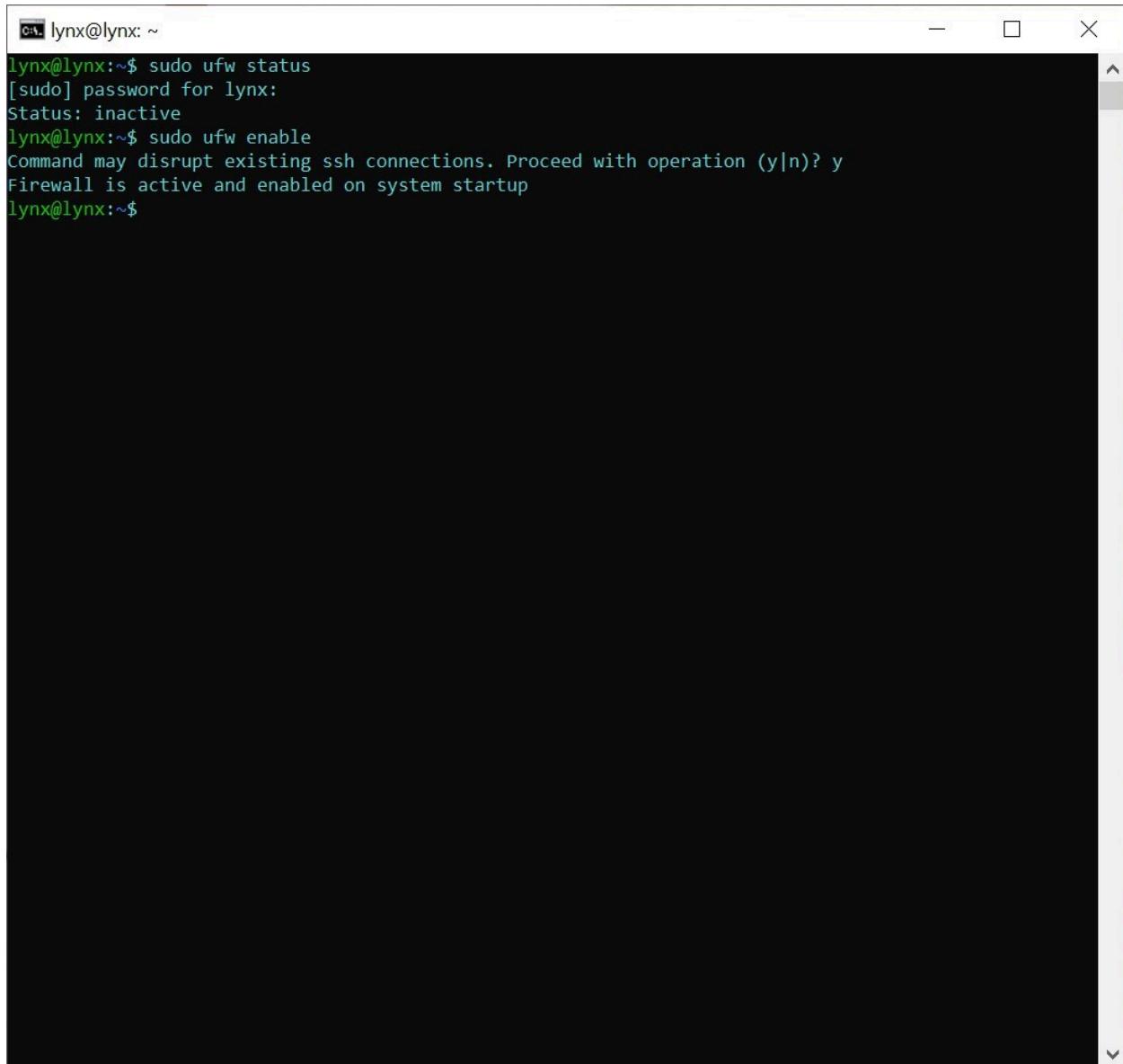


```
Administrator: Windows PowerShell
PS C:\Users\Administrator\Desktop>
PS C:\Users\Administrator\Desktop>
PS C:\Users\Administrator\Desktop> Remove-NetFirewallRule -DisplayName "Block Outbound 192.168.0.235"
PS C:\Users\Administrator\Desktop> Remove-NetFirewallRule -DisplayName "Block Inbound 192.168.0.235"
PS C:\Users\Administrator\Desktop>
```

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

Exercise 4

Task 1



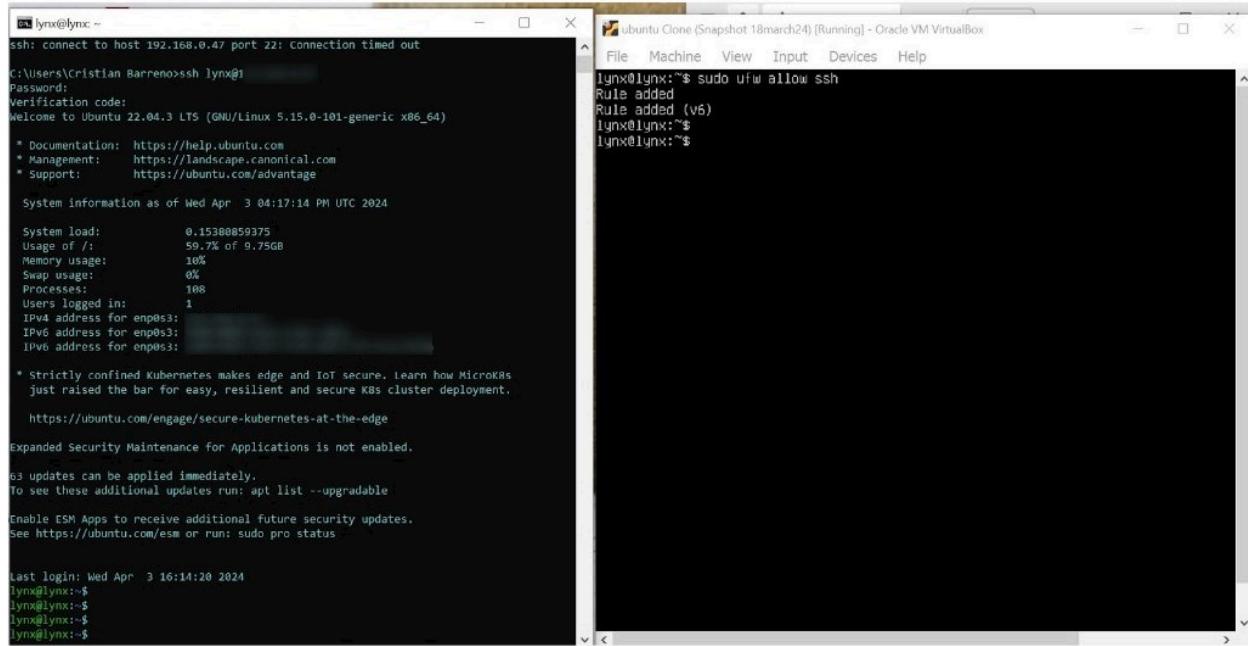
```
lynx@lynx:~$ sudo ufw status
[sudo] password for lynx:
Status: inactive

lynx@lynx:~$ sudo ufw enable
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y
Firewall is active and enabled on system startup

lynx@lynx:~$
```

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



```
lynx@lynx:~
ssh: connect to host 192.168.0.47 port 22: Connection timed out
C:\Users\Kristian Barreno>ssh lynx@192.168.0.47
Password:
Verification code:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-101-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Wed Apr  3 04:17:14 PM UTC 2024

System load:          0.15380859375
Usage of /:            59.7% of 9.75GB
Memory usage:          10%
Swap usage:            0%
Processes:             108
Users logged in:      1
IPv4 address for enp0s3: 
IPv6 address for enp0s3: 
IPv6 address for enp0s3: 

* strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s just raised the bar for easy, resilient and secure K8s cluster deployment.

  https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

63 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Last login: Wed Apr  3 16:14:20 2024
lynx@lynx:~$ 
lynx@lynx:~$ 
lynx@lynx:~$ 
lynx@lynx:~$ 
```

```
File Machine View Input Devices Help
lynx@lynx:~$ sudo ufw allow ssh
Rule added (v6)
Rule added (v6)
lynx@lynx:~$ 
lynx@lynx:~$ 
```

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



```
Select lynx@lynx: ~
lynx@lynx:~$ sudo ufw disable
[sudo] password for lynx:
Firewall stopped and disabled on system startup
lynx@lynx:~$ sudo ufw enable
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y
Firewall is active and enabled on system startup
lynx@lynx:~$ sudo ufw status
Status: active

To                         Action      From
--                         --          --
22/tcp                     ALLOW      Anywhere
22                         ALLOW      Anywhere (v6)
22/tcp (v6)                 ALLOW      Anywhere (v6)

lynx@lynx:~$ sudo ufw disable
Firewall stopped and disabled on system startup
lynx@lynx:~$ sudo ufw status
Status: inactive
lynx@lynx:~$ 
```

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

```
lynx@lynx: ~
lynx@lynx:~$ sudo ufw allow http
Rules updated
Rules updated (v6)
lynx@lynx:~$
```

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

Task 5

```
lynx@lynx: ~
lynx@lynx:~$ sudo ufw allow from 192.168.0.247/24 to any port 80
[WARN]: Rule changed after normalization
Rules updated
lynx@lynx:~$ sudo ufw status
Status: inactive
lynx@lynx:~$
```

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`

```
lynx@lynx: ~
lynx@lynx:~$ sudo ufw status
Status: active

To          Action      From
--          --          --
22/tcp      ALLOW      Anywhere
22          ALLOW      Anywhere
80          ALLOW      192.168.0.0/24
22/tcp (v6)  ALLOW      Anywhere (v6)
22 (v6)     ALLOW      Anywhere (v6)

lynx@lynx:~$
```

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

Sudo ufw status