# 5CS031 Network Security

# Workshop 6: Linux Firewall

**Student Name:\_\_\_\_\_Loucas Xiourouppa\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Student Number:\_\_\_\_2007307\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**This is an assessed workshop. You will need to complete the workshop tasks, answer the questions and then submit the Word file, complete with your screenshots and answers, before the deadline posted on Canvas.**

**Assessment**

You are required to insert a series of screen captures of your work into this document and then to upload the file to the correct area in Canvas for your workshop assessments. Failure to do so will result in no marks being allocated for the work.

**Scenario**

You will be configuring a host-based firewall (IPTables) on a Linux server, so that only a few specific services are available to an "external" computer, and several other services are also additionally available to a designated "internal" computer.

**Resources**

For further information on IPTables, please refer to the documentation on these websites:

<http://wiki.centos.org/HowTos/Network/IPTables>

<http://www.cyberciti.biz/tips/linux-iptables-examples.html>

**Prepare the environment**

The next stages must be completed in the VMware virtual environment as you need administrator/root rights and must be disconnected from the university network.

1. Start the Linux Server that you used in previous workshops. If you haven’t done so before, read the previous workshops on how to set it up.
2. Copy down the value for the IP address (inet) for eth0 below:  
     
   [Linux Server IP address]
3. 192.168.92.137
4. Find and also start the "Security Windows 7" virtual machine. This will server as a **potential hacker**
5. Check that the network settings for both machines are set to NAT
6. Copy down the value for the IP address of Windows 7 below:  
     
     
   [Windows 7 IP address]
7. 172.16.2.3

**VMware Ubuntu (Internal Computer/Safe)**

1. From Canvas, download the file called “Ubuntu.zip”. Right-click on this file and extract the zip file into a folder. Locate and start the machine and make sure it’s network settings are set to NAT.
2. Login to Ubuntu with

Username: **root**

Password: **toor**

1. Note down the value for the IP address (inet) for eth0.

[Ubuntu IP address]

127.0.0.1

1. Now test you have connectivity between the virtual machines. In Security Windows 7 open a command window and ping the LinuxServer VM's IP address, and then Ubuntu's IP and so on. Make sure that all 3 virtual machines can ping each other before proceeding any further.

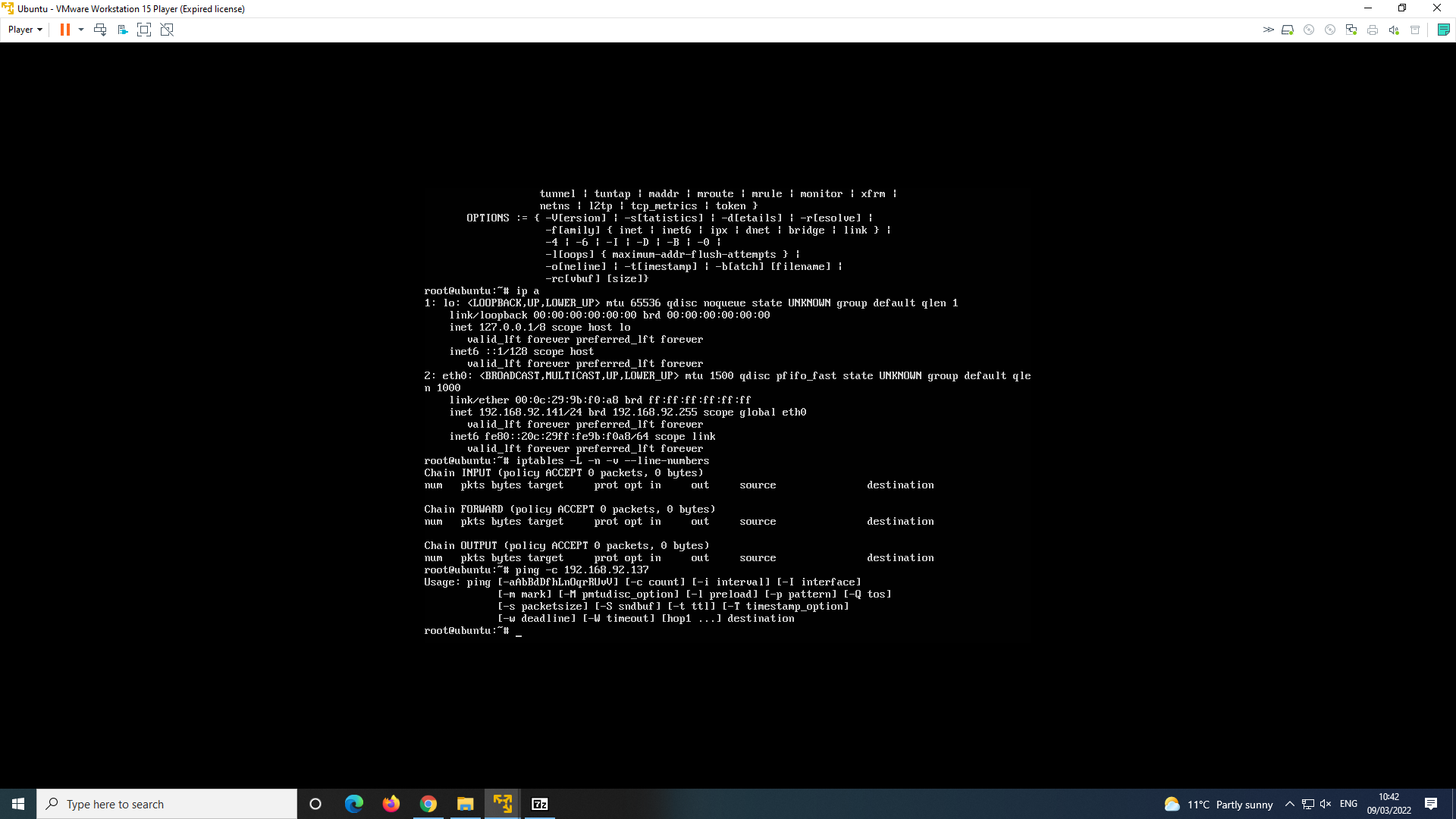
**Clearing the Linux Server Firewall**

1. On the Linux Server, display the current firewall rule by entering the following command:  
     
   **iptables -L -n -v --line-numbers**  
     
   This will list all the existing firewall rules in force on the server.
2. Even if there are no existing rules, to be on the safe side, **clear all existing rules** and set the default policy to accept everything, before you start. Enter the following commands:  
     
   **iptables -F  
   iptables -P INPUT ACCEPT**

**Basic ping tests**

1. On the Ubuntu VM, ping the Linux Server:  
     
   **ping -c 5 192.168.xxx.xxx**
2. Make sure that you replace the xxx IP address with your Linux Server’s IP address. Are your pings successful?  
     
   [your answer here]

Yes, my pings are now successful.



1. On the Windows 7 Command Prompt, ping the Linux Server:  
     
   **ping 192.168.xxx.xxx**
2. Make sure that you replace the xxx IP address with your own Linux Server’s IP address. Are your pings successful?  
     
   [your answer here]

Yes My ping from windows to linux is also successful

2. On the Linux Server, configure the IPTables firewall to reject ping requests from all machines. Enter the following command on the Linux Server:  
     
   **iptables -A INPUT -p icmp -j REJECT**
3. What this does is to add a rule for input network traffic of the type ICMP (ping) and the action is to reject the traffic.
4. Now try to ping the Linux Server from both the Ubuntu and the Security Windows7 machines. If you have done this correctly, you will not be successful from either machine. What was the ping error message?  
     
   It said “unreachable host”
5. Now clear the IPTables rule from the Linux Server:
6. Configure a new IPTables rule:  
     
   **iptables –A INPUT –p icmp –j DROP**
7. Now try to ping the Linux Server from both the Ubuntu and the Security Windows 7 machines, again. Look at the difference in the ping error message this time. Why do you think this is?  
     
   [your answer here]

The reason why we have a different error message is because we just added a rule to “DROP” any icmp pings.

1. Clear the IPTables rule from the Linux Server again:  
     
   **iptables –F**
2. Configure a new IPTables rule:  
     
   **iptables –A INPUT -s 192.168.yyy.yyy –p icmp –j REJECT**
3. Make sure that you replace the yyy IP address with the Security Windows 7 virtual machine's IP address.
4. Now ping the Linux Server from the Security Windows 7. Are you successful?  
     
   [your answer here]

No the ping was not successful.

1. Then ping the Linux Server from the Ubuntu machine. Is there a difference? Why do you think this is?  
     
   [your answer here]

When I ping the linux server from ubuntu it successfully pings to it unlike on windows. The reason why is because we set a new rule to reject an icmp (ping command) from the ip address that belongs to the windows machine.

1. Now clear the IPTables rule from the Linux Server again:

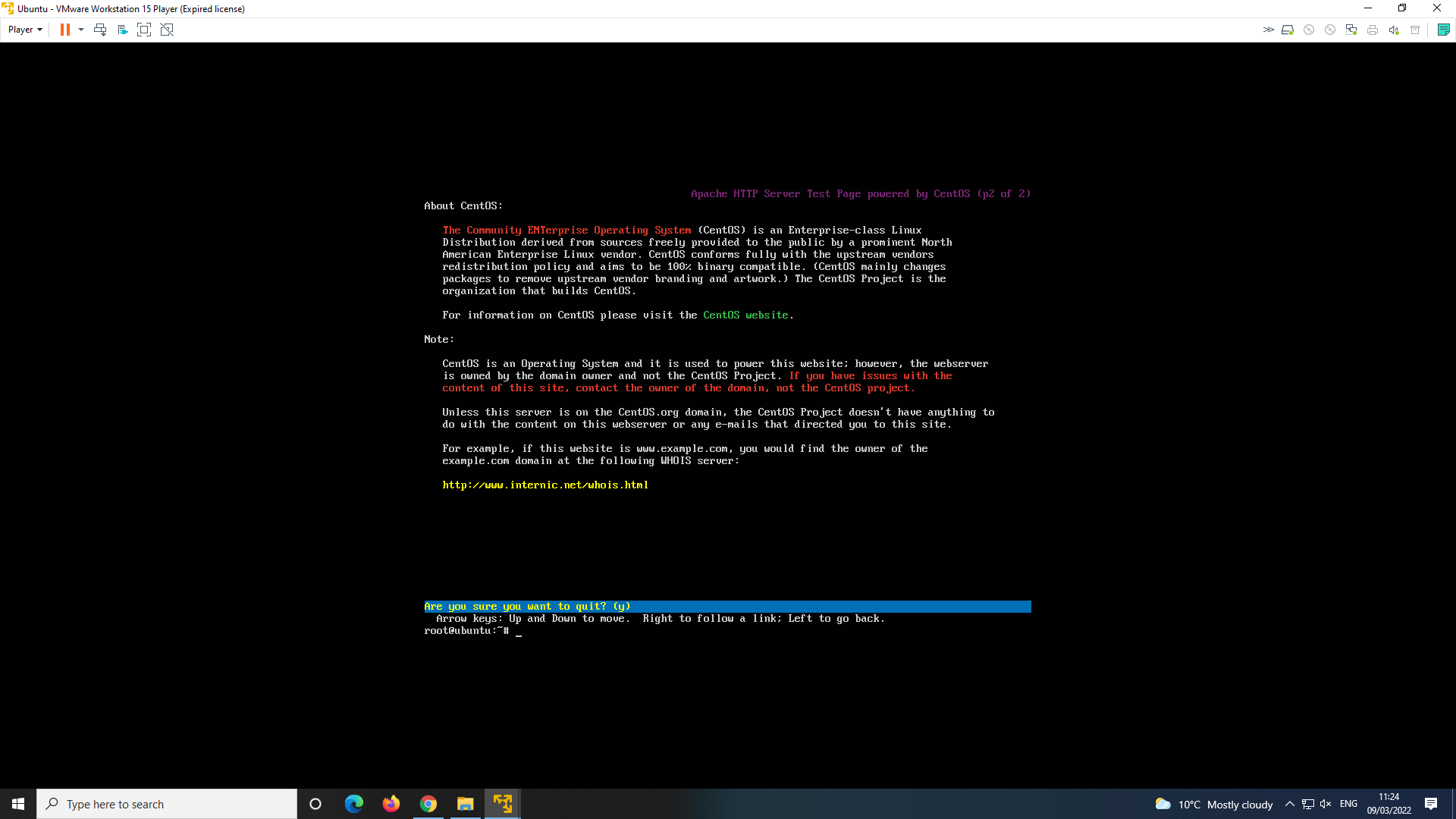
**Scanning the Linux server**

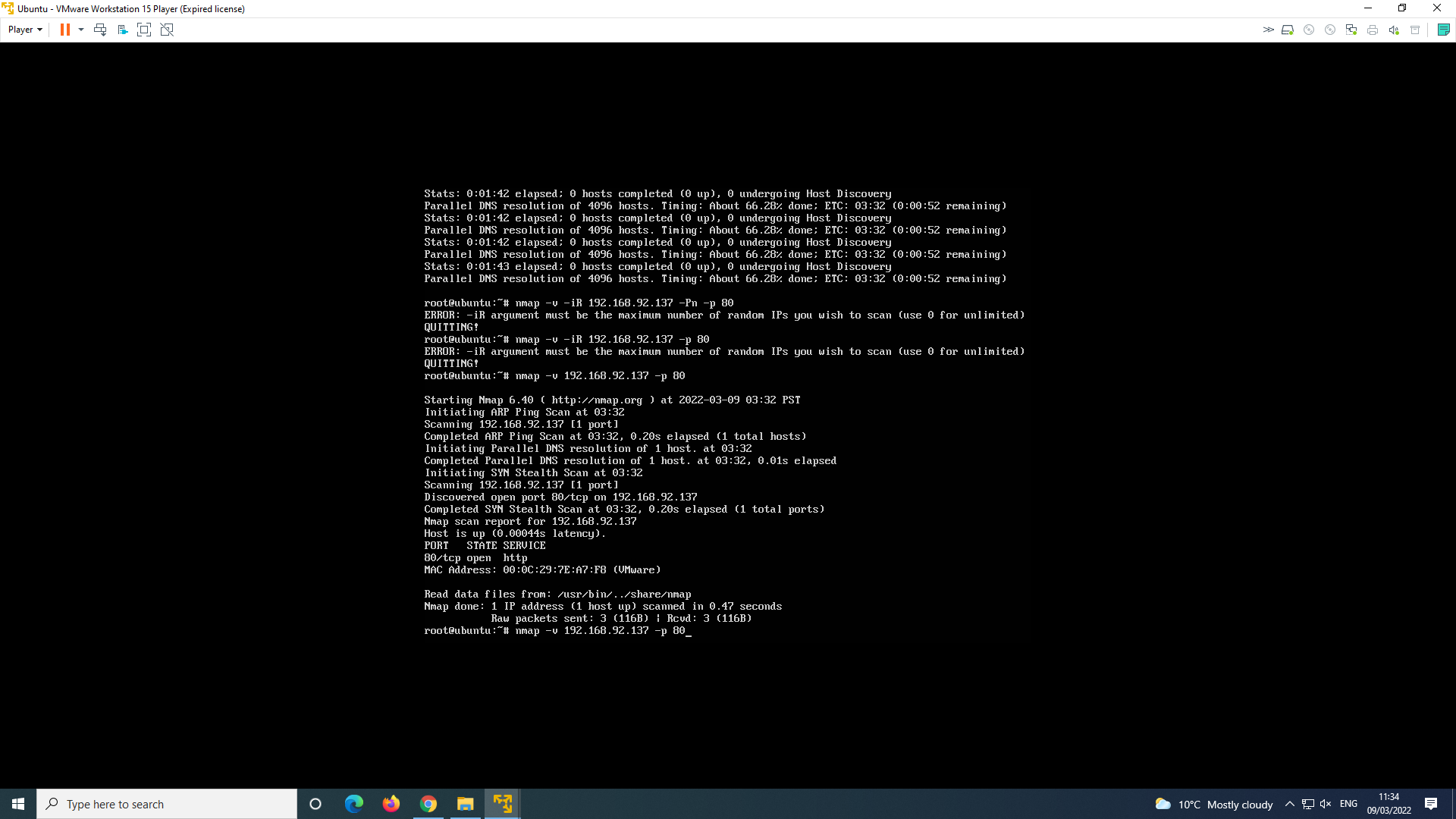
1. **nmap** is a "Network Mapping" or scanning tool used by security professionals and hackers to scan for ports and services on network computers. You are going to use it to see what services or ports on the Linux Server can be seen from both computers.
2. On the Security Windows 7, start a command prompt window (and maximize it) and then enter:  
     
   **nmap 192.168.xxx.xxx**
3. Make sure that you replace the xxx IP address with your own Linux Server’s IP address. When the nmap scan has completed, it will tell you what ports and services it has found on the Linux Server. Copy the first 13 of those services and ports into the table below:

|  |  |  |
| --- | --- | --- |
| PORT | STATE | SERVICE |
| 21/tcp | open | ftp |
| 22/tcp | open | ssh |
| 23/tcp | open | telnet |
| 25/tcp | open | smtp |
| 53/tcp | open | domain |
| 79/tcp | open | finger |
| 80/tcp | open | http |
| 110/tcp | open | pop3 |
| 111/tcp | open | rpcbind |
| 139/tcp | open | netbios-ssn |
| 143/tcp | open | imap |
| 443/tcp | open | https |
| 445/tcp | open | microsft-ds |

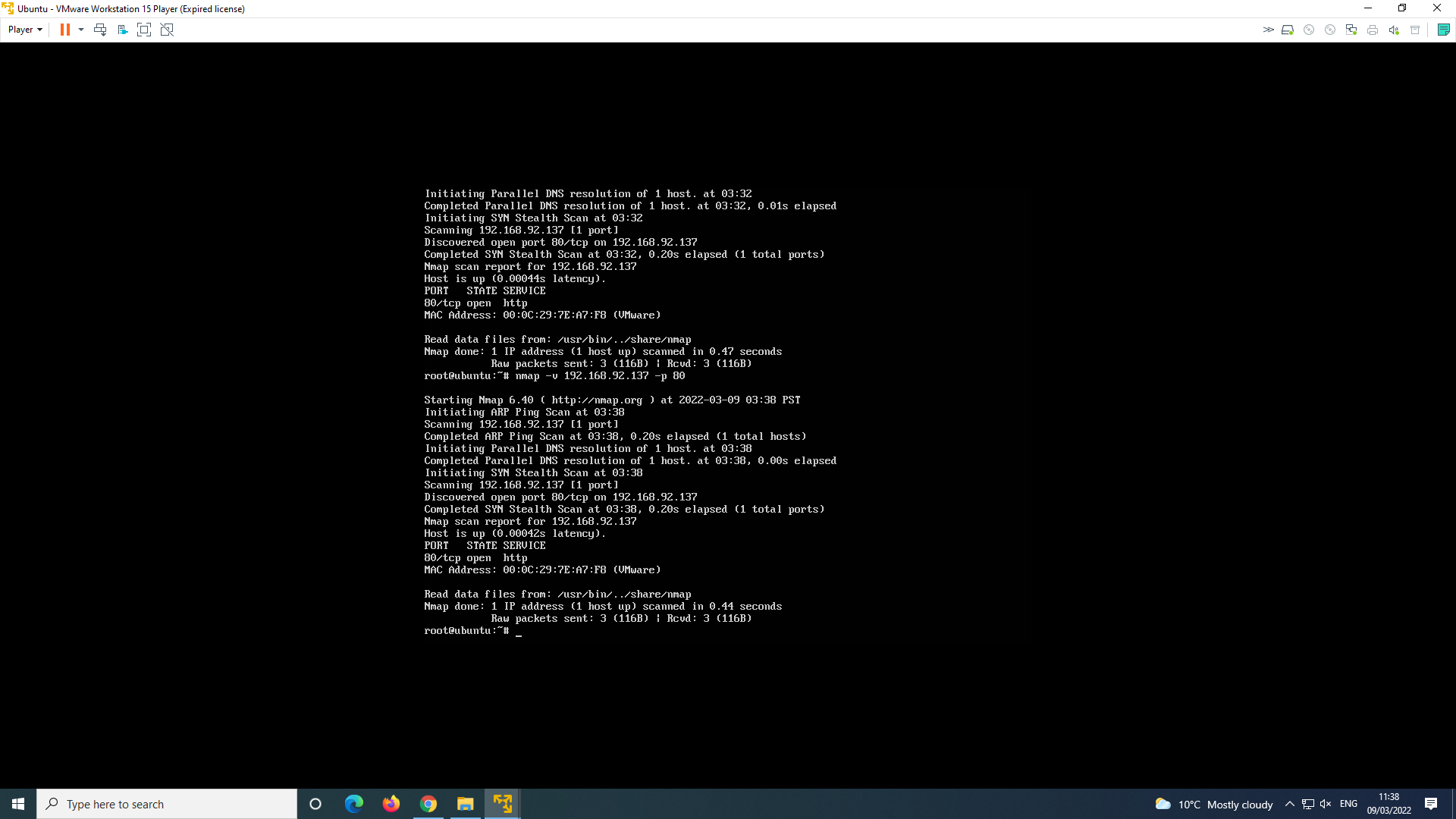
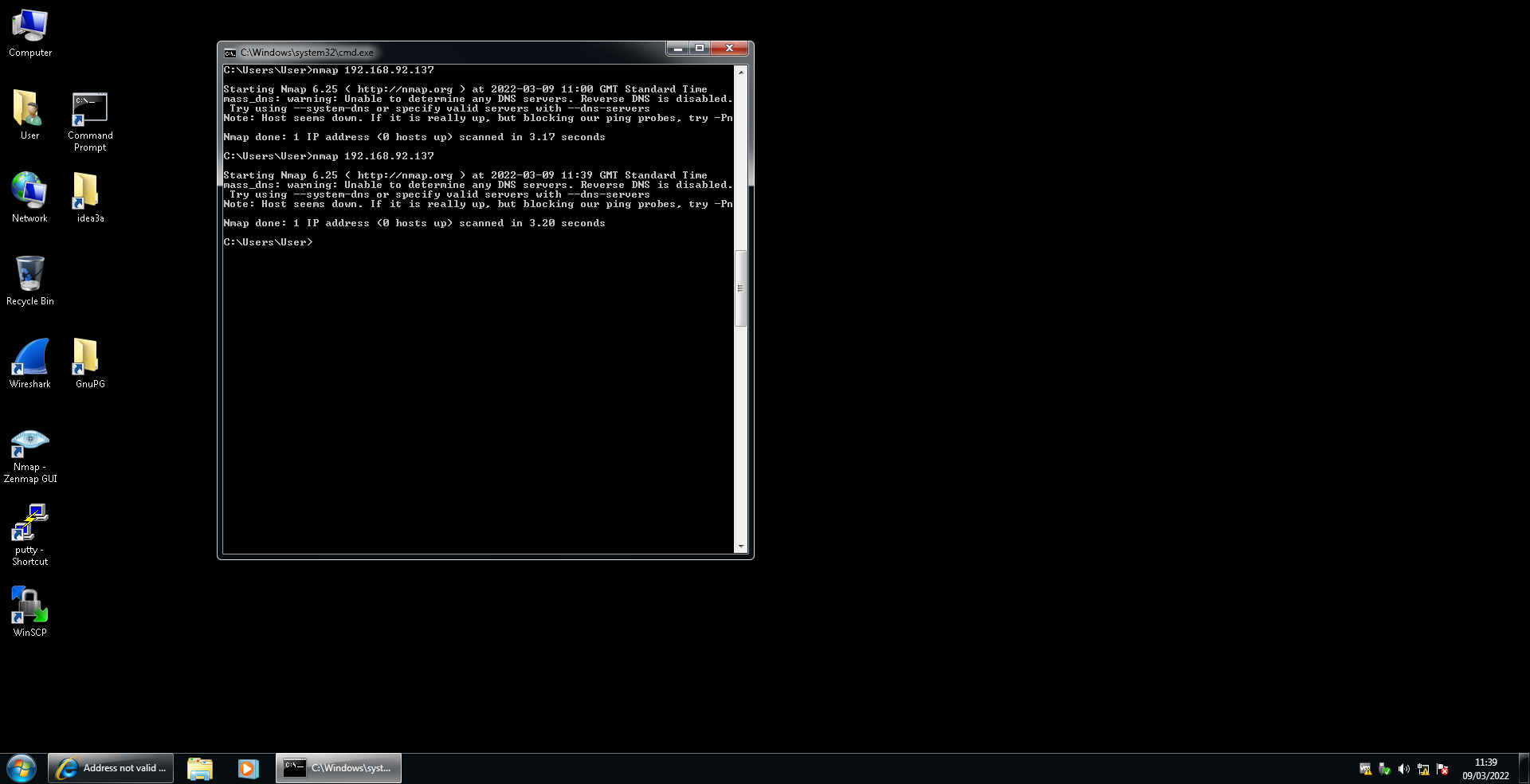
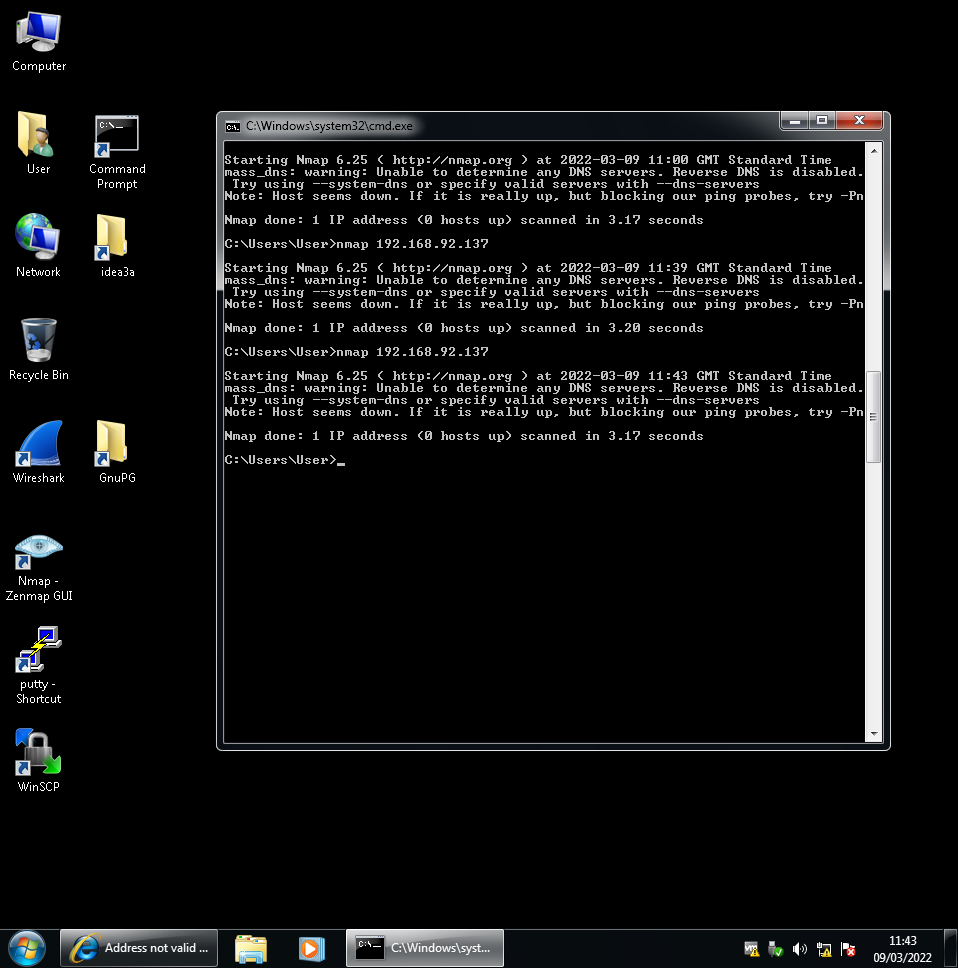
1. Now go to the Ubuntu machine and execute the same command. Are the results the same?  
     
   [your answer here]
2. Yes, I get the same results.
3. On the Linux Server, set the default policy of the firewall to block (drop) everything:
4. Now scan the server again from both machines nmap. What is the difference? Can either machine see any services or ports?   
     
   [your answer here]
5. Now I can neither see any services or ports on ubuntu or windows
6. Try using the Web browser on your Security Windows 7 to connect to your Linux server. Are you successful?   
   [your answer here]

No i am not successful

1. Create a new firewall rule on the Linux Server to allow web browsers to connect to the server:  
     
   **iptables -A INPUT -p tcp --dport 80 -j ACCEPT**
2. This rule says, accept incoming network traffic, with the protocol of TCP, going to the destination port of 80.
3. Try using the Web browser on your Security Windows 7 to connect to your Linux server again. Are you successful? Screen capture the Web browser and paste it below:
4. Now see if you can see the text-based Web browser Lynx on the Ubuntu VM by using the command below:  
     
   **lynx http://192.168.xxx.xxx/**
5. Make sure that you replace the IP address with your own Linux Server’s IP address. Screen capture the Ubuntu windows with the Lynx Web browser and paste it below:  
     
    ****
6. When you want to leave the Lynx web browser, press the Q key first (for quit) and then the Y key (for yes).
7. You can also use the nmap command to scan against the web port of 80 to see if it is accessible. This just asks nmap to scan only one port, the port 80, which is the web port, on the Linux Server. Again, make sure that you replace the IP address with your own Linux Server’s IP address. What’s the syntax of the command and what did nmap output for the port 80?  
     
   [your answer here]
8. the syntax is = **nmap -v 192.168.92.137**

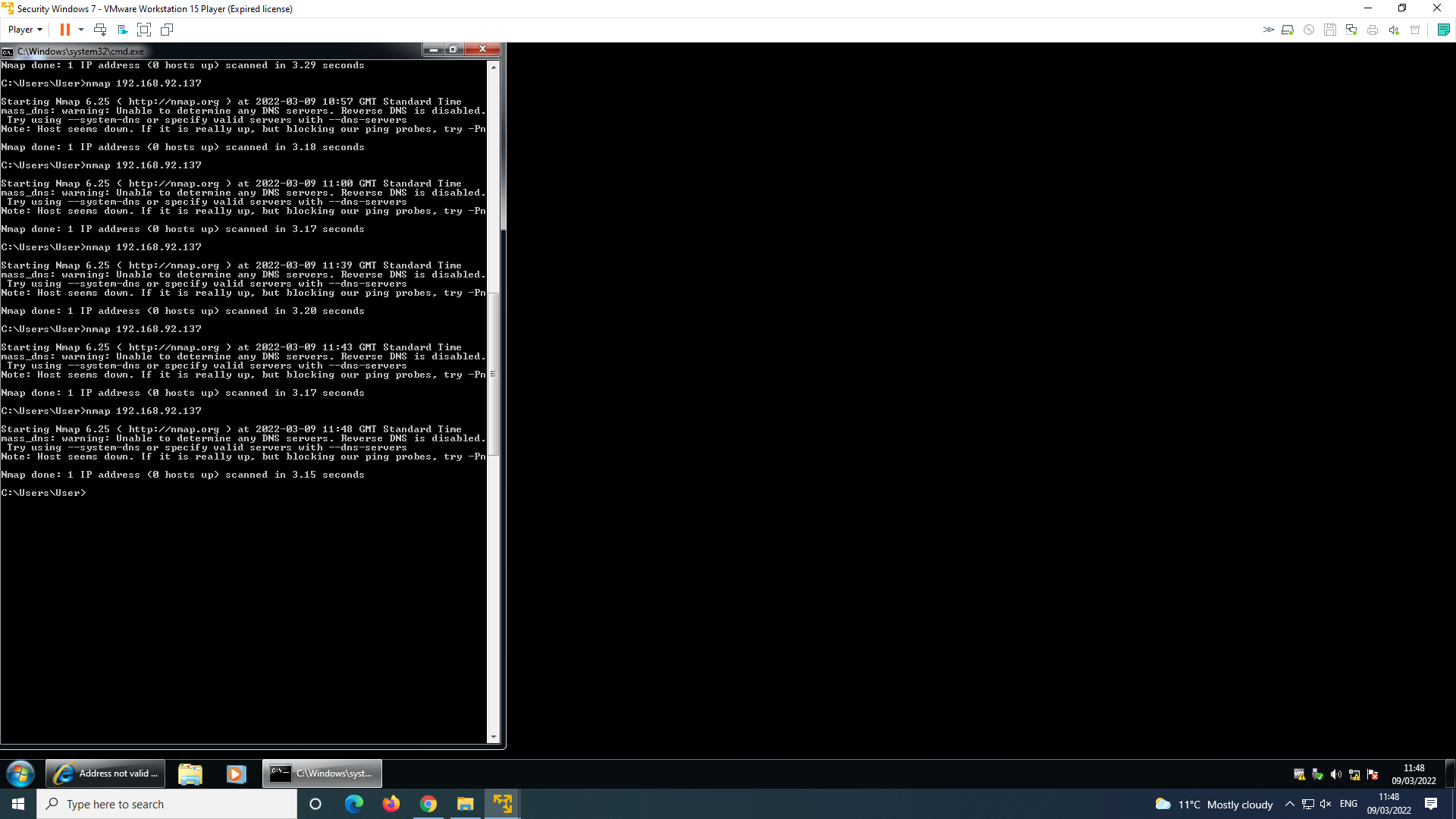
****

**Accepting Connections**

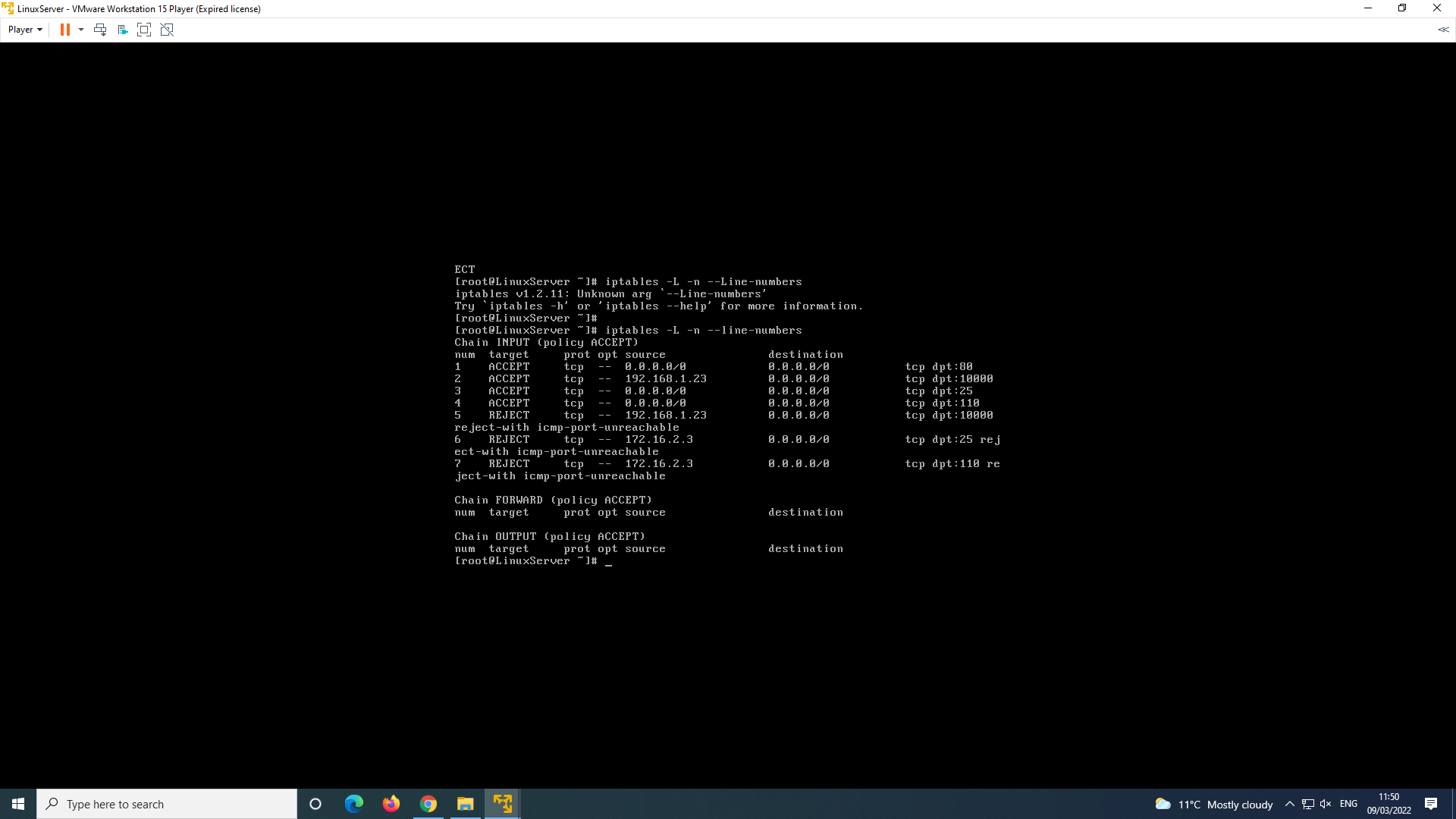
1. To create a rule that allow a computer to connect to a port on the server, you need a rule in the following format:  
     
   **iptables -A INPUT -s 192.168.1.23 -p tcp --dport 10000 -j ACCEPT**
2. The above rule allows the computer with the source (-s) IP address of 192.168.1.23 to connect with the TCP protocol to the destination port of 10000.
3. Clear all existing rules and set the default policy to accept everything. Enter the following commands:  
     
   Now create the necessary IPTables rules such that **only** the "internal" computer (Ubuntu) can connect to your Linux Server on the following ports: 21, 22, 25, 80, 110, 143 and 445.
4. When you have created the rules, use nmap on the Ubuntu to scan the Linux server, and screen capture the results. Paste the screen capture below:  
     
   [your screen capture here]
5. 
6. Do the same with the Security Windows 7. Paste the screen capture below:  
     
   [your screen capture here]
7. 
8. What is the difference between the two results?  
     
   [your answer here]
9. ubuntu let me use nmap on the linux server but nmap was not successful from the windows vm
10. Now create the necessary IPTables rules suchthat **any** computer can connect to the three ports 25, 80 and 110. You may need to delete some of your existing rules before inserting new ones as IPTables will match the rules in strict top-down order. Look at the information on rules line number in the second Web URL at the beginning of this workshop.
11. When you have created the rules, use nmap on the Security Windows 7 to scan the Linux server, and screen capture the results. Paste the screen capture below:  
      
    [your screen capture here]
12. 

**Rejecting Connections**

1. To create a rule that active rejects a computer to connect to a port on the server, you need a rule in the following format:  
     
   **iptables -A INPUT -s 192.168.1.23 -p tcp --dport 10000 -j REJECT**
2. The above rule rejects the computer with the source IP address of 192.168.1.23 from connecting to the port 10000.
3. On the Linux Server, create the necessary rules such that **the Security Windows 7** computer would be actively rejected from connecting to ports 25 and 110.

1. Then scan the Linux Server again from Security Windows 7 with nmap, and screen capture the results. Paste the screen capture below:  
     
   [your screen capture here]
2. 
4. On your Linux Server, use the following command to list all the firewall rules that you have created:

**iptables -L -n -v --line-numbers**  
  
Capture the screen, and paste the screen capture below:  
  
[your screen capture here]



1. Please make sure that all the rules are visible as you will be marked on every rule that you create.
2. Now clear all the rules and set the default policy to accept everything on the Linux Server.
3. Shutdown both your Linux Server and Ubuntu respectively by entering the command in each of them:  
     
   **shutdown -h now**
4. Shutdown your Security Windows VM.

**Workshop Questions**

**Use the Web** (and the documents mentioned earlier) as a research tool to search for answers to the following questions:

1. Why do you think there are the two similar options of REJECT as well as DROP in the IPTables rules?   
     
   [your answer]

Reject is when you want the other end of the port to know that it's unreachable, however DROP is for connections to hosts you don't want other users to see. it's more private.

1. How would you specify a rule to block a range of IP addresses, rather than just a single address?   
     
   [your answer]

If you want to block ip addresses that start with 116.xx.xxx.x you could write this block of input “$ sudo iptables -A INPUT -s 116.0.0.0/8 -j DROP”. This will drop any pings coming at you if the following address starts with 116.

1. Would a host-based firewall like IPTables be effective in protecting a large network of computers? Why?  
     
   [your answer]

Although deploying IPTables has its benefits like stopping unwanted traffic heading to your system. Deploying it on a large network may be time consuming because to configure a host based firewall and many servers is not practical.