|  |  |
| --- | --- |
| **1Durham College** | |
| **Course** | **INFT1103** |
| **Professor** | **Ida Leung** |
| **Student Name** | Maisha Khatoon |
| **Lab#4 Linux System** | |

**Part 1: Basic Linux Administration**

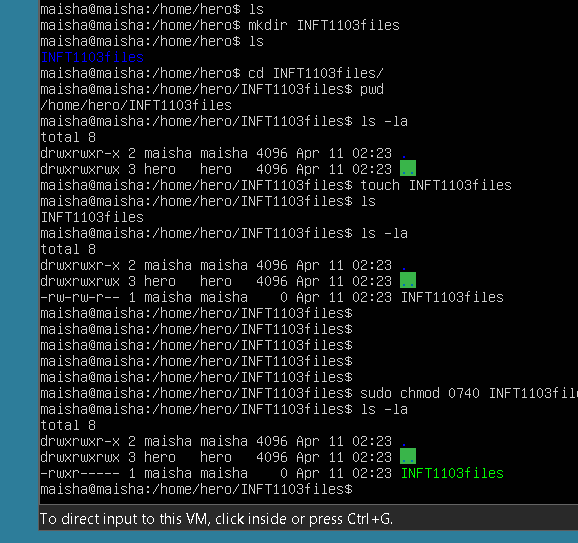
1. Download Ubuntu Server 22.04 from here: <https://ubuntu.com/download/server> (choose “manual server installation” to get the download file)
2. Create a new VM using the Ubuntu Server 22.04 iso
   1. For the username setup, use your name
3. If you are using AWS, select the right version to install
4. Once the server is installed, login with your created username (your name)
5. Once you are logged in, use the command “cd /”
6. Use the command “ls -la”
7. Use the command “locale”
8. Create a local user account. Use the command (without the brackets): *sudo adduser [your favorite movie character]*
9. Use the command *cd /home*
10. Use the command *sudo chmod 0777 /home/[movie character]*
    1. Use the command *ls -ld /home/[movie character]*
    2. What does the *chmod 0777* command do?

Command gives read write execute privileges to all users meaning owner group and others. ‘0’ sets the highest level of permission.

1. Use the command *cd /home/[movie character]*
2. Create a directory using the command *mkdir INFT1103files*
3. Browse to that directory
4. Create a file within the INFT1103 directory using the command *touch INFT1103file*
5. Use the command *ls -la* to confirm the file permissions.
6. Change the file permissions on the *INFT1103file* as follows:
   1. Owner: rwx
   2. Group: x
   3. Other: none
      1. What command did you use?

Sudo chmod 0740

1. Use the command *ls -la* to show the files contained in your directory and their permissions.
   1. Take a screenshot and paste it here:



**Part 2: Define iptables/nftables rules**

In the following lab, you can use either iptables or nftables to define the rule.

Create another Ubuntu Server 22.04 server as well. Make sure these two servers have connectivities to each other.

Test the ssh function from Server#2 to Server#1. It should be able to ssh to.

Now, check out the iptables/nftables existing rules by issuing the command:

Iptables –L / nft list ruleset

You may need to use sudo to execute those commands

Take a screenshot and paste it here:

Now define an incoming rule on server#1 to prohibit any ssh connection from the source IP of server#2

Check out the IP used for Server#2 to communicate with Server#1. ipconfig –a may able to help out.

What is the configuration you have added to the iptables or nftables?

Now, check out the iptables/nftables existing rules by issuing the command:

Iptables –L / nft list ruleset

You may need to use sudo to execute those commands

Take a screenshot and paste it here:

Try ssh from server#2 to server#1. Success or fail? Why?

Take a screenshot and paste it here: