**Assignment**

**Student Name:** Eryk Gloginski **(L00157413)**

**Course:** BSc Computing

**Module:** Secure System Administration

**Lecturer:** Saim Ghafoor

**Submission Date:** 11/30/2022

**Question 1:**

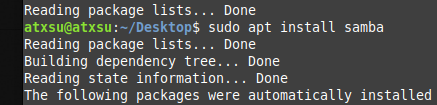
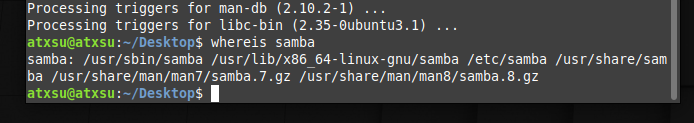
**Part A:**

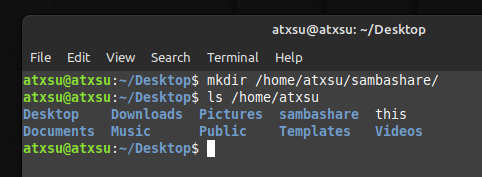
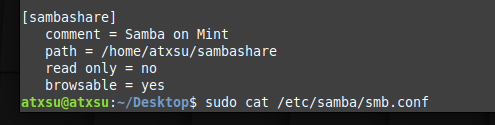
**/etc/systemd/system** – Stores **.service** files which contain a description, requirements, and executable path for a script.  
**/usr/bin** – Stores **distribution-managed** normal everyday use user scripts.  
**/usr/sbin** – Stores **system-managed** super user scripts.

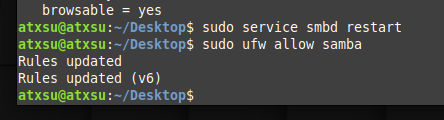
**Part B:**

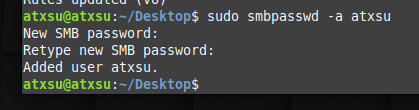
Samba Server is a file server that allows for **file sharing** between **different operating systems** such as Windows, MacOS or Linux.

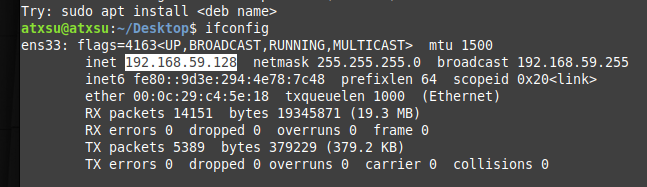
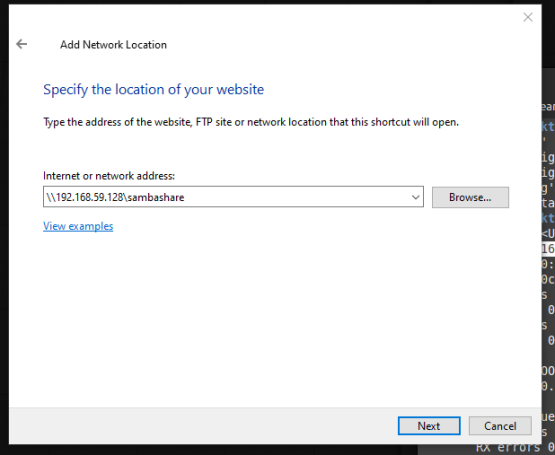
**Part C:**

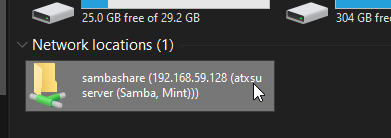
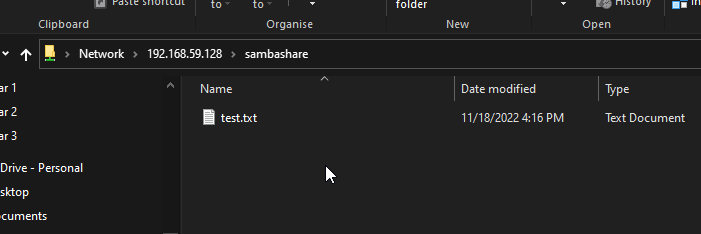
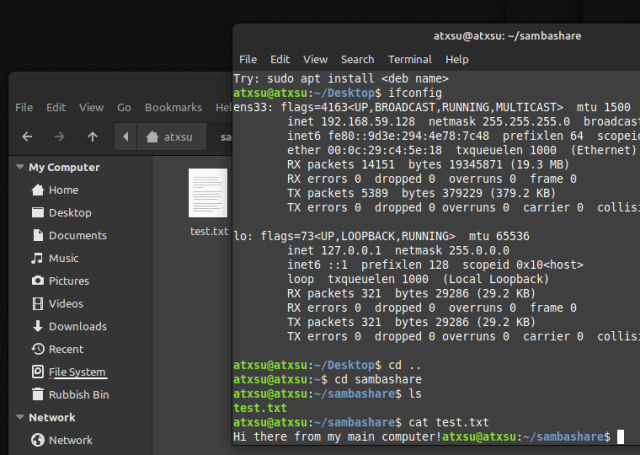
First, I install the **Samba Server** and check if the installation was **successful**.  
  


I make a folder for samba called “**sambashare**” and add it to the config file using “**sudo nano /etc/samba/smb.conf**”. I then save everything pressing **Ctrl + O**, confirming the file name and exiting using **Ctrl + X**.  
  


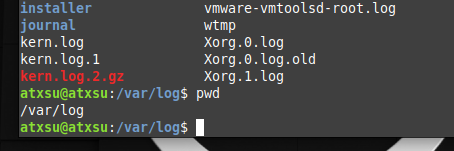
I restart the **smbd** service and update the **firewall** rules to allow **Samba**.  


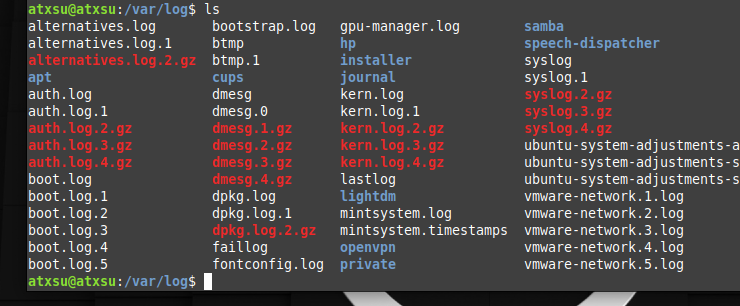
I add a login and password for **Samba** that I will use later to connect through with my Windows 10 computer.  


As this is now set up, I begin checking the **local address** of my current virtual machine and use that to **add a network location** on my main computer in “**This PC**” section by right clicking under “**Devices and drives**”.  
  


You will have to use the login and password that you have specified earlier and after this is complete, you can access that “**sambashare**” folder on your windows computer! I have created a small file called “**test.txt**” where I wrote “Hi there from my main computer!”.  
  
  


**Question 2:**

**Part A:** Folder for logs in Linux. “**/var/log**”  


**Part B:** What types of files exist in this folder? There are **.log files** which for example, contain logs about the booting of the system, **.gz files** which are compressed archives of previous logs and **folders** containing more **.log files**. There is also a **.timestamps** file.  


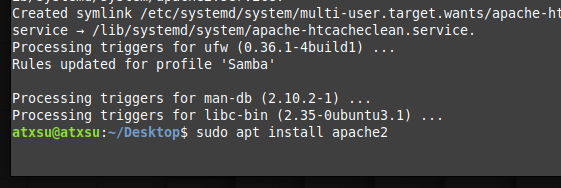
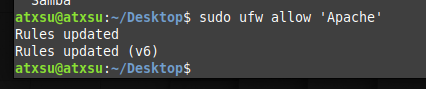
**Part C:** What different commands or ways can be used to filter the log entries?  
**grep** – filters output lines of a file that you have specified – “**sudo grep ‘Manager’ boot.log**”  
**sed** – replaces first input text to second input text – “**sed 's/main/first/' test.txt**”  
**head** – prints out the first 10 lines of a file – “**sudo head boot.log**”  
**tail** – prints out the last 10 lines of a file – “**sudo tail boot.log**”

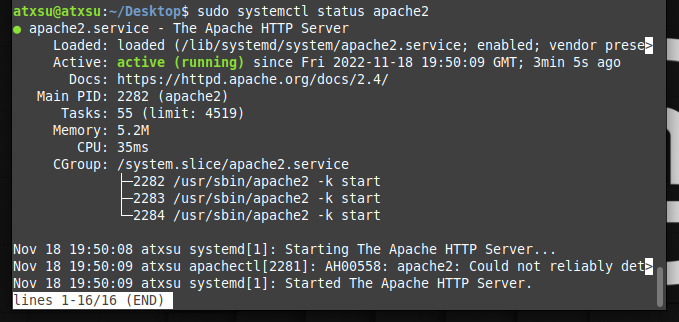
**Part D:** Incomplete…

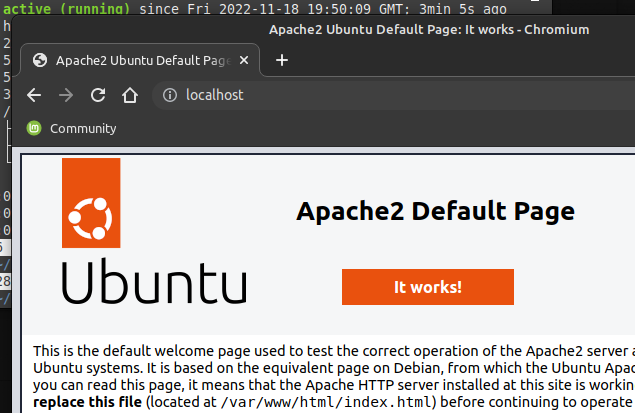
**Part E:** Incomplete…

**Question 3:**

**Part A:**

I install **apache2** using the command “**sudo apt install apache2**” and when I get prompted for anything I select “**Y**” as yes. After the installation is finished, I update the **firewall** rules to allow **Apache**.  
  


Here I show that the **Apache** service is currently running.  


By going to [**http://localhost**](http://localhost), or also in my case [**http://192.168.59.128**](http://192.168.59.128), I can see that the default **Apache** website is up. I am free to edit this **webpage** as I please by using the command “**nano /var/www/info.net/html/index.html**”.  


**Part B:** What different ways can be used to secure the webserver?

Disabling the “**server-info**” directive because you can **view details** about the Apache **configuration** or **sensitive information** regarding the server settings if it is enabled. <http://localhost/server-info>

Disabling the “**server-status**” directive because it **shows information** containing the performance and information of the server, such as uptime, load, current requests, and IP addresses. <http://localhost/server-status>

Disabling the **directory listing** because it allows anyone to **discover and view files** on the webserver when it is enabled.

Setting up a **proper user and group** for the **Apache** server because by default it runs under the **daemon** user and group.

Setting up and **enabling logs** so that it provides **useful information** about the requests of users that have been made on the webserver.