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:

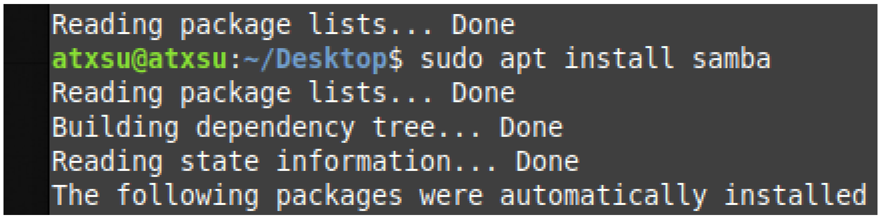
/etc/systemd/system – Stores **.service** files which contain a description, requirements, and executable path for a script.
/usr/bin – Stores **distribution-managed** normal everyday use user scripts.
/usr/sbin – Stores **system-managed** super user scripts.

Part B:

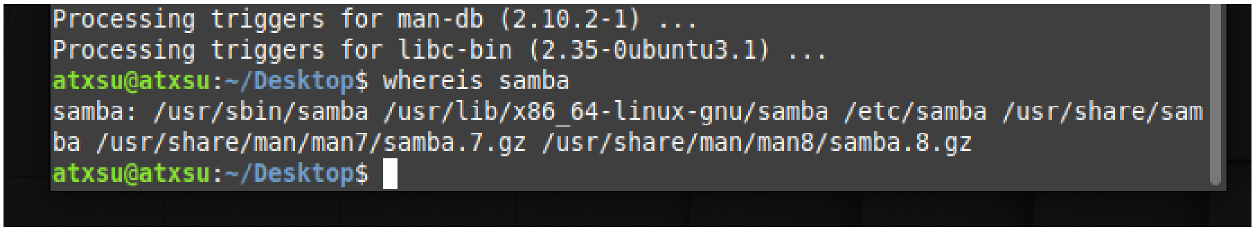
Samba Server is a file server that allows for **file sharing** between **different operating systems** such as Windows, MacOS or Linux.

Part C:

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

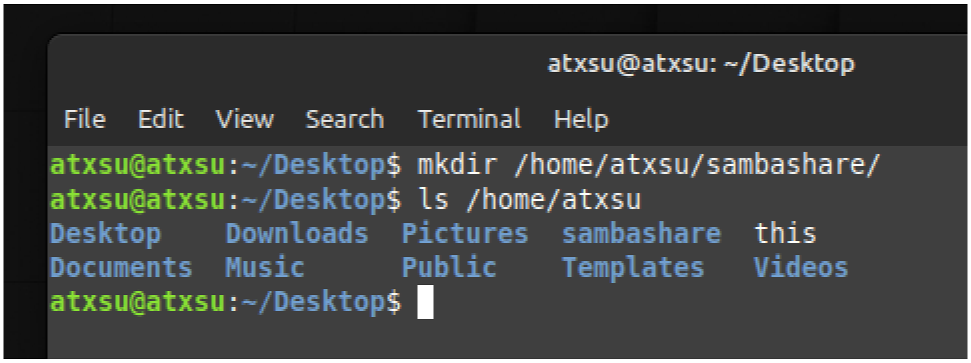


```
Reading package lists... Done
atxsu@atxsu:~/Desktop$ sudo apt install samba
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed
```

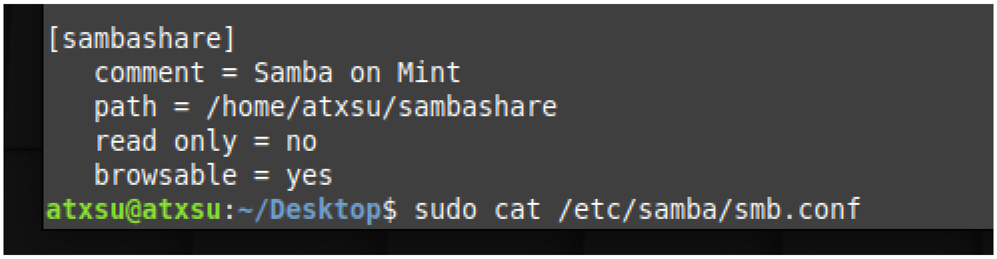


```
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for libc-bin (2.35-0ubuntu3.1) ...
atxsu@atxsu:~/Desktop$ whereis samba
samba: /usr/sbin/samba /usr/lib/x86_64-linux-gnu/samba /etc/samba /usr/share/sam
ba /usr/share/man/man7/samba.7.gz /usr/share/man/man8/samba.8.gz
atxsu@atxsu:~/Desktop$ 
```

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**.

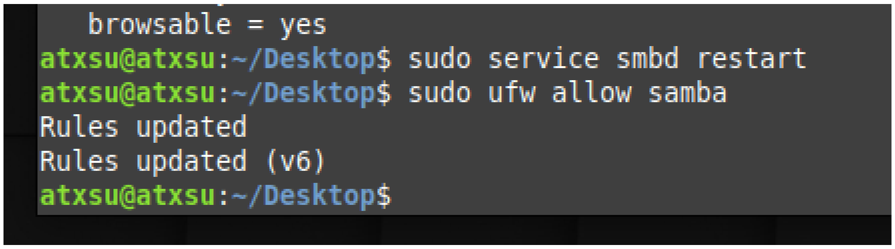


```
atxsu@atxsu:~/Desktop$ mkdir /home/atxsu/sambashare/
atxsu@atxsu:~/Desktop$ ls /home/atxsu
Desktop    Downloads  Pictures  sambashare  this
Documents  Music      Public    Templates   Videos
atxsu@atxsu:~/Desktop$
```



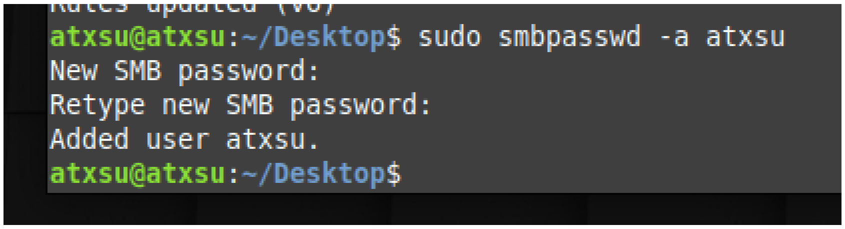
```
[sambashare]
   comment = Samba on Mint
   path = /home/atxsu/sambashare
   read only = no
   browsable = yes
atxsu@atxsu:~/Desktop$ sudo cat /etc/samba/smb.conf
```

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



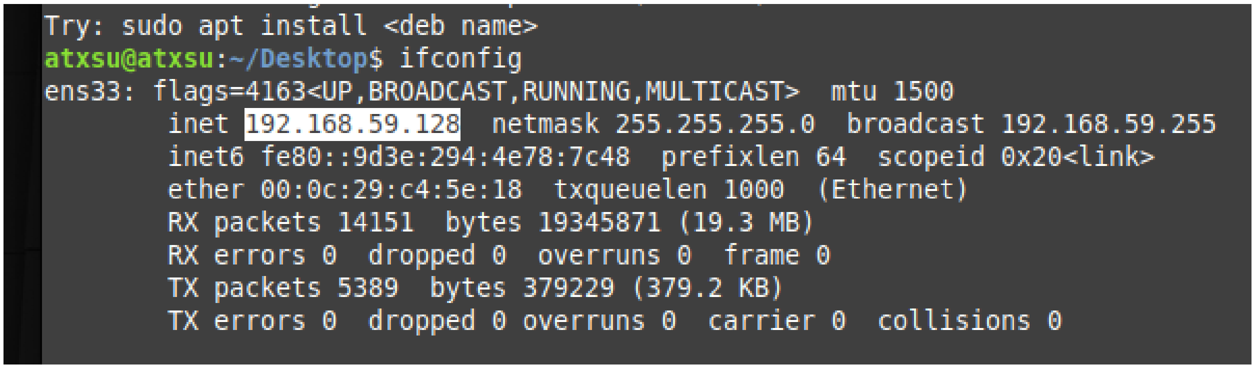
```
   browsable = yes
atxsu@atxsu:~/Desktop$ sudo service smbd restart
atxsu@atxsu:~/Desktop$ sudo ufw allow samba
Rules updated
Rules updated (v6)
atxsu@atxsu:~/Desktop$
```

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

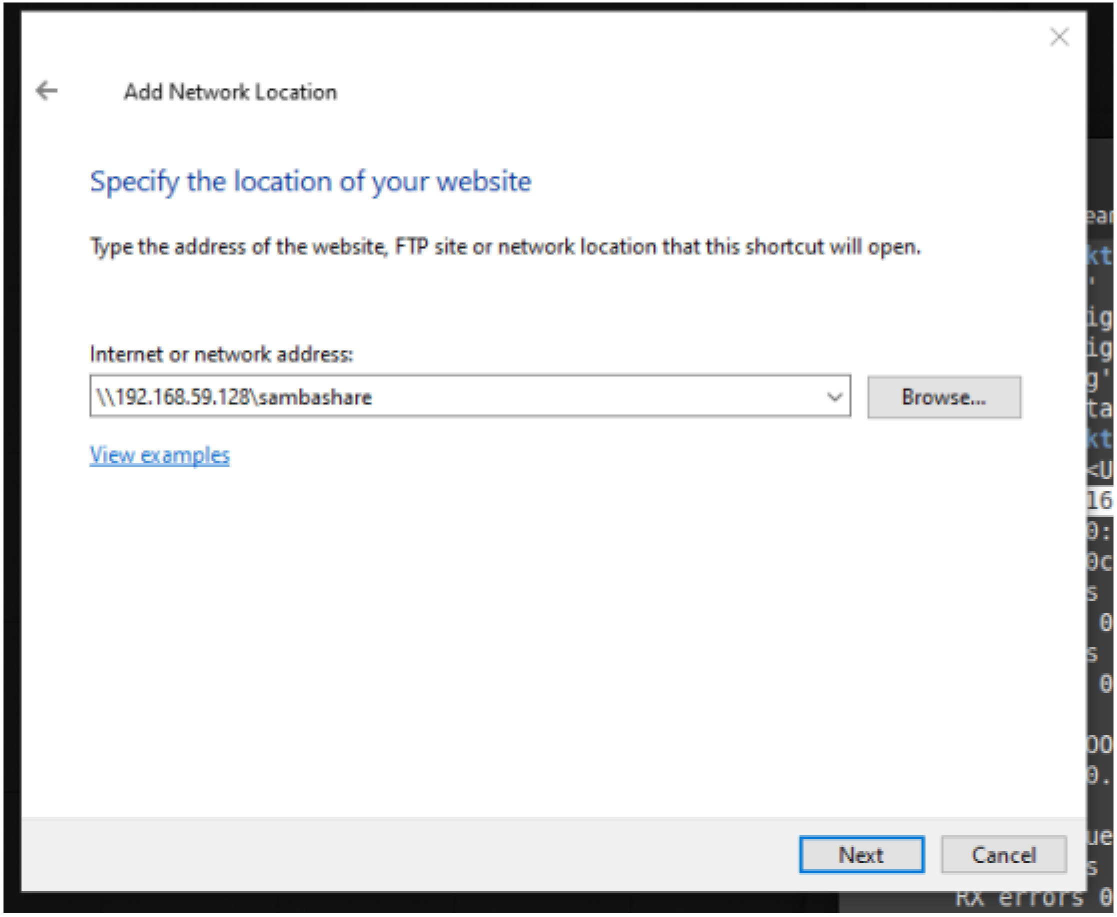


```
Rules updated (v6)
atxsu@atxsu:~/Desktop$ sudo smbpasswd -a atxsu
New SMB password:
Retype new SMB password:
Added user atxsu.
atxsu@atxsu:~/Desktop$
```

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**”.



```
Try: sudo apt install <deb name>
atxsu@atxsu:~/Desktop$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.59.128  netmask 255.255.255.0  broadcast 192.168.59.255
        inet6 fe80::9d3e:294:4e78:7c48  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:c4:5e:18  txqueuelen 1000  (Ethernet)
        RX packets 14151  bytes 19345871 (19.3 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 5389  bytes 379229 (379.2 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```



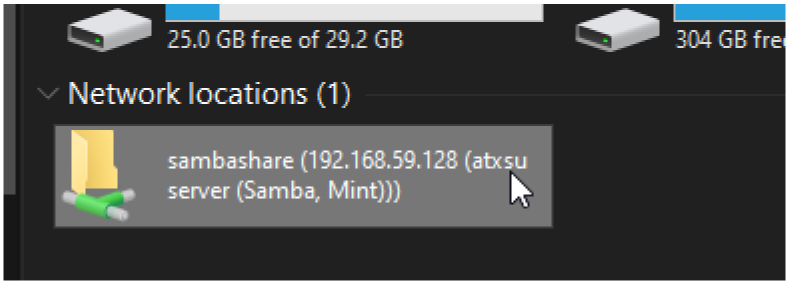
Add Network Location

Specify the location of your website

Type the address of the website, FTP site or network location that this shortcut will open.

Internet or network address: \\192.168.59.128\sambashare

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!”.

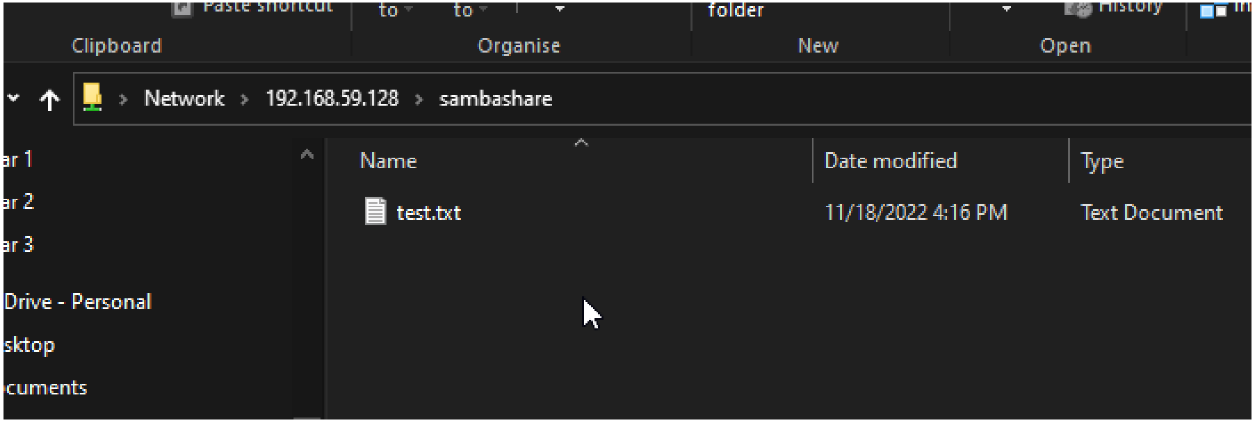


25.0 GB free of 29.2 GB

304 GB fre

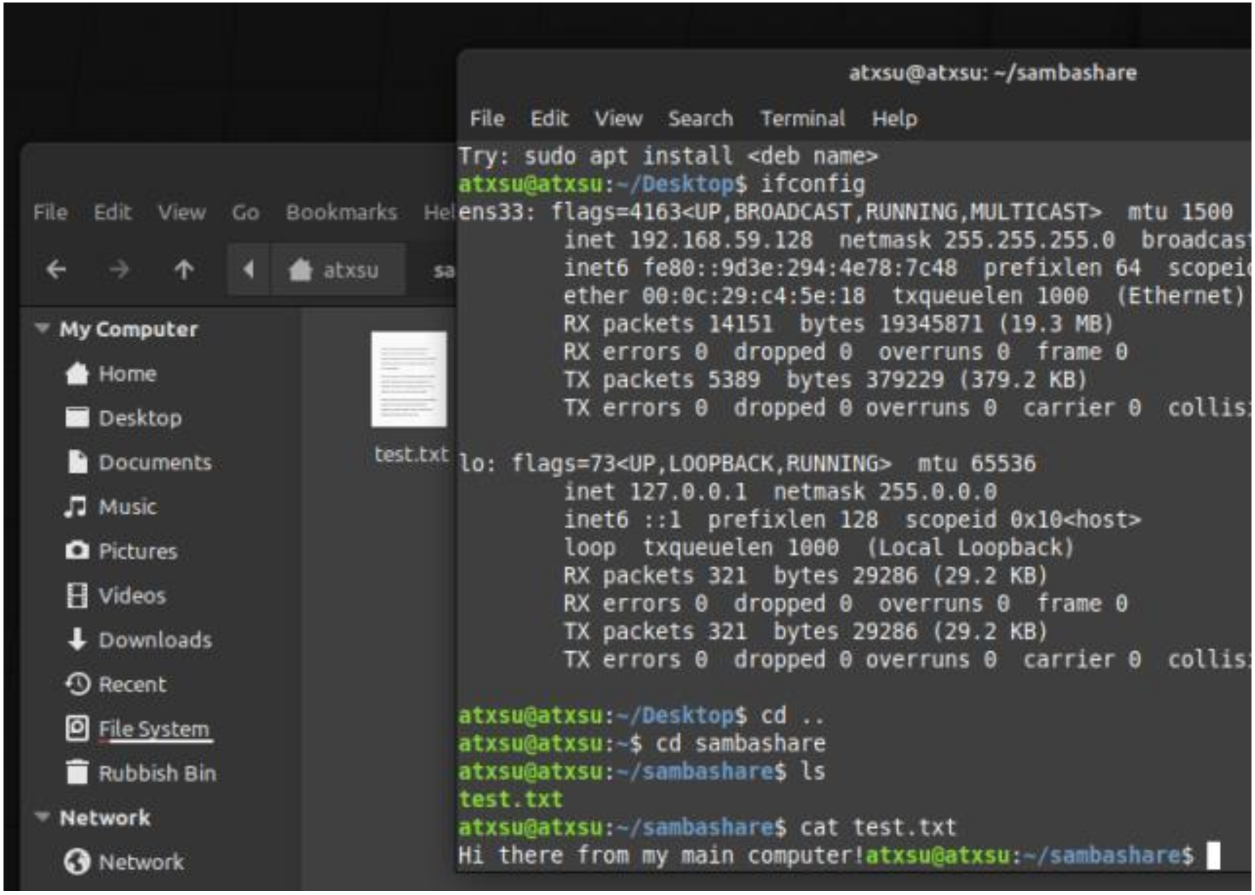
Network locations (1)

sambashare (192.168.59.128 (atxsu server (Samba, Mint)))



Network › 192.168.59.128 › sambashare

Name	Date modified	Type
test.txt	11/18/2022 4:16 PM	Text Document



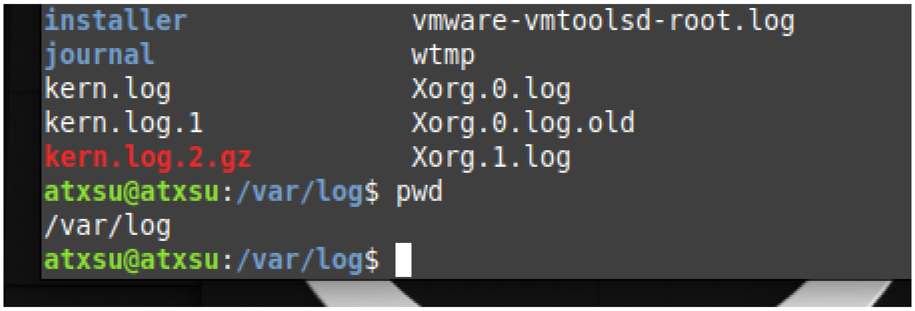
```
Try: sudo apt install <deb name>
atxsu@atxsu:~/Desktop$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.59.128  netmask 255.255.255.0  broadcas
        inet6 fe80::9d3e:294:4e78:7c48  prefixlen 64  scopei
        ether 00:0c:29:c4:5e:18  txqueuelen 1000  (Ethernet)
        RX packets 14151  bytes 19345871 (19.3 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 5389  bytes 379229 (379.2 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collis

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 321  bytes 29286 (29.2 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 321  bytes 29286 (29.2 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collis

atxsu@atxsu:~/Desktop$ cd ..
atxsu@atxsu:~$ cd sambashare
atxsu@atxsu:~/sambashare$ ls
test.txt
atxsu@atxsu:~/sambashare$ cat test.txt
Hi there from my main computer!atxsu@atxsu:~/sambashare$
```

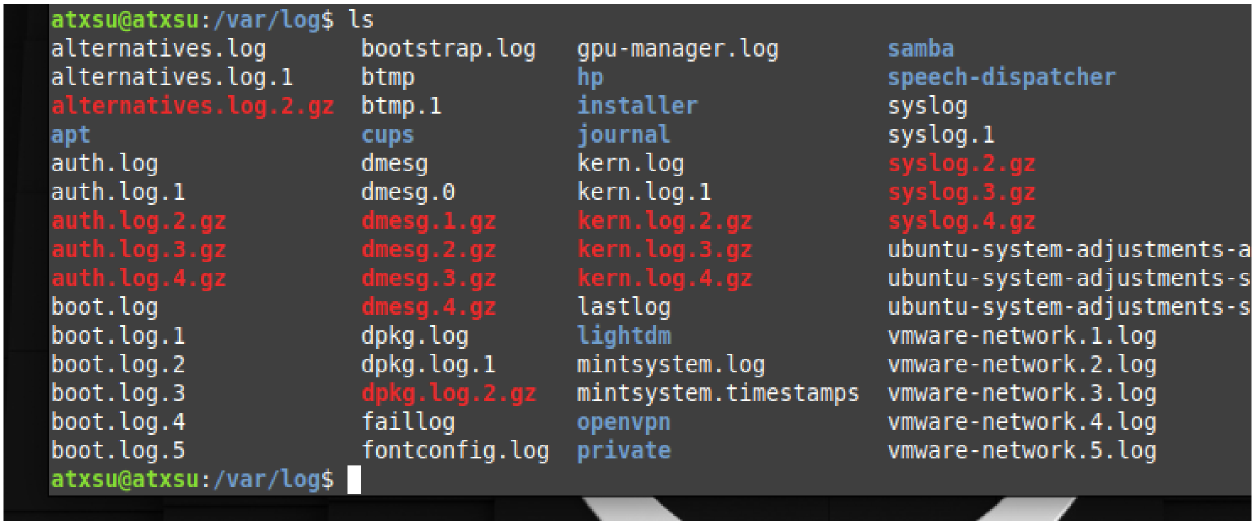
Question 2:

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



```
installer              vmware-vmtoolsd-root.log
journal                wtmp
kern.log               Xorg.0.log
kern.log.1             Xorg.0.log.old
kern.log.2.gz          Xorg.1.log
atxsu@atxsu:/var/log$ pwd
/var/log
atxsu@atxsu:/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.



```
atxsu@atxsu:/var/log$ ls
alternatives.log       bootstrap.log   gpu-manager.log        samba
alternatives.log.1     btmp            hp                     speech-dispatcher
alternatives.log.2.gz  btmp.1          installer              syslog
apt                    cups            journal                syslog.1
auth.log               dmesg           kern.log               syslog.2.gz
auth.log.1             dmesg.0         kern.log.1             syslog.3.gz
auth.log.2.gz          dmesg.1.gz      kern.log.2.gz          syslog.4.gz
auth.log.3.gz          dmesg.2.gz      kern.log.3.gz          ubuntu-system-adjustments-a
auth.log.4.gz          dmesg.3.gz      kern.log.4.gz          ubuntu-system-adjustments-s
boot.log               dmesg.4.gz      lastlog                ubuntu-system-adjustments-s
boot.log.1             dpkg.log        lightdm                vmware-network.1.log
boot.log.2             dpkg.log.1      mintsystem.log         vmware-network.2.log
boot.log.3             dpkg.log.2.gz   mintsystem.timestamps  vmware-network.3.log
boot.log.4             faillog         openvpn                vmware-network.4.log
boot.log.5             fontconfig.log  private                vmware-network.5.log
atxsu@atxsu:/var/log$
```

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**"

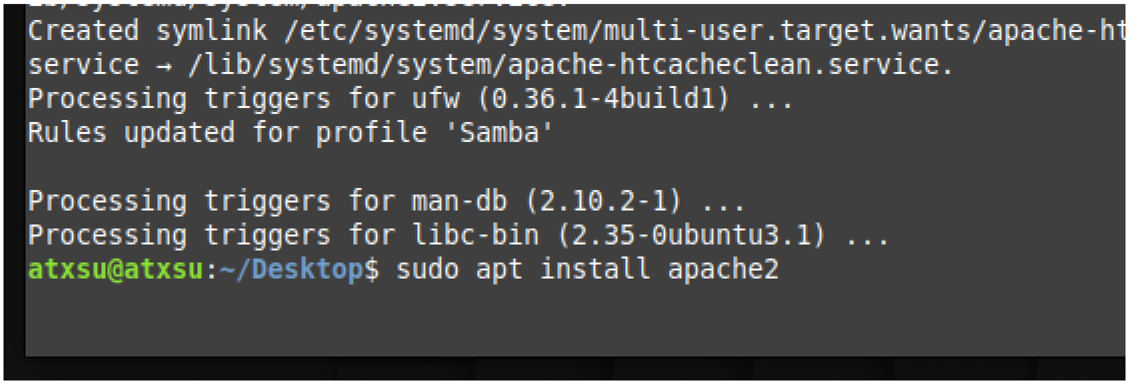
Part D: Incomplete…

Part E: Incomplete…

Question 3:

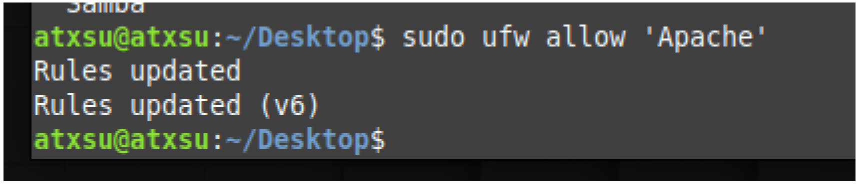
Part A:

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**.



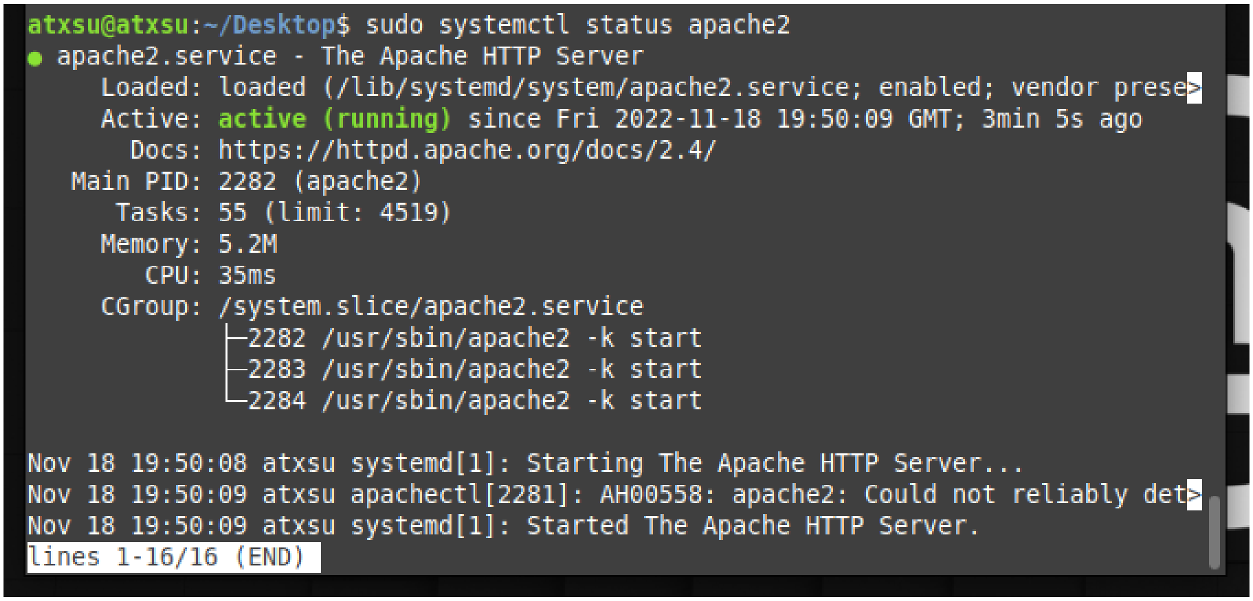
```
Created symlink /etc/systemd/system/multi-user.target.wants/apache-ht
service → /lib/systemd/system/apache-htcacheclean.service.
Processing triggers for ufw (0.36.1-4build1) ...
Rules updated for profile 'Samba'

Processing triggers for man-db (2.10.2-1) ...
Processing triggers for libc-bin (2.35-0ubuntu3.1) ...
atxsu@atxsu:~/Desktop$ sudo apt install apache2
```



```
  Samba
atxsu@atxsu:~/Desktop$ sudo ufw allow 'Apache'
Rules updated
Rules updated (v6)
atxsu@atxsu:~/Desktop$
```

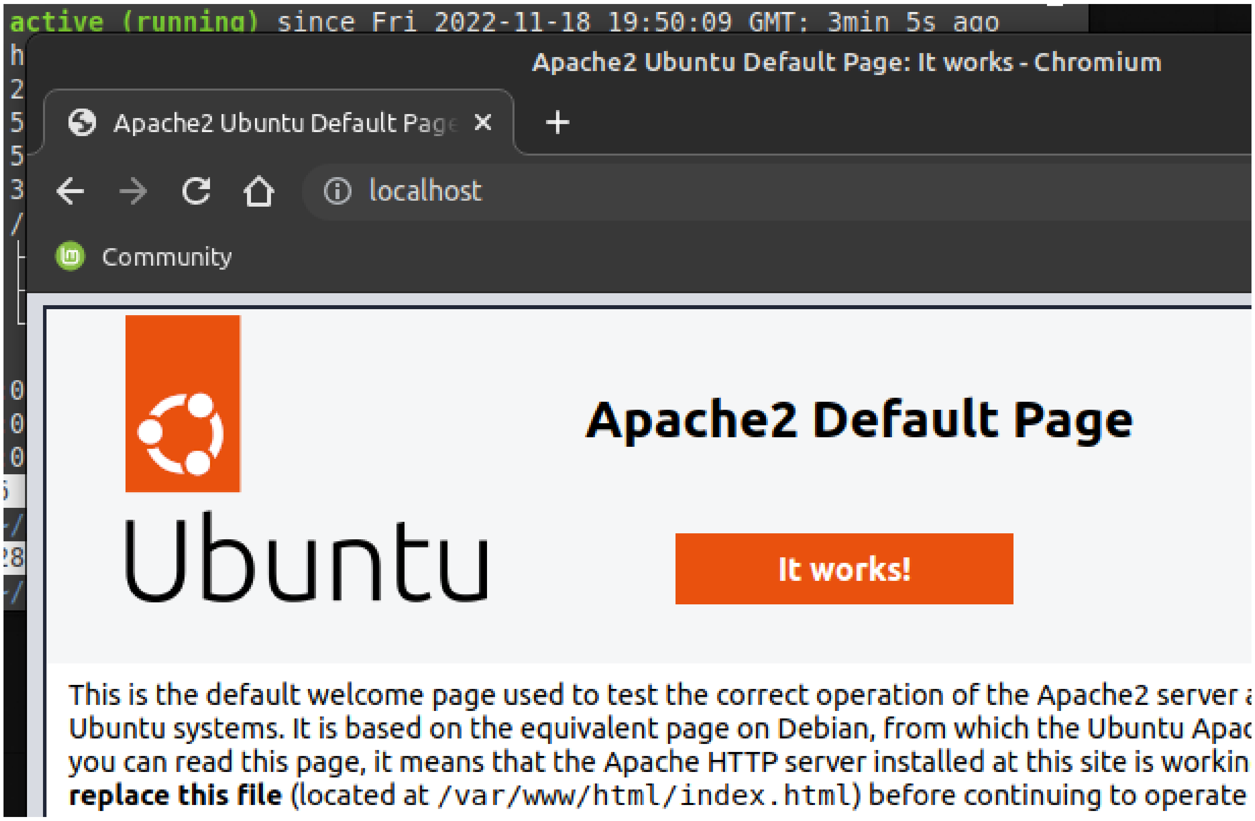
Here I show that the **Apache** service is currently running.



```
atxsu@atxsu:~/Desktop$ sudo systemctl status apache2
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor prese>
     Active: active (running) since Fri 2022-11-18 19:50:09 GMT; 3min 5s ago
       Docs: https://httpd.apache.org/docs/2.4/
   Main PID: 2282 (apache2)
      Tasks: 55 (limit: 4519)
     Memory: 5.2M
        CPU: 35ms
     CGroup: /system.slice/apache2.service
             ├─2282 /usr/sbin/apache2 -k start
             ├─2283 /usr/sbin/apache2 -k start
             └─2284 /usr/sbin/apache2 -k start

Nov 18 19:50:08 atxsu systemd[1]: Starting The Apache HTTP Server...
Nov 18 19:50:09 atxsu apachectl[2281]: AH00558: apache2: Could not reliably det>
Nov 18 19:50:09 atxsu systemd[1]: Started The Apache HTTP Server.
lines 1-16/16 (END)
```

By going to http://localhost, or also in my case 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**".



```
active (running) since Fri 2022-11-18 19:50:09 GMT; 3min 5s ago
```

Apache2 Ubuntu Default Page: It works - Chromium
Apache2 Ubuntu Default Page
localhost
Community
Ubuntu

Apache2 Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server a
Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apac
you can read this page, it means that the Apache HTTP server installed at this site is workin
replace this file (located at `/var/www/html/index.html`) before continuing to operate

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.