**Logo, company name

Description automatically generated**

**GROUP ASSIGNMENT**

**CT106-3-2-SNA**

**SYSTEM AND NETWORK ADMINISTRATION**

**APD2F2309CS(CYB)**

**HAND OUT DATE : 3RD WEEK**

**HAND IN DATE : 14TH WEEK**

|  |  |
| --- | --- |
| **NAME** | **TPNUMBER** |
| **IBRAHEEM MOHAMMED IMADELDIN AWAD** | **TP070765** |
| **ABDULELAH HUSSEIN ABDULRAHMAN AL-KAF** | **TP069319** |
| **MUHAMAD AHMAD AL MUHDAR** | **TP070208** |
| **ABDULRAHMAN GAMIL MOHAMMED AHMED** | **TP071012** |

**TABLE OF CONTENT**

[INTRODUCTION 4](#_Toc154152588)

[1.0 SYSTEM INSTALLATION. 5](#_Toc154152589)

[1.1 SYSTEM SPECIFICATIONS. 5](#_Toc154152590)

[1.2 INSTALLATION. 5](#_Toc154152591)

[2.0 SYSTEM CONFIGURATION. 11](#_Toc154152592)

[2.1 User Configuration. 11](#_Toc154152593)

[2.2 File and Directory Management 11](#_Toc154152594)

[3.0 NETWORK CONFIGURATION. 16](#_Toc154152595)

[4.0 IP TABLE CONFIGURATION. 20](#_Toc154152596)

[5.0 NETWORK FILE SYSTEM (NFS) CONFIGURATION. 21](#_Toc154152597)

[6.0 CERTIFICATE AUTHORITY (CA) CONFIGURATION. 26](#_Toc154152598)

[CONCLUSION 29](#_Toc154152599)

[REFERENCES 30](#_Toc154152600)

**LIST OF FIGURES**

[Figure 1 6](#_Toc154140213)

[Figure 2 7](#_Toc154140214)

[Figure 3 8](#_Toc154140215)

[Figure 4 8](#_Toc154140216)

[Figure 5 9](#_Toc154140217)

[Figure 6 9](#_Toc154140218)

[Figure 7 10](#_Toc154140219)

[Figure 8 10](#_Toc154140220)

[Figure 9 11](#_Toc154140221)

[Figure 10 11](#_Toc154140222)

[Figure 11 12](#_Toc154140223)

[Figure 12 12](#_Toc154140224)

[Figure 13 13](#_Toc154140225)

[Figure 14 13](#_Toc154140226)

[Figure 15 14](#_Toc154140227)

[Figure 16 14](#_Toc154140228)

[Figure 17 14](#_Toc154140229)

[Figure 18 15](#_Toc154140230)

[Figure 19 15](#_Toc154140231)

[Figure 20 16](#_Toc154140232)

[Figure 21 17](#_Toc154140233)

[Figure 22 18](#_Toc154140234)

[Figure 23 18](#_Toc154140235)

[Figure 24 19](#_Toc154140236)

[Figure 25 20](#_Toc154140237)

[Figure 26 21](#_Toc154140238)

[Figure 27 21](#_Toc154140239)

[Figure 28 22](#_Toc154140240)

[Figure 29 22](#_Toc154140241)

[Figure 30 23](#_Toc154140242)

[Figure 31 24](#_Toc154140243)

[Figure 32 24](#_Toc154140244)

[Figure 33 24](#_Toc154140245)

[Figure 34 25](#_Toc154140246)

[Figure 35 25](#_Toc154140247)

[Figure 36 26](#_Toc154140248)

[Figure 37 26](#_Toc154140249)

[Figure 38 27](#_Toc154140250)

[Figure 39 28](#_Toc154140251)

[Figure 40 29](#_Toc154140252)

[Figure 41 30](#_Toc154140253)

# INTRODUCTION

The introduction of new technologies has greatly increased the need for stable server settings, especially when it comes to Linux systems. The modern digital environment has increased the need for thorough instructions and skillful methods for installing and configuring Linux servers. This study is evidence of how carefully and thoroughly the many factors that are necessary to create a safe and effective Linux server environment have been addressed.

Examining a wide range of crucial processes, such as the first system installation, complex network setups, and strict security protocols, the study carefully outlines the necessary actions and protocols. The thorough examination of Linux administration tasks presented in the book clearly demonstrates the extent of planning and implementation needed for optimal server performance and strengthened system security.

# 1.0 SYSTEM INSTALLATION.

## SYSTEM SPECIFICATIONS.

Specification for the installation of Ubuntu is the same for all members.

1. Operating System Type: Linux
2. Version: Ubuntu 64bit
3. System memory (RAM): 2GB
4. Storage: 50GB

## 1.2 INSTALLATION.

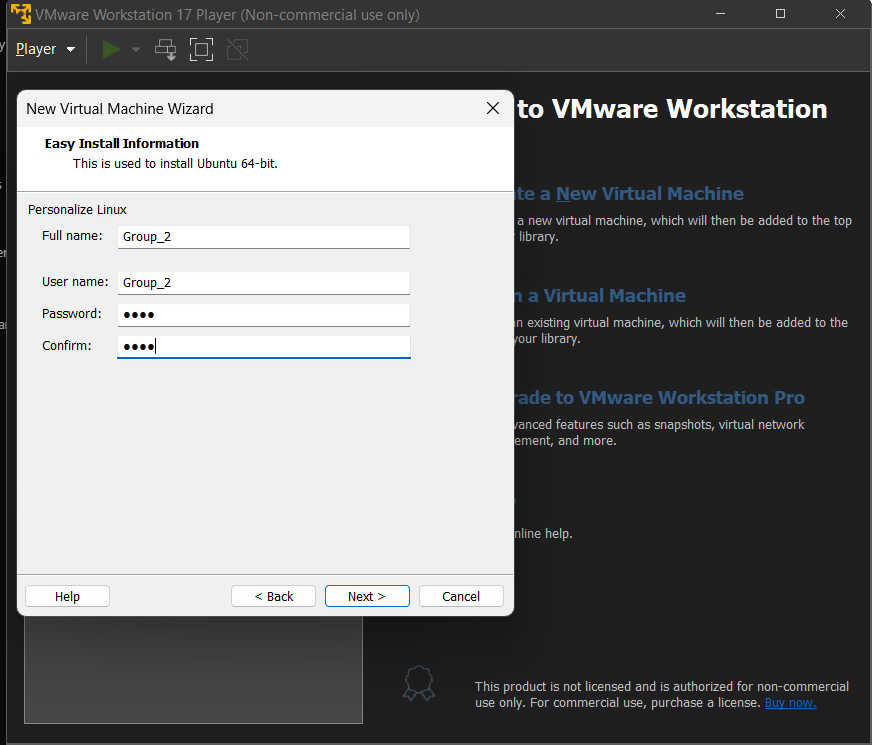


Figure 1

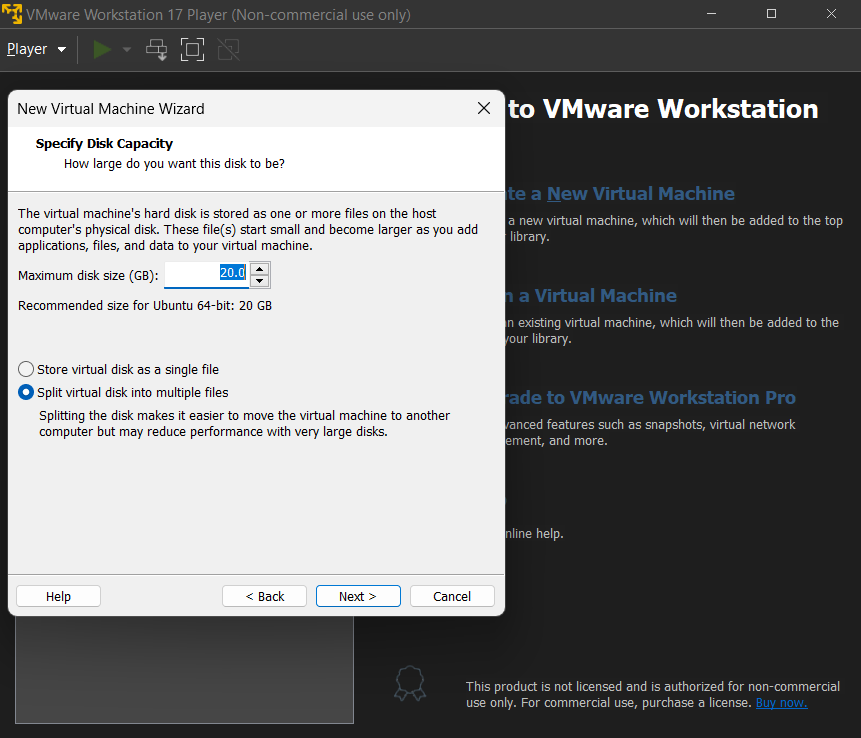


Figure 2

A screenshot of a computer

Description automatically generated

Figure 3

A screenshot of a computer

Description automatically generated

Figure 4

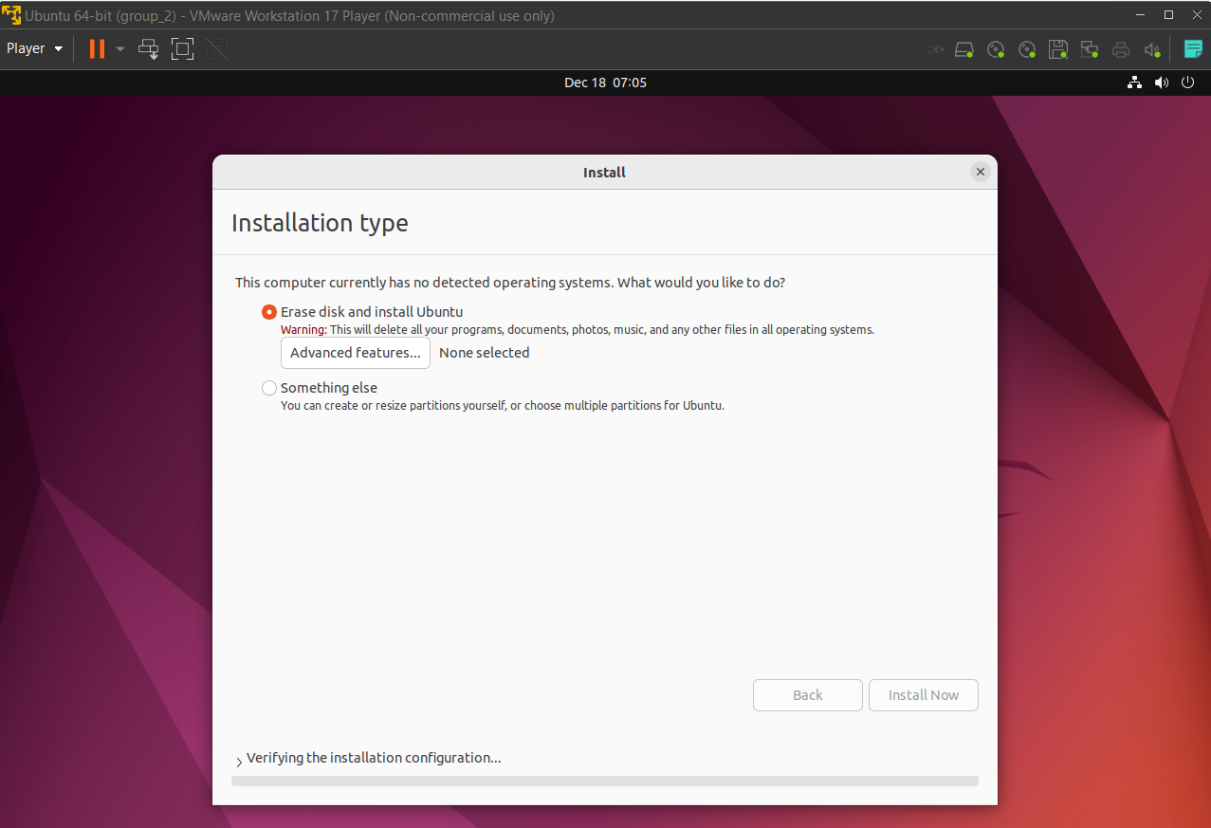


Figure 5

A screenshot of a computer

Description automatically generated

Figure 6

A screenshot of a computer

Description automatically generated

Figure 7

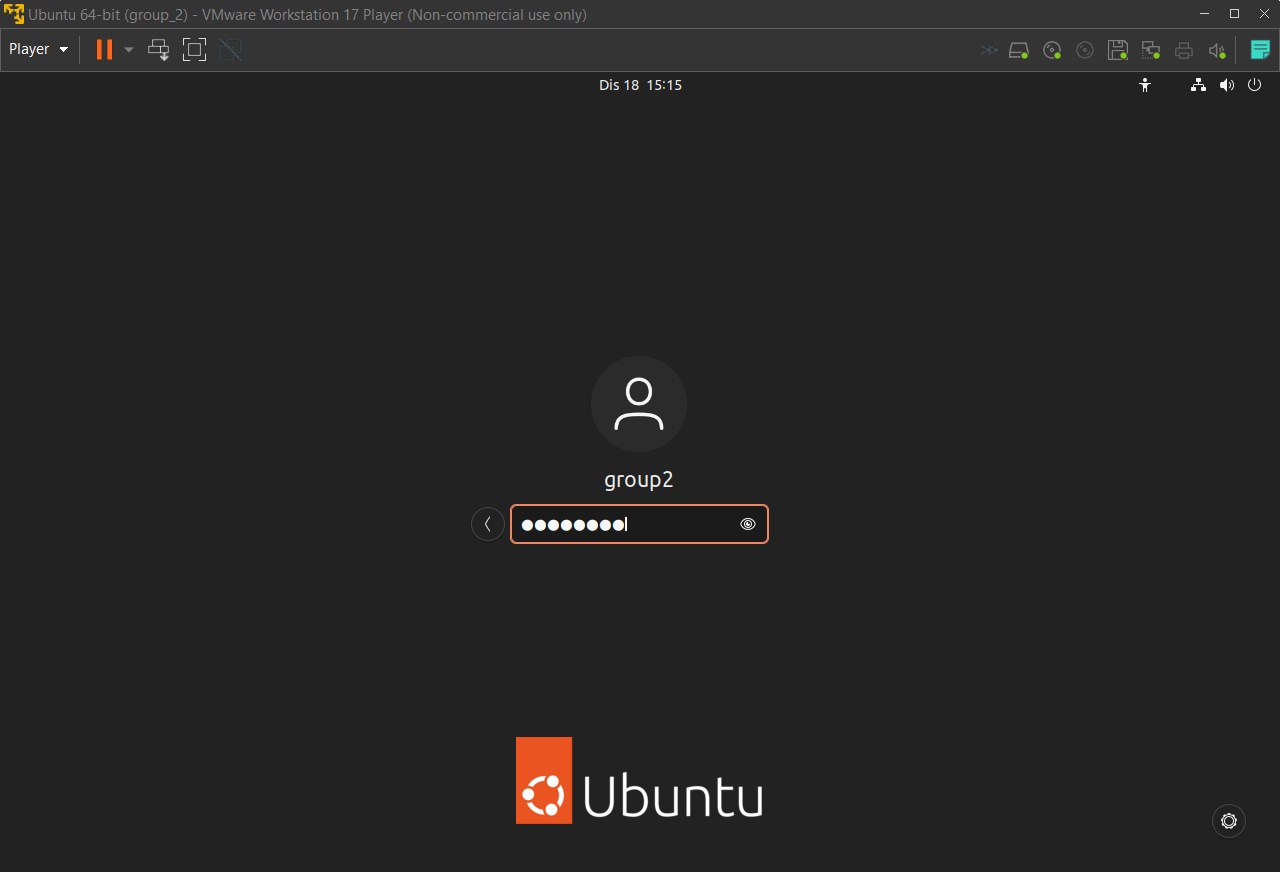
\

Figure 8

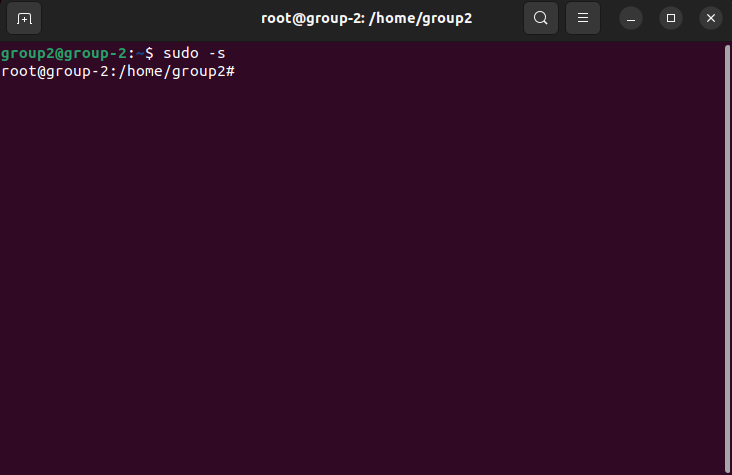


Figure 9

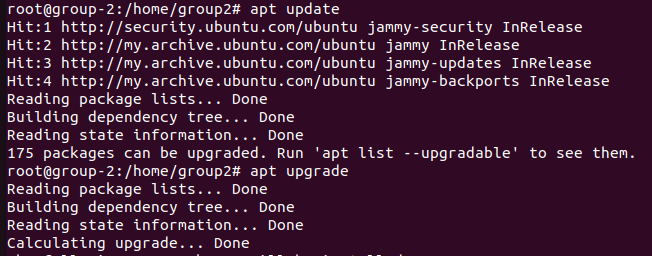


Figure 10

Figures 1 to 10 show the creation process, setting up and installation process, as well as opening the terminal and accessing the root, and finally updating and upgrading the system to have the latest updates installed on the operating system.

# 2.0 SYSTEM CONFIGURATION.

## User Configuration.

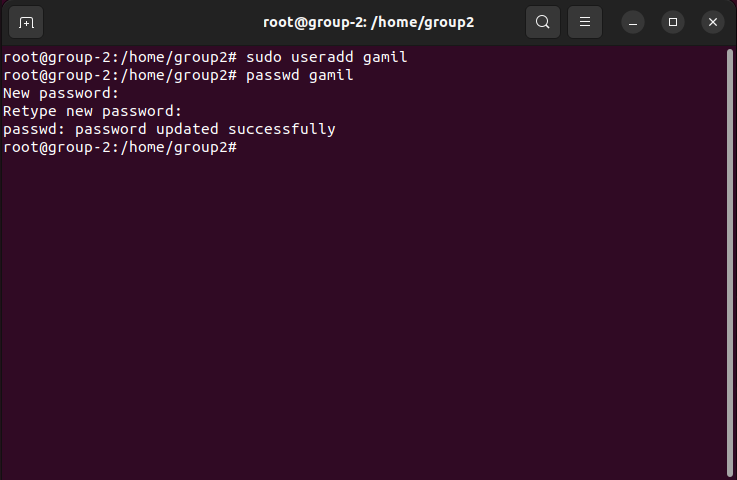


Figure 11

Figure 11 shows the command “sudo useradd gamil” being used to create a new user account named “gamil”, following that the “passwd gamil” command was then used to specify a password for the newly created user.

## File and Directory Management

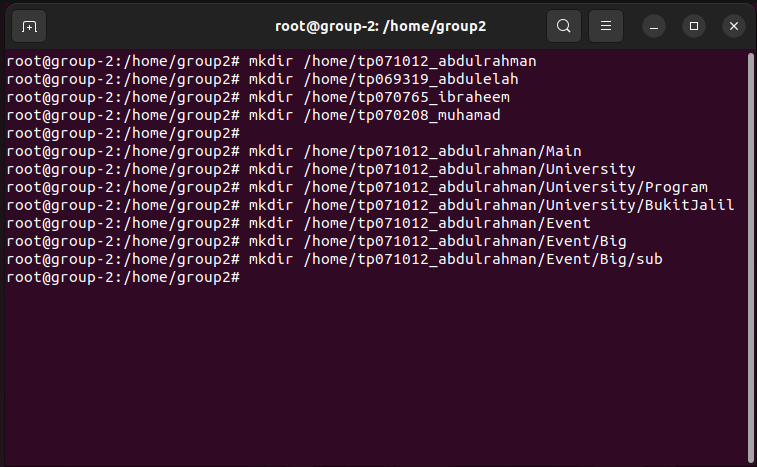


Figure 12

Using the “mkdir” command, the root user creates several user-specific folders under the Linux system's home directory in the terminal session that is shown in Figure 12. The first step in this process entails naming the main directories after specific users: Abdulrahman, Abdullelah, Ibraheem, and Muhammad. After completing these steps, the user creates an organized hierarchy of subdirectories inside of Abdulrahman's directory. These include subdirectories, sub and Big, as well as categories like University, Program, and Main. The user data is organized with great care, and there is even an Event directory that branches out into other directories.

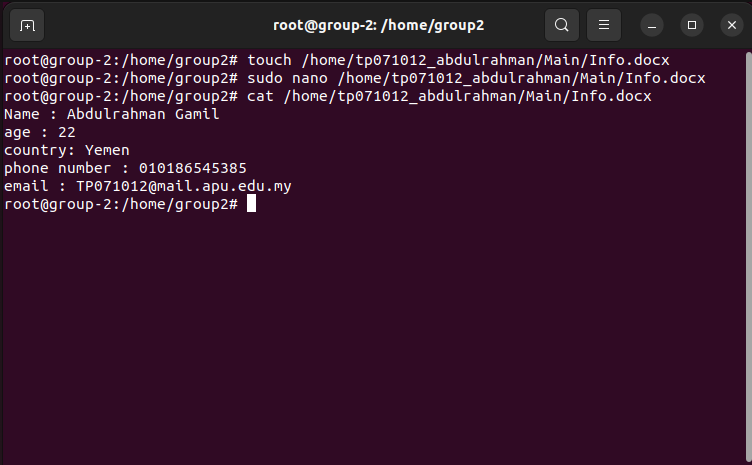


Figure 13

Figure 13 shows a new document being created under the “tp071012\_abdulrahman” directory where the “Info.docx” document created is used to store information of “Abdulrahman Gamil” and that is made possible by using the “cat” command.

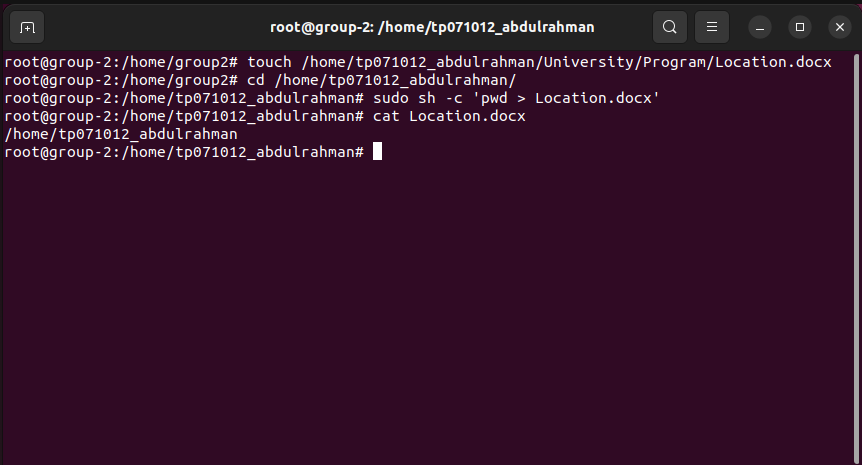


Figure 14

Figure 14 shows the “Location.docx” document being created in the “Program” directory which is under the “University” directory. The “pwd” command is used to print the current working directory in which the user is in.



Figure 15

Figure 15 shows the creation of the “Time.docx” document under the “BukitJalil” directory where the server time zone will stored and the time zone will be obtained by using the time zone command “timedatectl | grep "Time zone".

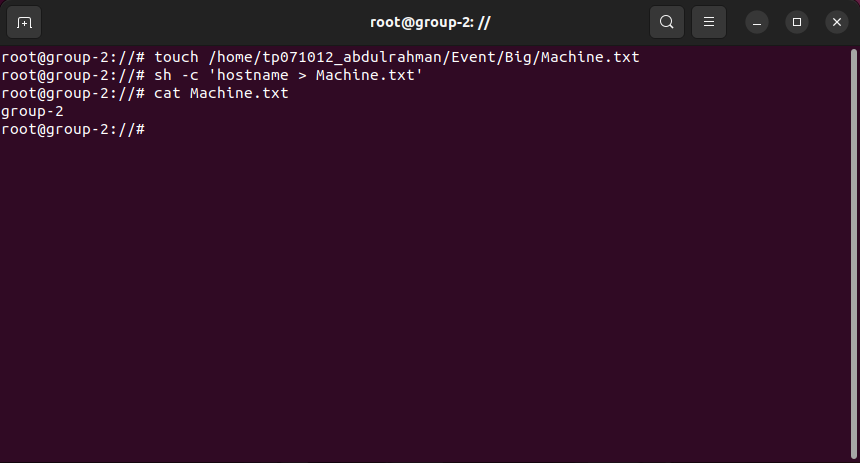


Figure 16

Figure 16 shows the creation of a new, empty file named “Machine.txt”. This file is created under the “Big” directory which is under the “Event” directory. A shell command is then executed using the “sh -c” which is used to redirect the output of “hostname”, this writes the network name of the system to “Machine.txt”. When the contents of the file are finally seen using cat Machine.txt, the hostname of the system is shown to be "group-2".

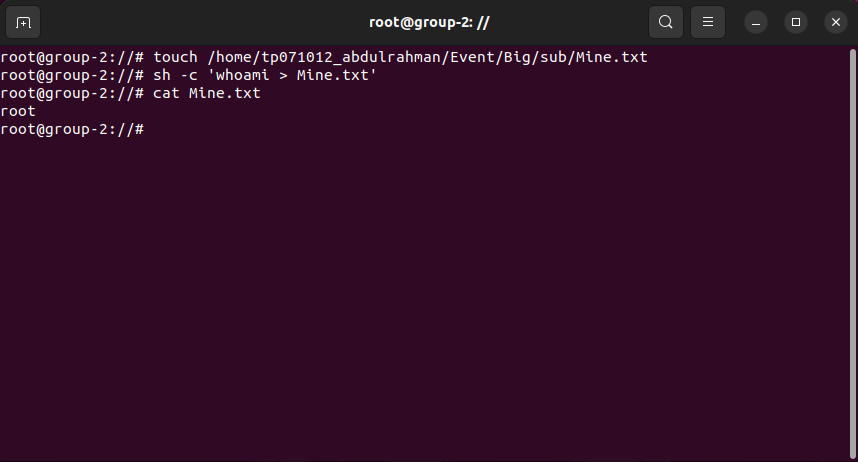


Figure 17

Figure 17 shows that an empty file named "Mine.txt" is created in a subfolder of Abdulrahman's event directory. then issue a command to write the current user's output from “whoami” into “Mine.txt”. The contents of “Mine.txt” are shown using the “cat” command, demonstrating that the current user is 'root'.

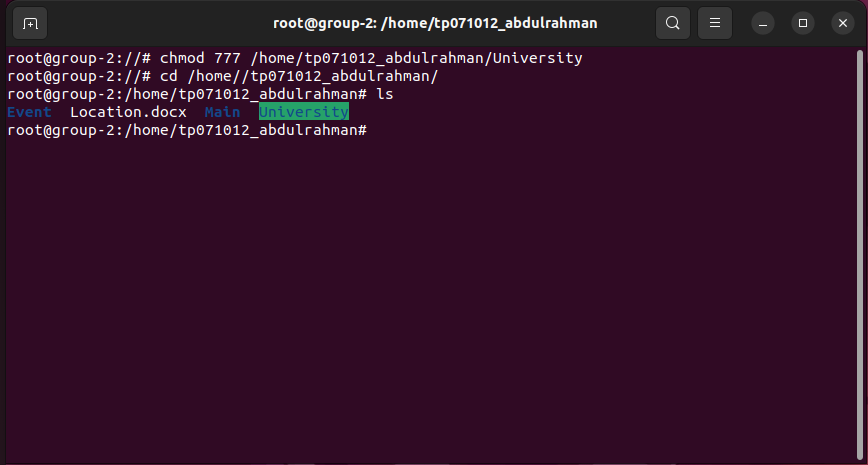


Figure 18

The root user in Abdulrahman's home directory sets all users' read, write, and execute rights (chmod 777) on the 'University' directory as shown in Figure 18. Then, the user uses the "cd" command to go to this directory, and the "ls" command lists its contents. This shows that there are four subdirectories and a file in this directory: Event, Location.docx, Main, and University.

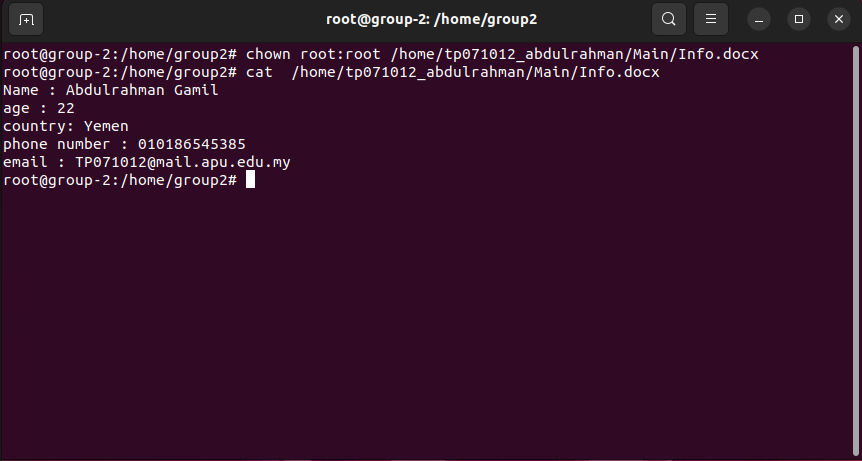


Figure 19

The command chown root: root is executed by the root user in Figure 19 to transfer ownership of the file 'Info.docx' to the root user and group. After that, 'Info.docx's contents are shown using cat, revealing the information of the user "Abdulrahman Gamil". His name, age, nationality, phone number, and email address are all provided. This implies an administrator with root rights reviewing or auditing user information.

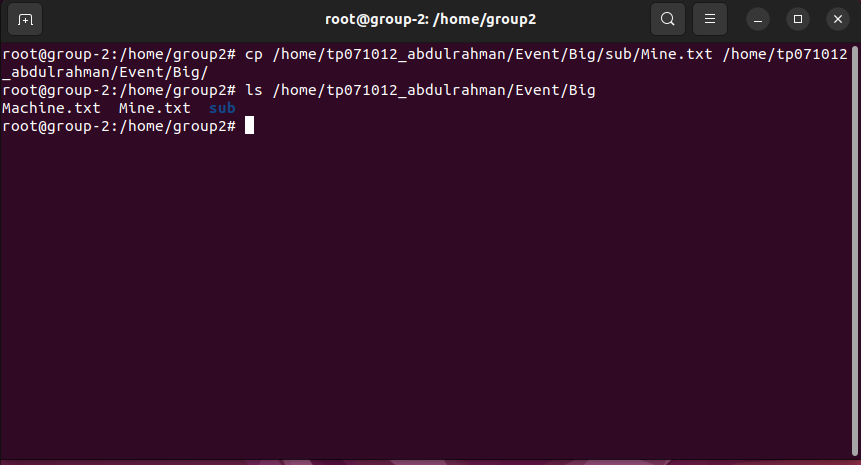


Figure 20

Figure 20 shows the root user executing the copy command “cp” to copy the “Mine.txt” from the subdirectory “sub” found within the “Big” directory to the “Big” directory. The command “ls” to show that the “Mine.txt” file has been copied successfully to the “Big” directory.

# 3.0 NETWORK CONFIGURATION.

Network setup is a basic activity for Linux servers that determines how a server interfaces with other systems and the internet. Network interfaces are usually assigned IP addresses, subnet masks, gateways, and DNS servers. Using command-line tools like ifconfig, ip, nmcli, or netplan apply, you may manage this configuration by altering system files, which are typically located in "/etc/network/" for conventional interfaces or "/etc/netplan/" for more recent Ubuntu versions. For server security and accessibility, a proper network configuration is essential. Network configurations may be uniformly applied across several servers using scripts or configuration management systems like Ansible, Puppet, or Chef for automated deployment and administration.

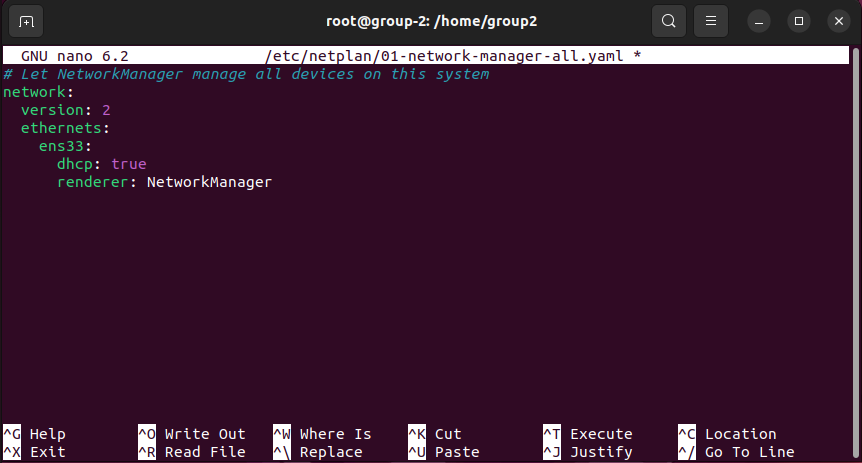
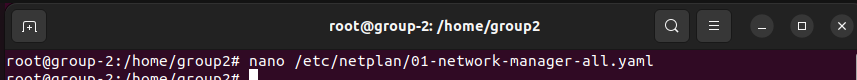


Figure 21

Netplan configuration file "/etc/netplan/01-network-manager-all.yaml" is normally found at this location; Figure 21 illustrates how to update it. All network interfaces on the system may be managed by “NetworkManager” thanks to the setting of this specific Netplan. The network block designates “NetworkManager” as the renderer, meaning that it should manage the network setup for the “ens33” ethernet interface. It also specifies a DHCP-enabled configuration for that interface.

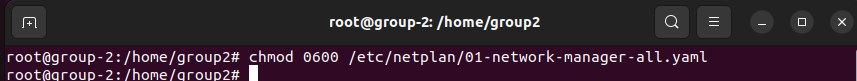


Figure 22

Figure 22 shows the “chmod 0600” command being used where the permissions are changed so that only the owner of the file where only the root user can read and write the file. This ensures that no other users can view or edit this critical networking configuration file, hence enforcing security protocols.

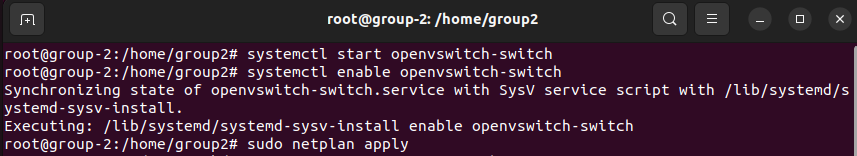
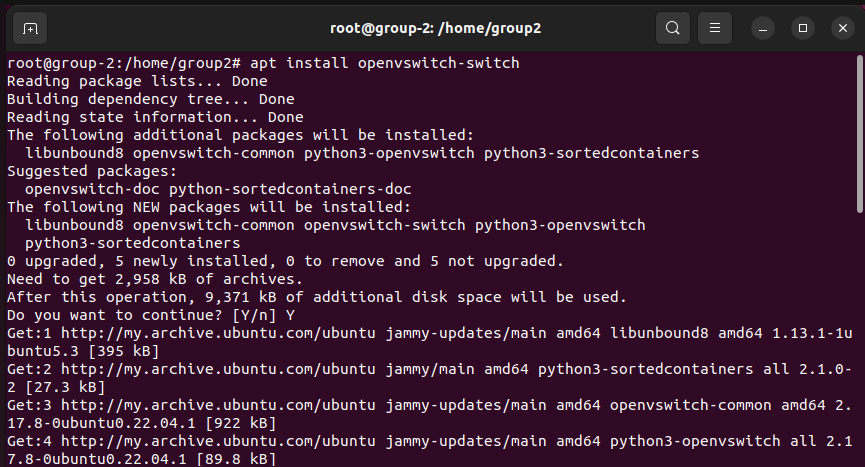


Figure 23

Figure 23 displays two pictures. In the first, the apt command is being used by the root user to install the Open vSwitch software package. This program downloads and installs all required packages and dependencies. In the second screenshot, the user is using “systemctl” to start and enable the “Open vSwitch” service, making sure it launches automatically. To deploy network configuration modifications that connect with the recently installed “Open vSwitch, sudo netplan apply” is finally utilized.

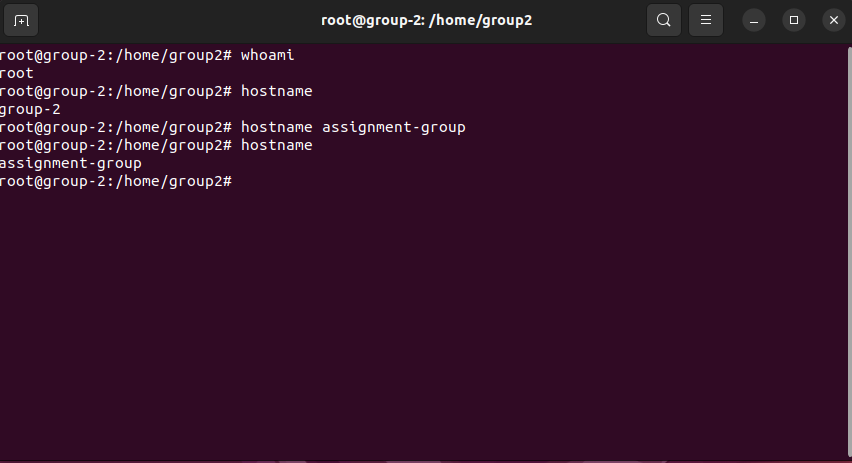


Figure 24

Figure 24 shows the “whoami” command being used to view the current hostname of the machine. The hostname is then changed to “assignment-group” using the “hostname” command as shown in the figure.

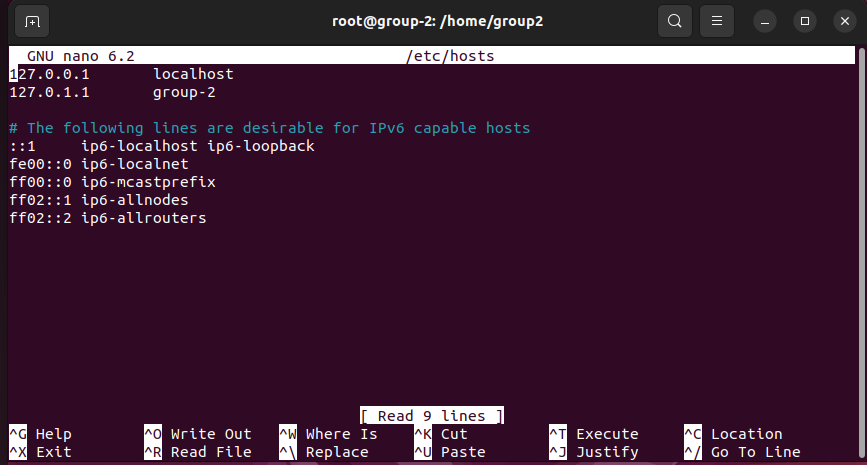
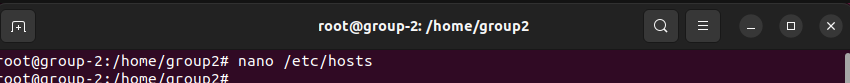


Figure 25

Figure 25 shows the command “nano /etc/hosts” being used to edit the configuration in the   
“/etc/hosts” file. IP addresses and hostnames are mapped in this file. 'group-2' is linked to the loopback IP address '127.0.1.1', as can be seen in the Figure. This is a standard way of giving the local system a name. The file also contains default entries that indicate the local machine and different IPv6 multicast addresses for the localhost and IPv6 addresses.

# 4.0 IP TABLE CONFIGURATION.



Figure 26

We will Display the firewall status by writing the following command.

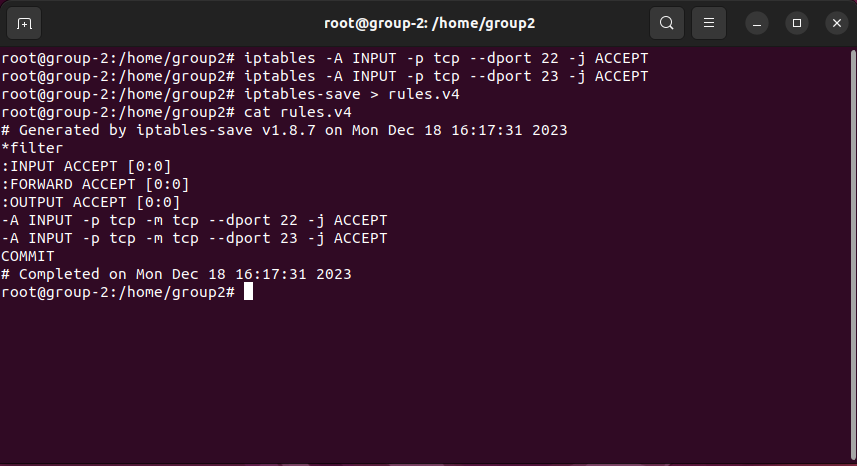


Figure 27

The following figure shows the command that allows incoming TCP traffic on port 22, which is the port that is used for SSH and allows incoming TCP traffic on port 23, which is the port that is used for telnet.These rules would allow anyone to connect to the server using SSH or telnet. In a production environment, it would be more common to only allow SSH connections from specific IP addresses or networks. the iptables rules have been saved to a file called **rules.v4**.

# 5.0 NETWORK FILE SYSTEM (NFS) CONFIGURATION.

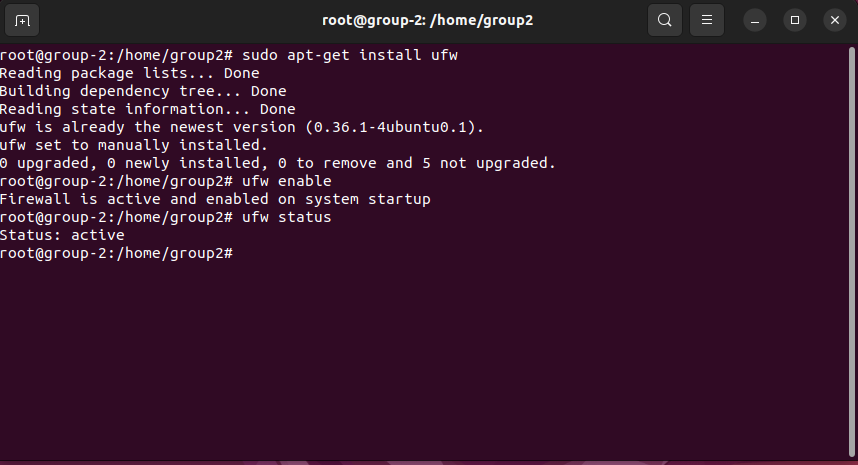


Figure 28

Figure 28 shows the installation, enabling, and checking the status of the UFW (Uncomplicated Firewall). The command used to install the UFW is “sudo apt-get install ufw” which is then followed by the command “ufw enable” which activates the firewall, and “ufw status” confirms that the status of the firewall is “active” indicating that the firewall has been setup and has been activated successfully.

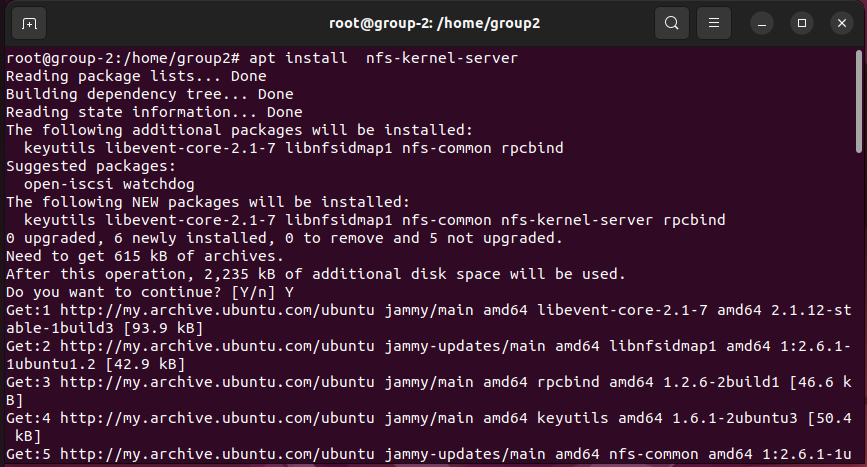


Figure 29

The command “apt install nfs-kernel-server” is shown in the terminal, starting the installation process along with any necessary dependencies. The system starts to download the packages from Ubuntu's repositories when the user gives permission, signifying that the installation process has started successfully.

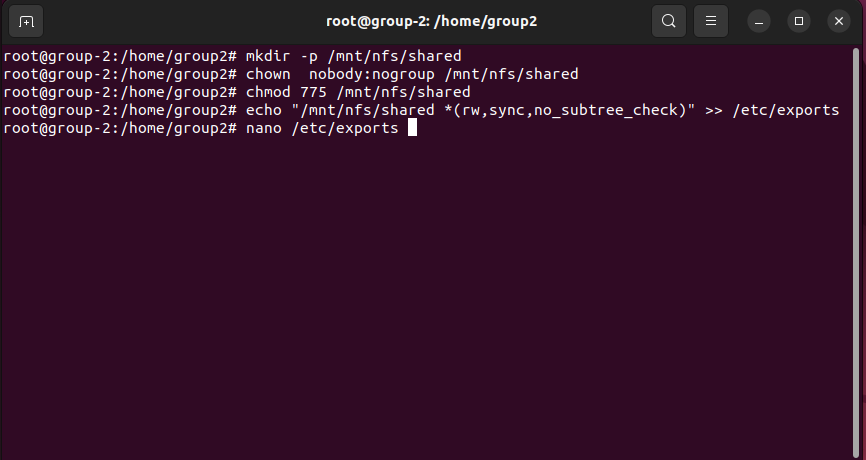


Figure 30

**1. mkdir -p /mnt/nfs/shared:** This command creates a directory called ‘**shared**‘ at the path **/mnt/nfs/shared**.

**2. chown nobody:nogroup /mnt/nfs/shared:** This command changes the ownership of the **/mnt/nfs/shared** directory to the user ‘**nobody’** and the group ‘**nogroup’**. This is a widespread practice for NFS shares, as it helps to ensure that only authorized users can access the files in the share.

**3. chmod 775 /mnt/nfs/shared:** This command sets the permissions on the ‘**/mnt/nfs/shared’** directory to ‘**775’**. This means that the owner of the directory has full read, write, and execute permissions.

**4. echo "/mnt/nfs/shared \*(rw,sync,no\_subtree\_check)" >> /etc/exports:** This command adds a line to the ‘**/etc/exports’** file. The ‘**/etc/exports’** file is used by the NFS server to determine which directories it should export and what permissions should be granted to clients.

**5. nano /etc/exports:** This command opens the **‘/etc/exports’** file in the **‘nano’** text editor.

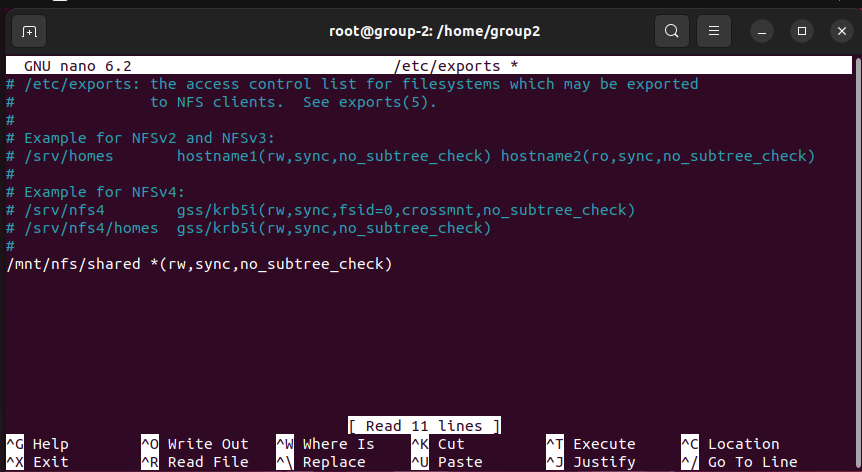


Figure 31

The above figure shows after opening the ‘/etc/exports/’ This file is used to configure the NFS server and define which directories are accessible to clients and what permissions they have. We will add on the last the line the **‘ /mnt/nfs/shared \*(rw, sync, no\_subtree\_check) ‘** file

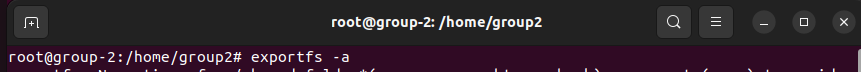


Figure 32

The above figures show that Re-exports all directories listed in the /etc/exports file, making them accessible to authorized clients over the Network File System (NFS).

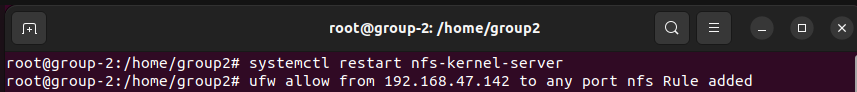


Figure 33

The above figure commands show restarting the NFS kernel server on the **‘system.The’** NFS kernel server is responsible for exporting file systems over the network using the NFS protocol. Restarting the server may be necessary if it has crashed or if you have made changes to the NFS configuration that require a restart. The second command adds a rule to the firewall that allows traffic from the IP address 192.168.47.142 to access the NFS server on any port. This is necessary because by default, the firewall blocks all incoming traffic.

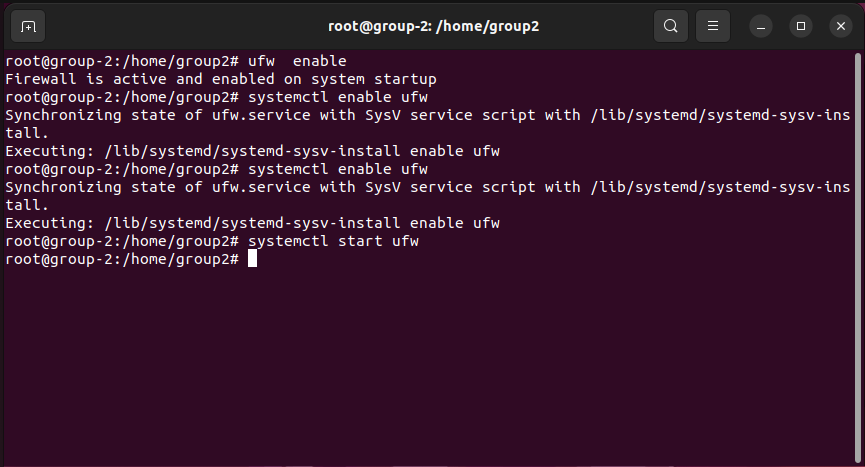


Figure 34

Now we will enable the ufw table. As it shows it is active and enabled on system startup, and then we will restart the ufw.

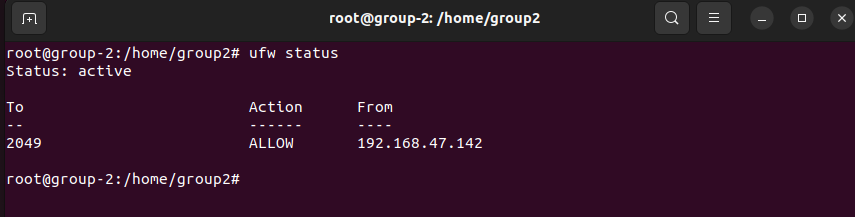


Figure 35

The above figure shows the output of the command in the image shows that the firewall is in a state labeled "active". This means that the firewall is currently running and filtering traffic according to the rules defined in its configuration.

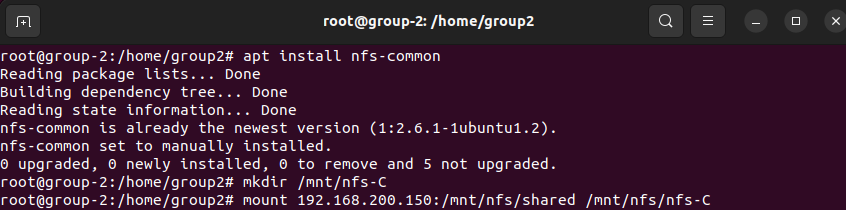


Figure 36

The figure above shows the installation of the nfs-common package, which provides tools and libraries needed for mounting and using NFS shares.

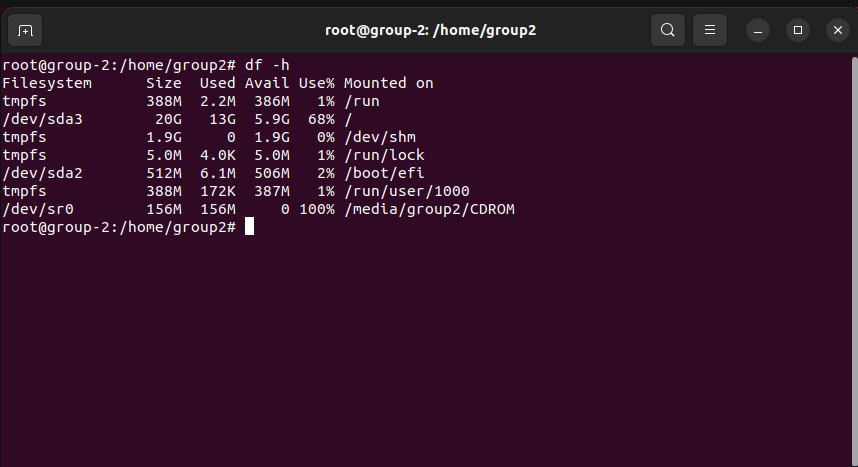


Figure 37

This is the output of the **‘df -h’** command, which is used to display information about disk space usage on a Linux system.

# 6.0 CERTIFICATE AUTHORITY (CA) CONFIGURATION.

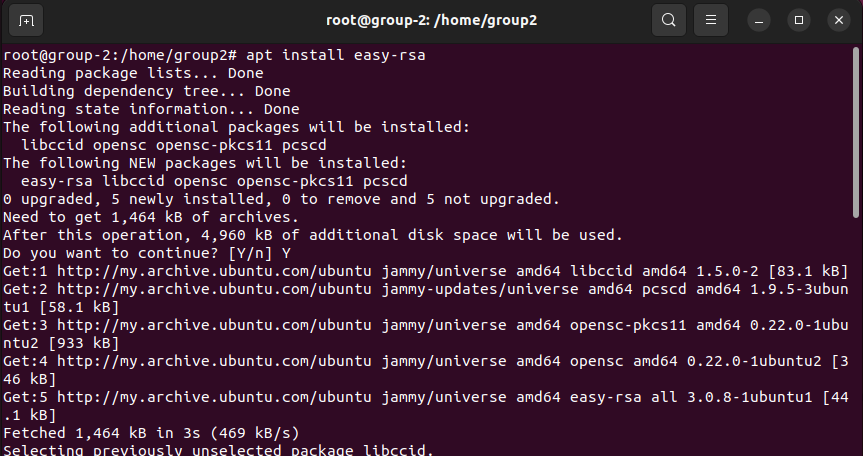


Figure 38

Figure 38 shows the command “apt install easy-rsa”, we are giving the package management instructions to download and install the easy-rsa package, which consists of a collection of scripts for controlling the OpenVPN Public Key Infrastructure (PKI) components. It makes the process of creating certificates for use with OpenVPN and setting up a Certificate Authority (CA) easier.

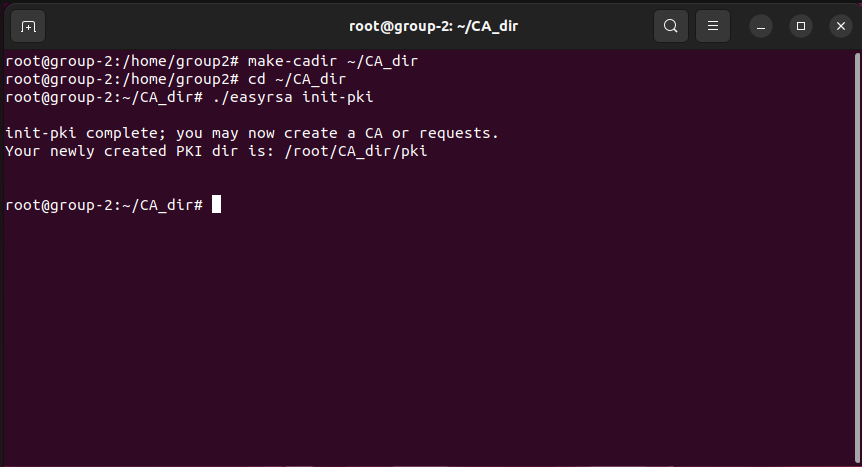


Figure 39

As we can see in figure 39, the first steps of setting up a Certificate Authority (CA) using the easy-rsa tool. The command “make-cadir ~/CA\_dir” creates a new directory called CA\_dir within your home directory. This directory will serve as the foundation for your Certificate Authority (CA) infrastructure. Then change the directory to ~/CA\_dir using the command cd ~/CA\_dir. Finally, create the the CA using the command “./easyrsa init-pki”.

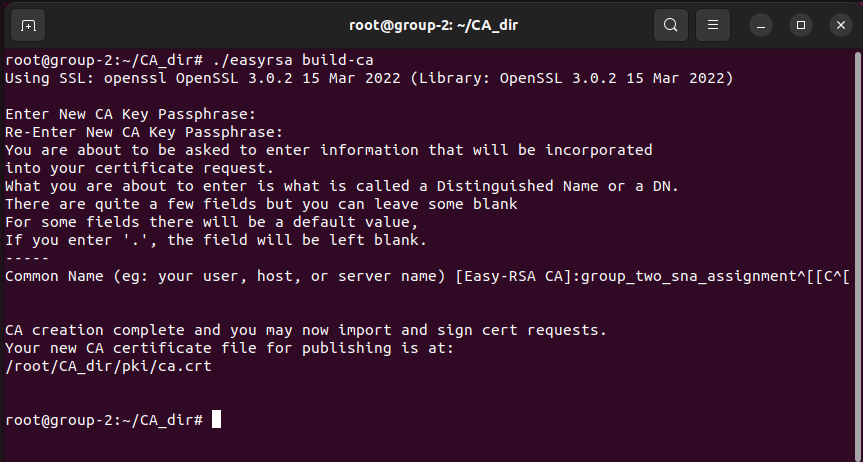


Figure 40

It is shown in the figure above the command “/easyrsa build-ca”. The command executed will result in building the CA. These prompts require us to enter and confirm a strong passphrase that will protect our CA private key. Then we must enter the common name which you have entered as "group\_two\_sna\_assignment". Finally, we can see that the CA creation is completed.

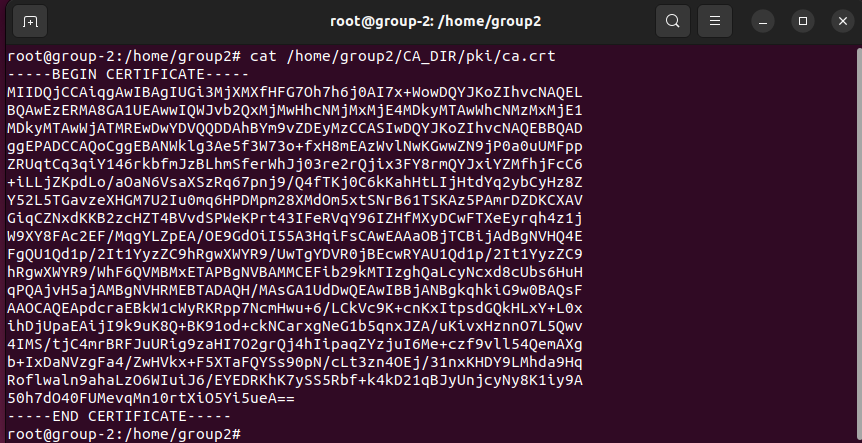


Figure 41

Figure 41 shows the command “cat /home/group2/CA\_DIR/pki/ca.crt”. The purpose of this command is to display the contents of the file ca.crt on the terminal. This file is often a certificate file, and using cat allows us to see the contents of the certificate directly in the terminal.

# CONCLUSION

In conclusion, the report carefully describes the procedures needed to set up and configure a Linux server environment, including everything from system installation and user administration to complex network and security setups. The meticulous preparation and execution of numerous Linux administration activities, such as installing and administering services, setting network parameters, and safeguarding the system with firewalls and Certificate Authority configuration, are demonstrated by every figure in the text. This all-encompassing strategy guarantees the server's functionality performance and security optimization, providing a solid basis for ongoing management and operations.

# REFERENCES

*Get Ubuntu Server | Download | Ubuntu*. (n.d.). Ubuntu. <https://ubuntu.com/download/server>

*VMware Workstation Player*. (2023, November 28). VMware. <https://www.vmware.com/products/workstation-player.html>

Loshin, P. (2022, April 14). *Network File System (NFS)*. Enterprise Desktop. <https://www.techtarget.com/searchenterprisedesktop/definition/Network-File-System>

*UFW - Community Help Wiki*. (n.d.). <https://help.ubuntu.com/community/UFW>

Both, D. (n.d.). *How to configure networking in Linux*. Opensource.com. <https://opensource.com/life/16/6/how-configure-networking-linux>

*Configuring networks | Ubuntu*. (n.d.). Ubuntu. <https://ubuntu.com/server/docs/network-configuration>