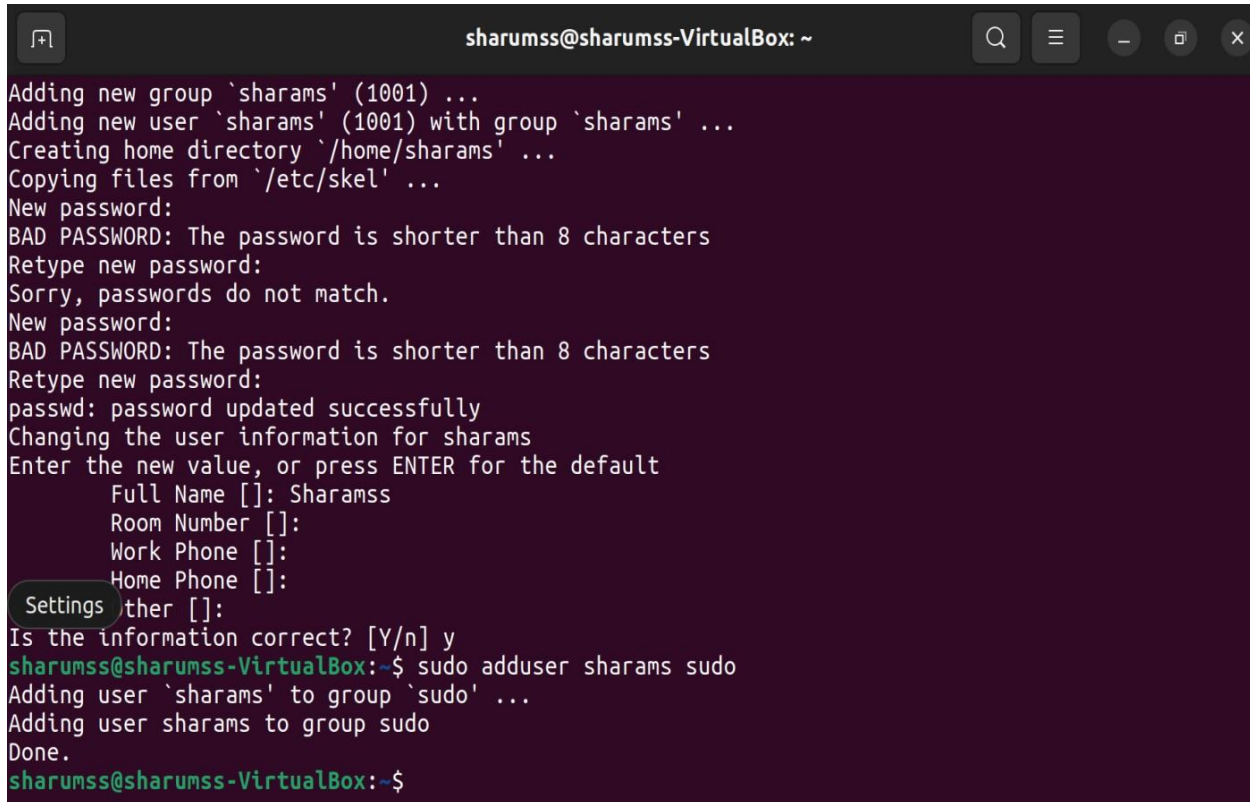


Assignment: 2 – Sharams Kunwar – SSH

Hands: on

A terminal window titled 'sharumss@sharumss-VirtualBox: ~' with standard window controls. The terminal output shows the process of adding a new user 'sharams'. It starts with 'Adding new group `sharams` (1001) ...', followed by 'Adding new user `sharams` (1001) with group `sharams` ...'. It then prompts for a password, which is rejected as being shorter than 8 characters. After two more attempts, the password is successfully updated. The user information is then set, including Full Name, Room Number, Work Phone, Home Phone, and a custom field 'Settings'. The information is confirmed as correct. Finally, the user is added to the 'sudo' group using the 'adduser' command, and the terminal shows the user is now part of the 'sudo' group.

```
sharumss@sharumss-VirtualBox: ~  
Adding new group `sharams' (1001) ...  
Adding new user `sharams' (1001) with group `sharams' ...  
Creating home directory `/home/sharams' ...  
Copying files from `/etc/skel' ...  
New password:  
BAD PASSWORD: The password is shorter than 8 characters  
Retype new password:  
Sorry, passwords do not match.  
New password:  
BAD PASSWORD: The password is shorter than 8 characters  
Retype new password:  
passwd: password updated successfully  
Changing the user information for sharams  
Enter the new value, or press ENTER for the default  
  Full Name []: Sharamss  
  Room Number []:  
  Work Phone []:  
  Home Phone []:  
  Settings ther []:  
Is the information correct? [Y/n] y  
sharumss@sharumss-VirtualBox:~$ sudo adduser sharams sudo  
Adding user `sharams' to group `sudo' ...  
Adding user sharams to group sudo  
Done.  
sharumss@sharumss-VirtualBox:~$
```

Here, a new user 'sharams' was added as an user using command 'adduser'. Upon which I was prompted to set a password and provide additional information.

Later, 'sharams' was also added to the group 'sudo', which grants administrative privileges.

Similarly, adding users can be done with alternate approach as well, i.e., using 'useradd' command:

However, it requires more manual configuration.

```
sharumss@sharumss-VirtualBox: ~  
sharumss@sharumss-VirtualBox:~$ echo "adding user using 'useradd' "  
adding user using 'useradd'  
sharumss@sharumss-VirtualBox:~$ echo "it is a bit of manual approach "  
it is a bit of manual approach  
sharumss@sharumss-VirtualBox:~$ sudo useradd -m -s /bin/bash shrooms  
sharumss@sharumss-VirtualBox:~$ sudo passwd shrooms  
New password:  
BAD PASSWORD: The password is shorter than 8 characters  
Retype new password:  
passwd: password updated successfully  
sharumss@sharumss-VirtualBox:~$
```

In the command, '-m' creates a home directory for the new user and '-s /bin/bash' sets the user's default shell to /bin/bash. The password was set up in the latter command.

```
sharumss@sharumss-VirtualBox:~$ cut -d: -f1 /etc/passwd | xargs -n1 -I{} groups {} | grep sh  
xargs: warning: options --max-args and --replace/-I/-i are mutually exclusive, ignoring previous  
--max-args value  
fwupd-refresh : fwupd-refresh  
sharumss : sharumss adm cdrom sudo dip plugdev lpadmin lxd sambashare  
sharams : sharams sudo  
shrooms : shrooms  
sharumss@sharumss-VirtualBox:~$
```

All the users created were displayed using the command above:

Cut splits the output of passwd each line separated by (:) into the fields and extracts only the first field which contains the username. Then, the groups belonging to the extracted username is displayed.

```
sharumss@sharumss-VirtualBox: ~  
sharumss@sharumss-VirtualBox:~$ su - sharumss  
Password:  
sharumss@sharumss-VirtualBox:~$ su - shrooms  
Password:  
shrooms@sharumss-VirtualBox:~$ su - sharumss  
Password:  
sharumss@sharumss-VirtualBox:~$
```

Similarly, we can switch between users using command su - (username) which has been demonstrated in the screenshot above.

```
sharumss@sharumss-VirtualBox:~$ sudo service ssh status
[sudo] password for sharumss:
Unit ssh.service could not be found.
sharumss@sharumss-VirtualBox:~$ sudo apt install openssh-server
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  ncurses-term openssh-sftp-server ssh-import-id
Suggested packages:
  molly-guard monkeysphere ssh-askpass
The following NEW packages will be installed:
  ncurses-term openssh-server openssh-sftp-server ssh-import-id
0 upgraded, 4 newly installed, 0 to remove and 2 not upgraded.
Need to get 751 kB of archives.
After this operation, 6,046 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://np.archive.ubuntu.com/ubuntu jammy-updates/main amd64 openssh-sftp-server amd64 1:8.9p1-3ubuntu0.4 [38.7 kB]
Get:2 http://np.archive.ubuntu.com/ubuntu jammy-updates/main amd64 openssh-server amd64 1:8.9p1-3ubuntu0.4 [434 kB]
Get:3 http://np.archive.ubuntu.com/ubuntu jammy-updates/main amd64 ncurses-term all 6.3-2ubuntu0.1 [267 kB]
Get:4 http://np.archive.ubuntu.com/ubuntu jammy/main amd64 ssh-import-id all 5.11-0ubuntu1 [10.1 kB]
Fetched 751 kB in 7s (109 kB/s)
Preconfiguring packages ...
Selecting previously unselected package openssh-sftp-server.
```

Then, after verifying that the ssh wasn't installed in the virtual machine, it was installed using "sudo apt install openssh-server".

```
sharumss@sharumss-VirtualBox:~$ sudo service ssh start
sharumss@sharumss-VirtualBox:~$ sudo systemctl enable ssh
Synchronizing state of ssh.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable ssh
sharumss@sharumss-VirtualBox:~$ ssh -V
OpenSSH_8.9p1 Ubuntu-3ubuntu0.4, OpenSSL 3.0.2 15 Mar 2022
sharumss@sharumss-VirtualBox:~$
```

Then, ssh service was started using command "sudo service ssh start". To enable ssh on boot, "sudo systemctl enable ssh" was executed.

```
sharumss@sharumss-VirtualBox:~$ ssh shrooms@192.168.100.5
The authenticity of host '192.168.100.5 (192.168.100.5)' can't be established.
ED25519 key fingerprint is SHA256:YpohYeeU6m7g+AMD0tWsDkUXDrPkAK1x9jBKs4qLGGw.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.100.5' (ED25519) to the list of known hosts.
shrooms@192.168.100.5's password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 6.2.0-33-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

shrooms@shrooms-VirtualBox:~$
```

Then, “ssh shrooms@remote-ip” was executed to ssh into our remote-server “shrooms”.

```
shrooms@shrooms-VirtualBox:~$ mkdir test
shrooms@shrooms-VirtualBox:~$ ls
Desktop  Downloads  Pictures  snap      test
Documents Music      Public   Templates Videos
shrooms@shrooms-VirtualBox:~$
```

Above is the screenshot of /home directory of shrooms, which we could easily access via sharumss.

Below is the screenshot:

```
shrooms@shrooms-VirtualBox:~$ ls
Desktop Documents Downloads Music Pictures Public snap Templates test Videos
shrooms@shrooms-VirtualBox:~$
```

Likewise, scp command was taken in use to securely copy file using ssh. “test.yaml” file was copied from ‘shrooms’ server to ‘sharumss’s Desktop’ via ssh. Below is the screenshot.

```
shroooms@shroooms-VirtualBox:~$ sudo scp test.yaml sharumss@192.168.100.4:Desktop/
sharumss@192.168.100.4's password:
test.yaml                                100% 12      9.9KB/s   00:00
shroooms@shroooms-VirtualBox:~$
```

```
sharumss@sharumss-VirtualBox:~$ ls Desktop
test.yaml
sharumss@sharumss-VirtualBox:~$
```

Key Concepts:

- Difference between curl and wget
 - Curl makes HTTP requests and is not only limited to downloading files but can be used to send data to servers also, unlike wget, which primarily focuses on recursive downloading of files.
 - Curl has a simpler syntax. It takes URL as an argument and retrieves the URL, while wget has more complex options on how to download files.
 - Curl displays output to terminal by default, while wget saves output to local file system by default.
- Difference between rsync and scp
 - Secure Copy or scp copies files between hosts over SSH using SSH protocol for encryption and authentication. It is a simple and secure way to transfer files and directories between systems.
 - Rsync or Remote Sync, on the other hand, is a powerful tool to sync files between two hosts, i.e., local, or remote. It is used for backup, mirroring and syncing. It is also used over ssh for secure transfers.
- Chown and Chmod

Chown is used to change the owner of a file or directory. It allows transfer of ownership from one user to another. It can be used only by superuser/root or the correct owner of the file/directory.

Meanwhile Chmod is used to change permissions of a file or directory. It helps specifying who can read/ write/ execute for everyone including owner/ the group and the others.

- **Command Piping:**
Command Piping in Linux allows one to take output of a code and use it as the input for another command in a single line. Pipes are represented by '|'.

Example:

```
ls -a | grep 's'
```

Now the list displays only the files starting form 's'.

- **Working of DNS**
When entering a URL into a web browser or application, a device needs to resolve the domain name to an IP address to establish a connection with the web server. The device checks its local DNS cache to see if it already knows the IP address for the requested domain. If it does, it can skip the DNS lookup and proceed directly to the website. If the IP address is not found in the local cache, the device sends a DNS query to a recursive DNS server. These servers are typically provided by the internet service provider (ISP) or configured manually in the network settings. The recursive DNS server then queries a root DNS server, redirecting the query to the appropriate top-level domain (TLD) server, and retrieving the DNS record. The device can then finally establish a connection with the web server hosting the requested website.