

Linux Command Line Security Lab

Cybersecurity Fundamentals

School: SUNY New Paltz

Author: Jack Lin

Course: CPS 493-02: Cybersecurity 748 – Fall 2025

Instructor: Kaitlin Hoffman

Assignment: Lab 1

Date: October 2, 2025

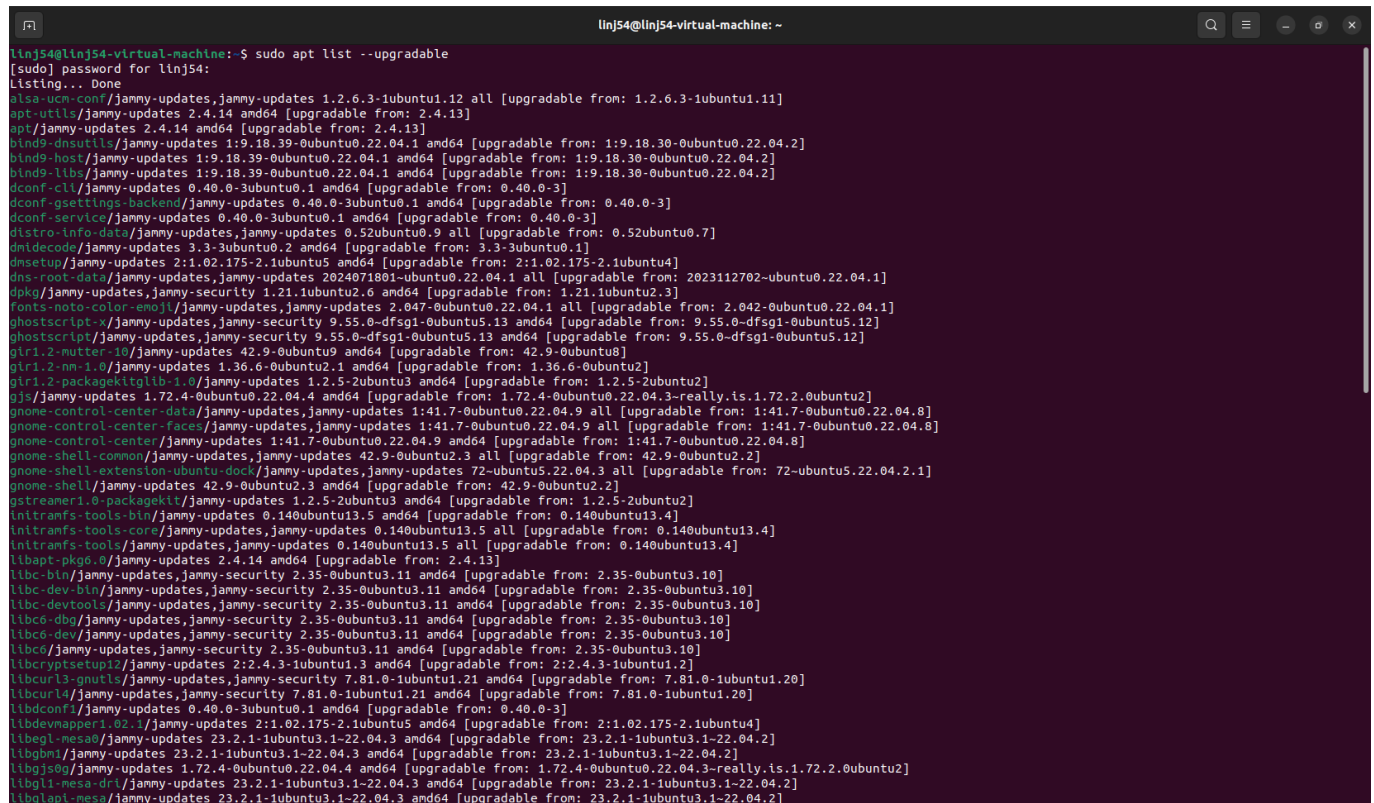
GitHub Repository: [Cybersecurity Labs](#)

System Updates and Maintenance

1. Check Available Updates

When you first ssh and open your virtual machine, you should be told how many updates that can be applied. Enter the command to list the updates available.

```
sudo apt list --upgradable
```

A terminal window titled 'linj54@linj54-virtual-machine: ~' showing the output of the command 'sudo apt list --upgradable'. The output lists various packages that can be upgraded, including 'alsa-ucm-conf', 'apt-utils', 'apt', 'bind9-dnswtills', 'bind9-host', 'bind9-lb', 'dconf-cl', 'dconf-gsettings-backend', 'dconf-service', 'distro-info-data', 'dmidecode', 'dnsmasq', 'dub-root-data', 'dpkg', 'fonts-noto-color-emoj', 'ghostscript', 'gir1.2-mutter-10', 'gir1.2-nm-1.0', 'gir1.2-packagekitlib-1.0', 'gjs', 'gnome-control-center-data', 'gnome-control-center-faces', 'gnome-control-center', 'gnome-shell-common', 'gnome-shell-extension-ubuntu-dock', 'gnome-shell', 'gstreame1.0', 'initramfs-tools-bin', 'initramfs-tools-core', 'initramfs-tools', 'libapt-pkg6.0', 'libc-bin', 'libc-dev-bin', 'libc-devtools', 'libc6-dbg', 'libc6-dev', 'libc6-jammy-security', 'libcryptsetup12', 'libcurl3-gnutls', 'libcurl4', 'libdconf1', 'libdevmapper1.02.1', 'libegl-mesa0', 'libgbm1', 'libgles0', 'libgl1-mesa-dri', and 'libglapi-mesa'. Each entry shows the package name, version, architecture, and the version it can be upgraded to.

```
linj54@linj54-virtual-machine: ~  
[sudo] password for linj54:  
Listing... Done  
alsa-ucm-conf/jammy-updates,jammy-updates 1.2.6.3-1ubuntu1.12 all [upgradable from: 1.2.6.3-1ubuntu1.11]  
apt-utils/jammy-updates 2.4.14 amd64 [upgradable from: 2.4.13]  
apt/jammy-updates 2.4.14 amd64 [upgradable from: 2.4.13]  
bind9-dnswtills/jammy-updates 1:9.18.39-0ubuntu0.22.04.1 amd64 [upgradable from: 1:9.18.39-0ubuntu0.22.04.2]  
bind9-host/jammy-updates 1:9.18.39-0ubuntu0.22.04.1 amd64 [upgradable from: 1:9.18.39-0ubuntu0.22.04.2]  
bind9-lb/jammy-updates 1:9.18.39-0ubuntu0.22.04.1 amd64 [upgradable from: 1:9.18.39-0ubuntu0.22.04.2]  
dconf-cl/jammy-updates 0.40.0-3ubuntu0.1 amd64 [upgradable from: 0.40.0-3]  
dconf-gsettings-backend/jammy-updates 0.40.0-3ubuntu0.1 amd64 [upgradable from: 0.40.0-3]  
dconf-service/jammy-updates 0.40.0-3ubuntu0.1 amd64 [upgradable from: 0.40.0-3]  
distro-info-data/jammy-updates,jammy-updates 0.52ubuntu0.9 all [upgradable from: 0.52ubuntu0.7]  
dmidecode/jammy-updates 3.3-3ubuntu0.2 amd64 [upgradable from: 3.3-3ubuntu0.1]  
dnsmasq/jammy-updates 2:1.02.175-2.1ubuntu5 amd64 [upgradable from: 2:1.02.175-2.1ubuntu4]  
dub-root-data/jammy-updates,jammy-updates 2024071801-ubuntu0.22.04.1 all [upgradable from: 2023112702-ubuntu0.22.04.1]  
dpkg/jammy-updates,jammy-security 1.21.1ubuntu2.6 amd64 [upgradable from: 1.21.1ubuntu2.3]  
fonts-noto-color-emoj/jammy-updates,jammy-updates 2.047-0ubuntu0.22.04.1 all [upgradable from: 2.042-0ubuntu0.22.04.1]  
ghostscript/x/jammy-updates,jammy-security 9.55.0-dfsg1-0ubuntu5.13 amd64 [upgradable from: 9.55.0-dfsg1-0ubuntu5.12]  
ghostscript/jammy-updates,jammy-security 9.55.0-dfsg1-0ubuntu5.13 amd64 [upgradable from: 9.55.0-dfsg1-0ubuntu5.12]  
gir1.2-mutter-10/jammy-updates 42.9-0ubuntu9 amd64 [upgradable from: 42.9-0ubuntu8]  
gir1.2-nm-1.0/jammy-updates 1.36.6-0ubuntu2.1 amd64 [upgradable from: 1.36.6-0ubuntu2]  
gir1.2-packagekitlib-1.0/jammy-updates 1.2.5-2ubuntu3 amd64 [upgradable from: 1.2.5-2ubuntu2]  
gjs/jammy-updates 1.72.4-0ubuntu0.22.04.4 amd64 [upgradable from: 1.72.4-0ubuntu0.22.04.3-really.is.1.72.2.0ubuntu2]  
gnome-control-center-data/jammy-updates,jammy-updates 1:41.7-0ubuntu0.22.04.9 all [upgradable from: 1:41.7-0ubuntu0.22.04.8]  
gnome-control-center-faces/jammy-updates,jammy-updates 1:41.7-0ubuntu0.22.04.9 all [upgradable from: 1:41.7-0ubuntu0.22.04.8]  
gnome-control-center/jammy-updates 1:41.7-0ubuntu0.22.04.9 amd64 [upgradable from: 1:41.7-0ubuntu0.22.04.8]  
gnome-shell-common/jammy-updates,jammy-updates 42.9-0ubuntu2.3 all [upgradable from: 42.9-0ubuntu2.2]  
gnome-shell-extension-ubuntu-dock/jammy-updates,jammy-updates 72-ubuntu5.22.04.2.1 all [upgradable from: 72-ubuntu5.22.04.2.1]  
gnome-shell/jammy-updates 42.9-0ubuntu2.3 amd64 [upgradable from: 42.9-0ubuntu2.2]  
gstreame1.0/packagekit/jammy-updates 1.2.5-2ubuntu3 amd64 [upgradable from: 1.2.5-2ubuntu2]  
initramfs-tools-bin/jammy-updates 0.140ubuntu13.5 amd64 [upgradable from: 0.140ubuntu13.4]  
initramfs-tools-core/jammy-updates,jammy-updates 0.140ubuntu13.5 all [upgradable from: 0.140ubuntu13.4]  
initramfs-tools/jammy-updates,jammy-updates 0.140ubuntu13.5 all [upgradable from: 0.140ubuntu13.4]  
libapt-pkg6.0/jammy-updates 2.4.14 amd64 [upgradable from: 2.4.13]  
libc-bin/jammy-updates,jammy-security 2.35-0ubuntu3.11 amd64 [upgradable from: 2.35-0ubuntu3.10]  
libc-dev-bin/jammy-updates,jammy-security 2.35-0ubuntu3.11 amd64 [upgradable from: 2.35-0ubuntu3.10]  
libc-devtools/jammy-updates,jammy-security 2.35-0ubuntu3.11 amd64 [upgradable from: 2.35-0ubuntu3.10]  
libc6-dbg/jammy-updates,jammy-security 2.35-0ubuntu3.11 amd64 [upgradable from: 2.35-0ubuntu3.10]  
libc6-dev/jammy-updates,jammy-security 2.35-0ubuntu3.11 amd64 [upgradable from: 2.35-0ubuntu3.10]  
libc6/jammy-updates,jammy-security 2.35-0ubuntu3.11 amd64 [upgradable from: 2.35-0ubuntu3.10]  
libcryptsetup12/jammy-updates 2:2.4.3-1ubuntu1.3 amd64 [upgradable from: 2:2.4.3-1ubuntu1.2]  
libcurl3-gnutls/jammy-updates,jammy-security 7.81.0-1ubuntu1.21 amd64 [upgradable from: 7.81.0-1ubuntu1.20]  
libcurl4/jammy-updates,jammy-security 7.81.0-1ubuntu1.21 amd64 [upgradable from: 7.81.0-1ubuntu1.20]  
libdconf1/jammy-updates 0.40.0-3ubuntu0.1 amd64 [upgradable from: 0.40.0-3]  
libdevmapper1.02.1/jammy-updates 2:1.02.175-2.1ubuntu5 amd64 [upgradable from: 2:1.02.175-2.1ubuntu4]  
libegl-mesa0/jammy-updates 23.2.1-1ubuntu3.1-22.04.3 amd64 [upgradable from: 23.2.1-1ubuntu3.1-22.04.2]  
libgbm1/jammy-updates 23.2.1-1ubuntu3.1-22.04.3 amd64 [upgradable from: 23.2.1-1ubuntu3.1-22.04.2]  
libgles0/jammy-updates 1.72.4-0ubuntu0.22.04.4 amd64 [upgradable from: 1.72.4-0ubuntu0.22.04.3-really.is.1.72.2.0ubuntu2]  
libgl1-mesa-dri/jammy-updates 23.2.1-1ubuntu3.1-22.04.3 amd64 [upgradable from: 23.2.1-1ubuntu3.1-22.04.2]  
libglapi-mesa/jammy-updates 23.2.1-1ubuntu3.1-22.04.3 amd64 [upgradable from: 23.2.1-1ubuntu3.1-22.04.2]
```

2. Update and Upgrade System

Update and Upgrade your system.

```
sudo apt update  
sudo apt upgrade -y
```

```
linj54@linj54-virtual-machine:~$ sudo apt update
Hit:1 http://us.archive.ubuntu.com/ubuntu jammy InRelease
Get:2 http://us.archive.ubuntu.com/ubuntu jammy-updates InRelease [128 kB]
Get:3 http://us.archive.ubuntu.com/ubuntu jammy-backports InRelease [127 kB]
Get:4 http://security.ubuntu.com/ubuntu jammy-security InRelease [129 kB]
Get:5 http://us.archive.ubuntu.com/ubuntu jammy-updates/main amd64 Packages [2,973 kB]
Get:6 http://us.archive.ubuntu.com/ubuntu jammy-updates/main i386 Packages [890 kB]
Get:7 http://us.archive.ubuntu.com/ubuntu jammy-updates/main Translation-en [463 kB]
Get:8 http://us.archive.ubuntu.com/ubuntu jammy-updates/main amd64 DEP-11 Metadata [112 kB]
Get:9 http://us.archive.ubuntu.com/ubuntu jammy-updates/main amd64 c-n-f Metadata [19.0 kB]
Get:10 http://us.archive.ubuntu.com/ubuntu jammy-updates/restricted amd64 Packages [4,637 kB]
Get:11 http://us.archive.ubuntu.com/ubuntu jammy-updates/restricted Translation-en [858 kB]
Get:12 http://security.ubuntu.com/ubuntu jammy-security/main i386 Packages [705 kB]
Get:13 http://us.archive.ubuntu.com/ubuntu jammy-updates/restricted amd64 DEP-11 Metadata [212 B]
Get:14 http://us.archive.ubuntu.com/ubuntu jammy-updates/universe i386 Packages [784 kB]
Get:15 http://us.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 Packages [1,230 kB]
Get:16 http://us.archive.ubuntu.com/ubuntu jammy-updates/universe Translation-en [306 kB]
Get:17 http://us.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 DEP-11 Metadata [359 kB]
Get:18 http://us.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 c-n-f Metadata [29.6 kB]
Get:19 http://us.archive.ubuntu.com/ubuntu jammy-updates/multiverse amd64 DEP-11 Metadata [940 B]
Get:20 http://us.archive.ubuntu.com/ubuntu jammy-backports/main amd64 DEP-11 Metadata [7,080 B]
Get:21 http://us.archive.ubuntu.com/ubuntu jammy-backports/restricted amd64 DEP-11 Metadata [212 B]
Get:22 http://us.archive.ubuntu.com/ubuntu jammy-backports/universe amd64 DEP-11 Metadata [9,724 B]
Get:23 http://us.archive.ubuntu.com/ubuntu jammy-backports/multiverse amd64 DEP-11 Metadata [212 B]
Get:24 http://security.ubuntu.com/ubuntu jammy-security/main amd64 Packages [2,689 kB]
Get:25 http://security.ubuntu.com/ubuntu jammy-security/main amd64 DEP-11 Metadata [54.5 kB]
Get:26 http://security.ubuntu.com/ubuntu jammy-security/main amd64 c-n-f Metadata [13.9 kB]
Get:27 http://security.ubuntu.com/ubuntu jammy-security/restricted amd64 DEP-11 Metadata [208 B]
Get:28 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 Packages [997 kB]
Get:29 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 DEP-11 Metadata [125 kB]
Get:30 http://security.ubuntu.com/ubuntu jammy-security/multiverse amd64 DEP-11 Metadata [208 B]
Fetched 17.6 MB in 5s (3,643 kB/s)
```

3. System Reboot

Reboot your system. (You may have to wait a few minutes to ssh again).

```
sudo reboot
```

User Tasks

4. Switch to Root User

Change the current user to root using the command `sudo su root`. What does the prompt look like?

```
sudo su root
```

Answer: Usually it changes from `ubuntu@machine:~$` to something like `root@machine:/home/ubuntu#`

5. User Creation Commands

Create a new user with the name bobby using the command `useradd`. Next, create another user with the name sally using the command `adduser`. What is the difference between the two?

```
sudo useradd bobby
sudo adduser sally
```

Answer:

- `useradd` creates a low-level account with nothing else
- `adduser` creates a high-level account with homedir, environment, and password setup necessary

```
root@linj54-virtual-machine:/home/linj54# sudo useradd bobby
useradd: user 'bobby' already exists
root@linj54-virtual-machine:/home/linj54# sudo adduser sally
adduser: The user `sally' already exists.
root@linj54-virtual-machine:/home/linj54#
```

6. Switch to Sally User

Change the current user to sally. What does the prompt look like now?

```
su - sally
```

Answer: Changes the prompt to look like: `sally@lin52-virtual-machine:~$`

7. Permission Testing

While you're logged in as sally still, try to create a new user with the name earl. What happens? Why?

Answer: "sally is not in the sudoers file. This incident will be reported" appears due to the fact that sally does not have adequate permission since only root/sudo users can do that.

8. User Deletion

Enter exit until you are the original user, ubuntu, again. Delete the user earl. I didn't show you the command, but Google it! "Googling" skills are a great skill in CS; It's impossible to know everything.

```
sudo userdel bobby
```

Note: The user earl doesn't actually exist, but I deleted bobby instead.

```
linj54@linj54-virtual-machine:~$ sudo deluser bobby
Removing user `bobby' ...
Warning: group `bobby' has no more members.
Done.
linj54@linj54-virtual-machine:~$
```

9. Password Management

Change the password of sally to something you can remember using `sudo passwd sally`.

```
sudo passwd sally
```

```
Done!  
linj54@linj54-virtual-machine:~$ sudo passwd sally  
New password:  
BAD PASSWORD: The password is shorter than 8 characters  
Retype new password:  
passwd: password updated successfully
```

10. Root User Security

For the rest of the tasks, use the ubuntu user. Even though it's easier to complete tasks/commands, why is it bad practice to stay logged in as root?

Answer: Staying as root is dangerous because any mistakes like `rm -rf /` could break the whole system, so it's better practice to work as a normal user and only use higher privilege when necessary.

11. User ID Check

Enter the command to see what your user id is.

```
id
```

```
linj54@linj54-virtual-machine:~$ id -u  
1000
```

Group Tasks

12. Group Membership

What groups does ubuntu belong to?

Groups and their purposes:

- `adm` = logs
- `cdrom` = disc access
- `sudo` = admin rights
- `dip` = network dial-up
- `plugdev` = USB devices
- `lpadmin` = printers
- `lxd` = containers
- `smbshare` = network file sharing

13. Sudo Access for Sally

Give sally the ability to execute sudo commands. Next, try to create a new user while logged in as sally.

```
sudo usermod -aG sudo sally
```

```
linj54@linj54-virtual-machine:~$ sudo usermod -aG sudo sally
linj54@linj54-virtual-machine:~$ su - sally
Password:
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

sally@linj54-virtual-machine:~$ sudo adduser testuser
[sudo] password for sally:
Adding user `testuser' ...
Adding new group `testuser' (1001) ...
Adding new user `testuser' (1001) with group `testuser' ...
Creating home directory `/home/testuser' ...
Copying files from `/etc/skel' ...
New password:
BAD PASSWORD: No password supplied
Retype new password:
Sorry, passwords do not match.
New password:
BAD PASSWORD: The password contains the user name in some form
Retype new password:
passwd: password updated successfully
Changing the user information for testuser
Enter the new value, or press ENTER for the default
    Full Name []:
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Is the information correct? [Y/n]
```

14-16. Group Management

- Create a new group called cybersec
- Add sally to the group, cybersec
- Check to see which groups sally belongs

```
sudo groupadd cybersec
sudo usermod -aG cybersec sally
groups sally
```

```
linj54@linj54-virtual-machine:~$ sudo usermod -aG sudo sally
linj54@linj54-virtual-machine:~$ su - sally
Password:
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

sally@linj54-virtual-machine:~$ sudo adduser testuser
[sudo] password for sally:
Adding user `testuser' ...
Adding new group `testuser' (1001) ...
Adding new user `testuser' (1001) with group `testuser' ...
Creating home directory `/home/testuser' ...
Copying files from `/etc/skel' ...
New password:
BAD PASSWORD: No password supplied
Retype new password:
Sorry, passwords do not match.
New password:
BAD PASSWORD: The password contains the user name in some form
Retype new password:
passwd: password updated successfully
Changing the user information for testuser
Enter the new value, or press ENTER for the default
    Full Name []:
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Is the information correct? [Y/n]
```

Permission and Access Control Lists

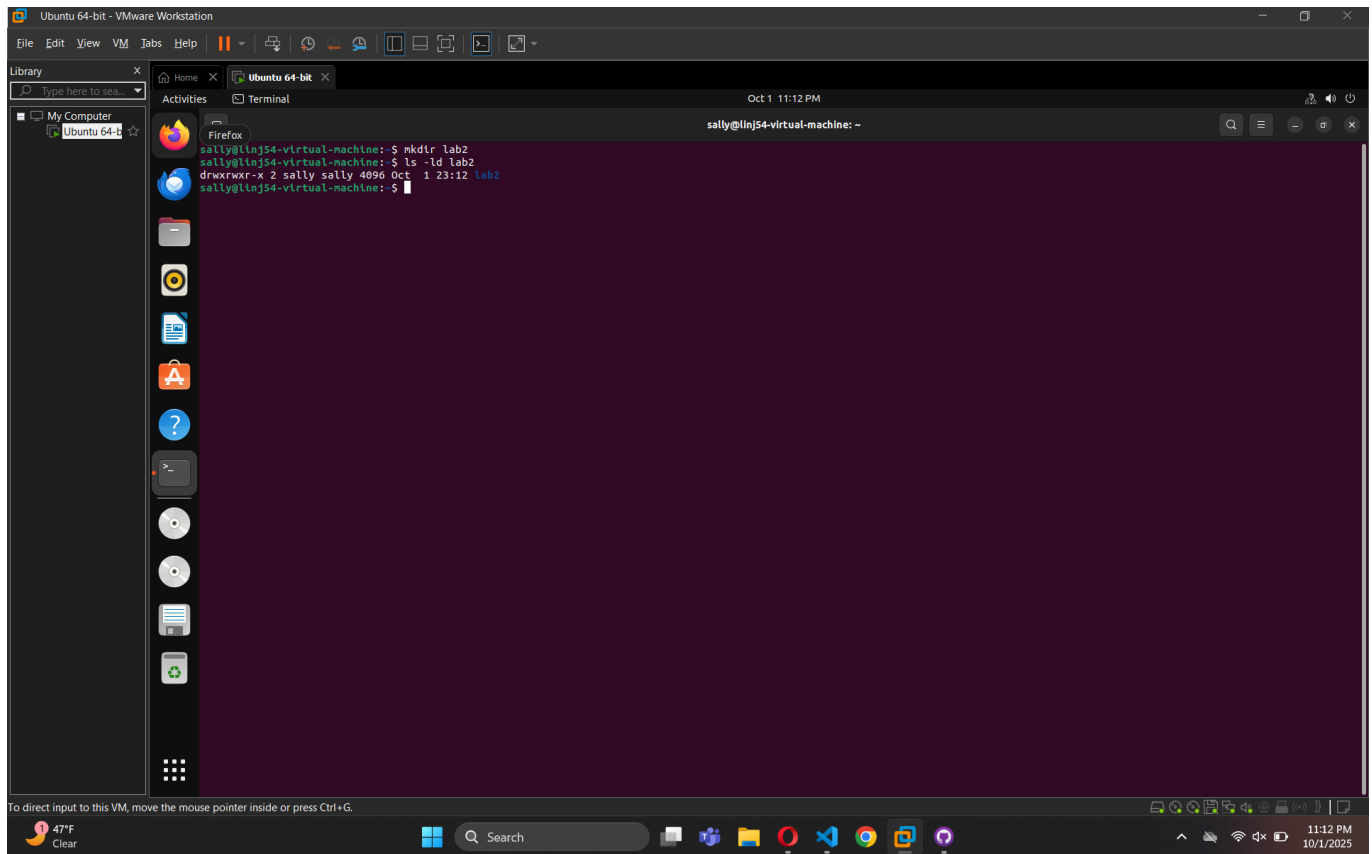
17. Directory Permissions

Create a new directory called lab1. Enter the command to find the permissions of the directory. Who is the owner and group owner of this directory? What permissions does the owner, group and other have?

```
mkdir lab1
ls -ld lab1
```

Answer:

- Owner has read, write, and execute permission
- Group has read, write, and execute permission
- Other has read and execute permission



18. Bash Script Creation

Change your directory to lab1. Create a new bash file called, helloWorld. When ran, your program should just print "Hello World!". (Don't forget to make your bash file executable).

```
cd lab1
nano helloWorld
chmod +x helloWorld
```

helloWorld script content:

```
#!/bin/bash
echo "Hello World!"
```

```
GNU nano 6.2
#!/bin/bash
echo "Hello World!"
```

Execution:

```
./helloWorld
```



```
GNU nano 6.2
#!/bin/bash
echo "Hello World!"
```

19. File Permissions Analysis

Enter the command `ls -la helloWorld`. What are the reading, writing, and executing permissions for the owner, group and other?

a. Change the permissions so the group also has w and x permissions.

```
ls -la helloWorld
```

Answer:

- Owner has read, write, and execute permission
- Group has read, write, and execute permission
- Other has read and execute permission

Note: Group already had w/x permissions

20. Access Control Lists (ACL)

Use the `getfacl` command to view the ACL of the file.

```
getfacl helloWorld
```

```
sally@linj54-virtual-machine:~/lab1$ getfacl helloWorld
# file: helloWorld
# owner: sally
# group: sally
user::rwx
group::rwx
other::r-x
```

21. ACL Modification

Using the `setfacl` command, allow the user, sally, the ability to read and write to the file.

```
sudo setfacl -m u:sally:rw helloWorld
```

```
sally@linj54-virtual-machine:~/lab1$ getfacl helloWorld
# file: helloWorld
# owner: sally
# group: sally
user::rwx
user:sally:rw-
group::rwx
mask::rwx
other::r-x
```

Using the setfacl command,

allow the user, sally, the ability to read and write to the file.

```
sudo setfacl -m u:sally:rw helloWorld
```

```
sally@linj54-virtual-machine:~/lab1$ getfacl helloWorld
# file: helloWorld
# owner: sally
# group: sally
user::rwx
user:sally:rw-
group::rwx
mask::rwx
other::r-x
```