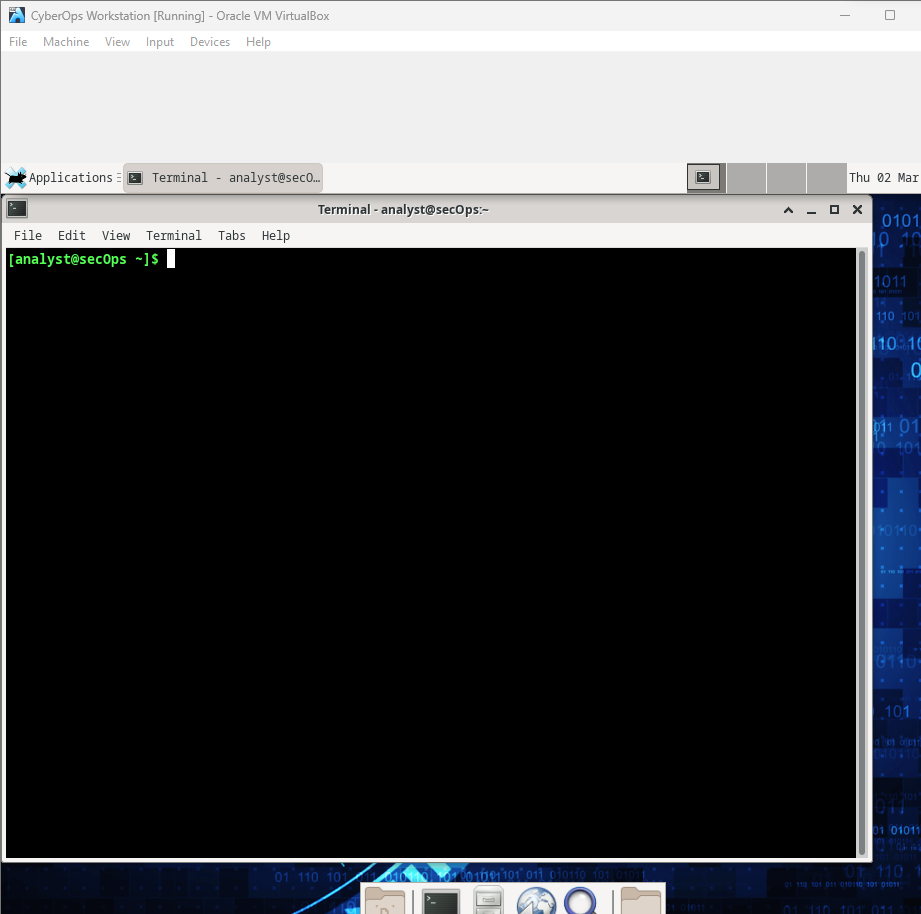
**Name: Joseph Dela Cruz Jr.**

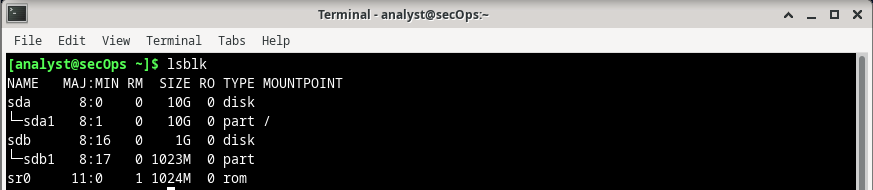
**Course: 4th year BSIT**

**Part 1**

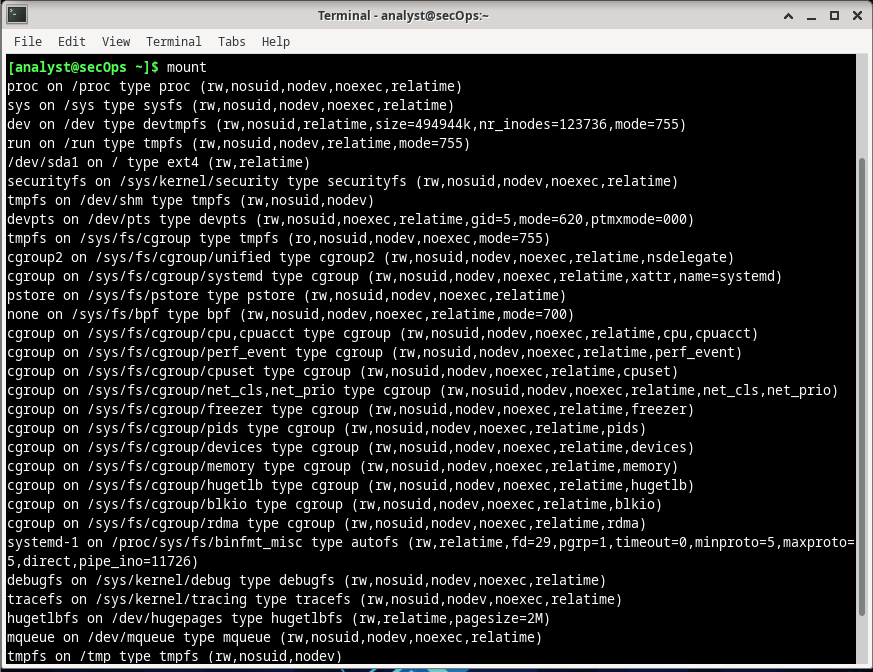
**Step 1 Open Command line**



**Step 2 – a**

****

**Step 2 – b**

****

**Step 2 – c**

****

**Step 2 – d**

**Text

Description automatically generated**

What is the meaning of the output? Where are the listed files physically stored?

The first command changes the directory to the root directory. The root directory is the highest level of the filesystems. Because /dev/sda1 is mounted on the root directory (“/”), by listing the files in the root directory, the user is actually listing files physically stored in the root of the /dev/sda1 filesystem.

Why is /dev/sdb1 not shown in the output above?

Because /dev/sdb1 is not currently mounted.

**Step 3 – a**

**Text

Description automatically generated**

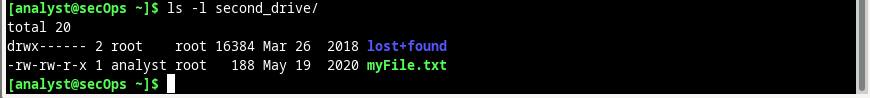
**Step 3 – b**



**Step 3 – c**

****

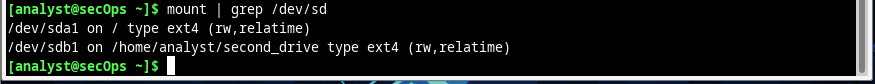
**Step 3 – d**

****

Why is the directory no longer empty? Where are the listed files physically stored?

After the mount, /home/analyst/second\_drive becomes the entry point to the filesystem physically stored in /dev/sdb1.

**Step 3 – e**

****

**Step 3 – f**

**A picture containing text

Description automatically generated**

**Part 2**

**Step 1 – a**



**Step 1 – b**

**Graphical user interface, text, application, chat or text message

Description automatically generated**

Consider the cyops.mn file as an example. Who is the owner of the file? How about the group?

Owner: analyst; Group: analyst

The permissions for cyops.mn are –rw-r--r--. What does that mean?

The analyst user who owns the file can read and write to it but cannot execute it (-rw). Other than the owner, members of the analyst group are only permitted to read files (-r-); no executing or writing is permitted. No other users are permitted to modify or run that file.

**Step 1 – c**

****

Why was the file not created? List the permissions, ownership and content of the /mnt directory and explain what happened. With the addition of -d option, it lists the permission of the parent directory. Record the answer in the lines below.

The root user owns the /mnt directory and has the rights drwxr-xr-x. In this manner, the /mnt folder can only be written to by the root user.



What can be done for the touch command shown above to be successful?

The /mnt directory's permissions can be changed, or the command can be run as root by appending sudo before it.

**Step 1 – d**



**Step 1 – e**

Graphical user interface

Description automatically generated with medium confidence

What are the permissions of the myFile.txt file?

The permission is -rw-r–r–.

**Step 1 – f**

**Text

Description automatically generated**

Did the permissions change? What are the permissions of myFile.txt?

Yes, it becomes -rw-rw-r-x.

What command would change the permissions of myFile.txt to rwxrwxrwx, granting any user in the system full access to the file?

The command will be sudo chmod 777 myFile.txt.

**Step 1 – g**

**Text

Description automatically generated**

**Step 1 – h**

**Text

Description automatically generated**

Was the operation successful? Explain.

Yes. The owner of the file is analyst, and the previous permissions of 665 are still in place. The owner and users belonging to the root group are able to edit the file due to the current permissions.

**Step 2 – a**

Graphical user interface, text

Description automatically generated

Compare the permissions of the malware directory with the mininet\_services file. What is the difference between beginning part of the malware line and the mininet\_services line?

There is a letter d at the beginning before the permissions for the malware directory.

**Part 3**

**Step 1 – a**

**A screenshot of a computer

Description automatically generated with medium confidence**

**Step 1 – b**

Text

Description automatically generated

**Step 1 – c**

A picture containing text

Description automatically generated

**Step 1 – d**

****

**Step 1 – e**

Text

Description automatically generated with low confidence

**Step 1 – f**

**A screenshot of a computer

Description automatically generated with medium confidence**

What do you think would happen to file2hard if you opened a text editor and changed the text in file2new.txt?

Because they both point to the same inode on the hard disk drive, changing the contents of one file would also modify the contents of the other.

**Reflection**

File permissions and ownership are two of the most important aspects of Linux. They are also a common cause of problems. A file that has the wrong permissions or ownership set will not be available to the programs that need to access it. In this scenario, the program will usually break, and errors will be encountered.