Lab 7 Instructions for Virginia Cyber Range (Without VirtualBox)

Note: login as root when doing the assignment to avoid issues.

Command: Sudo su

This assignment is specifically for those using the Virginia Cyber Range or macOS to complete Lab 7. If you are using VirtualBox, please refer to the slides and follow the steps demonstrated there.

Part I: Check Your File System (20 Points)

Submit screenshots for each command output in this part.

Step 1: Check Hard Disk Devices

Run the following commands to list the current hard disk devices. Use whichever command matches the naming convention in your environment (either /dev/sd* or /dev/nvme*).

sudo ls /dev/sd* # For devices with /dev/sd* naming

sudo ls /dev/nvme* # For devices with /dev/nvme* naming

Step 2: List Current Hard Disk Partitions

Use the fdisk command to display a detailed list of your current partitions.

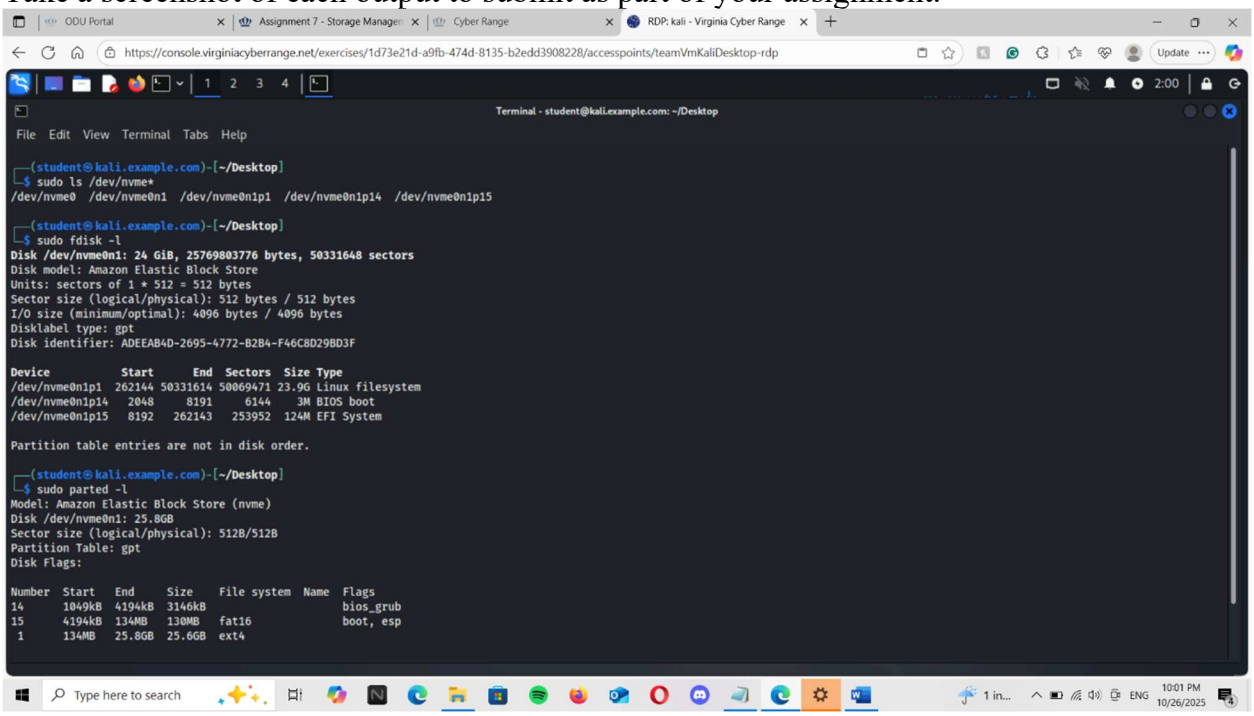
sudo fdisk -l

Step 3: List Partition Table

Use the parted command to see the partition table.

sudo parted -l

Take a screenshot of each output to submit as part of your assignment.



Part II: Create a New Virtual Disk (20 Points)

Submit screenshots for each step in this part.

Step 1: Create a Virtual Disk File

Run this command to create a 200 MB virtual disk file. Replace YourMIDAS with your MIDAS ID.

sudo dd if=/dev/zero of=~/YourMIDAS.vdi bs=1M count=200

Step 2: Attach the Virtual Disk as a Loop Device

Use the losetup command to attach this file as a loop device. This will make it appear as a new disk.

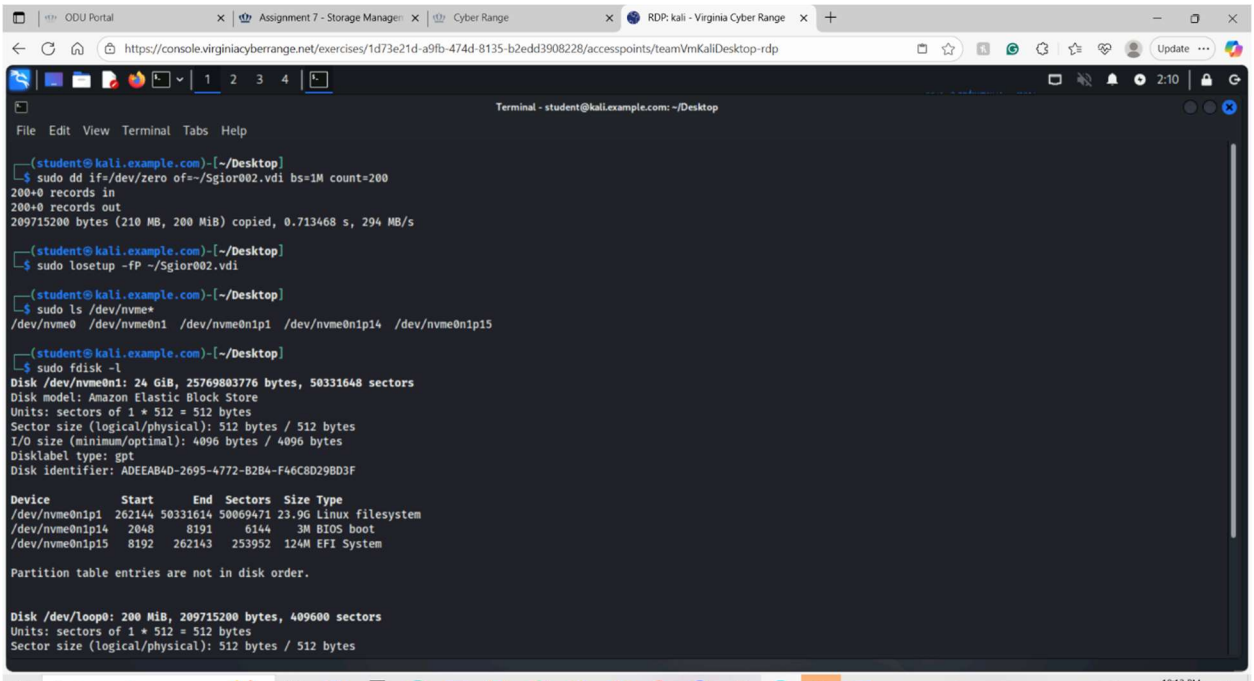
sudo losetup -fP ~/YourMIDAS.vdi

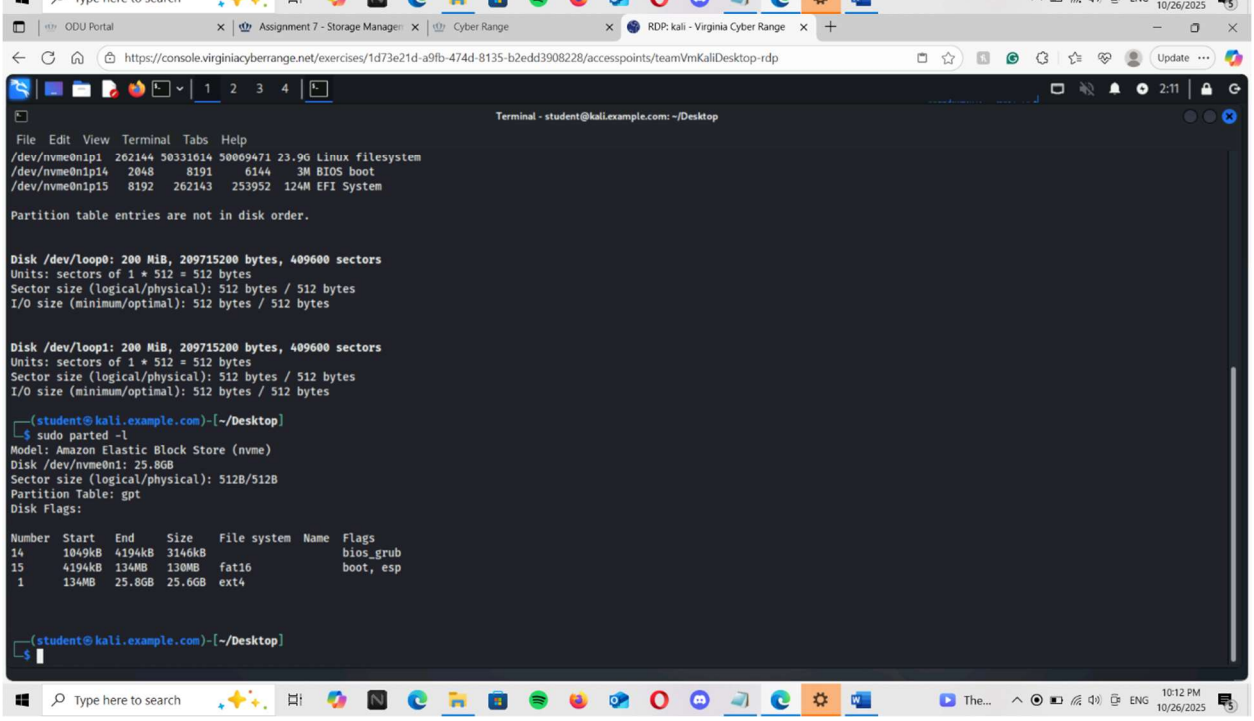
Step 3: Repeat Part I Commands and Highlight Differences

Run the same commands from Part I to confirm that the new loop device (e.g., /dev/loop0) has been added:

- sudo ls /dev/sd* or sudo ls /dev/nvme* (depending on the naming convention)
- sudo fdisk -l
- sudo parted -l

Take screenshots of these outputs, highlighting the new virtual disk file (/dev/loop0 or similar).





Part III: Creating Filesystems and Mounting the Virtual Disk (30 Points)

Submit screenshots for each of the following steps.

Step 1: Format the Loop Device Directly

Since we are not creating a separate partition, format the entire loop device (/dev/loop0) with the ext4 filesystem.

sudo mkfs.ext4 /dev/loop0 (the name of the disk can be different, make sure of that)

Step 2: Mount the Loop Device

Create a directory named /cyse and mount the loop device (/dev/loop0) to this directory.

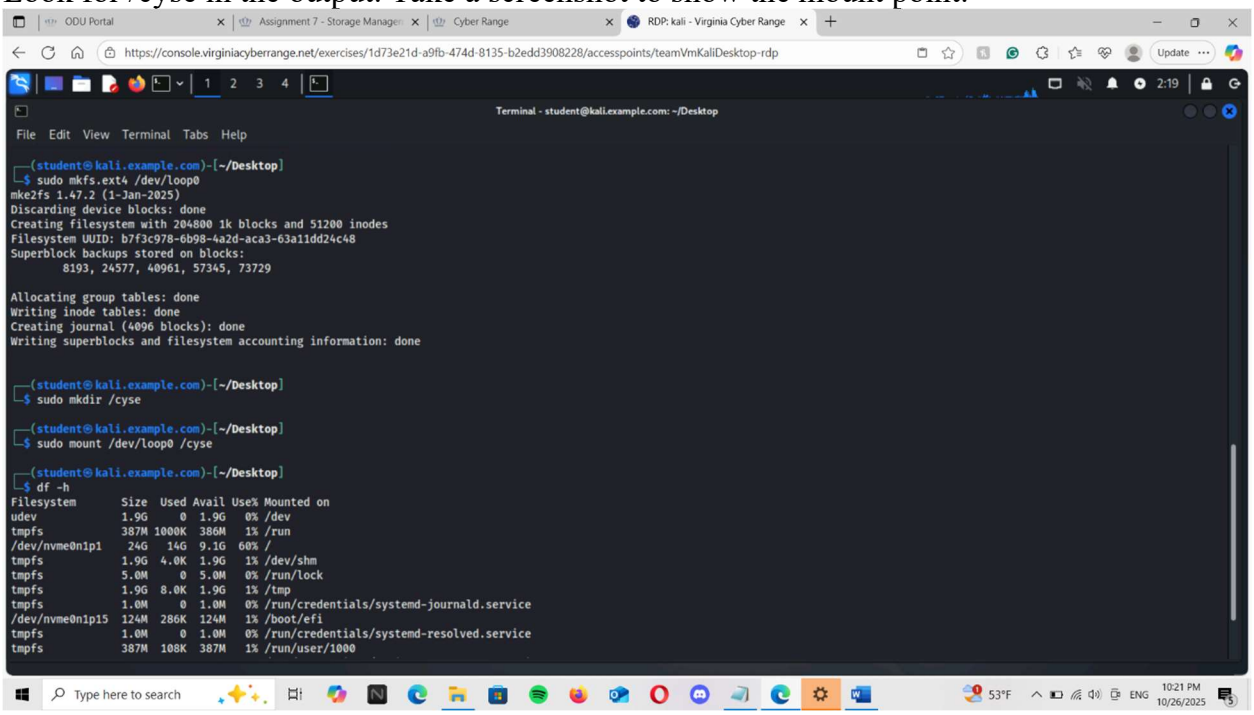
```
sudo mkdir /cyse
sudo mount /dev/loop0 /cyse
```

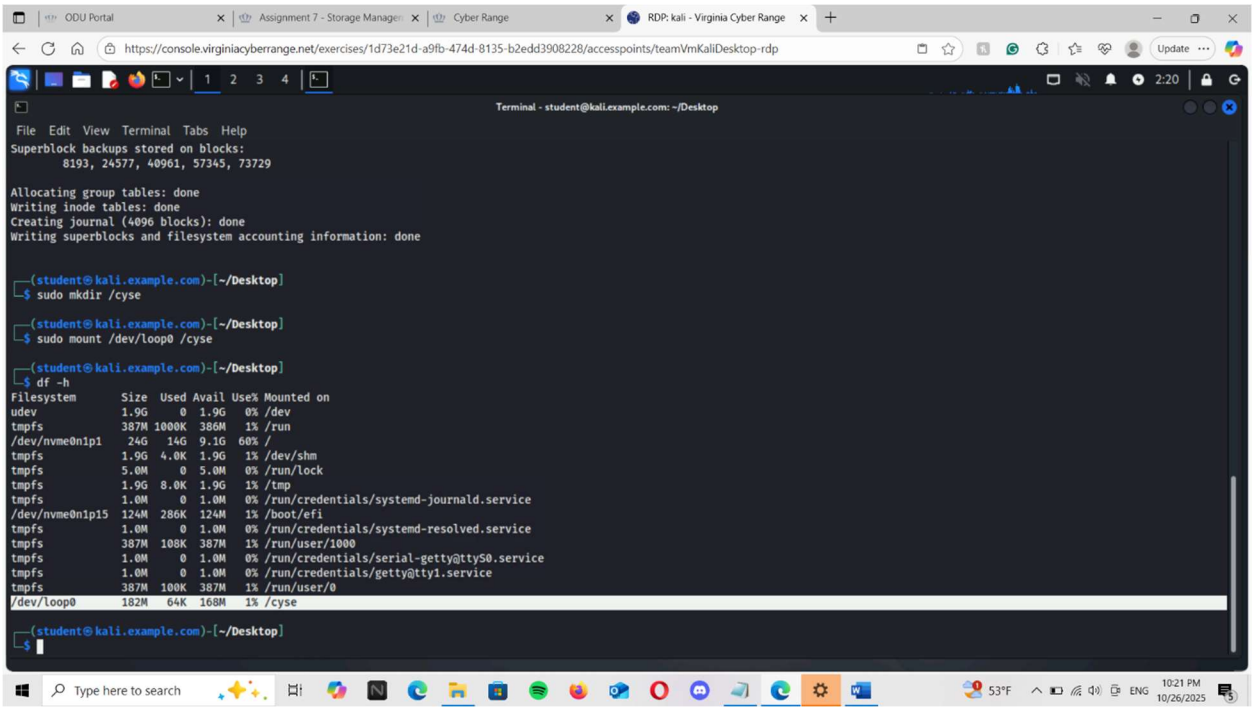
Step 3: Check the Mount Point

Use the df command to confirm the partition is mounted on /cyse.

```
df -h
```

Look for /cyse in the output. Take a screenshot to show the mount point.





Step 4: Create a File Named YourMIDAS.txt

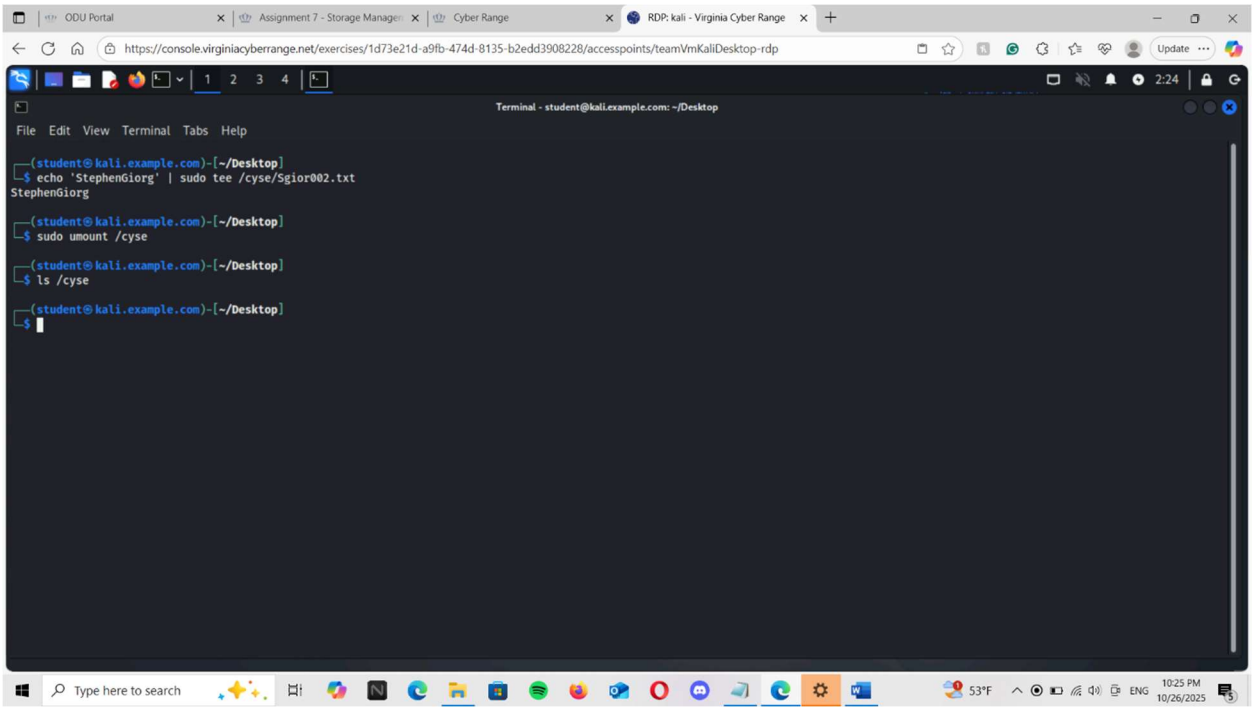
Create a file in /cyse containing your name. Replace YourMIDAS with your MIDAS ID.
echo 'Your Name' | sudo tee /cyse/YourMIDAS.txt

Step 5: Unmount the /cyse Directory

Once you've created the file, unmount the partition from /cyse.
sudo umount /cyse

Step 6: Check the Contents of /cyse

After unmounting, confirm that /cyse is now empty by running:
ls /cyse
This should return no output, as the directory is no longer associated with the mounted partition.



Part IV: Answer the following questions (30 Points)

1. Explain the purpose of using the `sudo` command with `ls /dev/sd*` and `ls /dev/nvme*`. Why is administrator privilege required in this context?
/dev will have permission requirements, especially in a virtual environment like cyber range. It also ensures that the command will be executed.

2. What is a loop device, and why do we use `losetup` to attach the virtual disk file as a loop device in this lab?
A loop device is a regular file that can be treated like a physical disk the losetup command allows the system to see the loop device as a physical disk and allow for the other commands, like mkfs, mount, and fdisk, to work as if it was a physical disk.

3. Why do we format the virtual disk using `mkfs.ext4`? Explain what this command does and why we chose the `ext4` filesystem specifically.
Simply, the command makes a extf filesystem. A filesystem that has favorable compatibility and reliability. For the sake of this lab, because it is compatible with tools like mount.

4. After mounting the virtual disk to `/cyse`, what changes should you observe in the output of `df -h`? Explain how `df` helps verify that the disk is mounted correctly.
Df -h will show the name, size, used vs available space and mount point. The mount point in particular shows the device was mounted correctly.

5. Why is it important to unmount a directory (like `/cyse` in this lab) before detaching a virtual disk? What could happen if you detach a disk without unmounting it first?
The system may have errors and data could be corrupted because you could be

unintentionally calling upon data that is no longer available. The filesystem could also be damaged because it would be ending abruptly.

6. After creating a file on the mounted virtual disk and then unmounting the disk, what do you expect to see when you check the contents of `/cyse`? Explain why this happens.
Because the disk is detached, the mount point will revert to its original state because the data was on the virtual disk and not the original directory.

7. How does using a virtual disk file differ from using a physical disk partition on your system? What are some advantages and disadvantages of using virtual disks in cybersecurity labs?
The virtual disk is ideal for testing and experimentation because it can be used in isolation, can be transferred digitally between systems, and can easily be cloned or reset. The added flexibility comes at the cost of size, speed, and requiring slightly more set up.