**Assignment- User Management**

**Name: Harpreet Kaur**

**Student Id: 200534234**

Ans1. In Linux, a user can have one primary group at a time, and it's all laid out in the /etc/passwd file. But here's the cool part: a user can also be part of multiple secondary groups! Now, groups themselves can't directly belong to other groups in the traditional file system permissions and user management context. However, if you want to get fancy, you can set up more complex arrangements using access control lists (ACLs) or directory services like LDAP. That's where nested group memberships come into play.

Ans2. Windows and Unix/Linux-based systems use different files that hold the hash representations of account passwords and a list of local accounts.

**For Linux-based systems:**

• The list of local accounts is typically found in /etc/passwd.

• The hash representations of account passwords are usually stored in /etc/shadow.

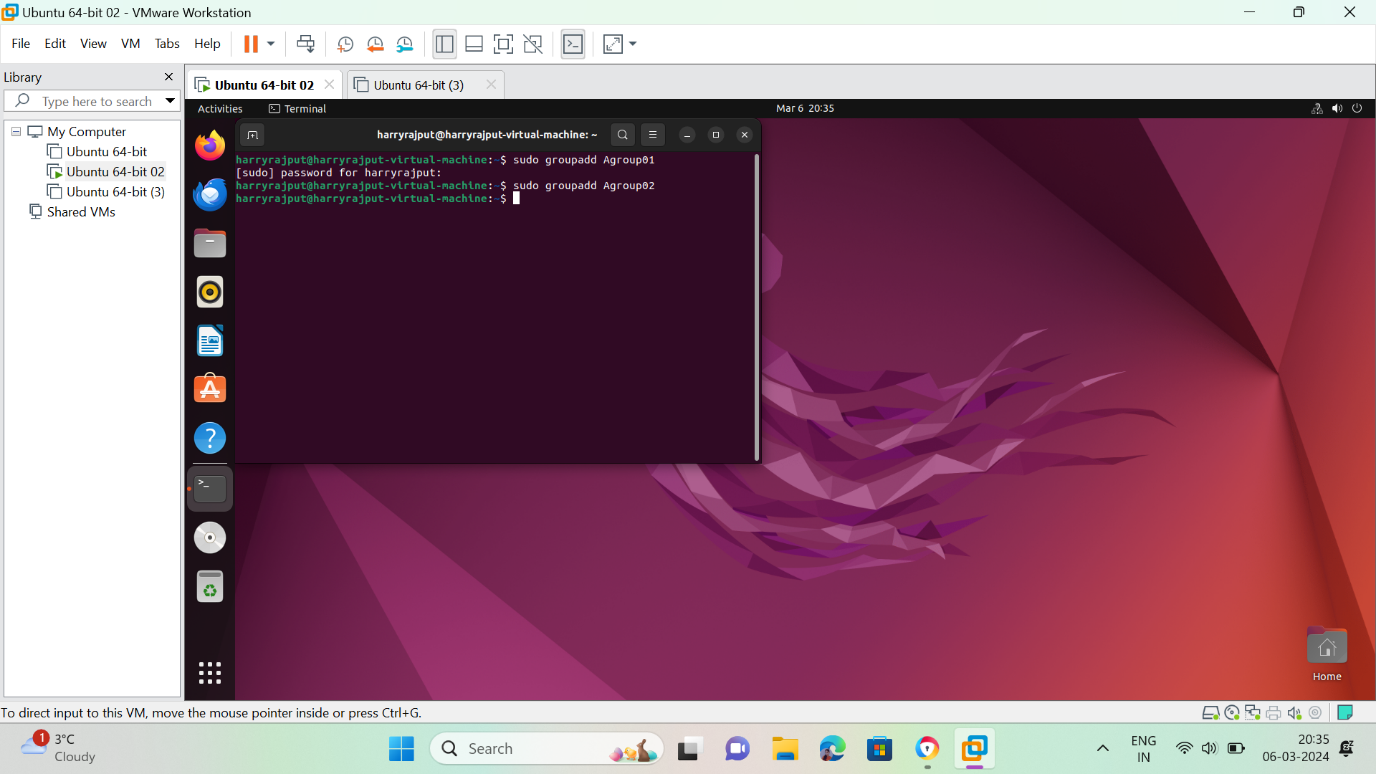
**Regarding Windows-based systems:**  
Because it is situated in %SystemRoot%\system32\config\SAM, the Security Accounts Manager (SAM) database houses the list of local accounts and their hash representations. During operation, the SAM database cannot be directly accessed. Nevertheless, while the system is not in use, external tools can be used to read the SAM file. Alternatively, programs like regedit can be used to access the registry, which houses these details.

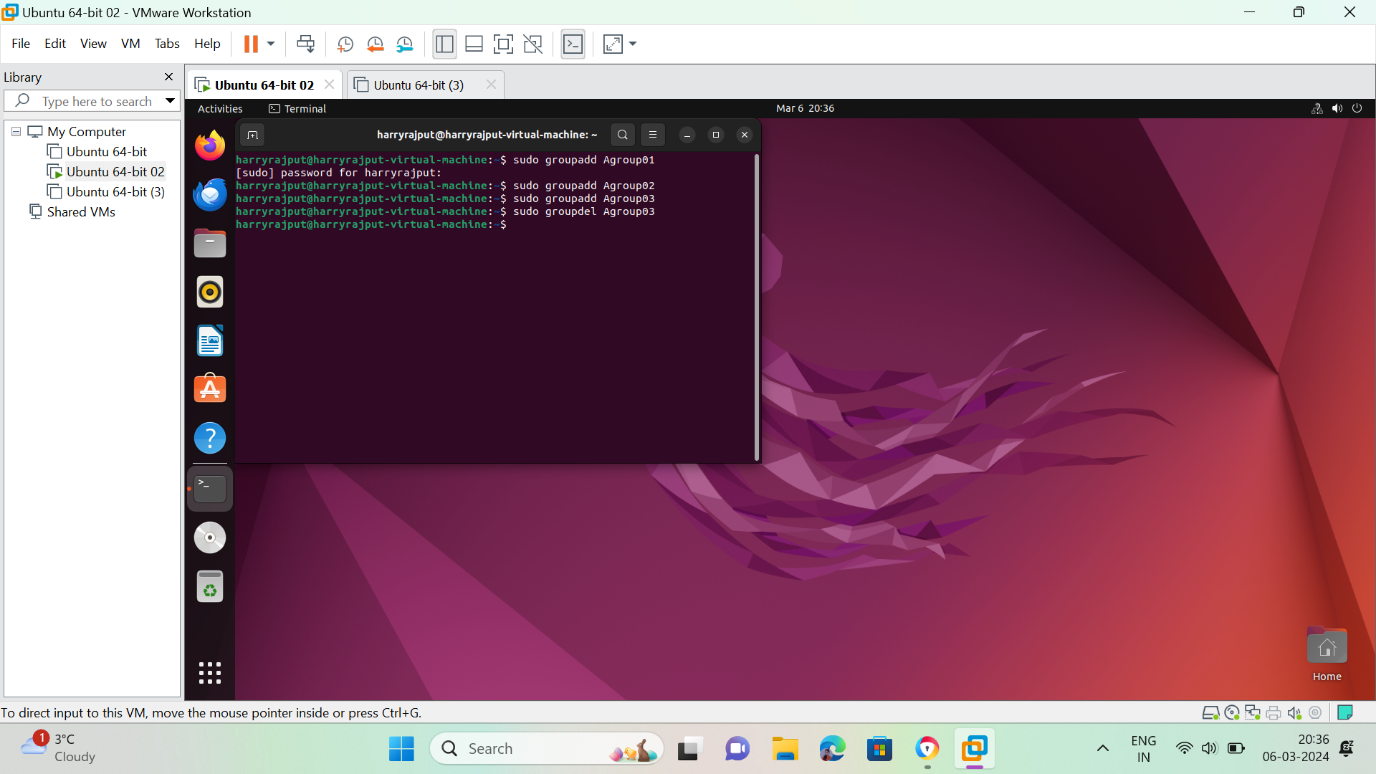
Ans3. The `/etc/login.defs} file defines the shadow password suite's default values. This user account management configuration file establishes default system settings, such as password behavior policies like password length and expiration time, for newly created users. Utilities like `usermod`, `passwd}, and `useradd` use it.

**Part-B**

Ans1. Command to create and delete groups:

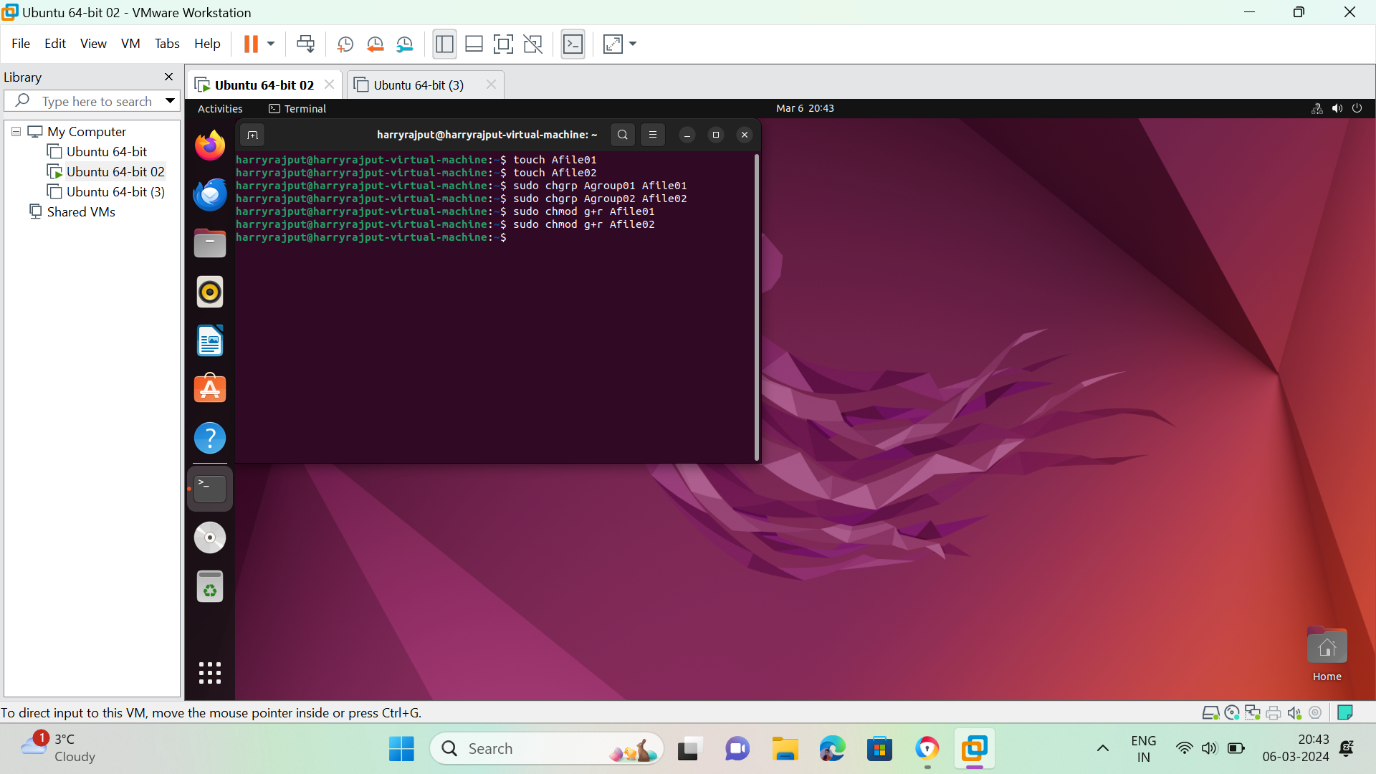
We use the ‘groupadd’ command to create groups and ‘groupdel’ to delete groups as shown in the screenshots below





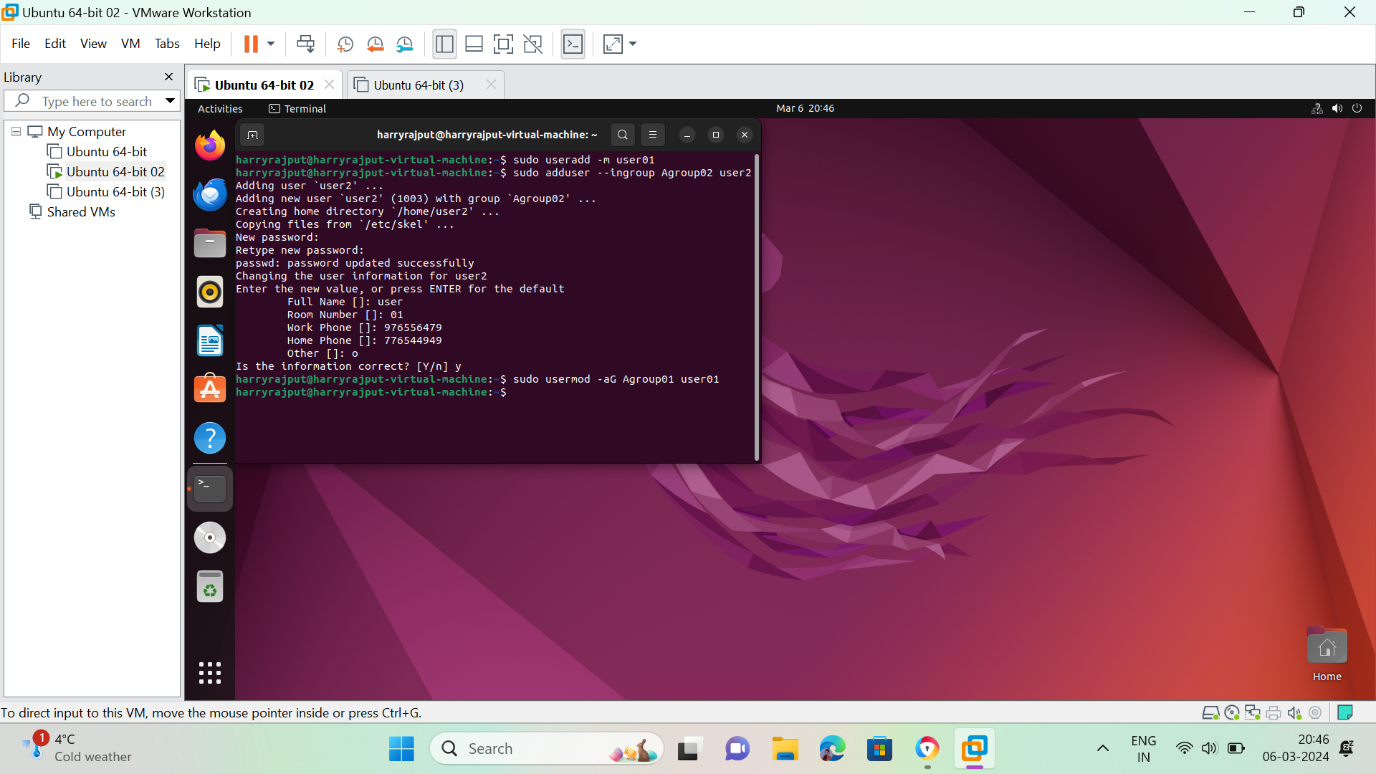
Ans2**. Commands to add files to groups and change group permissions:**

Use ‘chgrp’ command to add files to the group, user chmod to change permissions of group for a file or folder.



Ans3. **Commands to create and add users to the group:**

To add the users to a group, follow the ‘usermod’ command which requires the user to be originally added before. If you want to create and add user simultaneously, use ,adduser-ingroup’ followed by <groupname> and <username> as shown below.



**Part-3**

Ans1. Meaning of two(!!)exclamation mark in the shadow file:

Linux indicates that a user account has been created, but no password has been assigned, when there are two exclamation marks (!!) next to the account name in the shadow file. Because anyone can access the account without a password, there is a security risk in this scenario. Double exclamation points denote the existence of an account for which there is no password, hence permitting unlimited access.

Ans2. Reasons for switching users and difference between su and sudo:

Su: The command su, which translates to "substitute user" or "switch user," does just that: it launches a second shell instance with the target user's rights. It asks for the target user's password to make sure you have permission to do that. Thus, the root password is necessary in order to become root. Your machine's root password will be the same for all users who need to run commands as root, so be sure they all know it. It is untidy to have to reset the root password and share it with only the individuals who require access in order to remove an administrator's privileges from a user.

Sudo: Super-User-DO, or sudo, is entirely distinct. It makes use of a configuration file called /etc/sudoers that identifies the users with the authority to perform particular tasks, such as running commands as root. In order to confirm that the person at the terminal is indeed "joe" who is listed in /etc/sudoers, it requests the password of the user who initiated it. You only need to change the configuration file (or remove the user from a group that is listed in that config) to cancel someone's admin credentials. As a result, privilege management is considerably more streamlined.

Ans3. Command to edit the superuser’s configuration file:

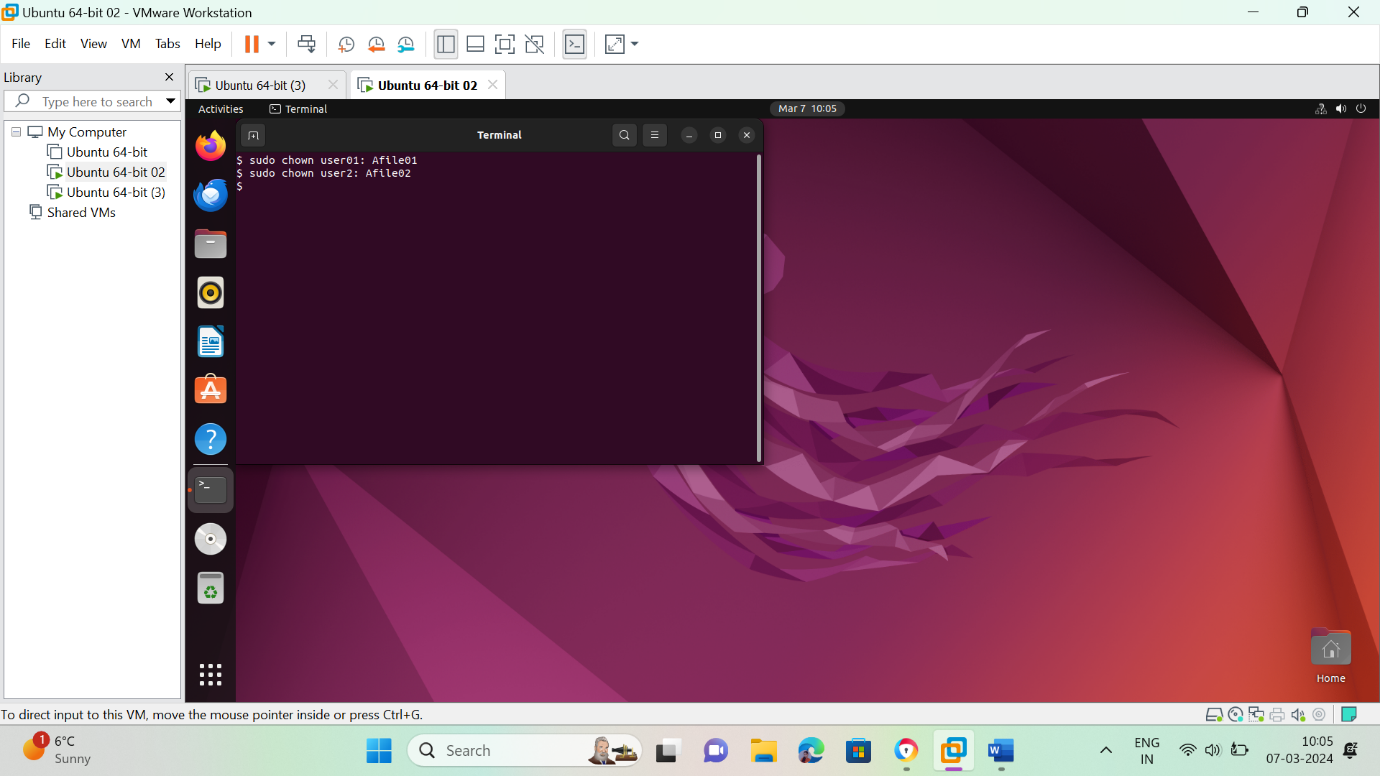
In Linux, you should use the visudo command to alter the super user's configuration file. The Sudoers file, found at /etc/sudoers, regulates user rights for running commands with superuser access. This command is essential for properly modifying the file.

Visudo reduces the possibility of errors that can affect system functionality by checking the file's syntax before saving modifications. When making adjustments, it is imperative to use caution and to fully comprehend the syntax and ramifications of the Sudoers file. Recall that the usage of visudo guarantees safe and regulated administration of superuser rights.

**Part-4**

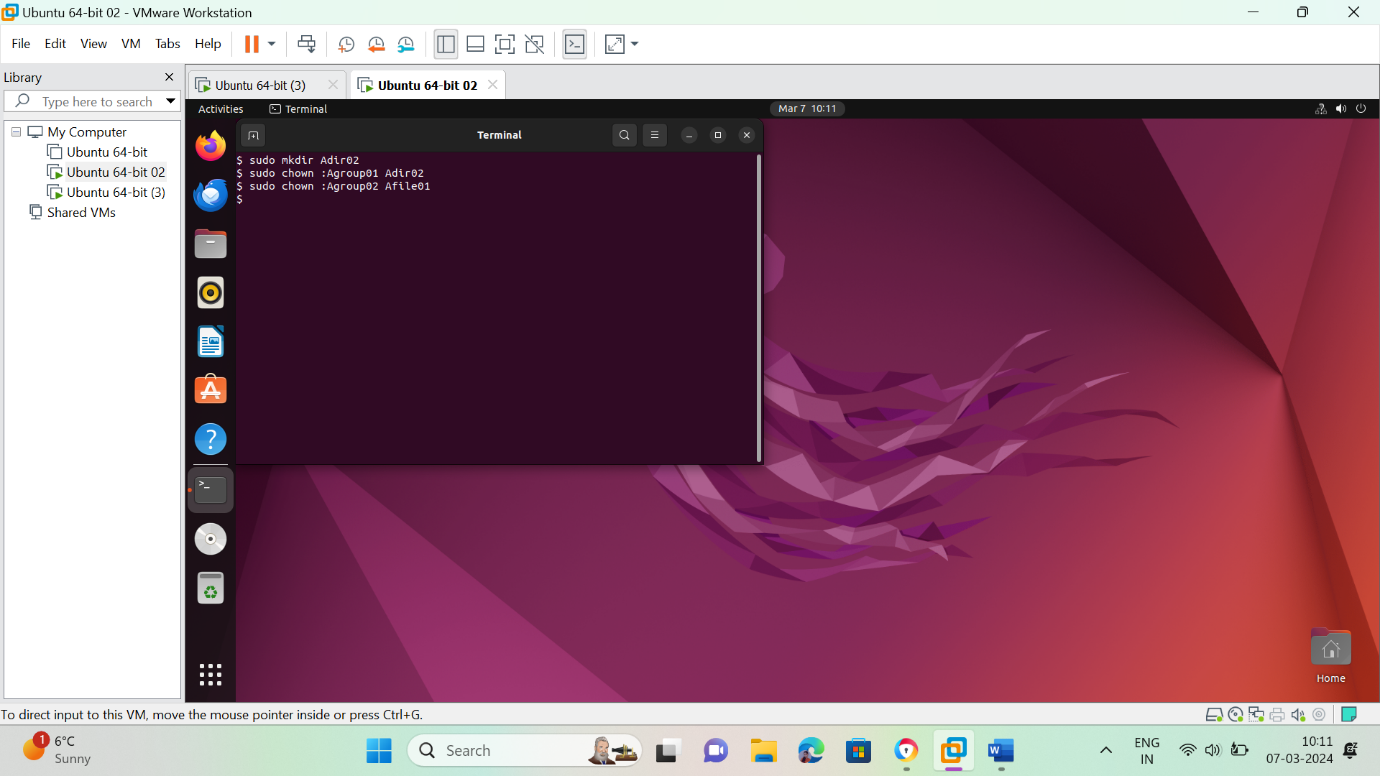
**Ans1. Command to change the owner of a file directory:**

The command ‘sudo chown new\_owner: new\_file’ is used to change the owner of the file



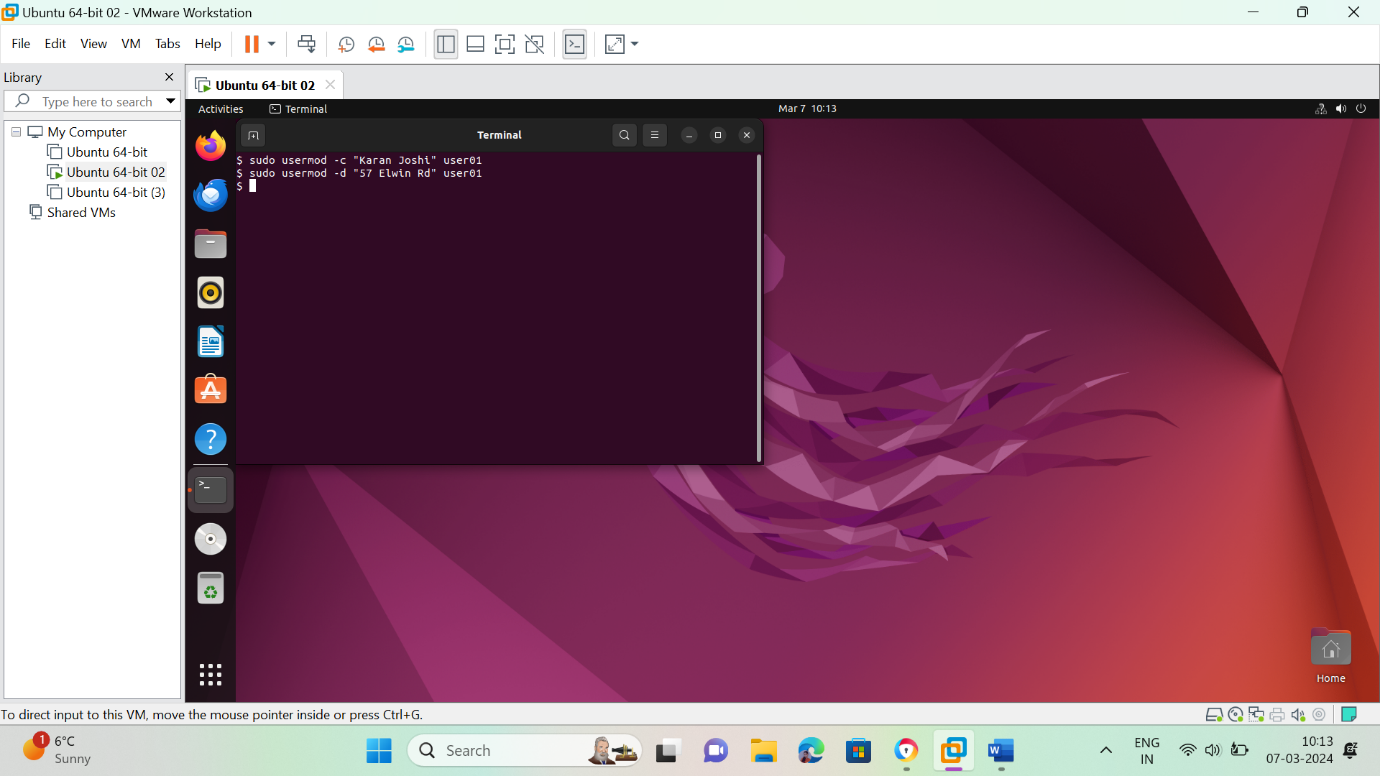
**Ans2. Command to change the group ownership of a file or directory:**

The command ‘sudo chown: new\_group new\_file’ is used to change group ownership of a file or directory.



**Ans3. Command to change user’s full name and other details:**

The command ‘sudo usermod username’ is used to change user’s details



**Ans4. Command to display detailed user information**:

The command ‘id or w or last username’ are used to display detailed user information.

