# 5CS031 Network Security

# Workshop 4: Windows and Linux Access Control Features

**Student Name:\_\_\_\_\_\_Loucas Xiourouppa\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Student Number:\_\_\_2007307\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**You will need to complete the workshop tasks, answer the questions and then submit this Word file, complete with any required screenshots and answers, before the deadline posted on Canvas.**

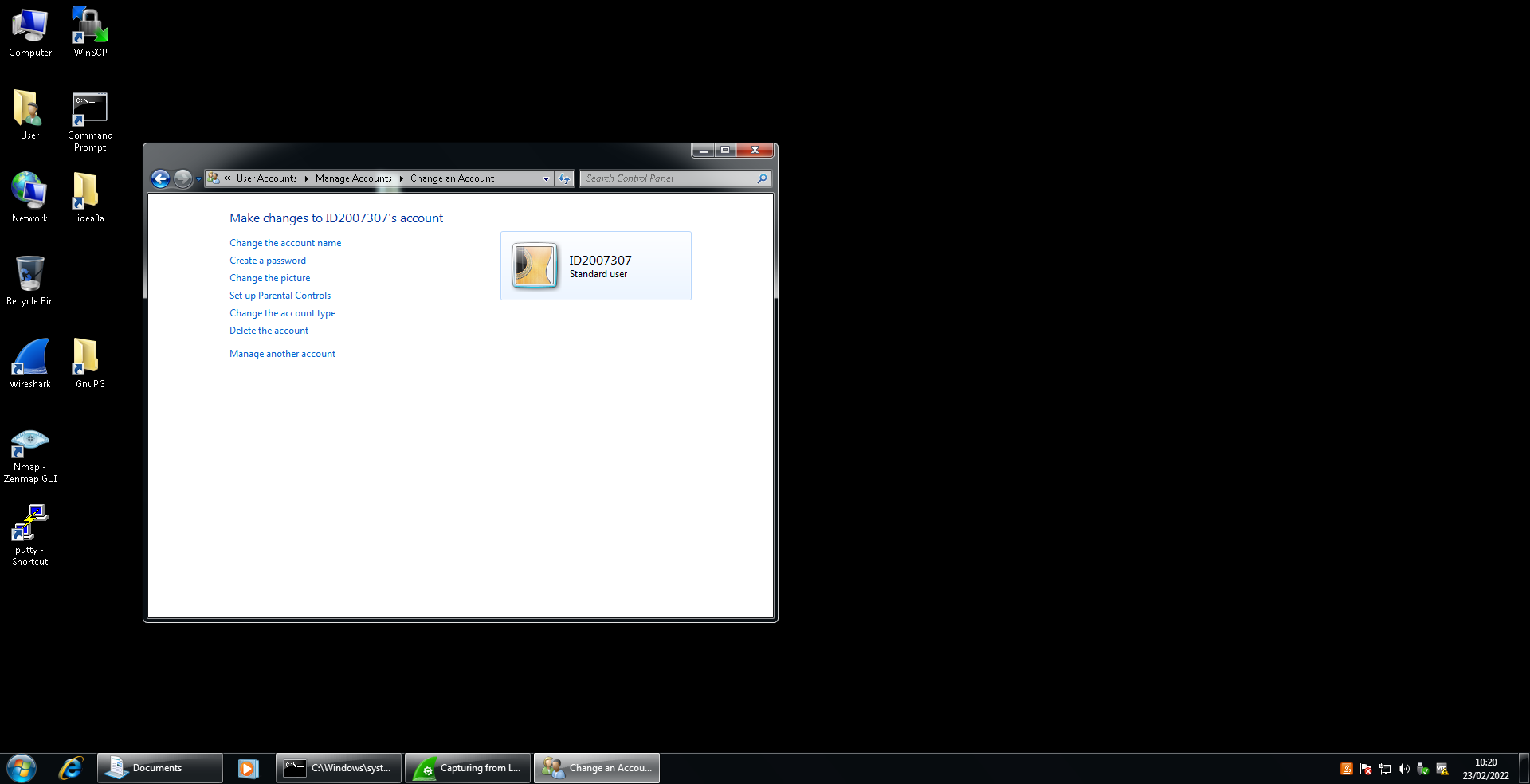
**Objective**

Access Control - The objective of the workshop is explore the access control features available in the Microsoft Windows and Linux-based systems and to compare them.

**Part 1**

You will be using Windows 7 running **within the VMware environment** to carry out this part of the workshop.

**Task 1: Adding users to the system**

1. Start VMware Player
2. Start the Virtual Machine called Security Windows 7.
3. Create a “Standard User” account with username as ID*xxxxxx*A where *xxxxxx* is your student ID. Therefore if you student ID is 987654321, you will name the user as ID*987654321*A
4. Capture the screenshot showing the new user account.  
     
   [Your Screenshot Here]
5. 

**Task 2: Investigating the effects of using the Read-Only and Hidden attributes of a file.**

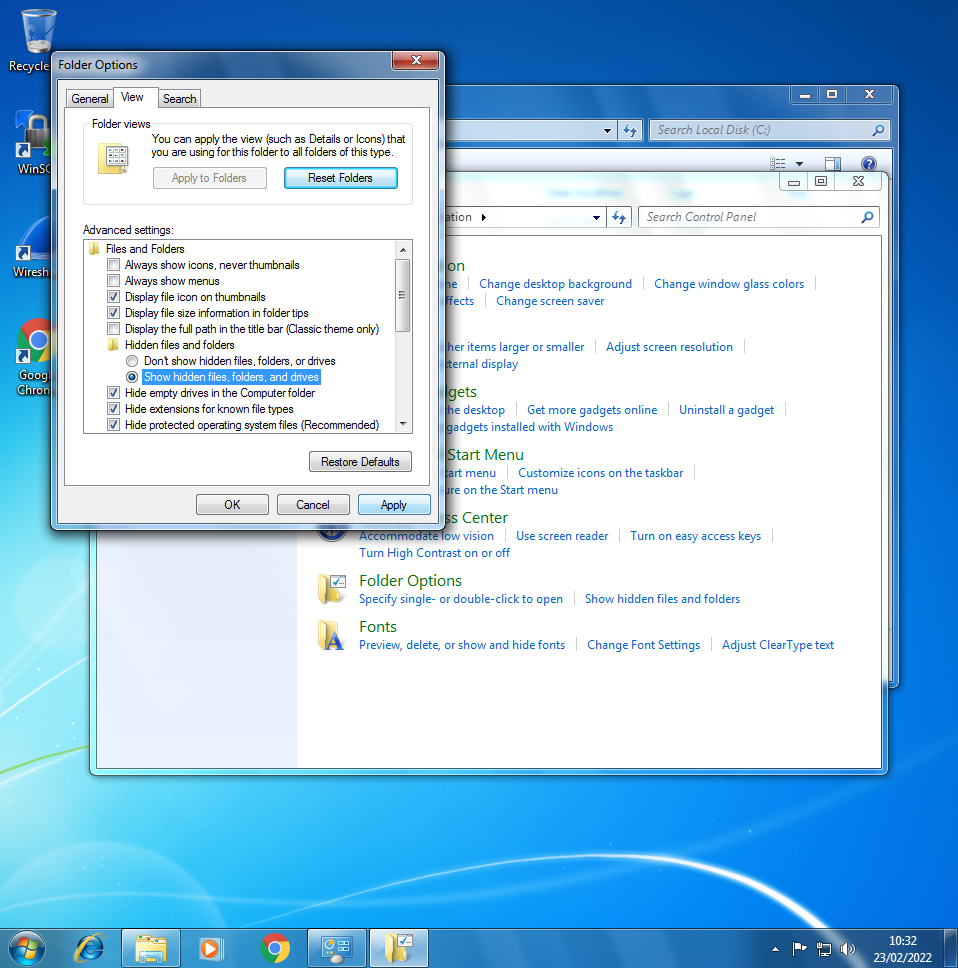
1. Still within the Security Windows 7 VM, you are going to create a folder and file to use for this task.
2. Create a new text file named "file1\_user.txt" inside a “Workshop3” folder on the Local Disk (C:). Put some text content into your file.
3. Change the properties of the files to a “Read-Only”
4. Open the file again, add some text and try to save the changes. What happens? Explain why it happens.

[Your Answer Here]

When I type something new in the file and try to save it, it tries to save it as entirely different file instead of just saving the file. This happens because we set the files as read only so you absolutely cannot change the contents inside it hence why it creates another file.

1. Log off from the "User" account and log on as the user ID*xxxxxx*A.
2. Open the "C:\Workshop3" folder and then show the Properties for the file "file1\_user.txt" (this might be shown as just "file1\_user" as filename extensions are sometimes not shown).
3. Check the Hidden property of the file, and click OK.
4. Close the window and then open the "C:\Workshop3" folder again.
5. Do you see the file now?  
     
   [Your Answer Here]
6. I cannot see the folder workshop 3
7. If you cannot see the file, try to find ways to show the hidden file. Google search for a solution if you can't work it out. Which method worked for you?  
     
   [Your Answer Here]

went in control panel > view files, then clicked on “show hidden files” and pressed ok. i can now see the hidden file



1. Log out from ID*xxxxxx*A.

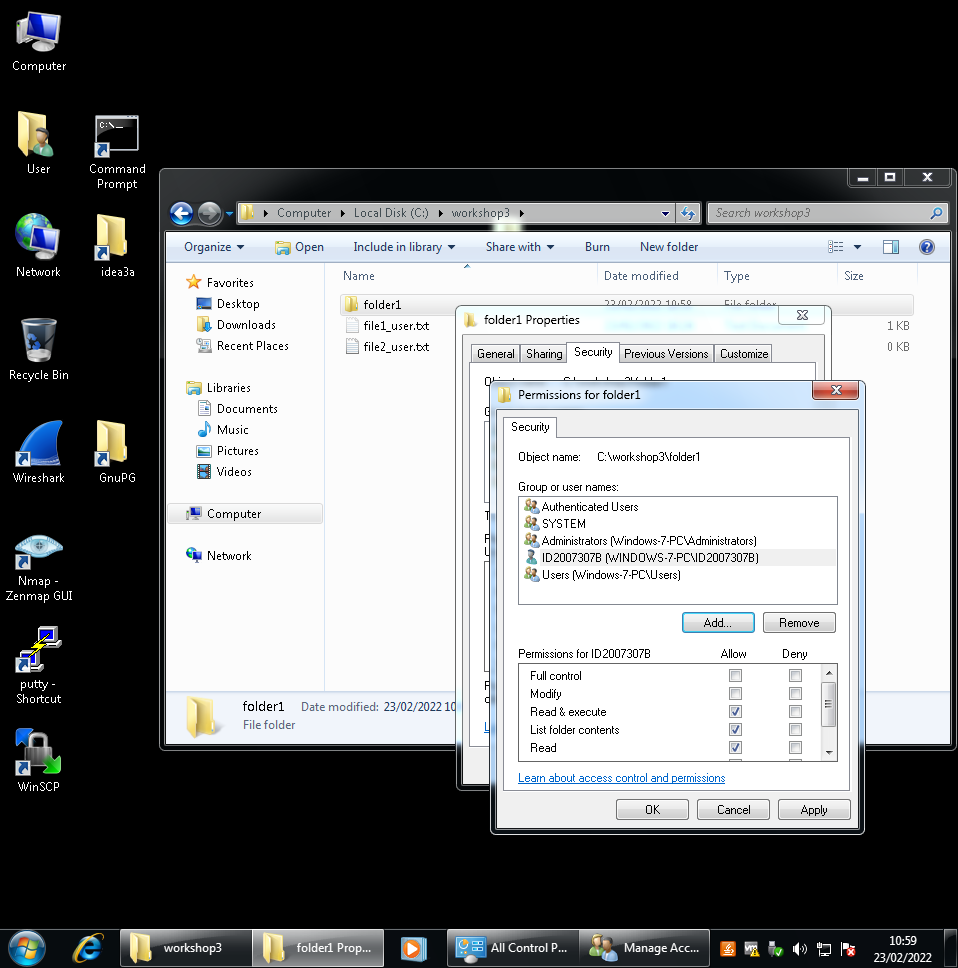
**Task 3: Explicitly assigning permissions to different users for a given file.**

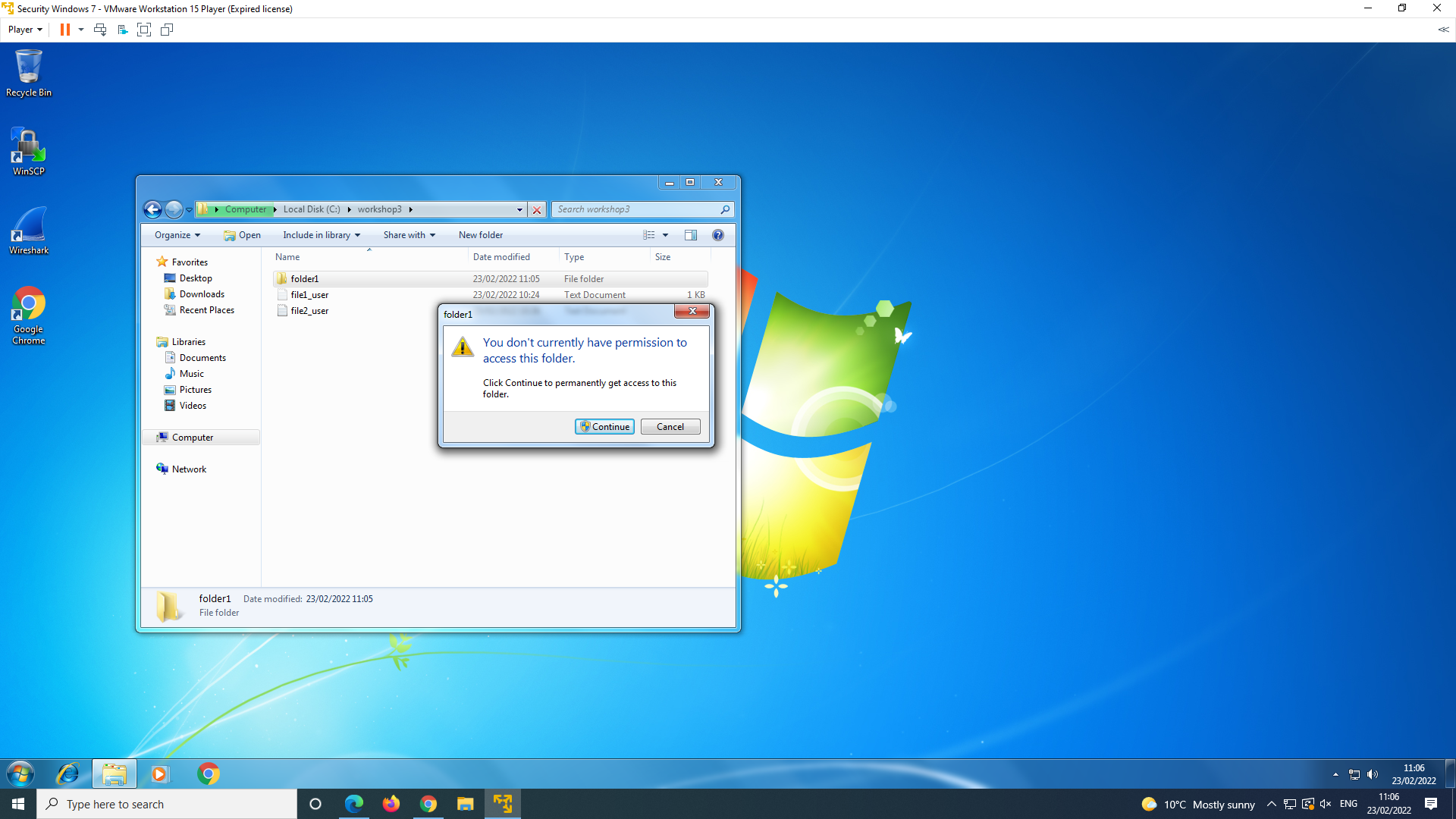
1. Log in as the user account "User" .
2. Create a text document in the "C:\Workshop3" folder with "file2\_user.txt" as the filename.
3. Give access to this file to the user ID*xxxxxx*A
4. What are the default permissions given to this user?

When I give him permission to the file, it instantly gives him authorization to look at it but not customise it.it sets the folder for him to “read” only. I then had to give him full control to be able to customise it.

2. Check the permissions assigned to the group called Users (Windows-7-PC\Users). Are the default permissions for this group different than those of the user you added to have access to the file?  
     
   [Your Answer Here]
3. this group can “Read and execute, list folder contents and read” where as the other user only had “Read”
4. View the advanced set of permissions for access to this file for user ID*xxxxxx*A .
5. What permissions are ow available for you to set?   
     
   My permissions access is “full control” but i can also change other users permissions
6. Click Ok until you are back to just the file in the folder.

**Task 4: Investigating the MS Windows access control mechanism**

1. Make sure you are still logged in as the default account "User"
2. Create another additional user in the system with the username of ID*xxxxxx*B where the X's are replaced by your student ID.
3. Create a new folder “folder1” inside "C:\Workshop3" folder
4. Give access to this folder to ID*xxxxxx*B .
5. What permissions are currently assigned to the user?  
     
   [Your Answer Here]
6. Read and execute
7. list folder contents
8. Read
9. 

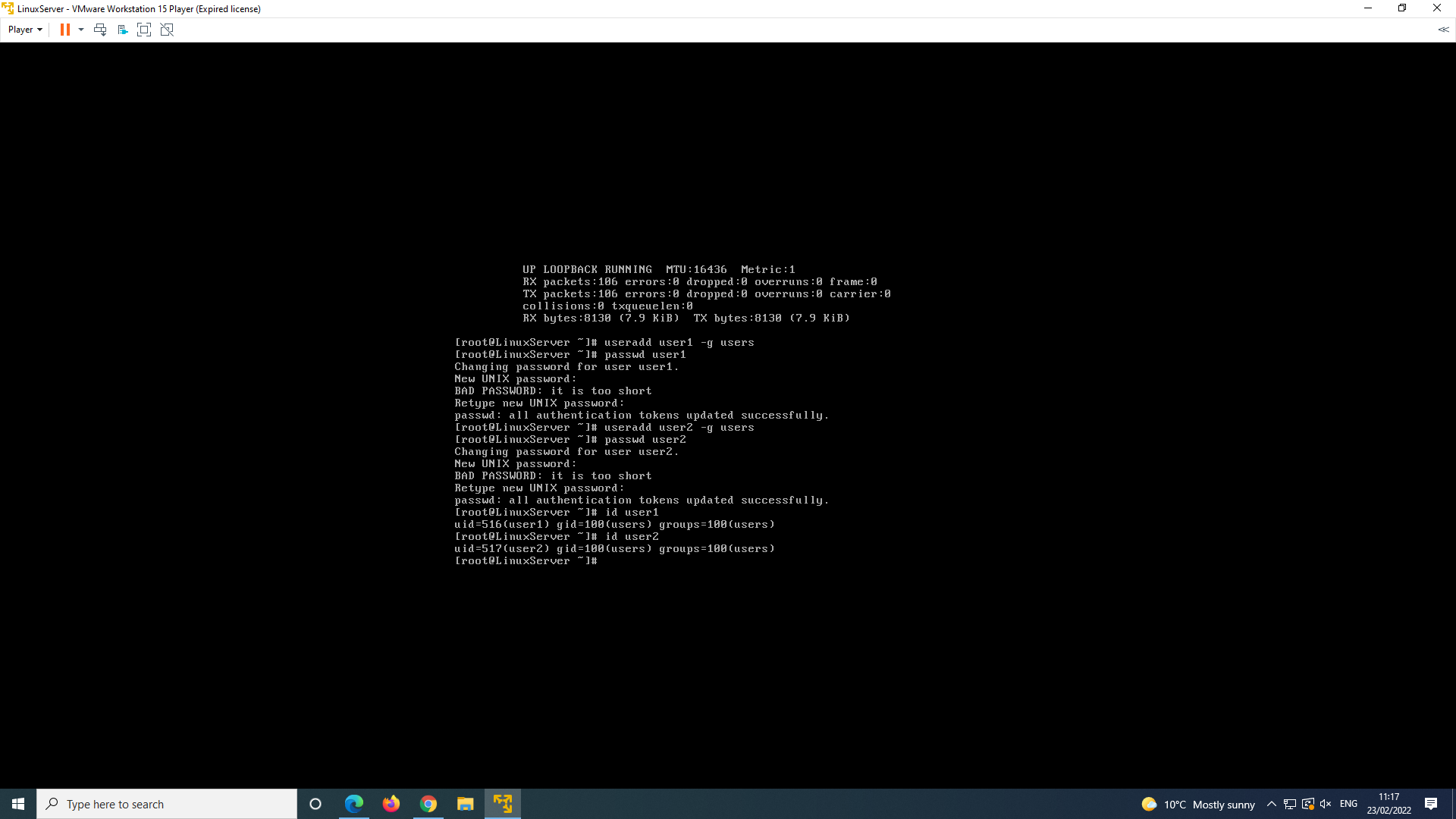
1. Mark the List folder contents permission under the Deny column. Click OK and approve all changes.
2. Logoff from the "User" account and log in as ID*xxxxxx*A
3. Open the Notepad application to create a text document
4. Type some text in the document and save it in the "C:\Workshop3\folder1" folder with the name "file3\_user.txt"
5. Open the "C:\Workshop3"\folder1" folder and verify that you can open the document you just created.
6. Logoff from the ID*xxxxxx*A account and log in as the ID*xxxxxx*B user
7. Open the "C:\Workshop3"\folder1".
8. Explain what happens when you access the folder and why?   
     
   It says I don't have permission to the folder because I ticked deny in the list of contents in properties so I'm not allowed to do anything with that folder.
9. 
10. What steps do you need to carry out if you want to make a file inside the "C:\Workshop3"\folder1"editable by the ID*xxxxxx*B user, if the file was originally created by the ID*xxxxxx*A user? (I suggest you try out the steps).   
      
    I would have to log in as user A and go into the properties for the folder and untick the deny list of contents click that we did and tick full control. that way user b will have access to do anything with that folder
11. Shutdown the Security Windows 7 VM. You have finished Part 1 of this workshop.

**Part 2**

**VMware Linux Server**

1. You will need to setup and configure your own personalised Linux Server virtual machine for this exercise.
2. From the Resources in Canvas, download the file called “LinuxServer.zip”. Right-click on this file and extract the zip file into a folder, and then rename the folder to “LinuxServer1234567”. Change the numbers to your own student ID.
3. Change the Virtual machine name from “LinuxServer” to “LinuxServer1234567”. Use your own Student ID for the numbers.
4. Start the virtual machine and if you are prompted with the question “Did you move this virtual machine, or did you copy it?”, select **“I moved it”** and click OK.
5. The workstation's anti-virus program may popup and ask if you allow this program. You will have to click "Allow".

**Task1: Setting up File Structure and User space**

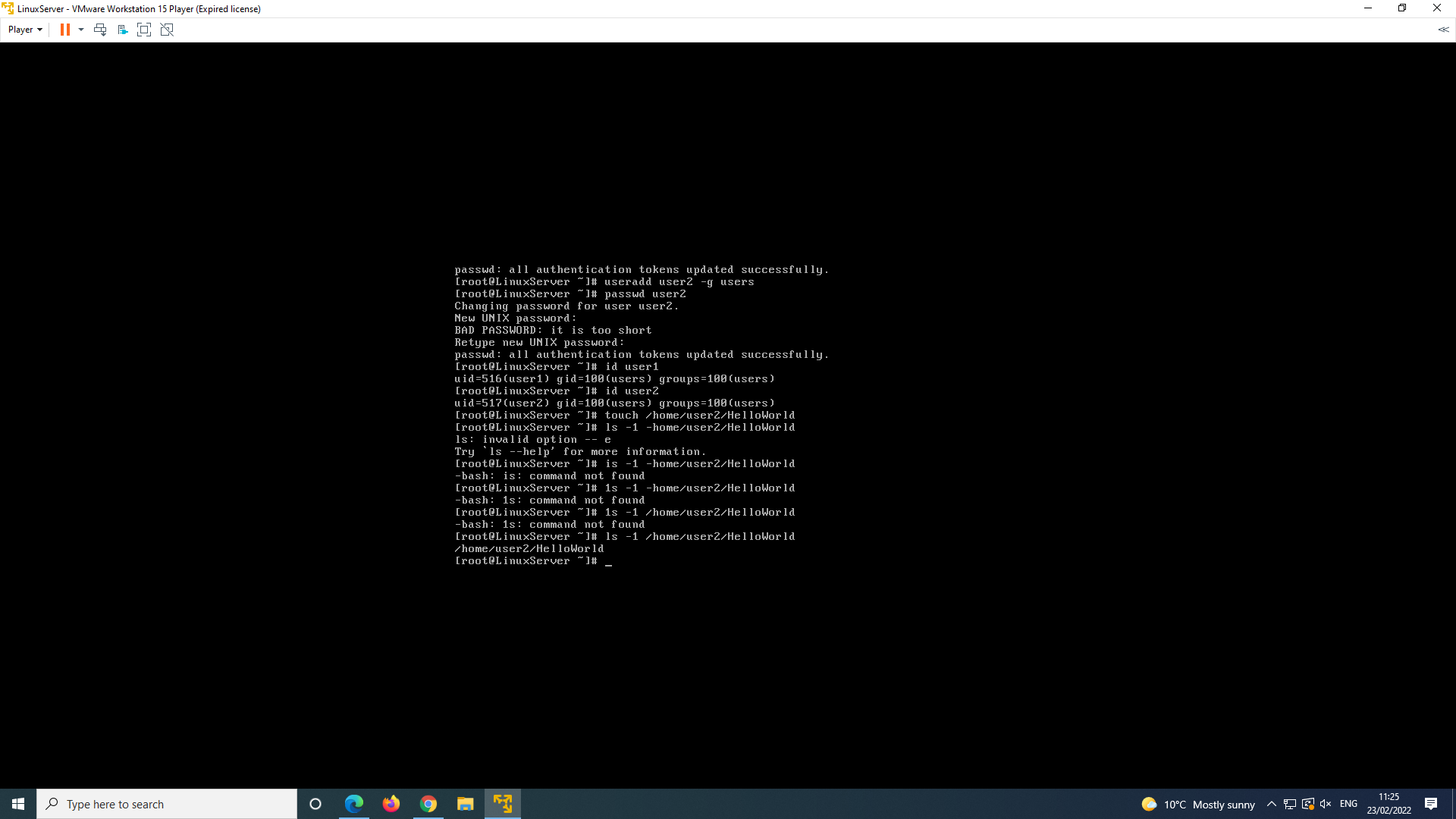
1. Start the LinuxServer Virtual Machine.
2. Login as root (password = "password")
3. Use useradd command create a new user “**user1**” as follows:  
     
   **useradd user1 -g users**Create a **password** for the user that you created. For convenience, set the passwords the same as the username
4. Create a second user “**user2**” and set a password for it.
5. Check user information with the id command.   
     
   **id user1  
     
   id user2**
6. Capture the screenshot for the output above and paste it below:  
     
   [Your Screenshot Here]
7. 

[What information can you observe from this output?]

This tells me how many groups of users there are which equals to 100

1. Create a new file (as **root user**):  
     
   **touch /home/user2/HelloWorld  
     
   ls -l /home/user2/HelloWorld**
2. What are the owner and group of HelloWorld?   
     
   [Your Answer Here]

user2



1. Change group ownership to “users” as well as user ownership to “user2” for the created file the file
2. What are the owner and group now for the file **/home/user2/HelloWorld**?

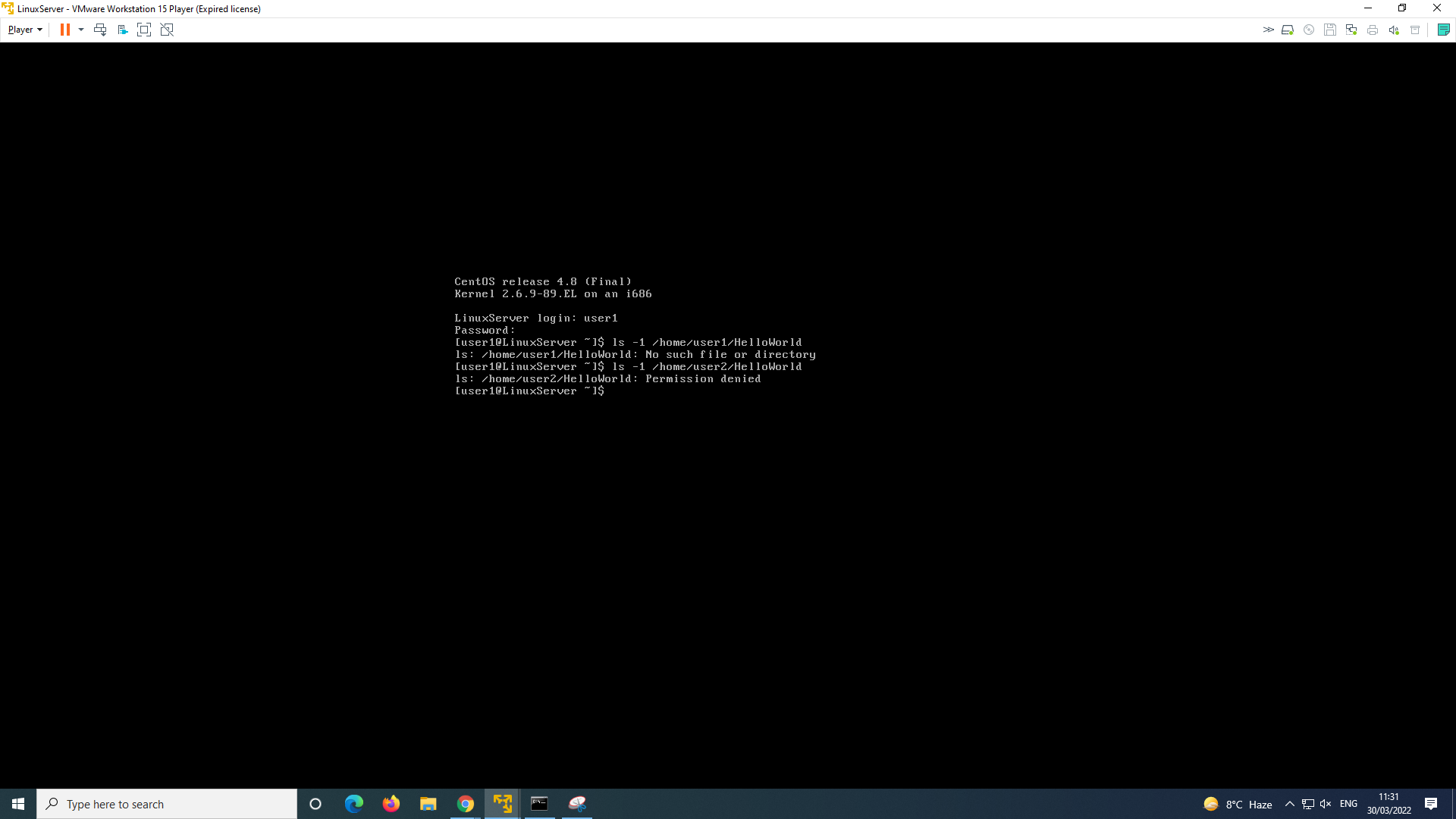
[Your screenshot and answer Here]

**/users/user2/HelloWorld**?

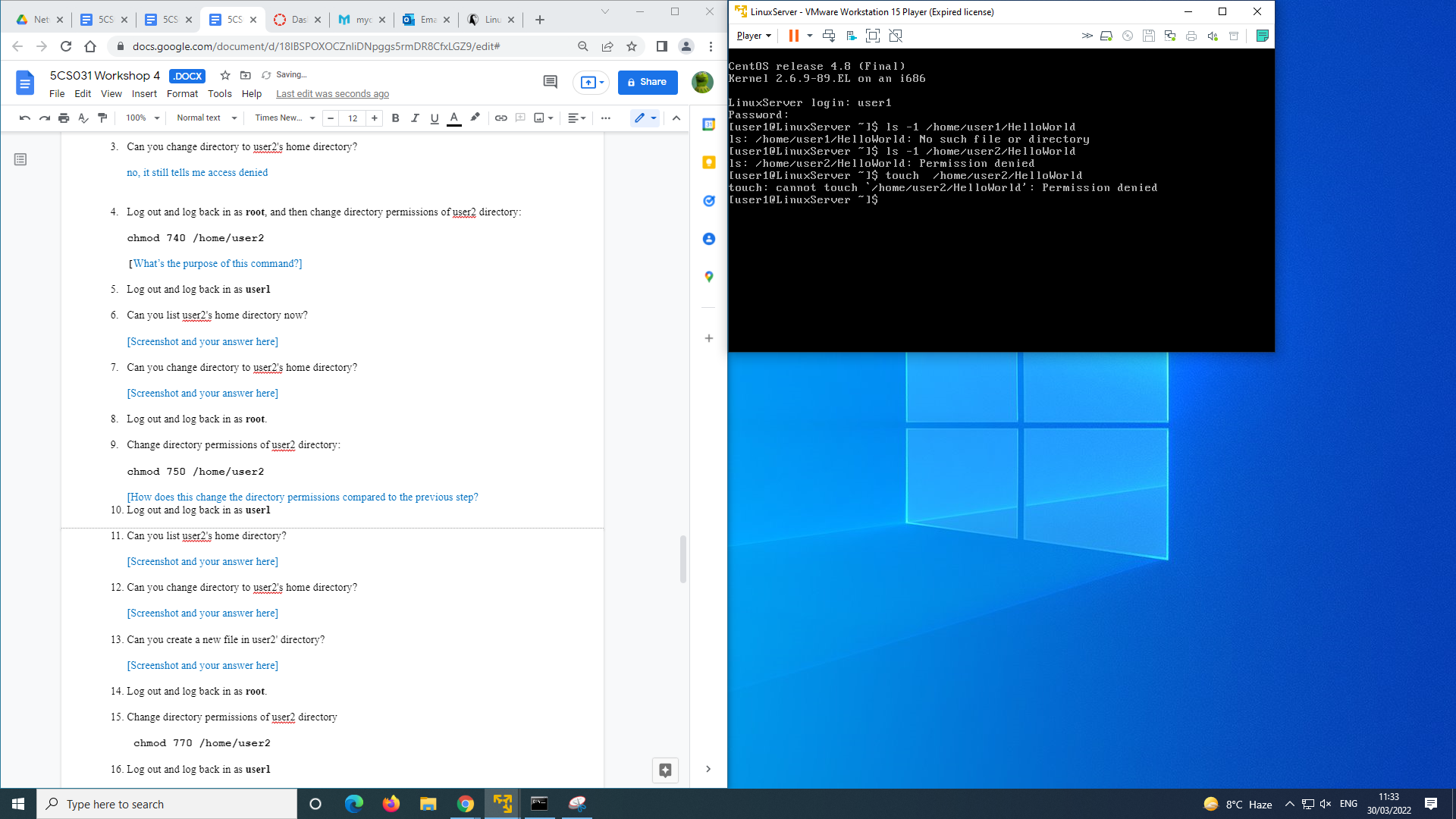
**Task 2: Differences in File and Folder Permissions**

The objective of the following tasks is to investigate the differences between file and folder (directory) permissions. The chmod command will be used to change file and directory permission to demonstrate the slight differences in permissions for files and directories. Make sure you are logged in as root.

1. Find the directory permissions for user1, user2 and test directories. First log out (**exit**) and log in as **user1**.
2. Can you list user2's home directory?  
     
   logged in as user1 i get permission denied when i try to list user 2 directory



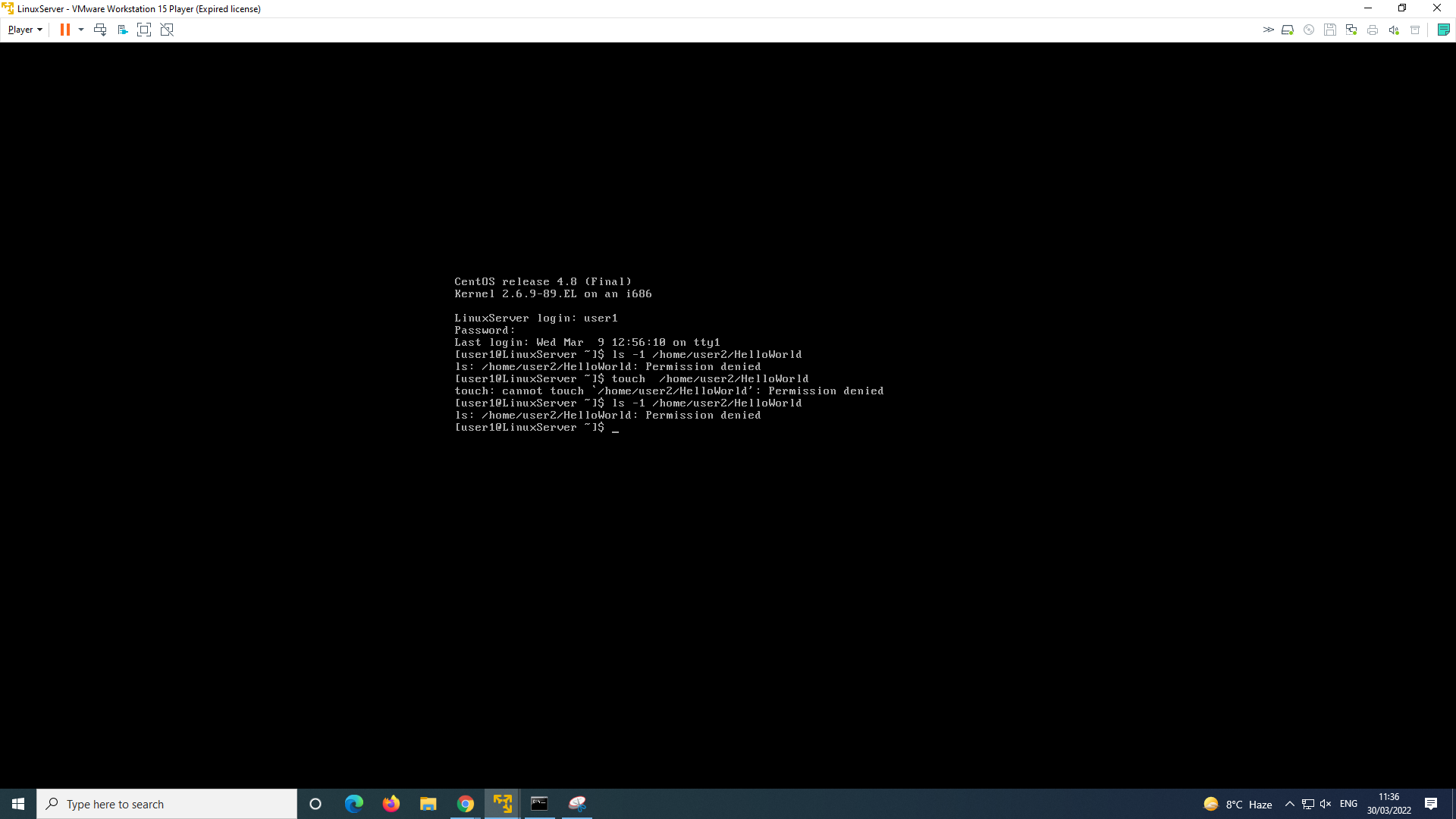
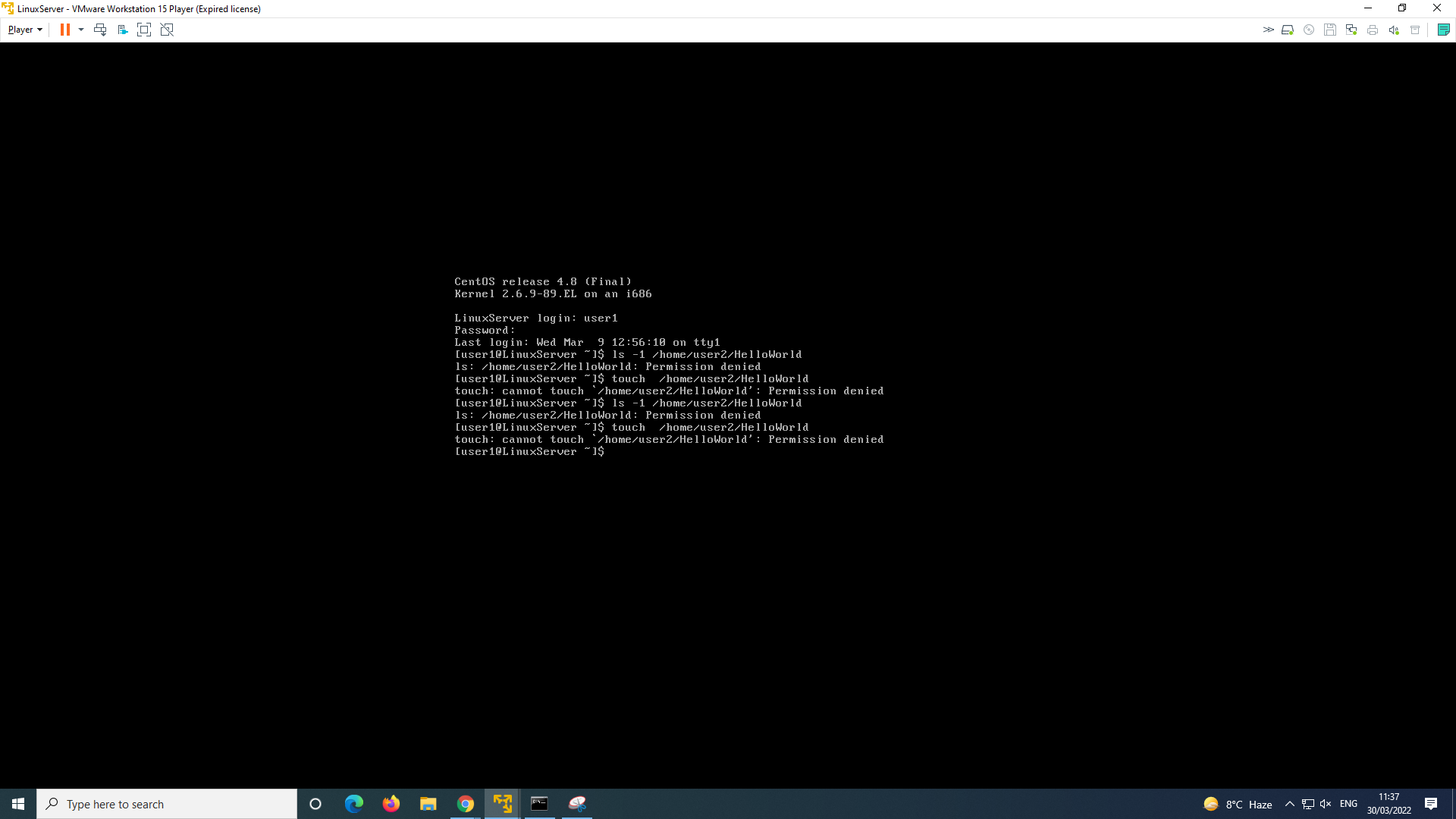
1. Can you change directory to user2's home directory?  
     
   no, it states permission denied.



1. Log out and log back in as **root**, and then change directory permissions of user2 directory:  
    **chmod 740 /home/user2**

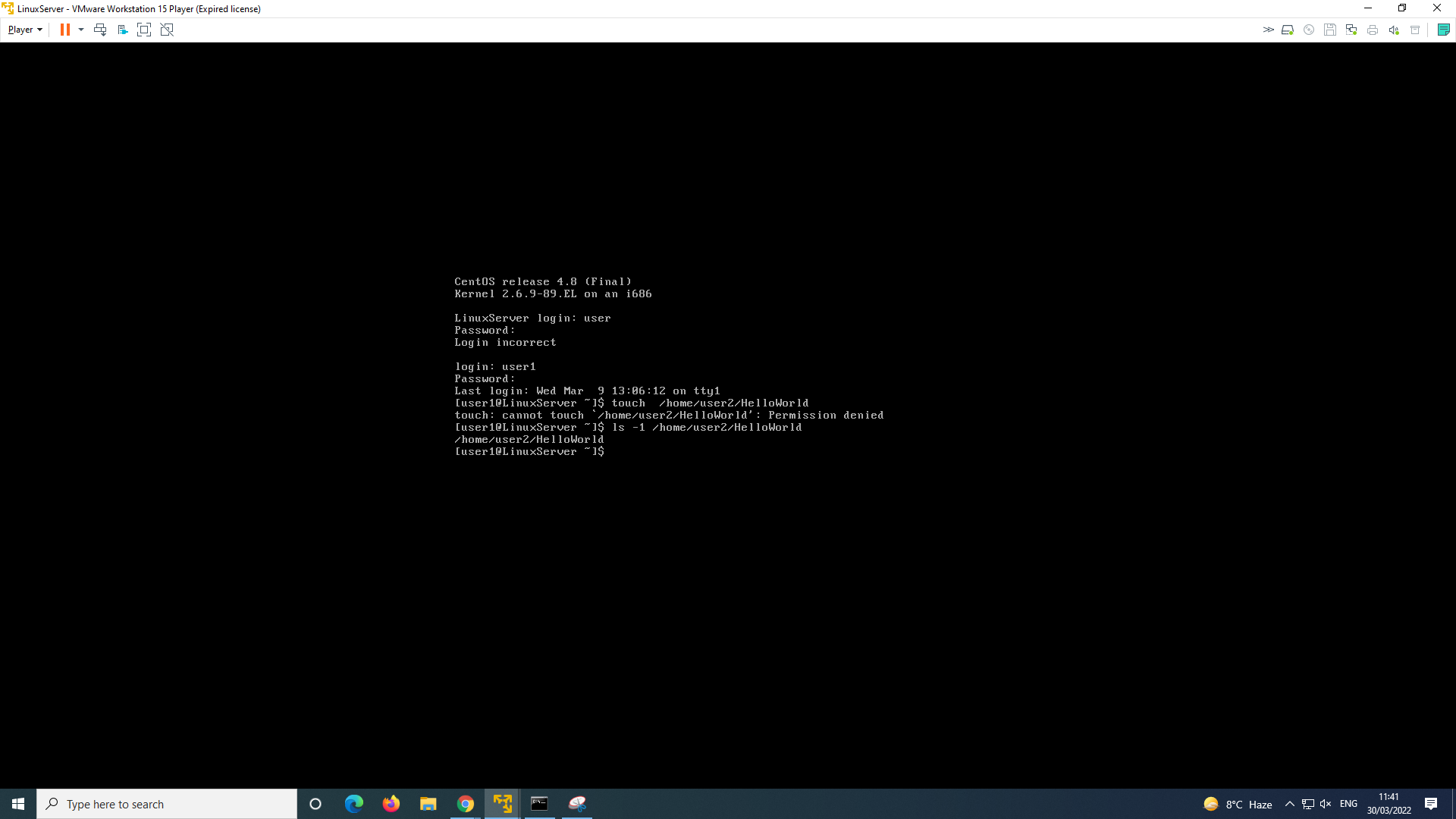
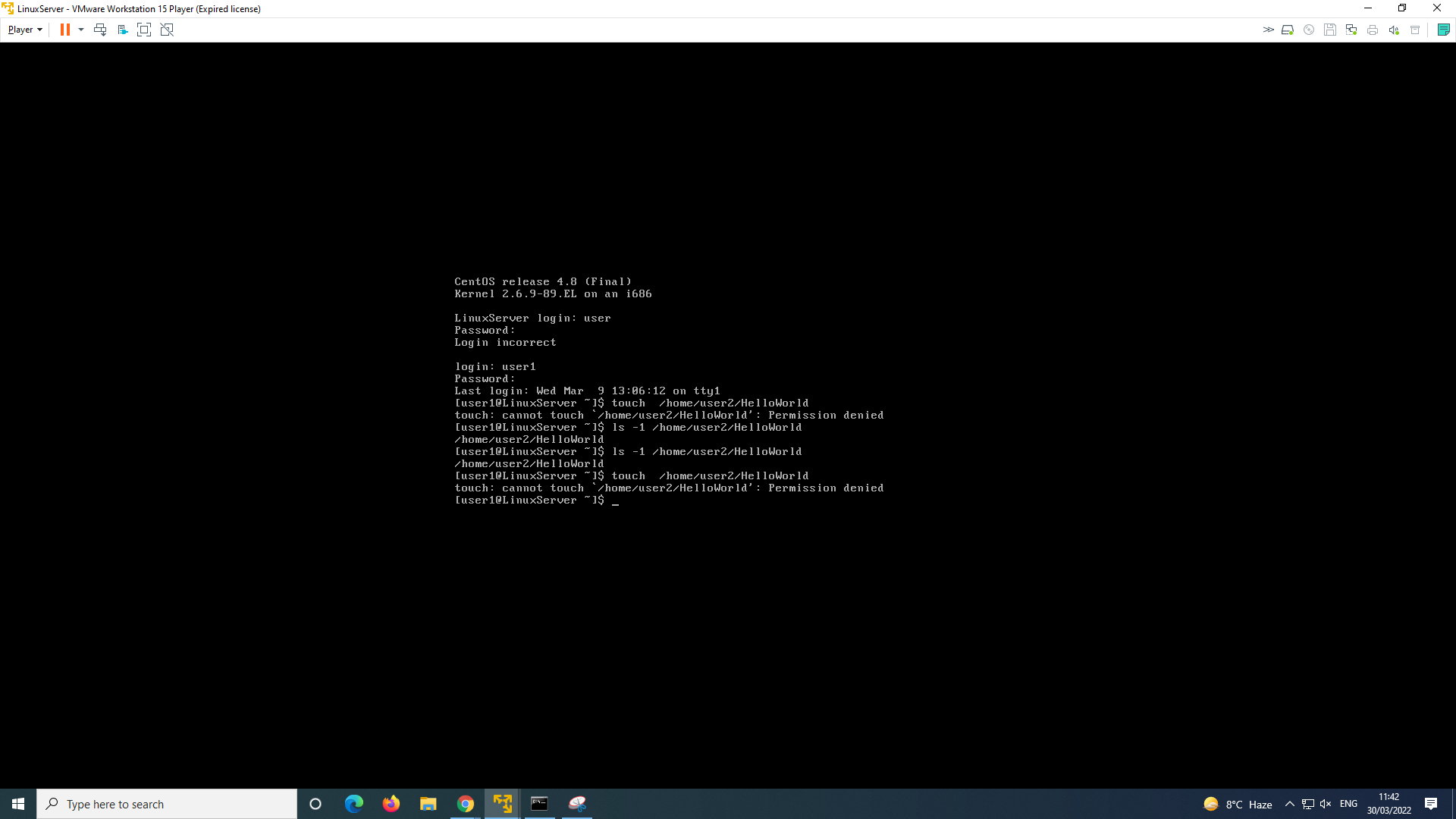
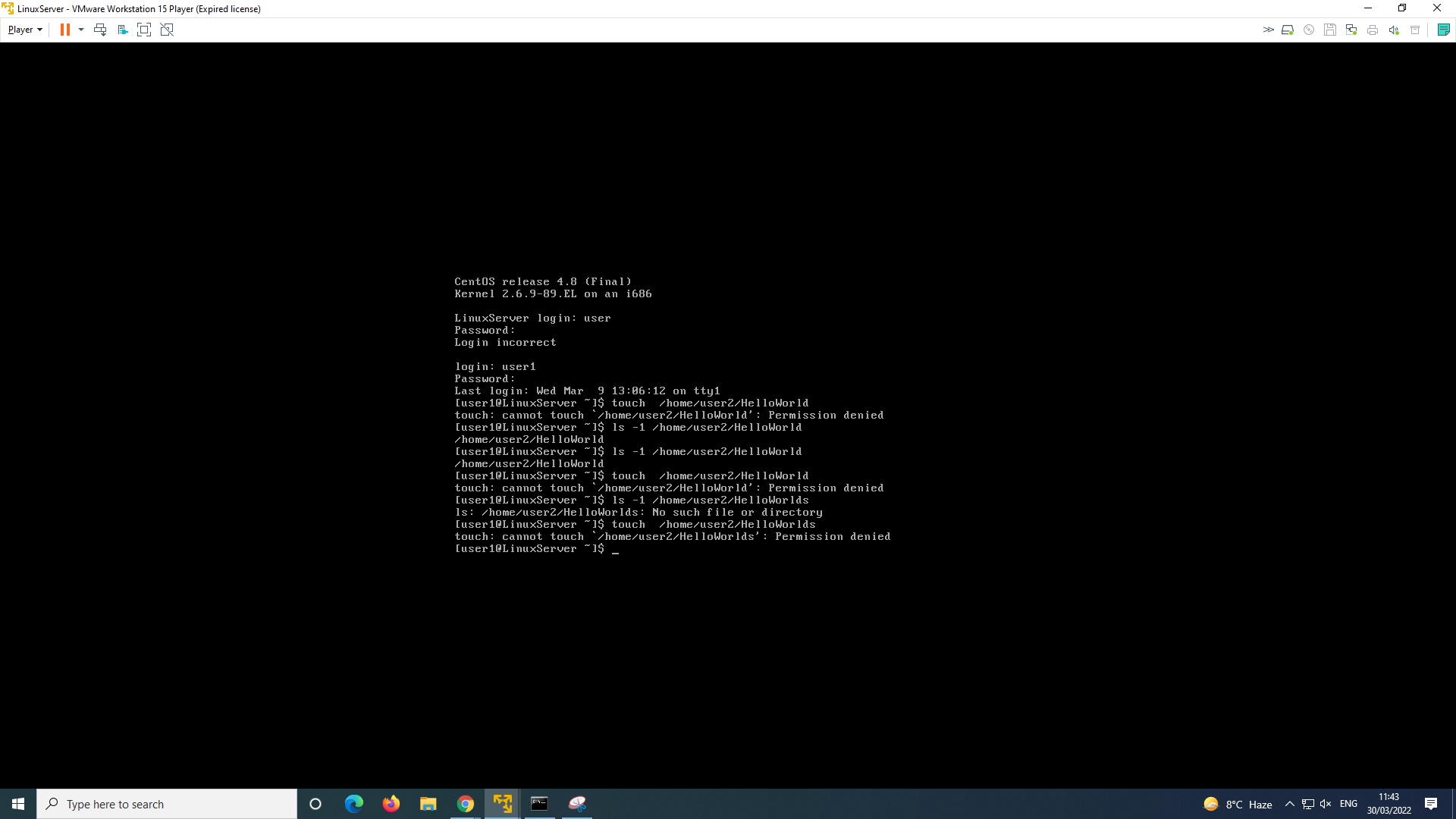
**[**What’s the purpose of this command?]

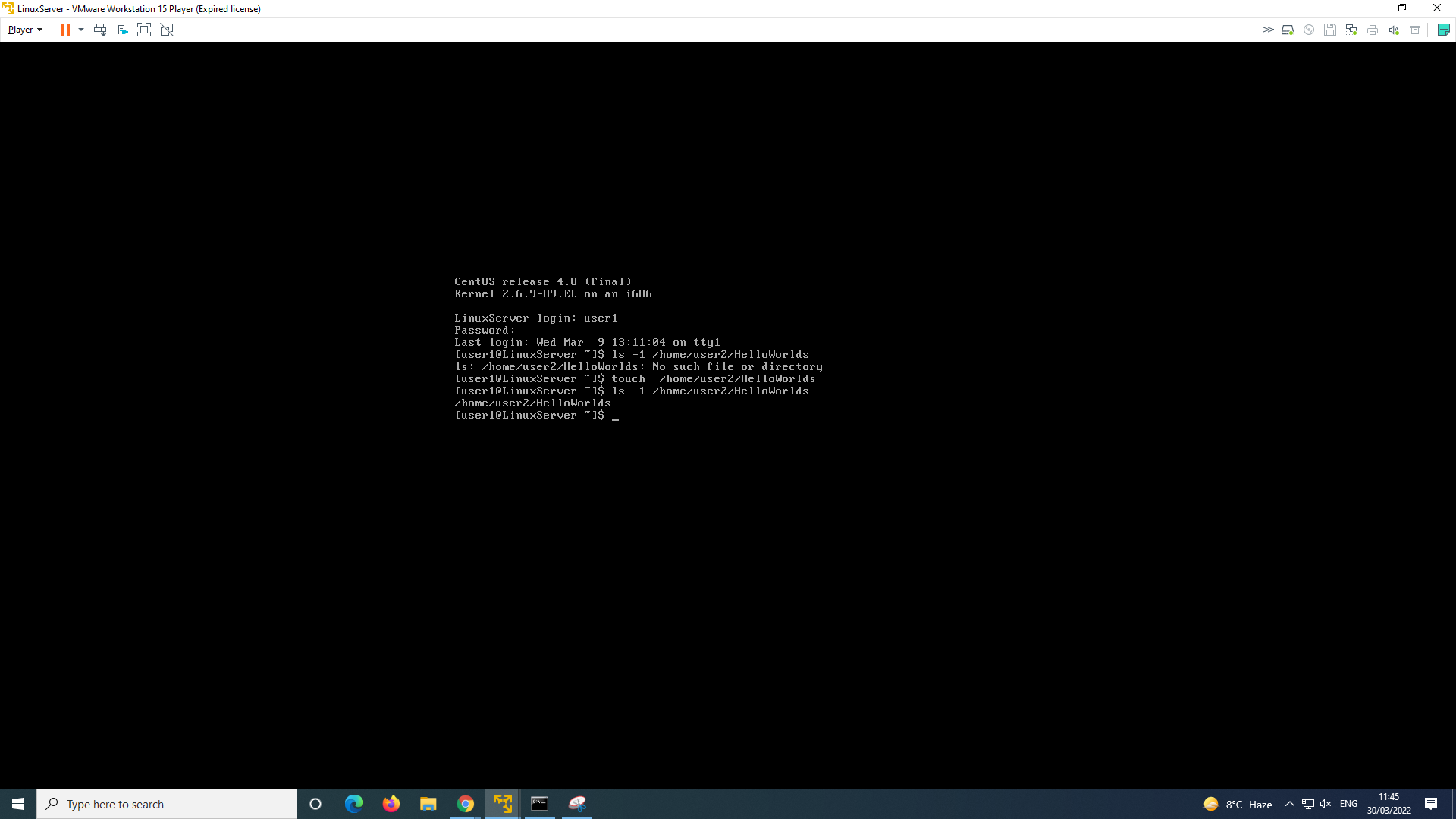
This command gives full permissions to the owner and read only to everyone else. so they can see it but not edit it.

1. Log out and log back in as **user1**
2. Can you list user2's home directory now?  
     
   [Screenshot and your answer here]  
   No it still won't let me
3. 
4. Can you change directory to user2's home directory?  
     
   [Screenshot and your answer here]
5. I cannot change user2 home directory.  
   
6. Log out and log back in as **root**.
7. Change directory permissions of user2 directory:  
     
   **chmod 750 /home/user2**

[How does this change the directory permissions compared to the previous step?

This command makes it so the current user has full control and the group cannot write and others cannot read, write or execute**.**

1. Log out and log back in as **user1**
2. Can you list user2's home directory?  
     
   yes i can list user2 directory
3. 
4. Can you change directory to user2's home directory?  
     
   i cannot change user2 directory
5. 
6. Can you create a new file in user2' directory?  
     
   No it won't let me create a new file.
7. ****
8. Log out and log back in as **root**.
9. Change directory permissions of user2 directory  
     
    **chmod 770 /home/user2**
10. Log out and log back in as **user1**
11. Can you create new file this time?  
    yes i can, i created a file called **HelloWorlds** instead of **HelloWorld**



1. Log out and log back in as root.

**Default file permissions and Group access control**

Whenever a new file is created a default set of permissions is assigned to it. Whatever the permissions are, the UNIX system allows the user to filter out unwanted permissions set by default. This default setting can be set by the user using the umask command.

The command takes the permissions set during creation of file and performs a bitwise AND to the bitwise negation of mask value. Some common umask values are 077 (only user has permissions), 022 (only owner can write), 002 (only owner and group members can write), etc.

There is also a "symbolic" version of the bitmask and permissions:

umask [letter] operator [symbol]

For example :

umask u-w

The [letter] represents either the user, group or others:

u = user

g = group

o = others

a = all (all three of the above)

The operator specifies how the permission modes of the mask should be adjusted.

| + | permissions specified are enabled, permissions that are not specified are unchanged. |
| --- | --- |
| - | permissions specified are prohibited from being enabled, permissions that are not specified are unchanged. |
| = | permissions specified are enabled, permissions that are not specified are prohibited from being enabled. |

The symbols indicate which file permission settings are to be allowed or prohibited by the mask

r = read read a file or list a directory's contents

w = write write to a file or directory

x = execute execute a file or recurse a directory tree

Example:

umask u-w,g=r,o+r

This would set the mask so that it would:

1. prohibit the write permission from being set for the user, while leaving the rest of the flags unchanged;
2. allow the read permission to be enabled for the group, while prohibiting write and execute permission for the group;
3. allow the read permission to be enabled for others, while leaving the rest of the other flags unchanged.

**Task 3: umask exercise**

1. Make sure you are logged in as the **root** user.
2. Use the umask command to check the current mask permission and assign a new mask:  
     
   **umask**
3. What is the current mask in octal format?  
     
   [Your Answer Here]

0022

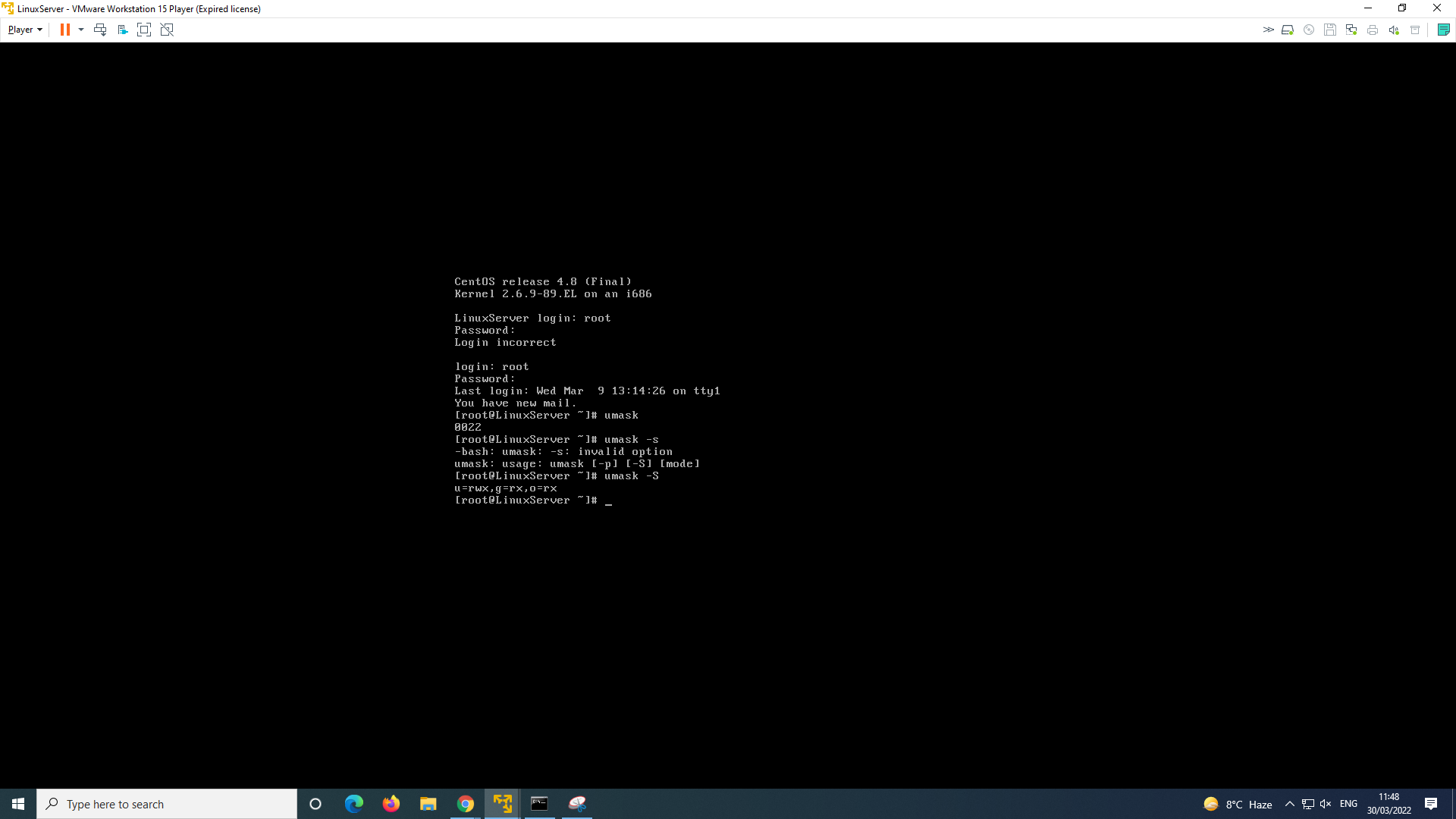
1. Now use the symbolic form of the command. Enter the following:  
     
   **umask -S**
2. What is the output in symbolic format?  
     
   [Your Answer Here]

u=rwx,g=rx,o=rx

1. What default rights do the user, group and other have according to the current umask?  
     
   [Your Answer Here]
2. I have read, write and execute permissions.

The group only has read and execute access.

Others also have read and execute.

1. Create a test directory called “test” and create a new file inside the directory and name it “testmask1”:
2. What are the permissions of the file testmask1  
   

The permissions for testmask 1 are rw-rw-r–

1. Change the umask:  
     
   **umask 0077  
     
   touch testmask2  
     
   ls –al**
2. Now what are the permissions of the file testmask2   
     
   [Your Answer Here]

My permissions for testmask2 are u=rwx, g=, o=

Only I have permissions to the files and directory because we just set the default permissions to mode 0700 or less .

1. What does it mean if the umask value is set to 0000?  
     
   [Your Answer Here]

This means that newly created files or directories won't have privileges revoked, it will cause all files created to be 0666 or writable.

1. When you have finished, shutdown the Linux Server with the following command:  
     
   **shutdown -h now**

**Task 4: Research questions**

1. How different is the UNIX access control architecture from that of Windows-based platforms?  
     
   [Your Answer Here]

It differs because NTFS (New Technology File System) can make it so each file can have an owner or create ACE’S (access control entries) to that folder which might be more flexible.

However Unix uses “mode bits” on each file which means a file might have an owner and also an owning group so it can be shared with more than one user.

1. How different is access control management in Windows, compared to UNIX?   
     
   [Your Answer Here]

Not that different because both do the same thing but differ the way they do it. For example windows can make files have owners but only the owners have the ability to share the folder which is considered a security aspect of it. However linux also does this because not only you can have roles to the file, you can command it who has access to the directory where the folder is located, you can only give people read which means they won't be able to edit the folder.

1. Which would you say is easier?

[Your Answer Here]

I'd say the windows ACE’S are easier to set up because in windows you can enter the name of a user that wants access to that folder and just like that they have access, however for linux, you have to know the command to give access to other users to the directory and folder.

1. Which is more efficient?   
     
   [Your Answer Here]

Linux’s ace’s are more efficient and secure because you have more flexibility to which role you want to give someone to that file and is faster to give the role than windows.

1. What is SELinux?   
     
   [Your Answer Here]

Security Enhanced Linux is an architecture that gives admins more control over who has access to the system they use, it basically holds more access control entries for admins.