CompTIA Linux+

Manage File Permissions and Ownership

Introduction

Welcome to the **Manage File Permissions and Ownership** Practice Lab. In this module you will be provided with the instructions and devices needed to develop your hands-on skills.

Permissions
Ownership
Security Maintenance

Learning Outcomes

In this module, you will complete the following exercise:

- Exercise 1 - Manage File Permissions and Ownership

After completing this lab, you will be able to:

- Manage access permissions
- Use various access modes to maintain security
- Change the umask of a file
- Manage file access to group members

Exam Objectives

The following exam objectives are covered in this lab:

- **LPI:** 104.5 Manage file permissions and ownership

- **CompTIA:** 3.1 Given a scenario, apply or acquire the appropriate user and/or group permissions and ownership.

Note: *Our main focus is to cover the practical, hands-on aspects of the exam objectives. We recommend referring to course material or a search engine to research theoretical topics in more detail.*

Lab Duration

It will take approximately **1 hour** to complete this lab.

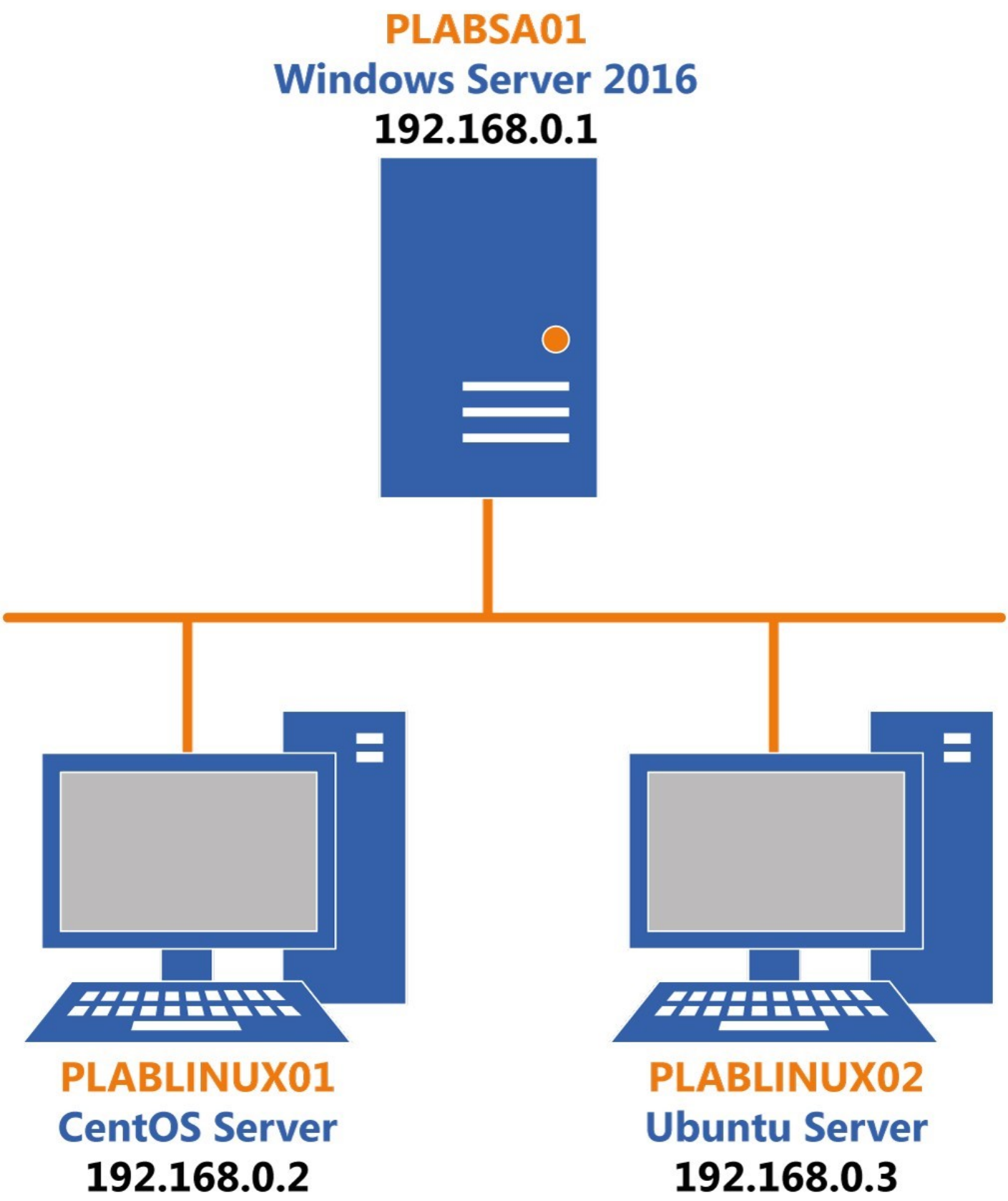
Help and Support

For more information on using Practice Labs, please see our **Help and Support** page. You can also raise a technical support ticket from this page.

Click Next to view the Lab topology used in this module.

Lab Topology

During your session, you will have access to the following lab configuration.



Depending on the exercises you may or may not use all of the devices, but they are shown here in the layout to get an overall understanding of the topology of the lab.

- **PLABSA01** (Windows Server 2016)
- **PLABLINUX01** (CentOS Server)
- **PLABLINUX02** (Ubuntu Server)

Click Next to proceed to the first exercise.

Exercise 1 - Manage File Permissions and Ownership

Each file that is created on the Linux system needs to have some type of permission. For example, the owner always has the read and write permissions. However, the owner may choose to deny any kind of permission on the respective file.

In this exercise, you will understand how to manage file permissions and ownership.

Learning Outcomes

After completing this exercise, you will be able to:

- Log into a Linux System
- Manage access permissions
- Use various access modes to maintain security
- Change the umask of a file
- Manage file access to group members

Your Devices

You will be using the following device in this lab. Please power these on now.

- **PLABLINUX01** (CentOS Server)

Task 1 - Manage Access Permissions

You can use file permissions to enable users to access a file or a directory for selective operations. For example, some users might have read rights only while other users

might have write permissions. Normally, the owner of the file has full rights - read, write, and execute - on a file. In this task, you will learn to access and change the access permissions on regular and special files as well as directories.

To manage access permissions, perform the following steps:

Step 1

On the desktop, right-click and select **Open Terminal**.

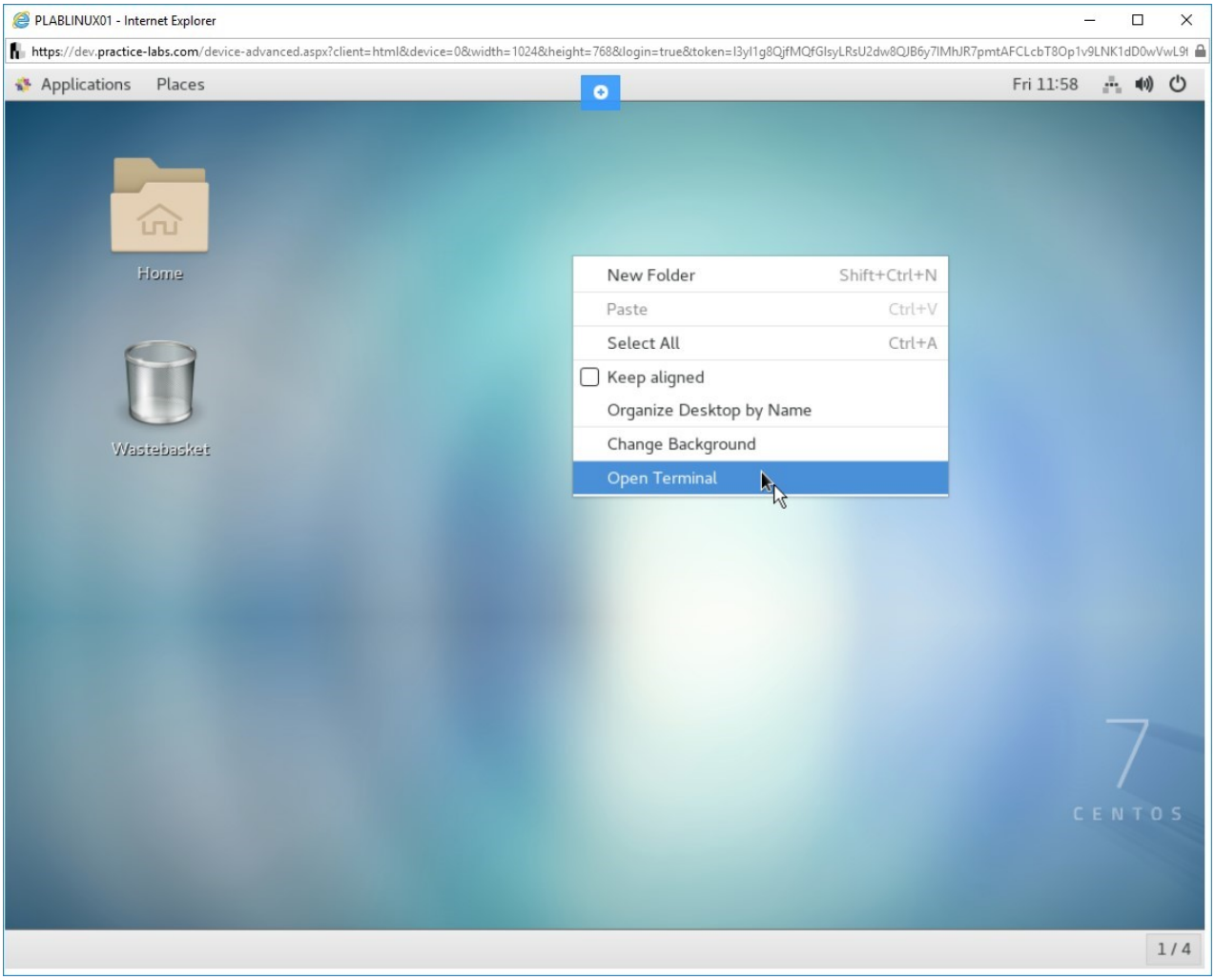


Figure 1.1 Screenshot of PLABLINUX01: Selecting the Open Terminal option from the context menu.

Step 2

The command prompt window is displayed. Type the following command:

```
su -
```

Press **Enter**.

At the **Password** prompt, type the following password:

```
Passw0rd
```

Press **Enter**.

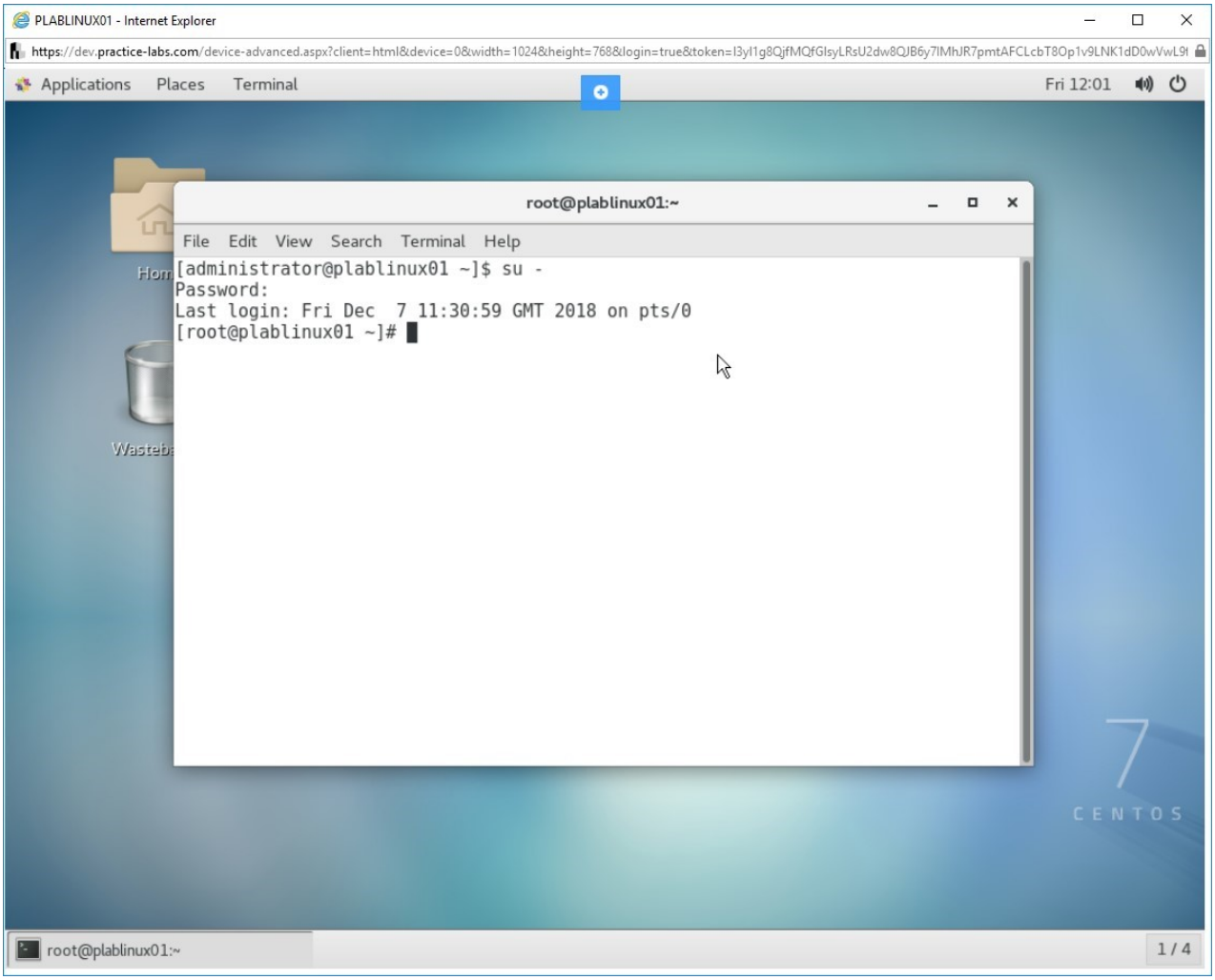


Figure 1.2 Screenshot of PLABLINUX01: Changing to the root account with the su command.

Step 3

Clear the screen by entering the following command:

```
Clear
```

***Note**: The clear command is used before every step to enable the learners to get a clear view of the output of each command. Otherwise, it is not mandatory to use the clear command before every command.*

Type the following command to change the directory:

```
cd ..
```

Press **Enter**.

To list the directories with the permissions, type the following command:

```
ls -l
```

Press **Enter**.

***Note**: The leftmost column lists the permissions on the directories listed. Permissions can be read=r, write=w and execute=x.*

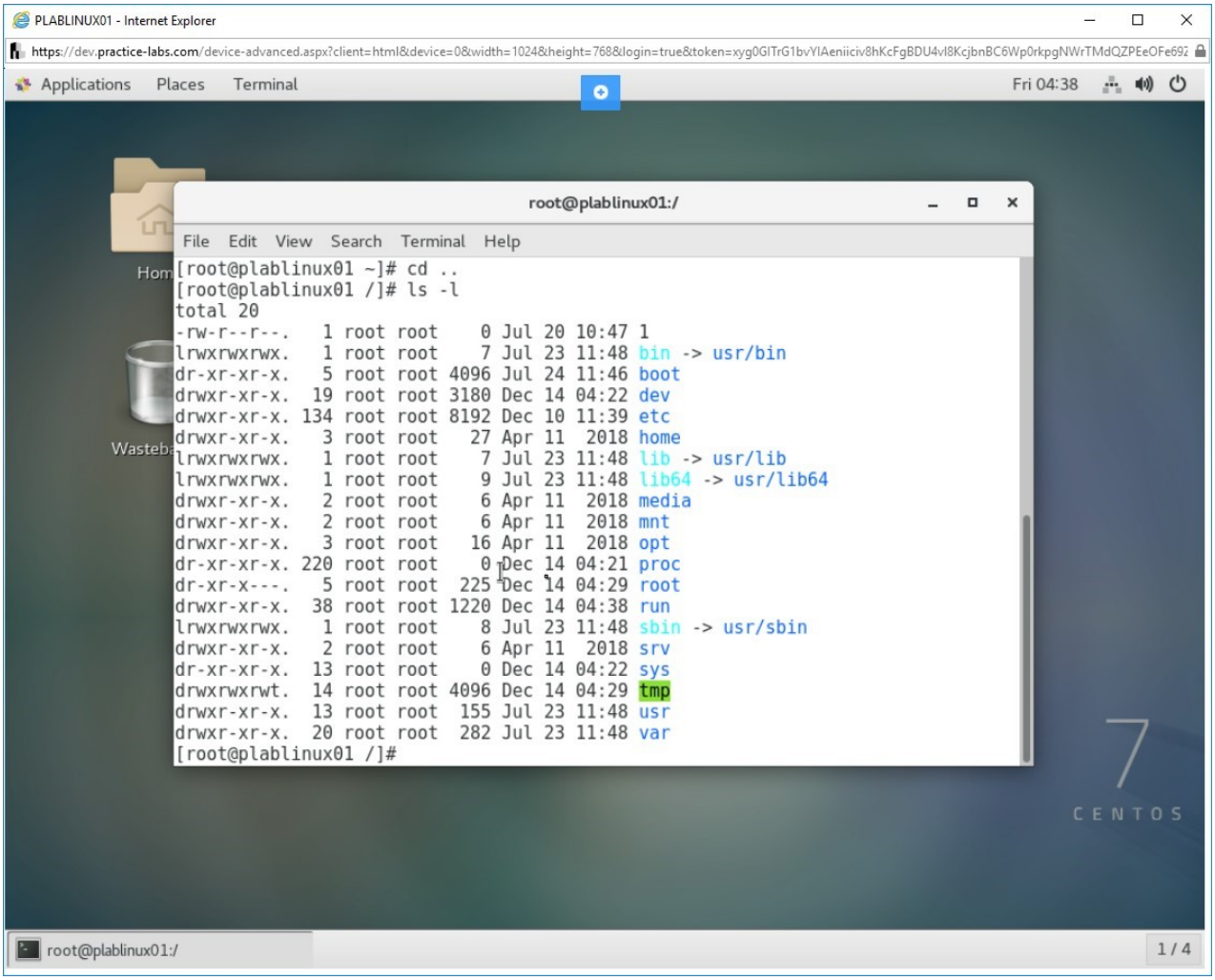


Figure 1.3 Screenshot of PLABLINUX01: Listing the directories with their permissions.

Step 4

Clear the screen by entering the following command:

```
clear
```

To change to the **/etc** directory, type the following command:

```
cd /etc
```

Press **Enter**.

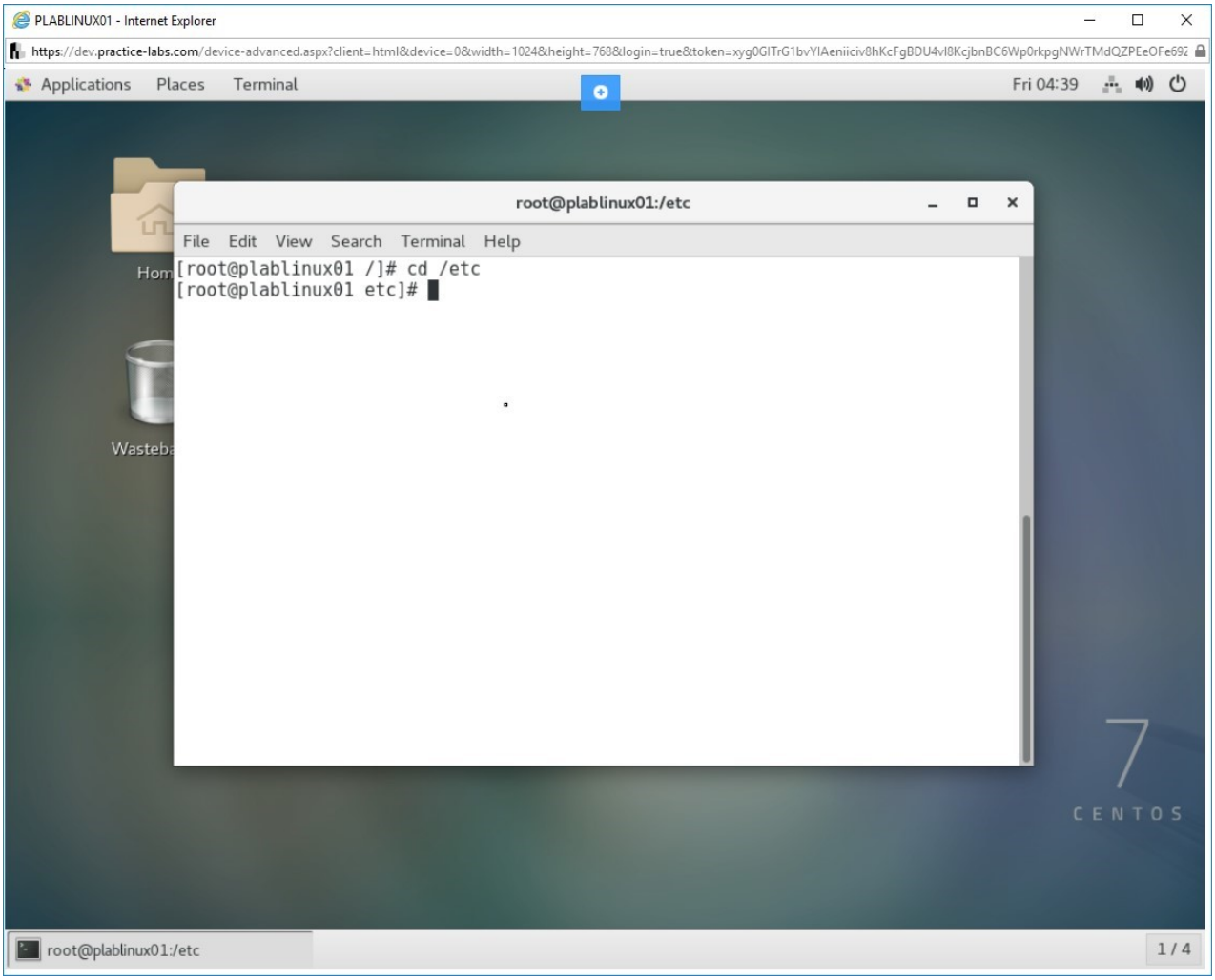


Figure 1.4 Screenshot of PLABLINUX01: Changing to the /etc directory.

Step 5

Clear the screen by entering the following command:

```
clear
```

Again, to list the directories with the permissions, type the following command:

```
ls -l
```

Press **Enter**.

Note that as a **root** user, you have read and write permissions on some of the files but not the execute permissions.

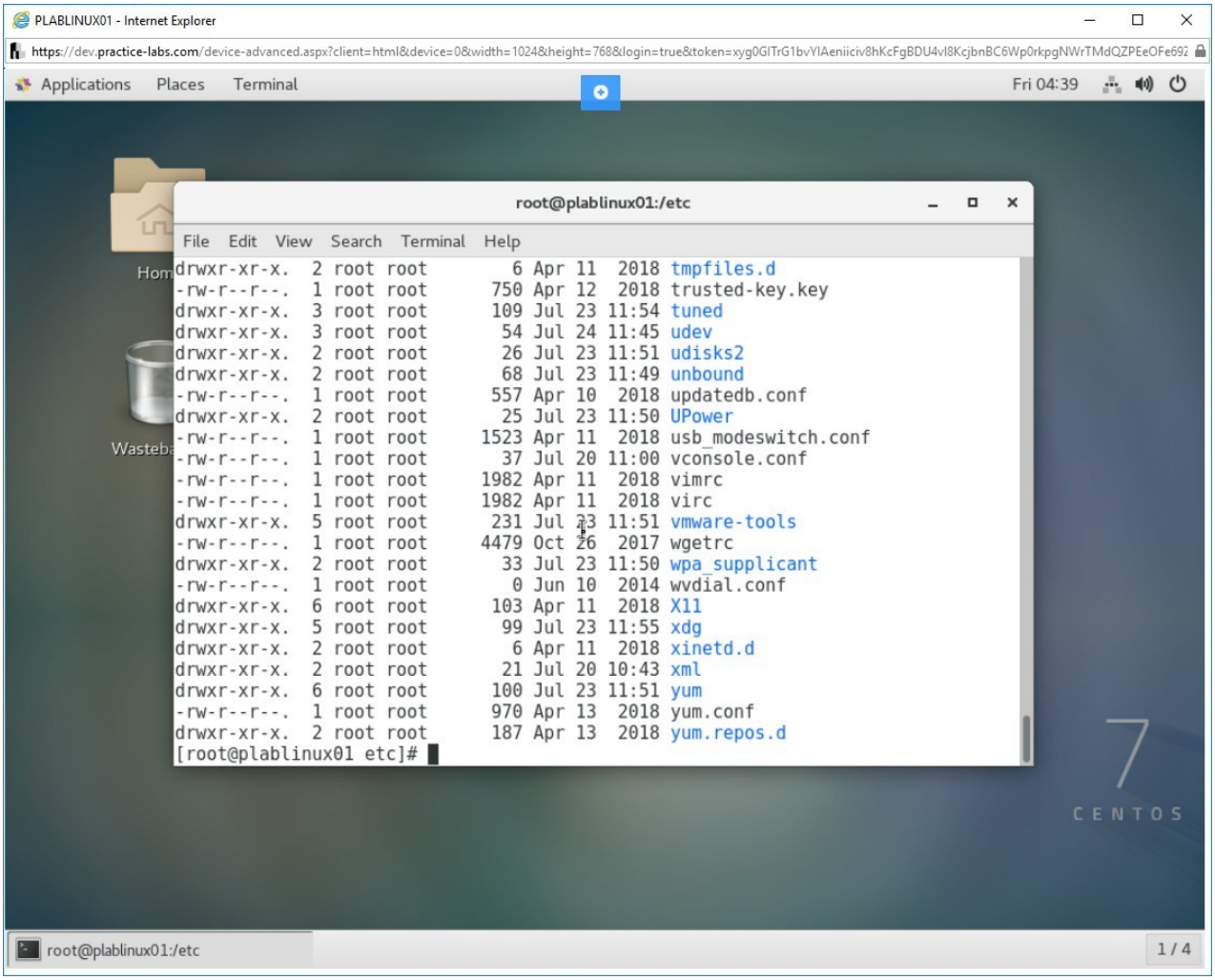


Figure 1.5 Screenshot of PLABLINUX01: Listing the files of the /etc directory.

Step 6

Clear the screen by entering the following command:

```
clear
```

Move out of the **/etc** directory to the root's home directory. Type the following command:

```
cd ~
```

Press **Enter**.

You are back to the root's home directory.

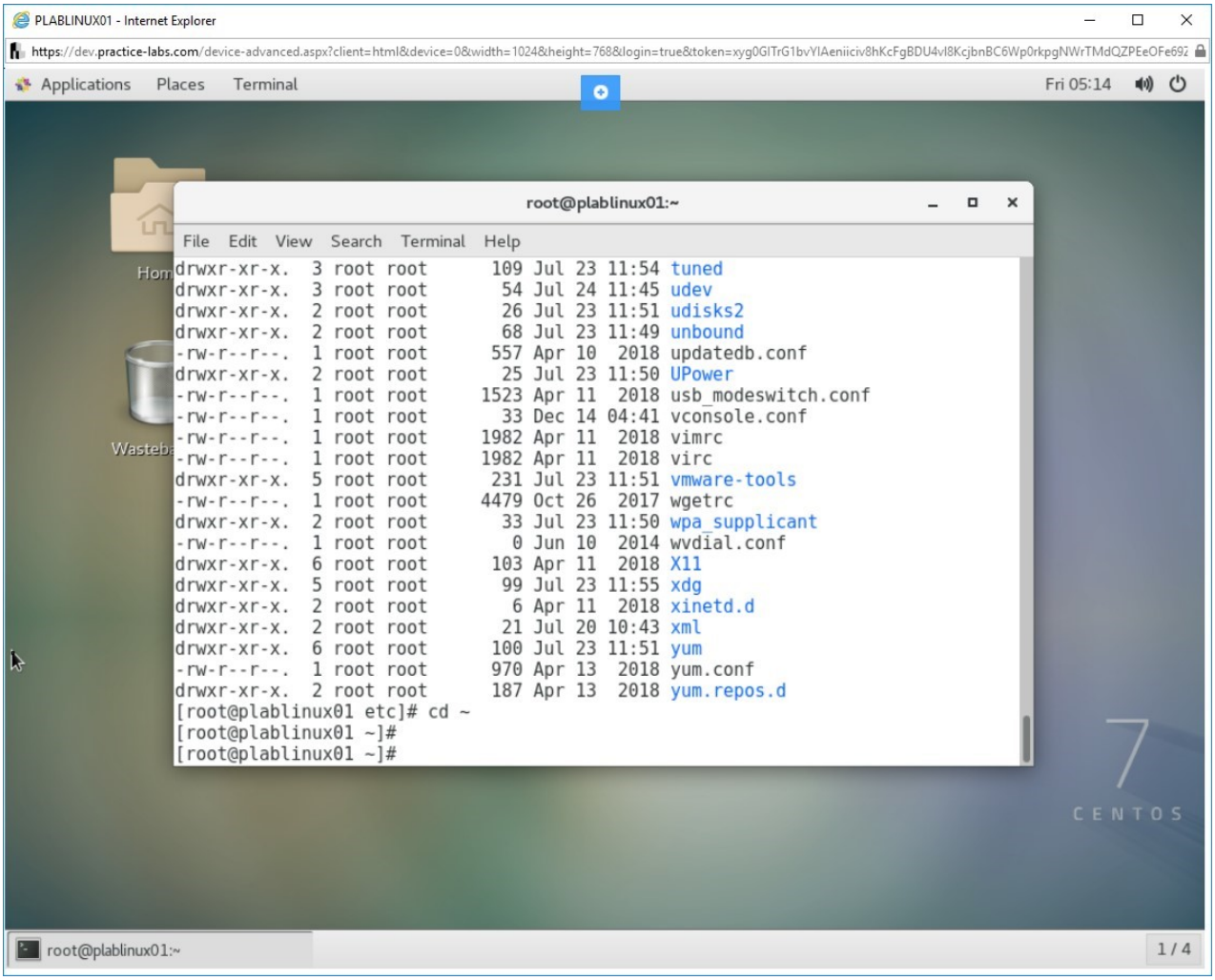


Figure 1.6 Screenshot of PLABLINUX01: Navigating back to the root's home directory.

Step 7

Clear the screen by entering the following command:

```
clear
```

You can also view the permissions for a specific file. To do that, type the following command:

```
ls -l anaconda-ks.cfg
```

Press **Enter**.

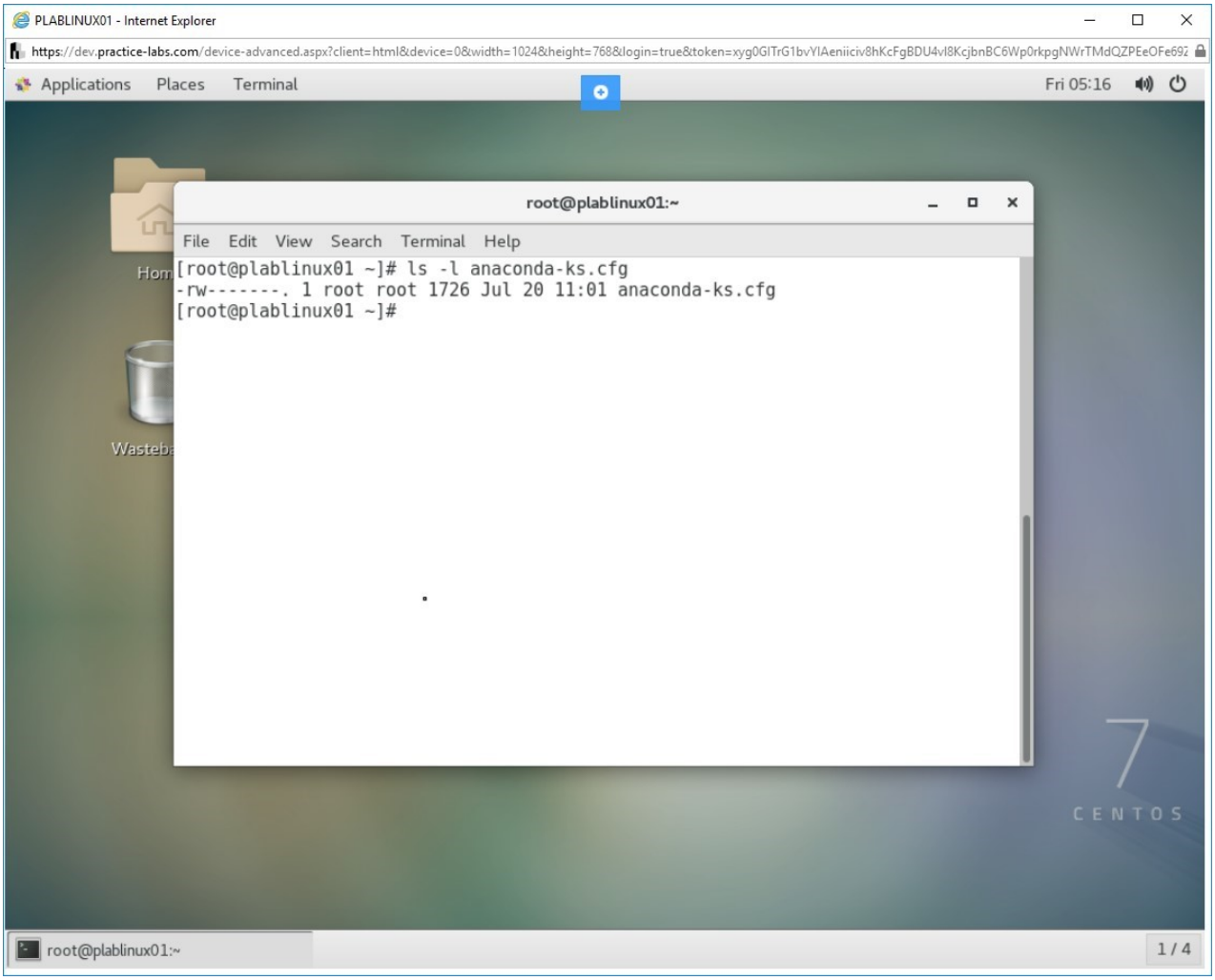


Figure 1.7 Screenshot of PLABLINUX01: Listing the permissions of the anaconda-ks.cfg file.

Step 8

You can also view the permissions for the system directories. When you view the permissions, the permissions are listed for the following: user, group, and others.

To view the files or directory permissions, you need to use the ls -l command. It provides a detailed permissions list for the mentioned directory or file name. For example, to view the permissions for /etc/hosts, type the following command:

```
ls -l /etc/hosts
```

Press **Enter**.

The permissions are listed.

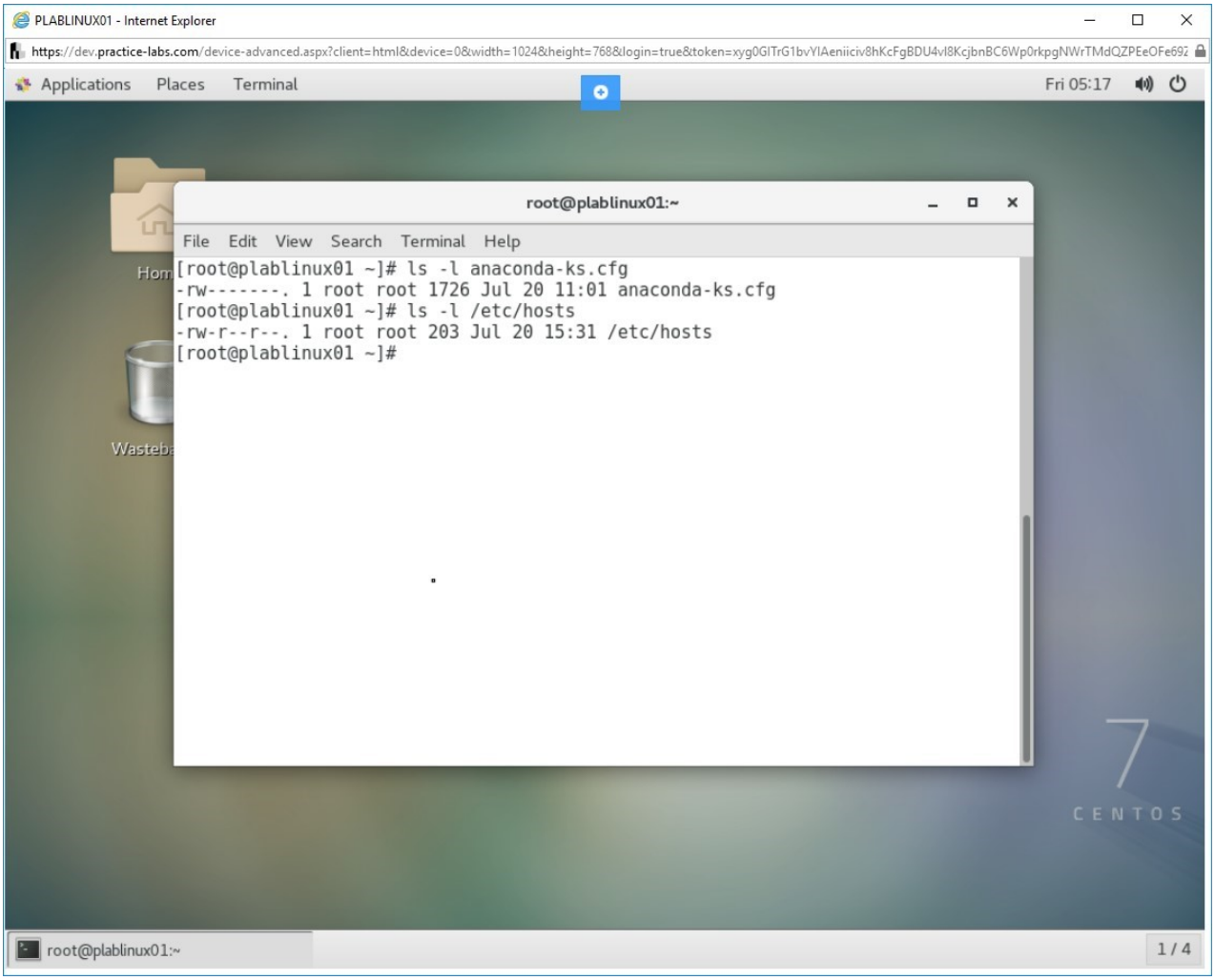


Figure 1.8 Screenshot of PLABLINUX01: Listing the permissions of the /etc/hosts file.

Task 2 - Use Various Access Modes to Maintain Security

In this task, you will use commands such as suid, sgid and the sticky bit to maintain the access permissions and manage the runlevels of files.

To use various access modes to maintain security, perform the following steps:

Step 1

To view the **SUID** for the **passwd** file, type the following command:

```
ls -l $(which passwd)
```

Press **Enter**.

The SUID for the passwd file is displayed.

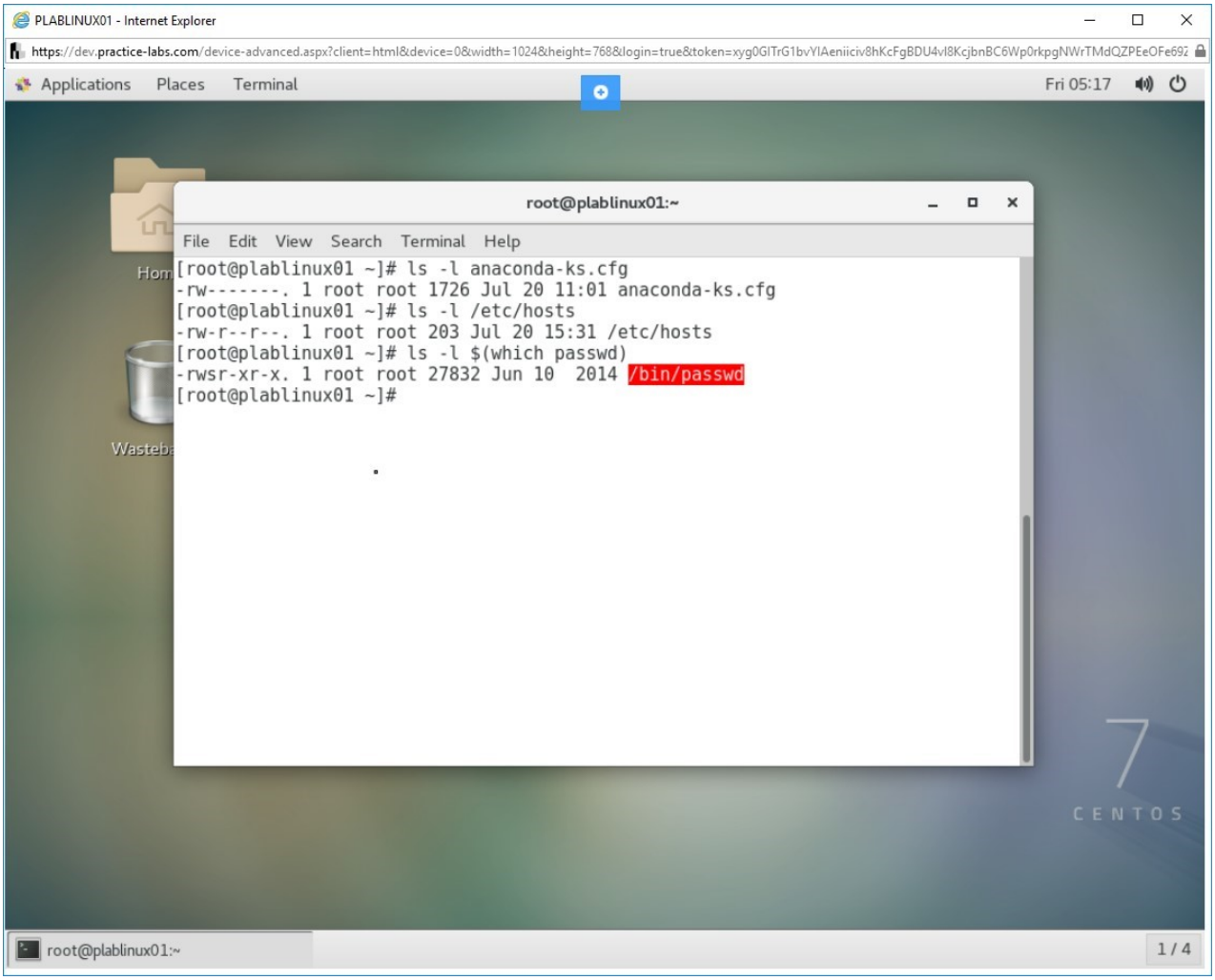


Figure 1.9 Screenshot of PLABLINUX01: Viewing the SUID for the passwd file.

Step 2

Note that the system displays the symbolic value, which is **s** for **/bin/passwd**. The stat command also displays values like when last accessed, modified, or changed. To view the numerical value, type the following command:

```
stat /bin/passwd
```

Press **Enter**.

The complete details for the /bin/passwd file are displayed.

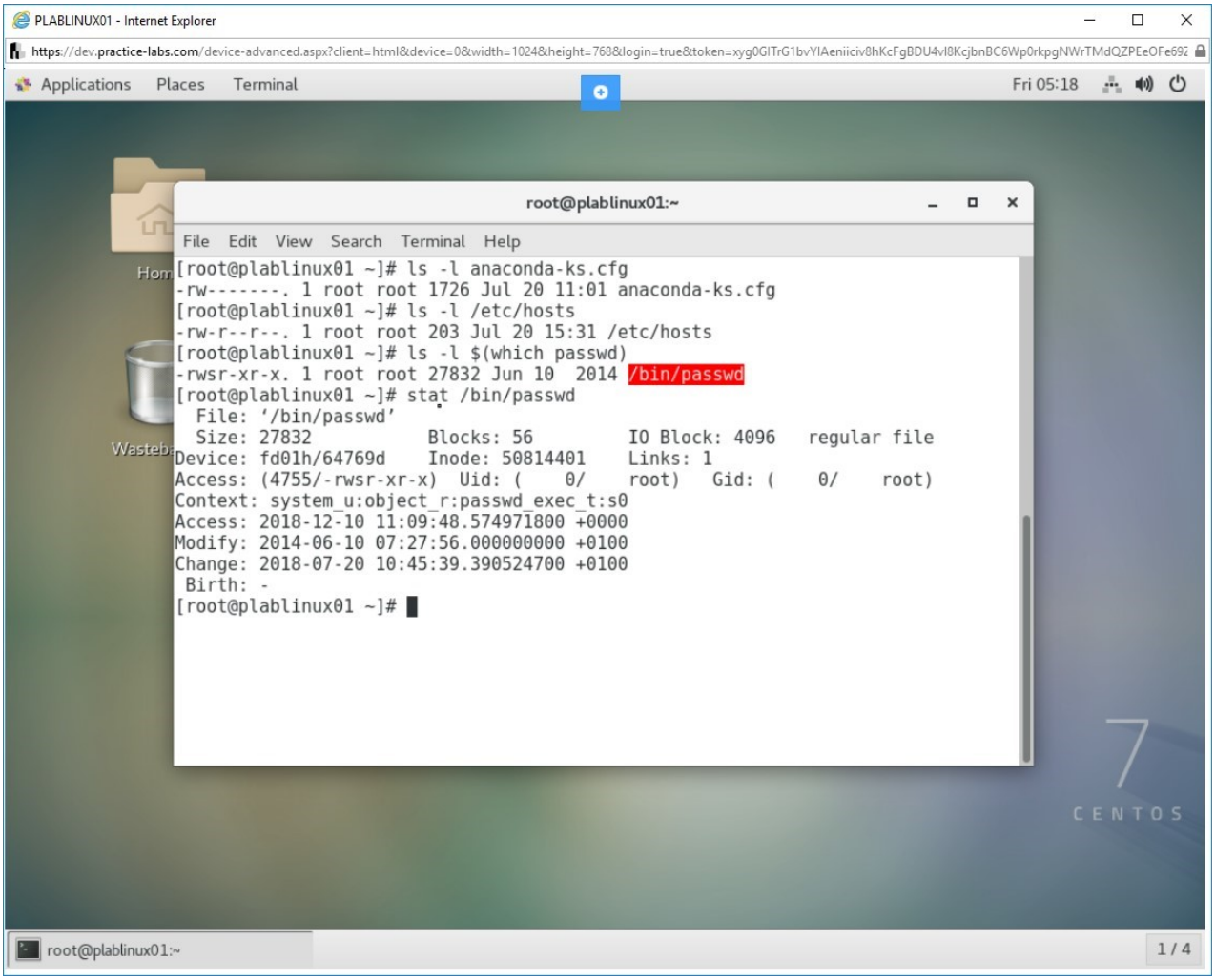


Figure 1.10 Screenshot of PLABLINUX01: Viewing the numerical values for the /etc/passwd file.

Step 3

Clear the screen by entering the following command:

```
clear
```

SGID can be used to change the group ownership. To view the **SGID** for the **anaconda-ks.cfg** file, type the following command:

```
chmod 2755 anaconda-ks.cfg
```

Press **Enter**.

With the **SGID**, you have changed the group ownership for the **anaconda-ks.cfg** file.

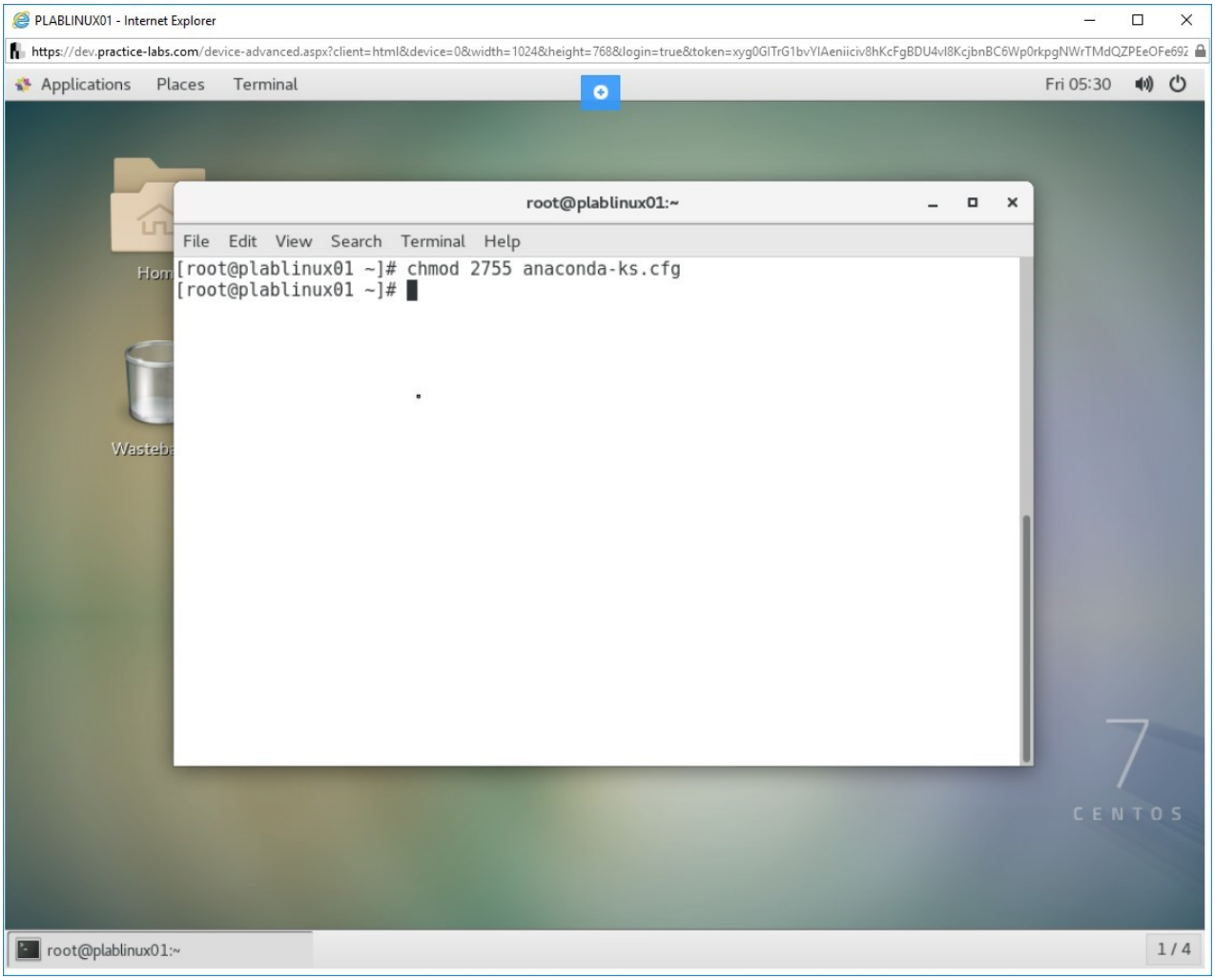


Figure 1.11 Screenshot of PLABLINUX01: Viewing the SGID for the anaconda-ks.cfg file.

Step 4

To view the current permissions on the **root** directory, type the following command:

```
ls -l
```

Press **Enter**.

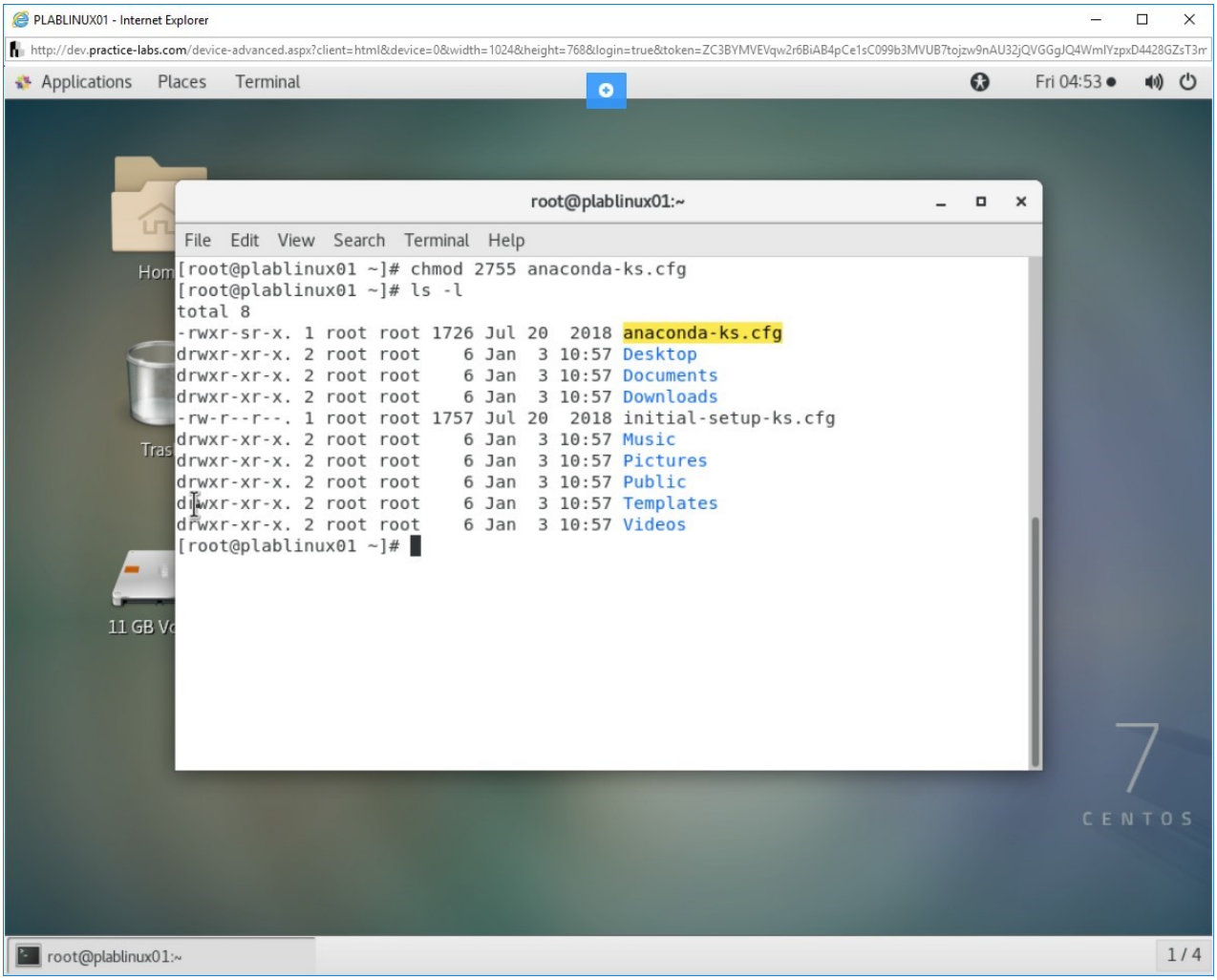


Figure 1.12 Screenshot of PLABLINUX01: Viewing the current permissions using the ls -l command.

Step 5

Clear the screen by entering the following command:

```
clear
```

The sticky bit is represented by **t**. This restricts the users other than owner or root to control the file on which sticky bit has been set.

To create a file, type the following command:

```
touch test1.txt
```

Press **Enter**.

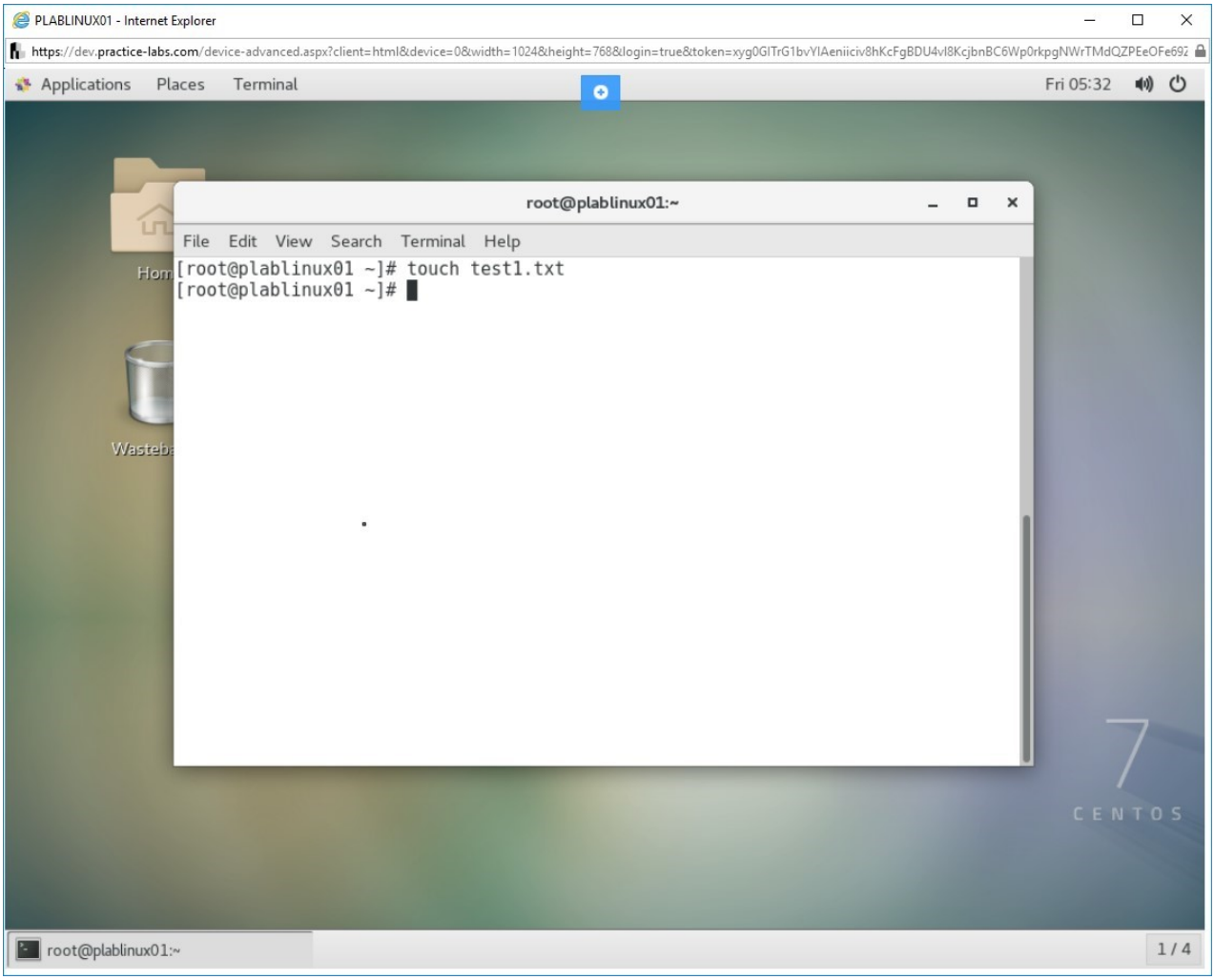


Figure 1.13 Screenshot of PLABLINUX01: Creating the test1.txt file using the touch command.

Step 6

To verify that the permissions have been changed, type the following command:

```
ls -l test1.txt
```

Press **Enter**.

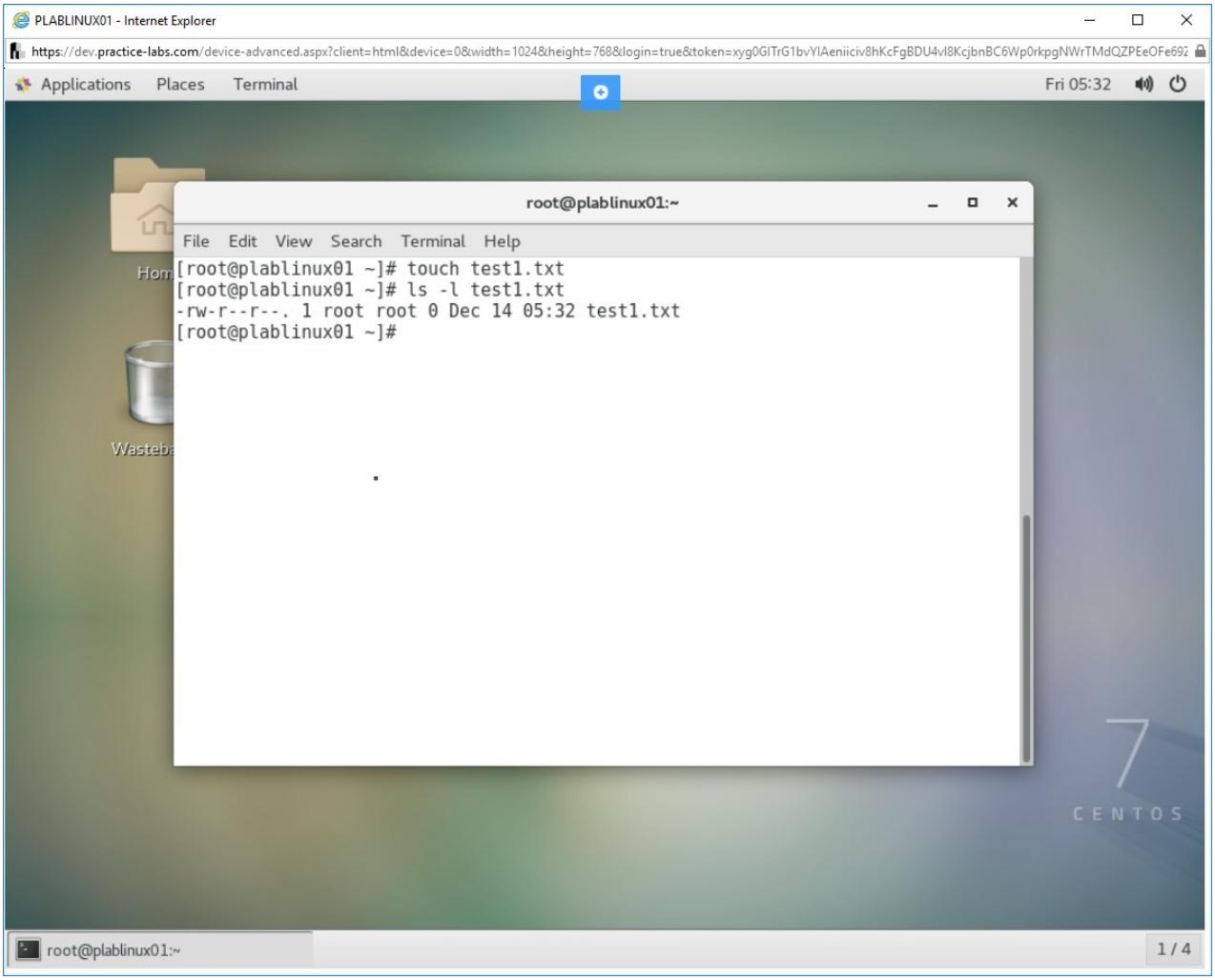


Figure 1.14 Screenshot of PLABLINUX01: Verifying the changed permissions.

Task 3 - Change the Umask of a File

Each permission has an octal value:

- Symbolic: read
- Octal: 4

- Symbolic: write
- Octal: 2

- Symbolic: execute
- Octal: 1

- Standard permission for files is 666 or -rw-rw-rw-
- Standard permission for directories is 777 or -rwxrwxrwx

Notice that the number **666**, which is an addition of the octal values of read and write permission. Similarly, 777 includes an octal **1** added for the execute permission. In this task, you will list and then change the umask of a file.

To change the umask value of a file, perform the following steps:

Step 1

Clear the screen by entering the following command:

```
clear
```

To check the **umask** for a specific directory, type the following command:

```
umask
```

Press **Enter**.

The umask for the current directory is displayed.

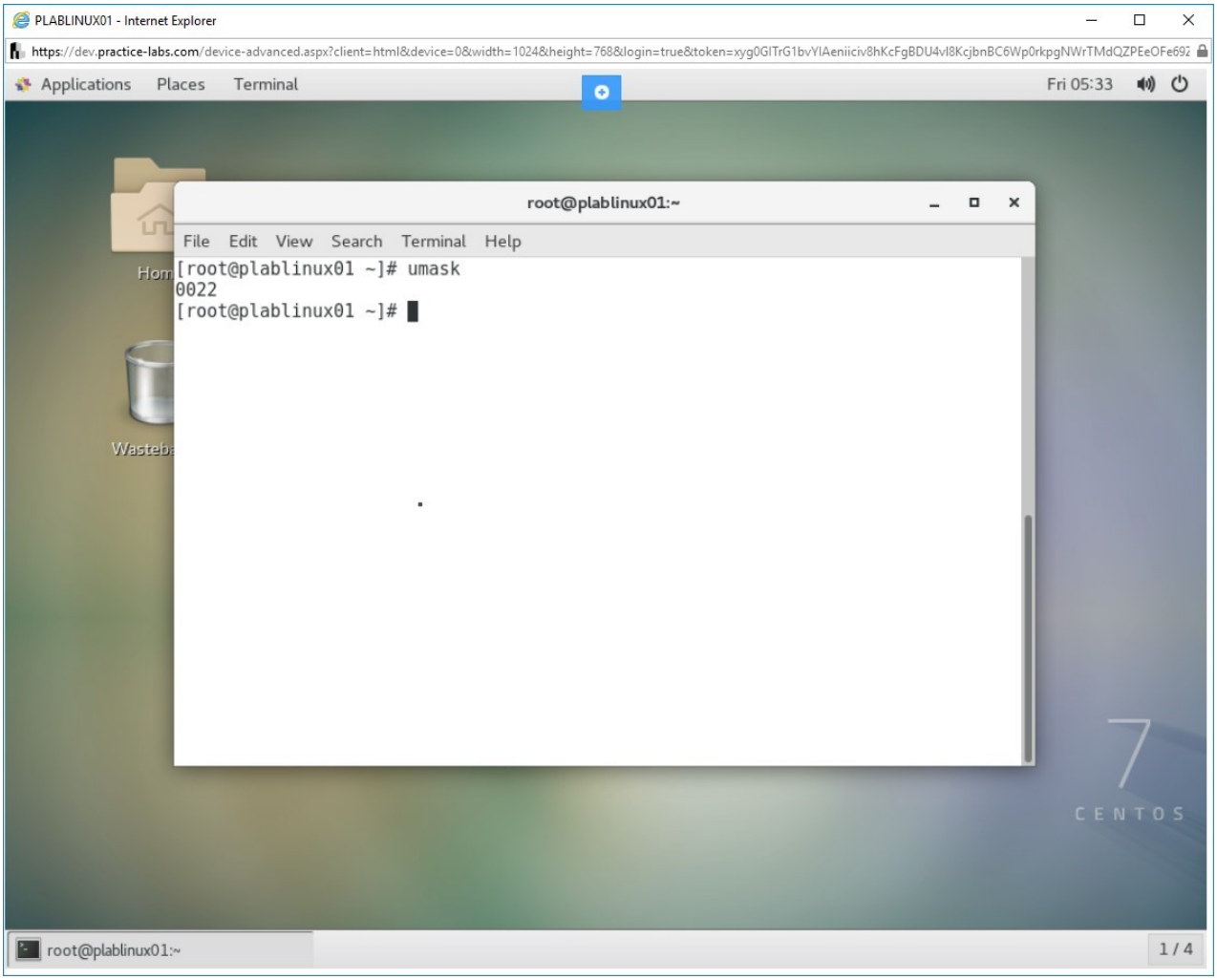


Figure 1.15 Screenshot of PLABLINUX01: Checking the umask for a specific directory.

Step 2

To change the **umask** for the directory, type the following command:

```
umask 666
```

Press **Enter**.

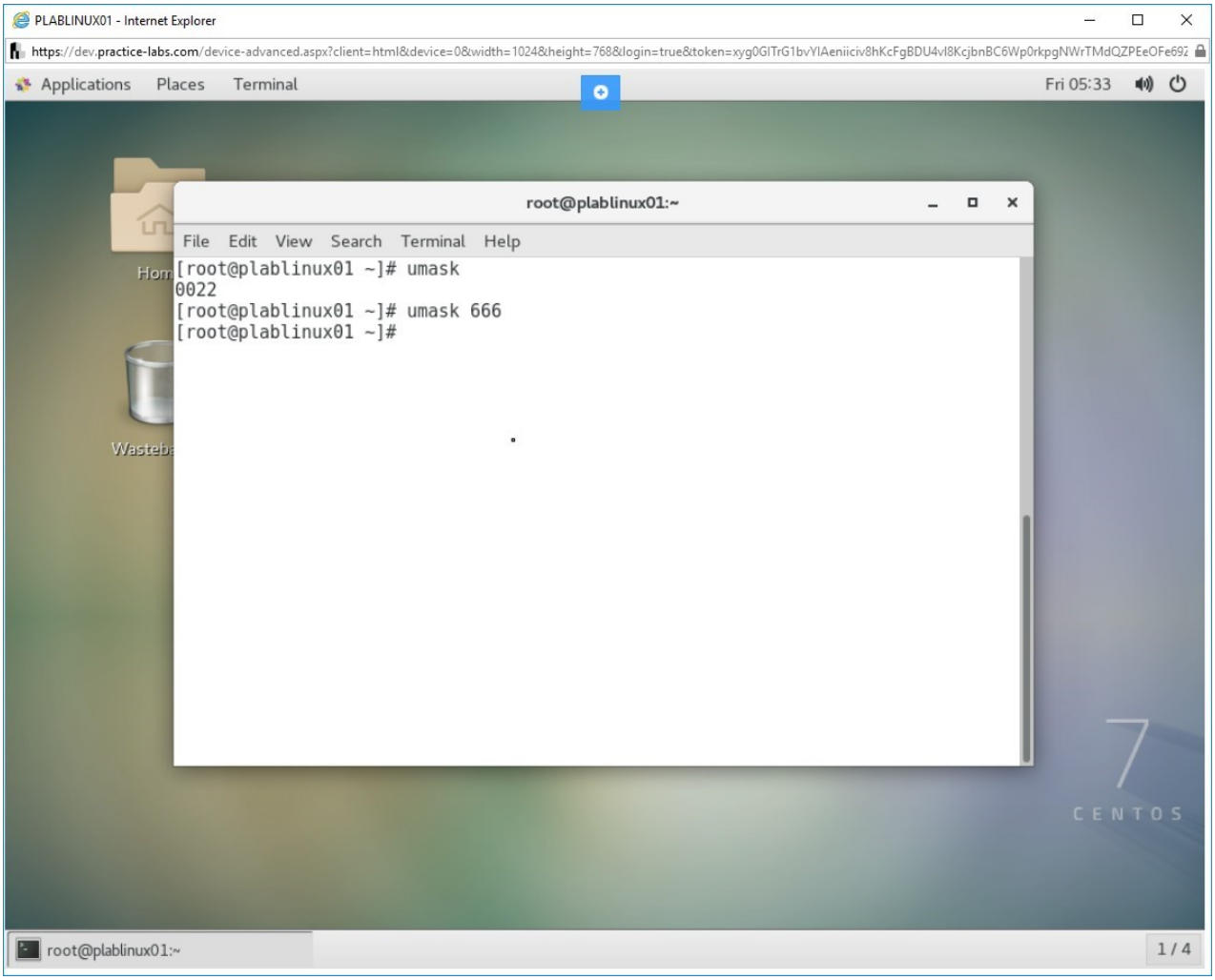


Figure 1.16 Screenshot of PLABLINUX01: Changing the umask for the directory.

Step 3

To verify that the umask is changed, type the following command:

```
umask
```

Press **Enter**.

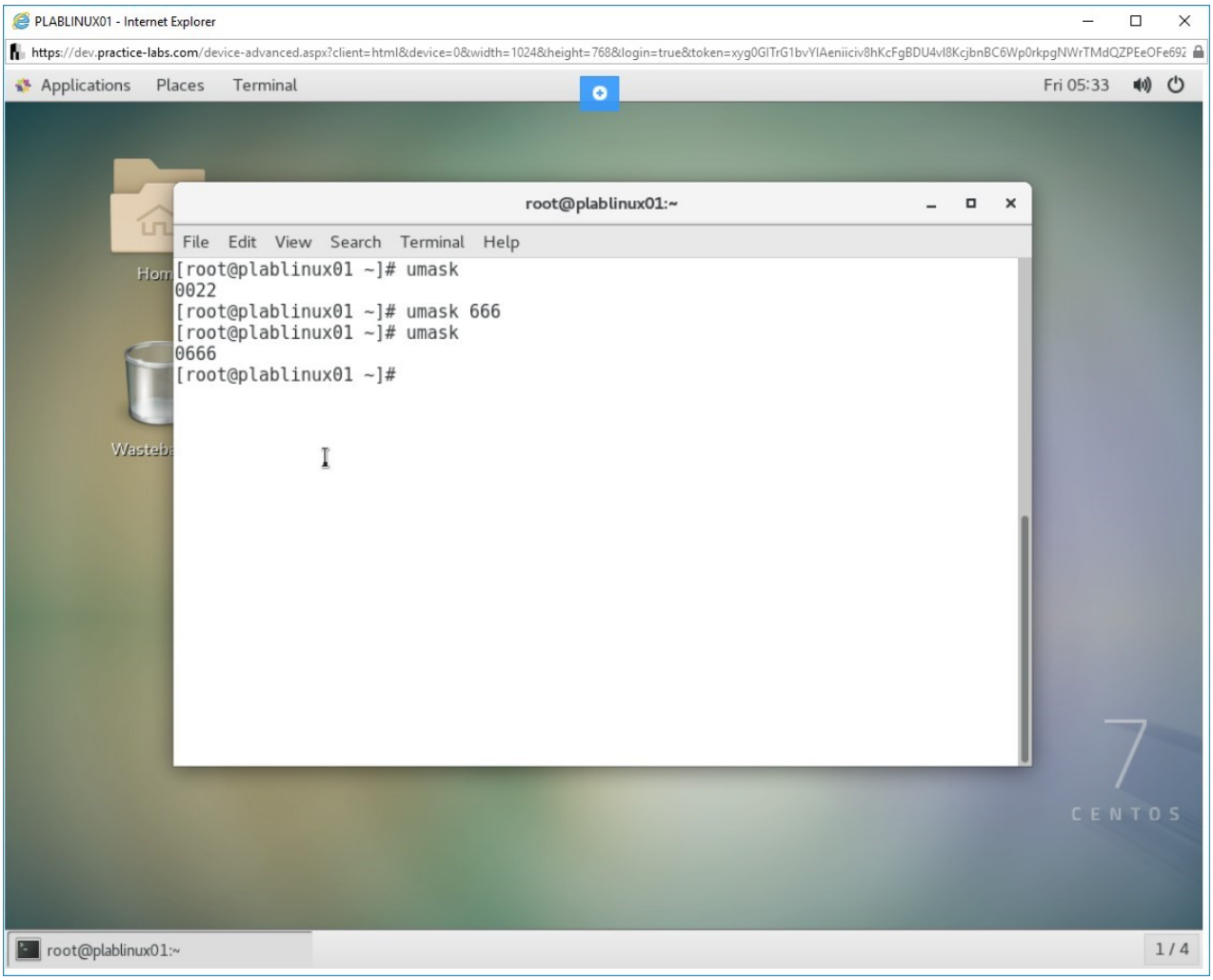


Figure 1.17 Screenshot of PLABLINUX01: Verifying the changed umask for the directory

Task 4 - Manage File Access to Group Members

Rather than assigning individual permissions to each user, you can issue a single command, using the group field, to grant file access to all the group members. In this task, you will use the **ch** command to manage the file access permission for various members of a group.

To manage file access to group members, perform the following steps:

Step 1

Clear the screen by entering the following command:

```
clear
```

Let's first create two files: **file1.txt** and **file2.txt**. To create the files, type the following commands:

```
touch file1.txt file2.txt
```

Press **Enter**.

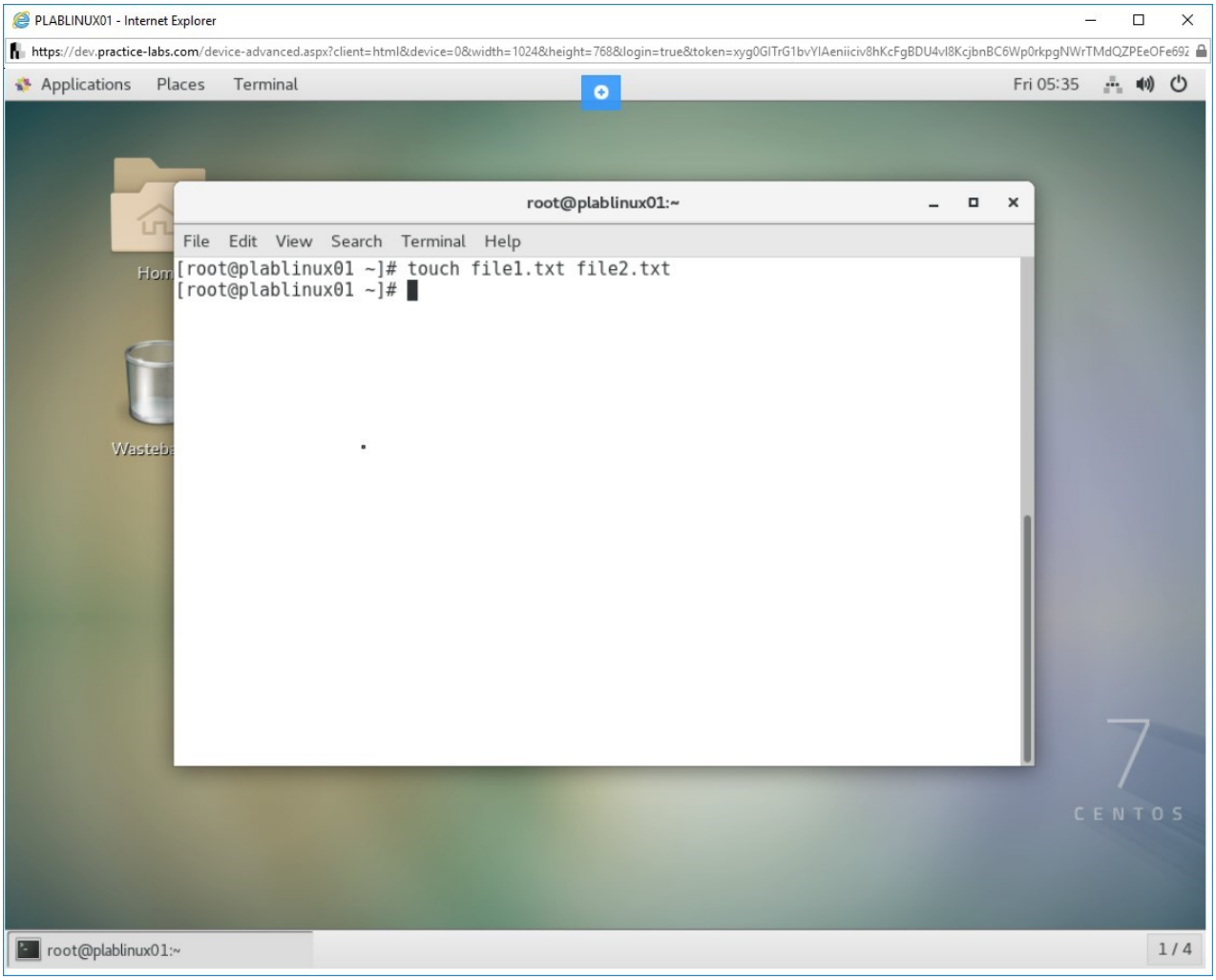


Figure 1.18 Screenshot of PLABLINUX01: Creating text files using the touch command.

Step 2

To verify that the files have been created, type the following command:

```
ls -l
```

Press **Enter**.

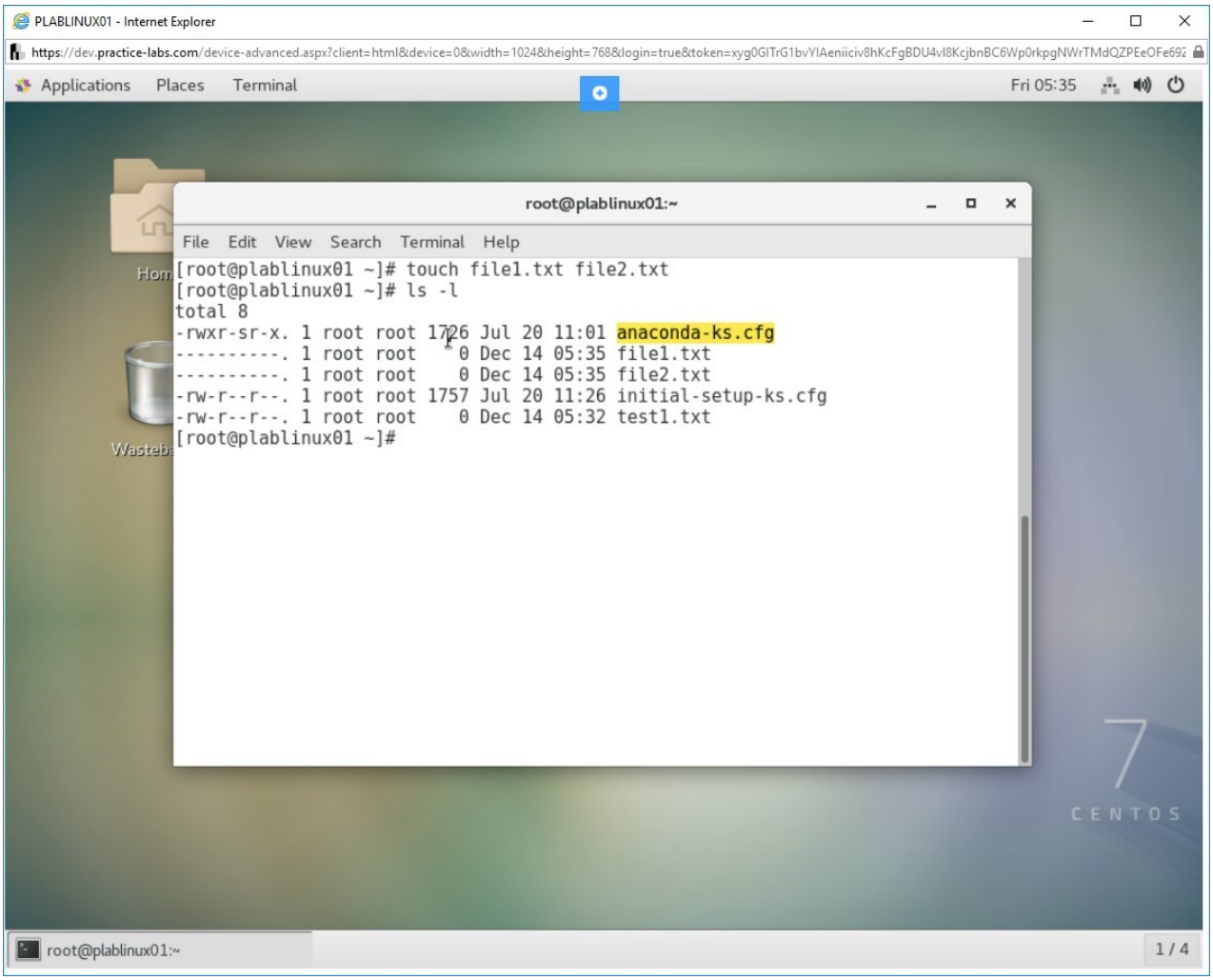


Figure 1.19 Screenshot of PLABLINUX01: Listing the files after creating them.

Step 3

To change the group ownership for **file1.txt**, type the following command:

```
chgrp adm file1.txt
```

Press **Enter**.

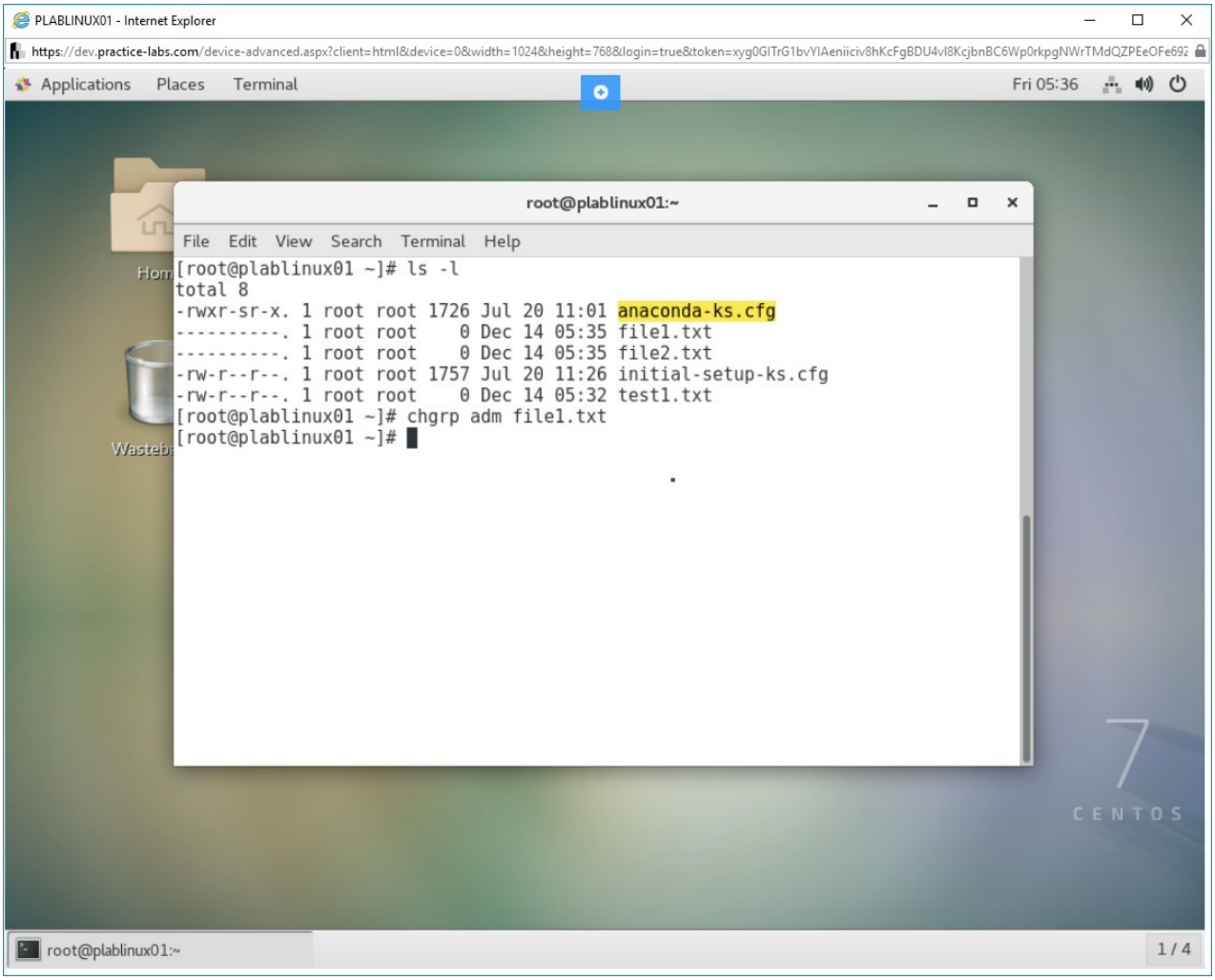


Figure 1.20 Screenshot of PLABLINUX01: Changing the group ownership for file1.txt.

Step 4

To verify that the group ownership is changed, type the following command:

```
ls -l
```

Press **Enter**.

Note that adm group is now listed for **file1.txt**.

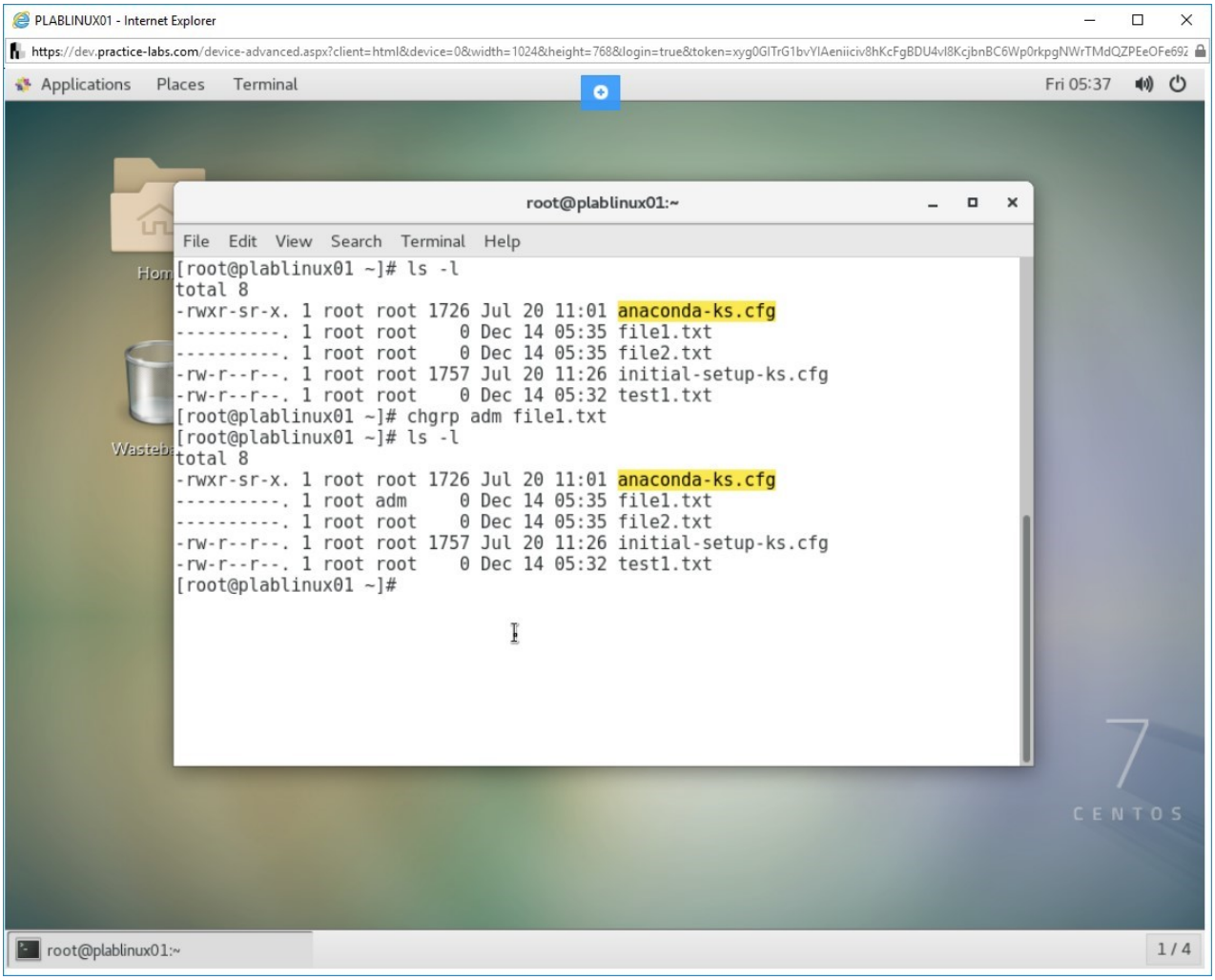


Figure 1.21 Screenshot of PLABLINUX01: Verifying that the group ownership is changed.

Step 5

Clear the screen by entering the following command:

```
clear
```

You can also change the ownership of a file. To change the ownership, type the following commands:

```
chown root file1.txt
```

Press **Enter**.

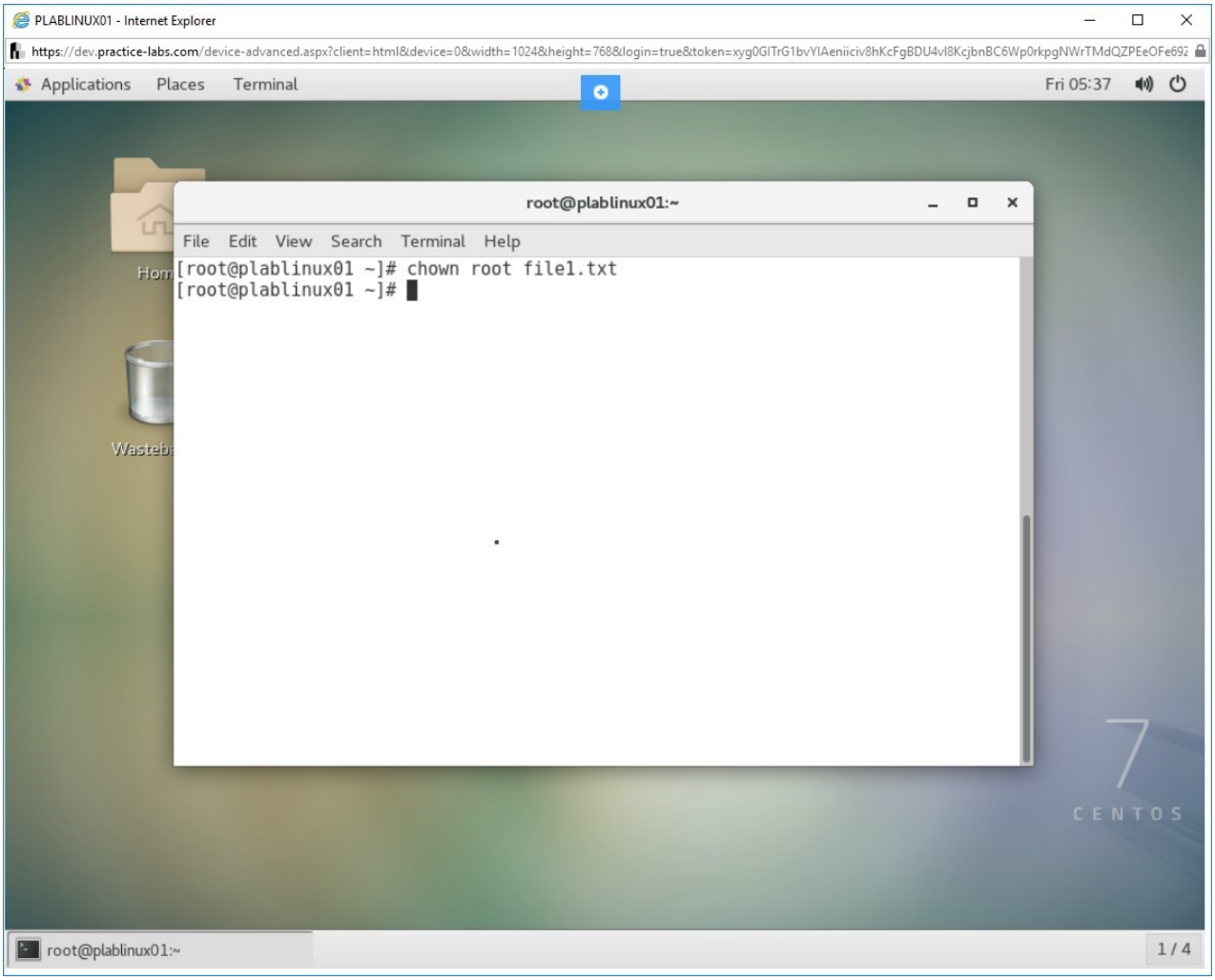


Figure 1.22 Screenshot of PLABLINUX01: Changing the ownership for the file1.txt file.

Step 6

Now, list the files to verify whether the ownership is changed. To verify the ownership, type the following command:

```
ls -l
```

Press **Enter**.

Note that the ownership is now changed to root user.

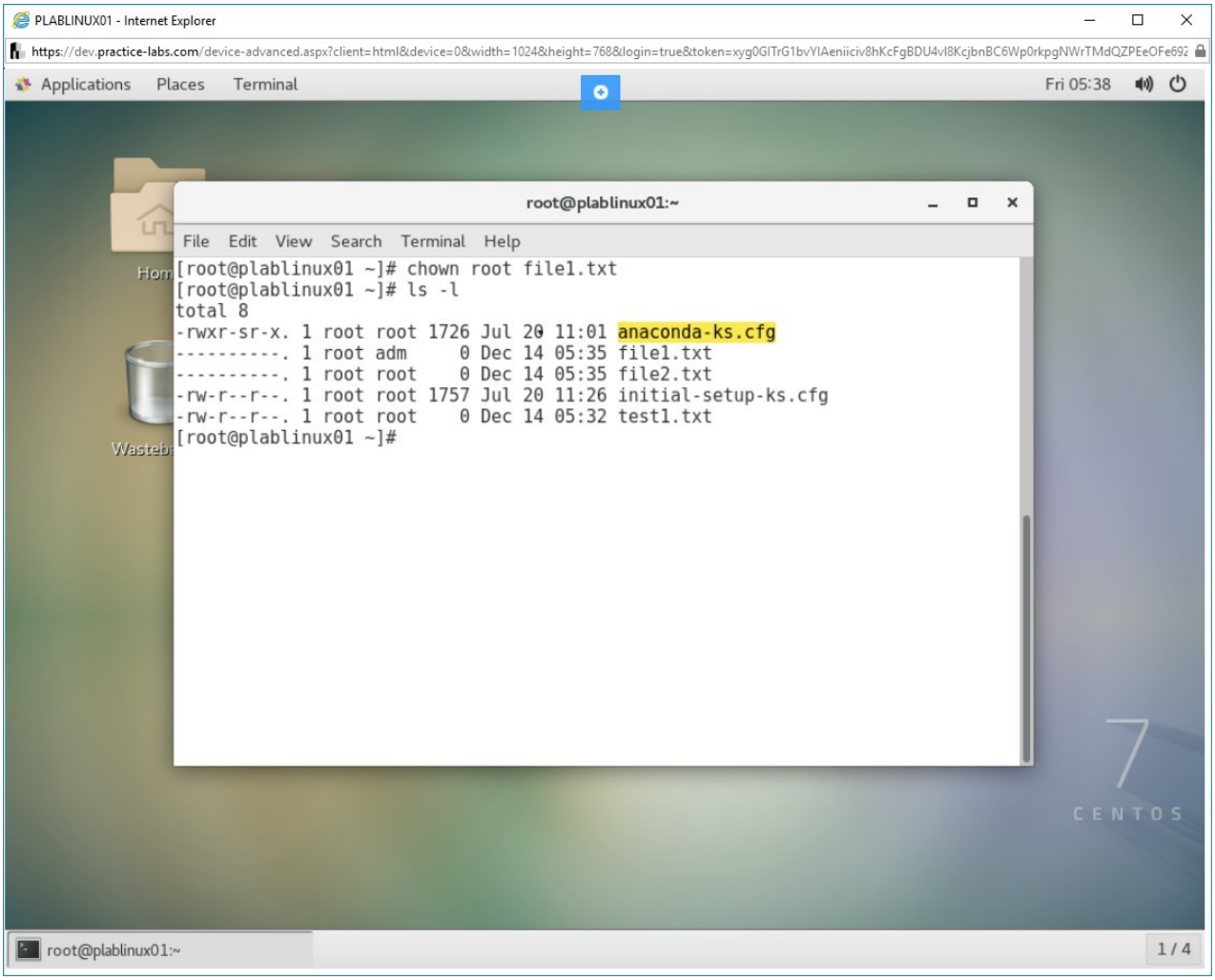


Figure 1.23 Screenshot of PLABLINUX01: Verifying whether the ownership of the file has changed.

Keep all devices in their current state and proceed to the next exercise.

Review

Well done, you have completed the **Manage File Permissions and Ownership** Practice Lab.

Summary

You completed the following exercise:

- Exercise 1 - Manage File Permissions and Ownership

You should now be able to:

- Manage access permissions
- Use various access modes to maintain security
- Change the umask of a file
- Manage file access to group members

Feedback

Shutdown all virtual machines used in this lab. Alternatively, you can log out of the lab platform.