CompTIA Linux+

Managing User and Group Accounts and Related System Files

Introduction

Welcome to the **Managing User and Group Accounts and Related System Files** Practice Lab. In this module you will be provided with the instructions and devices needed to develop your hands-on skills.

Group Accounts
System Files
Linux

Learning Outcomes

In this module, you will complete the following exercise:

- Exercise 1 - Manage User and Group Accounts and Related System Files

After completing this lab, you will be able to:

- Add, modify, and remove users and groups
- Access User/group password info
- Create and manage special purpose and limited accounts

Exam Objectives

The following exam objectives are covered in this lab:

- **LPI:** 107.1 Manage user and group accounts and related system files
- **LPI:** 110.1 Perform security administration tasks
- **CompTIA:** 2.2 Given a scenario, manage users and groups.

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.

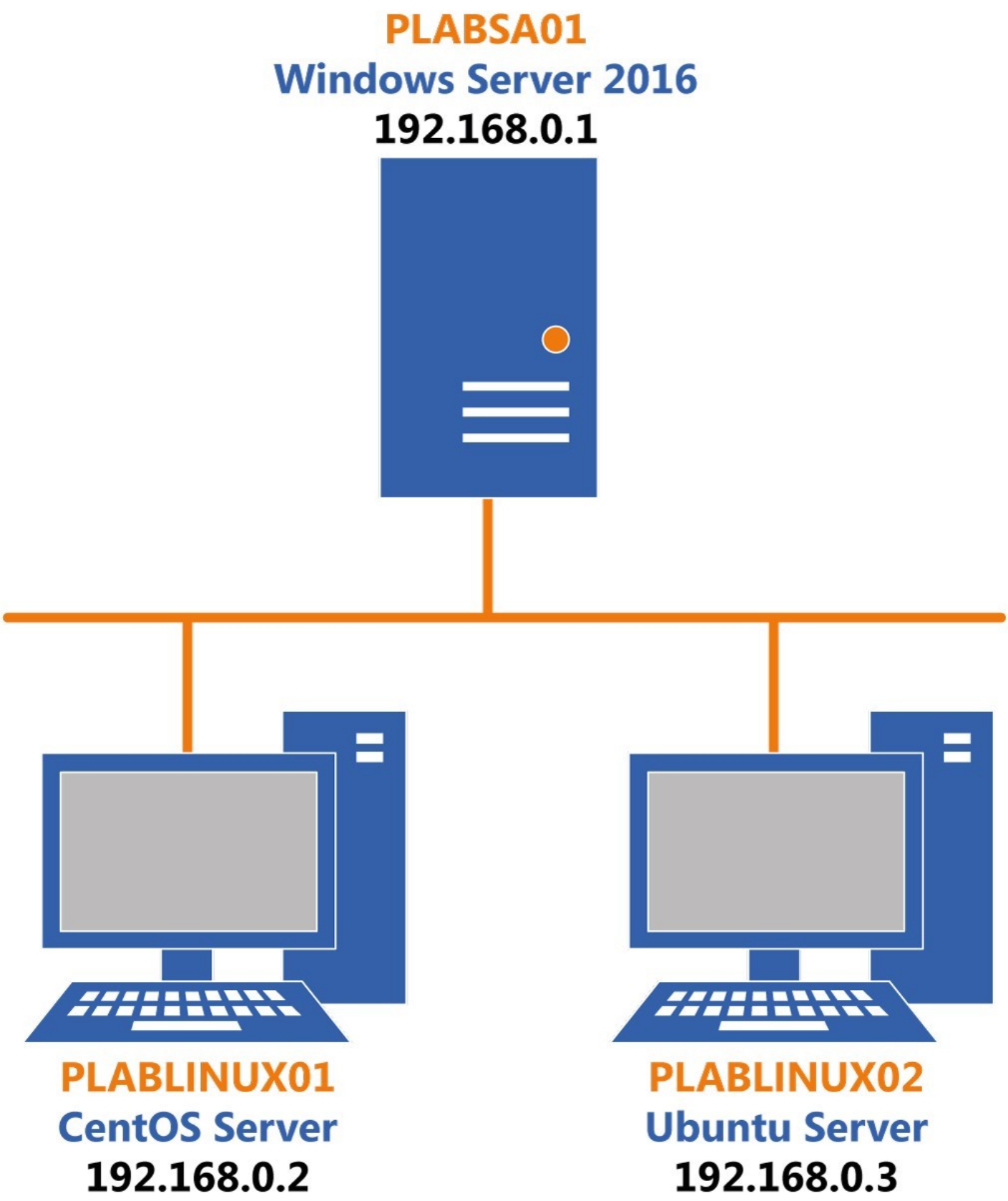
Help and Support

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 User and Group Accounts and Related System Files

Just like any other operating system, the Linux operating system can also contain user and group accounts. You can use these user and group accounts for various purposes.

In this exercise, you will understand how to manage user and group accounts and related system files.

Learning Outcomes

After completing this exercise, you will be able to:

- Log into a Linux System
- Add, modify, and remove users and groups
- Access User/group password info
- Create and manage special purpose and limited accounts

Your Devices

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

- **PLABLINUX01** (CentOS Server)

Task 1 - Add, Modify, and Remove Users and Groups

While creating users on a Linux system, root is typically the first user, and then you can create more users as required. Another entity on multiuser OS is groups. Groups comprise of multiple users. Groups are created to ease out the management of

multiple users of similar privileges. All the users in a group can be granted permissions by assigning the same to the group. This saves the tedious task of assigning permissions to individual users.

To add, modify, and remove users and groups, perform the following steps:

Step 1

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

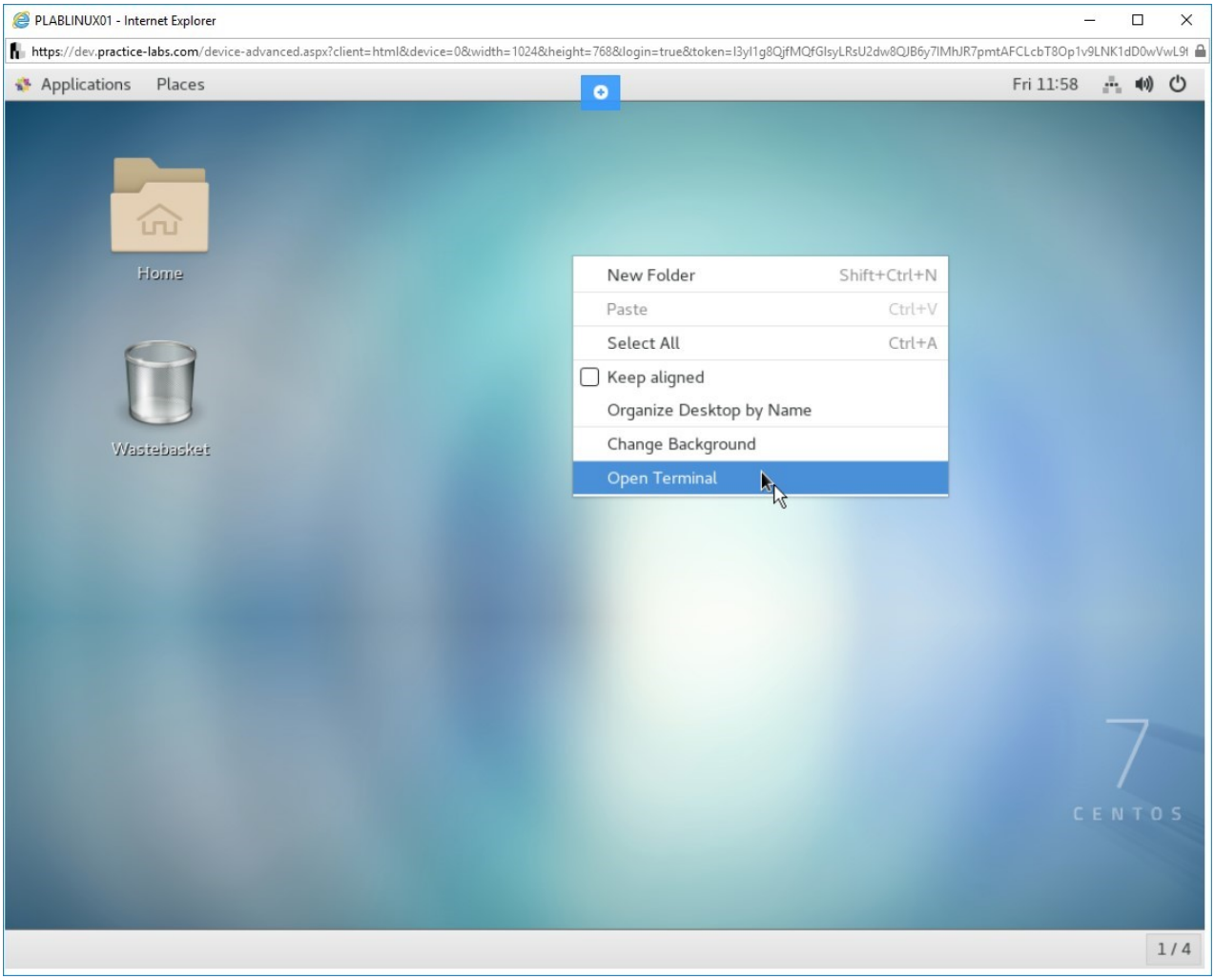


Figure 1.1 Screenshot of PLABLINUX01: Selecting the Open Terminal option from the context menu.

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**.

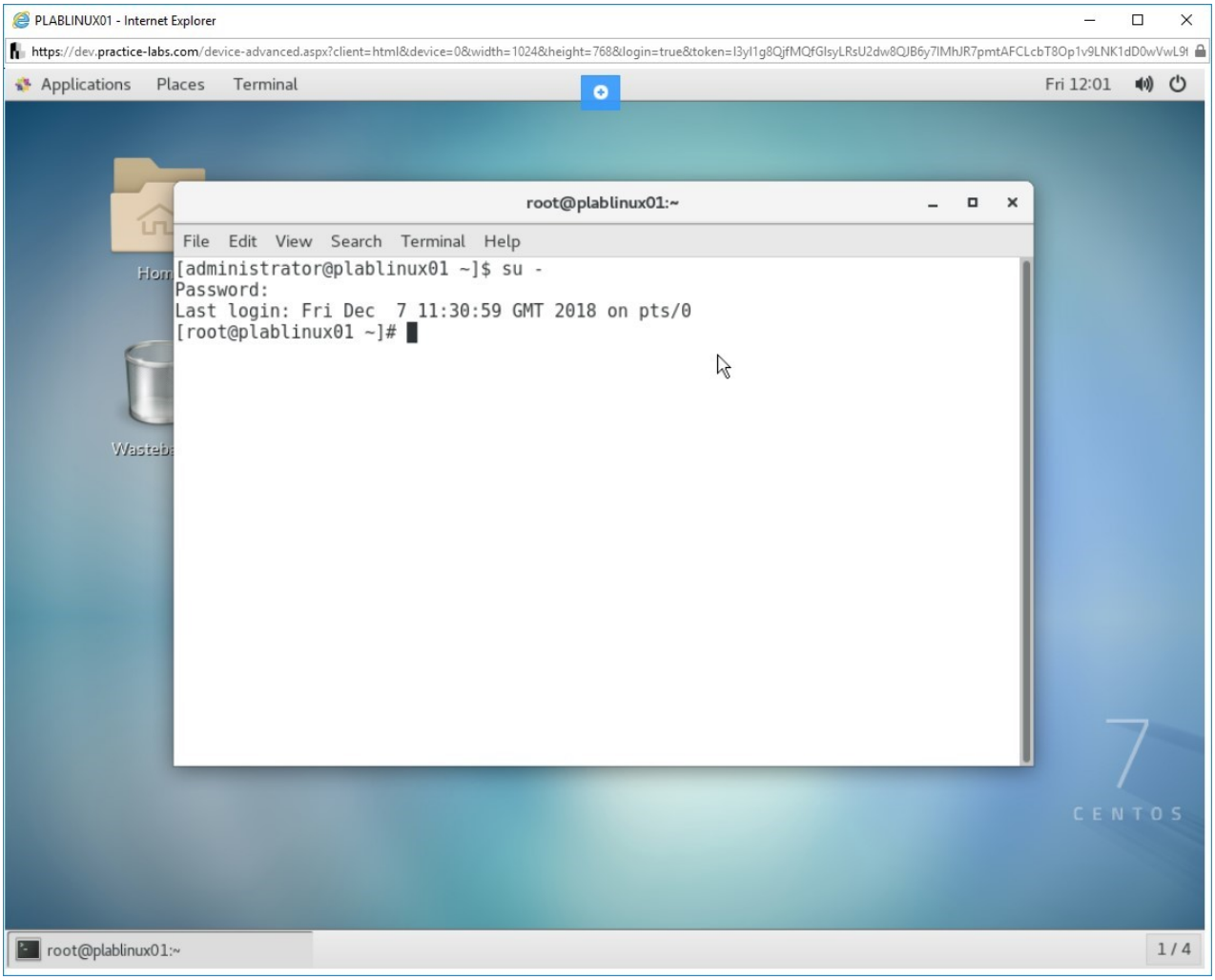


Figure 1.2 Screenshot of PLABLINUX01: Changing to the root account with the su command.

Step 3

Clear the screen by entering the following command:

```
clear
```

***Note**: The clear command should be used to clear the screen clutter. This enables 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.*

To add a user, you need to use the **useradd** command. Enter the following command:

```
useradd john
```

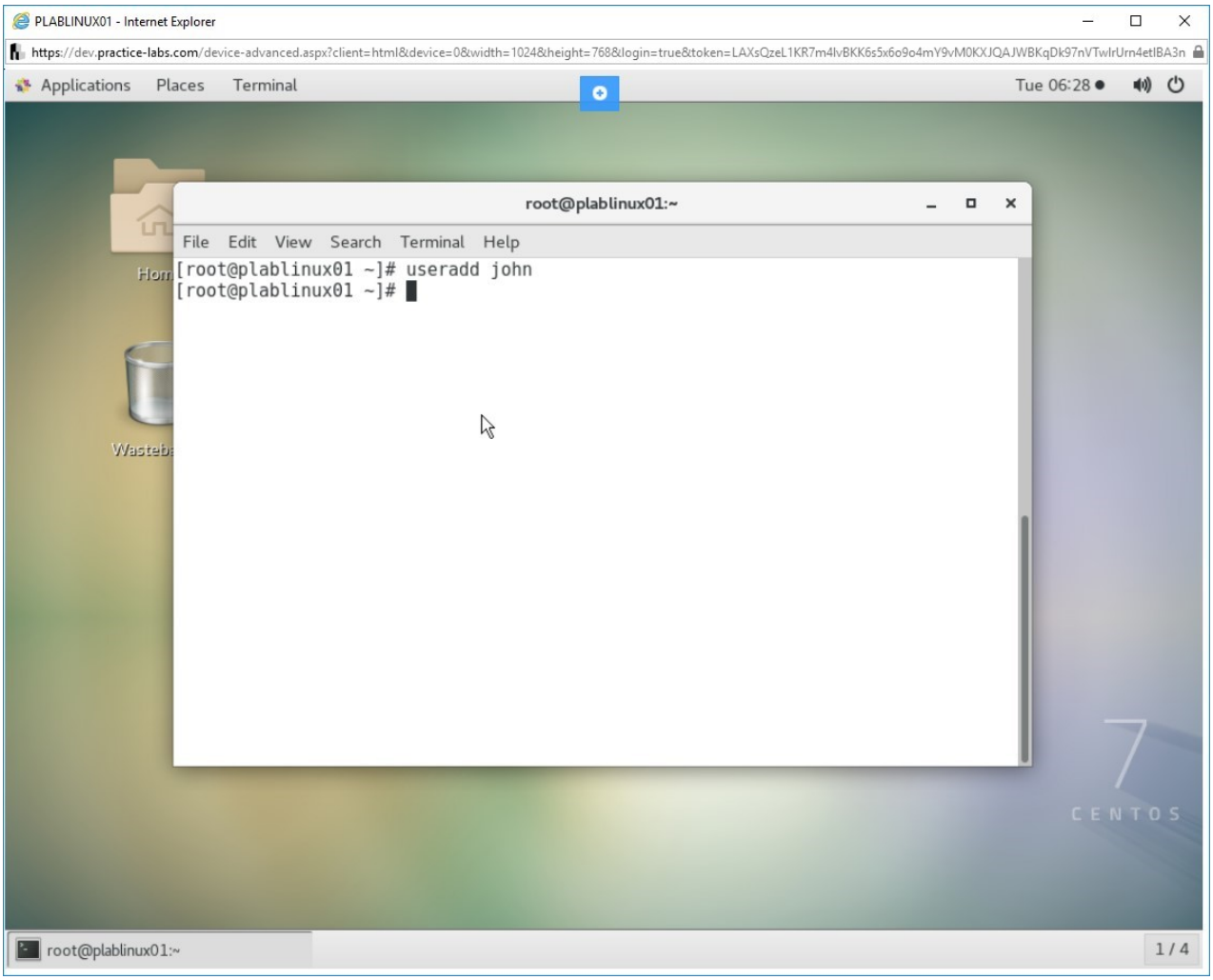


Figure 1.3 Screenshot of PLABLINUX01: Creating a user with the useradd command.

Step 4

When you create a user, it is in a locked state. It will be unlocked when you set its password. Enter the following command:

```
passwd john
```

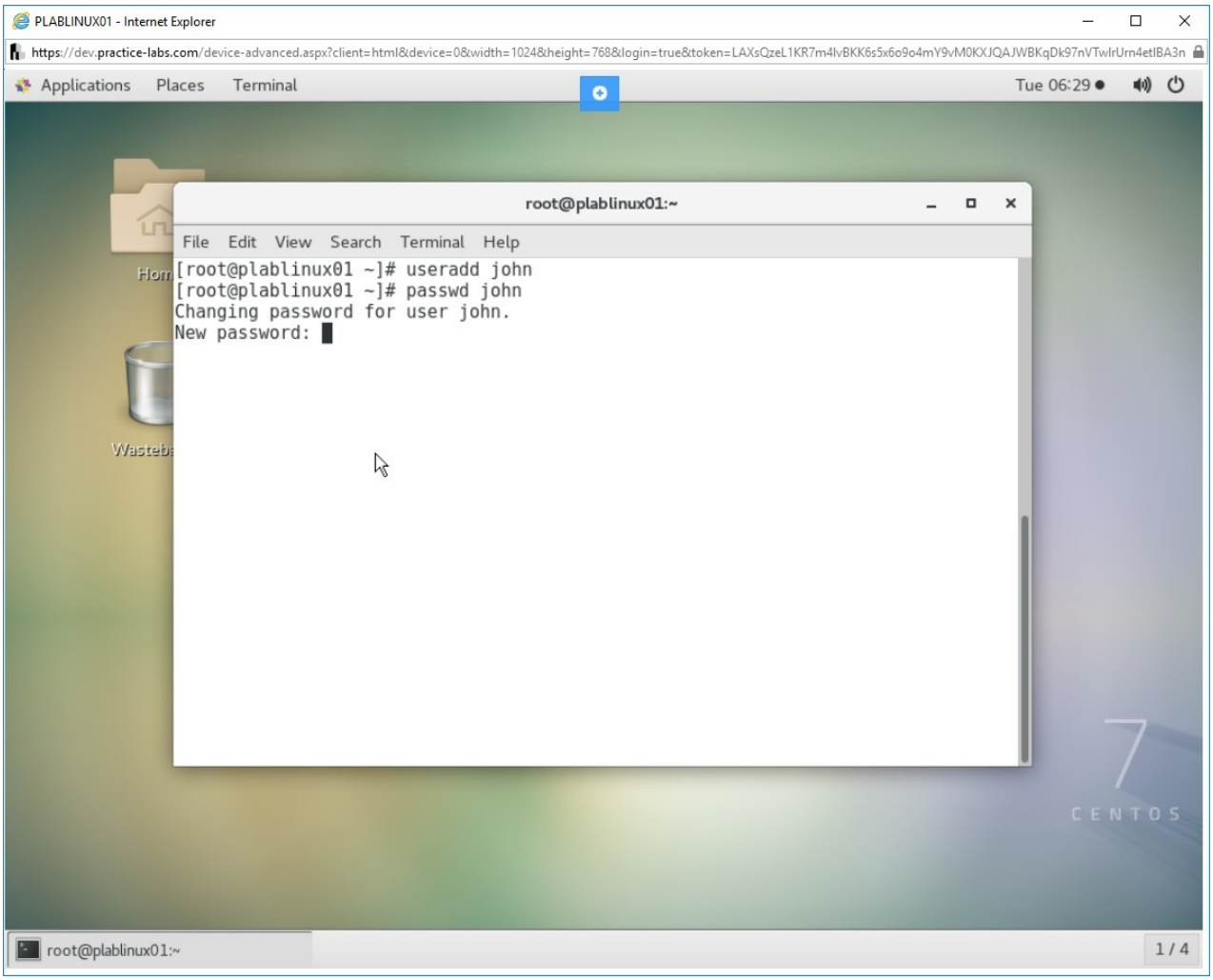


Figure 1.4 Screenshot of PLABLINUX01: Unlocking the user account by setting its password.

Step 5

You are prompted to enter the password. At the New password prompt, type the following password:

`Passw0rd`

Press **Enter**.

Type the following password at the Retype new password:

`Passw0rd`

Press **Enter**.

Once the password is updated, the system confirms the same by displaying a message on the screen.

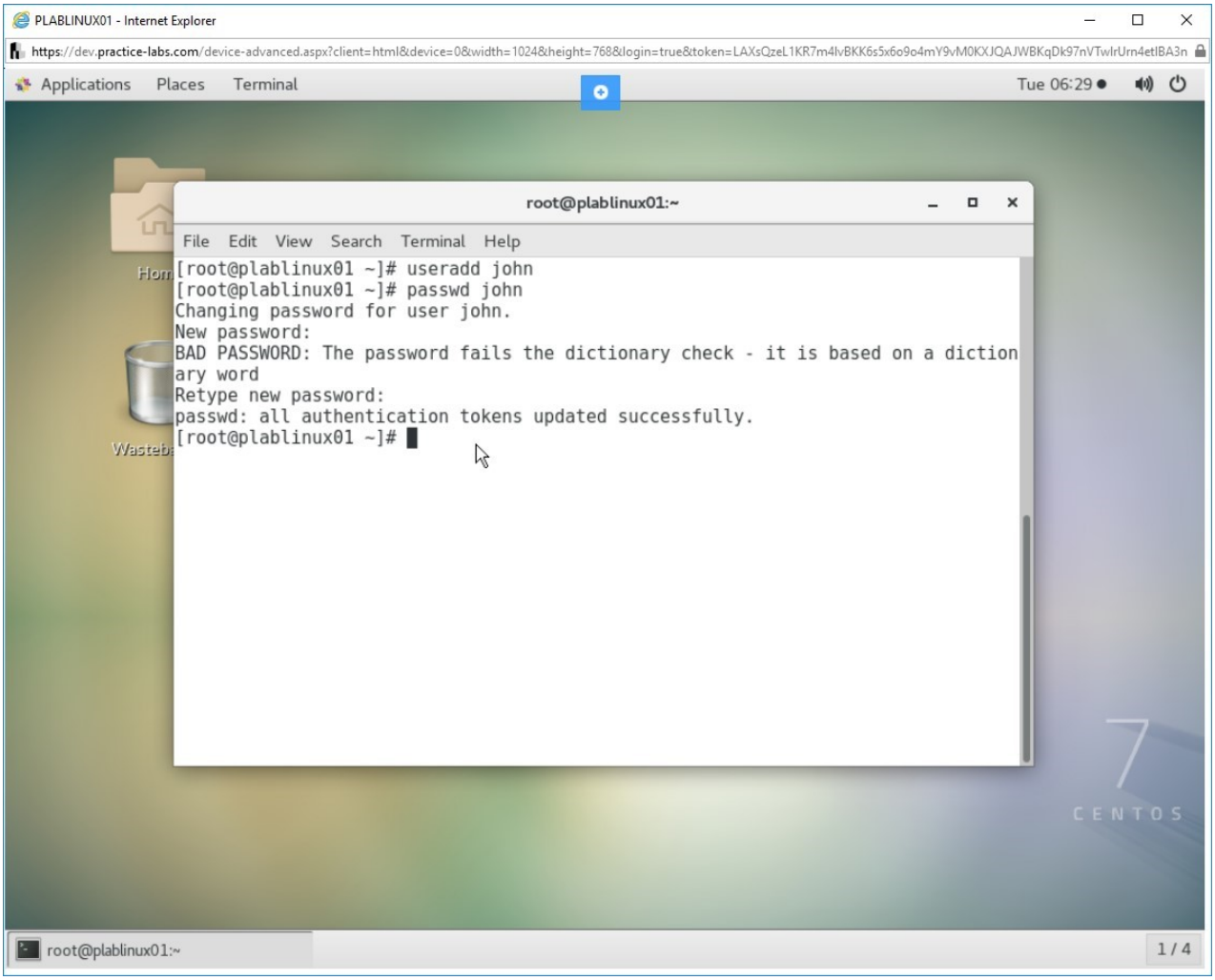


Figure 1.5 Screenshot of PLABLINUX01: Setting the password for the user named john.

Step 6

Clear the screen by entering the following command:

```
clear
```

You will now modify the user account, **john**, and set an expiration date for the same. You can modify the user account using the **usermod** command.

To set the expiration date, type the following command:

```
usermod  -e 12/12/2020 john
```

Press **Enter**.

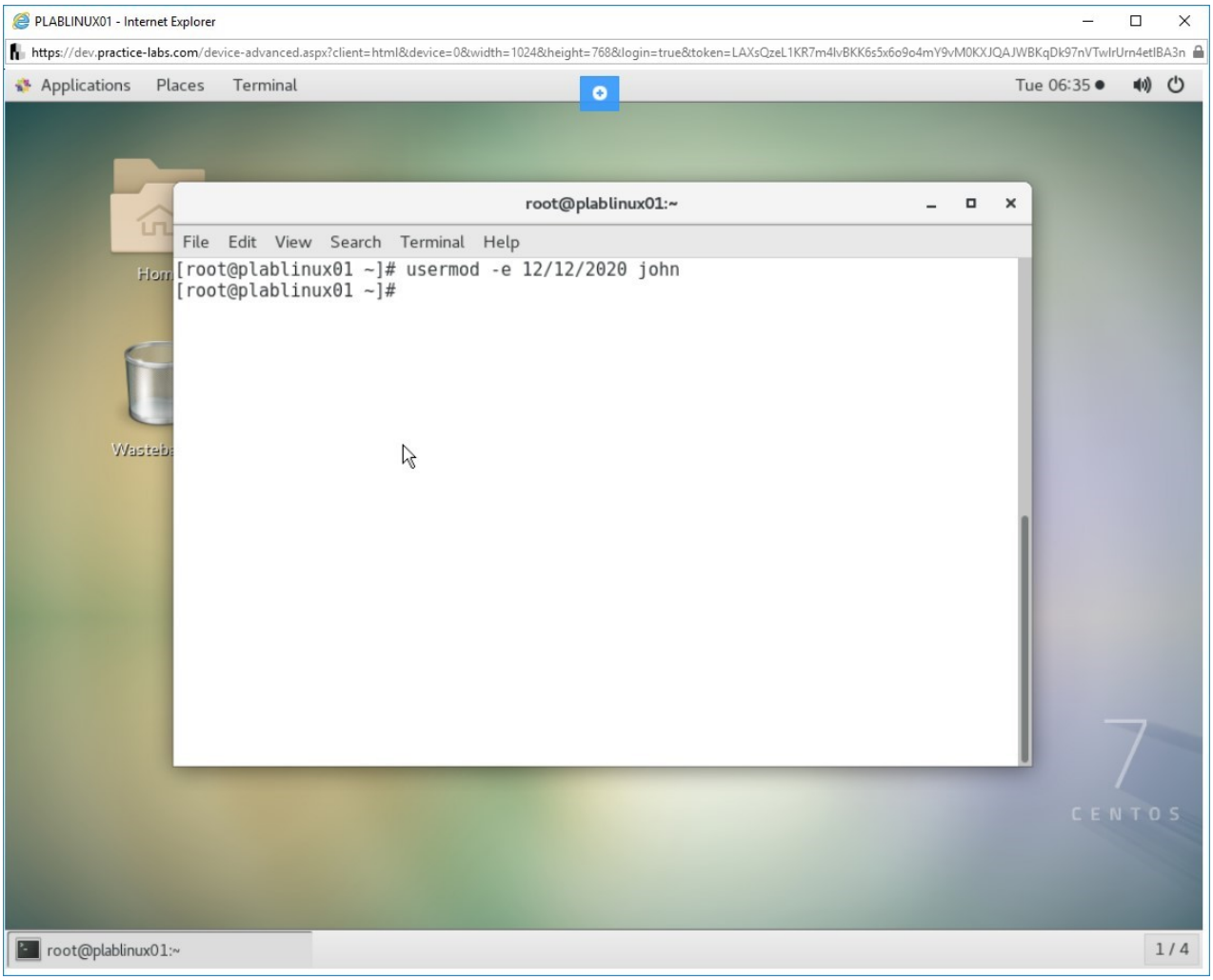


Figure 1.6 Screenshot of PLABLINUX01: Setting the expiration date for the user account.

Step 7

Using the **usermod** command, you can also perform tasks, such as locking the user account. To lock a user account, type the following command:

```
usermod -L john
```

Press **Enter**.

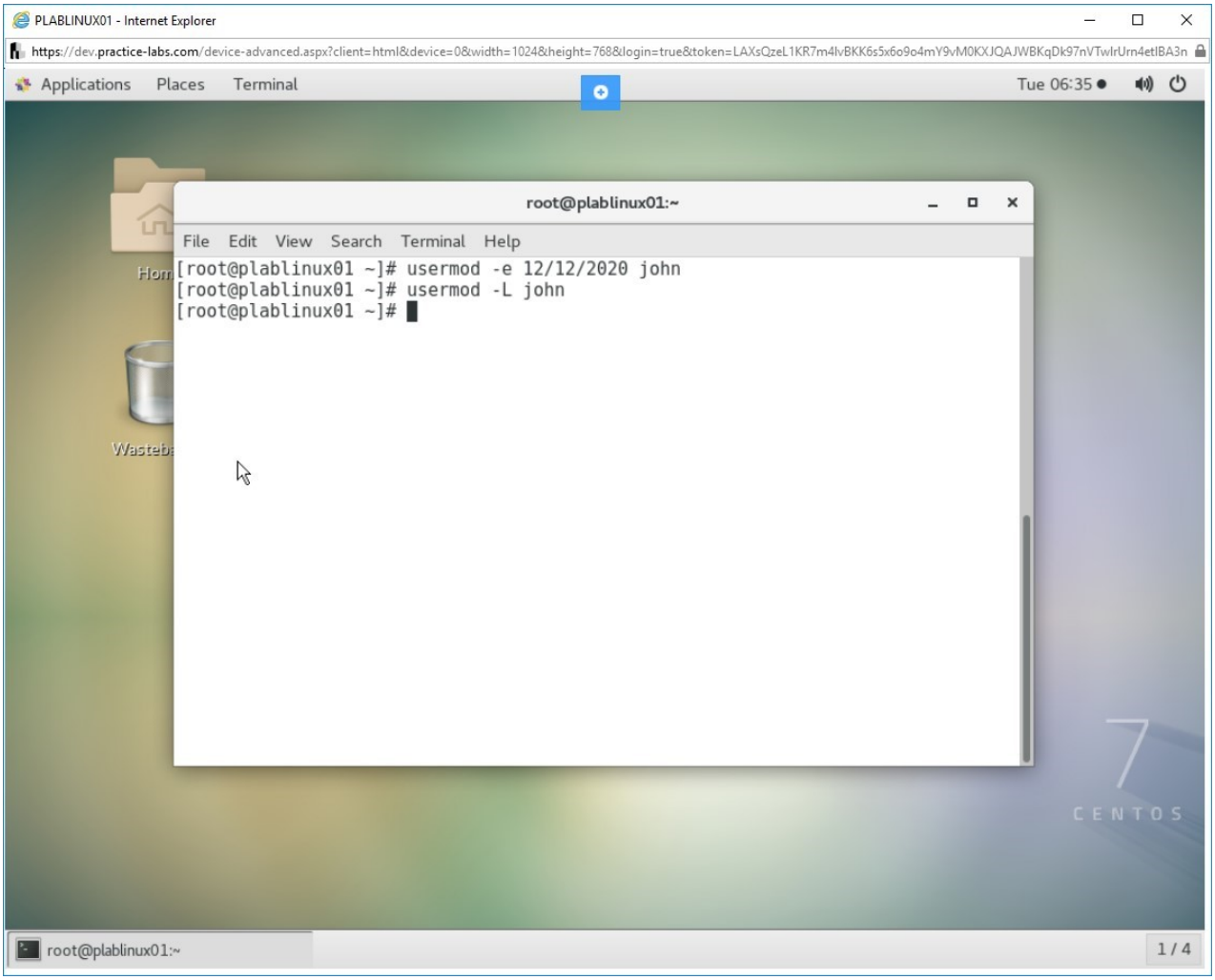


Figure 1.7 Screenshot of PLABLINUX01: Locking the user account.

Step 8

Other than the **usermod** command, you can also use the **chage** command to change the user password expiration information. For example, you can force immediate password expiration.

Type the following command:

```
chage -d 0 john
```

Press **Enter**.

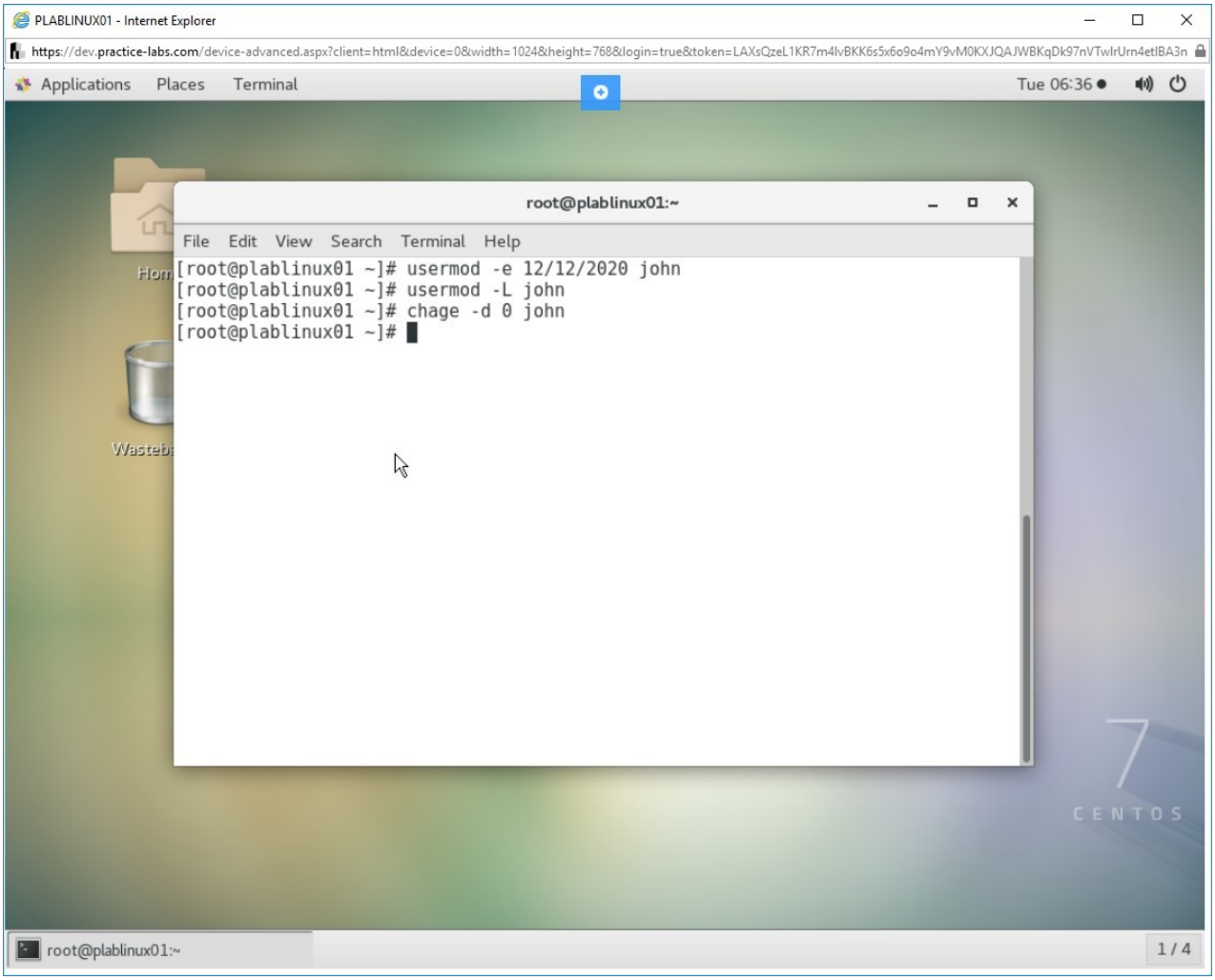


Figure 1.8 Screenshot of PLABLINUX01: Changing the password expiration date.

Step 9

Clear the screen by entering the following command:

```
clear
```

You can also delete a user with the **userdel** command. Type the following command:

```
userdel john
```

Press **Enter**.

Note that the **john** is now deleted.

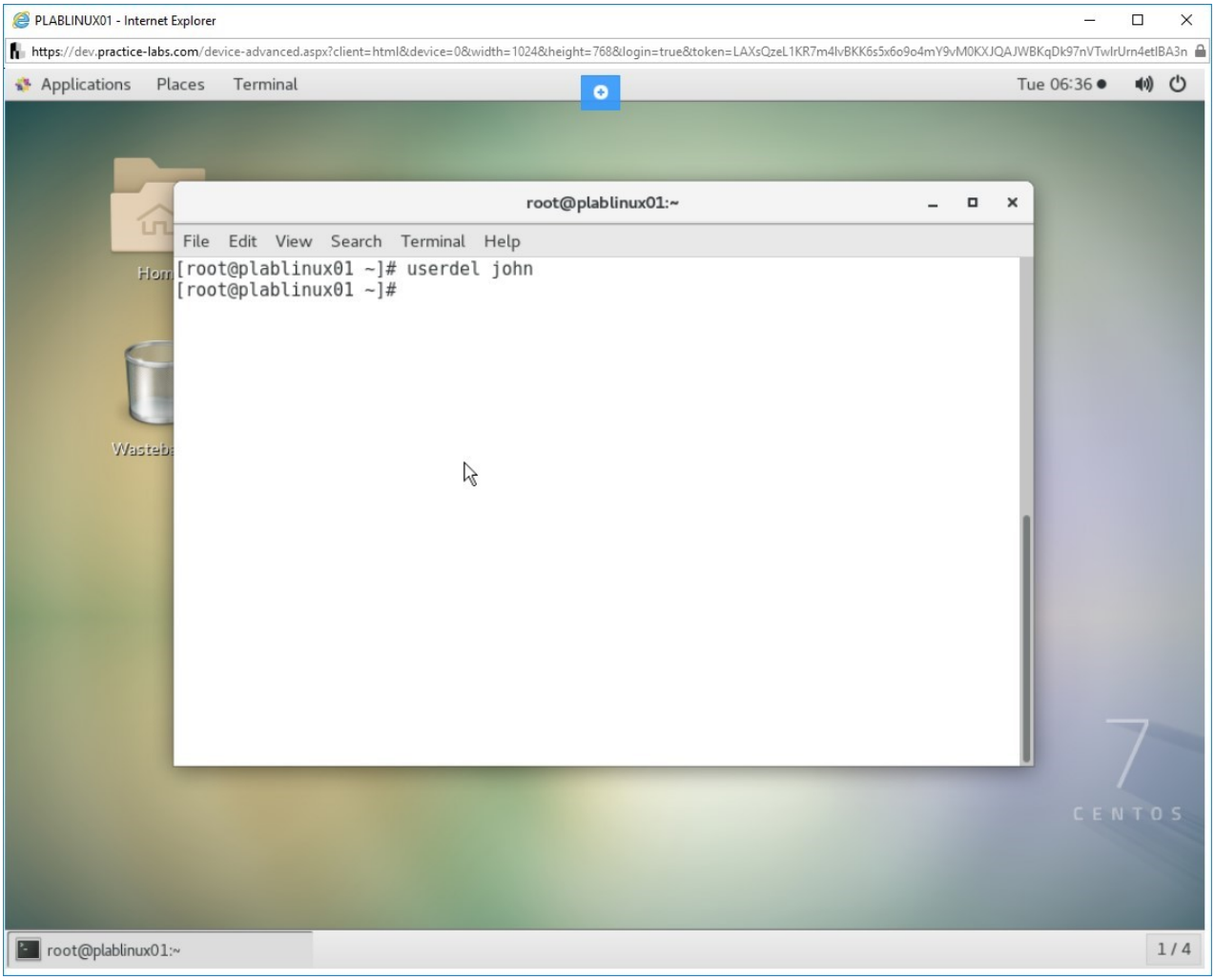


Figure 1.9 Screenshot of PLABLINUX01: Deleting the user account.

Step 10

Clear the screen by entering the following command:

```
clear
```

Let us now create a group on the Linux system. Before you create a group, you must create at least two users who will be a part of these groups.

Create the users, **john,** and **rebecca**, with the **useradd** command and then enable them with the **passwd** command by setting their password.

Use `Passw0rd` as the password.

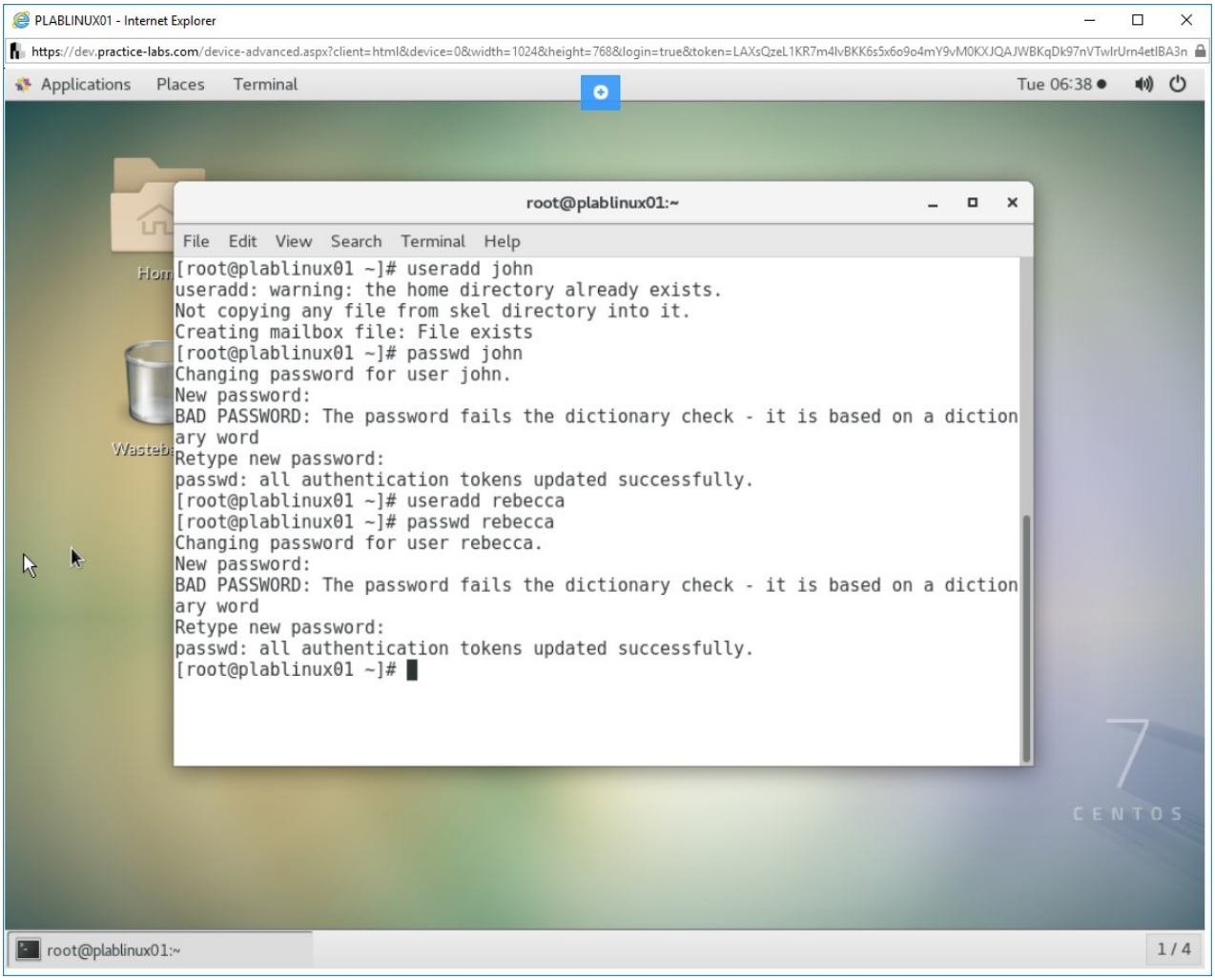


Figure 1.10 Screenshot of PLABLINUX01: Creating new user accounts.

Step 11

Clear the screen by entering the following command:

```
clear
```

Now, you can create a group with the two users. To create a group, type the following command:

```
groupadd -g 10000 plabuser
```

Press **Enter**.

A new group with the **group id 10000** will be created and named as **plabuser**.

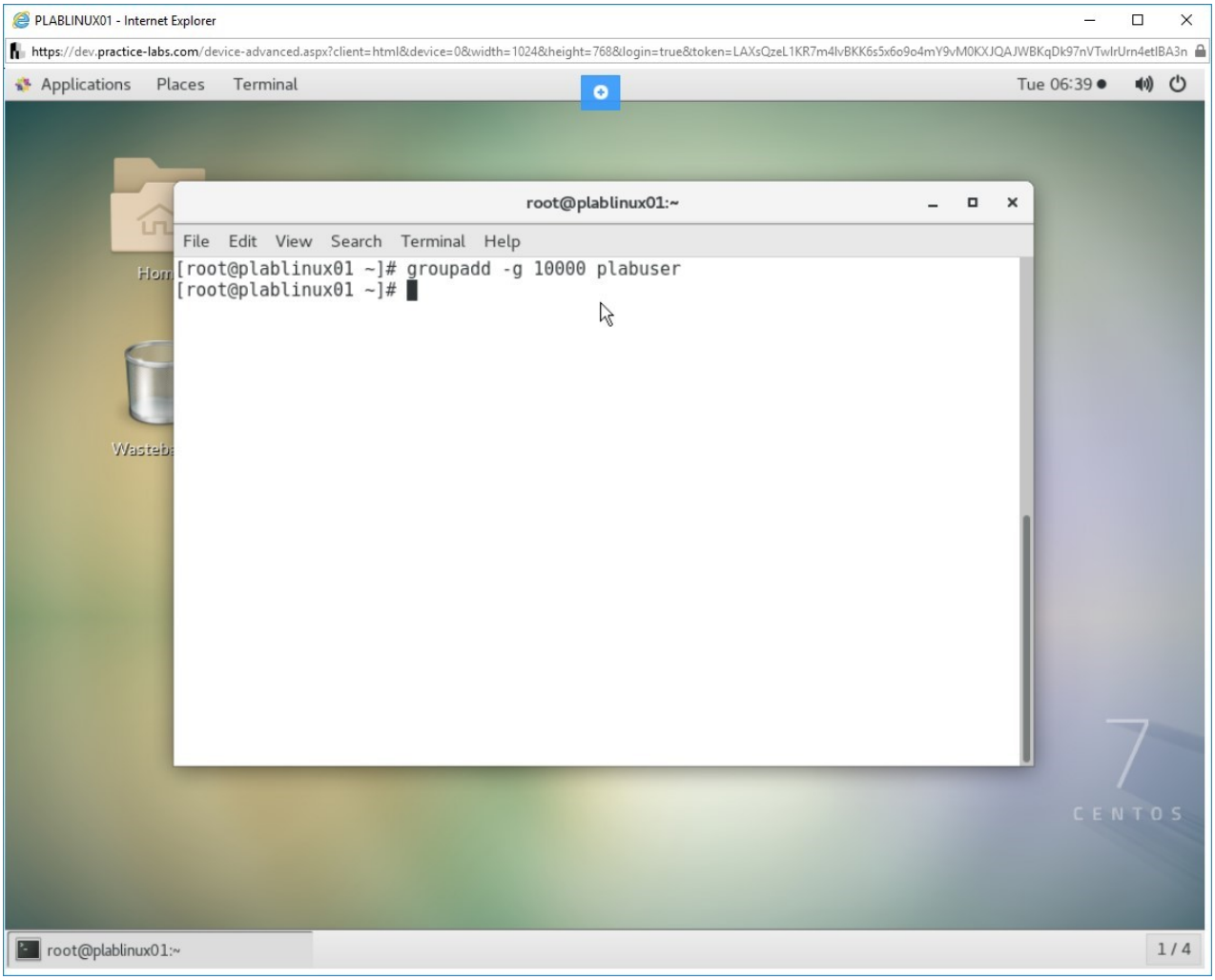


Figure 1.11 Screenshot of PLABLINUX01: Creating a group.

Step 12

Clear the screen by entering the following command:

```
clear
```

You can now add users to the **plabuser** group. You will need to use the **usermod** command. Type the following command:

```
usermod -aG plabuser john
```

Press **Enter**.

Then, repeat the same command for **rebecca**. Type the following command:

```
usermod -aG plabuser rebecca
```

Press **Enter**.

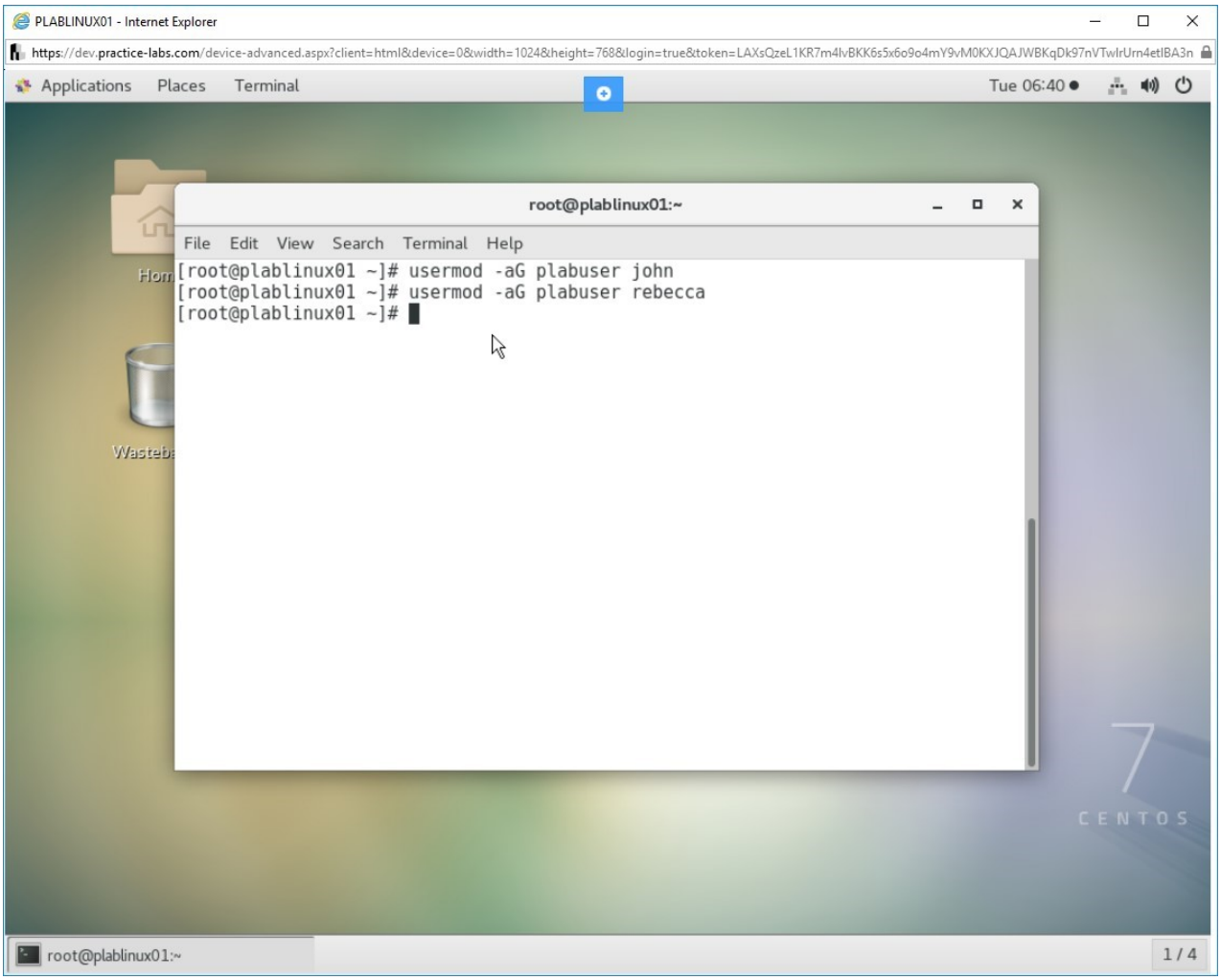


Figure 1.12 Screenshot of PLABLINUX01: Adding users to the group.

Step 13

Clear the screen by entering the following command:

```
clear
```

After you have added both the users, you can verify whether they have been added to the **plabuser** group. Type the following command:

```
id john
```

Press **Enter**.

Note the last group, **plabuser**. You can check for **rebecca** as well by typing the following command:

```
id rebecca
```

Press **Enter**.

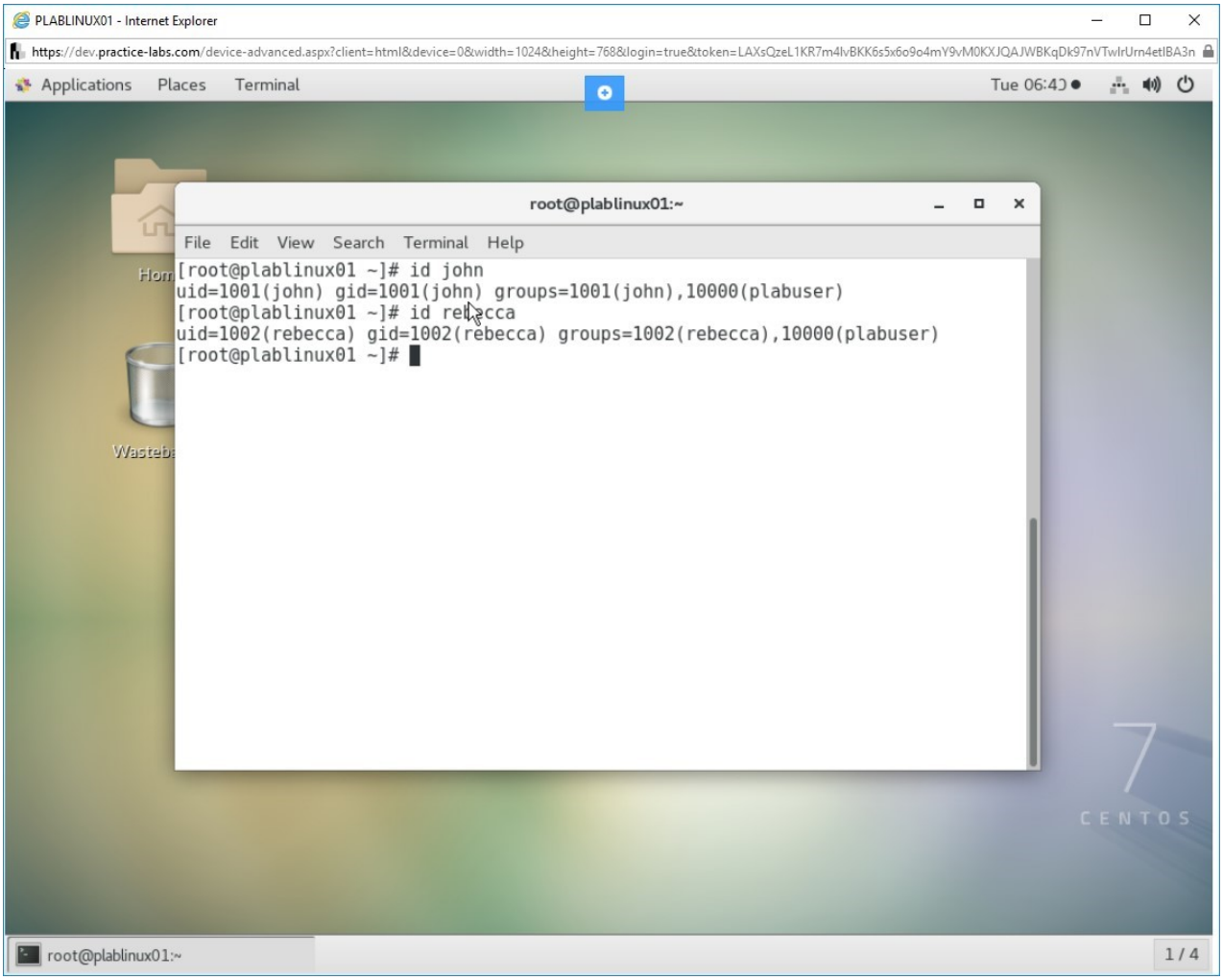


Figure 1.13 Screenshot of PLABLINUX01: Verifying the ids of the users.

Step 14

You can also modify a group. For example, if you want to change the group name, you can do it by typing the following command:

```
groupmod -n plab plabuser
```

Press **Enter**.

> ***Note**: The -n parameter is for changing the name. You can get more parameters by entering the man groupmod command.*

The first group name in this instance is plab, which is the new name and plabuser is the older name.

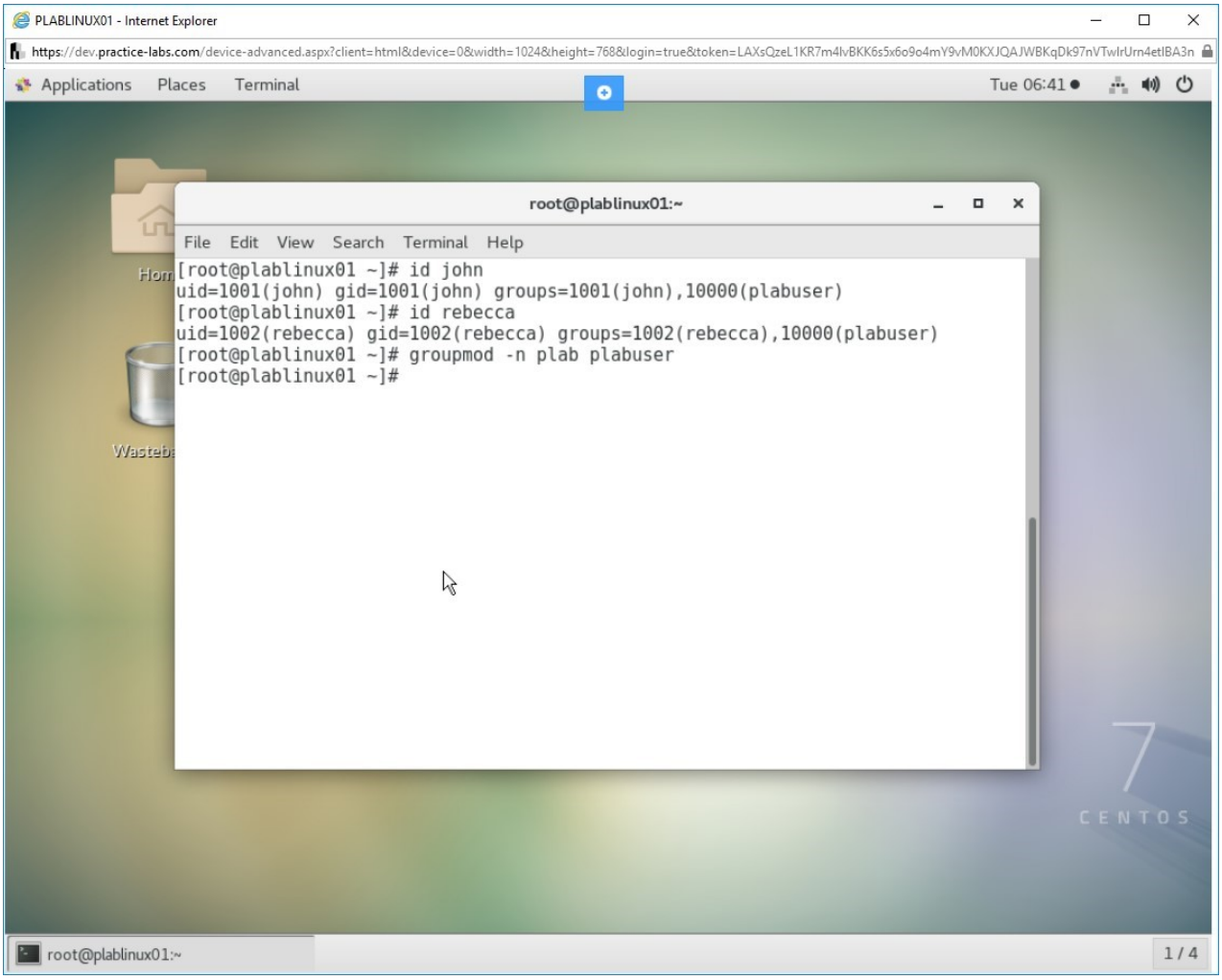


Figure 1.14 Screenshot of PLABLINUX01: Changing the group name.

Step 15

You can also delete a group with the **groupdel** command. When a group is deleted, note that the users are not deleted.

Type the following command:

```
groupdel plab
```

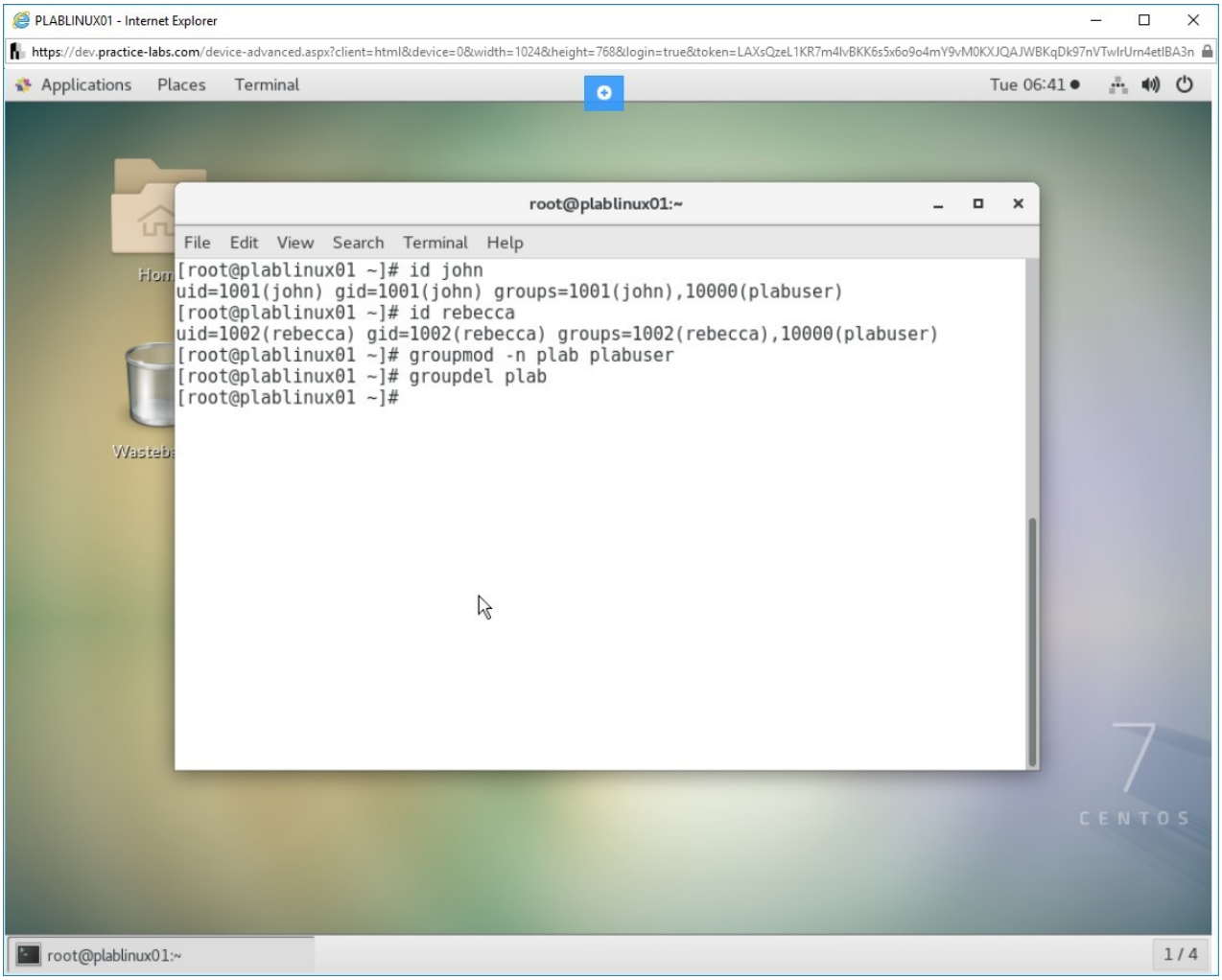


Figure 1.15 Screenshot of PLABLINUX01: Deleting the group.

Step 16

Clear the screen by entering the following command:

```
clear
```

Verify if john is still part of the deleted group **plab**. Type the following command:

```
id john
```

Press **Enter**.

You can check for **rebecca** as well by typing the following command:

```
id Rebecca
```

Press **Enter**.

Notice that the group **plab** is not listed as a part of the ID information as the group is now deleted.

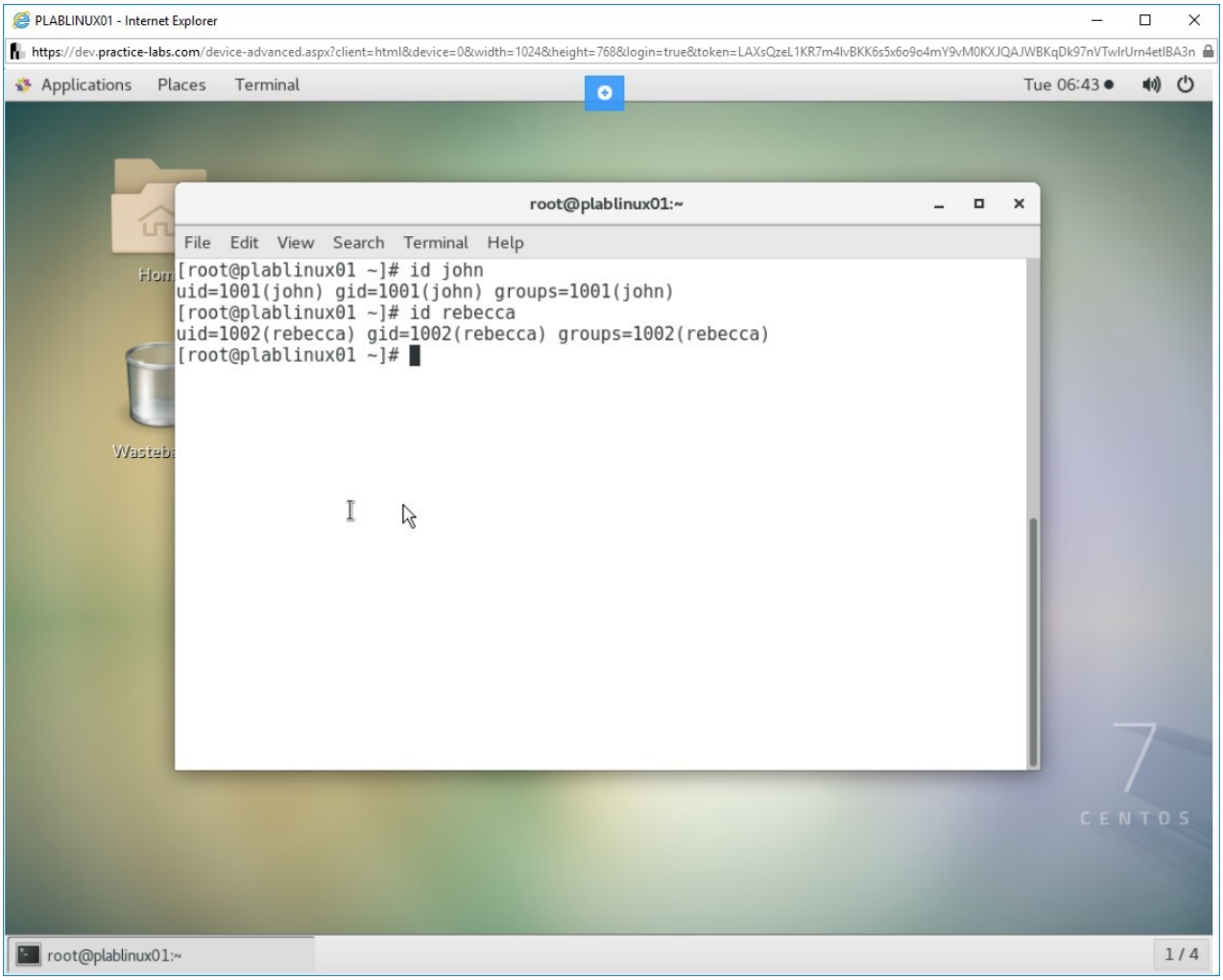


Figure 1.16 Screenshot of PLABLINUX01: Verifying the ids of the user accounts.

Task 2 - Access User/Group Password Info

In a multi-user environment, it is important to encrypt passwords to protect them from unauthorized access by other users on the system. The passwords are moved from /etc/passwd to the /etc/shadow file. The /etc/shadow file is readable only by the root user.

Shadow passwords are enabled by default by the **shadow-utils** package. In this task, you will access various password-files on the system to the view the passwords of individual users as well as groups.

To view the shadow passwords, perform the following steps:

Step 1

Clear the screen by entering the following command:

```
clear
```

To view the **/etc/passwd** file, type the following command:

```
cat /etc/passwd
```

Press **Enter**.

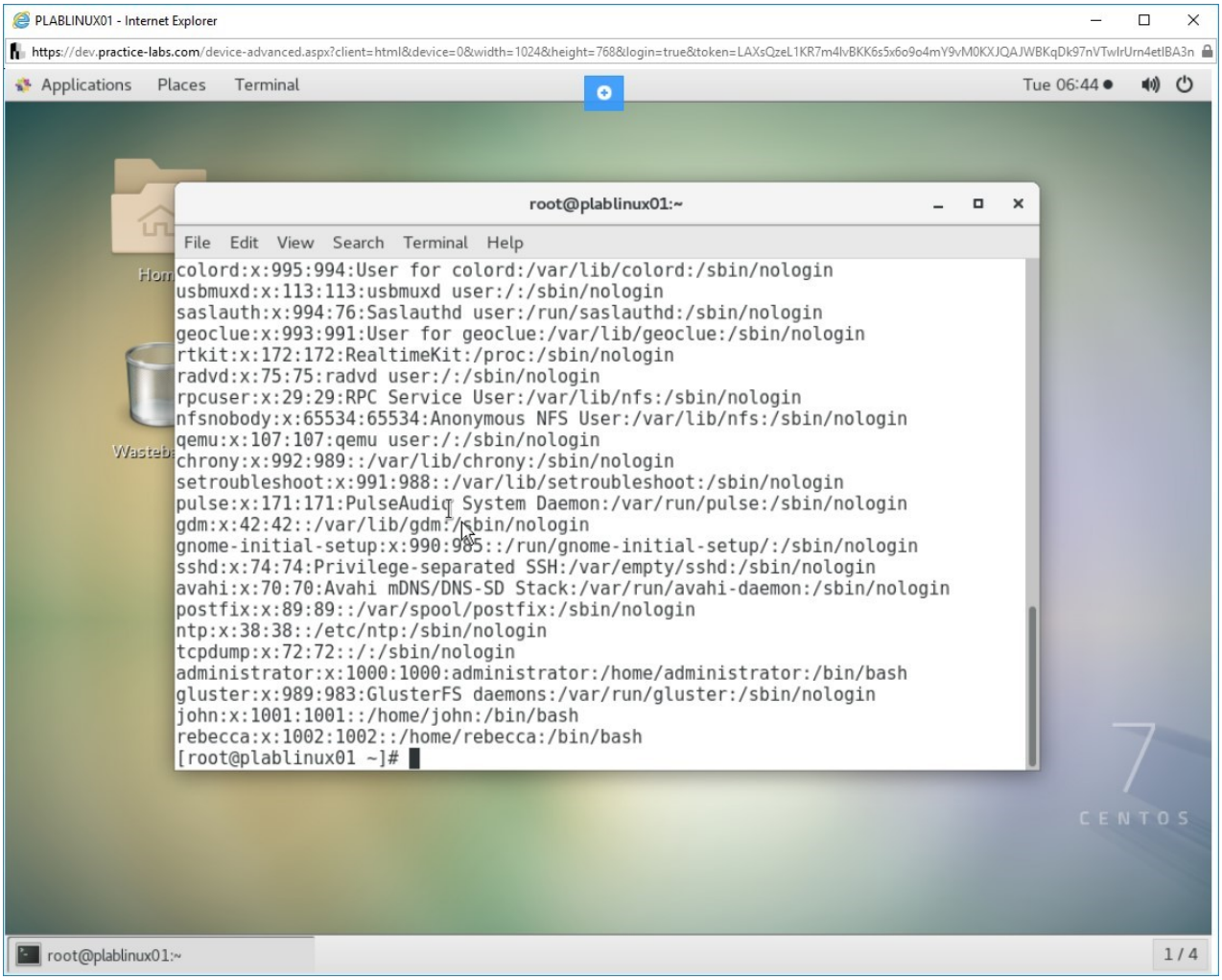


Figure 1.17 Screenshot of PLABLINUX01: Viewing the contents of the /etc/passwd file.

Step 2

Clear the screen by entering the following command:

```
clear
```

To view the **/etc/shadow** file, type the following command

```
cat /etc/shadow
```

Press **Enter**.

Note that all passwords are encrypted.

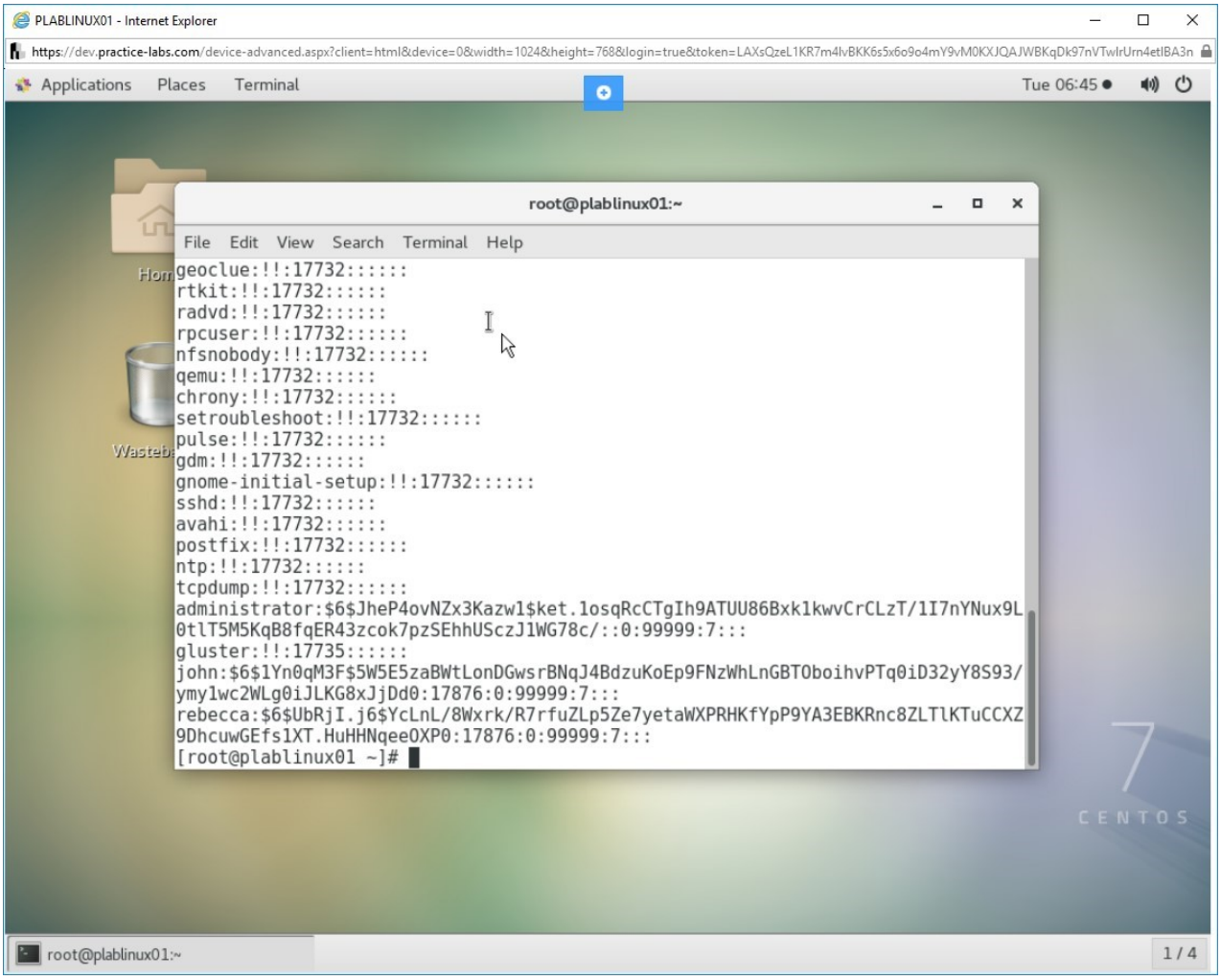


Figure 1.18 Screenshot of PLABLINUX01: Viewing the contents of the /etc/shadow file.

Step 3

Clear the screen by entering the following command:

```
clear
```

You can also view the passwords for various groups in the **/etc/group** file. To do this, type the following command:

```
cat /etc/group
```

Press **Enter**.

The list of groups is displayed.

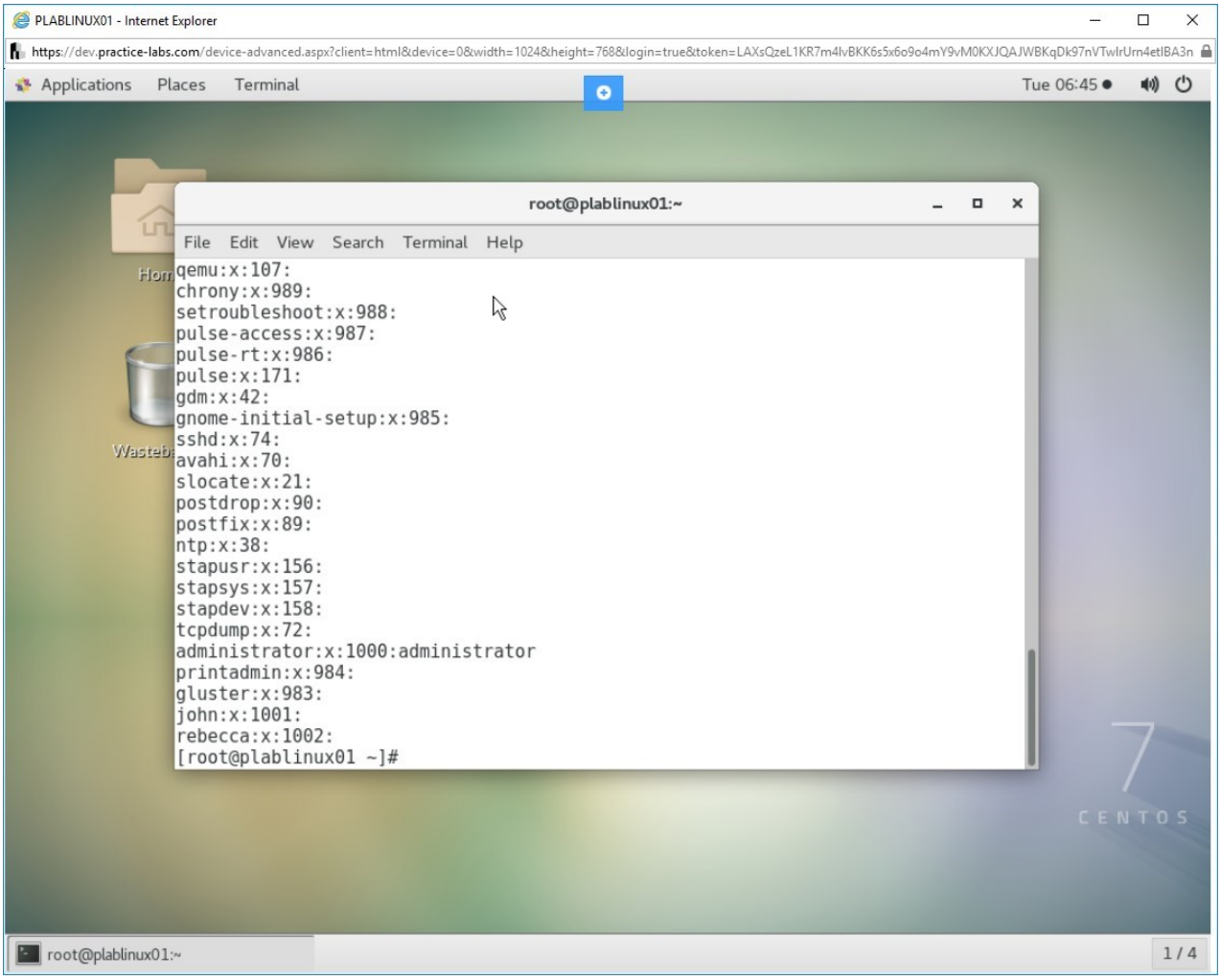


Figure 1.19 Screenshot of PLABLINUX01: Viewing the contents of the /etc/group file.

Task 3 - Create and manage special purpose and limited accounts

The **/etc/skel** file allows an administrator to create a default home directory for all new users on a computer. This ensures that the new users begin with the same settings in the environment they log in to.

To create and manage special purpose and limited accounts, perform the following steps:

Step 1

Clear the screen by entering the following command:

```
clear
```

To view the **/etc/skel** directory, type the following command:

```
ls -a /etc/skel
```

Press **Enter**.

The files in the **/etc/skel** directory are displayed.

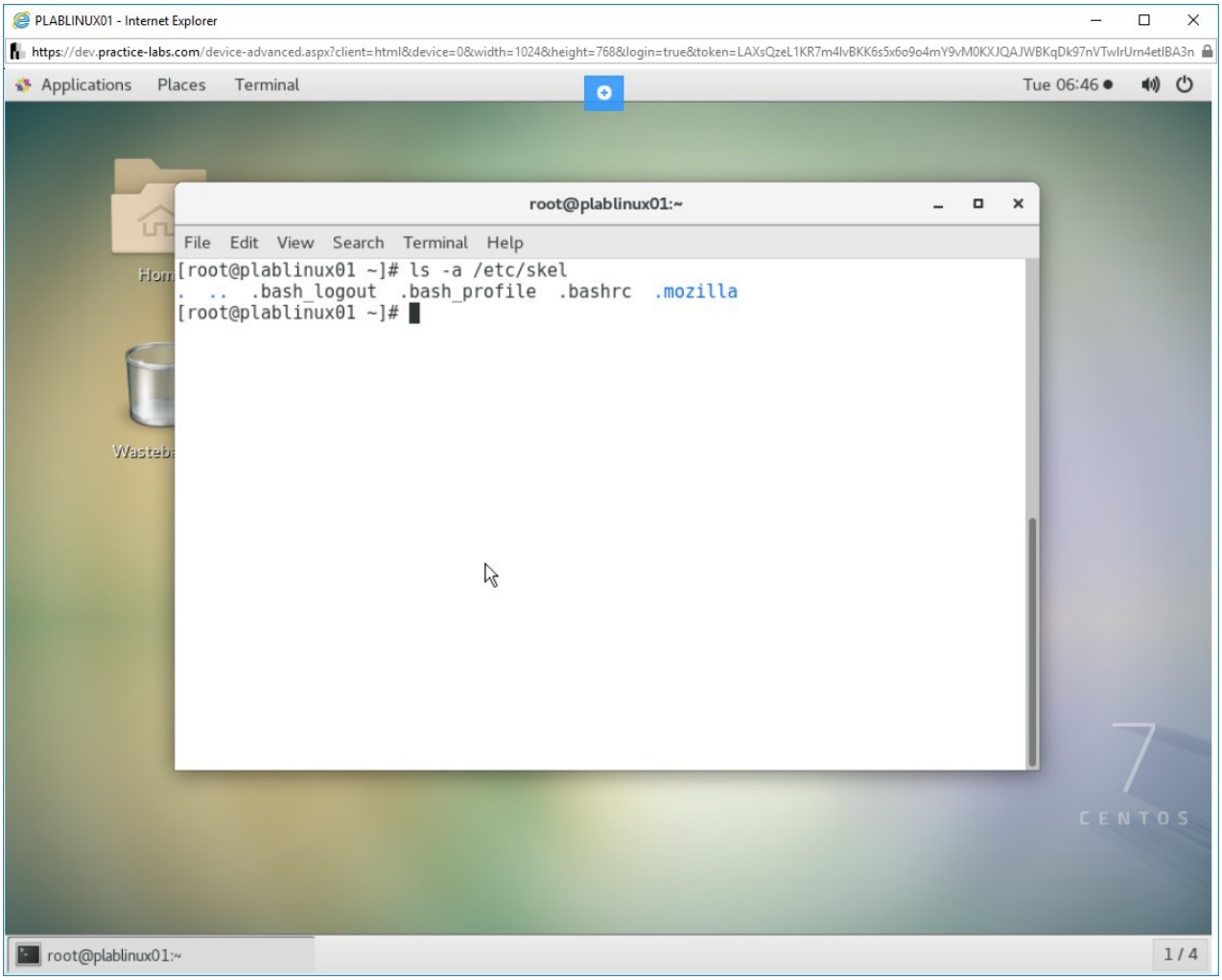


Figure 1.20 Screenshot of PLABLINUX01: Listing the contents of the /etc/skel directory.

Step 2

You can also disable logins into the system by creating the **/etc/nologin** file. By default, this file does not exist. If you create this file, only the root user will able to log on to the system. Login access to the remaining users will be disabled.

To create a **nologin** file, type the following command:

```
touch /etc/nologin
```

Press **Enter**.

The **/etc/nologin** file is created without anything inside it.

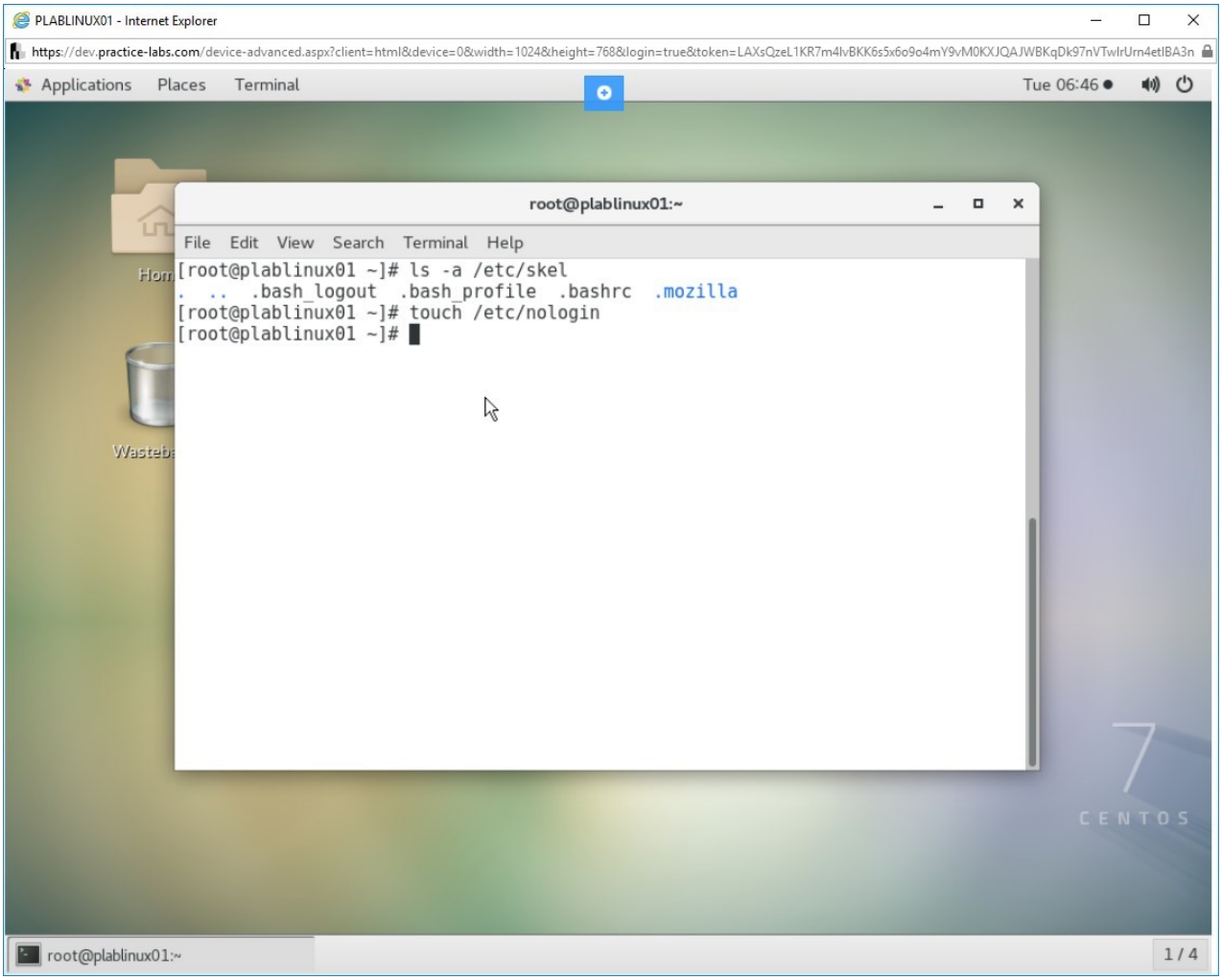


Figure 1.21 Screenshot of PLABLINUX01: Creating the nologin file.

Step 3

To view the **nologin** file, type the following command:

```
cat /etc/nologin
```

Press **Enter**.

Note that there are no contents in the file. It is simply blank.

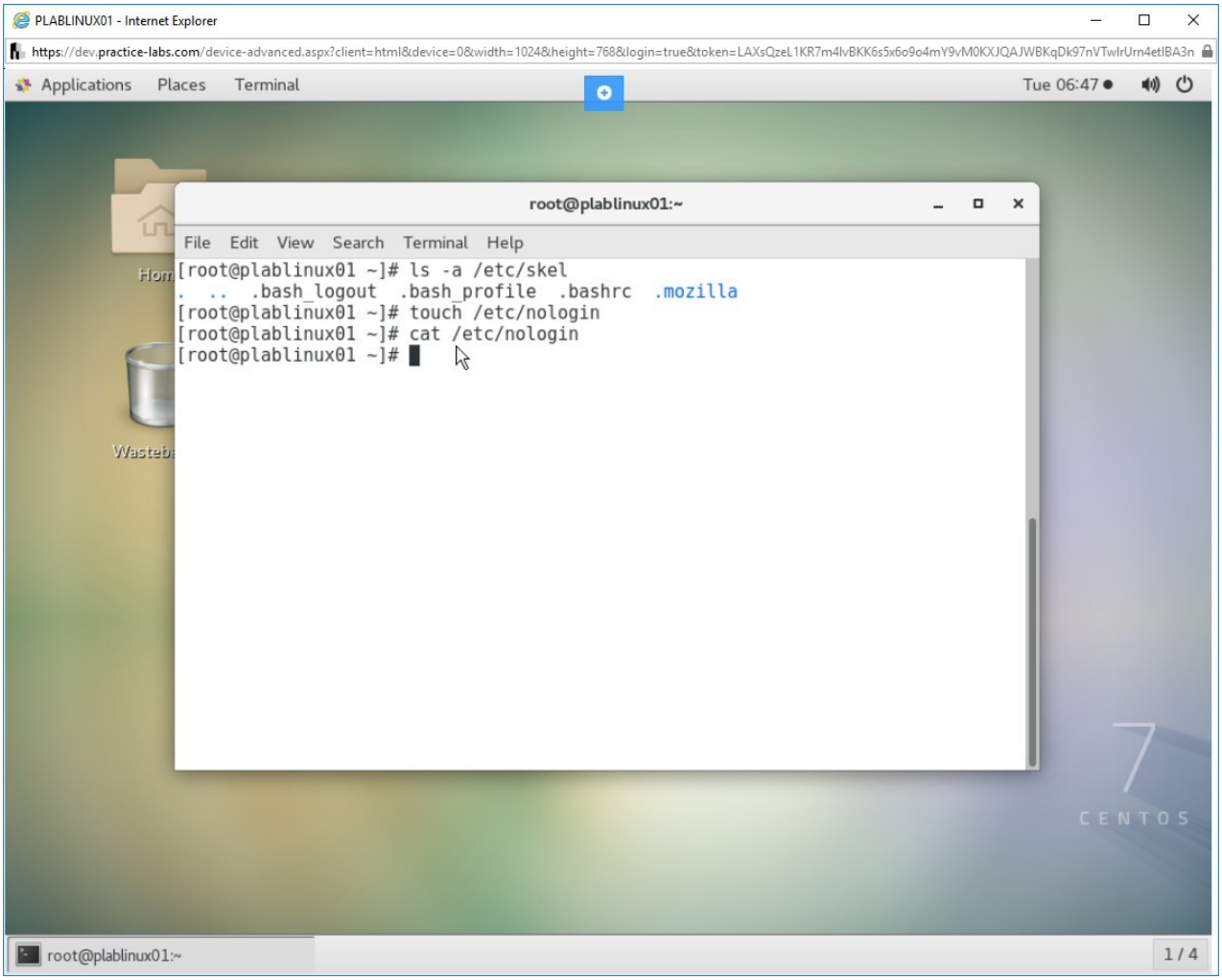


Figure 1.22 Screenshot of PLABLINUX01: Viewing the contents of the /etc/nologin file.

Step 4

The special purpose accounts are listed in the **/etc/passwd** file. Type the following command:

```
cat /etc/passwd
```

Press **Enter**.

The contents of the **/etc/passwd** file are displayed.

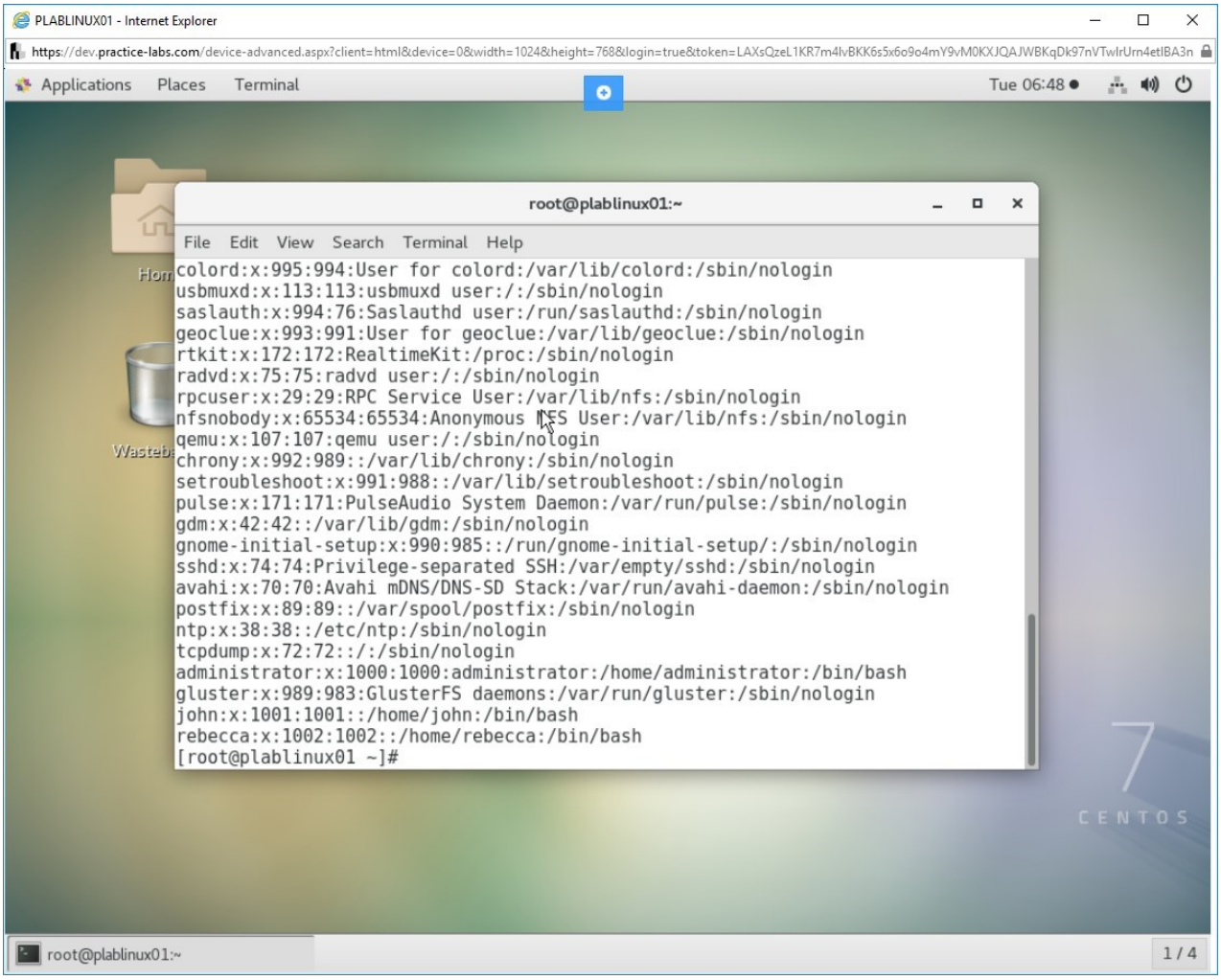


Figure 1.23 Screenshot of PLABLINUX01: Viewing the contents of the /etc/passwd file.

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

Review

Well done, you have completed the **Manage User and Group Accounts and Related System Files** Practice Lab.

Summary

You completed the following exercise:

- Exercise 1 - Manage User and Group Accounts and Related System Files

You should now be able to:

- Add, modify, and remove users and groups
- Access User/group password info
- Create and manage special purpose and limited accounts

Feedback

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