CompTIA Linux+

Perform Security Administration Tasks

Introduction

Welcome to the **Perform Security Administration Tasks** Practice Lab. In this module you will be provided with the instructions and devices needed to develop your hands-on skills.

Security
Administration
Linux System

Learning Outcomes

In this module, you will complete the following exercise:

- Exercise 1 - Perform Security Administration Tasks

After completing this lab, you will be able to:

- Find files with the suid/sgid bit set
- Manage user passwords and password-aging information
- List the users logged into the system
- Use the su command
- Use the sudo command
- Manage shell resources
- Discover open ports on a system

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.

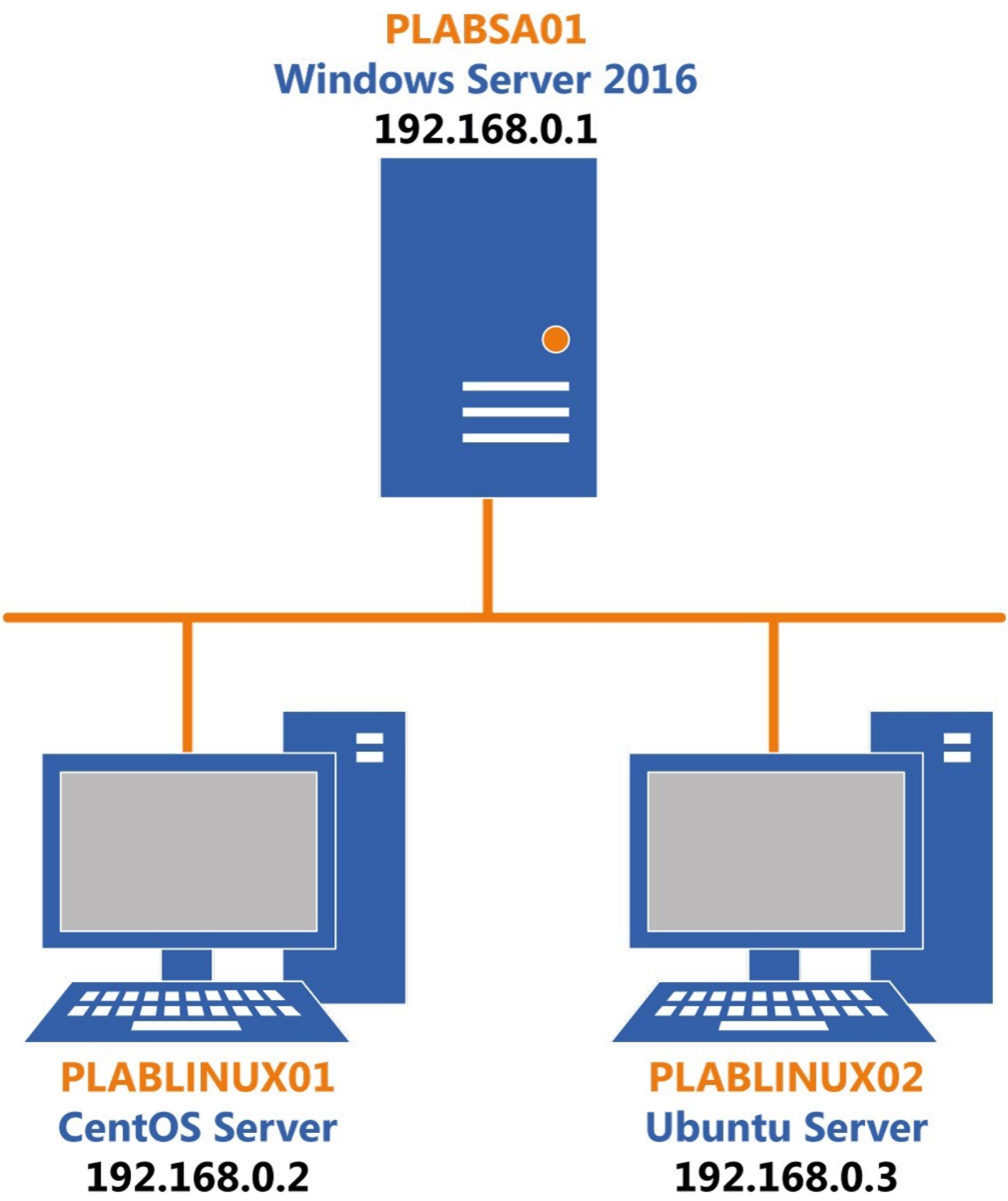
Help and Support

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 - Perform Security Administration Tasks

Security administration includes suid/sgid, in this exercise, you will understand how to perform security administration tasks.

Learning Outcomes

After completing this exercise, you will be able to:

- Log into a Linux System
- Find files with the suid/sgid bit set
- Manage user passwords and password-aging information
- List the users logged into the system
- Use the su command
- Use the sudo command
- Manage shell resources
- Discover open ports on a system

Your Devices

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

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

Task 1 - Find Files with the suid/sgid Bit Set

SUID stands for Set User ID. SUID bit, when set on an application or file, refers to the owner of application or file rather than the current user. For example, consider an application or a file whose owner is **root**. Now, this application or file has SUID bit set. When a normal user runs the application, it runs as root rather than the normal user. SUID bit tells the Linux system that if an application has SUID bit set, then the application must run as root, not the current user. SGID, short for Set Group ID, works in the same way but it is applicable for a group of users. In this task, you will audit the system to find files that have the suid/sgid bits set.

To audit a system to find files with the SUID/SGID, perform the following steps:

Step 1

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

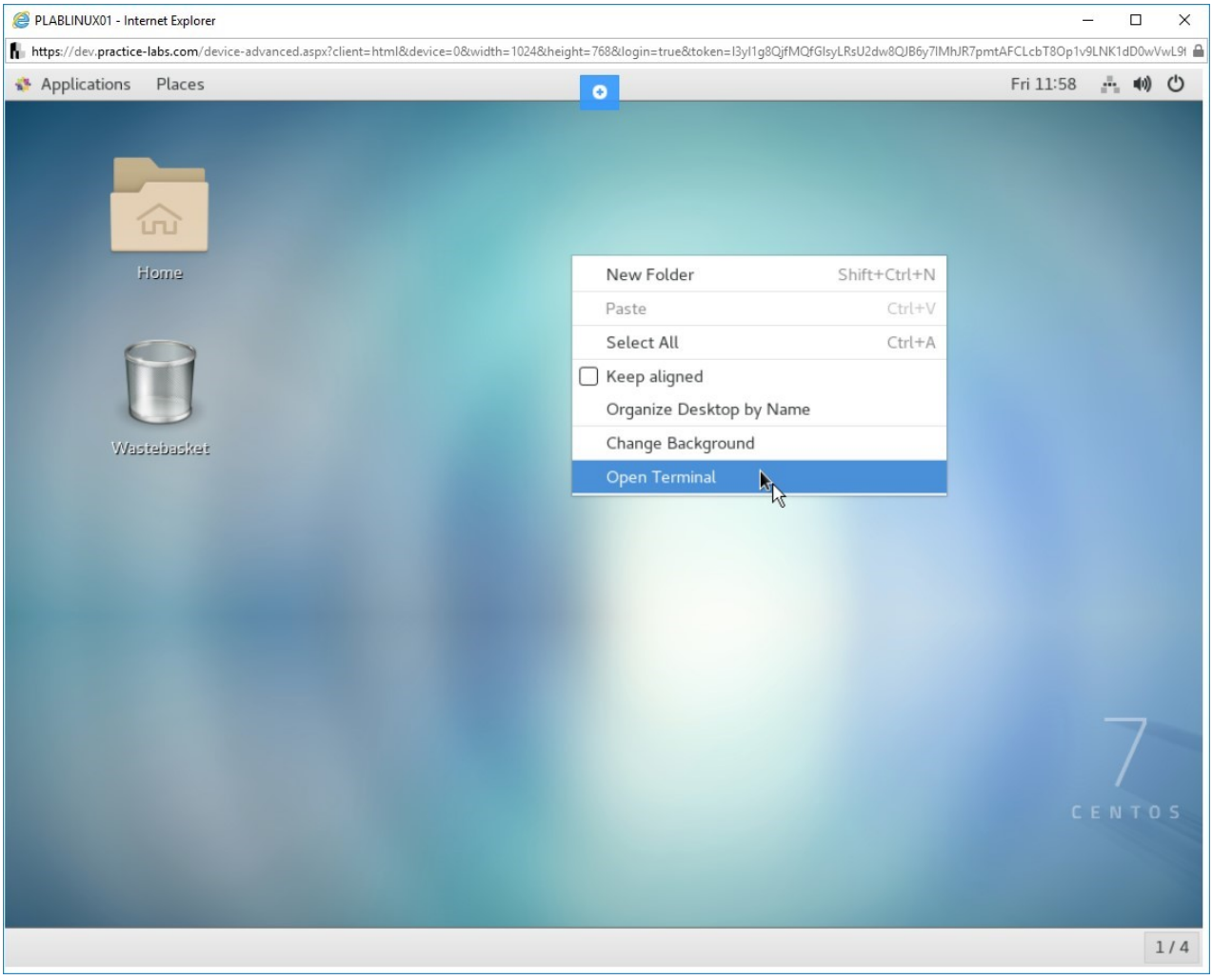


Figure 1.1 Screenshot of PLABLINUX01: Selecting the Open Terminal option from the context menu.

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**.

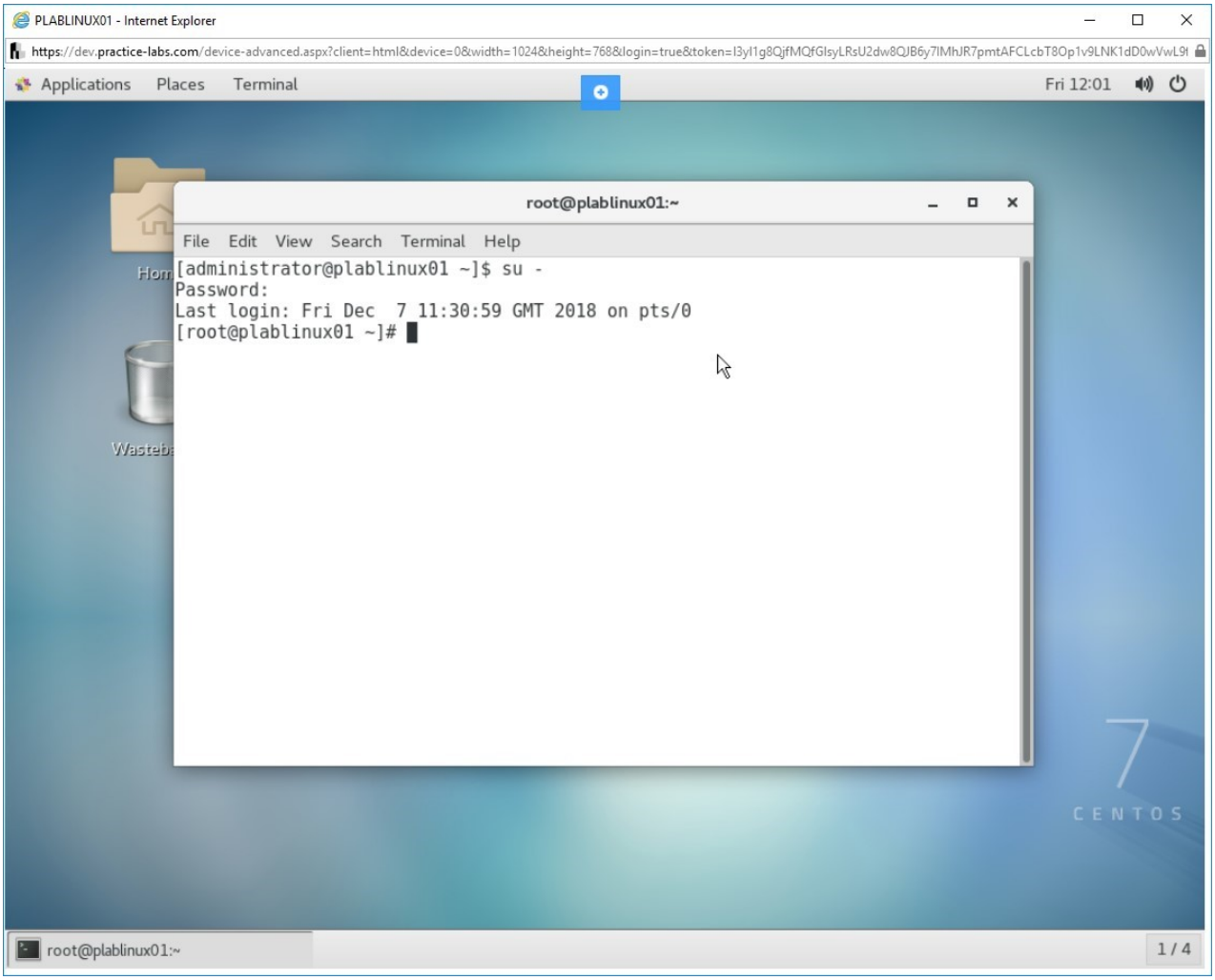


Figure 1.2 Screenshot of PLABLINUX01: Changing the account to the root account with the su command.

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.*

To view the SUID on a file, type the following command:

```
ls -l /usr/bin/write
```

Press **Enter**. Note that the results show an **s** in the permissions. This indicates that the SUID is set on the file.

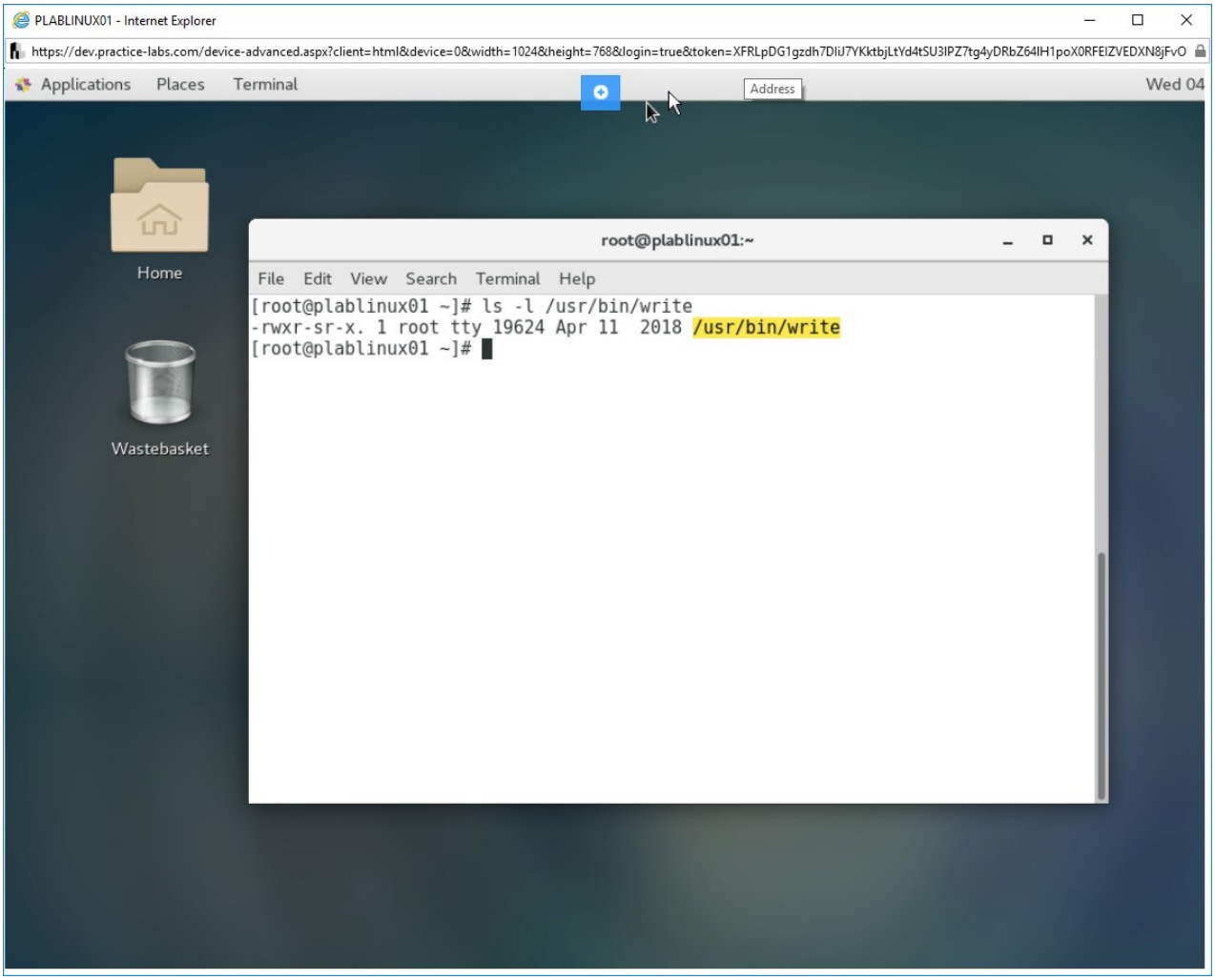


Figure 1.3 Screenshot of PLABLINUX01: Showing the s in the permissions.

Step 4

Clear the screen by entering the following command:

```
clear
```

To find all SUID root files, type the following command:

```
find / -user root -perm -4000 -print
```

Press **Enter**.

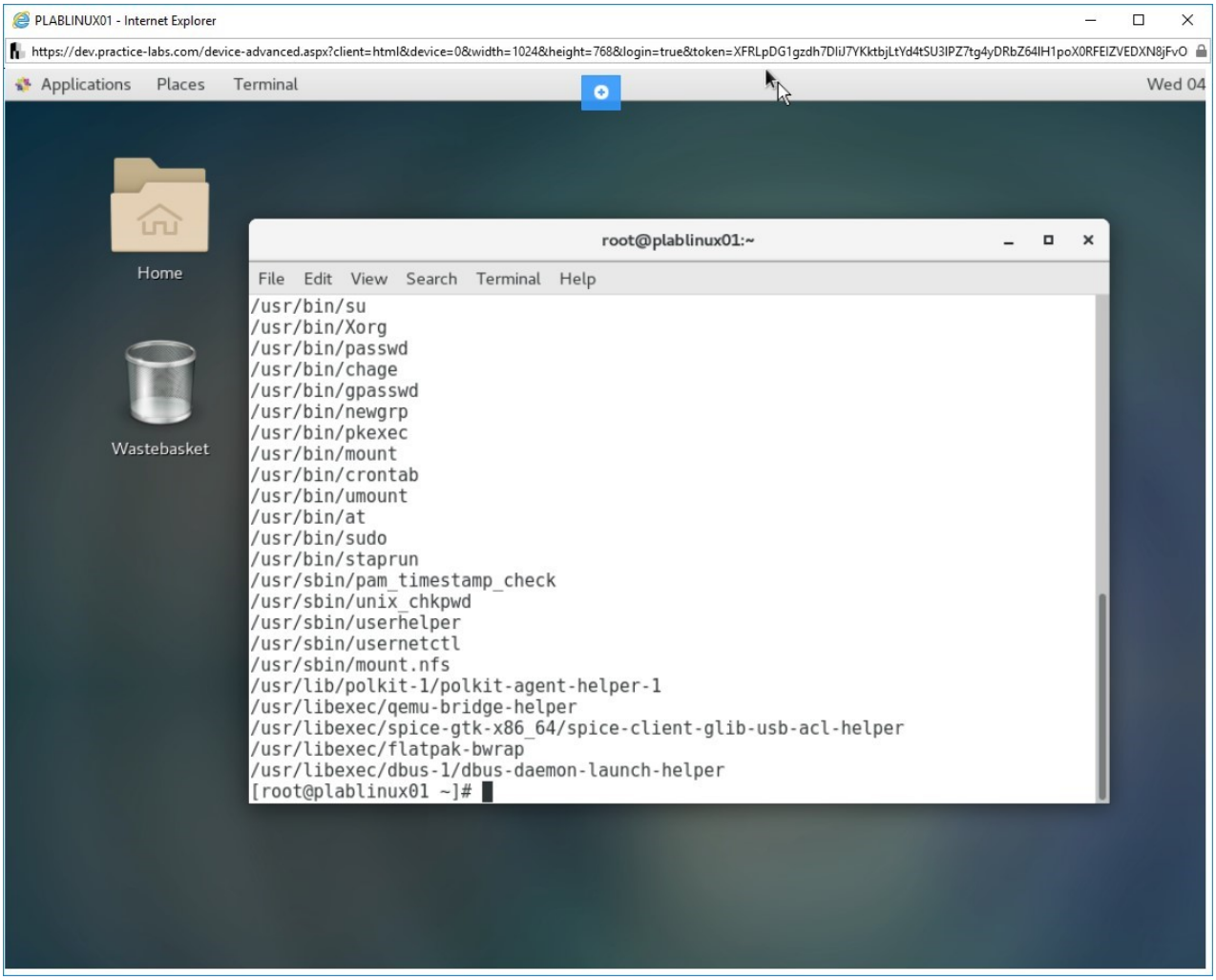


Figure 1.4 Screenshot of PLABLINUX01: Finding all SUID root files.

Step 5

Clear the screen by entering the following command:

```
clear
```

To find all SGID root files, type the following command:

```
find / -group root -perm -2000 -print
```

Press **Enter**.

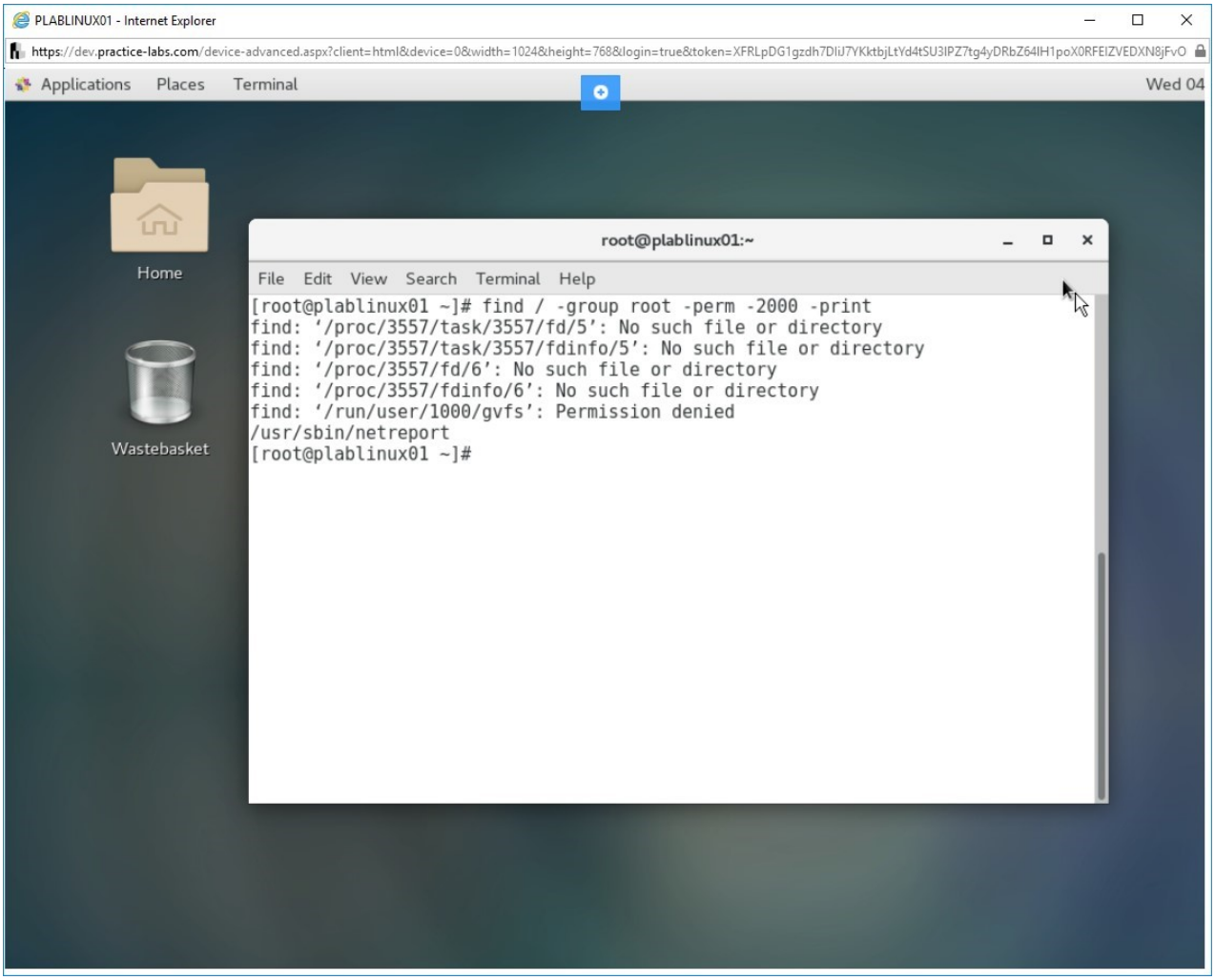


Figure 1.5 Screenshot of PLABLINUX01: Finding all the SGID root files.

Step 6

Clear the screen by entering the following command:

```
clear
```

To find all SUID and SGID files owned by anyone, type the following command:

```
find / -perm -4000 -o -perm -2000 -print
```

Press **Enter**.

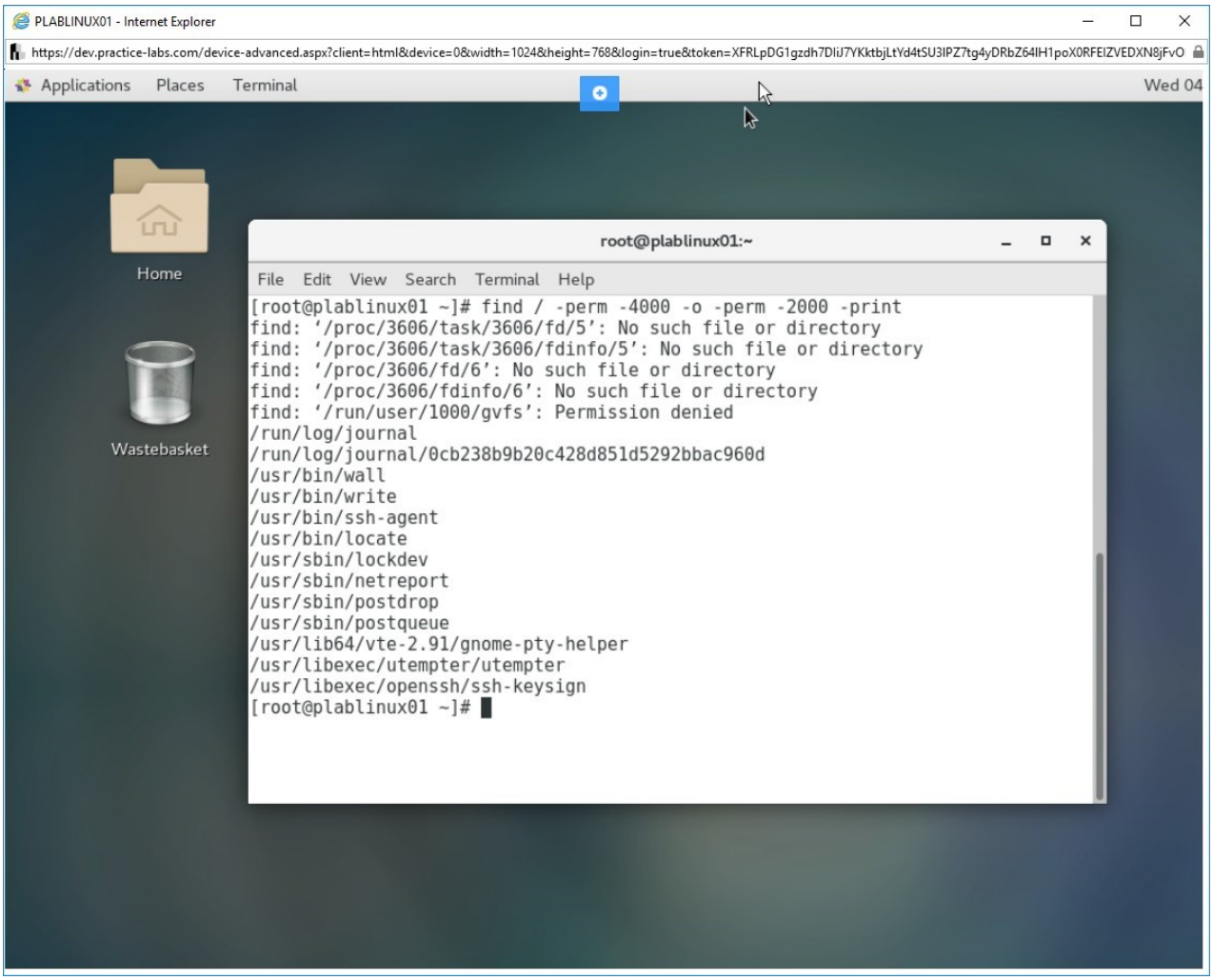


Figure 1.6 Screenshot of PLABLINUX01: Finding all the SUID and SGID files owned by anyone.

Task 2 - Manage User Passwords and Password-Aging Information

To set or change user passwords and password-aging information, perform the following steps:

Step 1

Ensure that you are connected to **PLABLINUX01** and the terminal window is open. Clear the screen by entering the following command:

```
clear
```

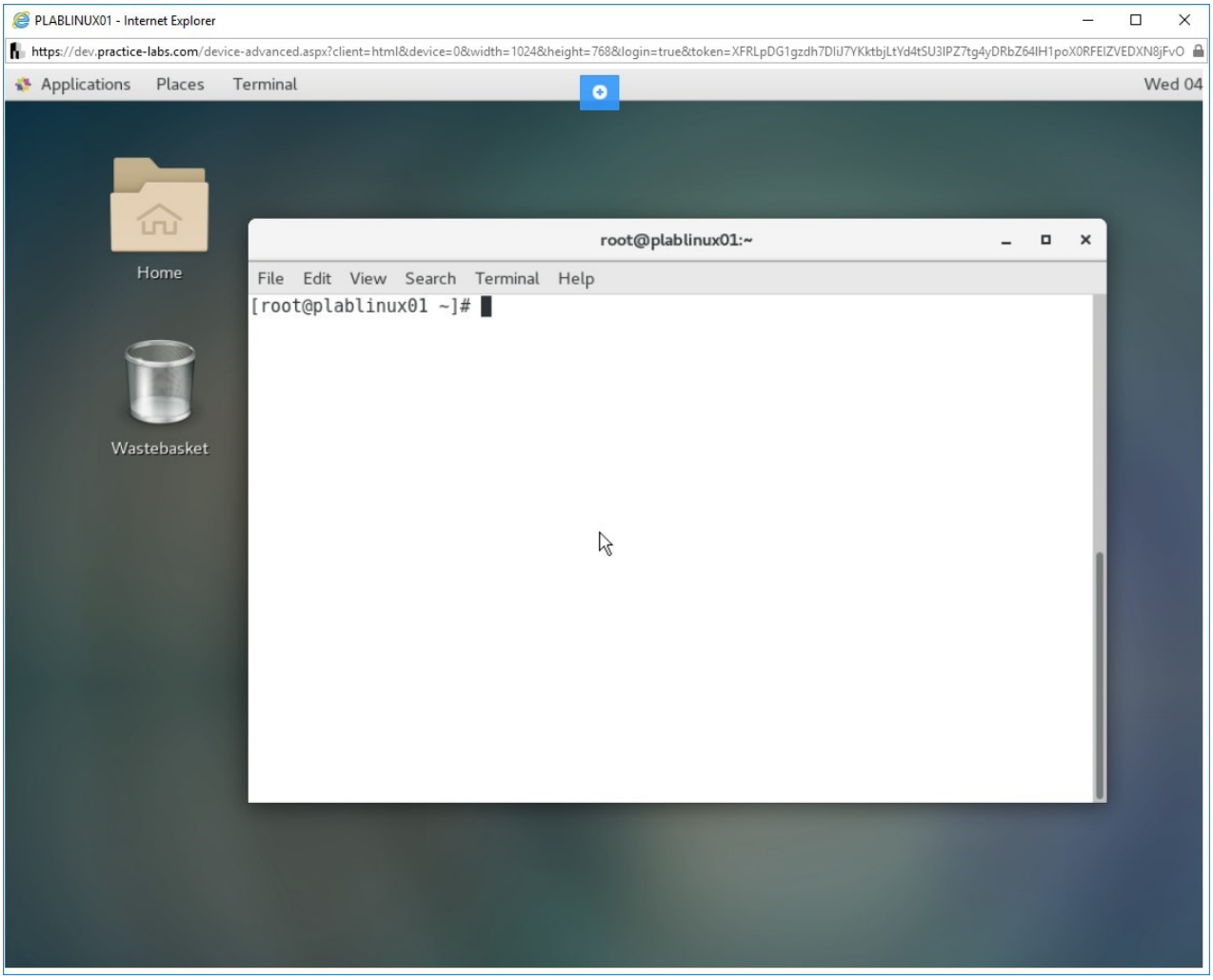


Figure 1.7 Screenshot of PLABLINUX01: Clearing the window.

Step 2

Before proceeding ahead, let's first create a user account and set its password. To create a user, type the following command:

```
useradd john
```

Press **Enter**.

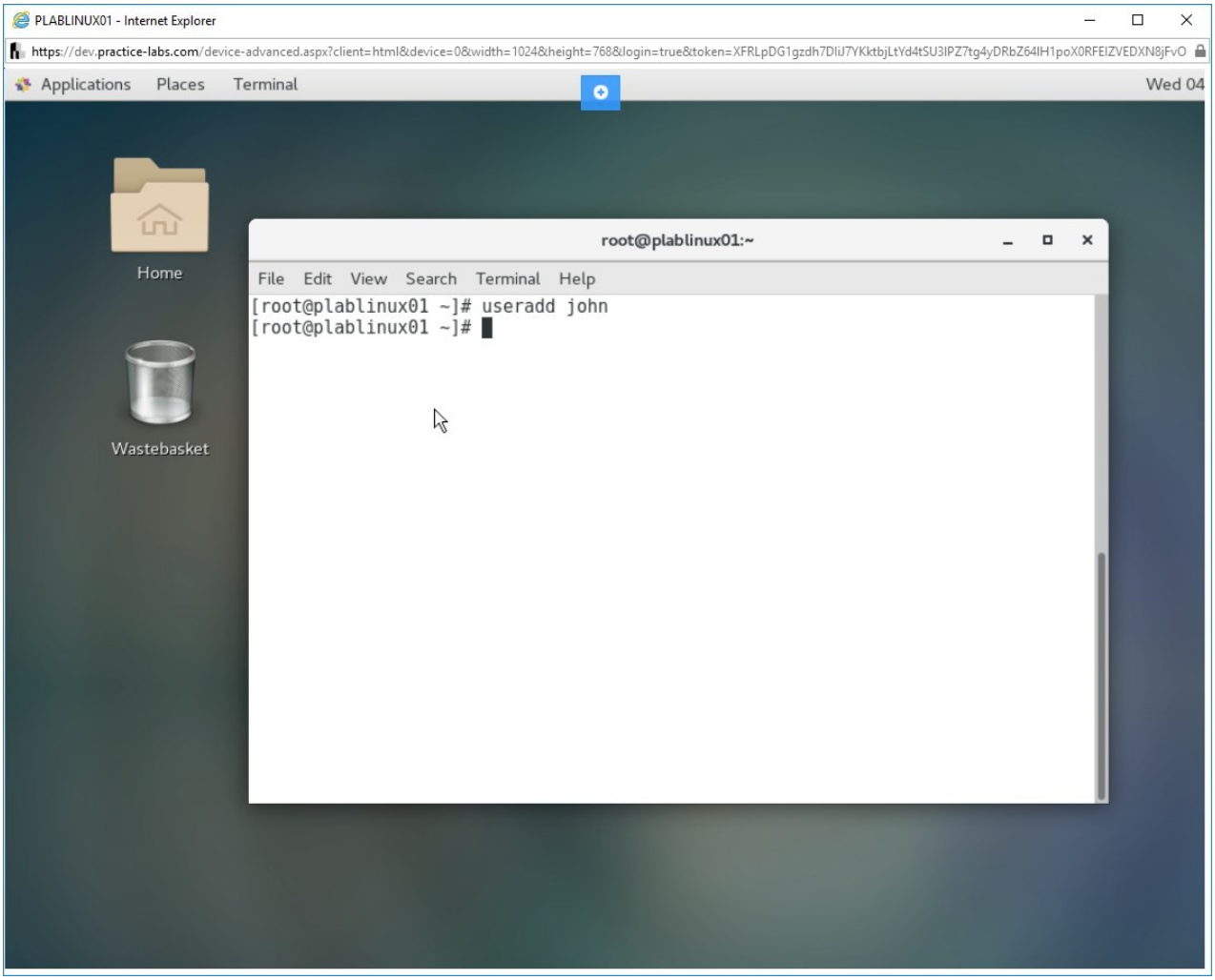


Figure 1.8 Screenshot of PLABLINUX01: Adding a user account.

Step 3

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

```
passwd john
```

Press **Enter**.

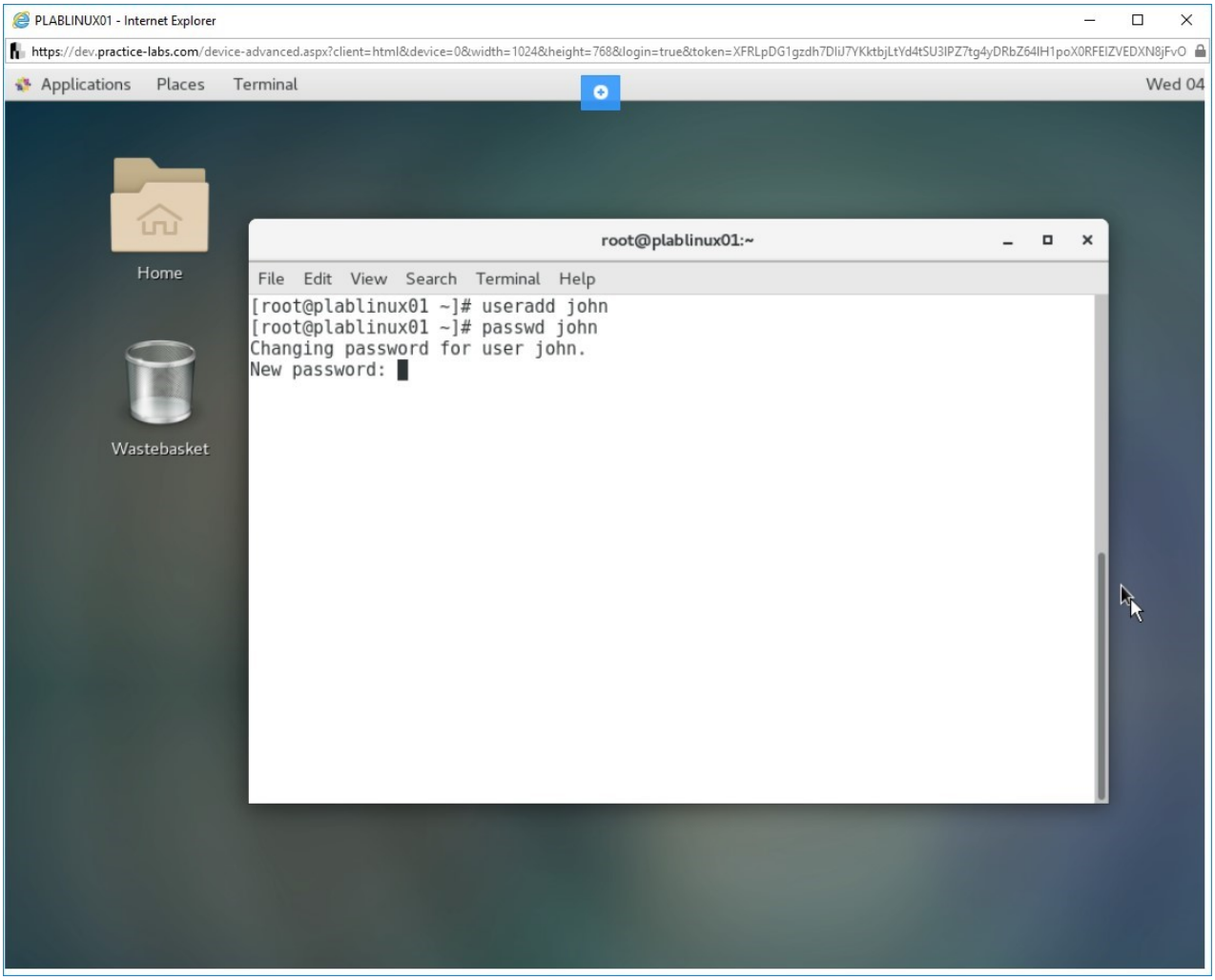


Figure 1.9 Screenshot of PLABLINUX01: Setting the password for the user.

Step 4

You are prompted to enter the password. Type the following password and then confirm the same:

`Passw0rd`

Press **Enter** after entering the password each time.

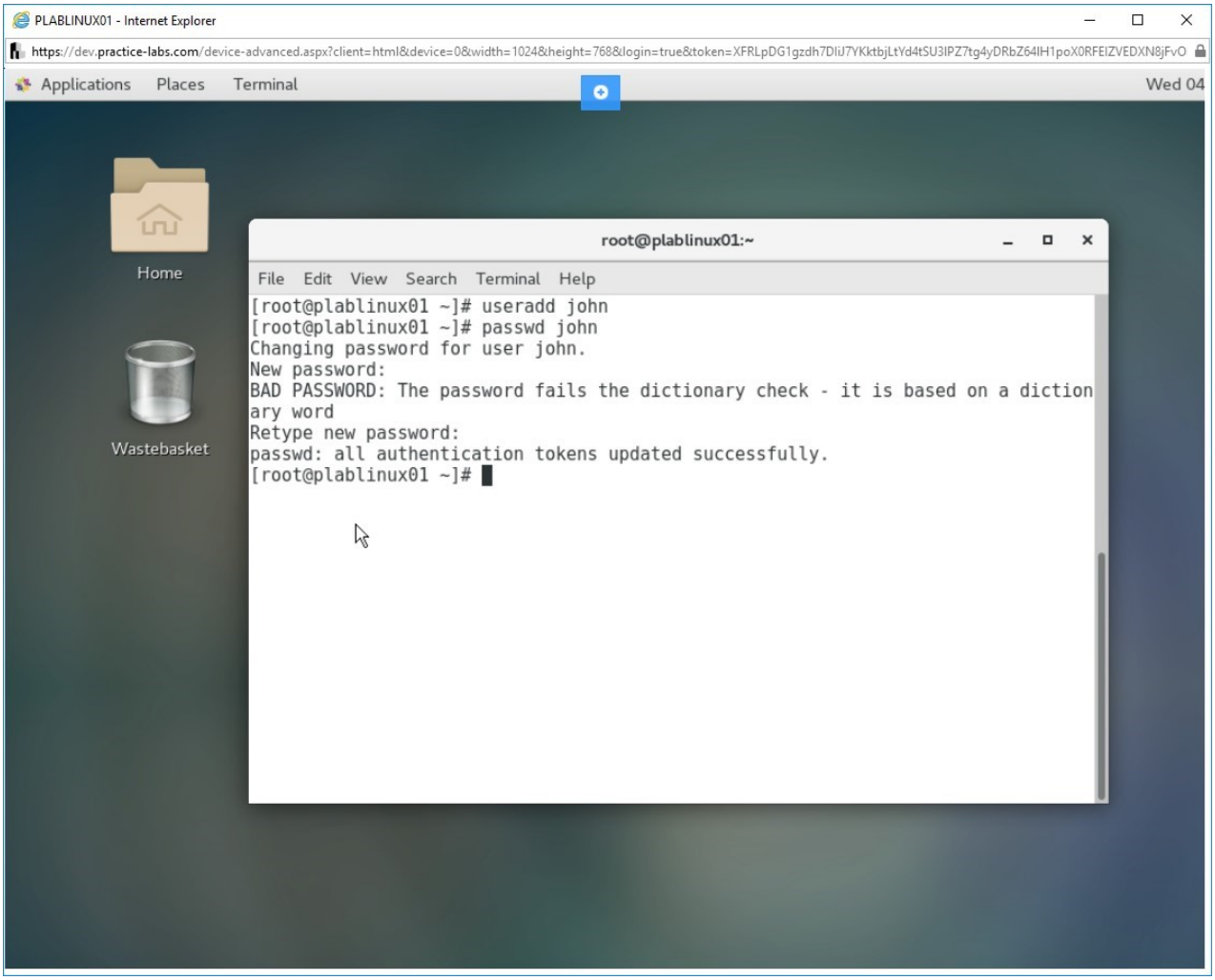


Figure 1.10 Screenshot of PLABLINUX01: Confirming the password for the user john.

Step 5

You will now modify the user account, **john**, and set the expiration date. 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**.

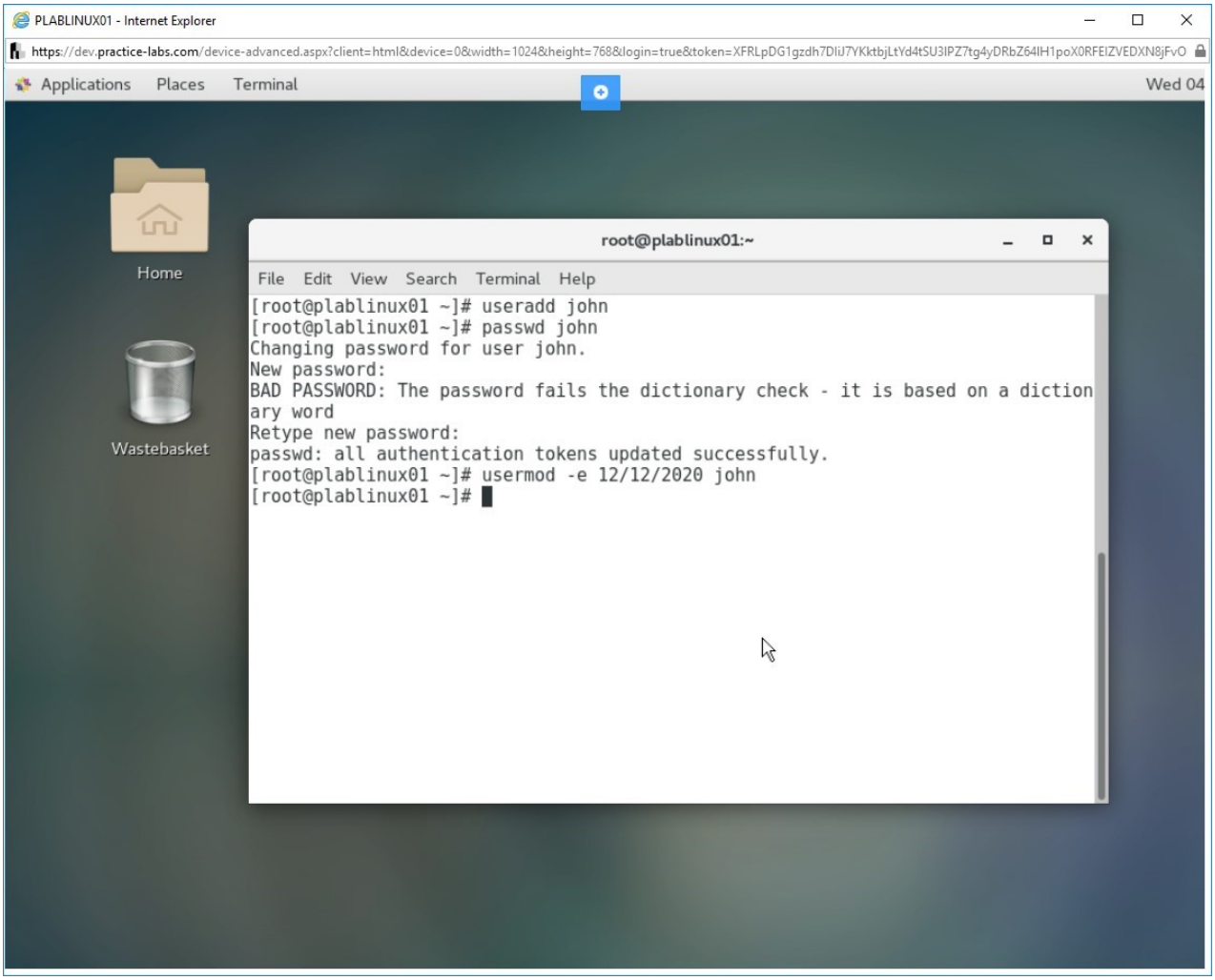


Figure 1.11 Screenshot of PLABLINUX01: Setting the password for the user account.

Step 6

Using this 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**.

Alert: Before proceeding, unlock the useraccount john. You can use the following command: ***usermod -U john***
You will require this user account later in the exercise.

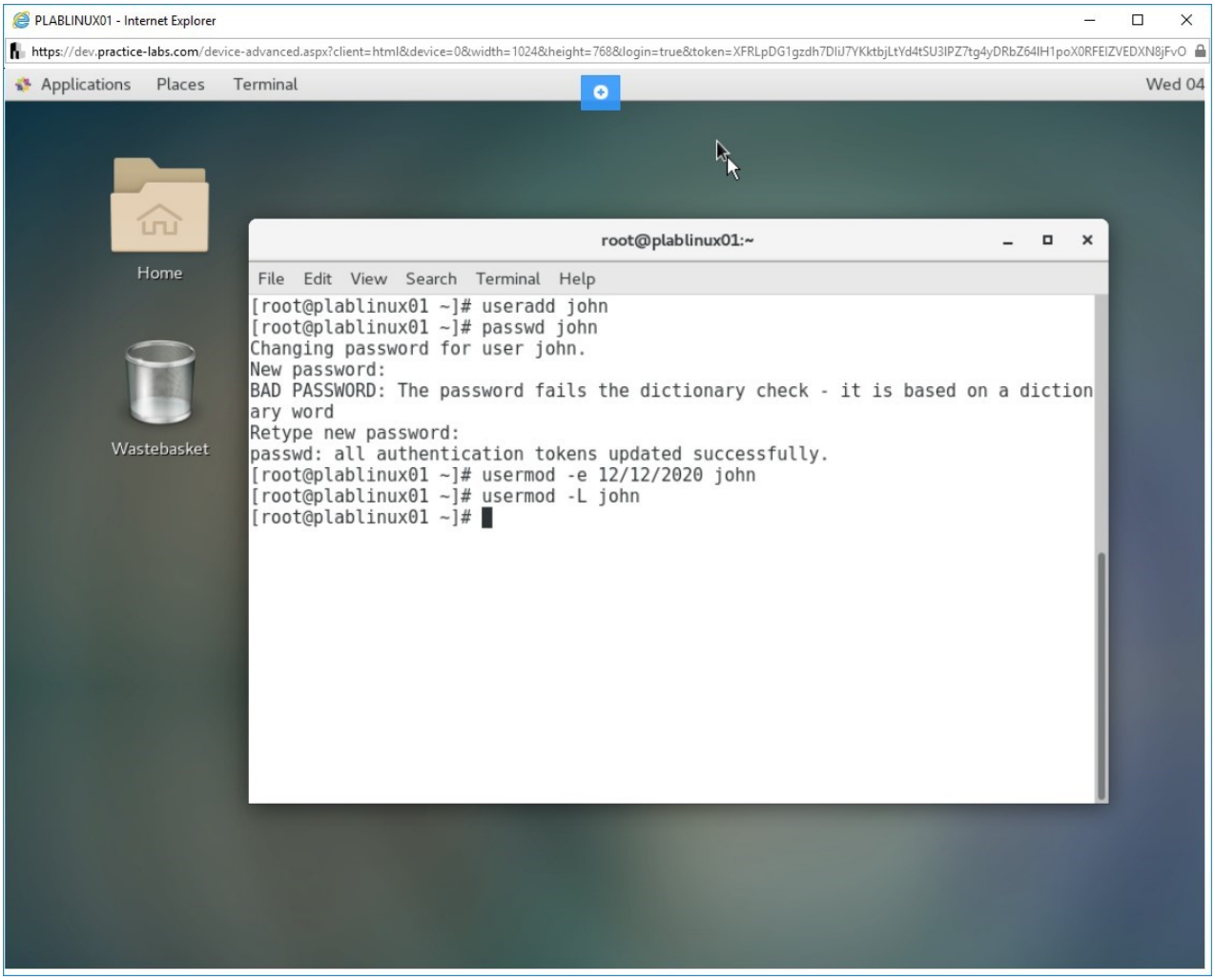


Figure 1.12 Screenshot of PLABLINUX01: Locking a user account.

Step 7

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**.

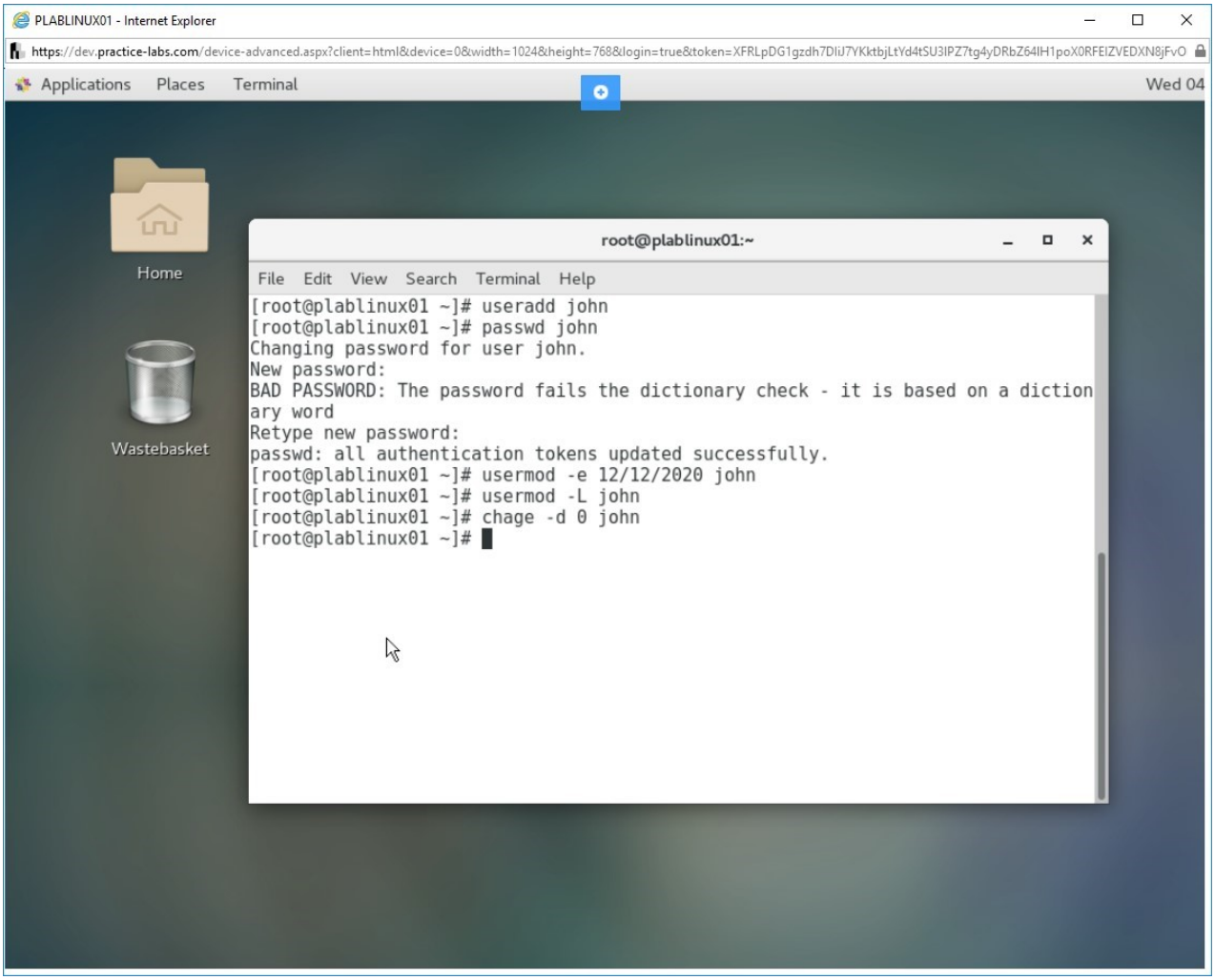


Figure 1.13 Screenshot of PLABLINUX01: Forcing an immediate user expiration.

Task 3 - List the Users Logged into the System

To determine which users have logged in to the system or are currently logged in, perform the following steps:

Step 1

Clear the screen by entering the following command:

```
clear
```

There will be situations when you want to determine the users who are currently logged into the system or had logged in.

To view the current logged on users, type the following command:

```
who
```

Press **Enter**.

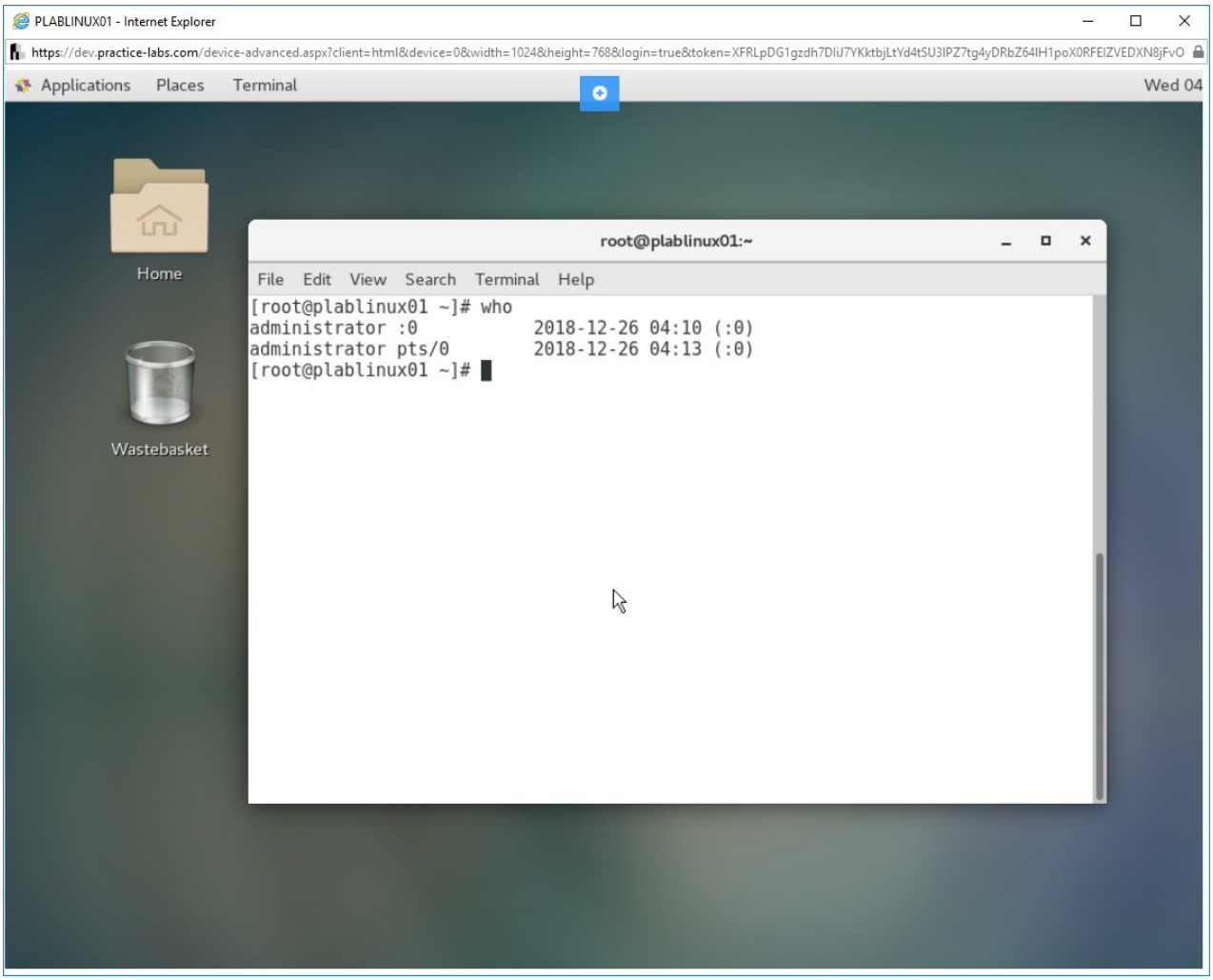


Figure 1.14 Screenshot of PLABLINUX01: Viewing the current logged on users.

Step 2

The w command shows who is logged in and what they are doing. Type the following command:

```
w
```

Press **Enter**.

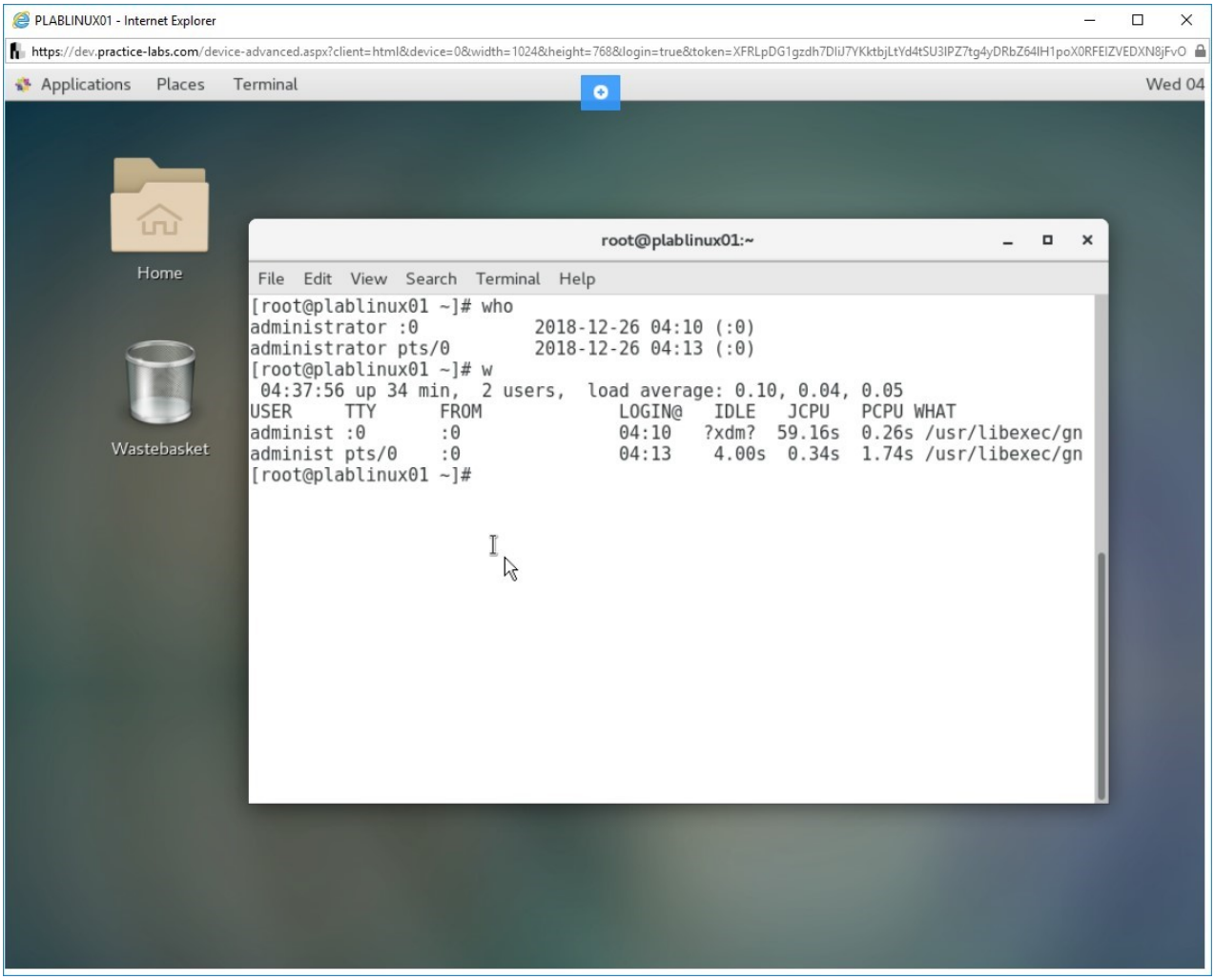


Figure 1.15 Screenshot of PLABLINUX01: Showing the current logged in users.

Step 3

Clear the screen by entering the following command:

```
clear
```

You can also view the recent logins done by all users. Type the following command:

```
last
```

Press **Enter**.

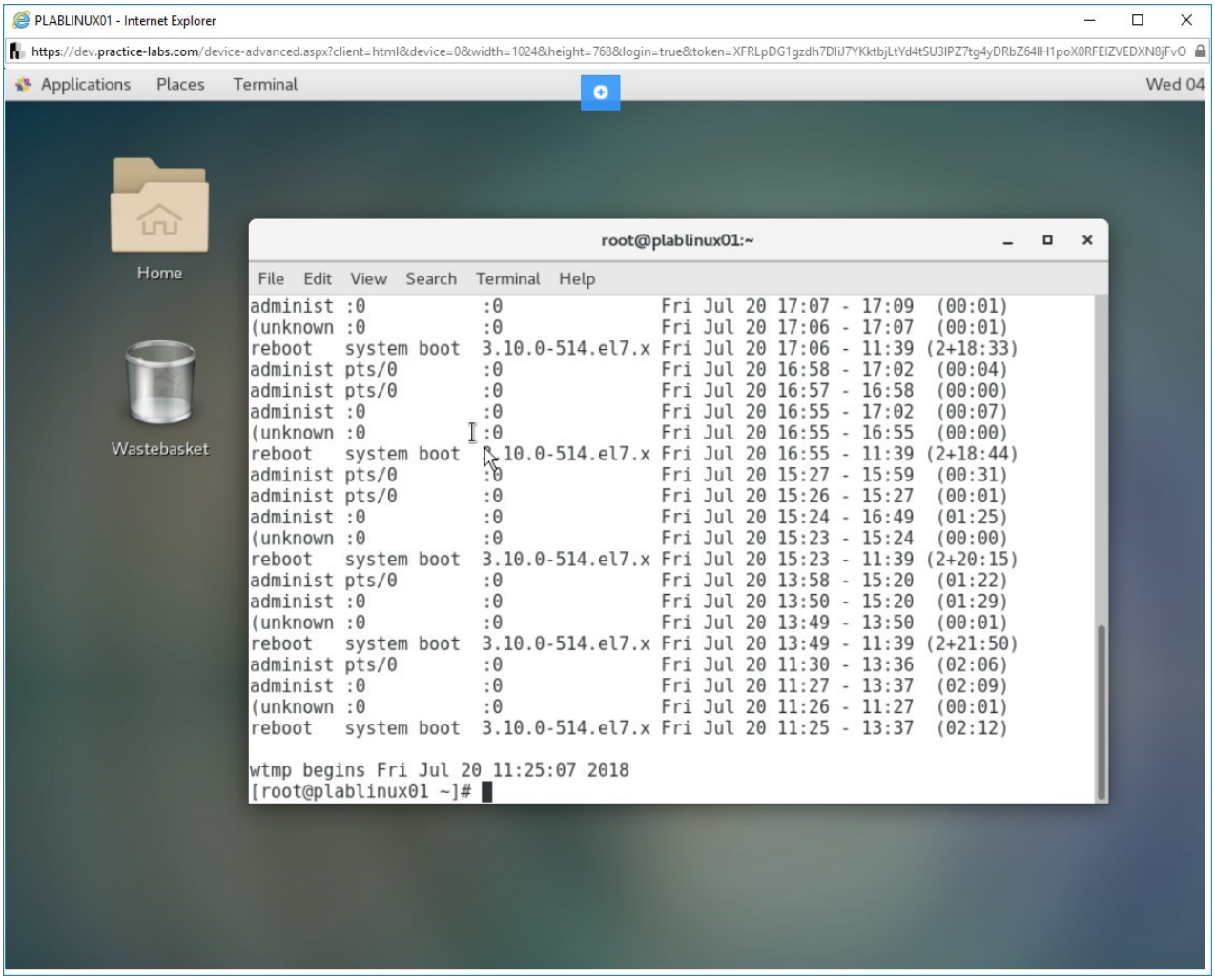


Figure 1.16 Screenshot of PLABLINUX01: Viewing the recent logins performed by the users.

Step 4

Clear the screen by entering the following command:

```
clear
```

You can also view the users who logged in last so many days.

For example, you want to view, which users have logged in the last 100 days. Type the following command:

```
lastlog -b 0 -t 100
```

Press **Enter**.

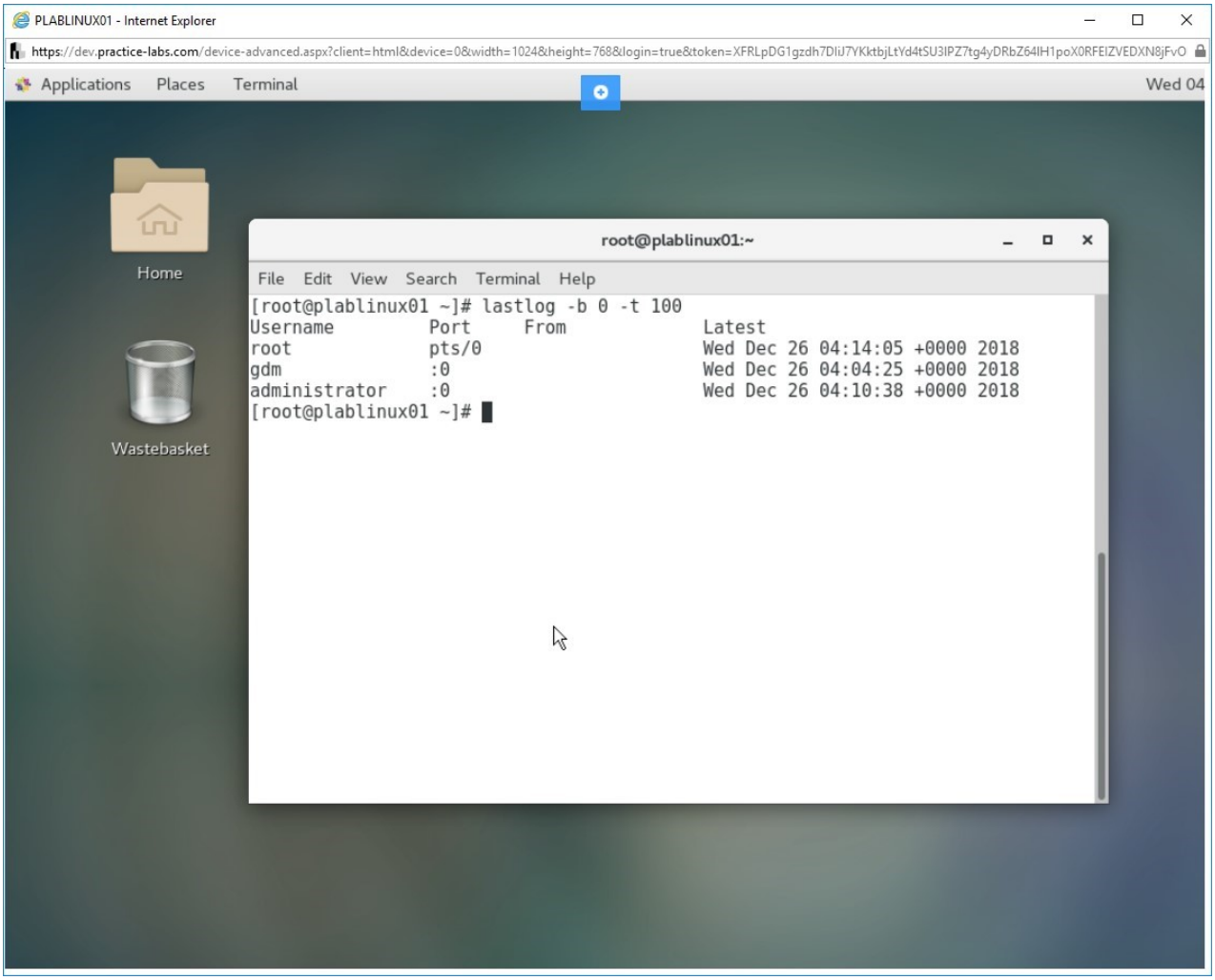


Figure 1.17 Screenshot of PLABLINUX01: Displaying the users who logged in last 100 days.

Task 4 - Use the su Command to Provide Privileges

The **su** command is used for providing root privileges to the users who do not have root privileges. In this task, you will learn the usage of the **su** command.

To use **su** command, perform the following steps.

Step 1

Ensure that you are connected to **PLABLINUX01** and the terminal window is open. Clear the screen by entering the following command:

```
clear
```

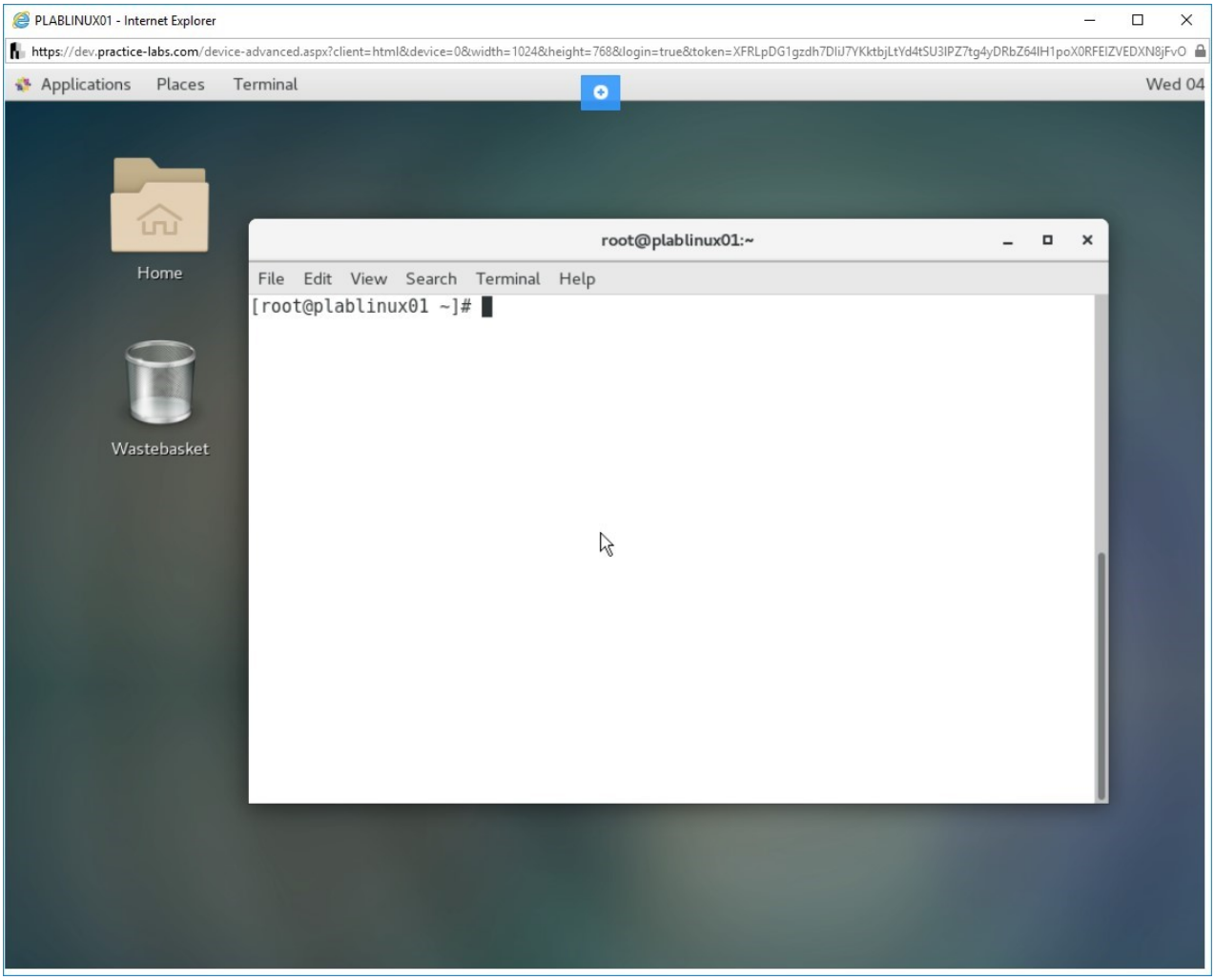


Figure 1.18 Screenshot of PLABLINUX01: Clearing the terminal window.

Step 2

Reboot the system by typing the following command and pressing **Enter**

```
reboot
```

When the system boots up, there are two users shown on the login screen. Click **john**.

> ***Note:*** *If you're logged in automatically as administrator after the reboot then go to the* ***power on/off symbol*** *in the top right corner, click* ***administrator****, click* ***Log Out*** *then click* ***Log Out*** *again.*

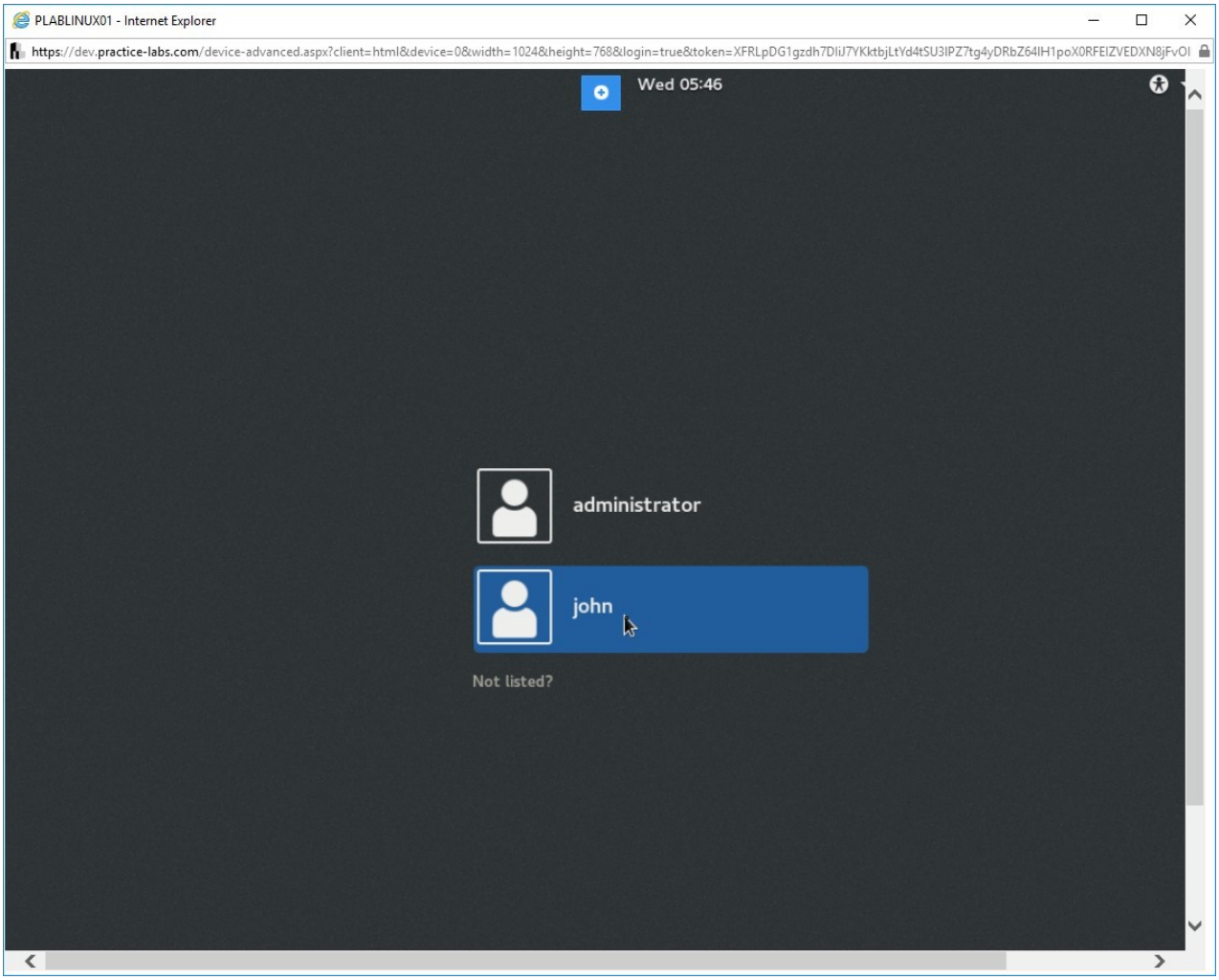


Figure 1.19 Screenshot of PLABLINUX01: Clicking the user john on the login window.

Step 3

In the **Password** text box, type the following password:

`Passw0rd`

Click **Sign In**.

> ***Note:*** *After clicking* ***Sign In*** *or pressing* ***Enter****, if you're required to change your password then enter* `Passw0rd` *again then you'll be asked to create a new password. What you change it to is entirely up to you but to stay safe, make sure it's at least 9 characters and include a capital letter and a number. You'll then be asked to retype your new password to login. Keep note of this password for later.*

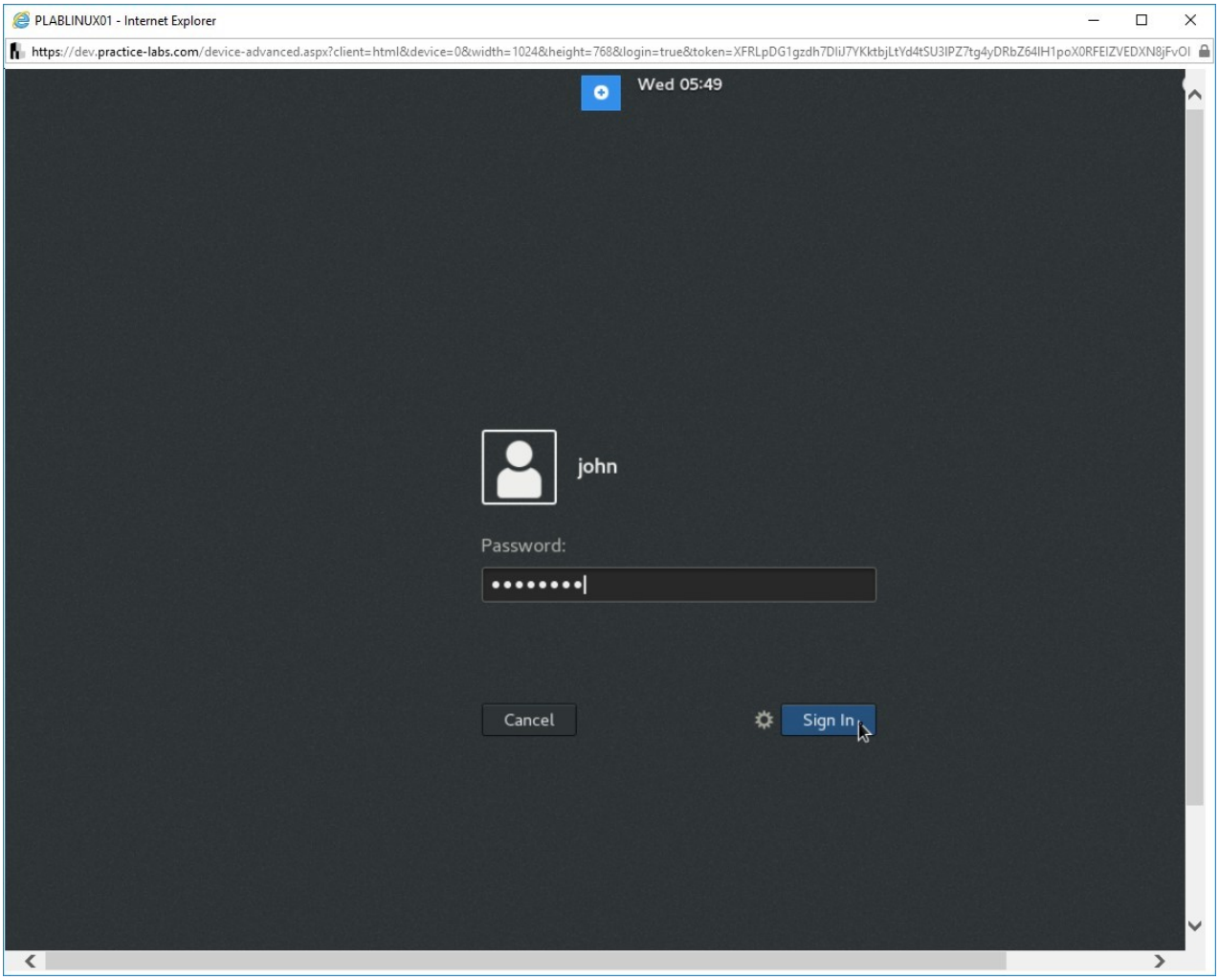


Figure 1.20 Screenshot of PLABLINUX01: Entering the password for the user john.

Step 4

On the **Welcome** screen, select **English (United States)** and click **Next**.

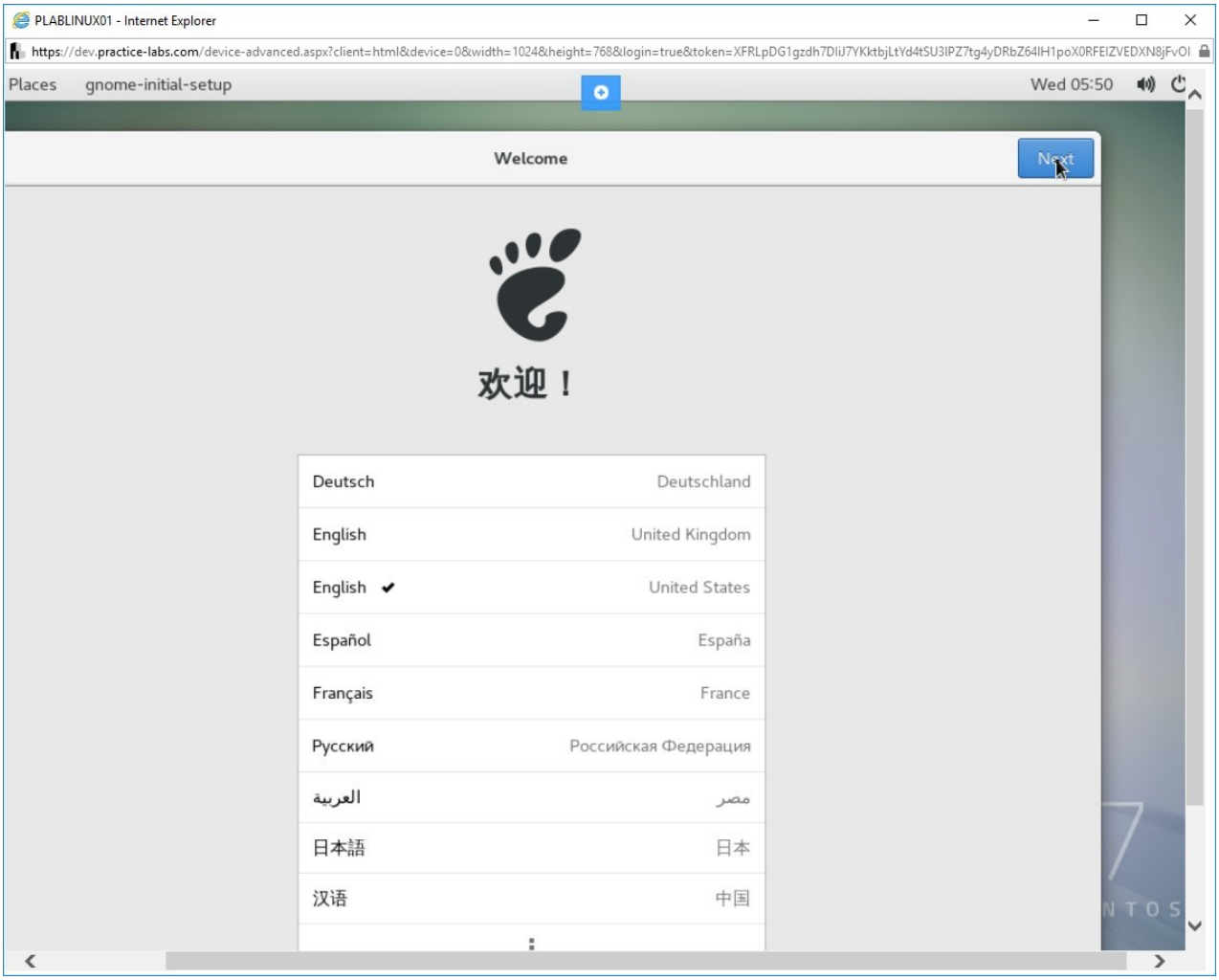


Figure 1.21 Screenshot of PLABLINUX01: Showing the Welcome screen post login.

Step 5

Ensure **English (US)** is selected on the **Typing** page. Click **Next**.

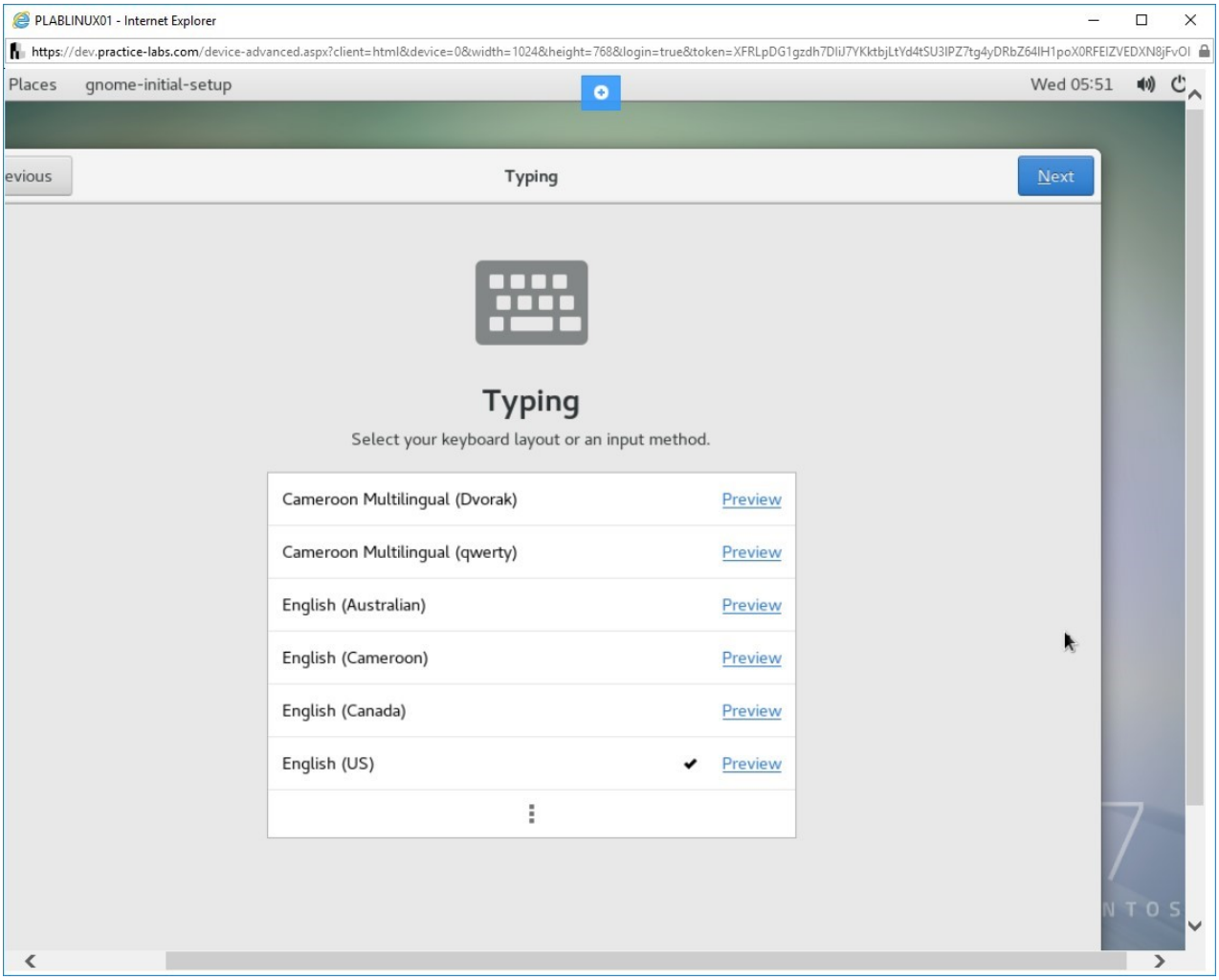


Figure 1.22 Screenshot of PLABLINUX01: Selecting English (US) as the login.

Step 6

On **Privacy** page, keep the default selection and click **Next**.

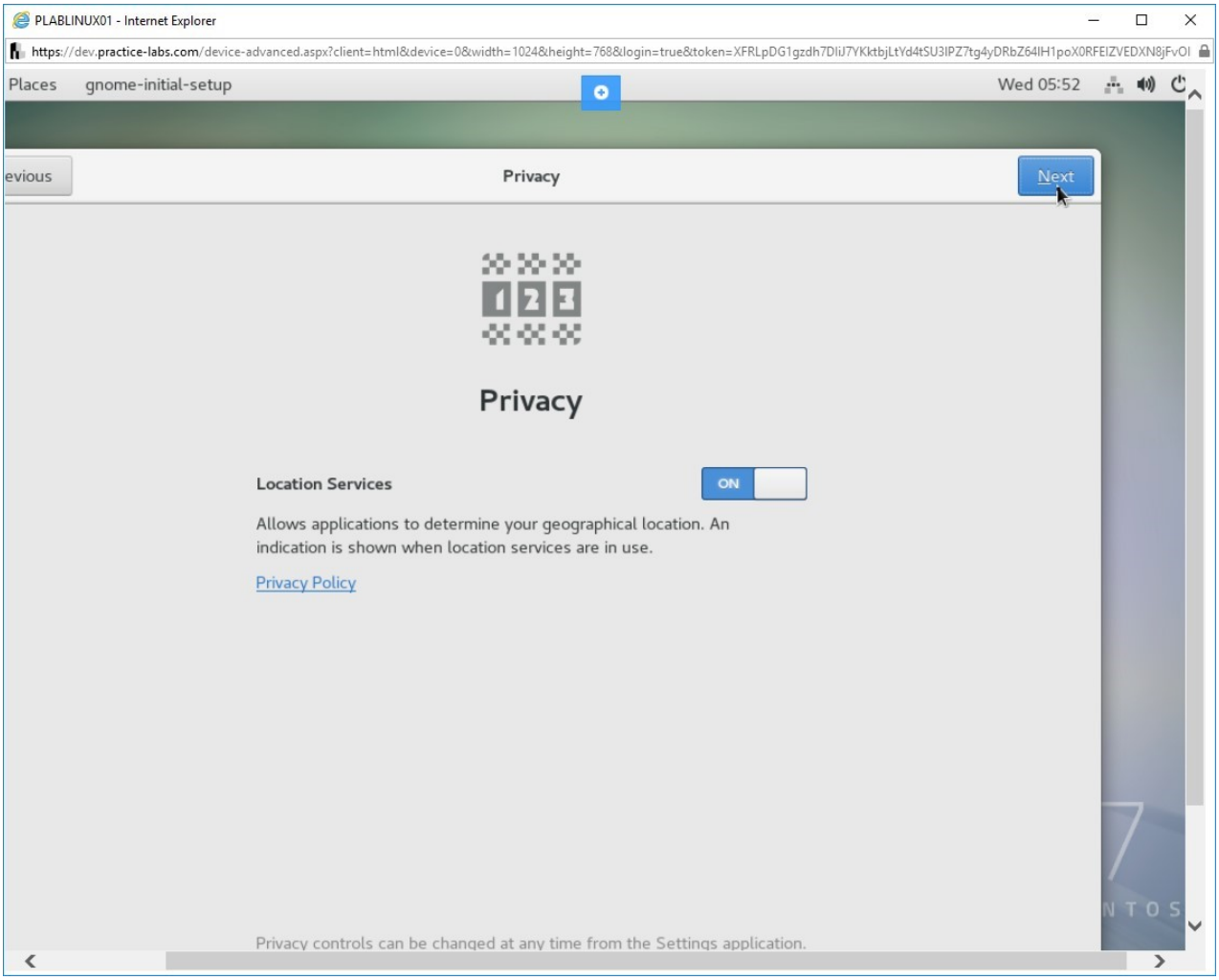


Figure 1.23 Screenshot of PLABLINUX01: Clicking Next on the Privacy page.

Step 7

If prompted for location access, click **Deny Access**. If not, move on to Step 8.

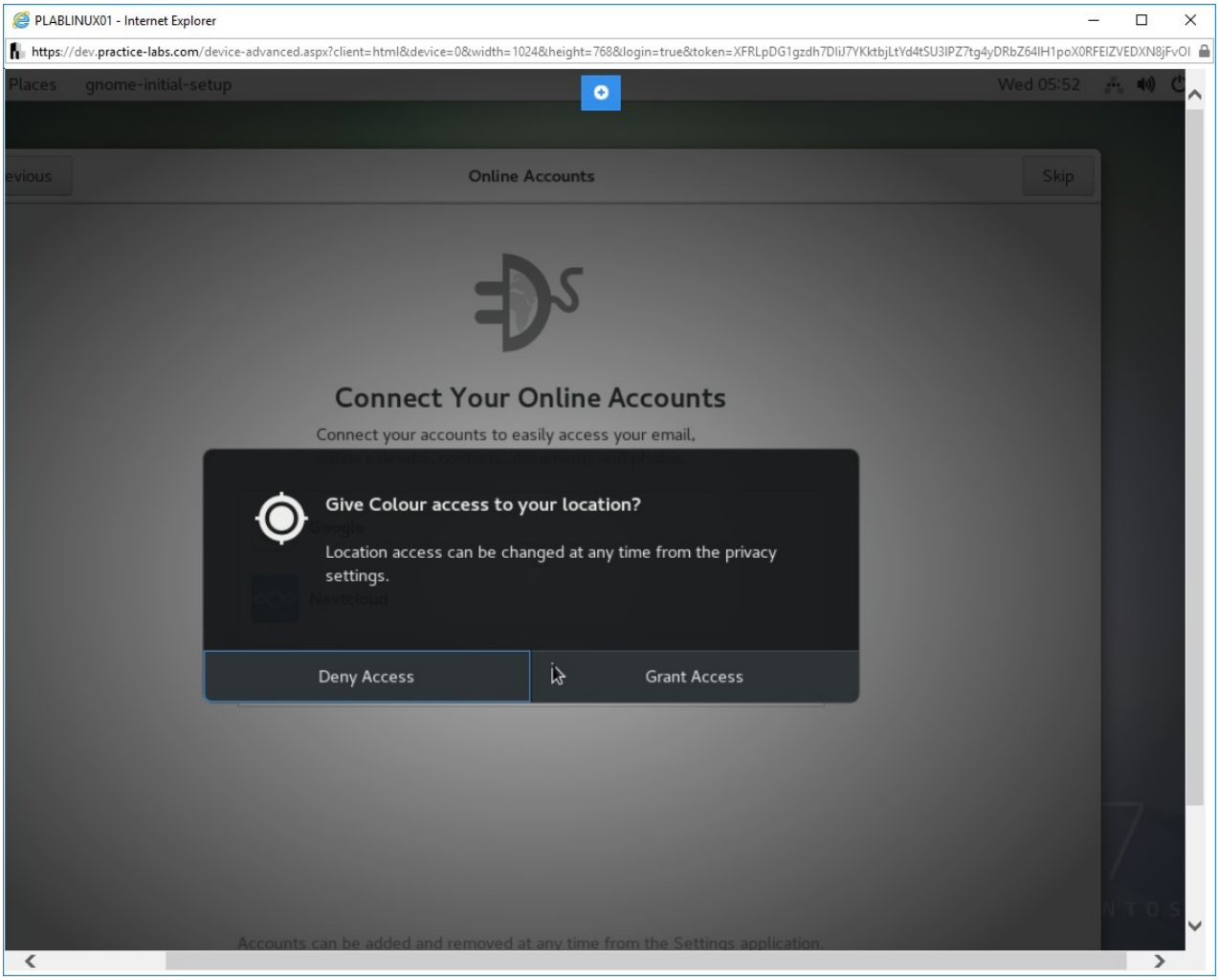


Figure 1.24 Screenshot of PLABLINUX01: Selecting Deny Access on the location prompt.

Step 8

On the **Connect Your Online Accounts** page, click **Skip**.

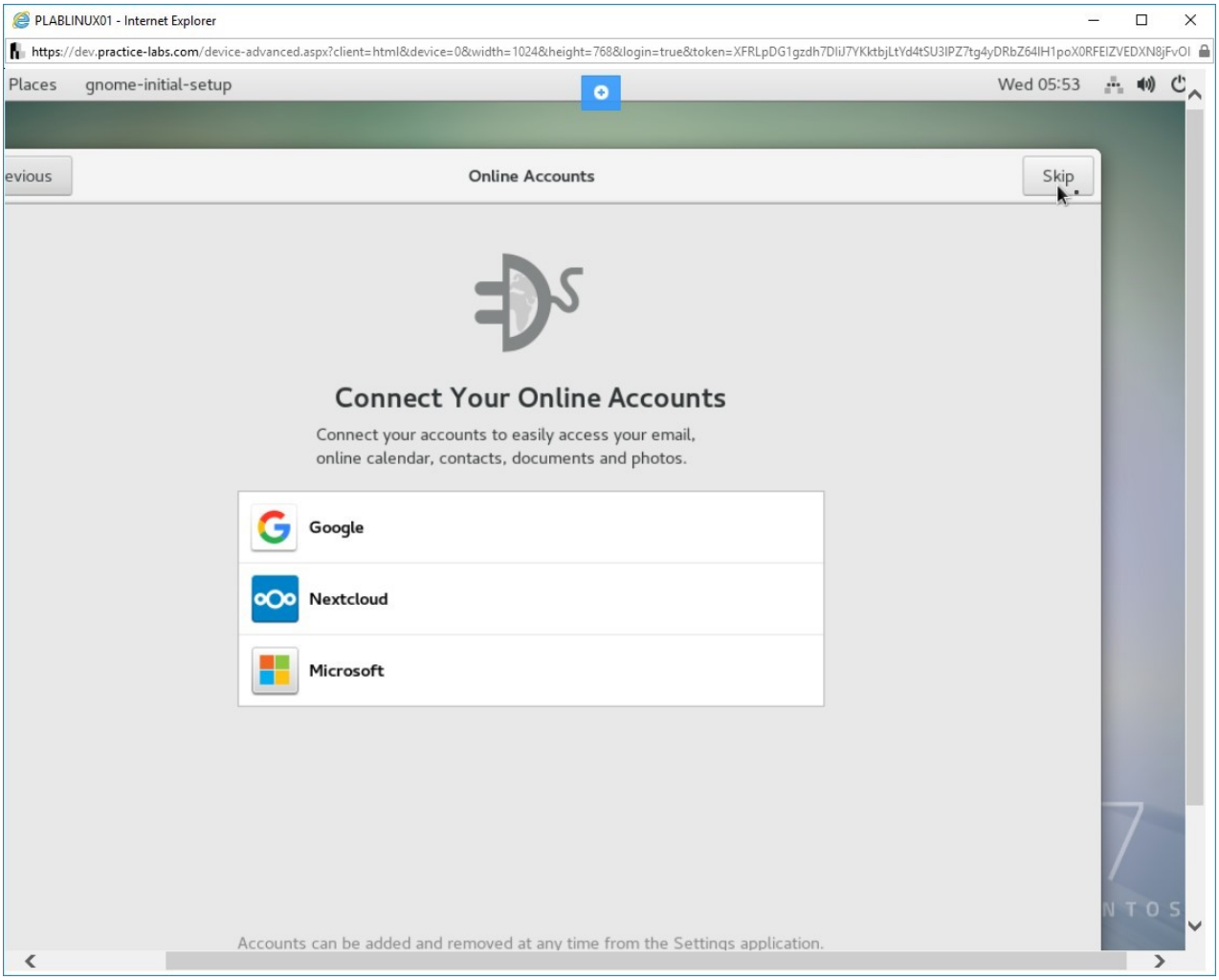


Figure 1.25 Screenshot of PLABLINUX01: Clicking Skip on the Connect Your Online Accounts.

Step 9

On the **You're ready to go!** page, click **Start** using **CentOS Linux**

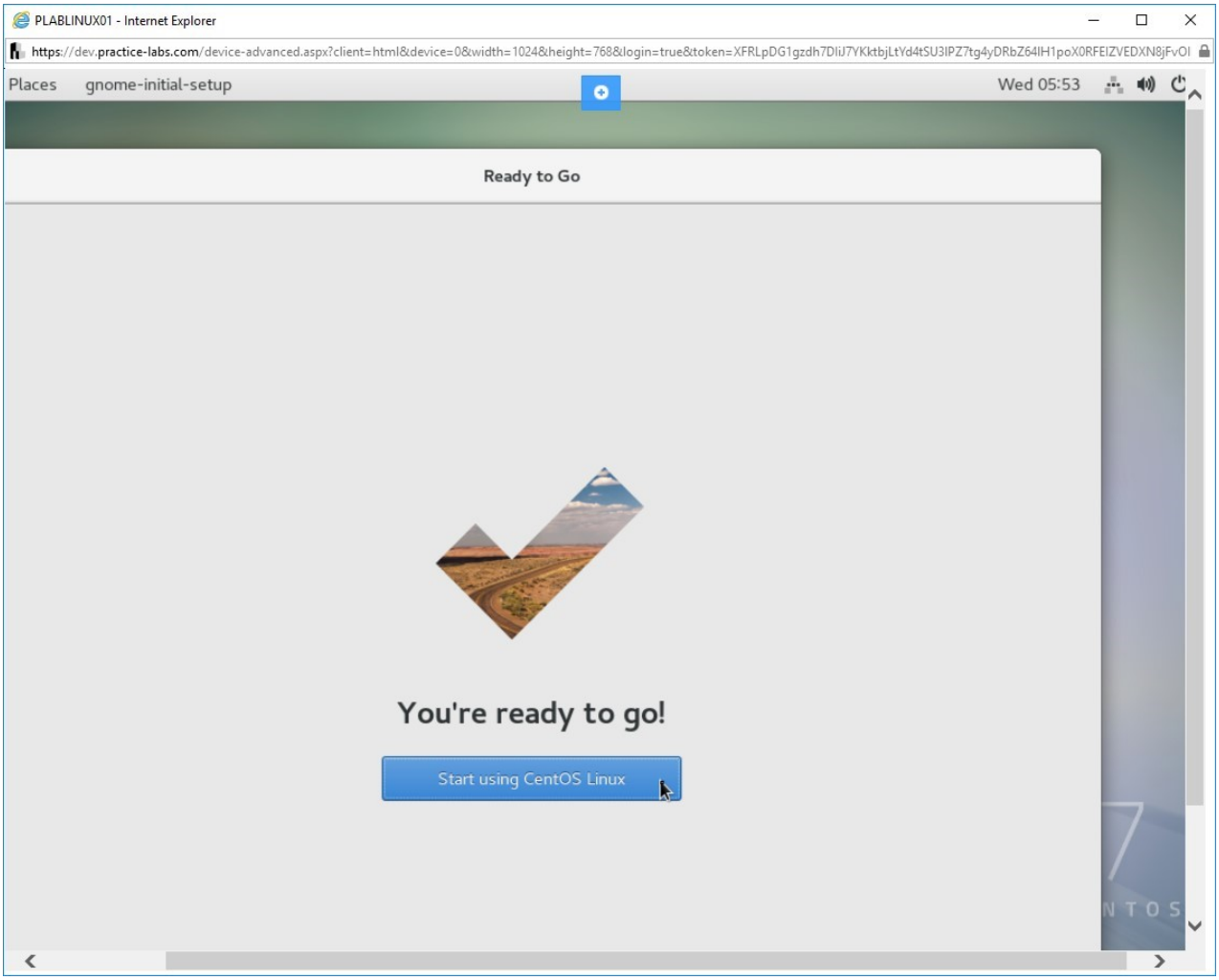


Figure 1.26 Screenshot of PLABLINUX01: Clicking Start using CentOS Linux on the You're ready to go! page.

Step 10

You are now on the desktop. Right-click on the desktop and select **Open Terminal**.

> ***Note:*** *If you see the help in the Web browser, simply close it.*

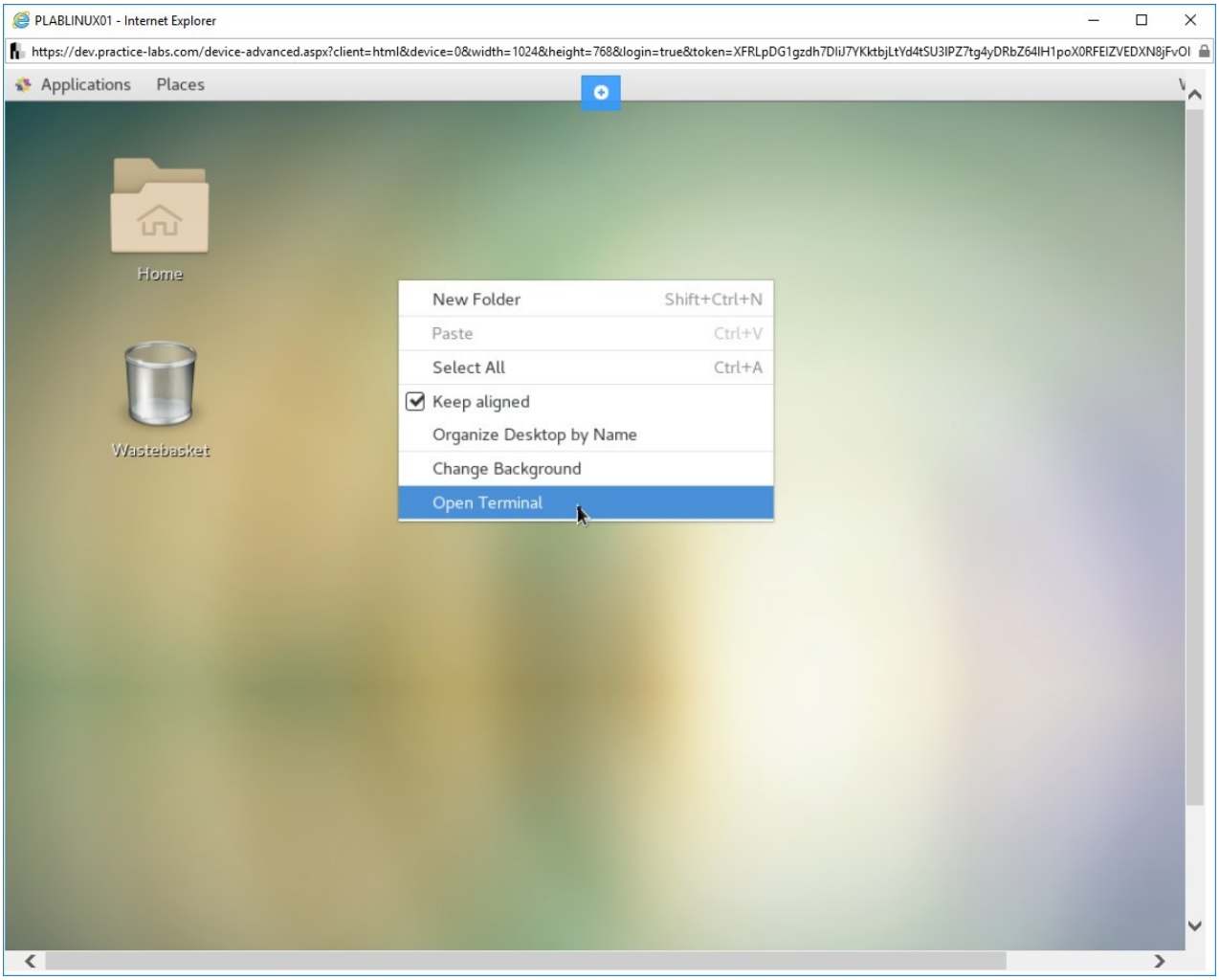


Figure 1.27 Screenshot of PLABLINUX01: Selecting the Open Terminal option from the context menu.

Step 11

You should now see the following command prompt:

```
john@plablinux01
```

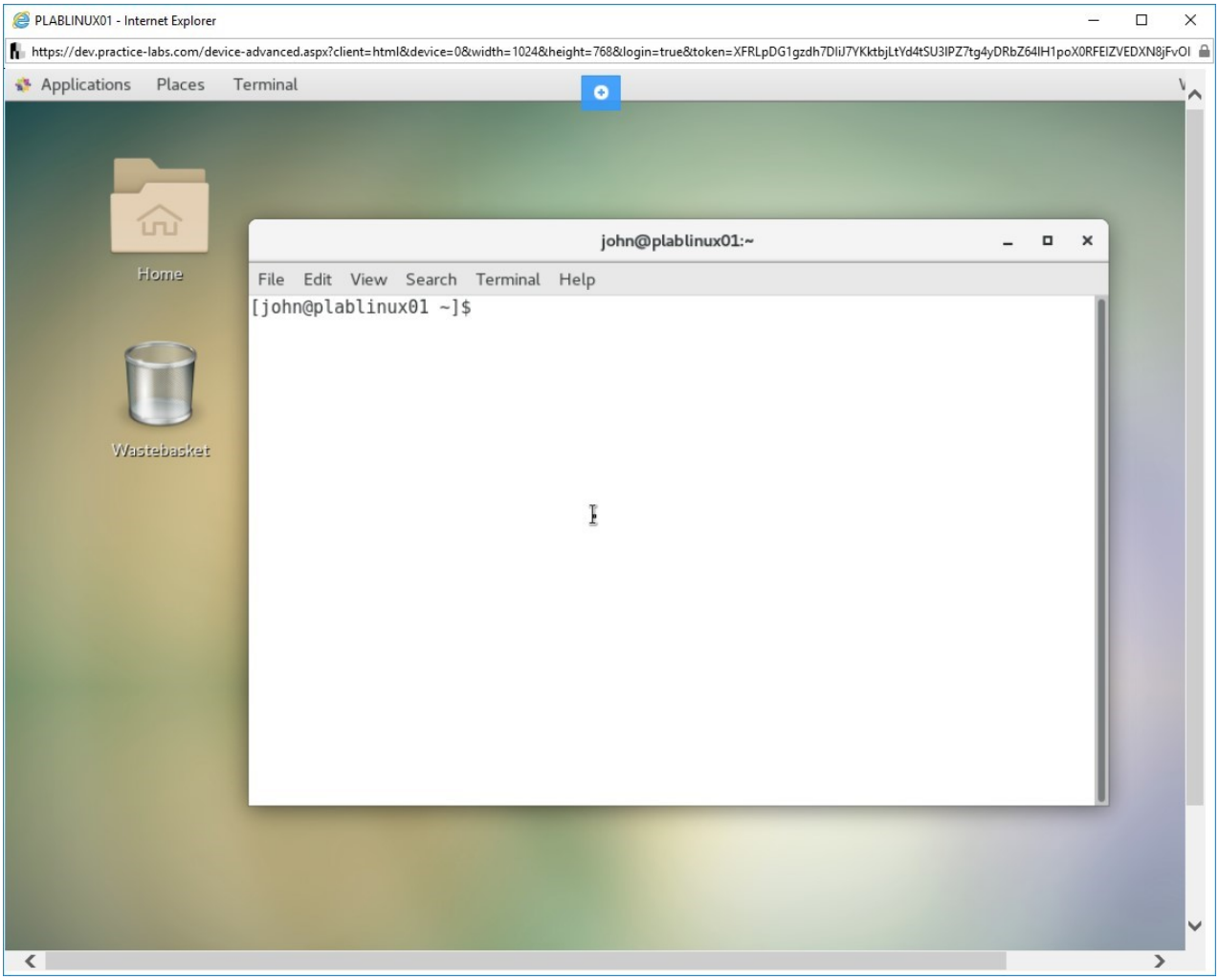


Figure 1.28 Screenshot of PLABLINUX01: Showing the command prompt in the terminal window.

Step 12

You can find the username. Type the following command:

```
whoami
```

Press **Enter**.

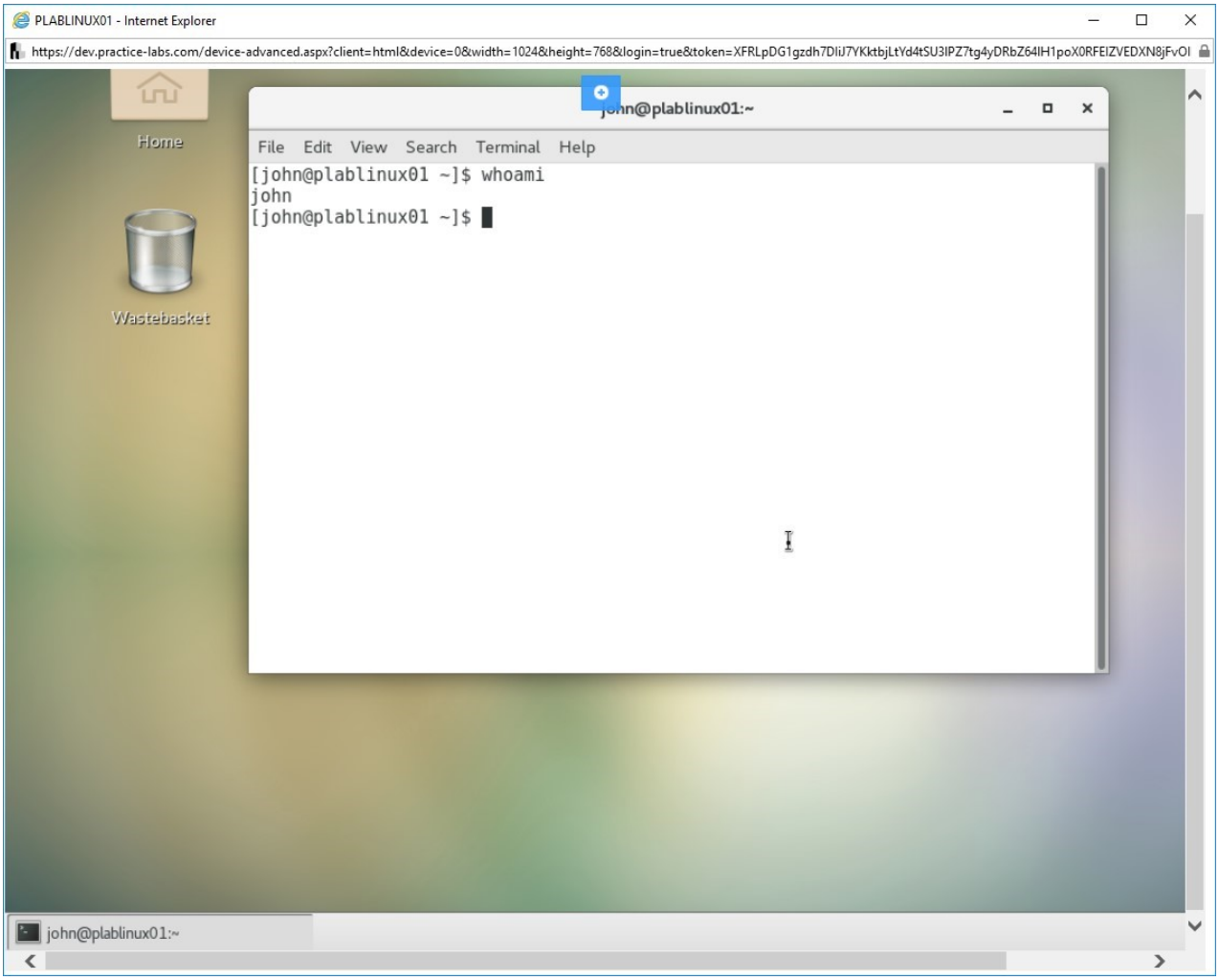


Figure 1.29 Screenshot of PLABLINUX01: Finding the username.

Step 13

Let's try to run a command that will require superuser privileges like **root**. Type the following command:

```
fdisk -l /dev/sda
```

Press **Enter**.

Note that you receive the **permission denied** error.

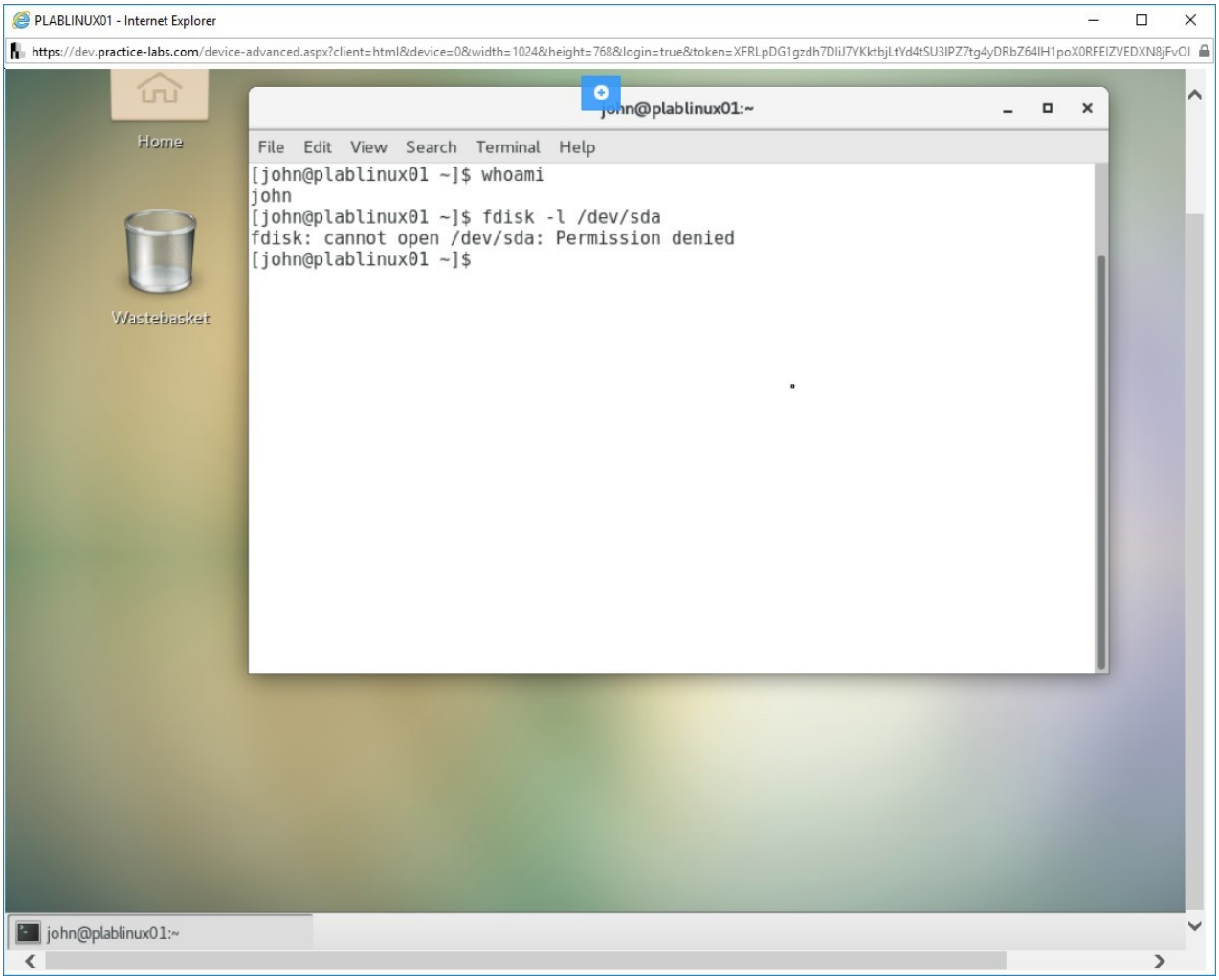


Figure 1.30 Screenshot of PLABLINUX01: Executing a command and receiving permission denied message.

Step 14

Let's use the su command to gain root privileges and then try this command. Type the following command:

```
su
```

Press **Enter**.

When prompted for the password, type the following:

```
Passw0rd
```

Press **Enter**.

The command prompt now mentions root.

> ***Note**: You can either use **su** or **su -**. There is a slight difference between both the commands. **su** with **-** (hyphen) tells the system to open a new shell that contains the **$PATH** environment as **root** does. The **$PATH** environment in **root** shell contains a few key directories that are used only by the **root** user. These directories are: **/sbin** and **/usr/sbin**.*

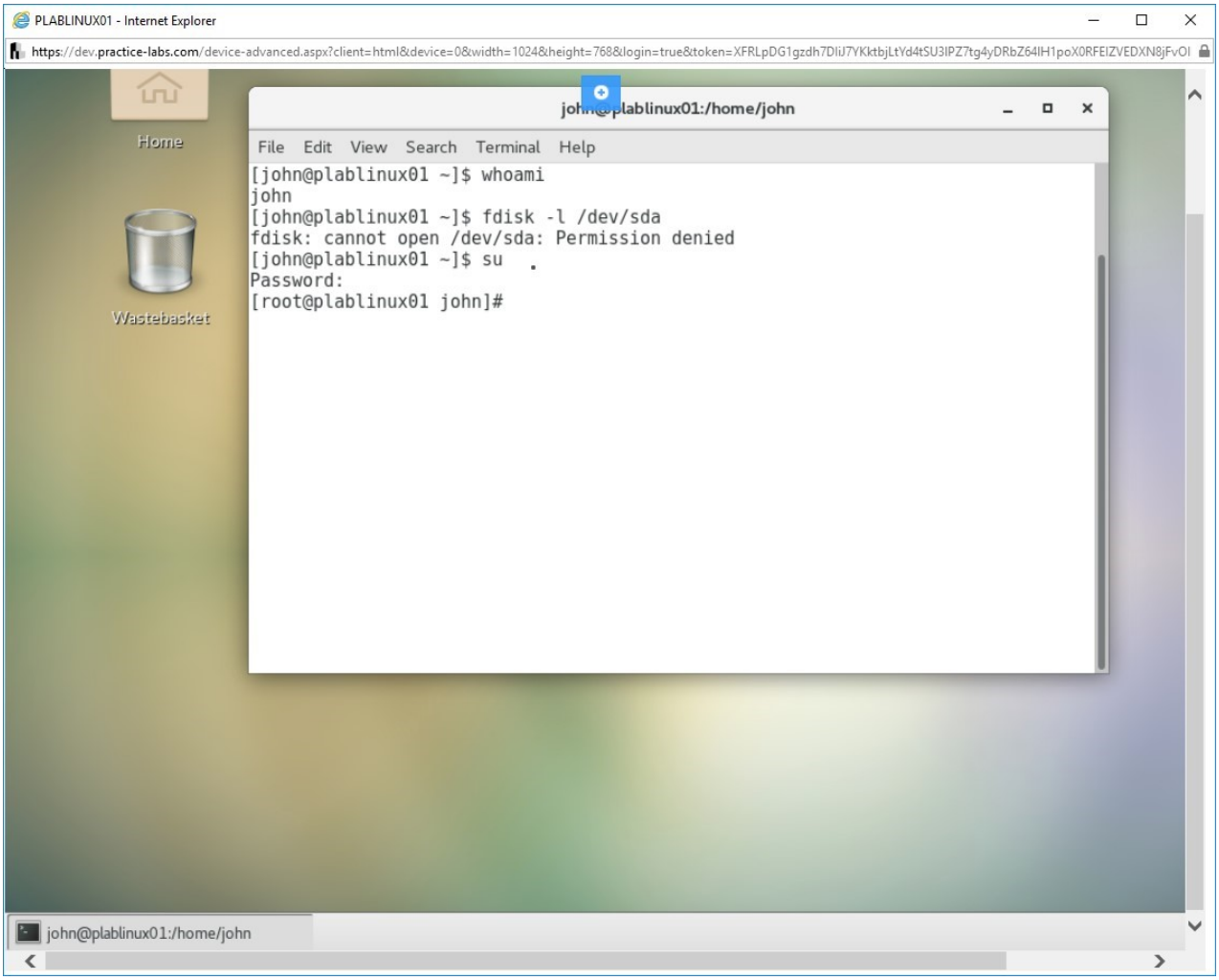


Figure 1.31 Screenshot of PLABLINUX01: Changing the account to the root account with the su command.

Step 15

Type the fdisk command once again:

```
fdisk -l /dev/sda
```

Press **Enter**.

Notice that the command displays the required results with the superuser privileges activated.

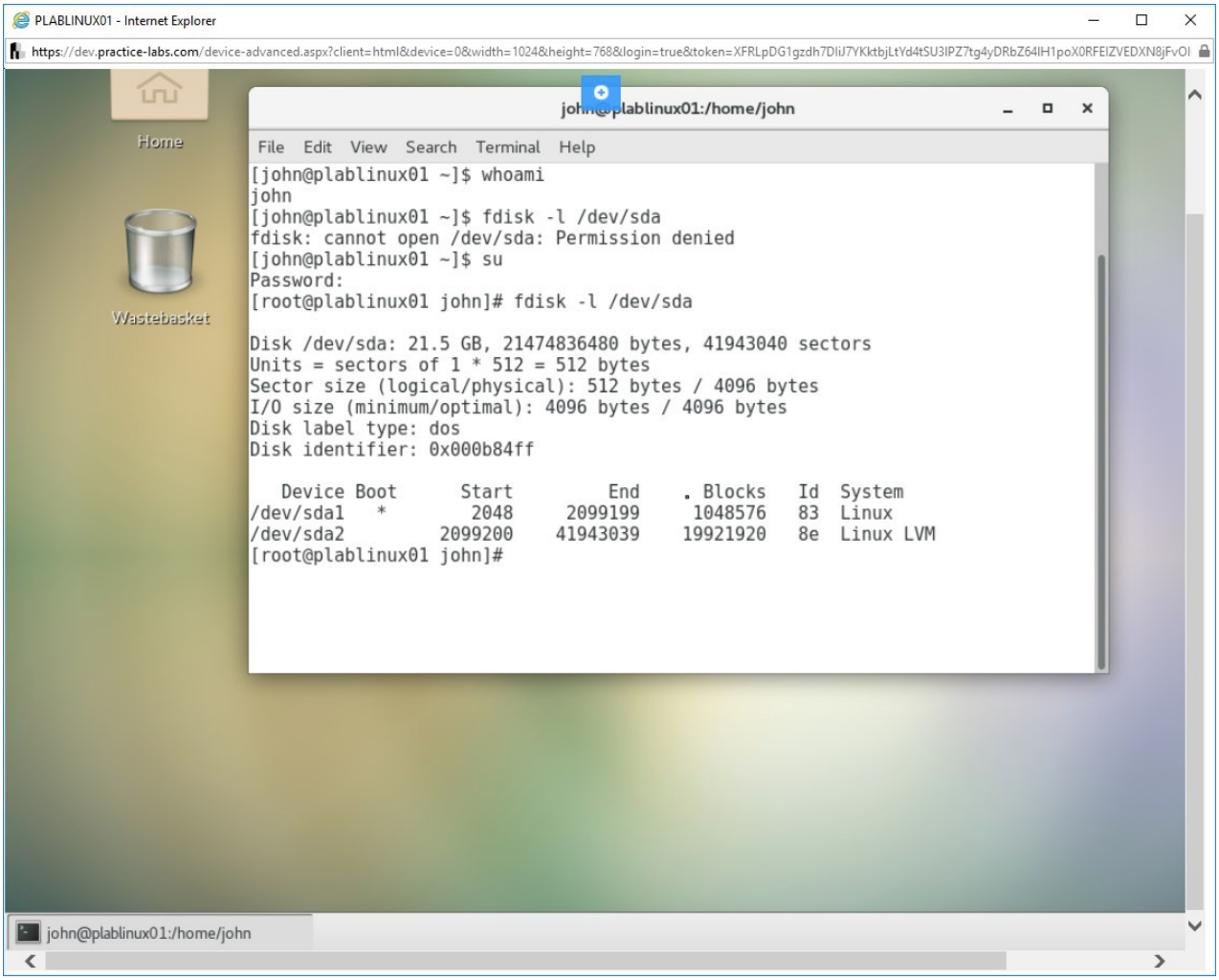


Figure 1.32 Screenshot of PLABLINUX01: Executing the fdisk command with the root privileges.

Step 16

Type the following command to exit the root shell, and now the login for the user **john** is displayed.

```
exit
```

Press **Enter**.

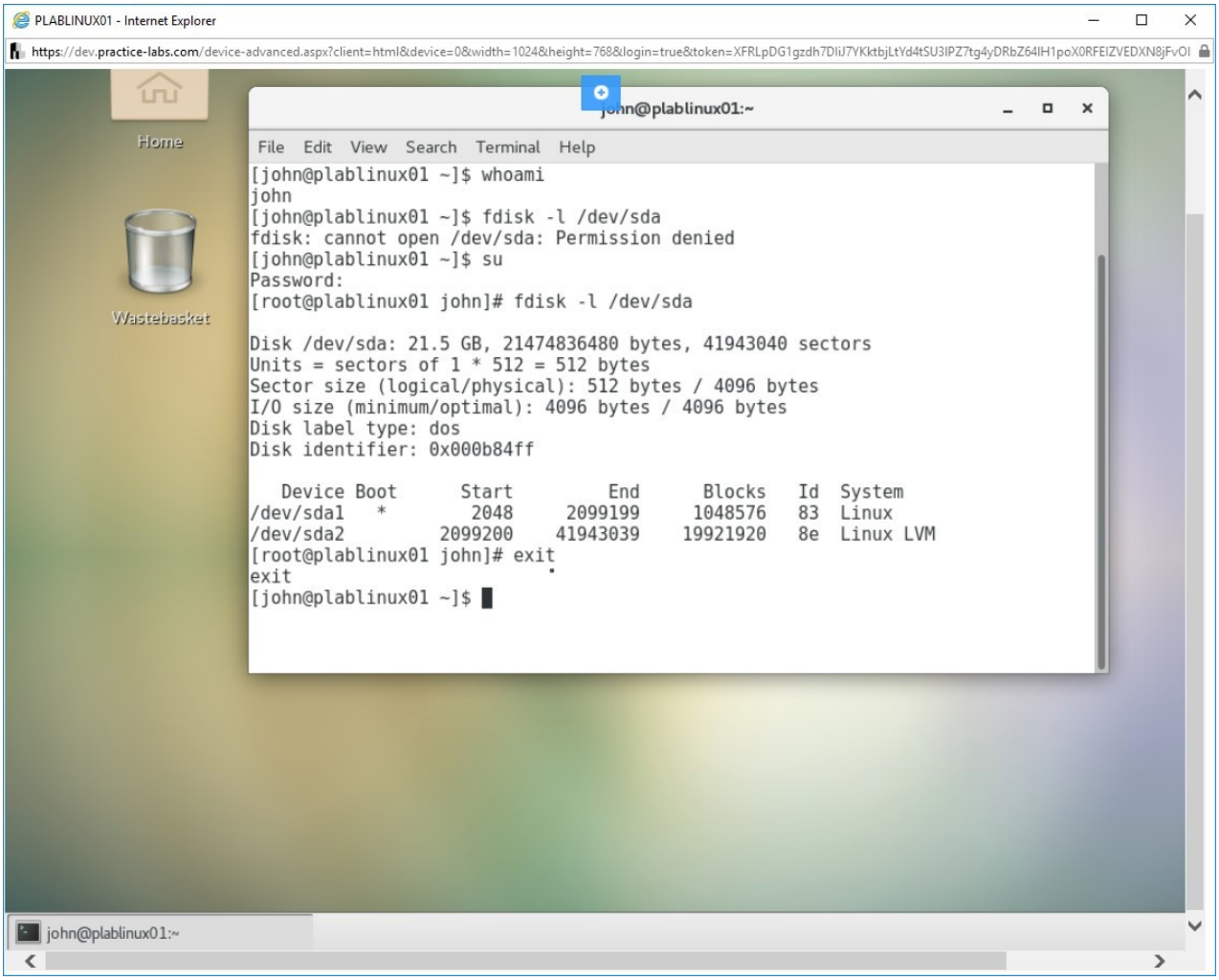


Figure 1.33 Screenshot of PLABLINUX01: Exiting the root account on the command prompt.

Task 5 - Use the sudo Command to Give Superuser Privileges

The **sudo** command allows a user to execute the command as a superuser. However, this user needs to be listed in the **/etc/sudoers** file. In this task, you will learn the usage of the **sudo** command.

To use the **sudo** command, perform the following steps.

Step 1

Clear the screen by entering the following command:

```
clear
```

Now, you will learn to use the sudo command.

Type the following command:

```
sudo root
```

Press **Enter**.

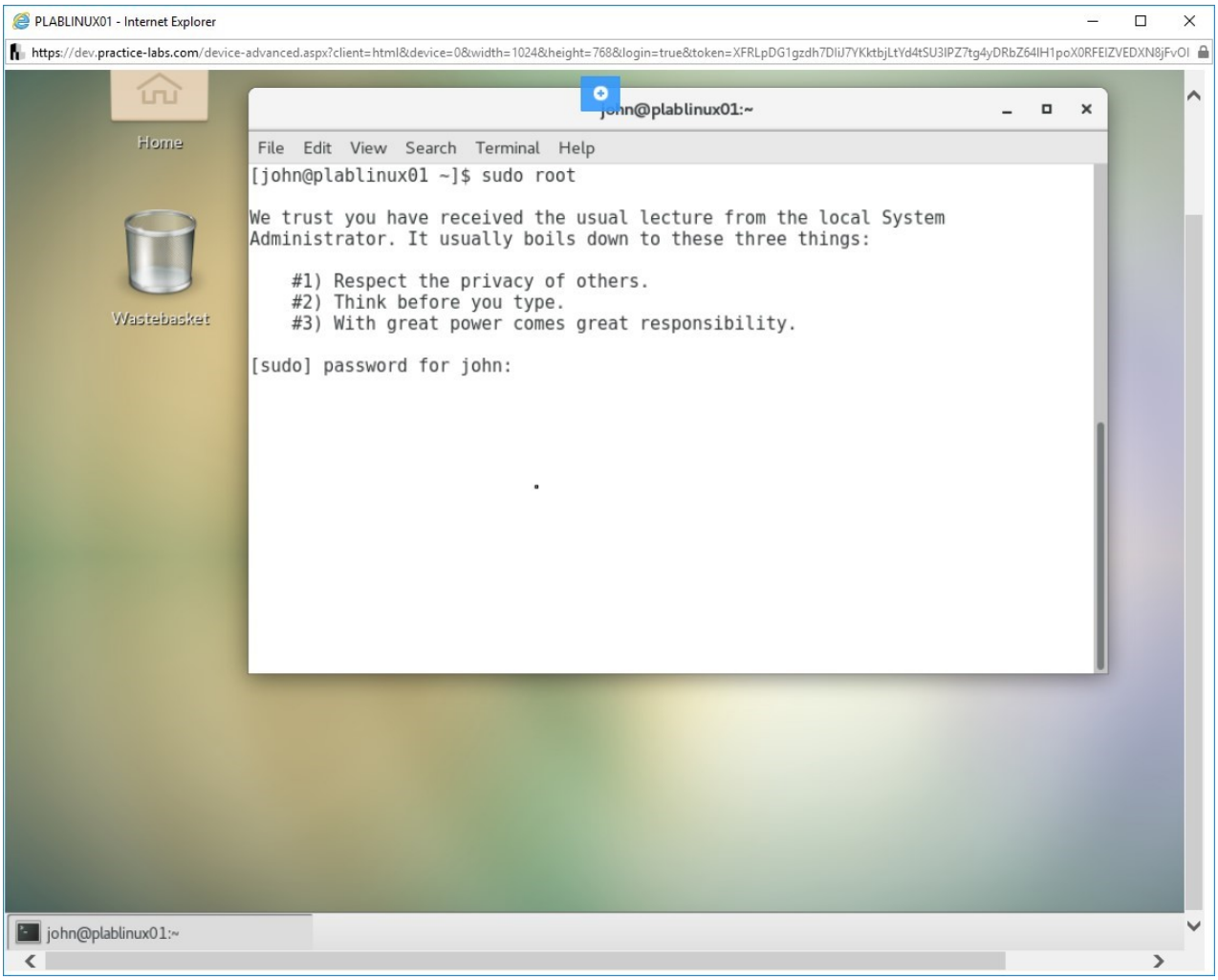


Figure 1.34 Screenshot of PLABLINUX01: Using the sudo command.

Step 2

When prompted for the password, type the password as:

`Passw0rd`

> ***Note:*** *If you had to change your password when logging in as john in task 5 step 3, that's the password you have to use here.*

Press **Enter**.

Note that now you are providing the password for **john**, not for **root**.

After you enter the password, you may notice that an error stops john from accessing root privileges.

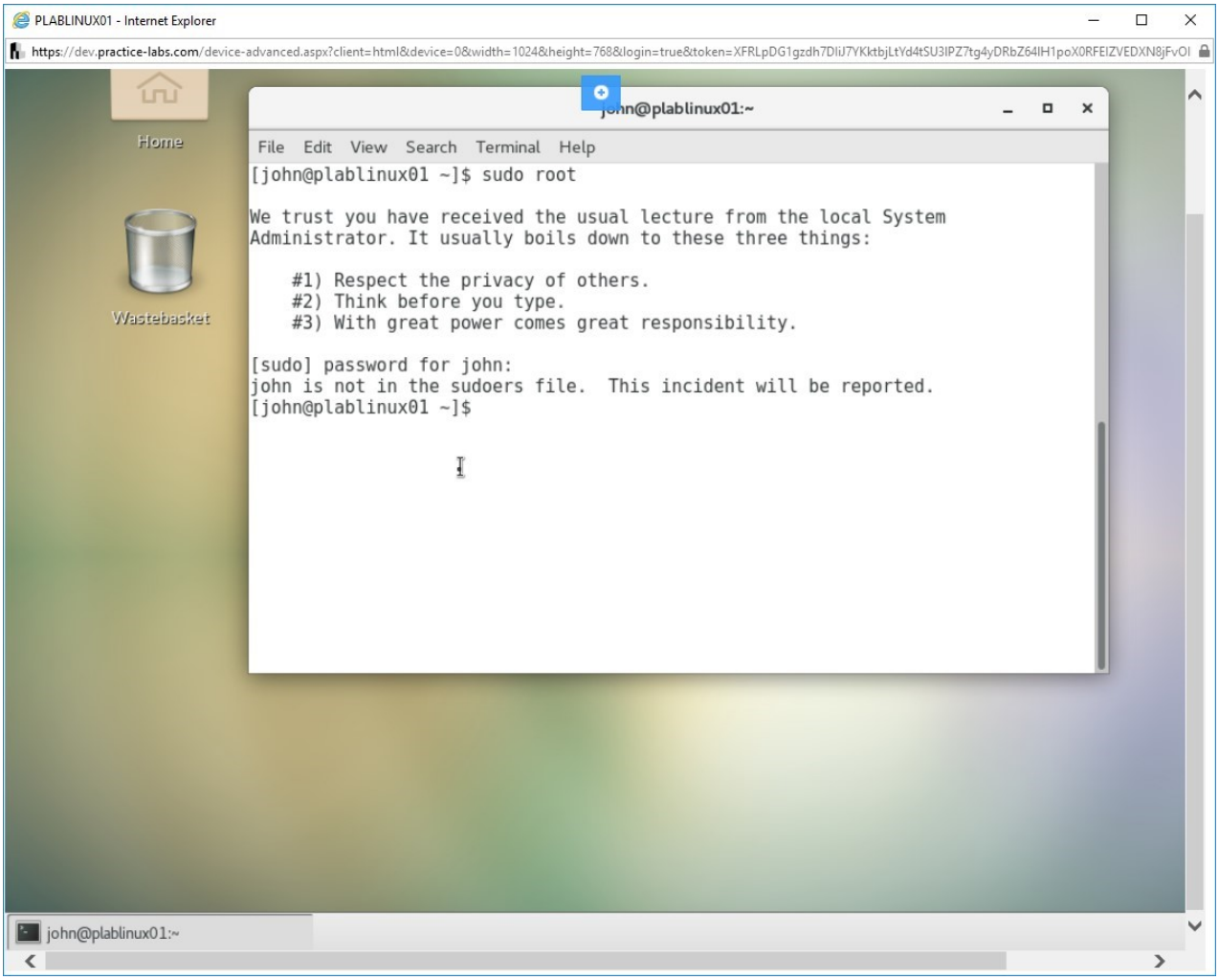


Figure 1.35 Screenshot of PLABLINUX01: Receiving an error on the sudo command.

Step 3

Clear the screen by entering the following command:

```
clear
```

Let's open the **/etc/sudoers** file and add john's name into it. To do this, you need to gain the privileges of **root** using the **su** command.

Type the following command:

```
su
```

Press **Enter**.

Type the password as:

`Passw0rd`

Press **Enter**.

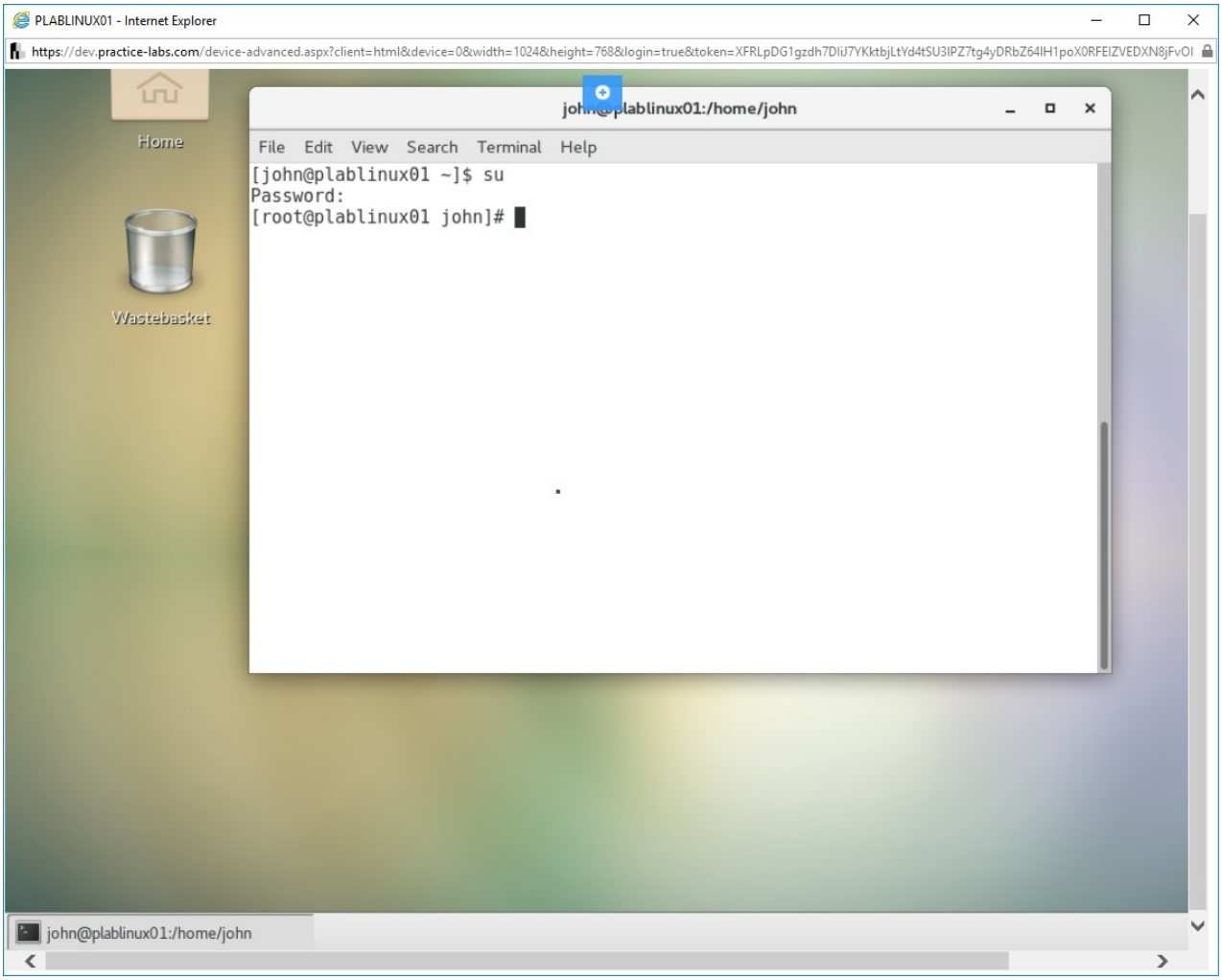


Figure 1.36 Screenshot of PLABLINUX01: Changing the account to the root account with the su command.

Step 4

It is important to note that **/etc/sudoers** is a read-only file. You have to make it writable before modifying it.

Type the following command:

```
chmod o+w /etc/sudoers
```

Press **Enter**.

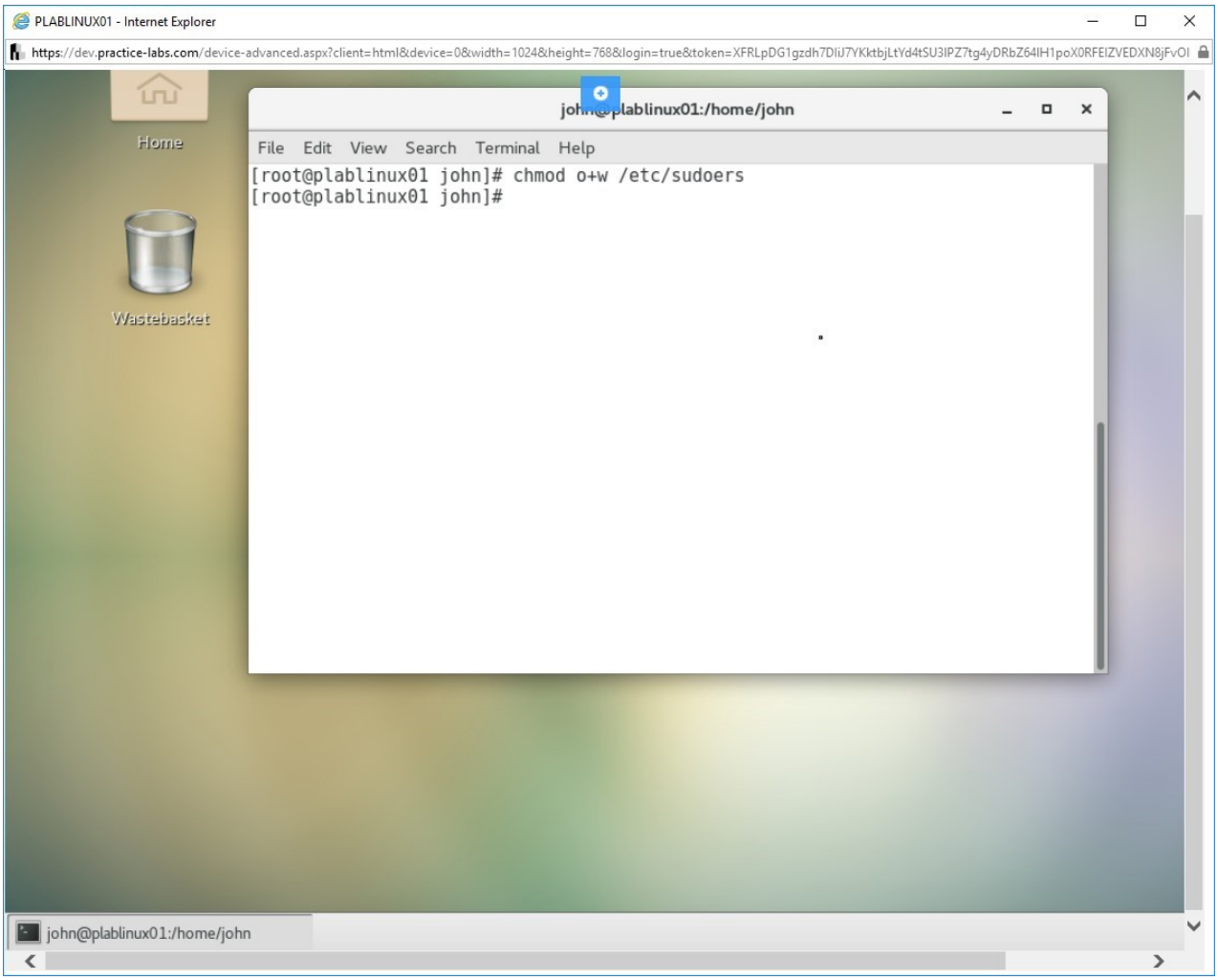


Figure 1.37 Screenshot of PLABLINUX01: Making the sudoers file writable.

Step 5

To open the **/etc/sudoers** file, type the following command:

```
vi /etc/sudoers
```

Press **Enter**.

The file is now displayed. Press **i** to change to the insert mode.

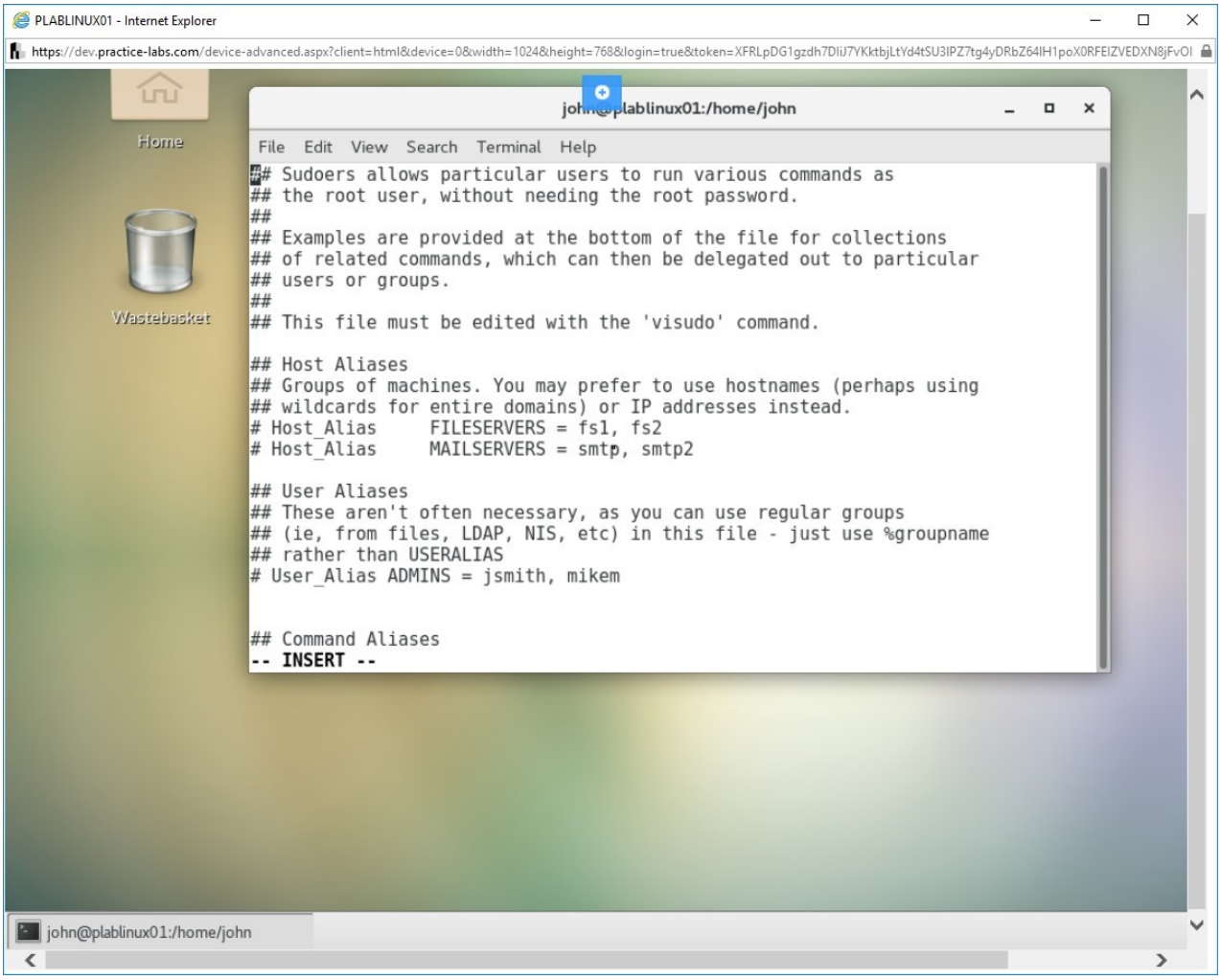


Figure 1.38 Screenshot of PLABLINUX01: Editing the sudoers file.

Step 6

Type the following for user **john**:

```
john ALL=NOPASSWD: /bin/vi
```

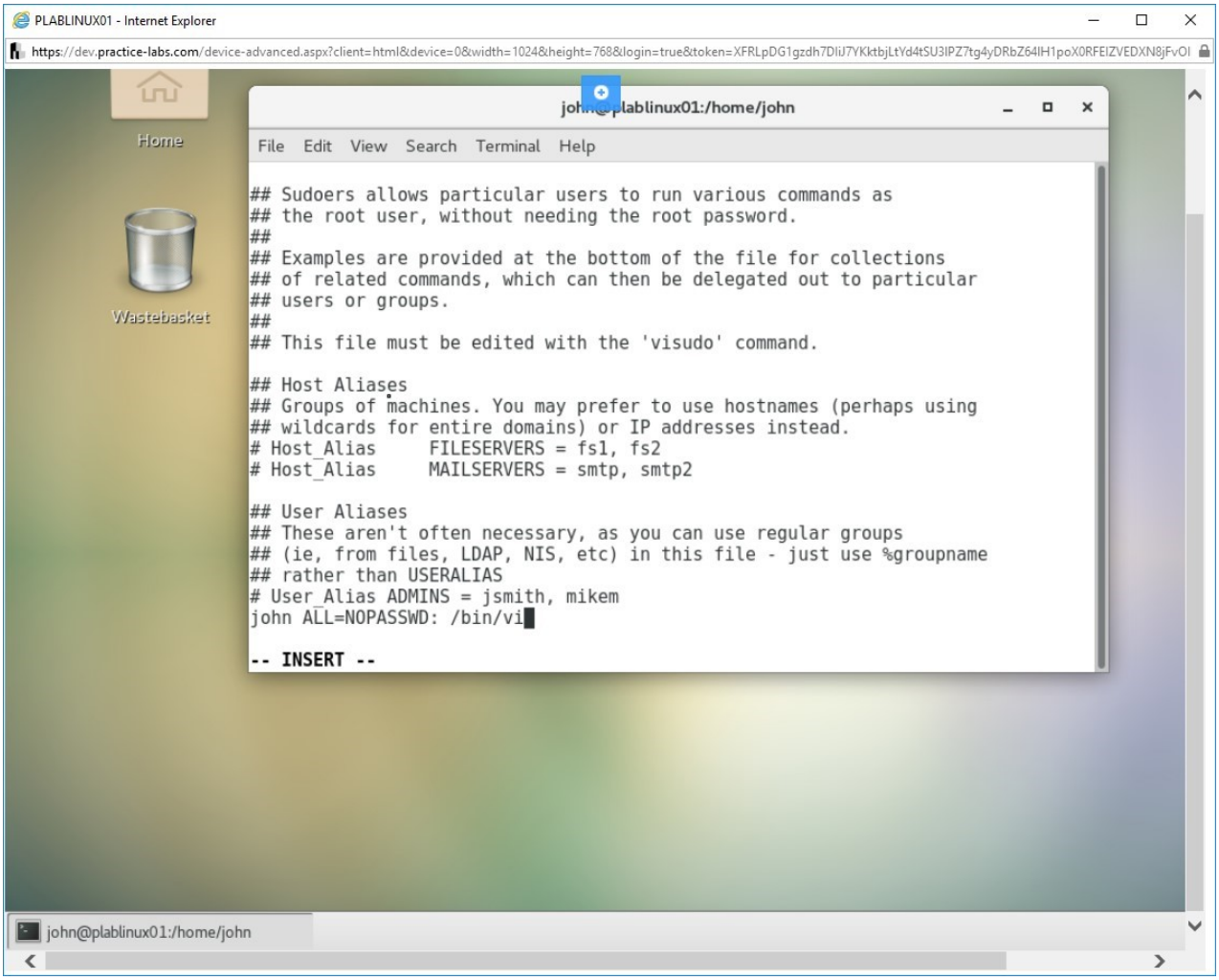


Figure 1.39 Screenshot of PLABLINUX01: Adding the user john in the sudoers file.

Step 7

Now save the file. Press **ESC** and type the following:

```
:wq
```

Press **Enter**.

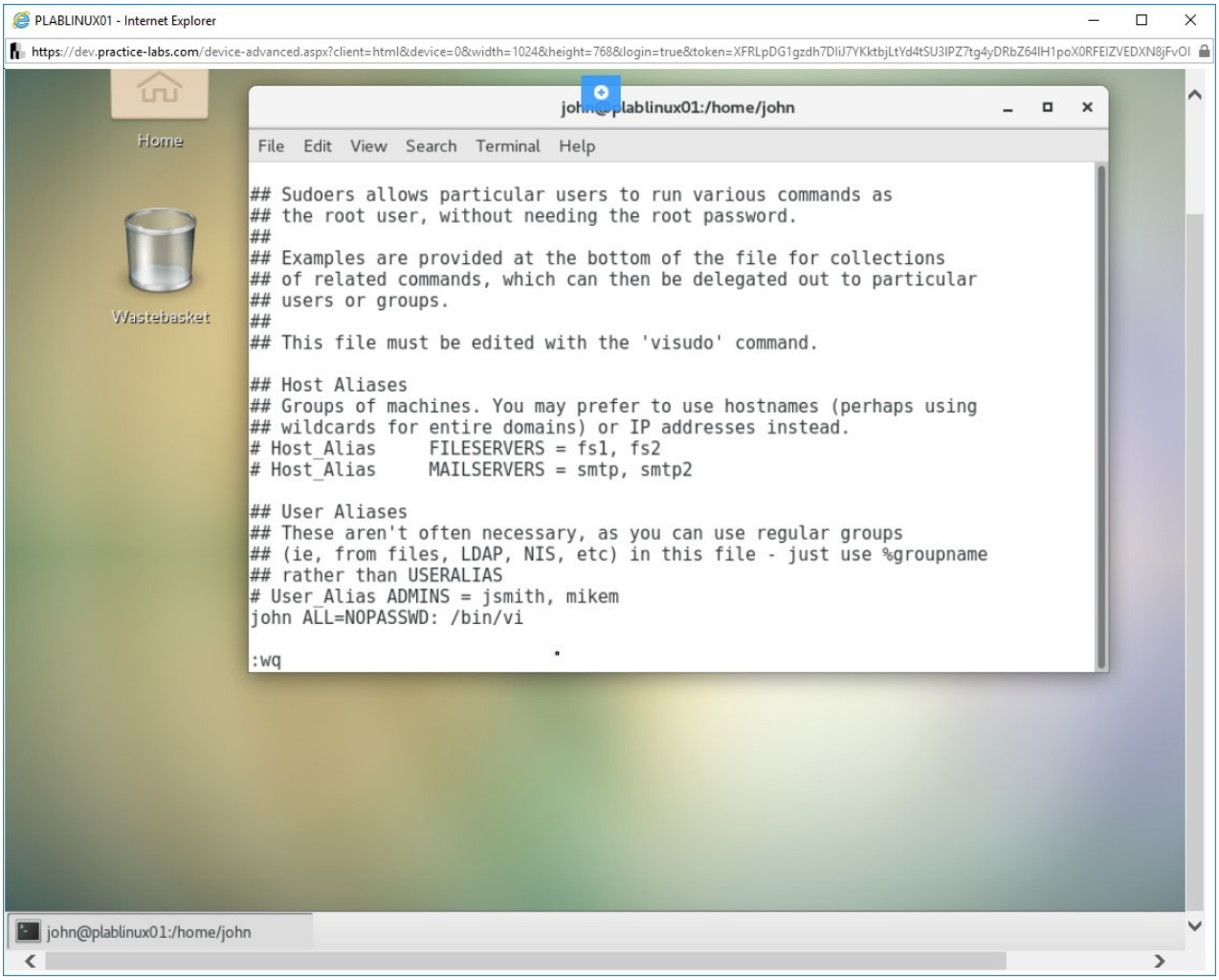


Figure 1.40 Screenshot of PLABLINUX01: Saving and closing the sudoers file.

Step 8

You are back on the command prompt.

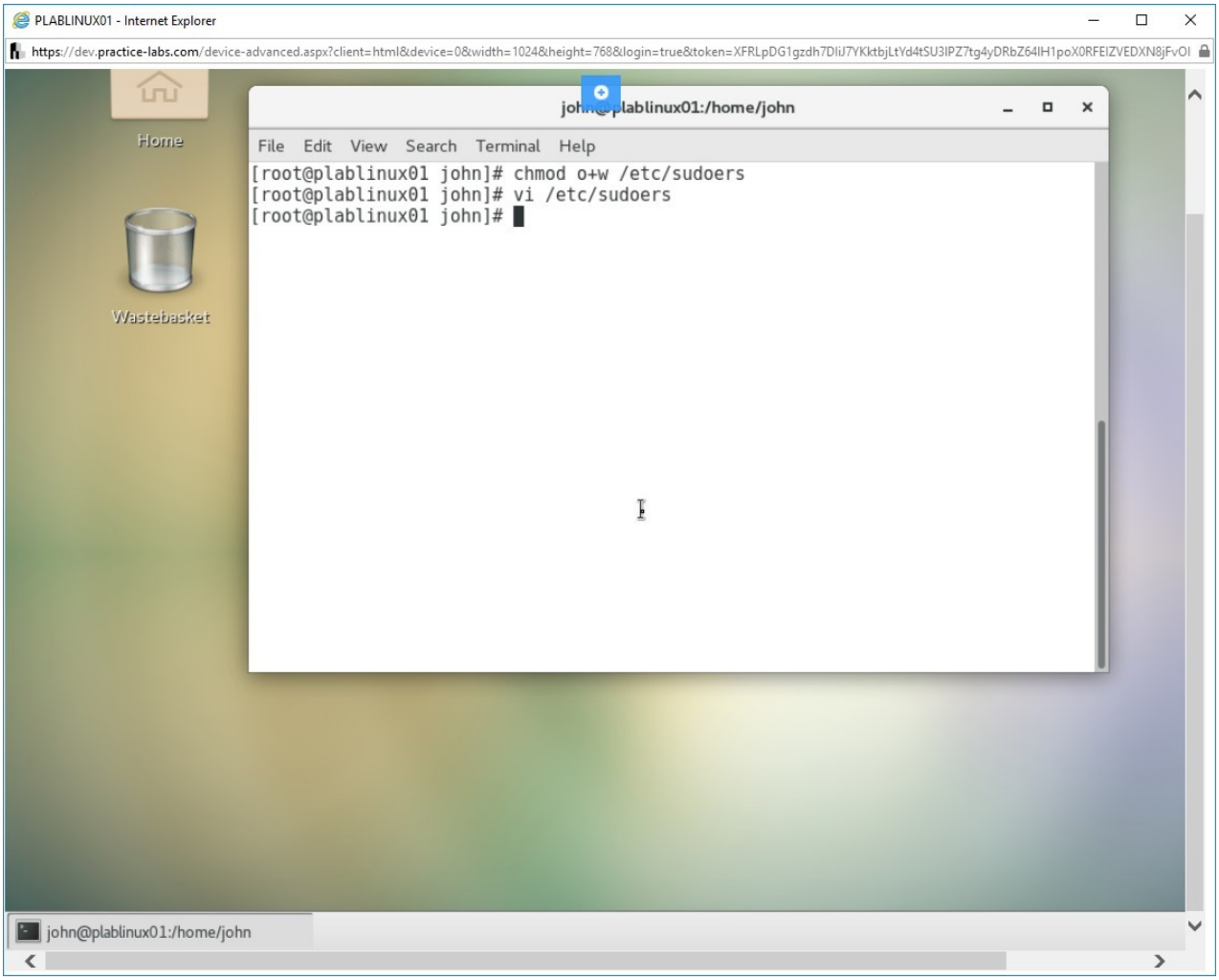


Figure 1.41 Screenshot of PLABLINUX01: Coming back to the command prompt.

Step 9

You now need to change the **/etc/sudoers** file to read-only. Type the following command:

```
chmod 440 /etc/sudoers
```

Press **Enter**.

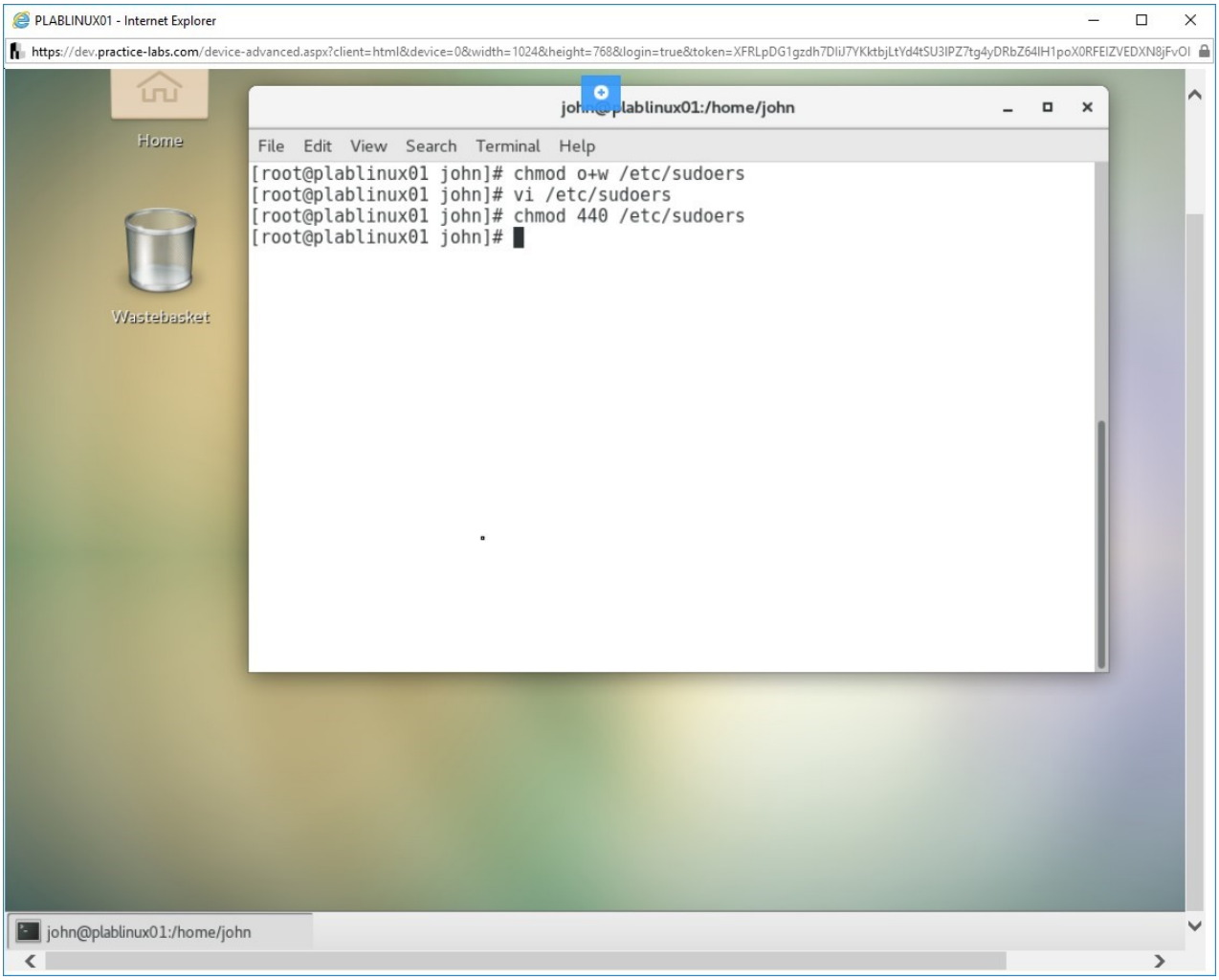


Figure 1.42 Screenshot of PLABLINUX01: Making the sudoers file read-only.

Step 10

Clear the screen by entering the following command:

```
clear
```

Type the following command:

```
exit
```

Press **Enter**.

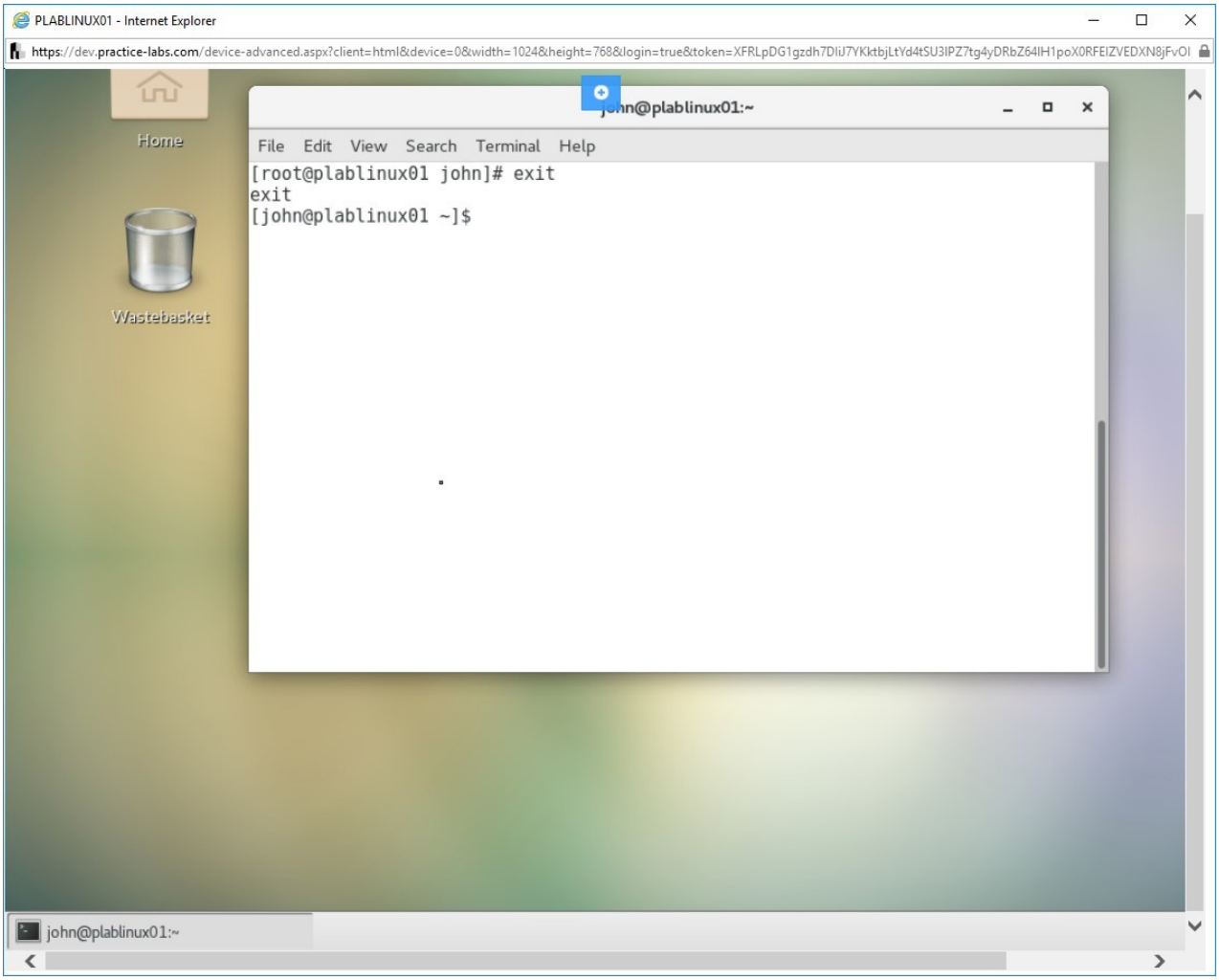


Figure 1.43 Screenshot of PLABLINUX01: Exiting the root prompt in the terminal window.

Task 6 - Manage Shell Resources

You can use the **ulimit** command to managing the resources available to the shell and its processes. Managing the resources includes setting limits on user logins, processes, and memory usage. Two types of limits can be defined:

- **Hard**: Set by superuser and cannot be superseded by a user
- **Soft**: Set by superuser but can be temporarily superseded by a user

These limits are specified in the **/etc/security/limits.conf** file. In this task, you will list and modify the limits for the user john. To manage shell resources, perform the following steps:

Step 1

Clear the screen by entering the following command:

```
clear
```

To view all the current limits for a user, type the following command:

```
ulimit -a
```

Press **Enter**.

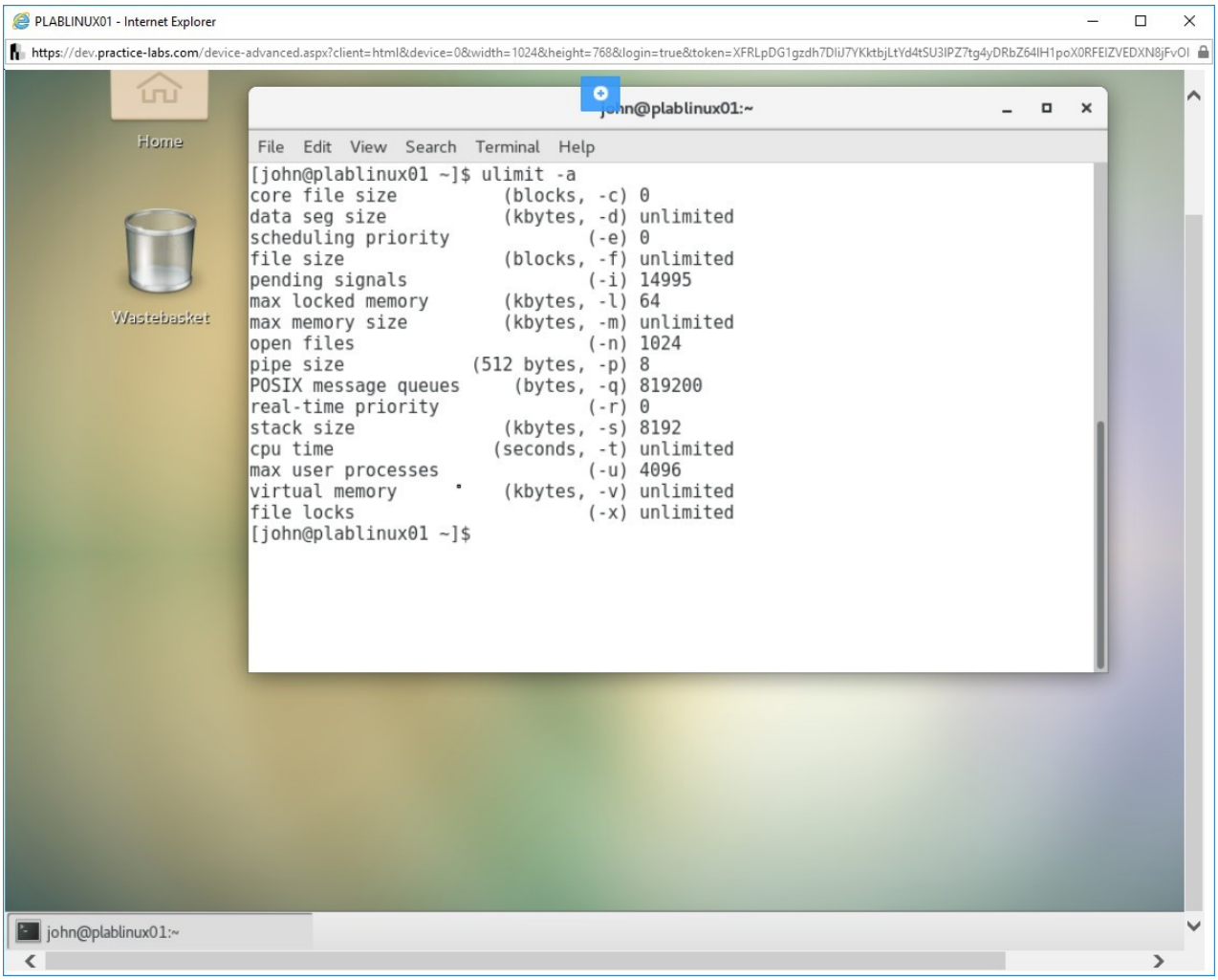


Figure 1.44 Screenshot of PLABLINUX01: Viewing all the current limits for a user.

Step 2

Clear the screen by entering the following command:

```
clear
```

You can view the hard limits. Type the following command:

```
ulimit -H
```

Press **Enter**.

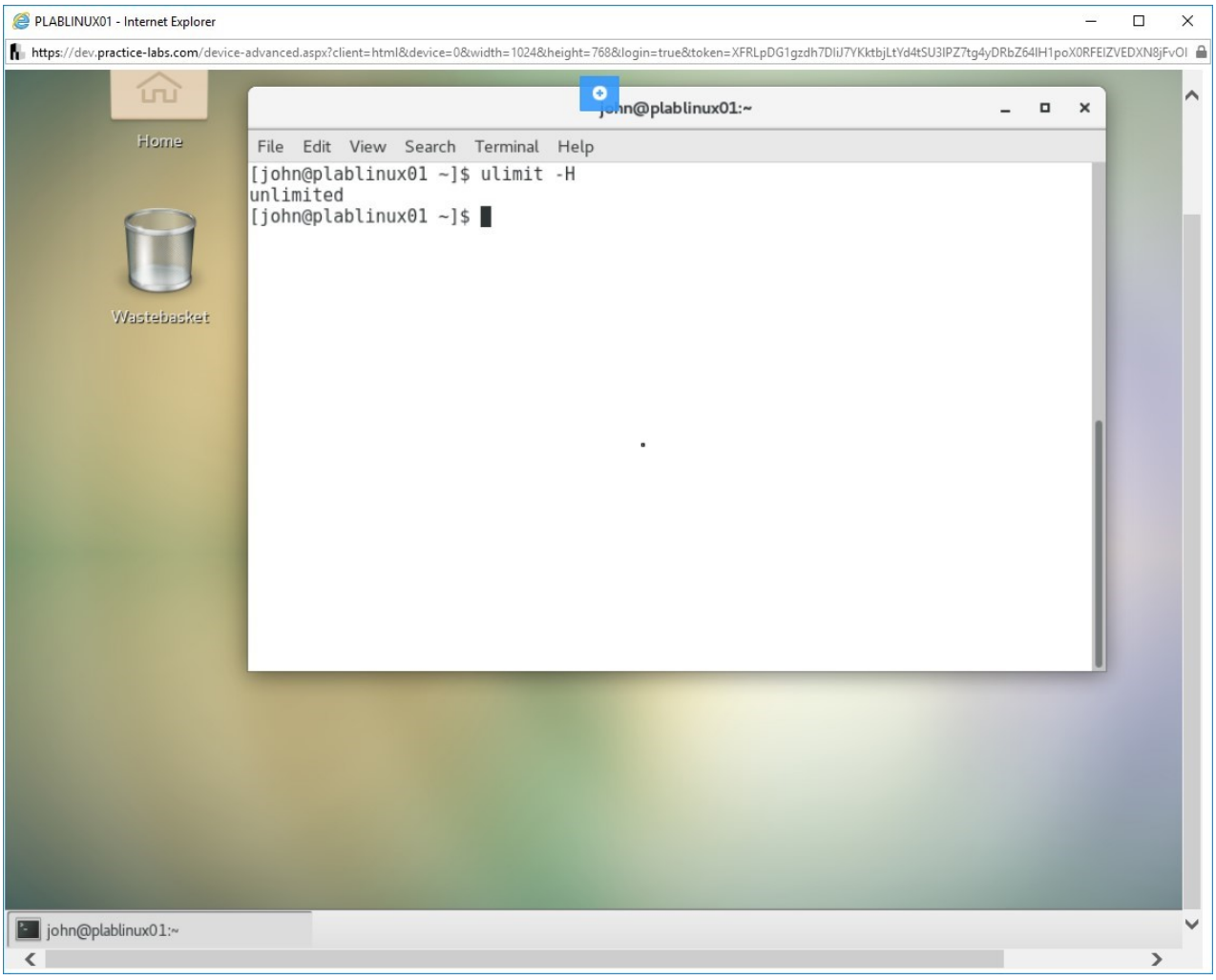


Figure 1.45 Screenshot of PLABLINUX01: Viewing the hard limits.

Step 3

Let's view the limits in the **/etc/security/limits.conf** file. Type the following command:

```
cat /etc/security/limits.conf
```

Press **Enter**.

Note that the limits are marked as soft or hard. You can alter them by putting this file in the edit mode.

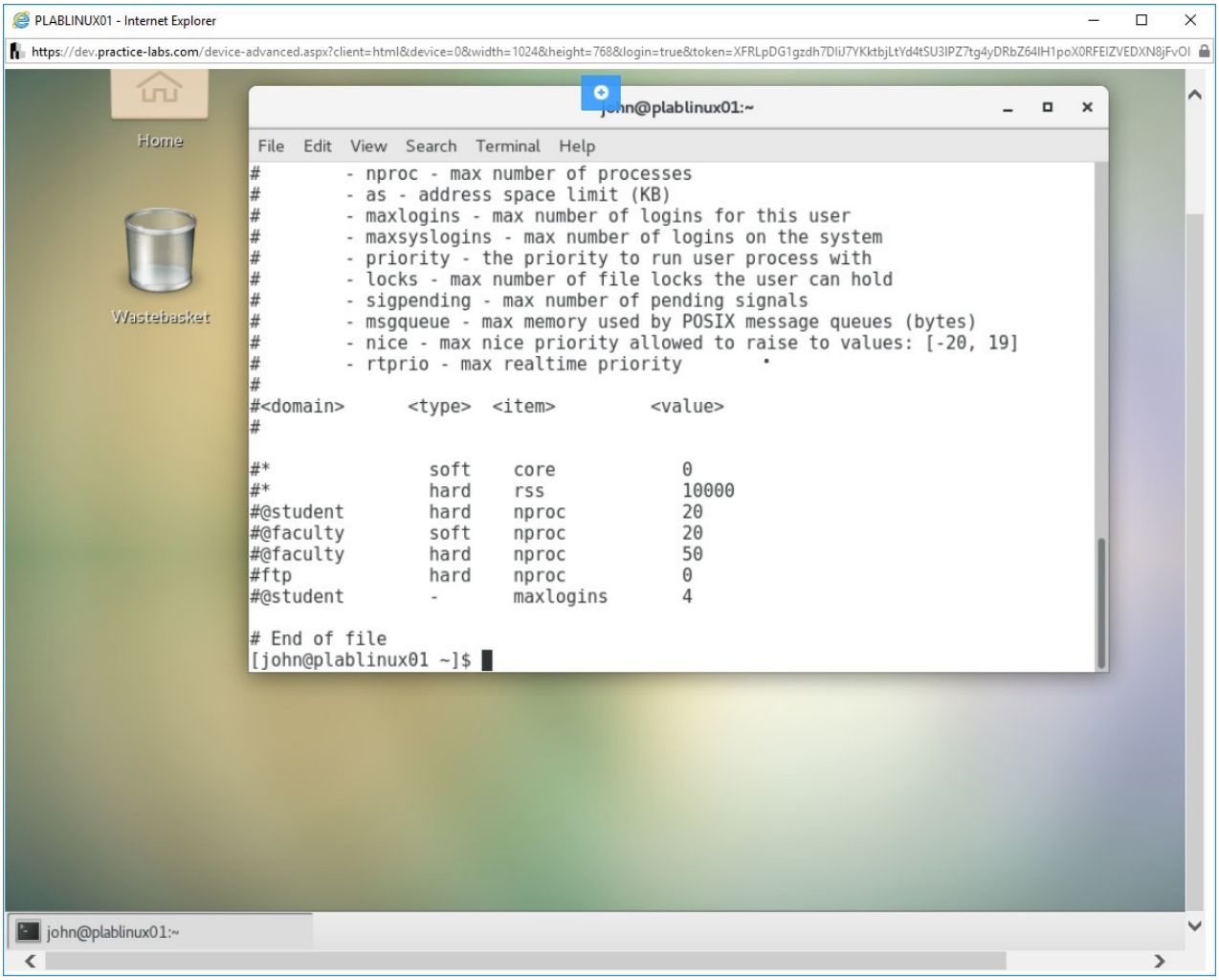


Figure 1.46 Screenshot of PLABLINUX01: View the limits in the /etc/security/limits.conf file.

Step 4

Clear the screen by entering the following command:

```
clear
```

The fuser command displays the list of processes that are using files and sockets.

To use the fuser command, type the following command:

```
fuser -all
```

Press **Enter**.

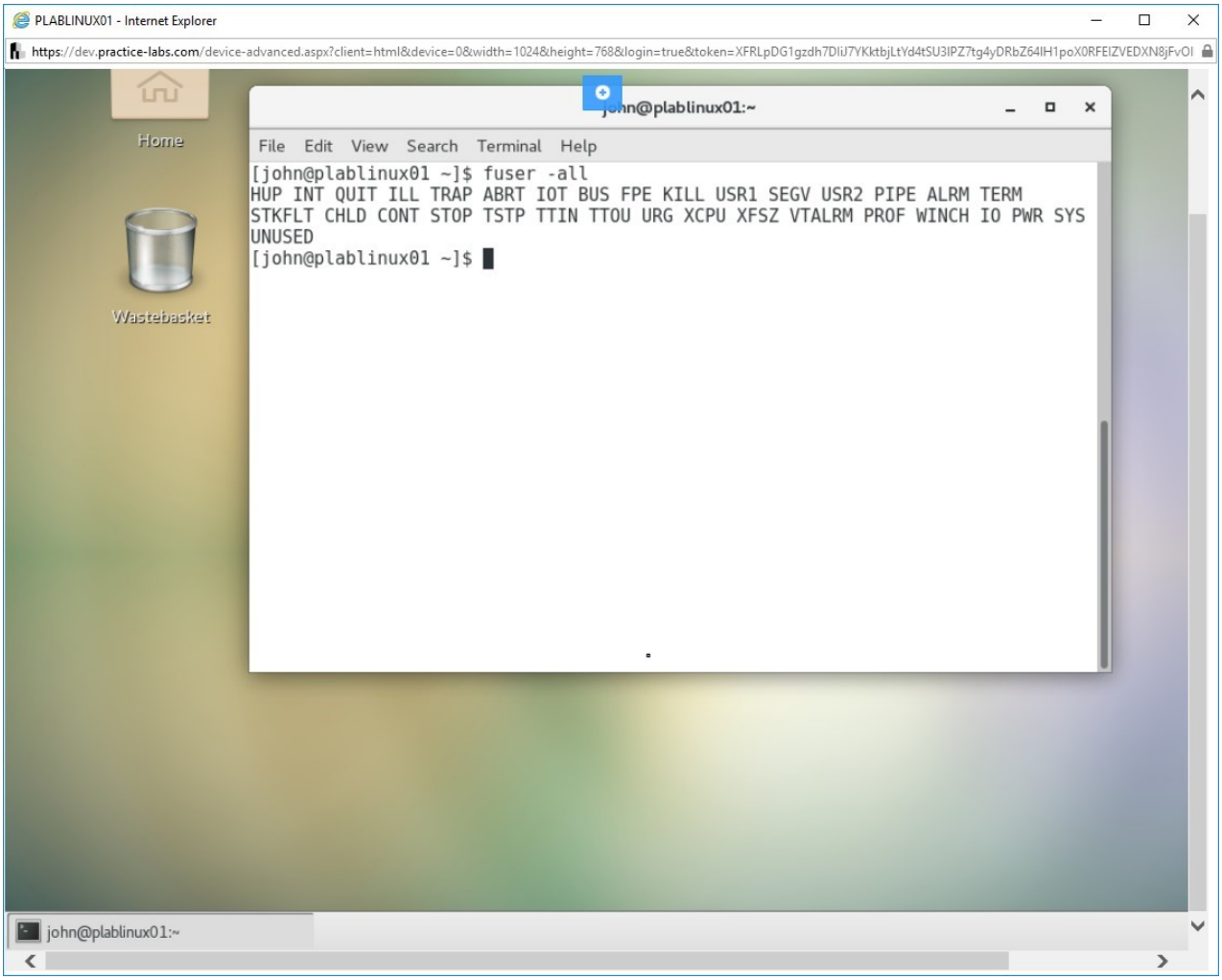


Figure 1.47 Screenshot of PLABLINUX01: Displaying the list of processes that are using files and sockets.

Step 5

To view which processes are using a particular file or directory, type the following command:

```
fuser .
```

Press **Enter**.

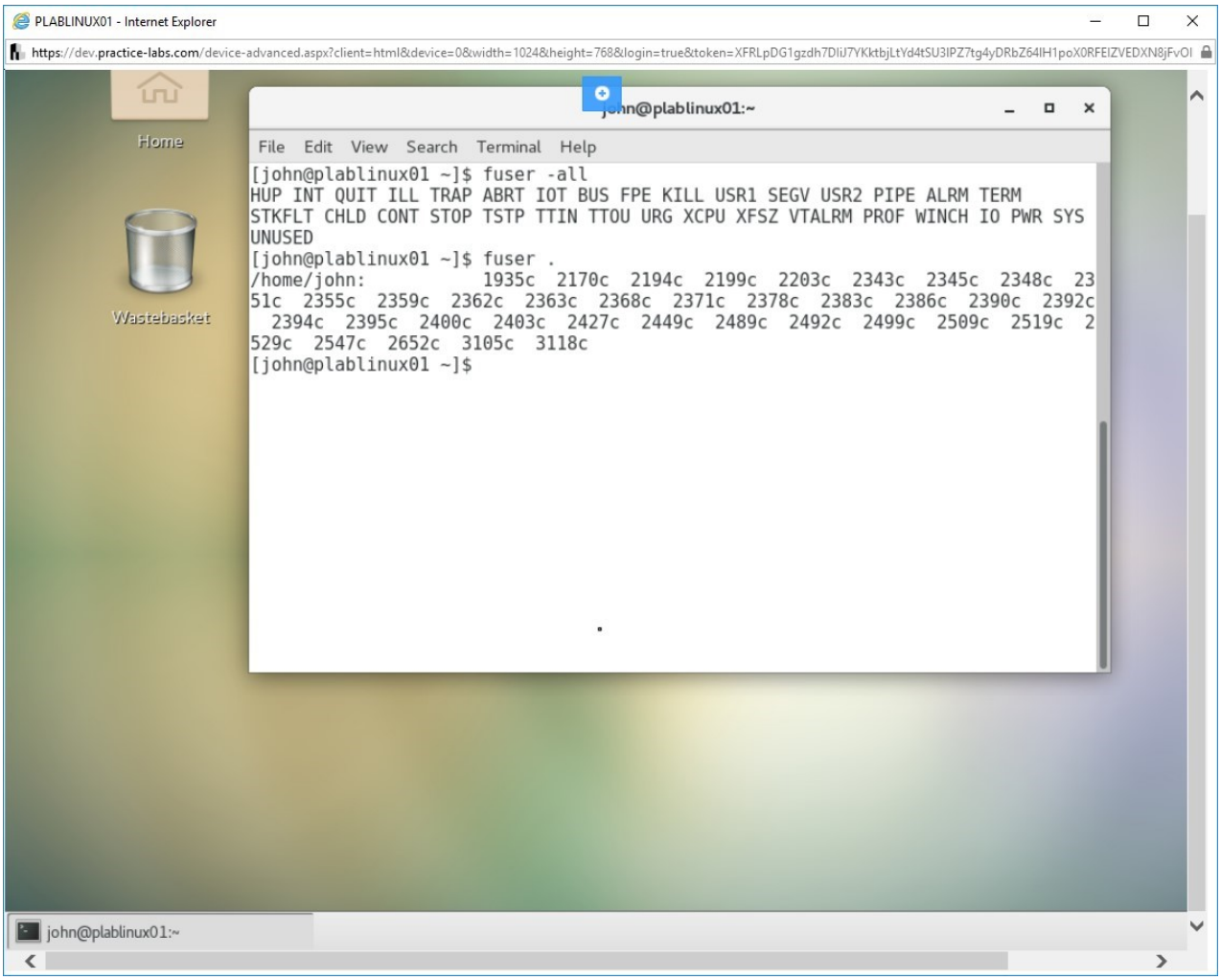


Figure 1.48 Screenshot of PLABLINUX01: Viewing that processes that are using a particular file or directory.

Step 6

You can run the fuser command on the current directory. The output will provide the information on all the processes that are using this directory. Type the following command:

```
fuser -v ./
```

Press **Enter**.

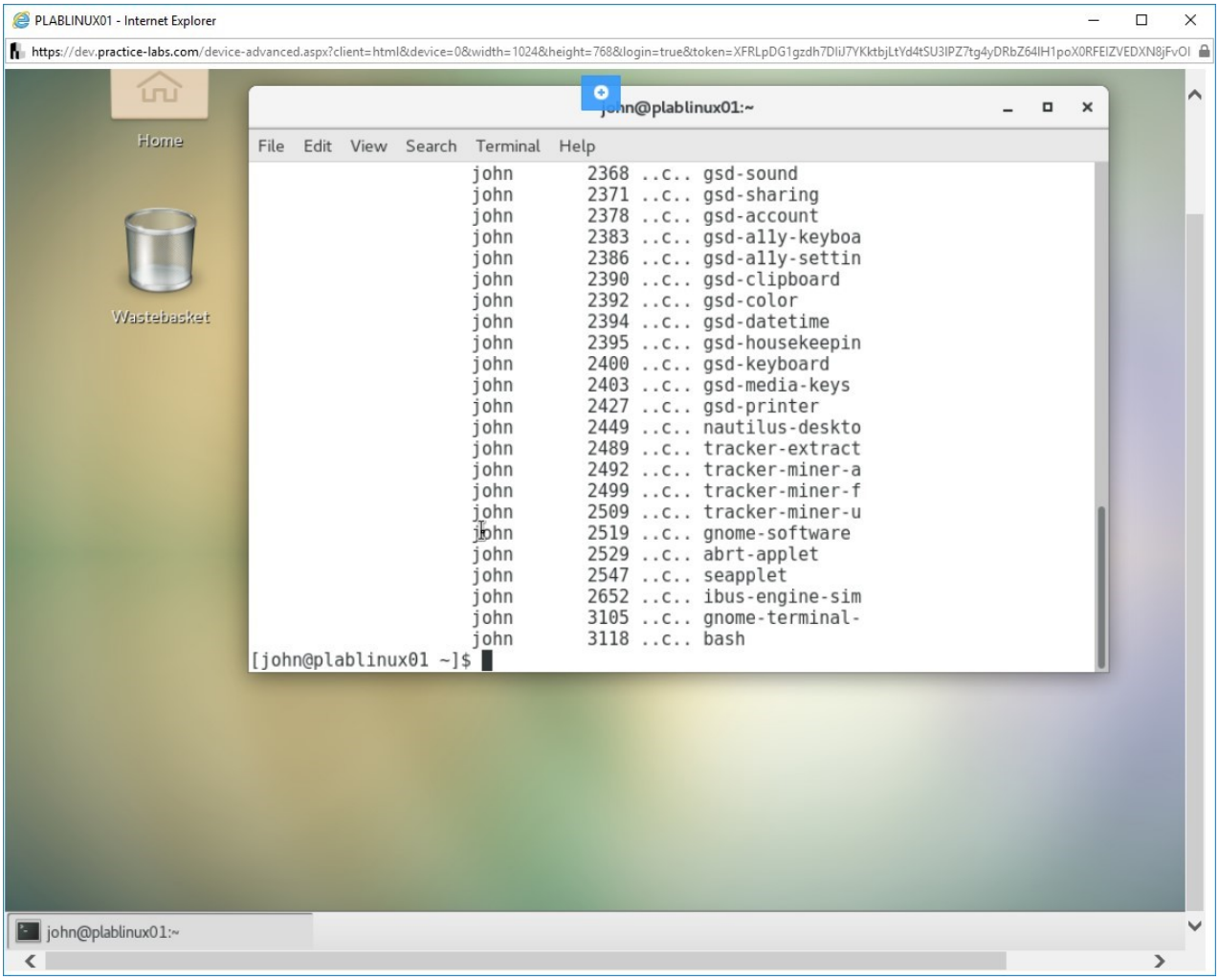


Figure 1.49 Screenshot of PLABLINUX01: Running the fuser command on the current directory.

Task 7 - Discover Open Ports on a System

nmap and **netstat** commands enable you to discover open ports on a system. Using the **nmap** command, you can perform port scanning of a specific system or more than one systems on the network. The **netstat** command is a network information tool that can provide information about the network connection, routing tables, and much more.

In this task, you will discover open ports on a system. To discover open ports on a system, perform the following steps:

Step 1

Clear the screen by entering the following command:

```
clear
```

To show protocol statistics, which means the protocols being used on the local system, type the following information:

```
netstat -s
```

Press **Enter**.

> ***Note:*** *The -s parameter shows the per-protocol statistics.*

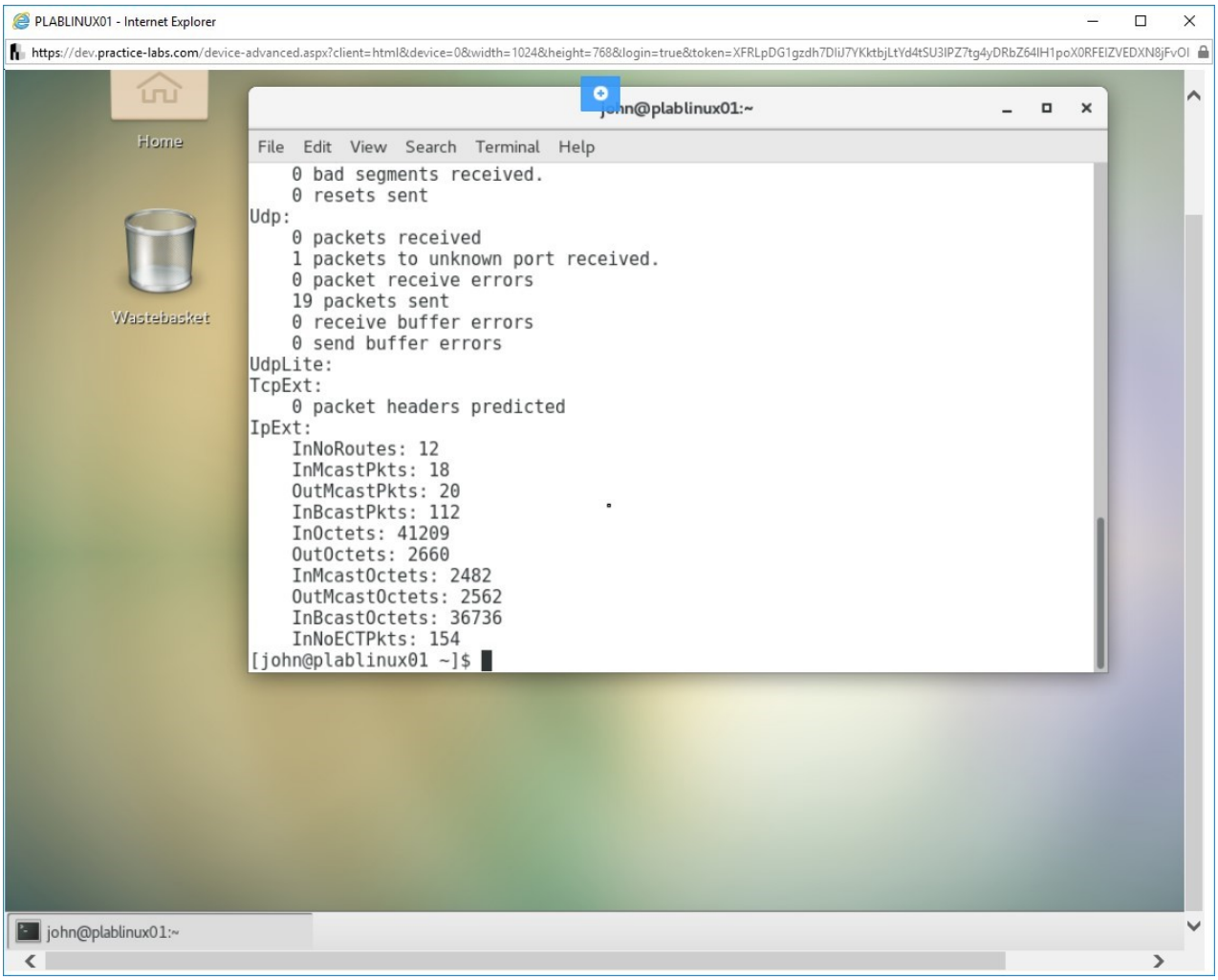


Figure 1.50 Screenshot of PLABLINUX01: Showing the protocol statistics using the netstat command.

Step 2

Clear the screen by entering the following command:

```
clear
```

To display the active TCP connections, type the following command:

```
netstat --tcp -n
```

Press **Enter**.

This command shows connections with the network addresses on the TCP protocol.

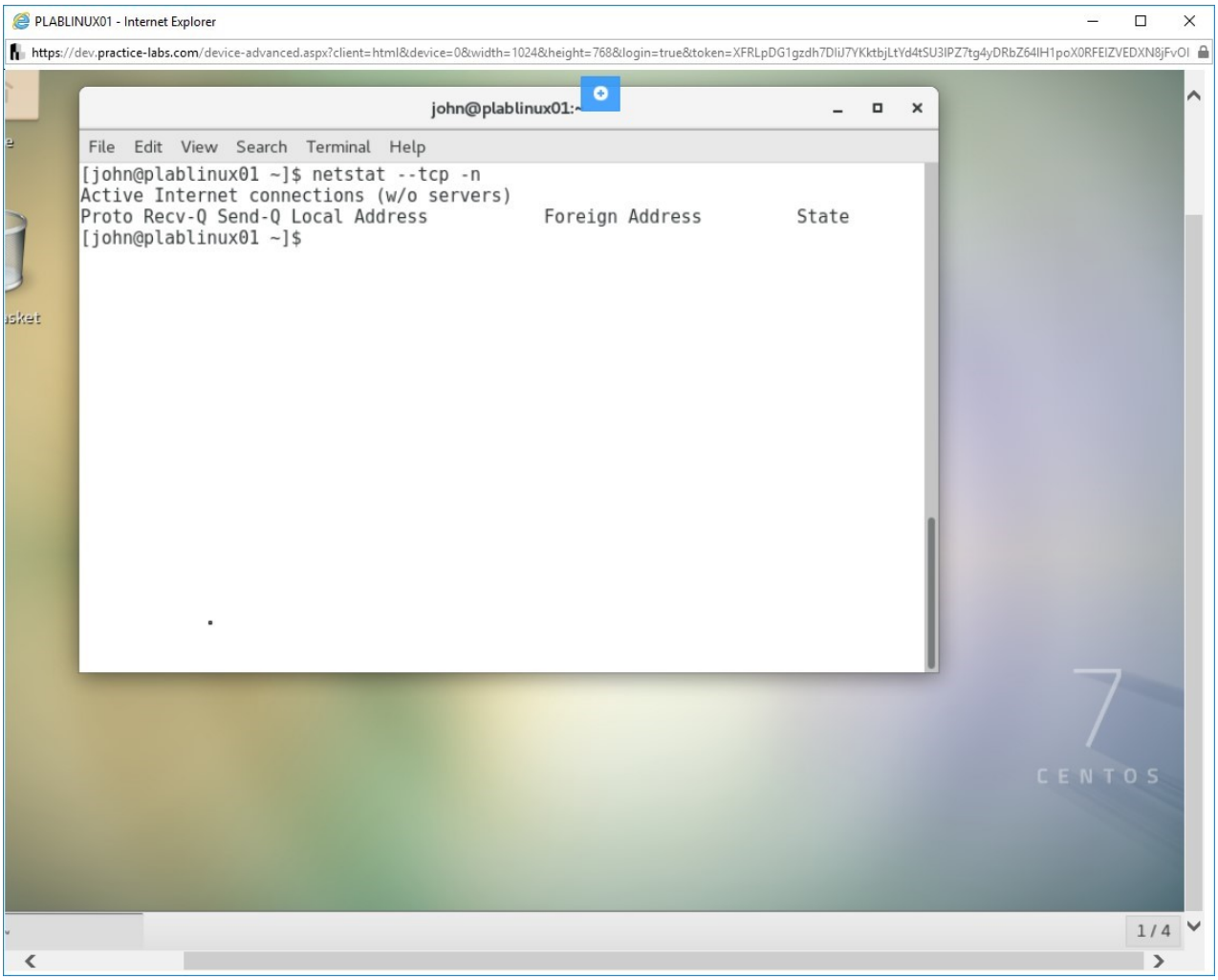


Figure 1.51 Screenshot of PLABLINUX01: Displaying the active TCP connections.

Step 3

Clear the screen by entering the following command:

```
clear
```

Change to the **root** account by typing the following command:

```
su -
```

Press **Enter**.

If prompted for the password, type the following:

`Passw0rd`

Press **Enter**.

To use the nmap command, you need first to install **nmap**. Type the following command:

```
yum install nmap
```

Press **Enter**.

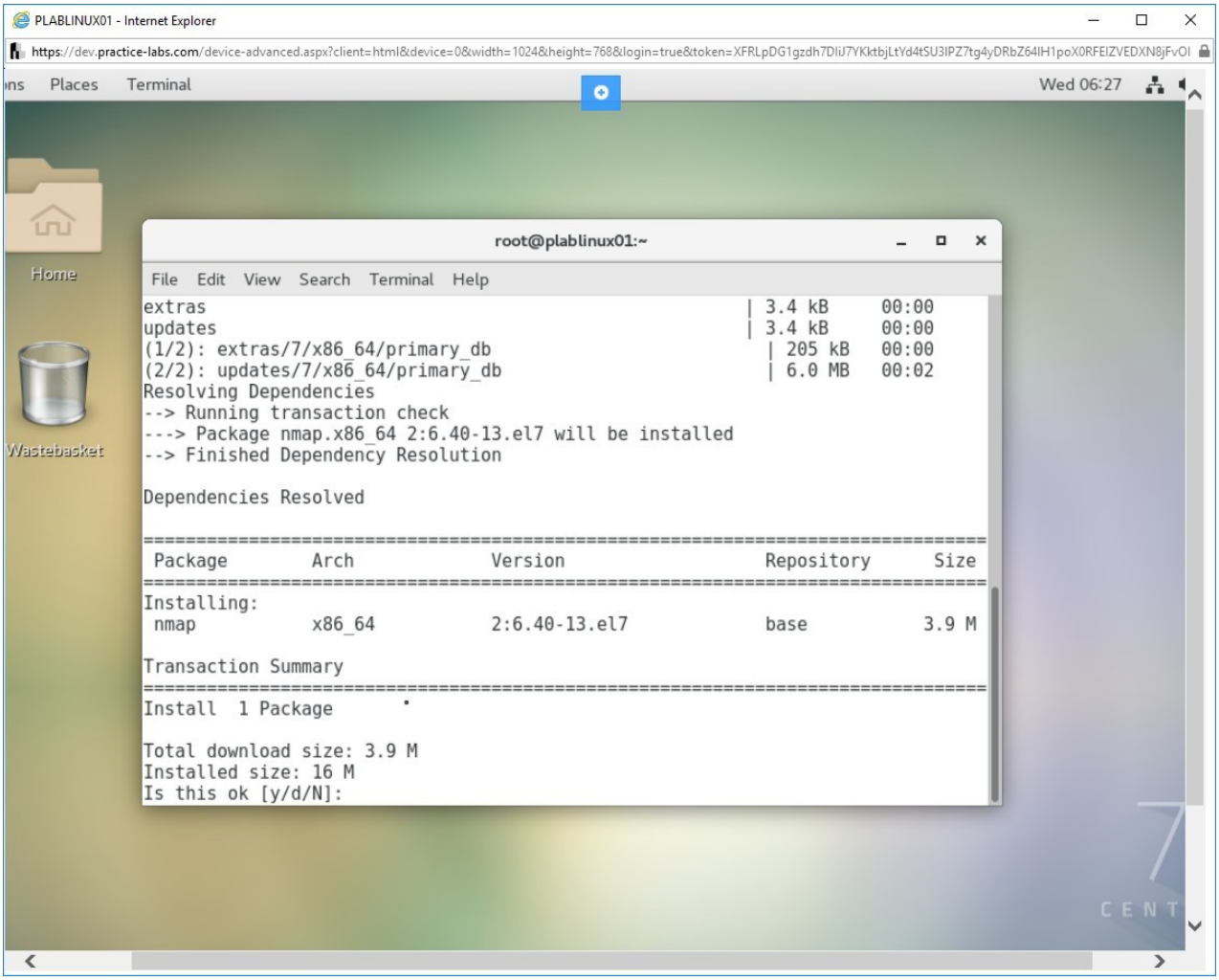


Figure 1.52 Screenshot of PLABLINUX01: Installing nmap with the yum install command.

Step 4

When prompted for confirmation, type the following:

```
y
```

Press **Enter**.

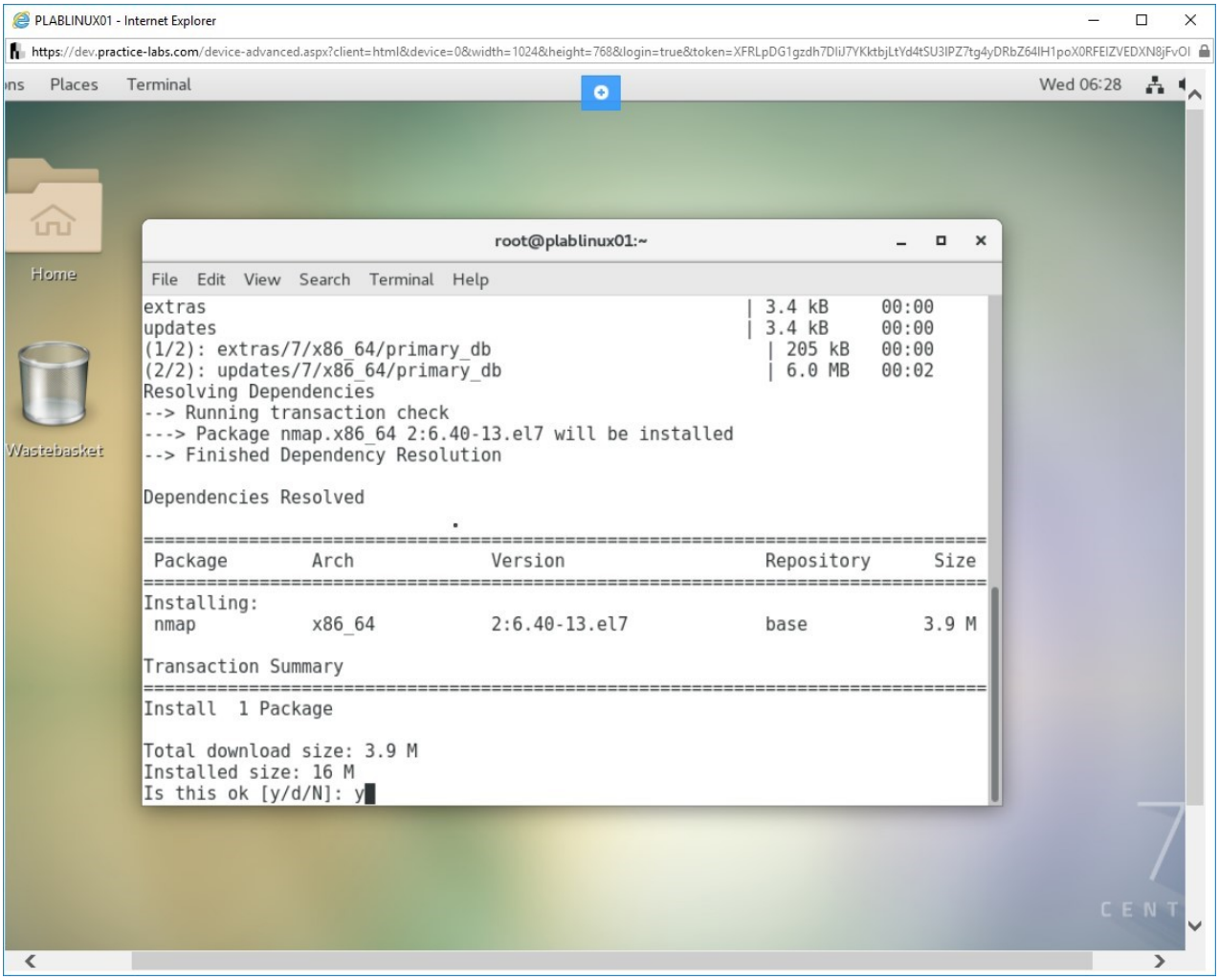


Figure 1.53 Screenshot of PLABLINUX01: Confirming the installation.

Once the installation is complete, a **Complete** message is displayed.

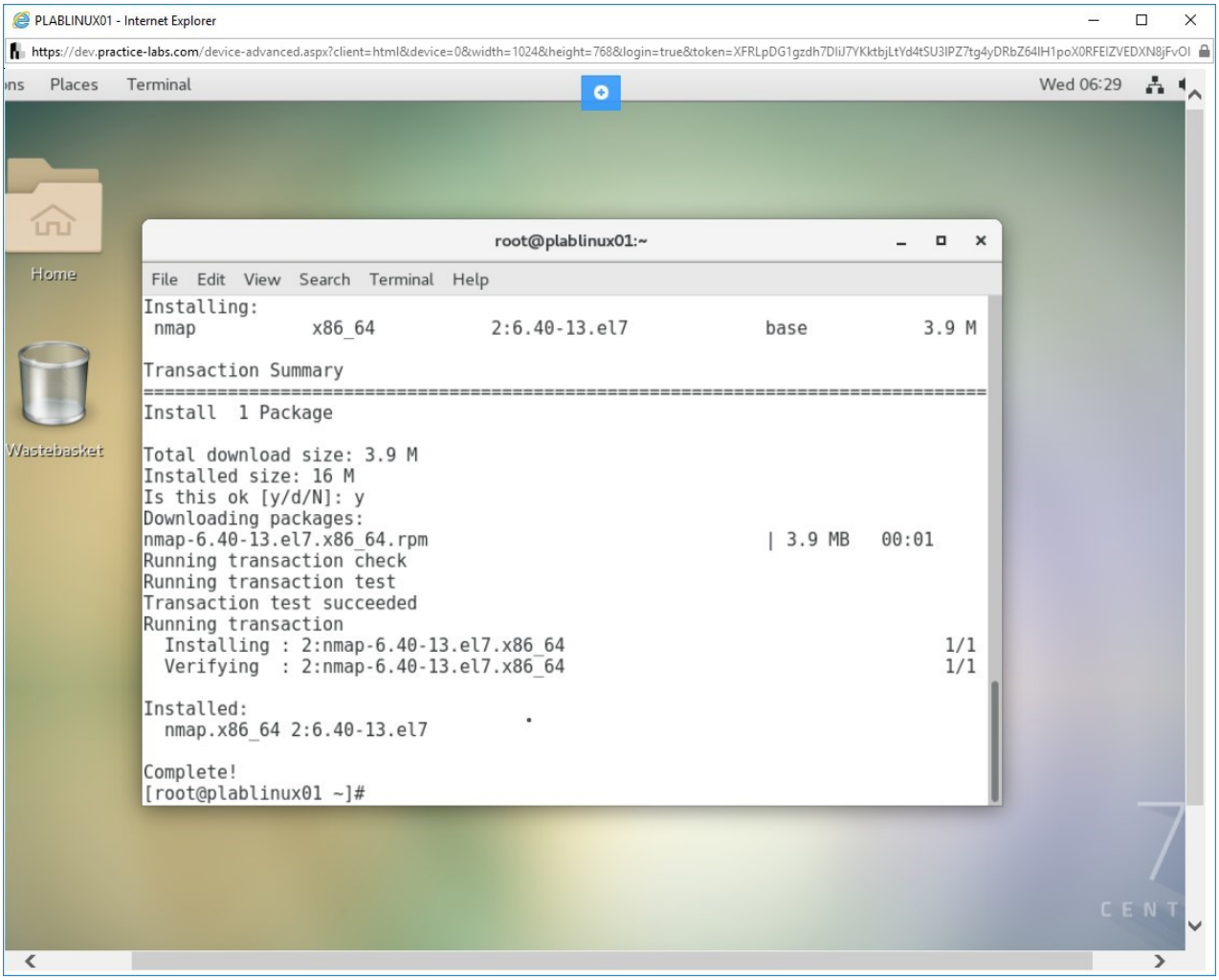


Figure 1.54 Screenshot of PLABLINUX01: Showing the completion of the installation.

Step 5

Let's now use the nmap command. Type the following command:

```
nmap 192.168.0.1
```

Press **Enter**.

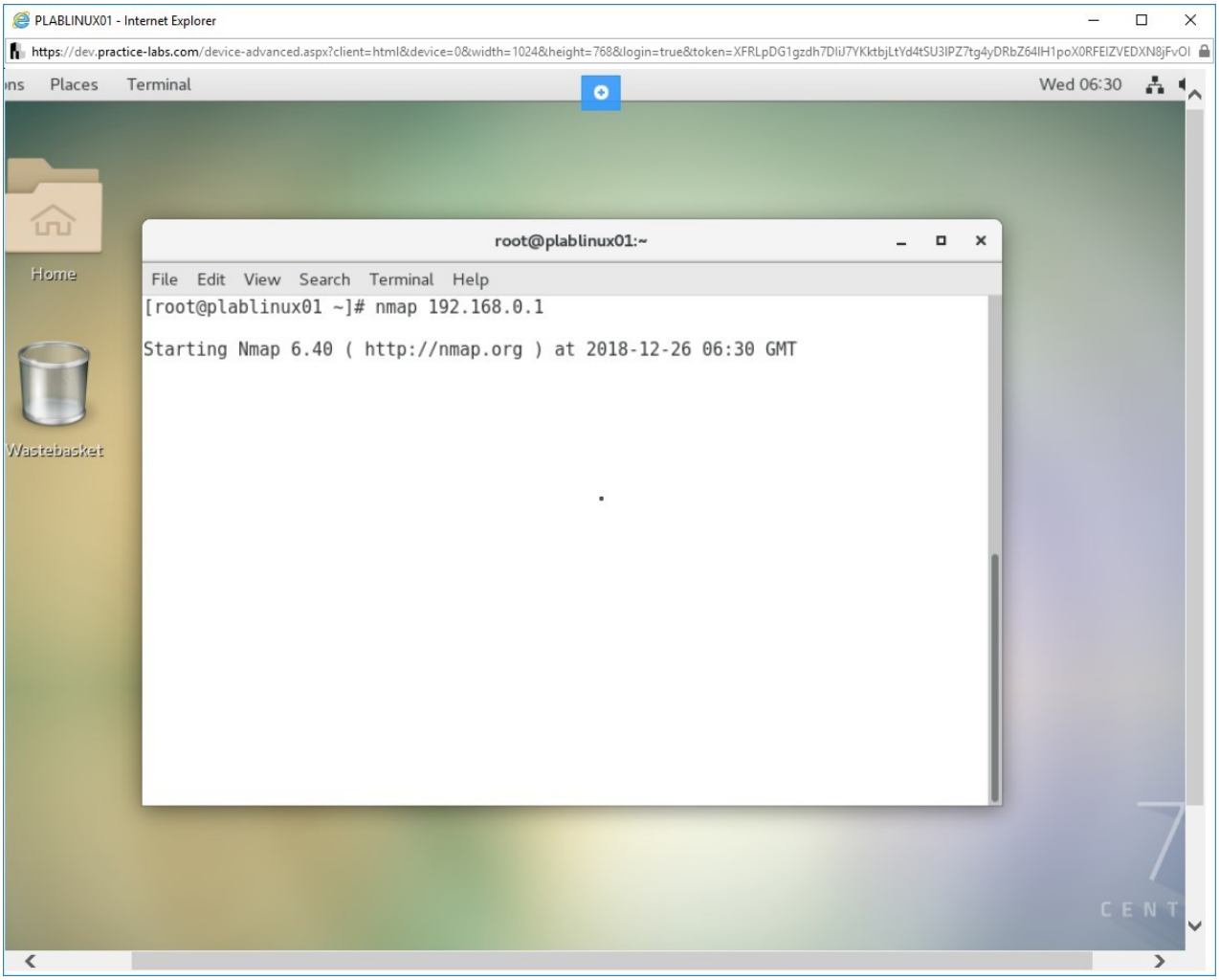


Figure 1.55 Screenshot of PLABLINUX01: Using the nmap command.

Step 6

The results are displayed.

The output shows the open ports with the protocols.

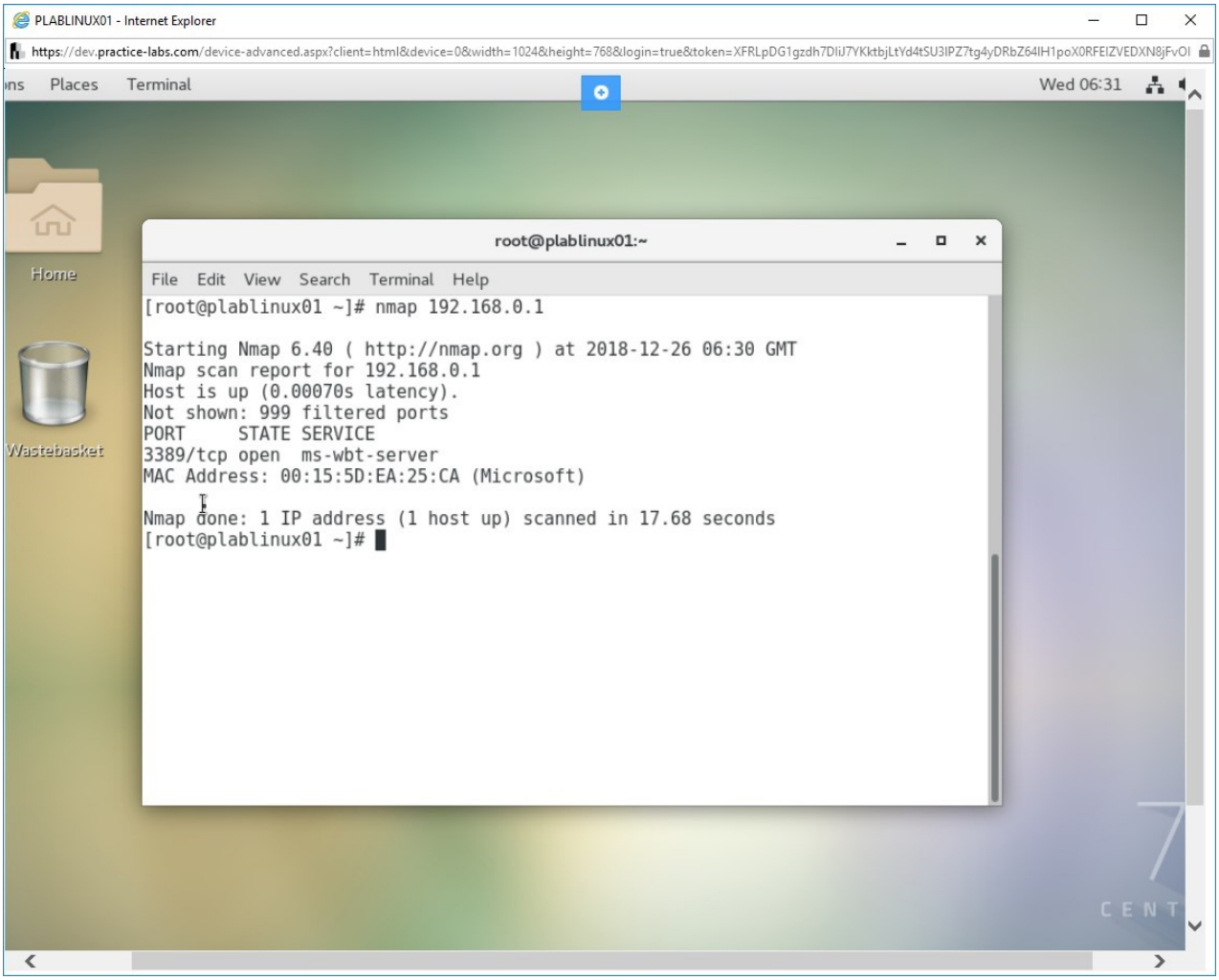


Figure 1.56 Screenshot of PLABLINUX01: Showing the result of the nmap command.

Step 7

You can also attempt to fingerprint the system, which means obtaining the system information including the operating system and its version, etc.

Type the following command:

```
nmap -O 192.168.0.1
```

Press **Enter**.

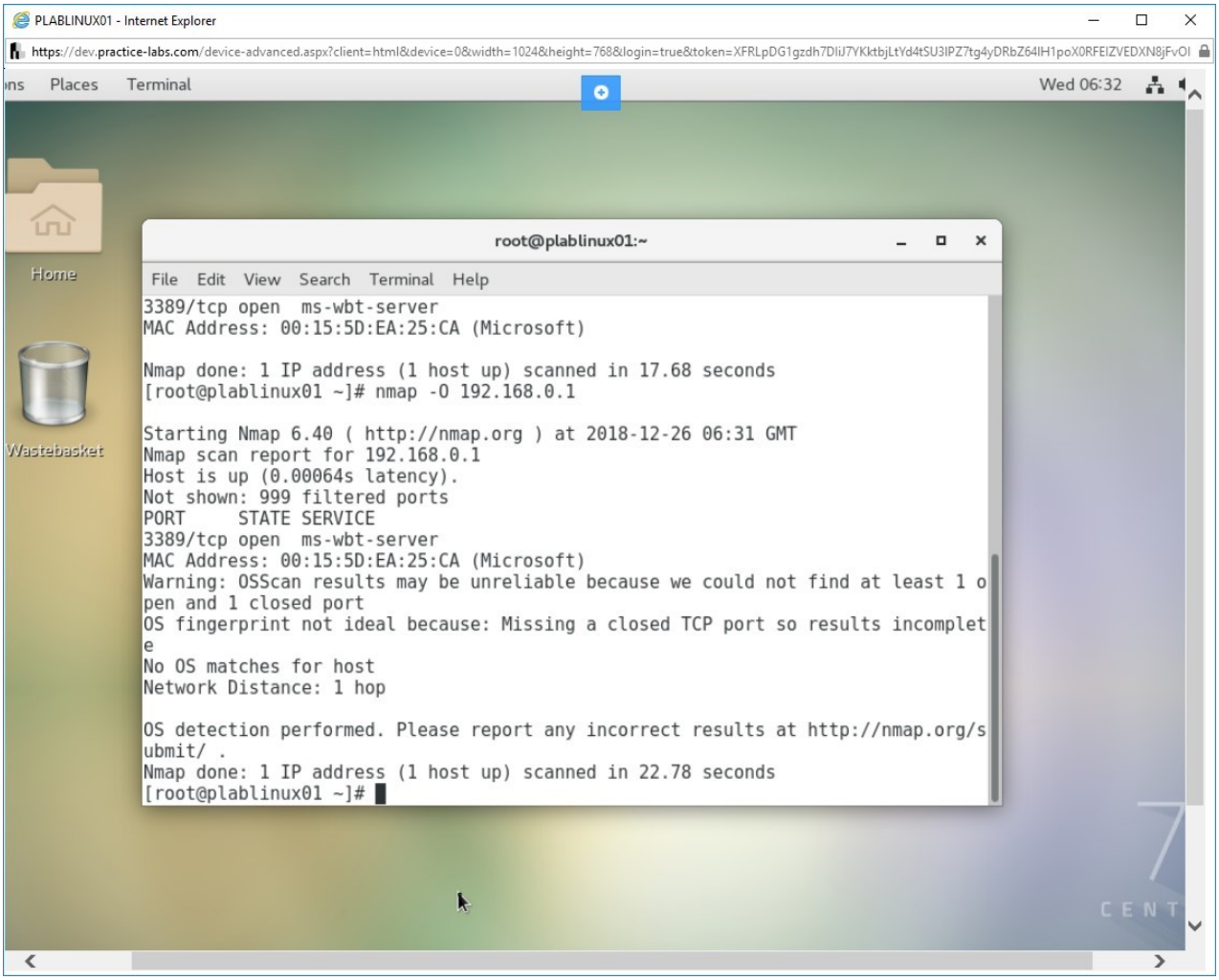


Figure 1.57 Screenshot of PLABLINUX01: Using nmap to fingerprint the system.

Step 8

Clear the screen with the following command:

```
clear
```

You can also scan a subnet of computers with the nmap command. Type the following command:

```
nmap -sP 192.168.0.0/24
```

Press **Enter**.

This command scans the 192.168.0.0 subnet.

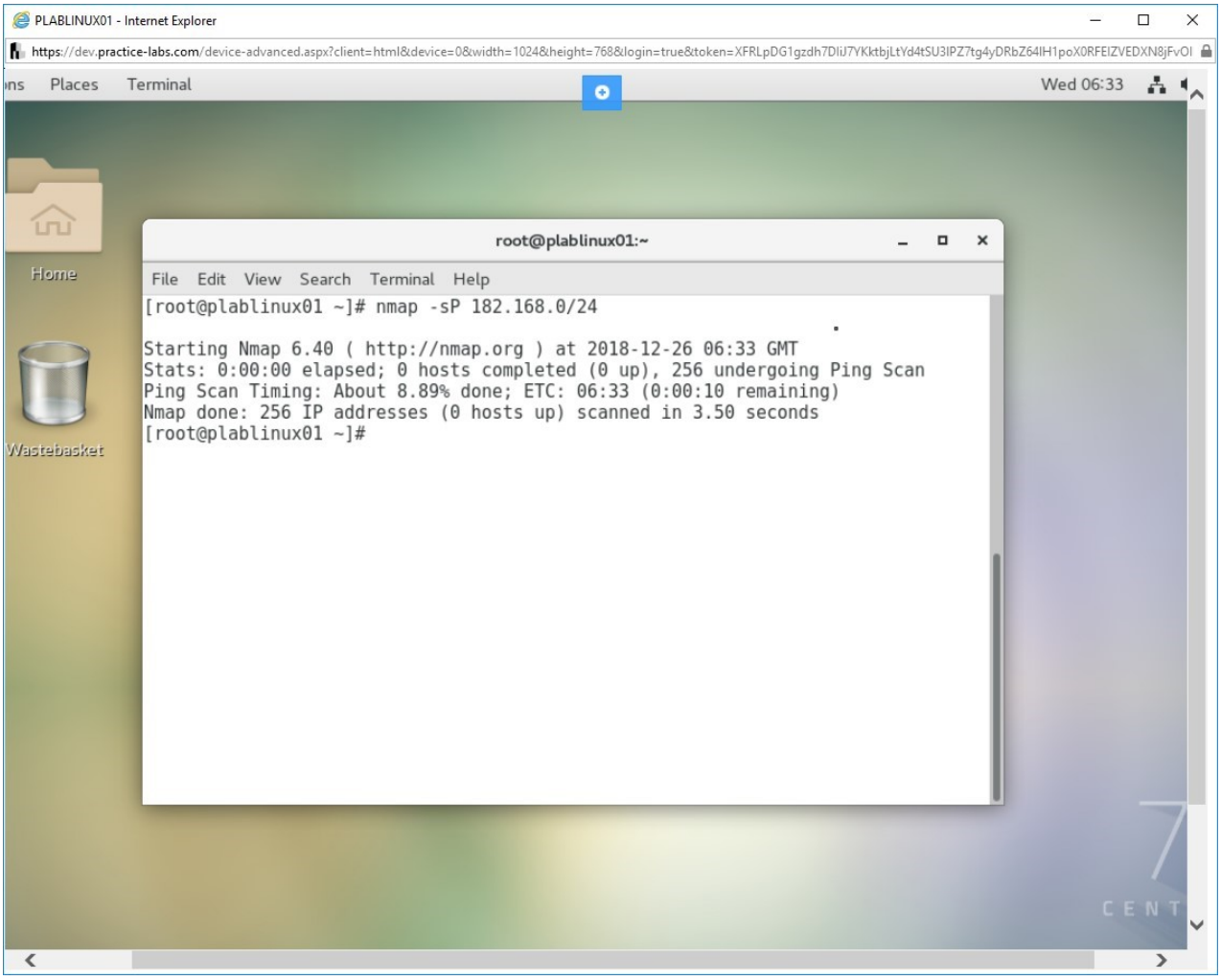


Figure 1.58 Screenshot of PLABLINUX01: Scanning a subnet of computers with the nmap command.

Step 9

Clear the screen with the following command:

```
clear
```

You can use the lsof command to list the open files on a system. Type the following command:

```
lsof
```

Press **Enter**.

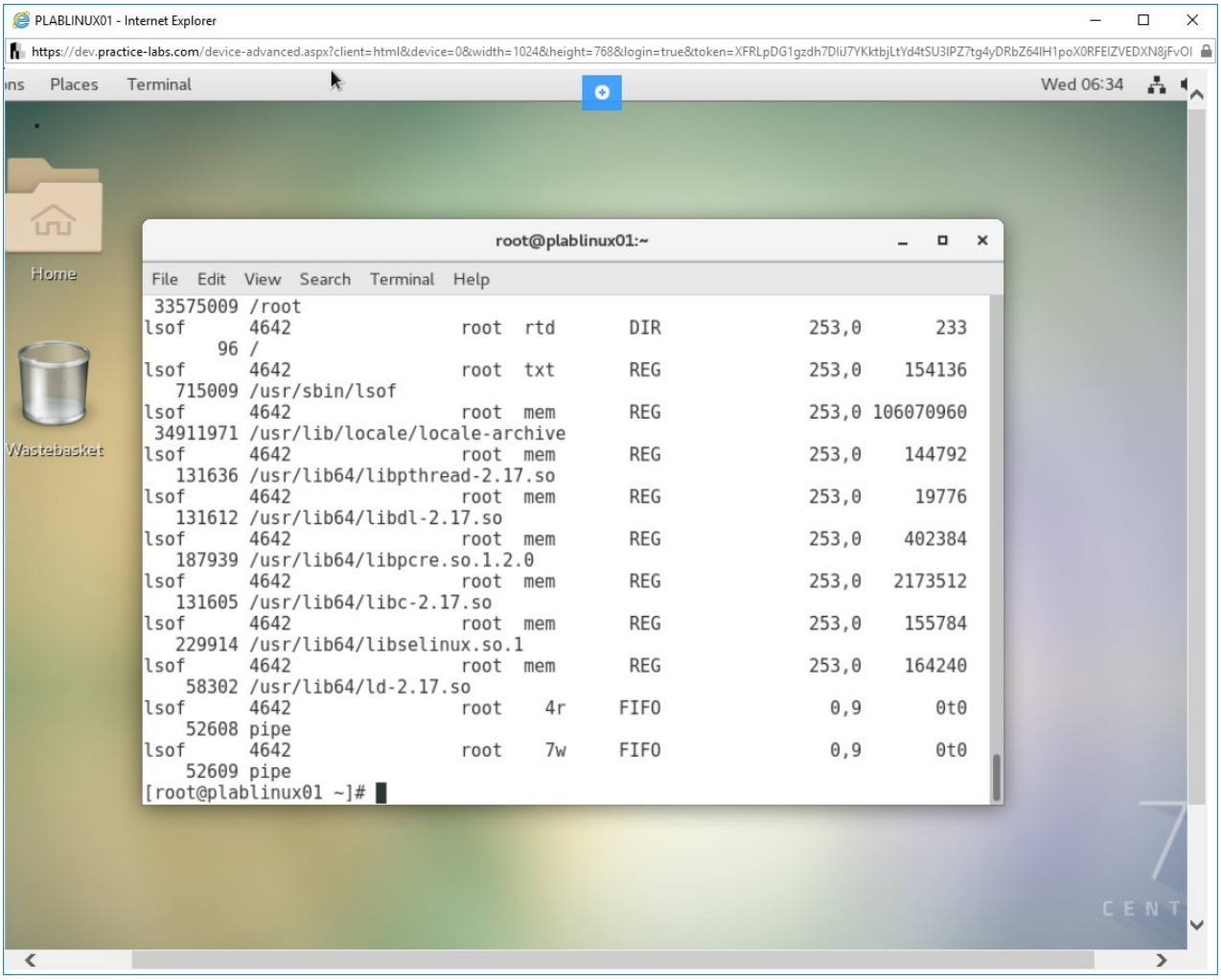


Figure 1.59 Screenshot of PLABLINUX01: Listing the open files on a system.

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

Review

Well done, you have completed the **Perform Security Administration Tasks** Practice Lab.

Summary

You completed the following exercise:

- Exercise 1 - Perform Security Administration Tasks

You should now be able to:

- Find files with the suid/sgid bit set
- Manage user passwords and password-aging information
- List the users logged into the system
- Use the su command
- Use the sudo command
- Manage shell resources
- Discover open ports on a system

Feedback

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