

Work with Pluggable Authentication Modules (PAM)

- **Introduction**
 - **Lab Topology**
 - **Exercise 1 - Work with Pluggable Authentication Modules (PAM)**
 - **Review**
-

Introduction

Welcome to the **Work with Pluggable Authentication Modules (PAM)** Practice Lab. In this module you will be provided with the instructions and devices needed to develop your hands-on skills.

Linux System

CentOS

PAM

Pluggable Authentication Modules

Learning Outcomes

In this module, you will complete the following exercise:

- Exercise 1 - Work with Pluggable Authentication Modules (PAM)

After completing this lab, you will be able to:

- Configure Network on CentOS
- Perform PAM Configuration
- Test PAM Configuration

Exam Objectives

The following exam objectives are covered in this lab:

- **LPI:** 110.1 Perform security administration tasks
- **CompTIA:** 3.2 Given a scenario, configure and implement appropriate access and authentication methods.

***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 - Work with Pluggable Authentication Modules (PAM)

PAM, or Pluggable Authentication Modules, is now installed on most recent versions of several Linux flavors. However, to be able to use it, you need to perform basic configuration. You can also add rules as part of the advanced configuration. Some of the key files and directories in PAM are:

- /etc/pam.conf
- /etc/pam.d/
- /lib/libpam.so.*
- /usr/lib/libpam.so.*

In this exercise, you will learn to work with PAM.

Learning Outcomes

After completing this exercise, you will be able to:

- Log into a Linux System
- Configure Network on CentOS
- Perform PAM Configuration
- Test PAM Configuration

Your Devices

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

- **PLABLINUX01** (CentOS Server)



Task 1 - Configure Network on CentOS

For a client to communicate on the network, it needs to have an IP address. If the client exists on the IPv4 network, then the client must have an IPv4 address. On the IPv6 network, the client must have IPv6 address.

In this task, you will configure an IP address on the client. To do this, perform the following steps:

Step 1

Connect to **PLABLINUX01**.

Click **Applications**, select **System Tools**, and then select **Settings**.

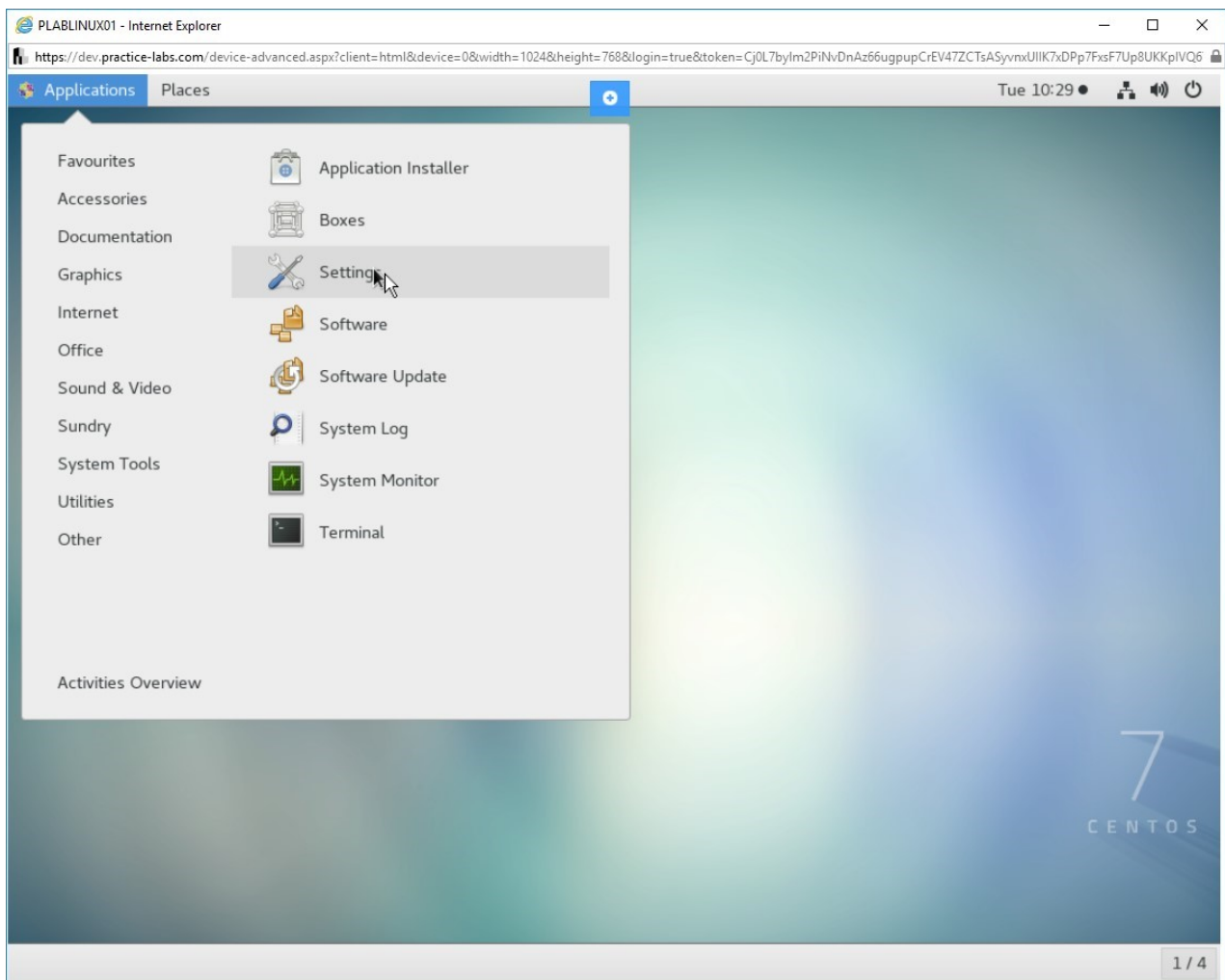


Figure 1.1 Screenshot of PLABLINUX01: Selecting the Settings option from the Applications > System Tools menu.

Step 2

From the **Settings** window, click **Network** in the left pane and then click the icon next to **ON** in the **Wired** section.

Note: If the **Wired** button is set to **OFF**, click the button on its left to switch it to **ON**.

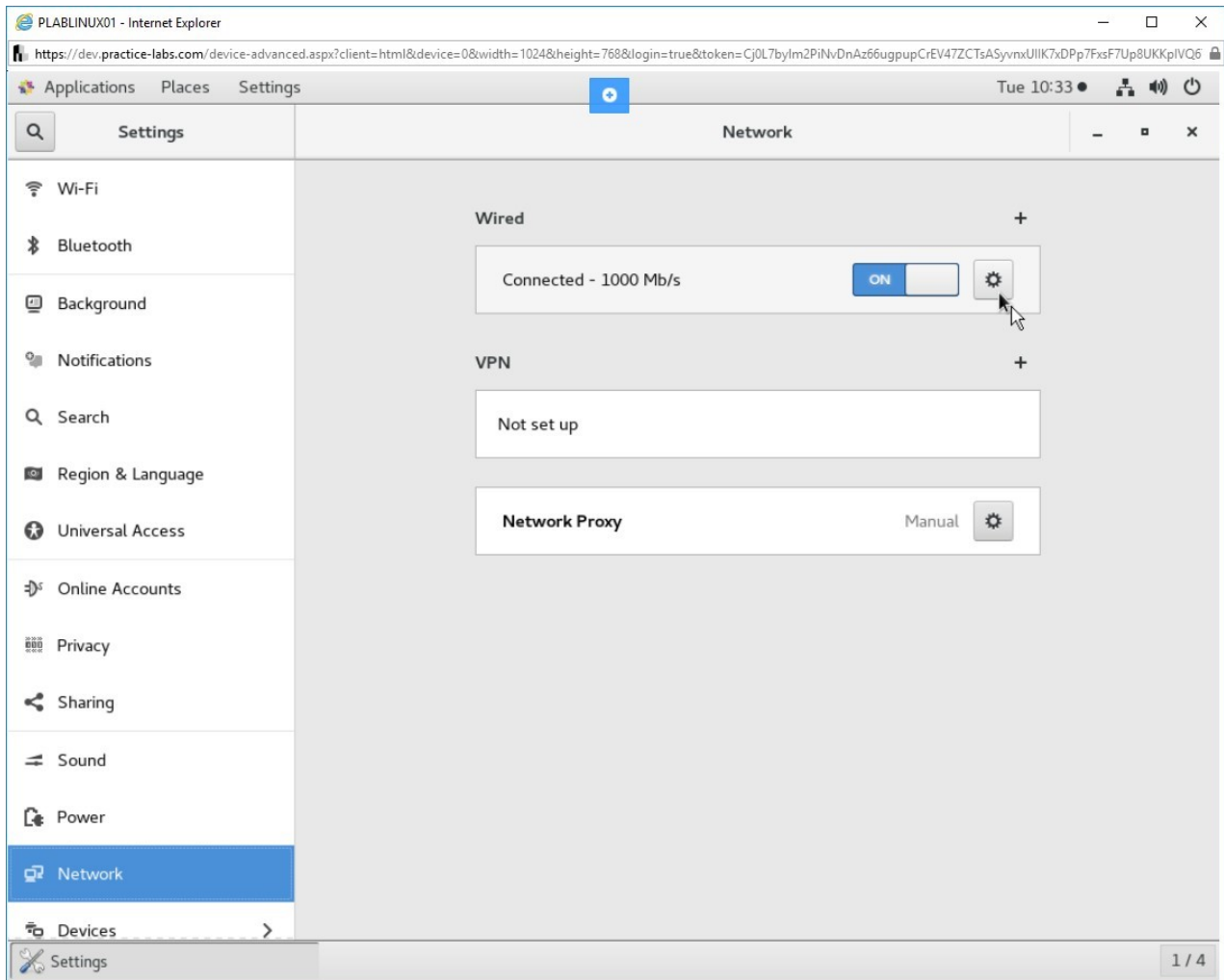


Figure 1.2 Screenshot of PLABLINUX01: Clicking the button to invoke the Wired dialog box.

Step 3

In the **Wired** dialog box, click the **IPv4** tab.

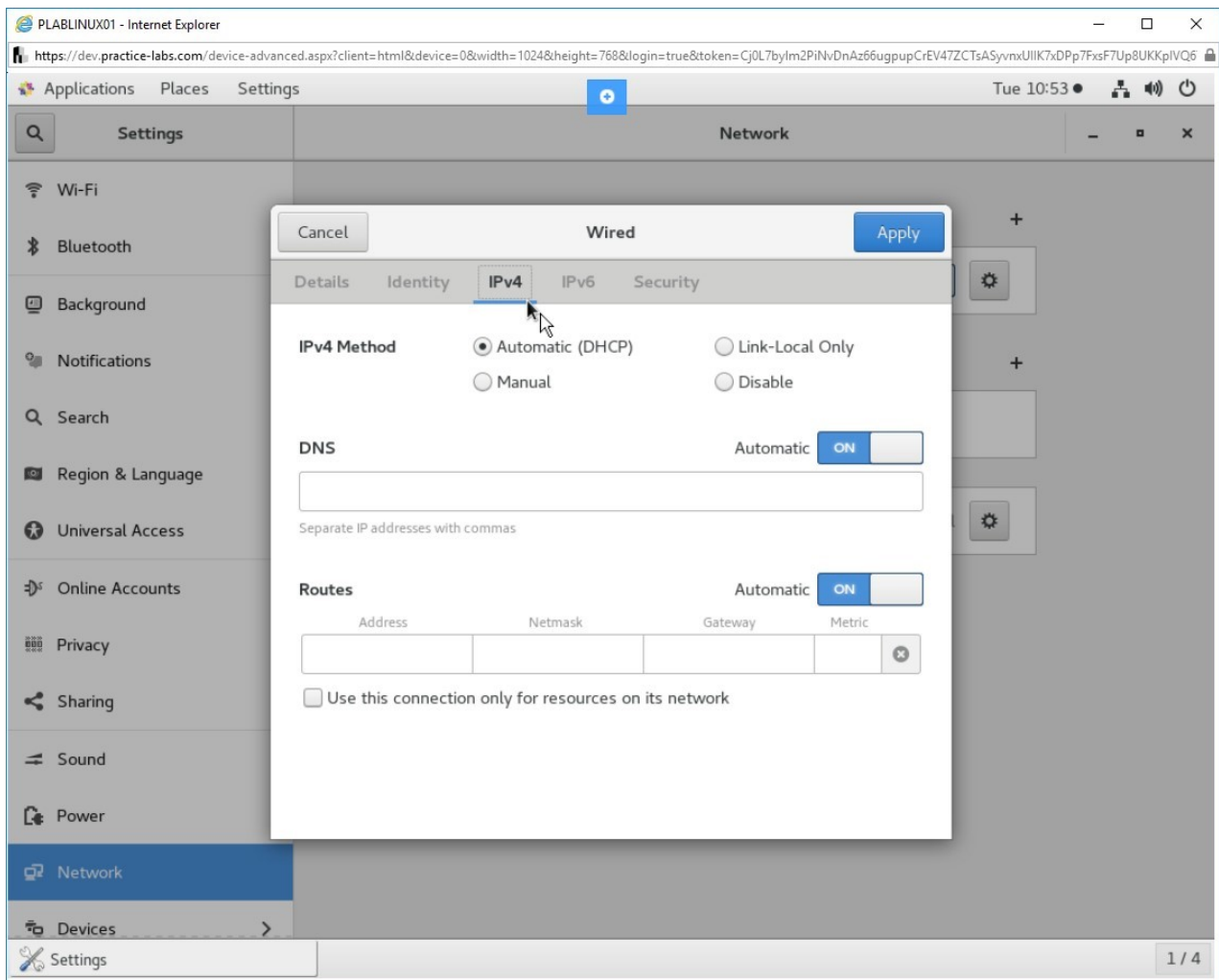


Figure 1.3 Screenshot of PLABLINUX01: Selecting the IPv4 tab in the Wired dialog box.

Step 4

Select **Manual** and provide the following details:

Address:

192.168.0.2

Netmask:

255.255.255.0

Gateway:

192.168.0.250

Click **Apply**.

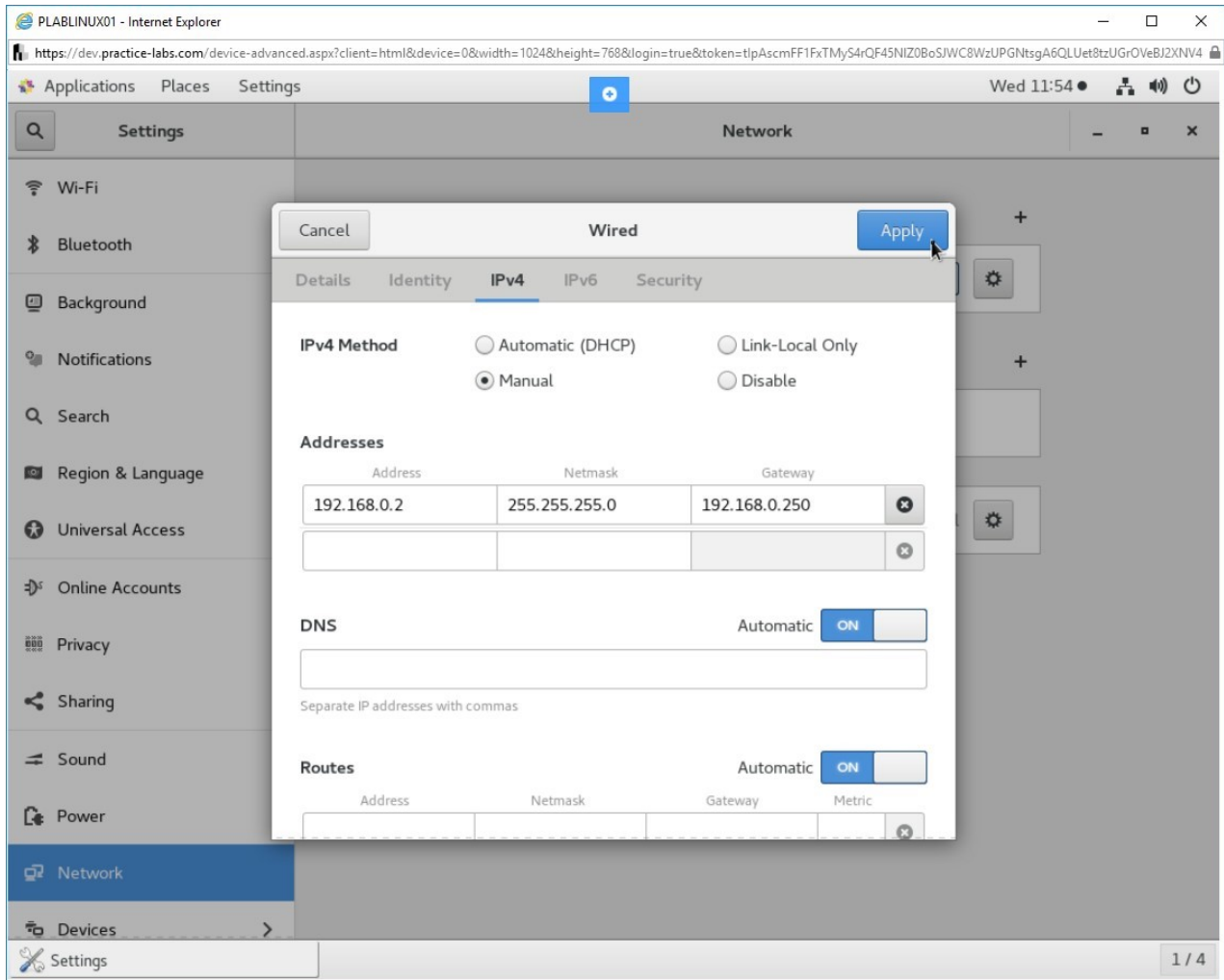


Figure 1.4 Screenshot of PLABLINUX01: Entering the network information and then clicking the Apply button.

Step 5

The **Wired** dialog box is closed automatically. Close the **Settings** window.

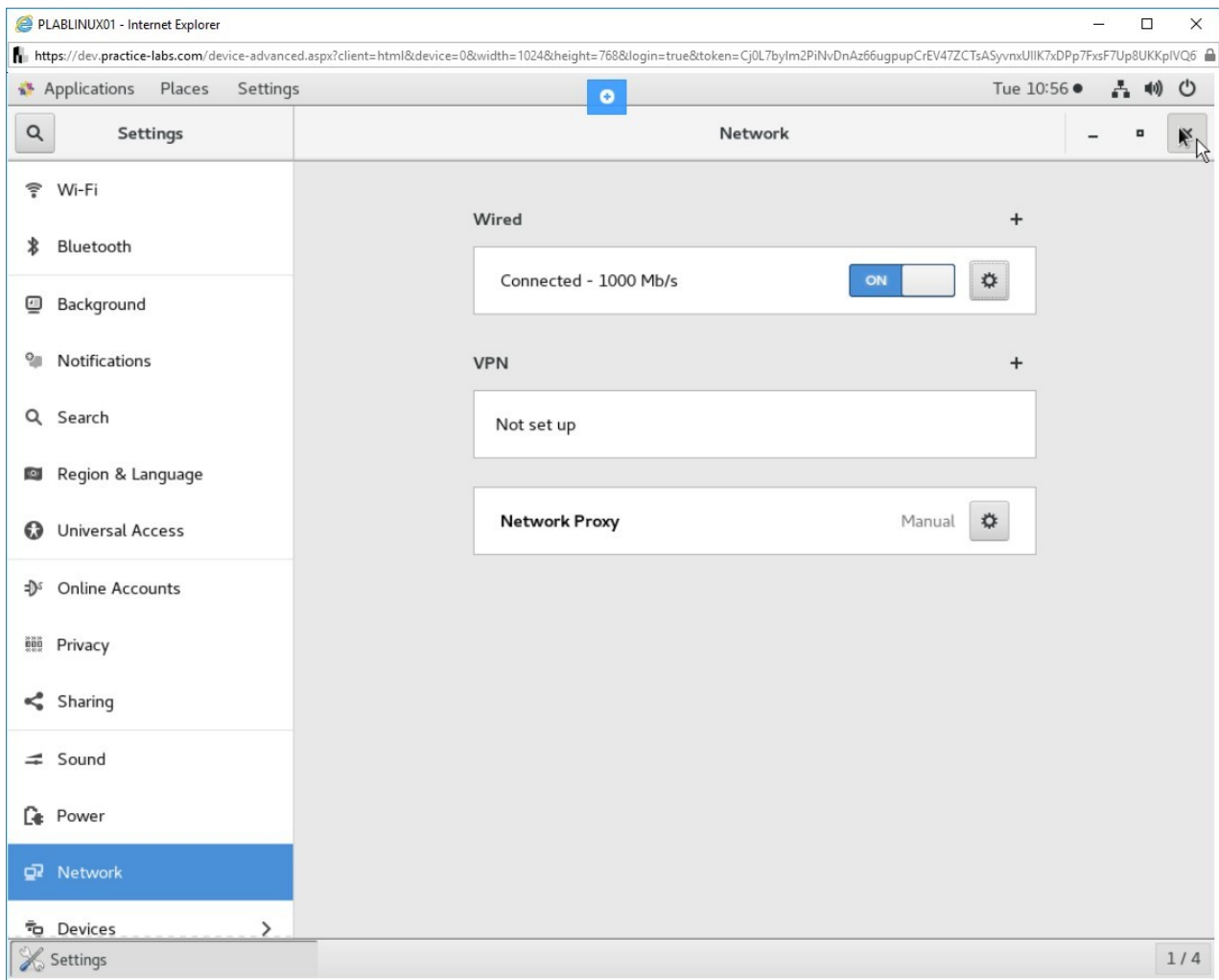


Figure 1.5 Screenshot of PLABLINUX01: Displaying the Settings window.

Task 2 - Perform PAM Configuration

Before you can use PAM, you need to perform basic configuration. You can also perform advanced configuration. This task focuses on the basic configuration only.

In this task, you will learn to perform the PAM configuration. To perform PAM configuration, perform the following steps:

Step 1

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

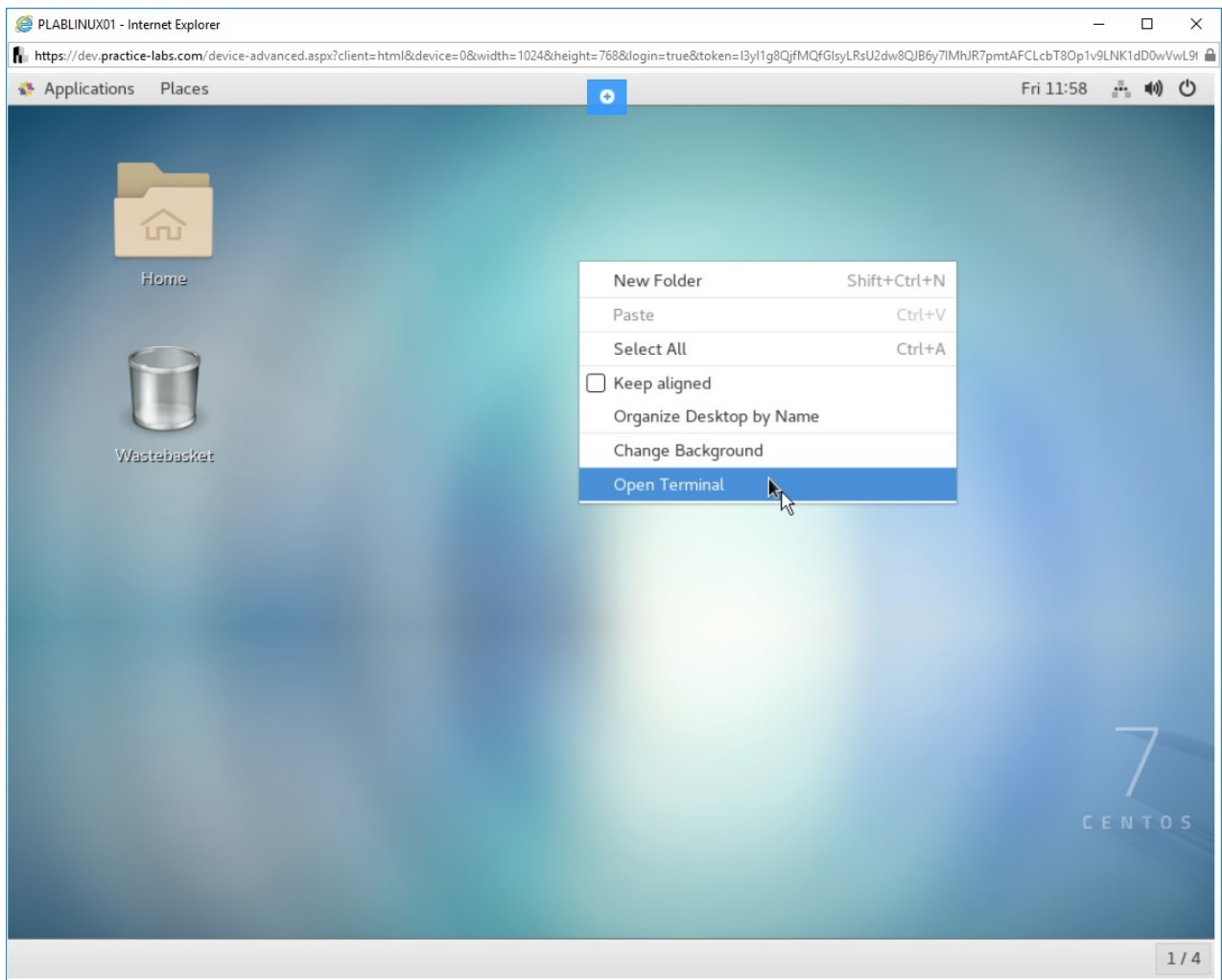


Figure 1.6 Screenshot of PLABLINUX01: Selecting the Open Terminal option from the context menu.

Step 2

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

```
su -
```

Press **Enter**.

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

Passw0rd

Press **Enter**.

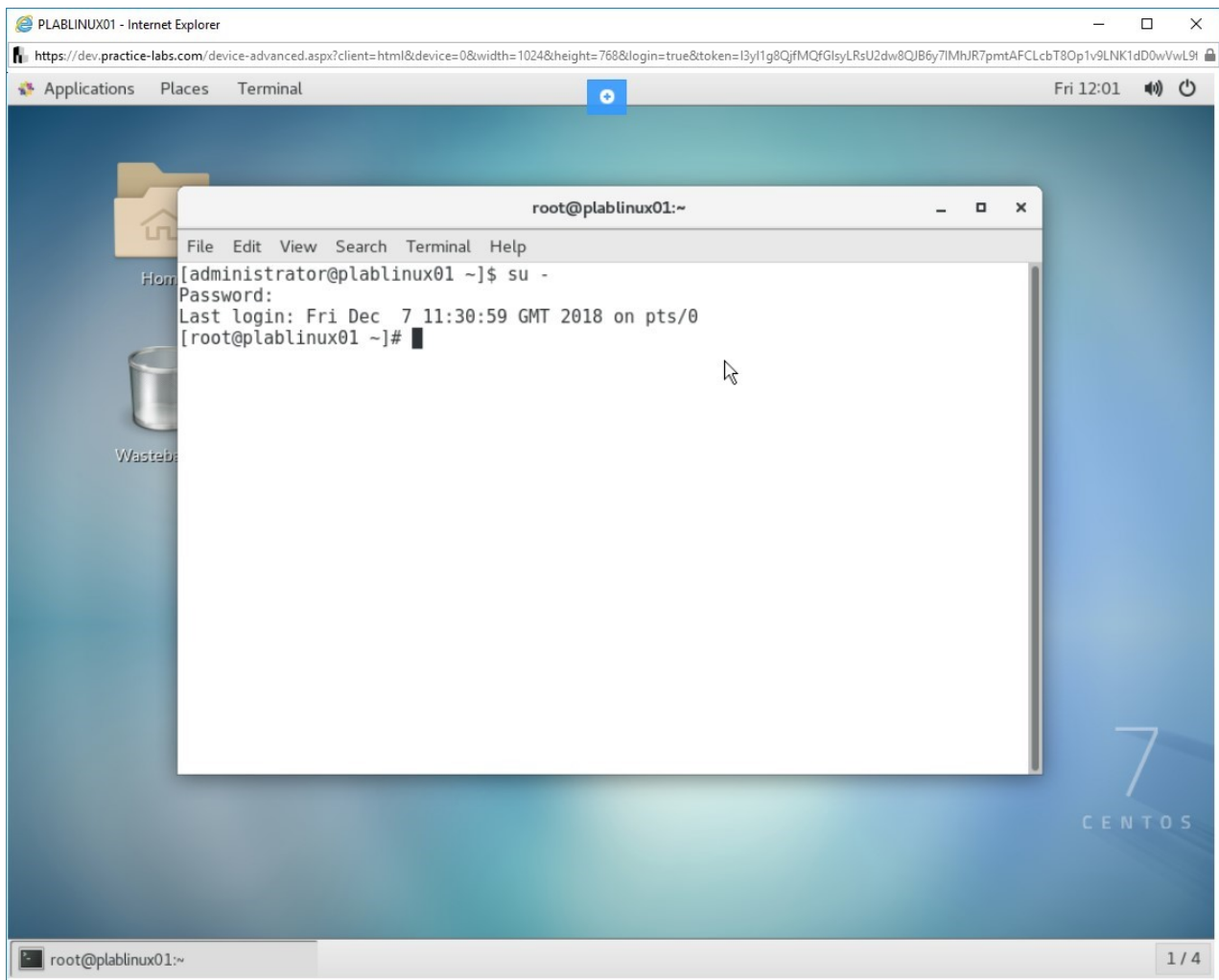


Figure 1.7 Screenshot of PLABLINUX01: Changing the account to the root account with the su command.

Step 3

Clear the screen by entering the following command:

```
clear
```

You should first update the packages on your system. Type the following command:

```
yum update
```

Press **Enter**. Notice that you are prompted to confirm the installation.

Note: There may be a possibility that the CentOS device is updated. In that case, Step 4 and 5 will not be required.

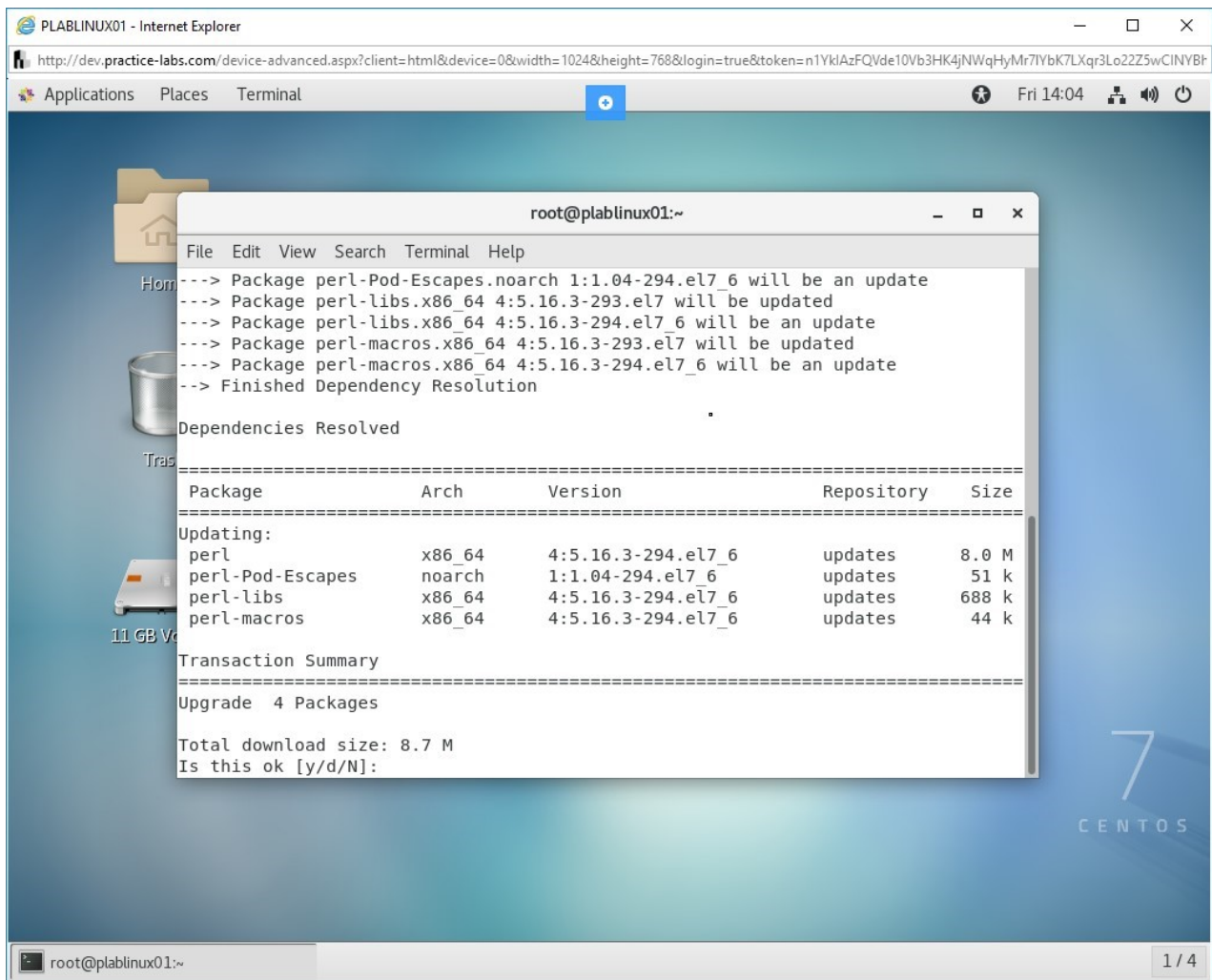


Figure 1.8 Screenshot of PLABLINUX01: Updating the packages on the system.

Step 4

To confirm the installation, type the following command:

y

Press **Enter**. The package updation will continue.

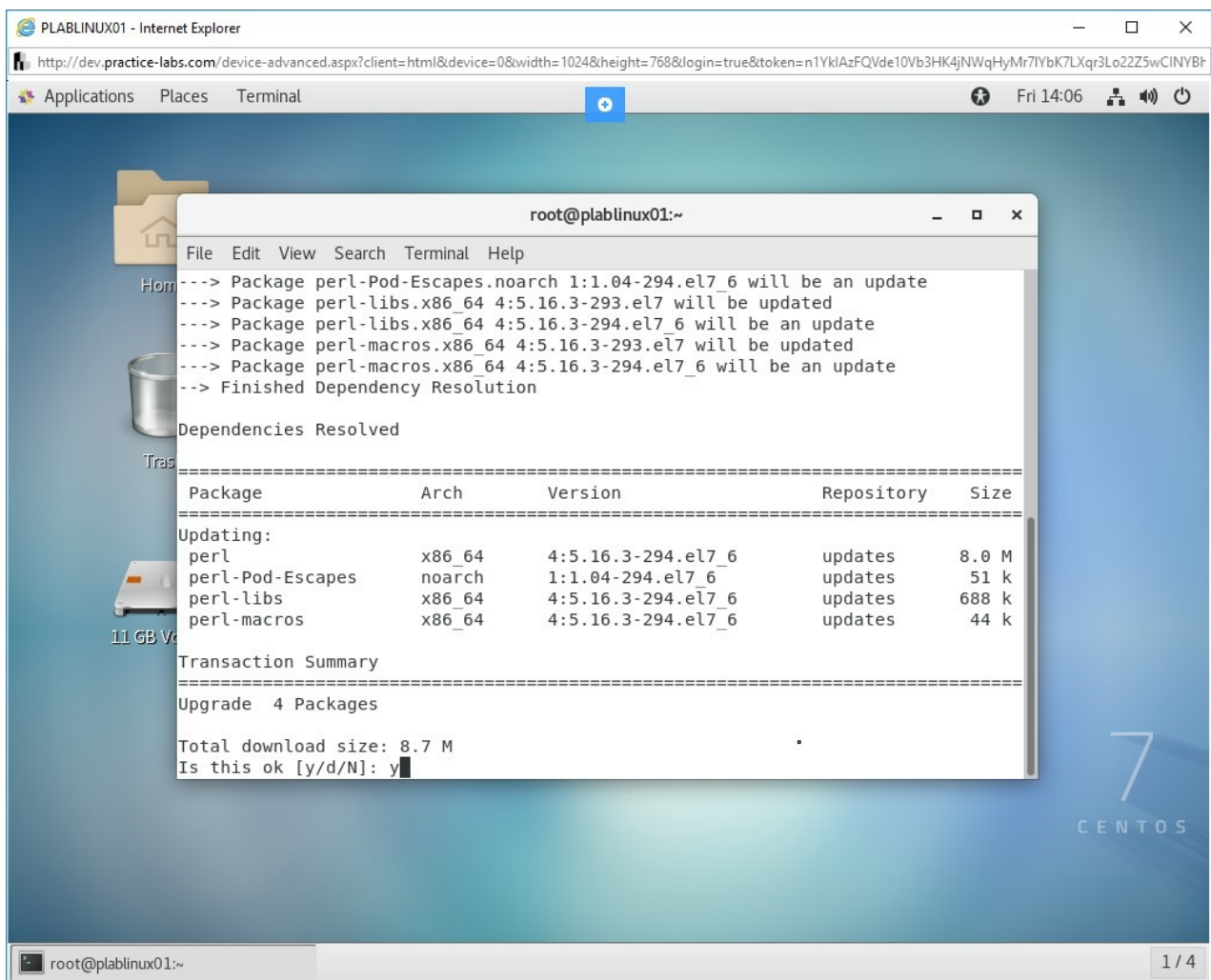


Figure 1.9 Screenshot of PLABLINUX01: Confirming the updation of packages.

Step 5

After the updation is complete, you will the **Complete!** message.

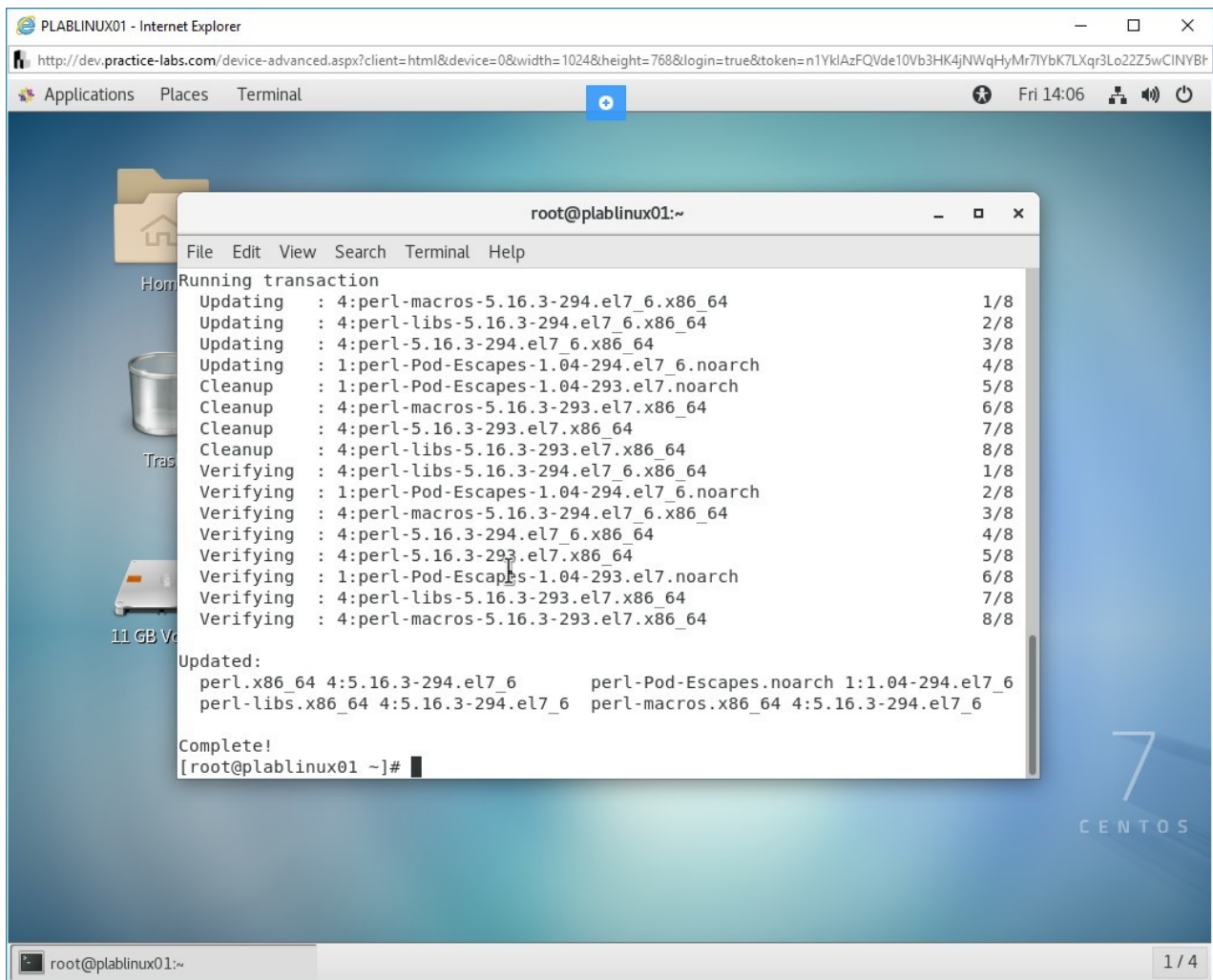


Figure 1.10 Screenshot of PLABLINUX01: Showing the completion message.

Step 6

Clear the screen by entering the following command:

```
clear
```

You will check if the PAM package is installed. To do this, type the following command:

```
rpm -qa | grep pam
```

Press **Enter**. Notice that the PAM package is already installed.

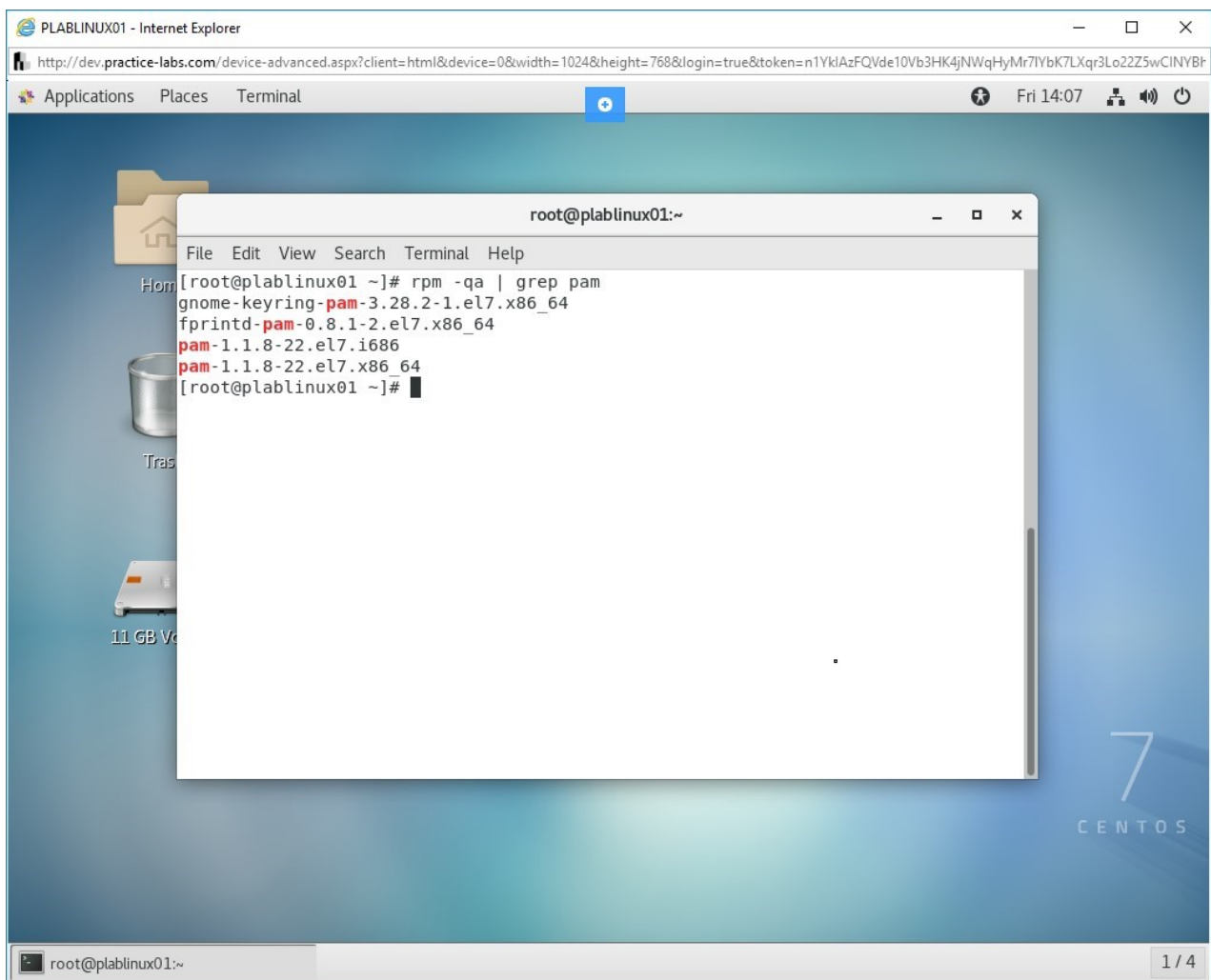


Figure 1.11 Screenshot of PLABLINUX01: Checking if the PAM package is installed.

Step 7

Next, you need to check if a package, such as **sshd**, is PAM-aware. For this purpose, you can use the **ldd** command. Type the following command:

```
ldd /usr/sbin/sshd | grep libpam.so
```

Press **Enter**.

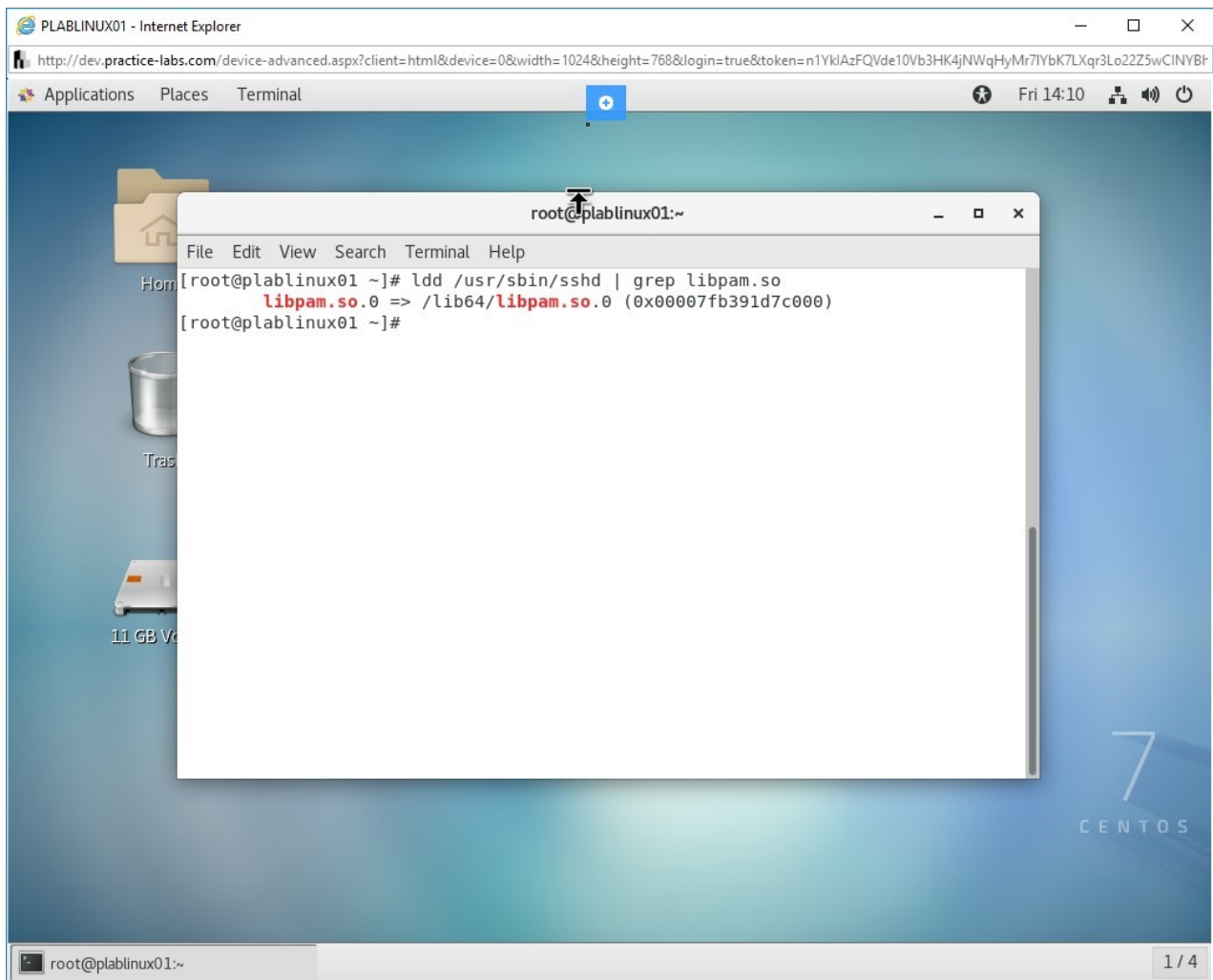


Figure 1.12 Screenshot of PLABLINUX01: Checking if sshd is PAM-aware.

Step 8

Clear the screen by entering the following command:

```
clear
```

You can use PAM to disable the root user's SSH access to a system. You will now disable the root user access to PLABLINUX01 by:

- restricting access to login
- restricting access sshd services

You will add two files: `/etc/pam.d/sshd` and `/etc/pam.d/login`

Let's first edit the `/etc/pam.d/sshd` file. Type the following command:


```
gedit /etc/pam.d/sshd
```

Press **Enter**.

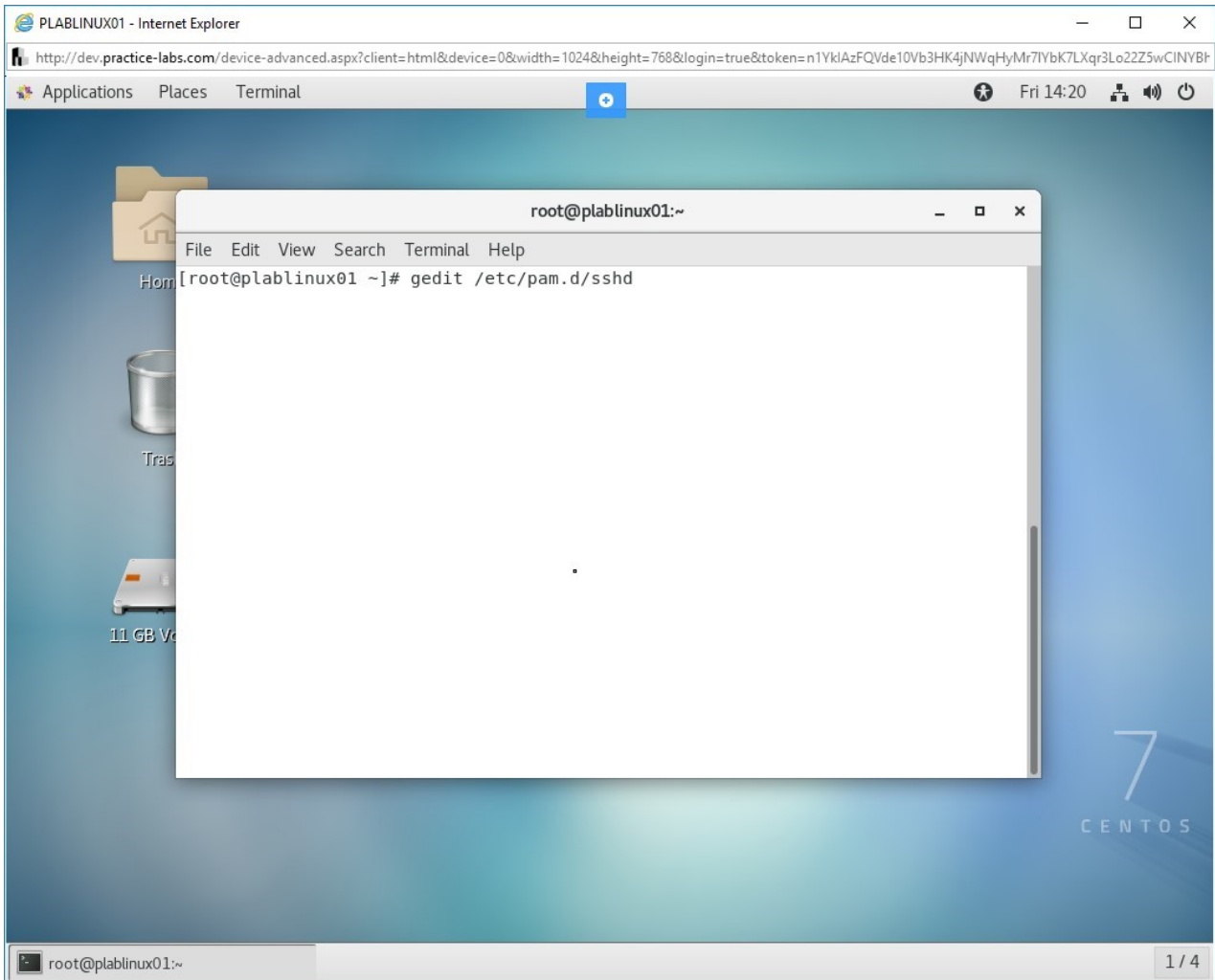


Figure 1.13 Screenshot of PLABLINUX01: Editing the /etc/pam.d/sshd file .

Step 9

Add the following rule in the /etc/pam.d/config file:

```
auth required pam_listfile.so \  
    onerr=succeed item=user sense=deny  
file=/etc/ssh/deniedusers
```

Press **Enter**.

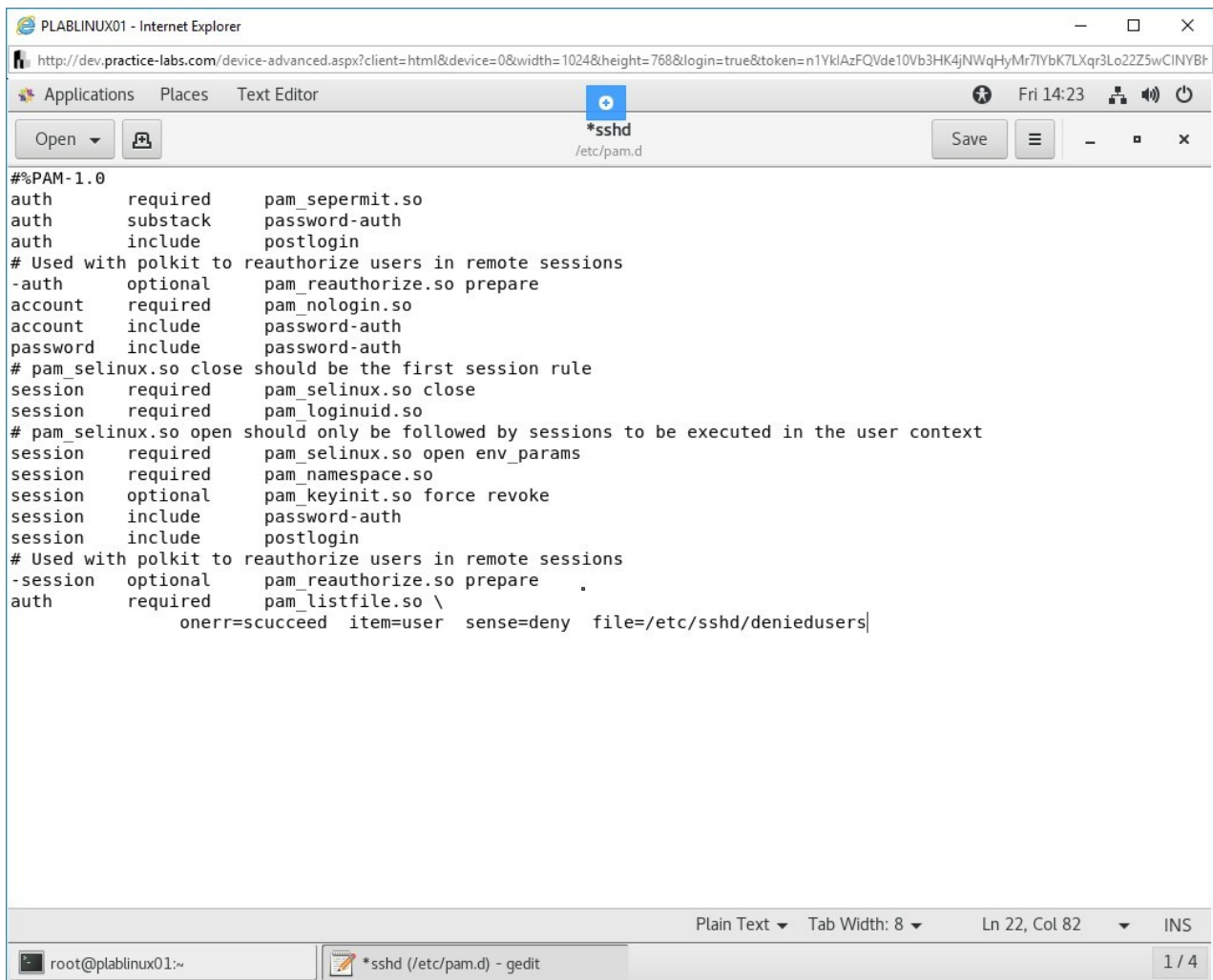


Figure 1.14 Screenshot of PLABLINUX01: Adding a rule in the /etc/pam.d/config file.

Step 10

Click **Save** to save the file. Then, close the file.

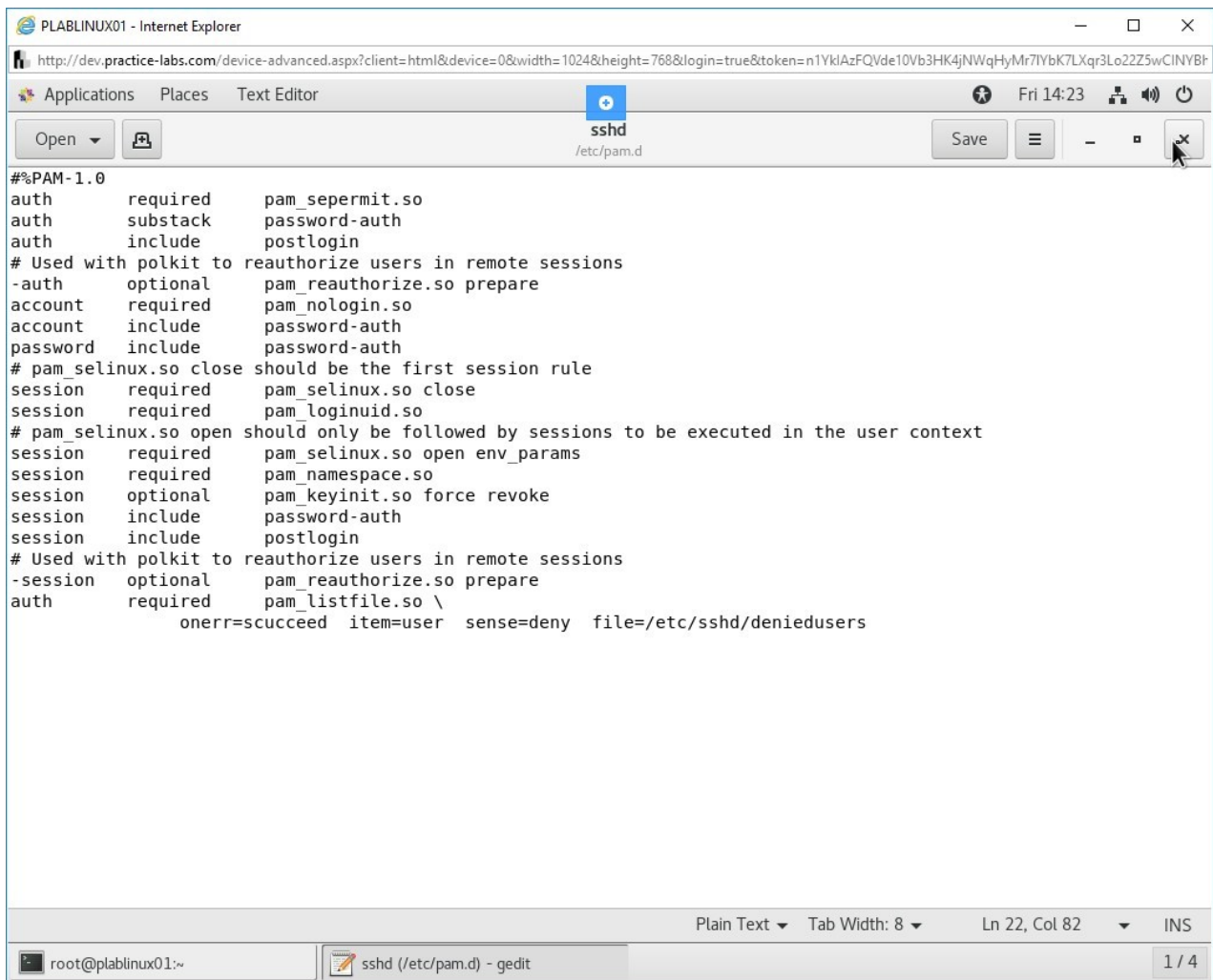


Figure 1.15 Screenshot of PLABLINUX01: Saving and closing the /etc/pam.d/config file.

Step 11

Clear the screen by entering the following command:

```
clear
```

Next, edit the **/etc/pam.d/login** file. Type the following command:

```
gedit /etc/pam.d/login
```

Press **Enter**.

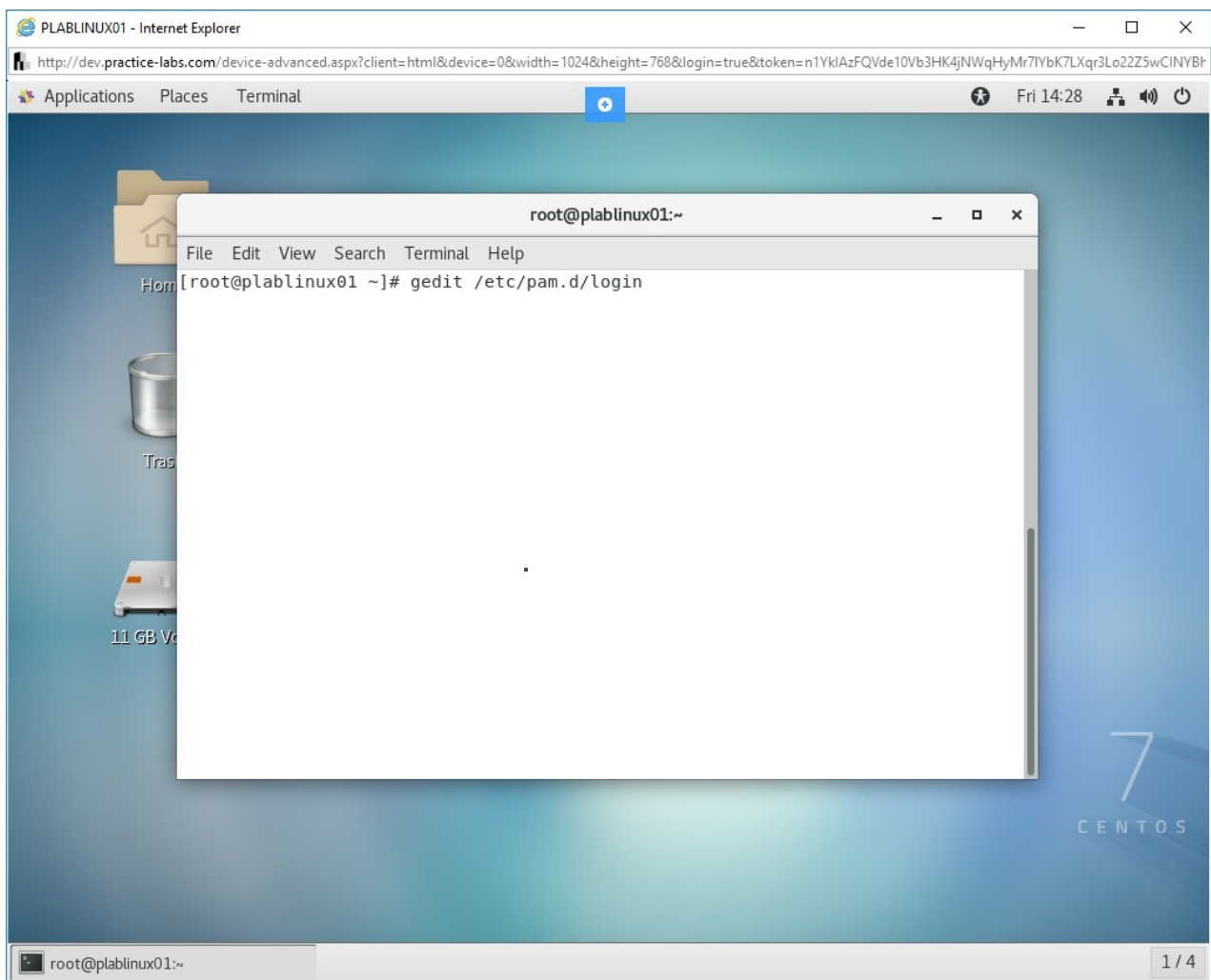


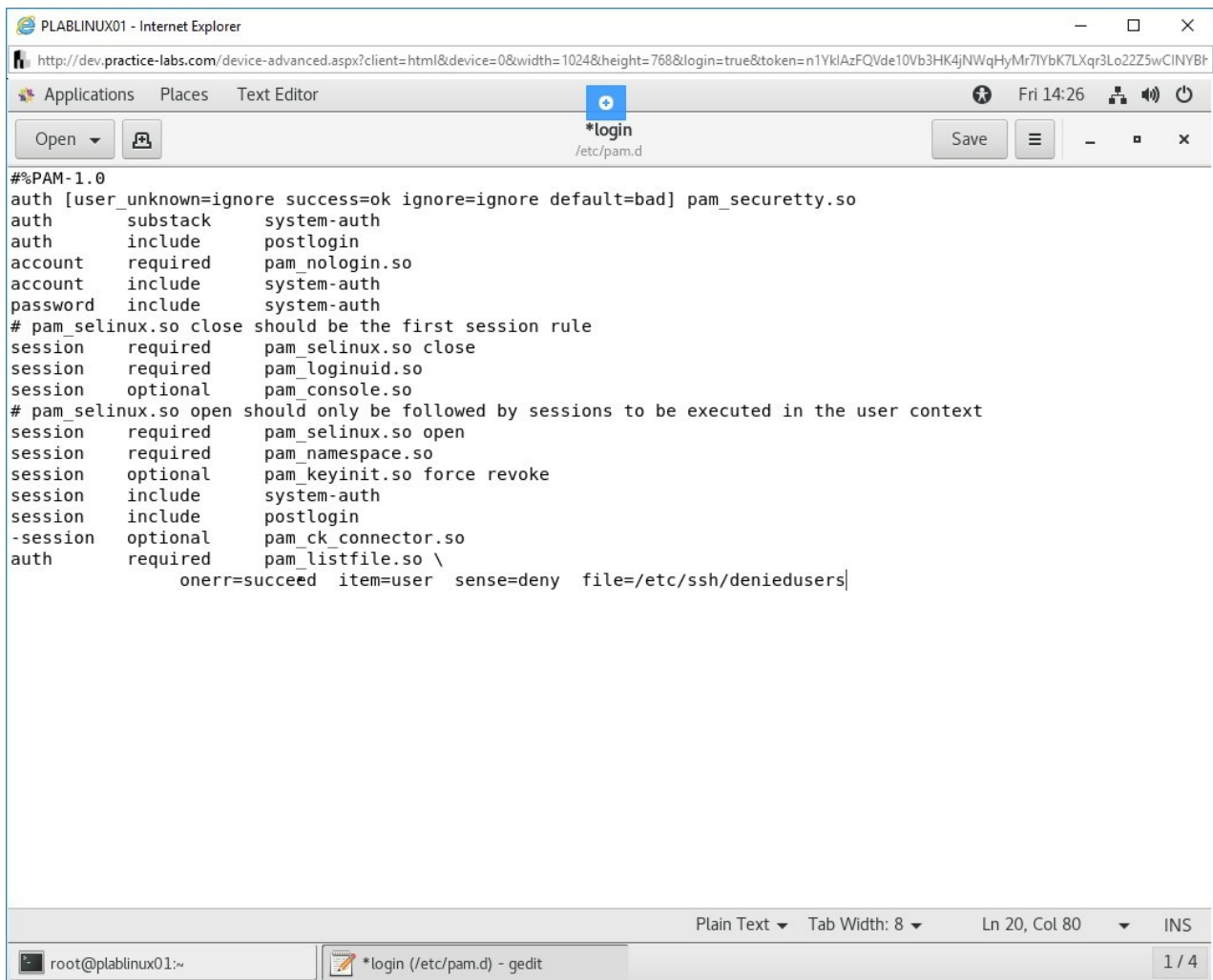
Figure 1.16 Screenshot of PLABLINUX01: Opening the `/etc/pam.d/login` file.

Step 12

Add the following rule in the `/etc/pam.d/login` file:

```
auth required pam_listfile.so \  
    onerr=succeed item=user sense=deny  
file=/etc/ssh/deniedusers
```

Press **Enter**.



The screenshot shows a web browser window titled "PLABLINUX01 - Internet Explorer". The address bar contains a URL from "dev.practice-labs.com". The browser's top bar shows "Applications", "Places", and "Text Editor" tabs. Below this, there's a toolbar with "Open", "Save", and other icons. The main content area displays a text editor window titled "*login (/etc/pam.d)". The text editor shows the following PAM configuration for the login file:

```
#%PAM-1.0
auth [user_unknown=ignore success=ok ignore=ignore default=bad] pam_securetty.so
auth      substack      system-auth
auth      include       postlogin
account   required      pam_nologin.so
account   include       system-auth
password  include       system-auth
# pam_selinux.so close should be the first session rule
session   required      pam_selinux.so close
session   required      pam_loginuid.so
session   optional      pam_console.so
# pam_selinux.so open should only be followed by sessions to be executed in the user context
session   required      pam_selinux.so open
session   required      pam_namespace.so
session   optional      pam_keyinit.so force revoke
session   include       system-auth
session   include       postlogin
-session  optional      pam_ck_connector.so
auth      required      pam_listfile.so \
            onerr=succeed item=user sense=deny file=/etc/ssh/deniedusers|
```

The status bar at the bottom of the browser shows "root@plablinux01:~" and a tab for "*login (/etc/pam.d) - gedit". The text editor's status bar indicates "Plain Text", "Tab Width: 8", "Ln 20, Col 80", and "INS".

Figure 1.17 Screenshot of PLABLINUX01: Adding a rule in the /etc/pam.d/login file.

Step 13

Click **Save** to save the file. Then, close the file.

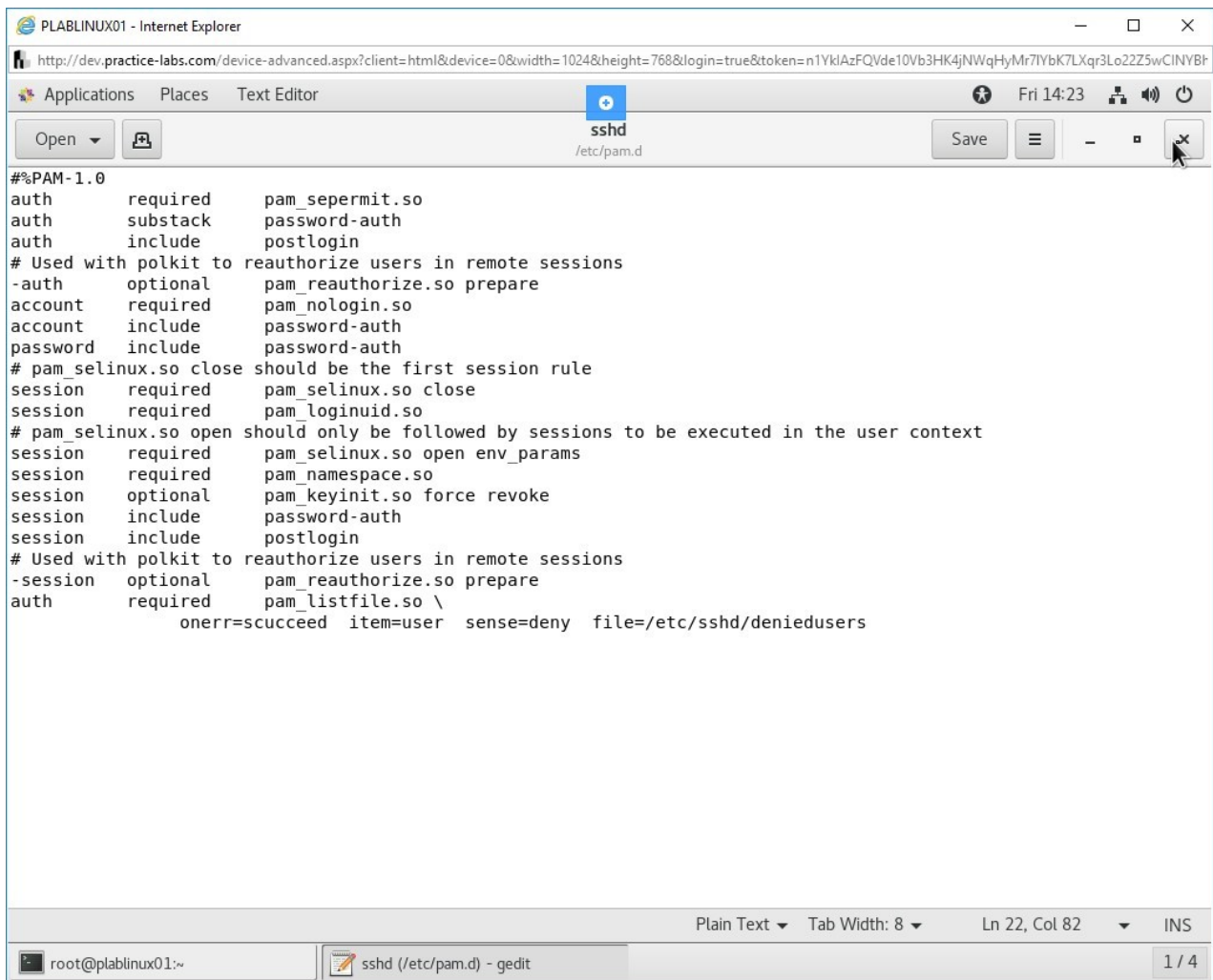


Figure 1.18 Screenshot of PLABLINUX01: Saving the /etc/pam.d/login file.

Step 14

Clear the screen by entering the following command:

```
clear
```

You will need to create a file named **/etc/ssh/deniedusers**. This is the file in which you will add the root user. Type the following command:

```
gedit /etc/ssh/deniedusers
```

Press **Enter**.

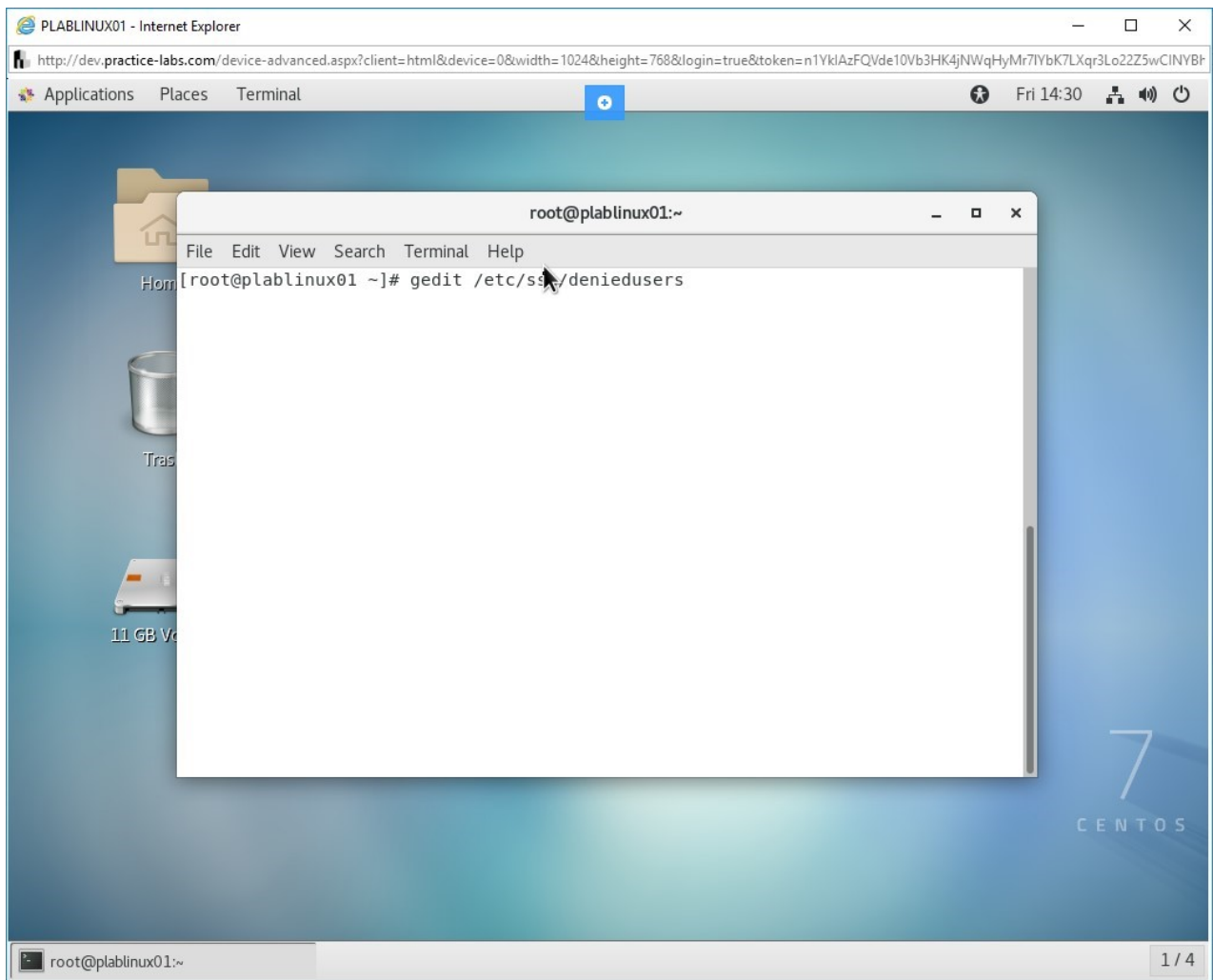


Figure 1.19 Screenshot of PLABLINUX01: Creating the `/etc/ssh/deniedusers` file.

Step 15

You need to add the root user in this file. Type the following:

```
root
```

Press **Enter**.

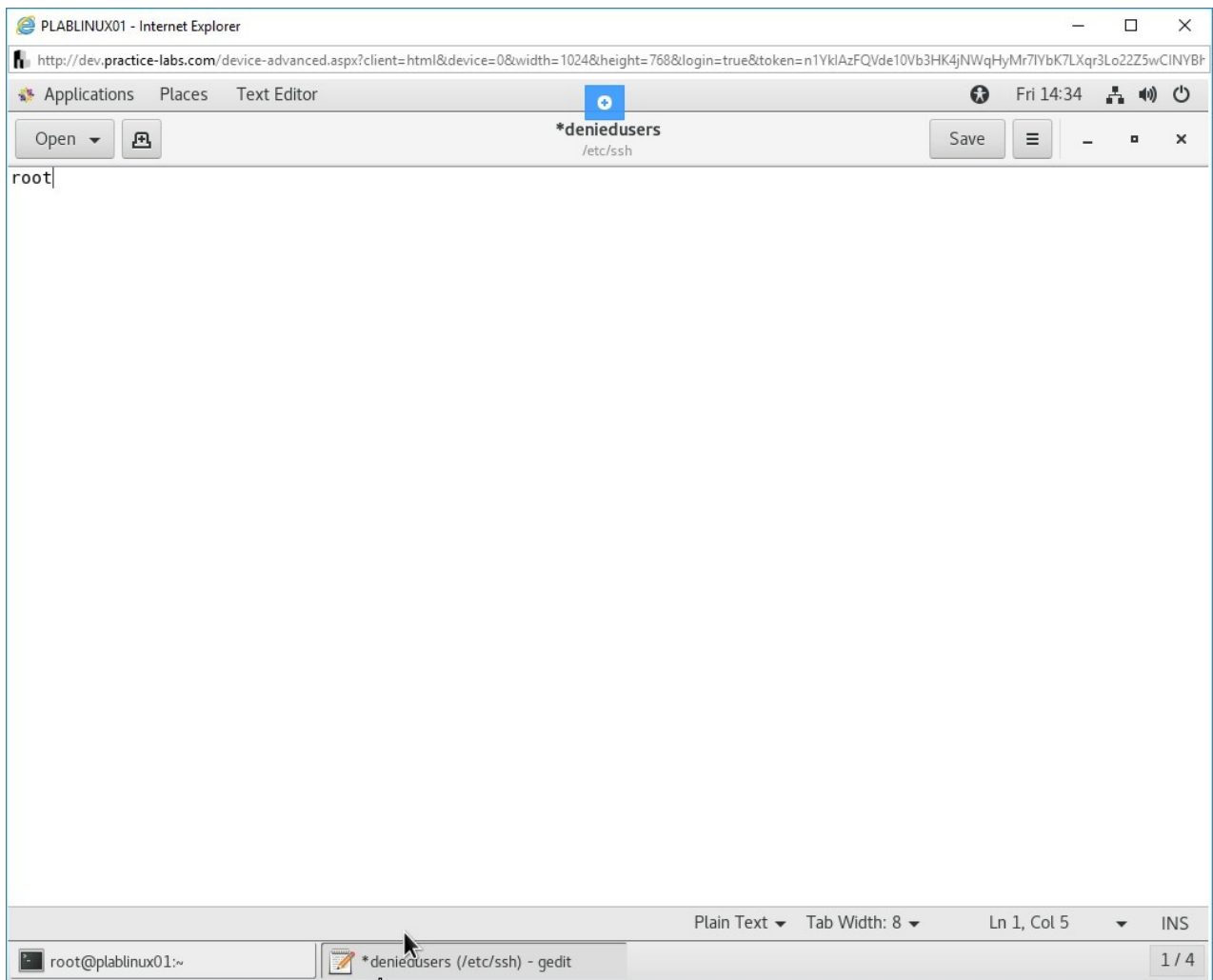


Figure 1.20 Screenshot of PLABLINUX01: Adding the root user in the /etc/ssh/deniedusers file.

Step 16

Click **Save** to save the file. Then, close the file.

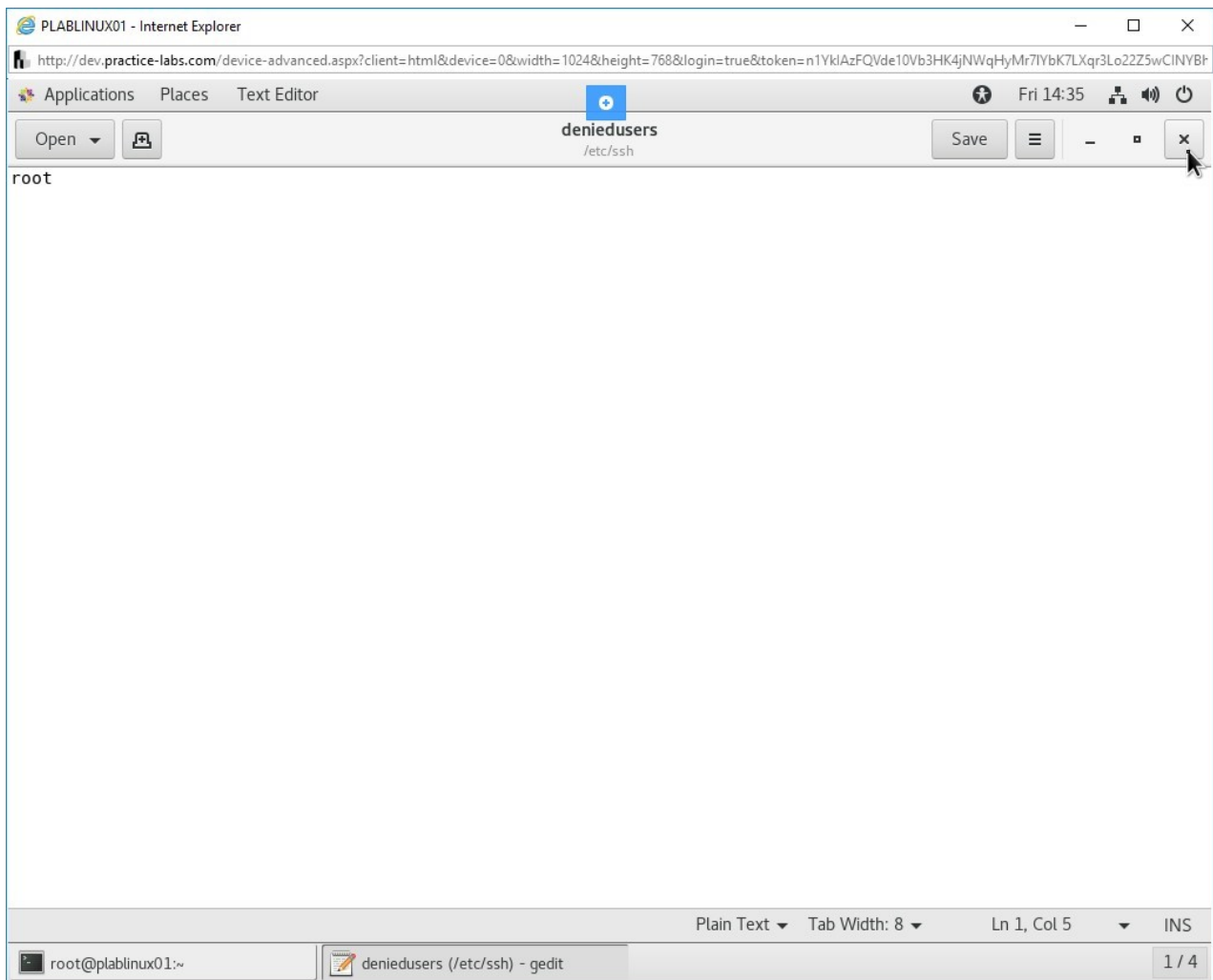


Figure 1.21 Screenshot of PLABLINUX01: Saving the `/etc/ssh/deniedusers` file.

Step 17

You should now set the permissions on the `/etc/ssh/deniedusers` file.

Type the following command:

```
chmod 600 /etc/ssh/deniedusers
```

Press **Enter**.

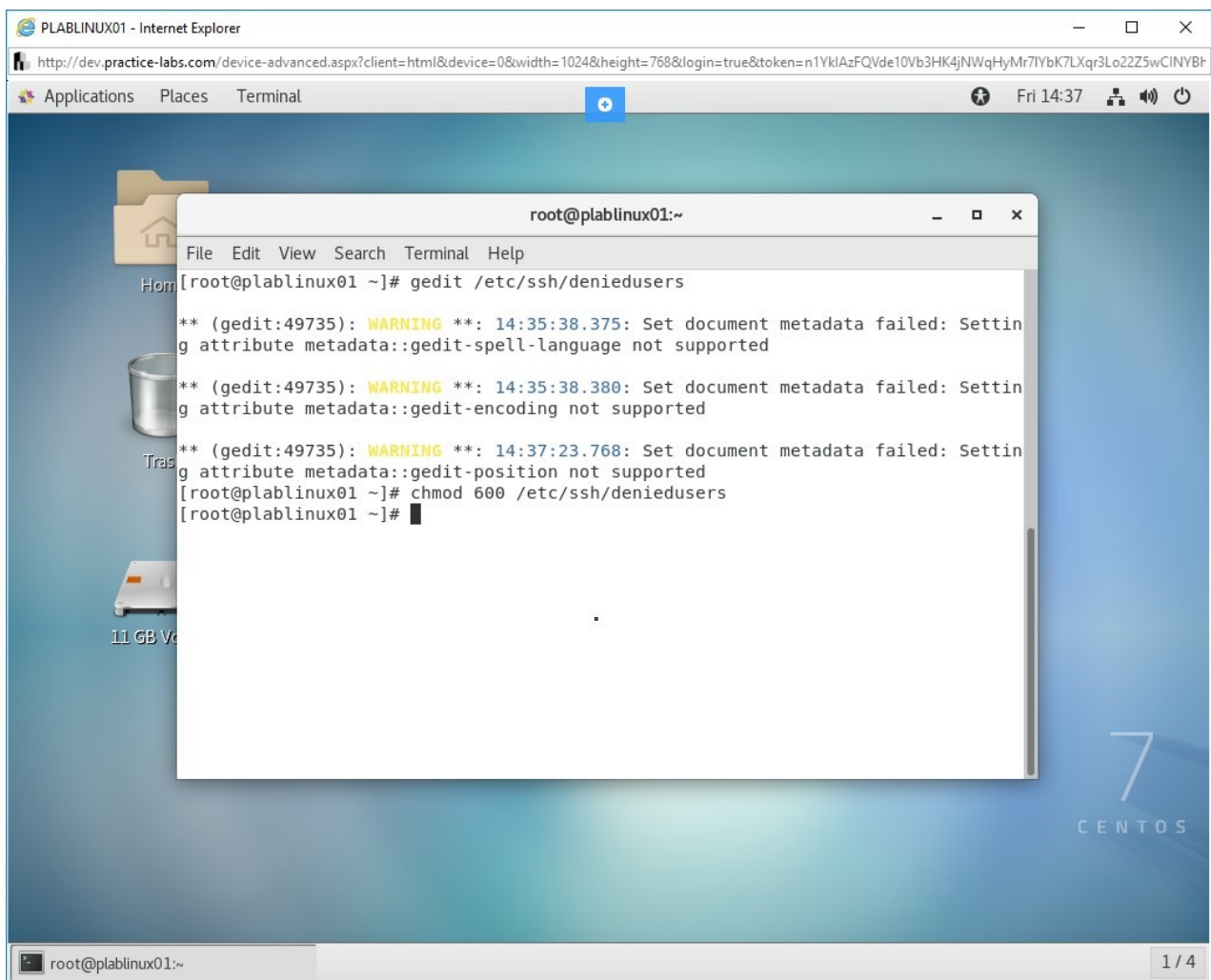


Figure 1.22 Screenshot of PLABLinux01: Changing the permissions of the /etc/ssh/deniedusers file.

Task 3 - Test PAM Configuration

After making basic configuration changes in PAM, you can now test the SSH connection for the root user.

In this task, you will learn to test PAM configuration. To test PAM configuration, perform the following steps:

Step 1

Ensure that the required devices are powered on. Connect to **PLABSA01**.

The **Server Manager** window is displayed automatically. You can close the **Server Manager** window.

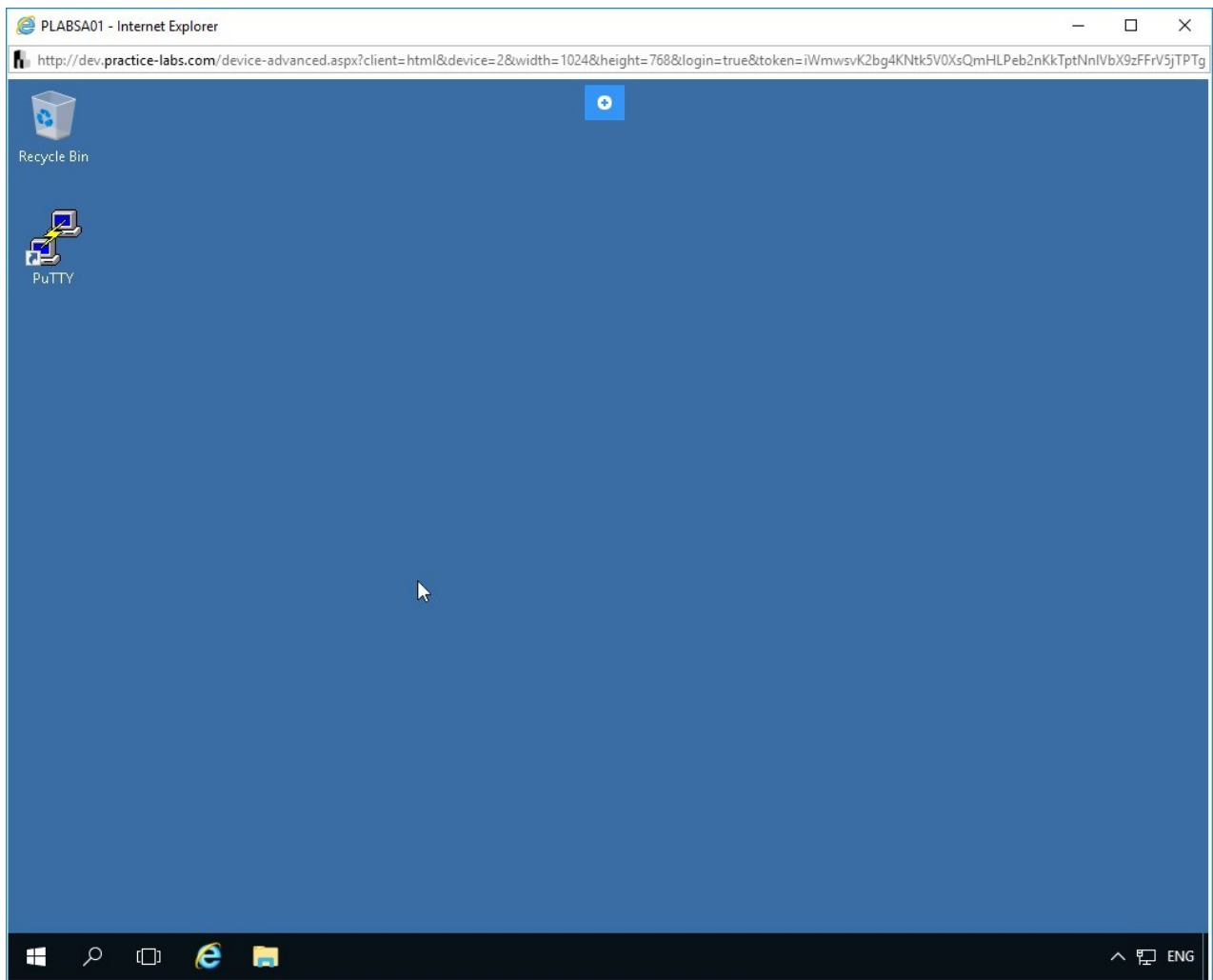


Figure 1.23 Screenshot of PLABSA01: Displaying the PLABSA01 desktop.

Step 2

On the desktop, double-click the **Putty** icon to launch PuTTY.

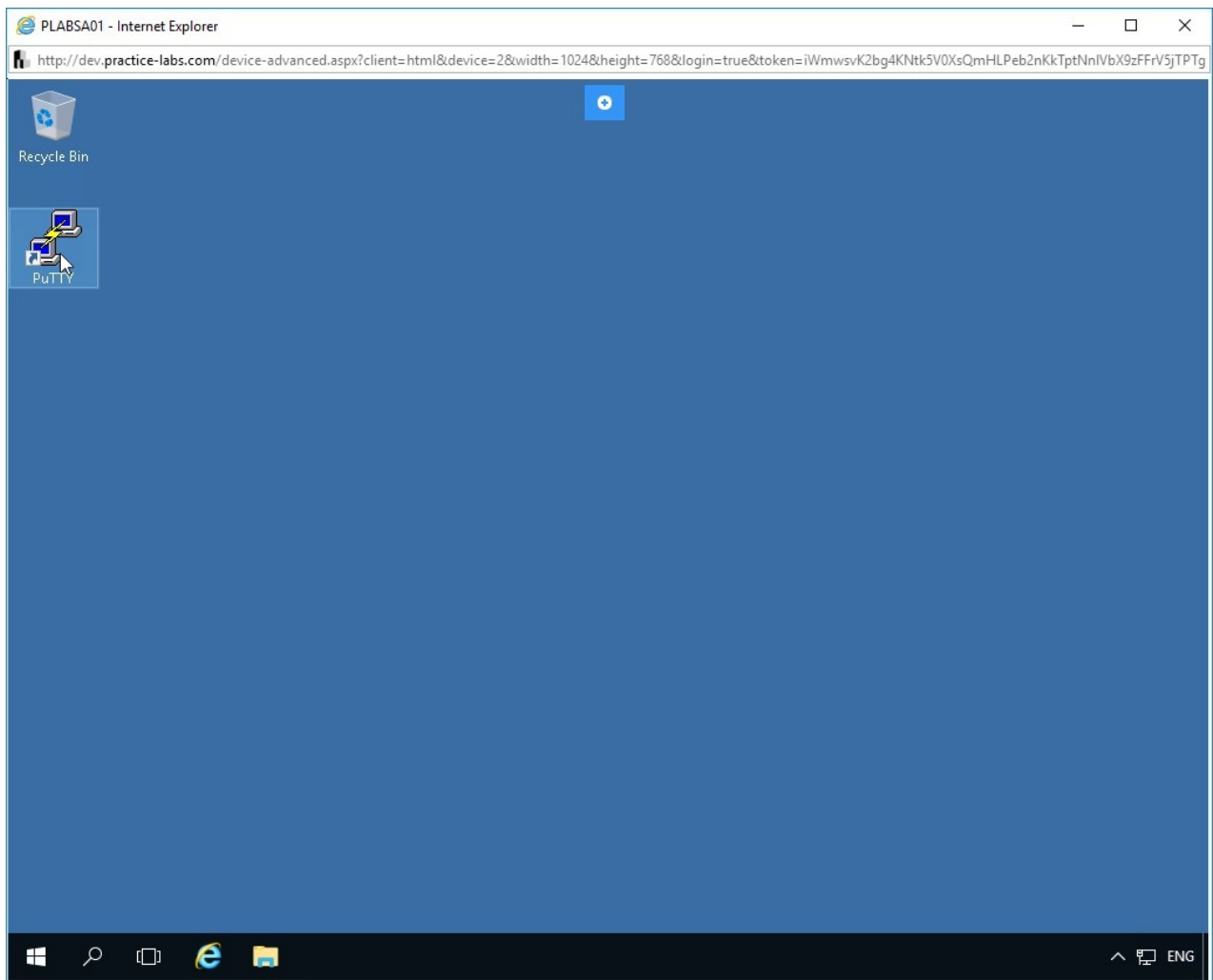


Figure 1.24 Screenshot of PLABSA01: Double-clicking the PuTTY icon.

Step 3

On the **PuTTY Configuration** dialog box, In the Host Name (or IP address) text box, type the following:

192.168.0.2

Ensure **SSH** is selected as the **Connection** type.

Click **Open**.

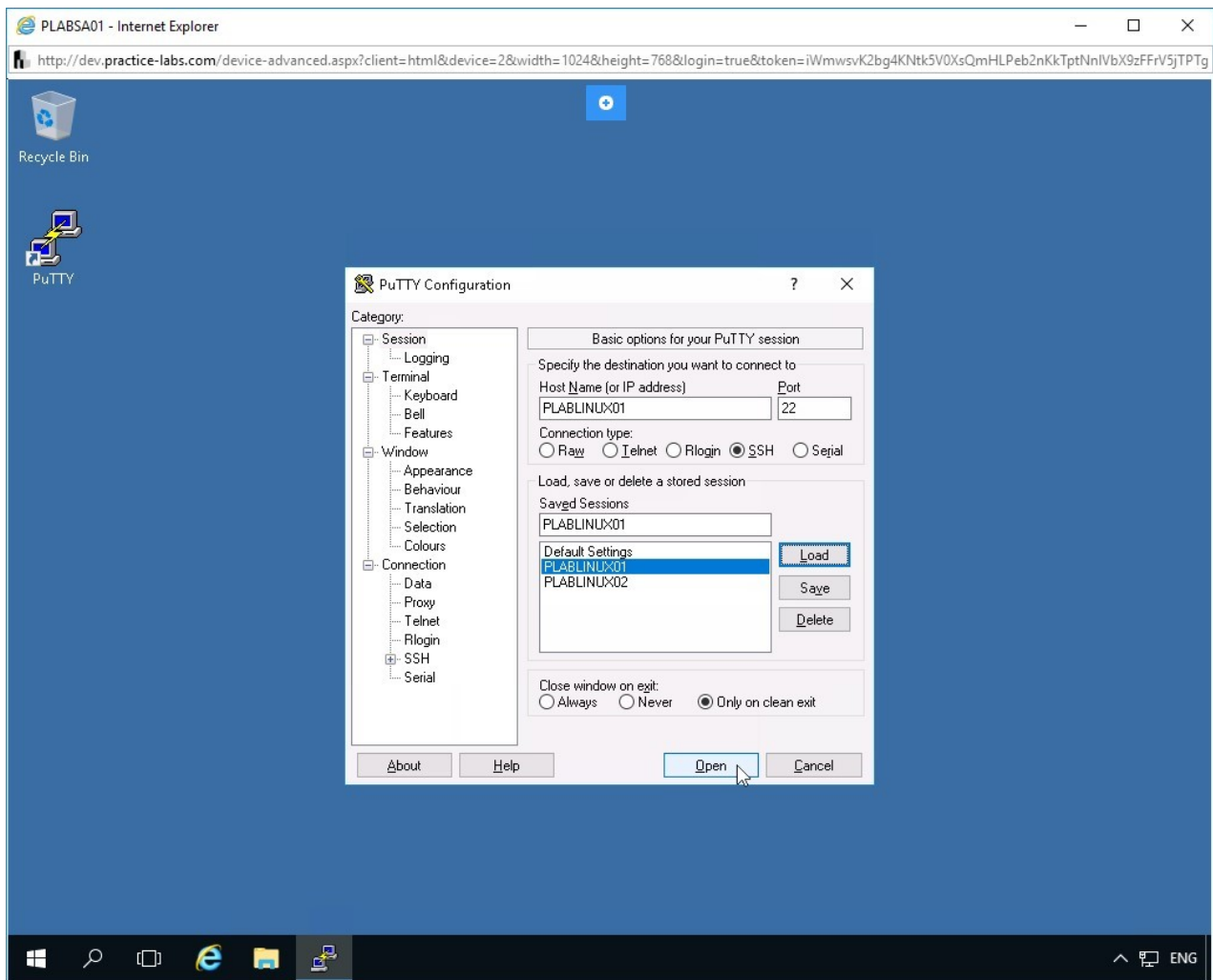


Figure 1.25 Screenshot of PLABSA01: Loading the PLABLINUX01 configuration.

Step 4

Notice that the SSH session window launches. Along with this window, the **PuTTY Security Alert** dialog box is displayed. Click **Yes**.

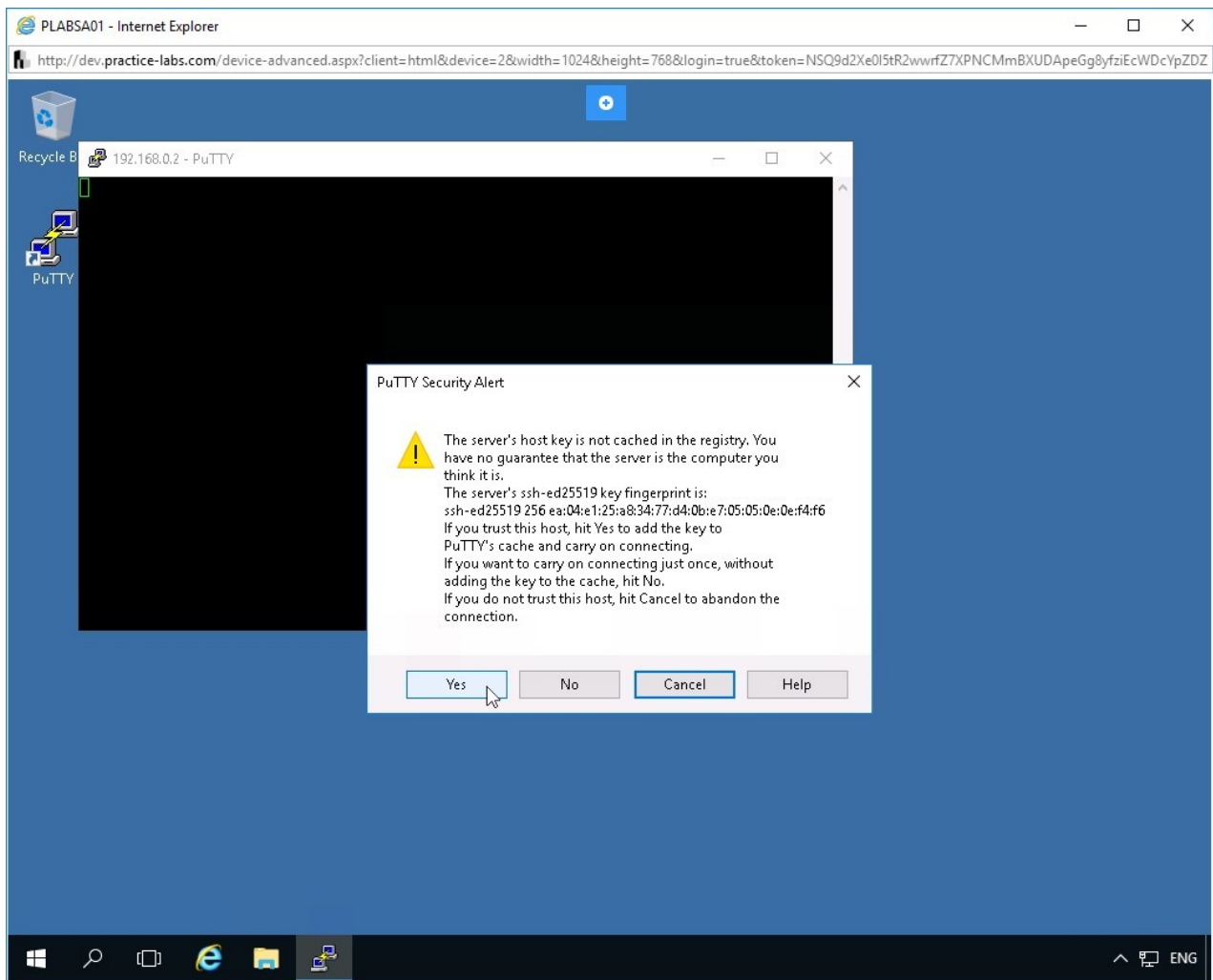


Figure 1.26 Screenshot of PLABSA01: Loading the PLABLINUX01 configuration.

Step 5

The **login as:** prompt is displayed.

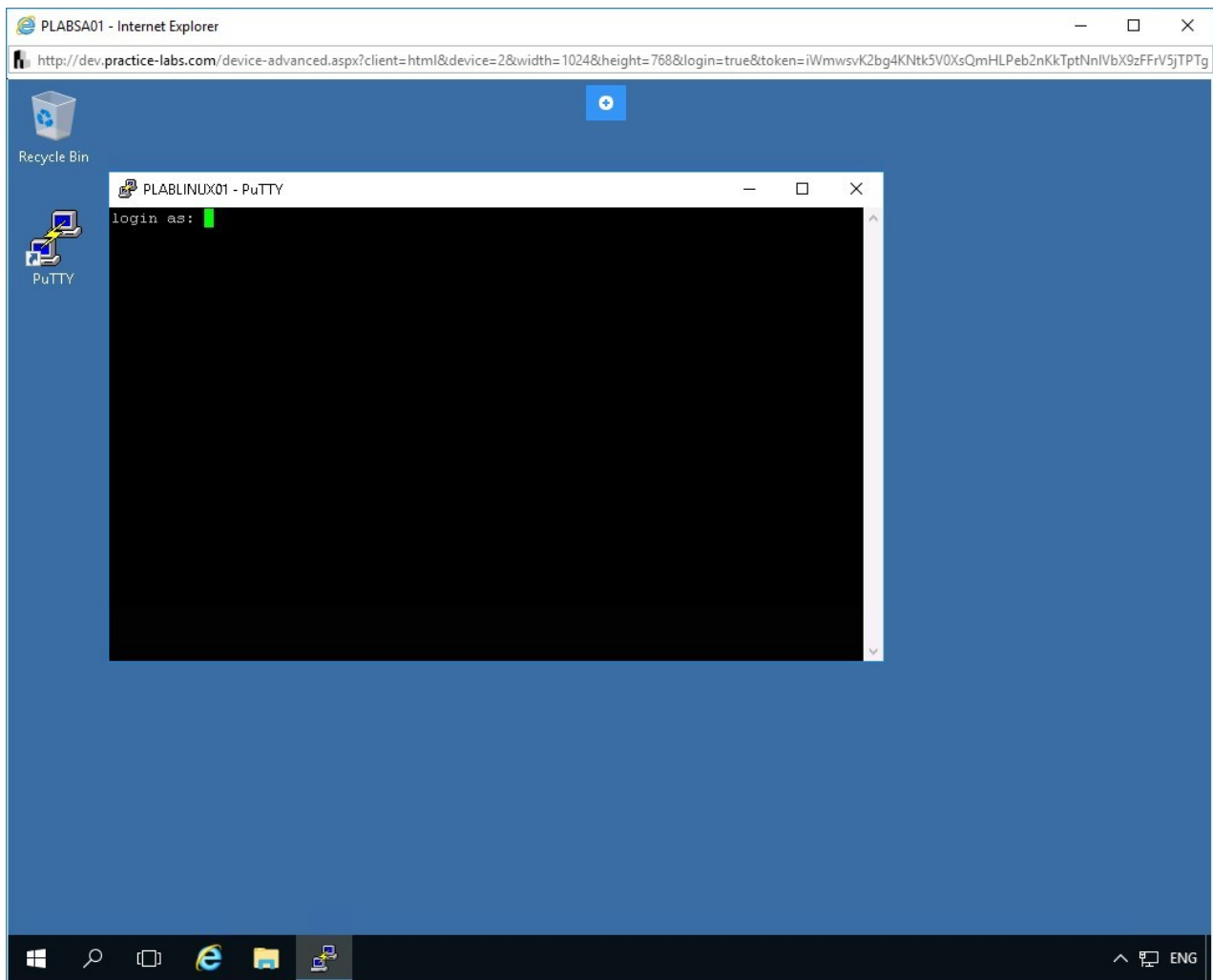


Figure 1.27 Screenshot of PLABLINUX01: Displaying the SSH session window.

Step 6

Enter the following credentials:

login as:

root

Password:

Passw0rd

Press **Enter**. Notice that the access is not permitted. You get the access denied message.

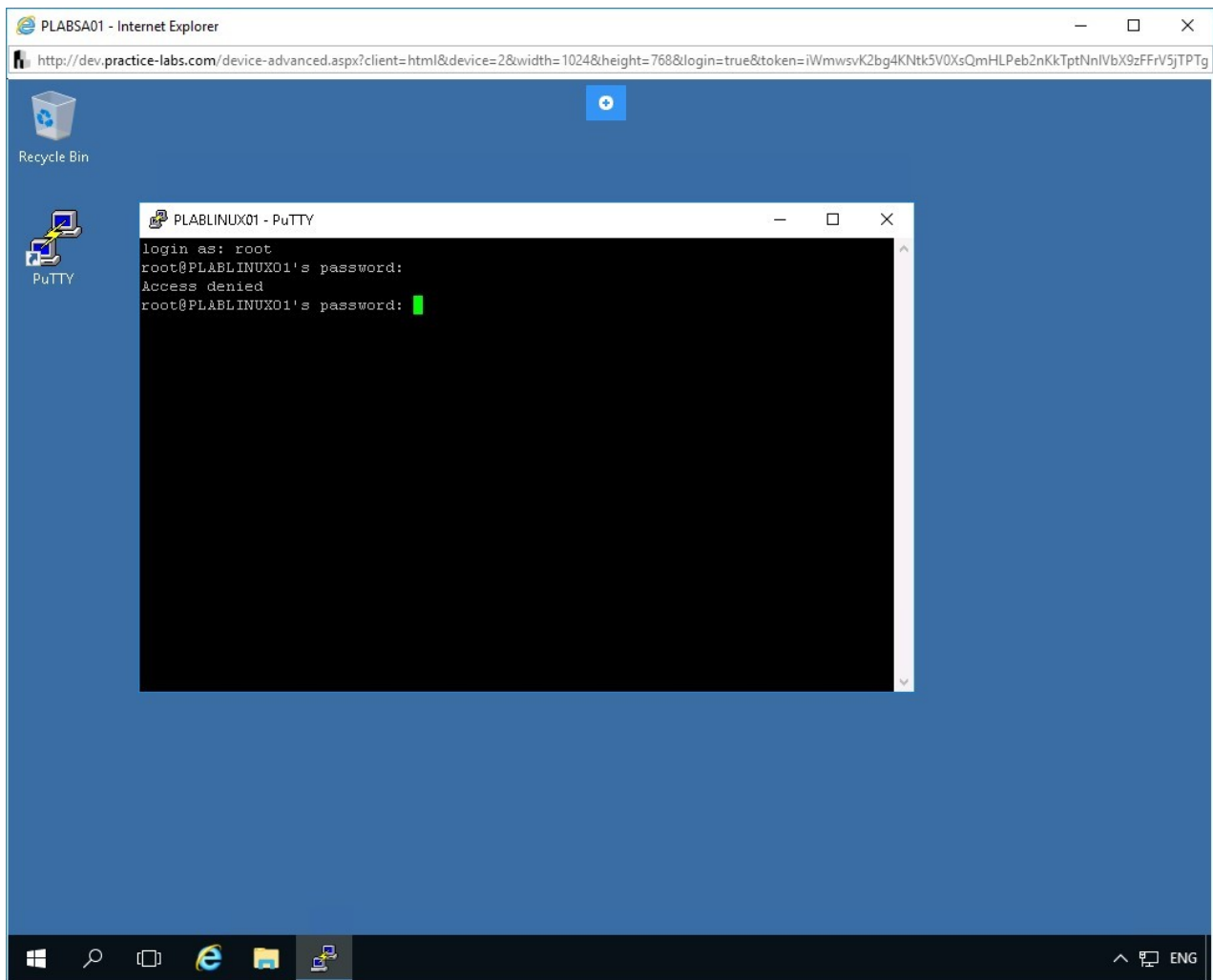


Figure 1.28 Screenshot of PLABLINUX01: Showing the access denied message after entering the credentials.

Step 7

Close the session window. Launch putty again. Load the **PLABLINUX01** session. When prompted for the login, use the following credentials:

login as:

administrator

Password:

Passw0rd

Press **Enter**. Notice that the session is now successful.

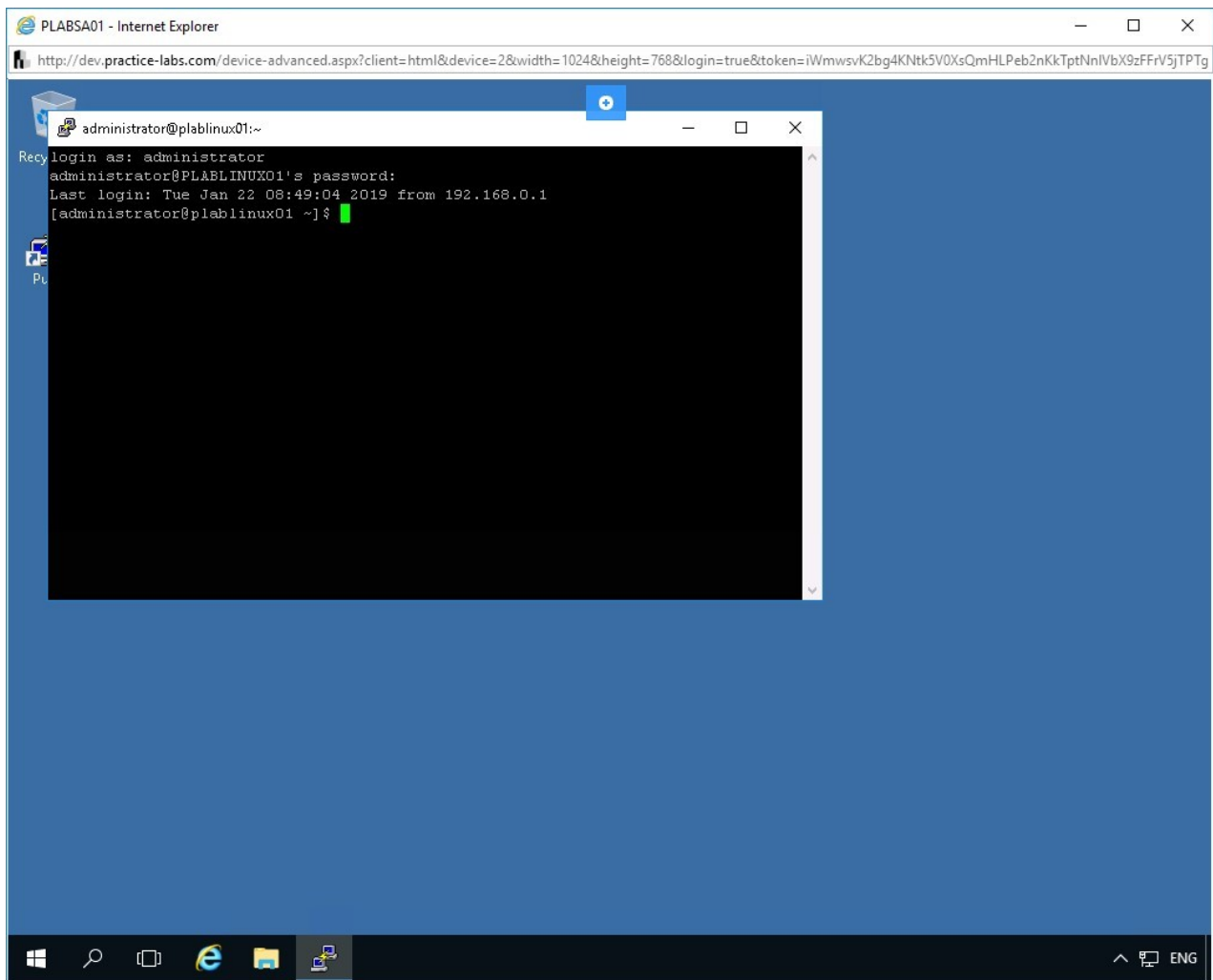


Figure 1.29 Screenshot of PLABLINUX01: Showing a successful connection after entering the credentials.

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

Review

Well done, you have completed the **Work with Pluggable Authentication Modules (PAM)** Practice Lab.

Summary

You completed the following exercise:

- Exercise 1 - Work with Pluggable Authentication Modules (PAM)

You should now be able to:

- Configure Network on CentOS
- Perform PAM Configuration
- Test PAM Configuration

Feedback

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