CompTIA Linux+

Secure a Linux Terminal and Implement Logging Services

Introduction

Welcome to the **Secure a Linux Terminal and Implement Logging Services** Practice Lab. In this module you will be provided with the instructions and devices needed to develop your hands-on skills.

Linux Terminal
Logging Services
SSH Port
SSH

Learning Outcomes

In this module, you will complete the following exercise:

- Exercise 1 - Secure a Linux Terminal and Implement Logging Services

After completing this lab, you will be able to:

- Disable Unnecessary Services
- Disable the root Login via SSH
- Change the Default SSH Port
- Verify the Last Logged in Users
- Know the Key Locations for logging

Exam Objectives

The following exam objectives are covered in this lab:

- **LPI:** 110.3 Securing data with encryption
- **CompTIA:** 3.4 Given a scenario, implement logging services.

> ***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.

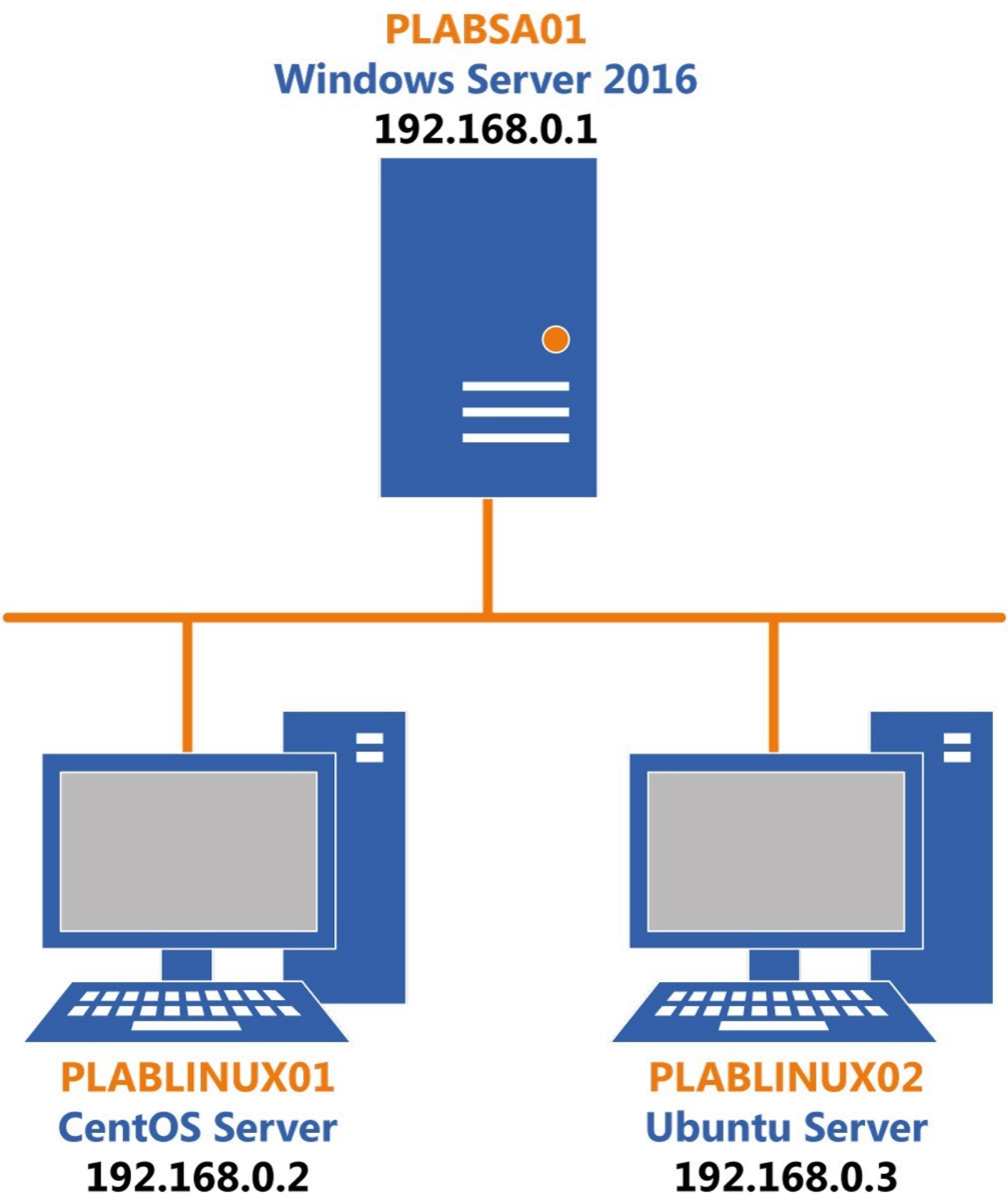
Help and Support

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 - Secure a Linux Terminal and Implement Logging Services

There is no doubt that as compared to Windows, Linux is more secure. Just like any other operating system, Linux has an in-built security model, which can be further fine-tuned. CentOS, being a flavour of Linux, carries the same security model. However, it is important to note that the out-of-the-box configuration cannot be highly secure. You must fine-tune the system as per your need and ensure that you have secured the system.

In this exercise, you will learn to secure a Linux terminal and implement logging services.

Learning Outcomes

After completing this exercise, you will be able to:

- Log into a Linux System
- Disable Unnecessary Services
- Disable the root Login via SSH
- Change the Default SSH Port
- Verify the Last Logged in Users
- Know the Key Locations for logging

Your Devices

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

- **PLABLINUX01** (CentOS Server)

Task 1 - Disable Unnecessary Services

Different flavours of Linux run certain services by default. All of these services may or may not be required. You should check for the required services and then disable the remaining services. Remember that fewer services are running, less the security risk is. This concept applies to CentOS as well.

In this task, you will learn to disable unnecessary services To disable unnecessary services, perform the following steps:

Step 1

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

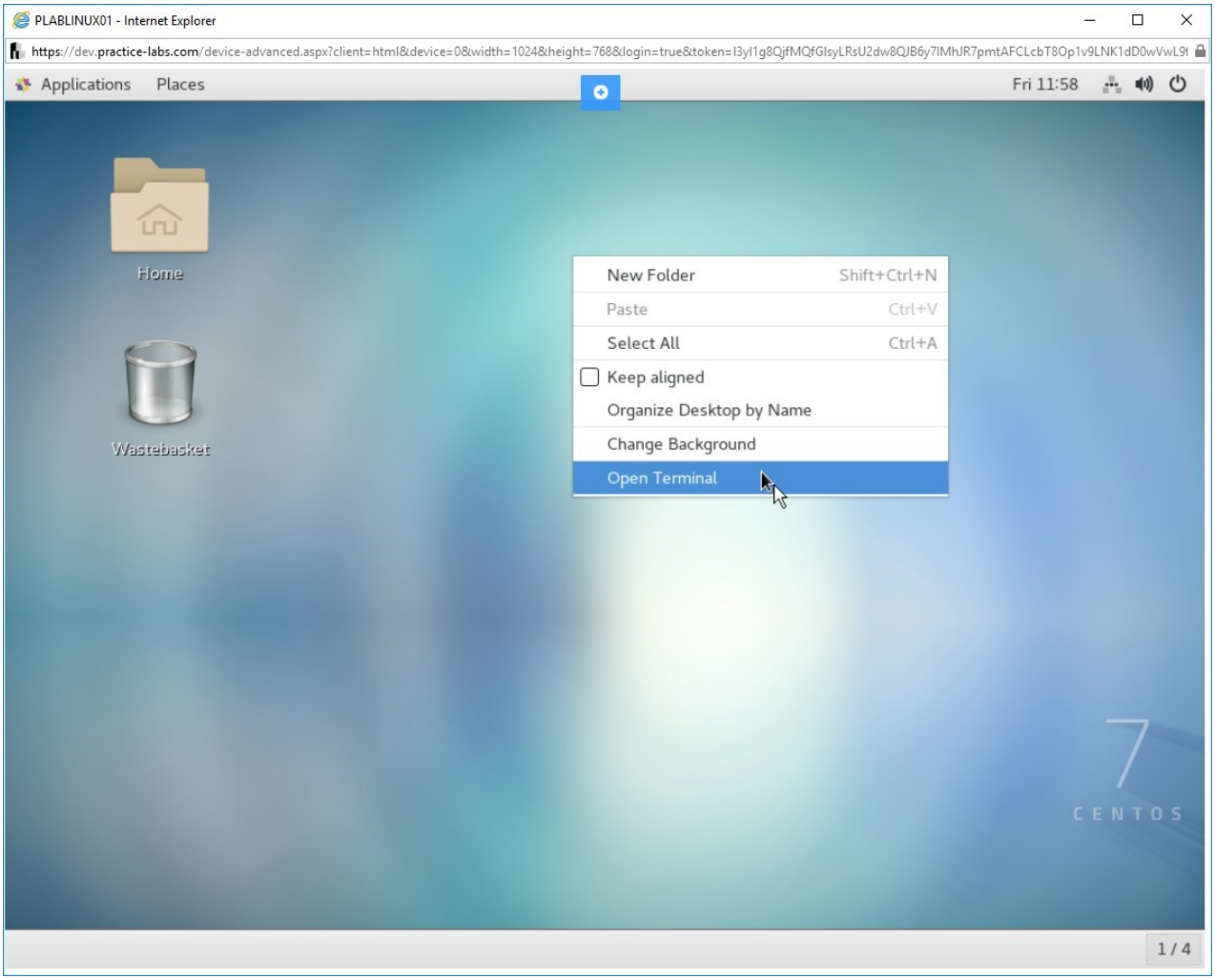


Figure 1.1 Screenshot of PLABLINUX01: Selecting the Open Terminal option from the context menu.

Step 2

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

```
su -
```

Press **Enter**.

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

`Passw0rd`

Press **Enter**.

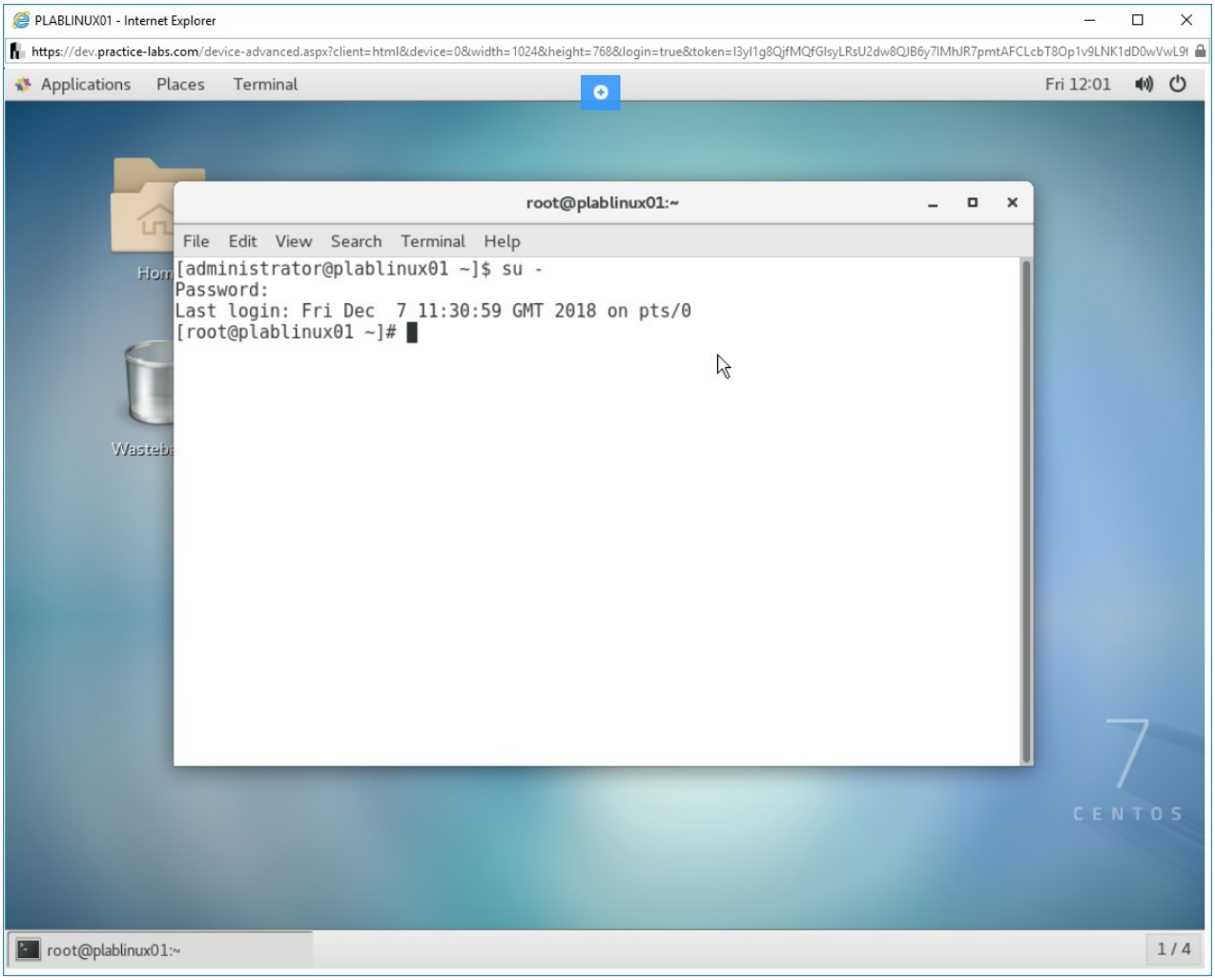


Figure 1.2 Screenshot of PLABLINUX01: Changing the account to the root account with the su command.

Step 3

Clear the screen by entering the following command:

```
clear
```

You should first check which service on which port is running. Type the following command:

```
netstat -npl
```

Press **Enter**.

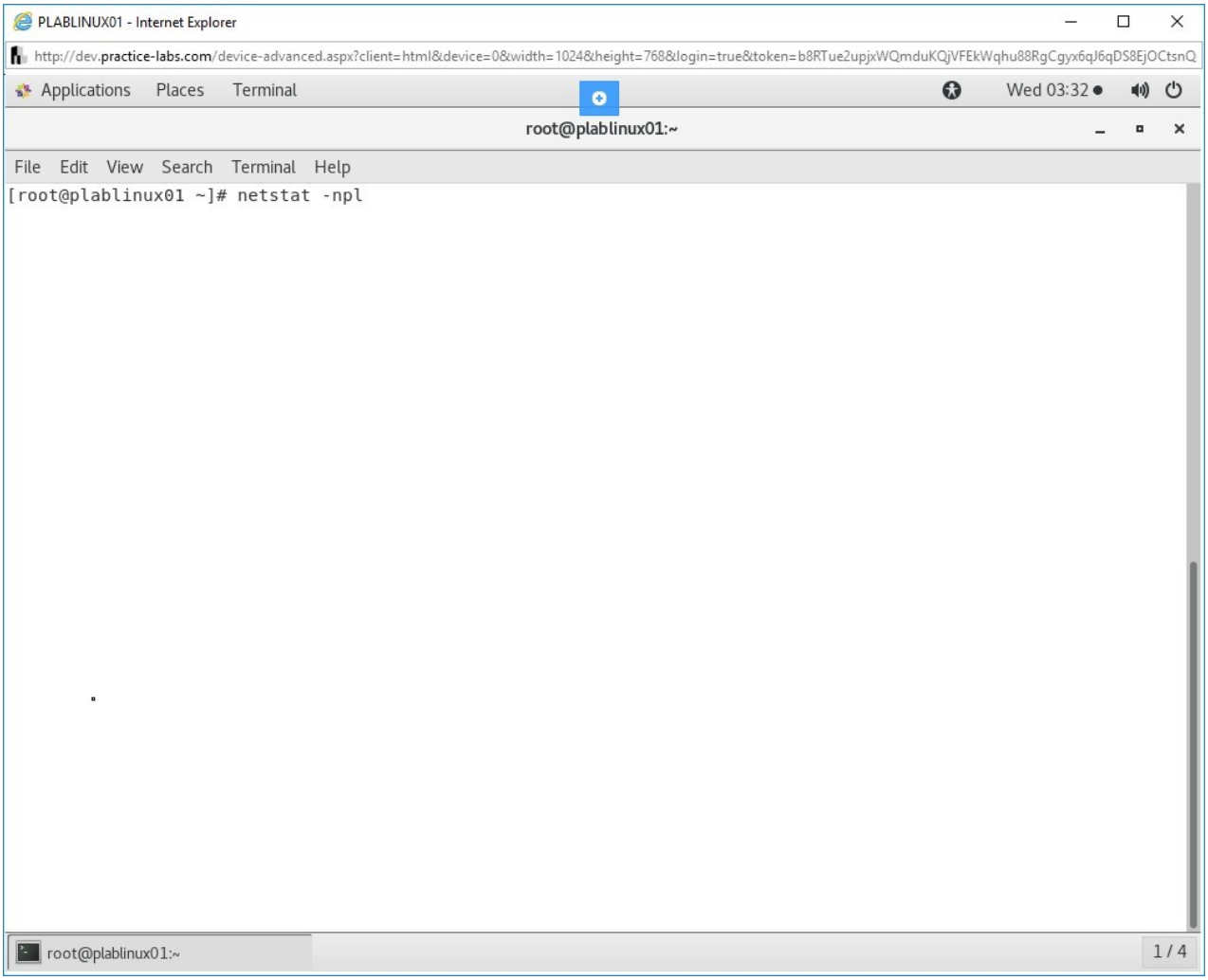


Figure 1.3 Screenshot of PLABLINUX01: Verifying which service is running on which port.

Step 4

Notice that the command output is now displayed.

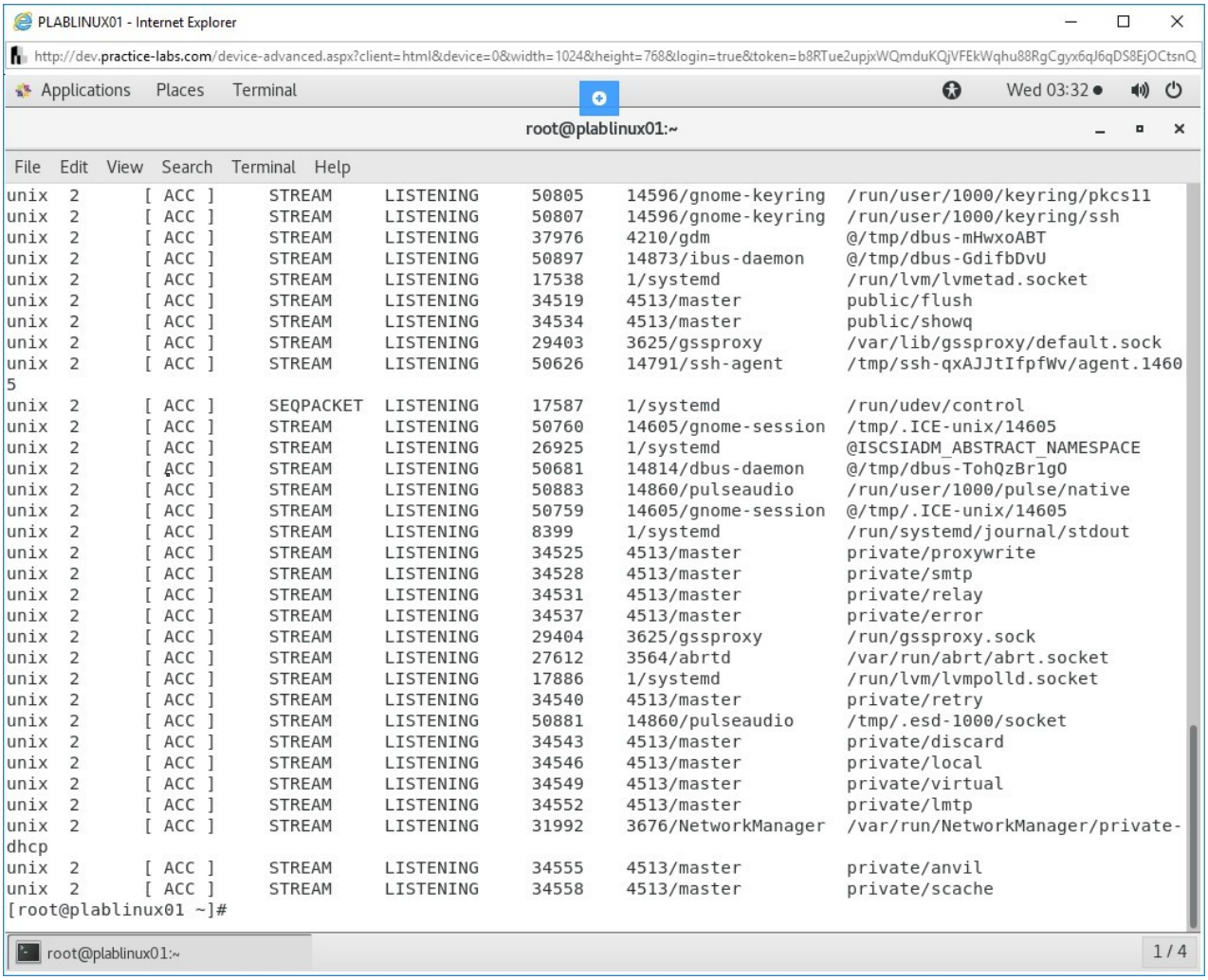


Figure 1.4 Screenshot of PLABLINUX01: Displaying the output of the netstat command.

Step 5

Scroll to the start of the output. Notice the headers. The I-Node is the port that is being used. The next column displays the PID/Program name. The last column displays the path of the program.

You can stop a specific service after ensuring that it is not required.

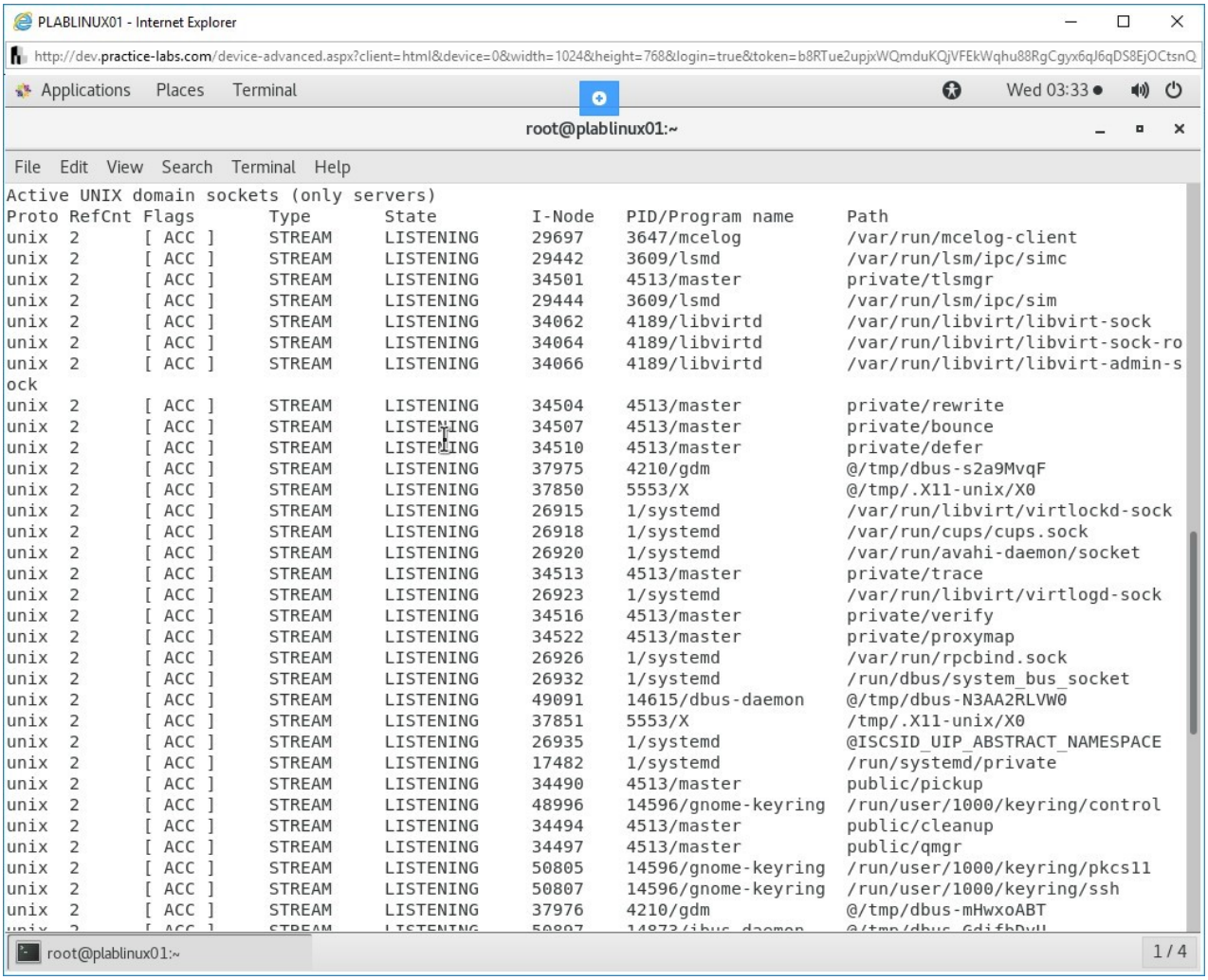


Figure 1.5 Screenshot of PLABLINUX01: Displaying the output of the netstat command.

Step 6

Clear the screen by entering the following command:

```
clear
```

You should check which services are configured to start at the system bootup. Type the following command:

```
systemctl list-unit-files --type=service | grep enabled
```

Press **Enter**.

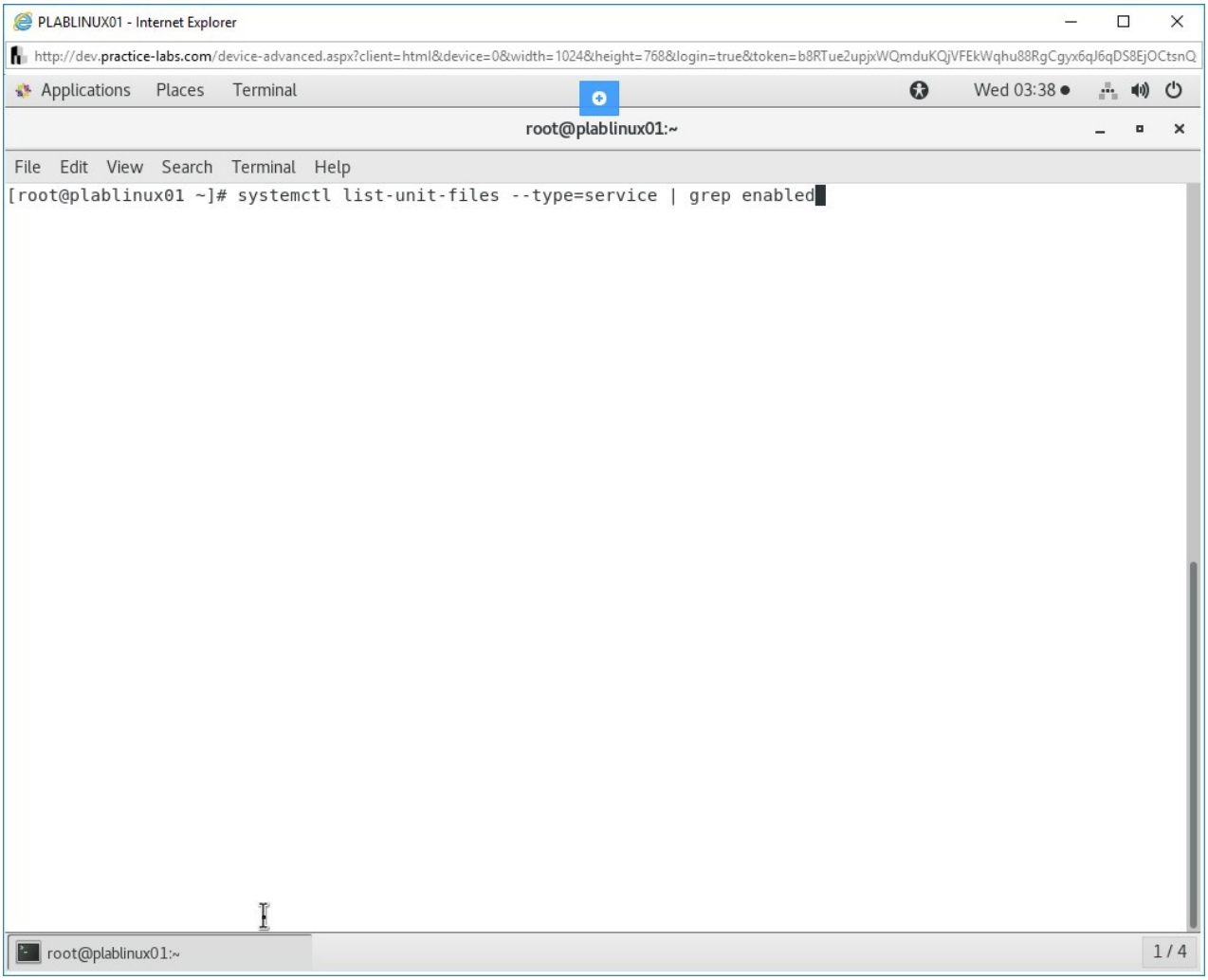


Figure 1.6 Screenshot of PLABLINUX01: Verifying which services are configured to start with the system bootup.

Step 7

Notice that the command output is now displayed.

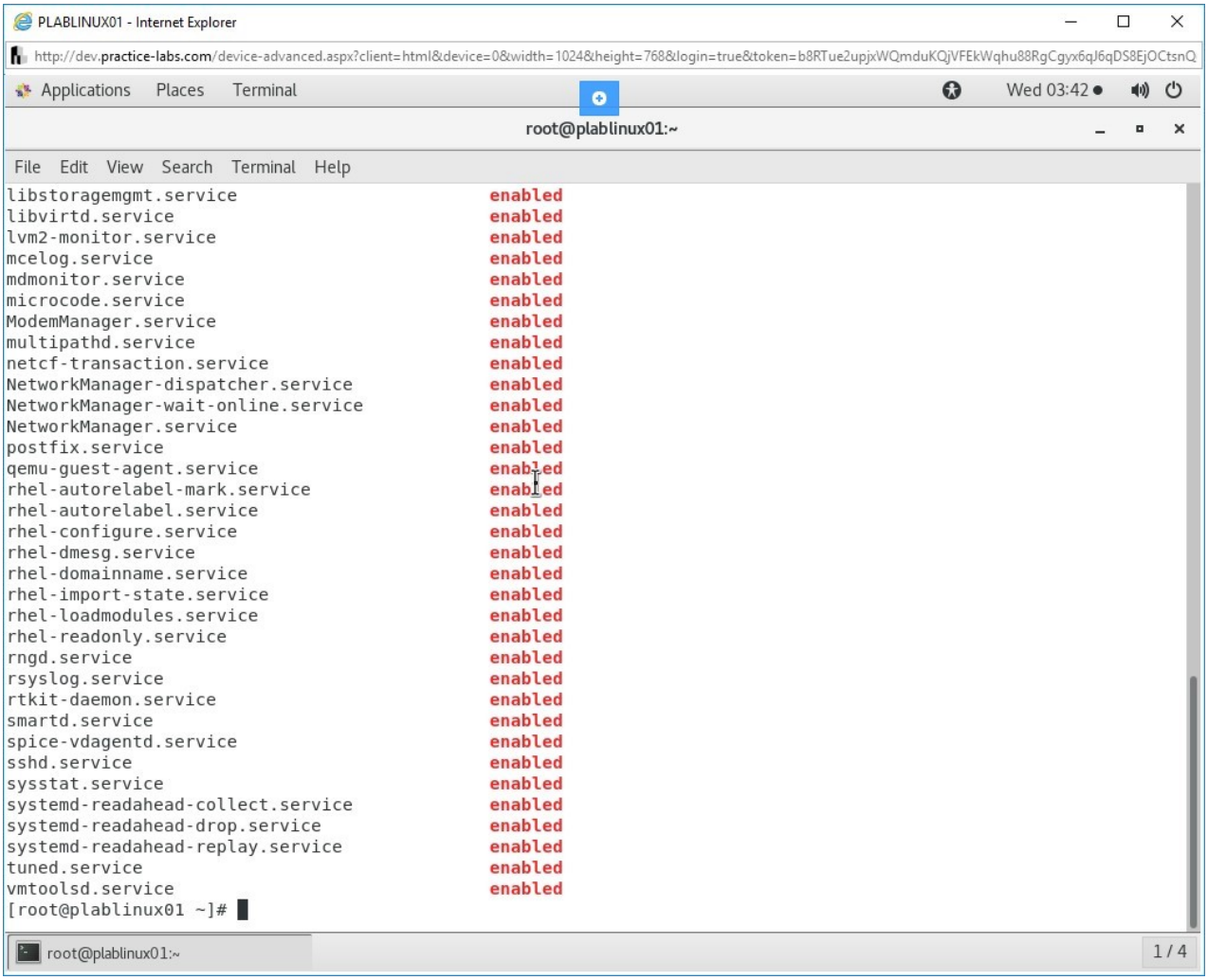


Figure 1.7 Screenshot of PLABLINUX01: Displaying the services that are configured to start with at the system bootup.

Step 8

Clear the screen by entering the following command:

```
clear
```

Let's assume that you do not want the **vmtoolsd.service** to be enabled. You can disable this service. Type the following command:

```
systemctl disable vmtoolsd.service
```

Press **Enter**. Notice that vmtoolsd.service is no longer enabled.

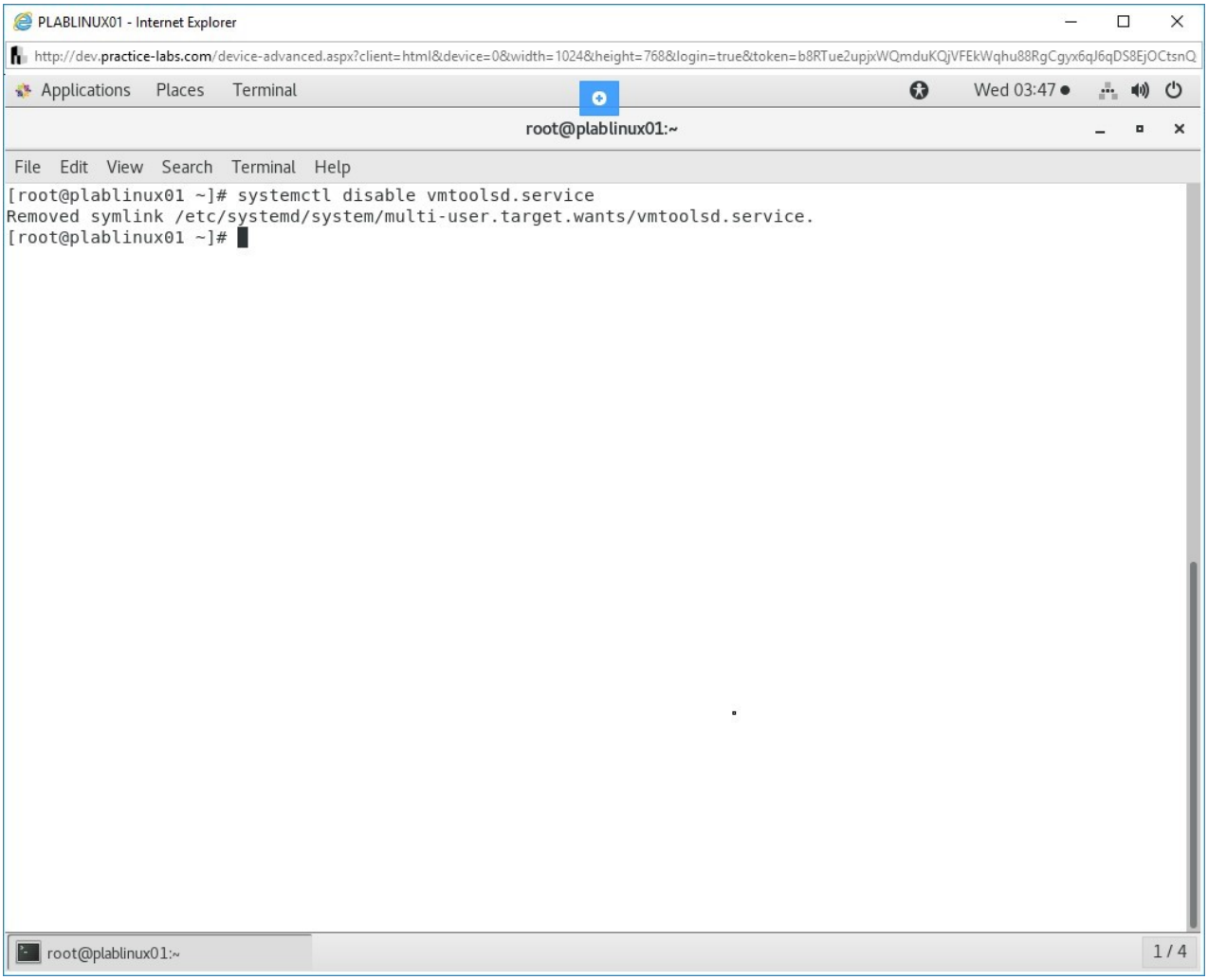


Figure 1.8 Screenshot of PLABLINUX01: Disabling the auto start of the vmtoolsd.service service.

Step 9

You should verify if **vmtoolsd.service** is still configured to start with the system bootup. Type the following command:

```
systemctl list-unit-files --type=service | grep enabled
```

Press **Enter**. Notice that the vmtoolsd.service no longer appears in the list.

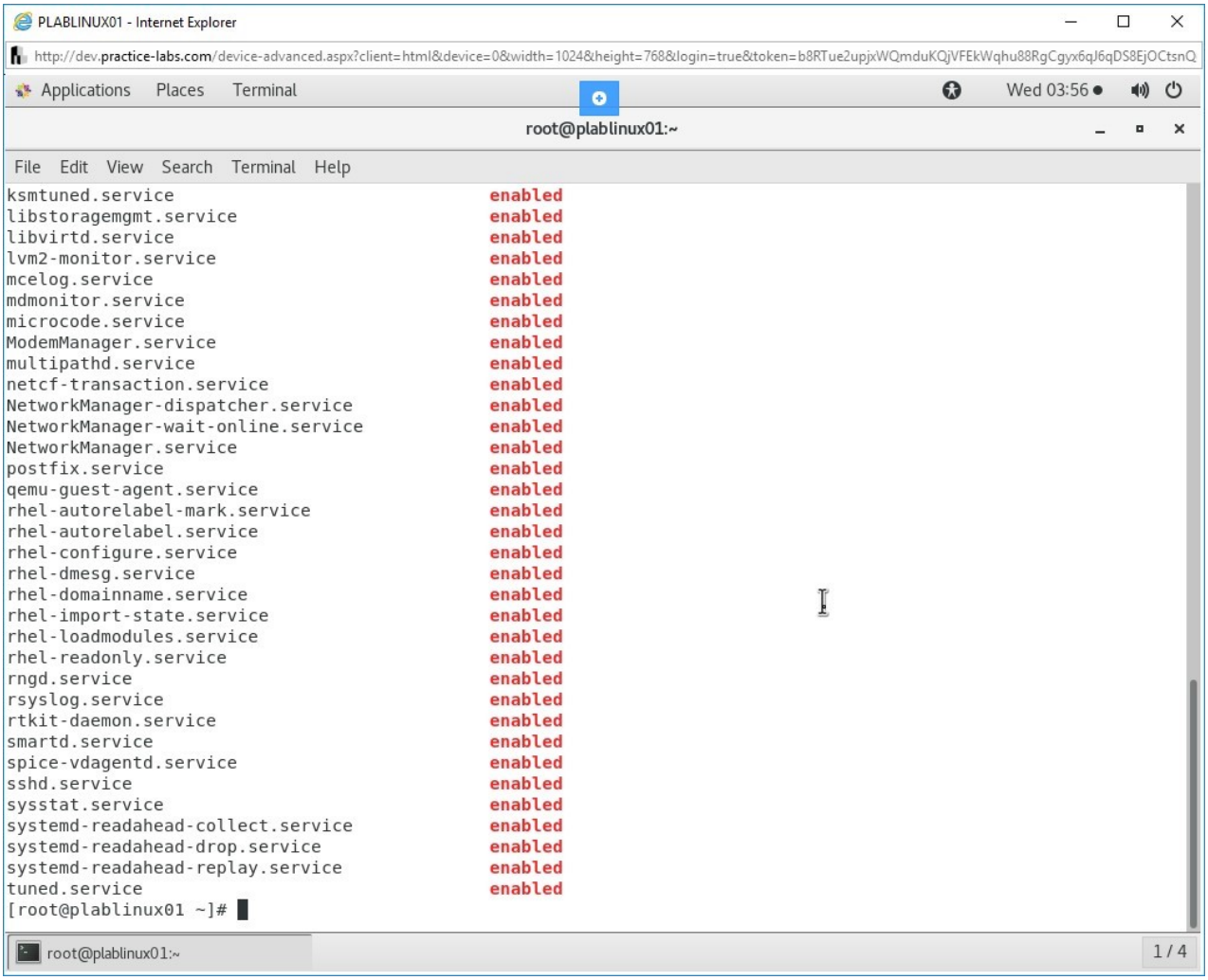


Figure 1.9 Screenshot of PLABLINUX01: Displaying the services that are configured to start with at the system bootup.

Task 2 - Disable the root Login via SSH

The **/etc/ssh/sshd_config** file contains the configuration settings for the OpenSSH Server. You can tweak the settings in this file to ensure optimal security. To secure the OpenSSH Server, perform the following steps:

Step 1

Ensure you are connected to **PLABLINUX01**. Restore the terminal window. Ensure that the **root** prompt is displayed.

Clear the screen by entering the following command:

```
clear
```

To make changes to the OpenSSH Server configuration, you need to edit the **/etc/ssh/sshd_config** file. Type the following command:

```
gedit /etc/ssh/sshd_config
```

Press **Enter**.

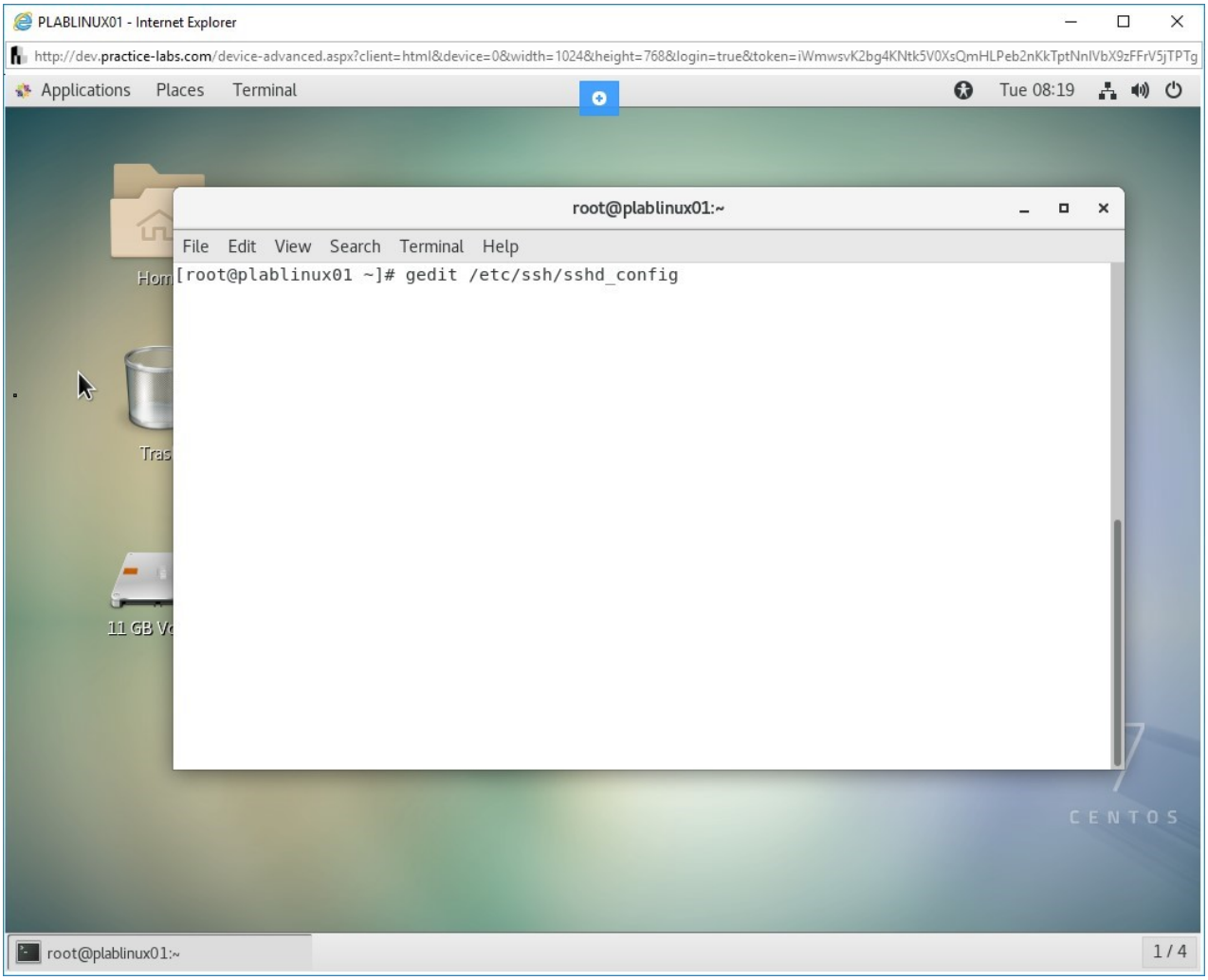


Figure 1.10 Screenshot of PLABLINUX01: Opening the /etc/ssh/sshd_config file.

Step 2

The **/etc/ssh/sshd_config** file is displayed.

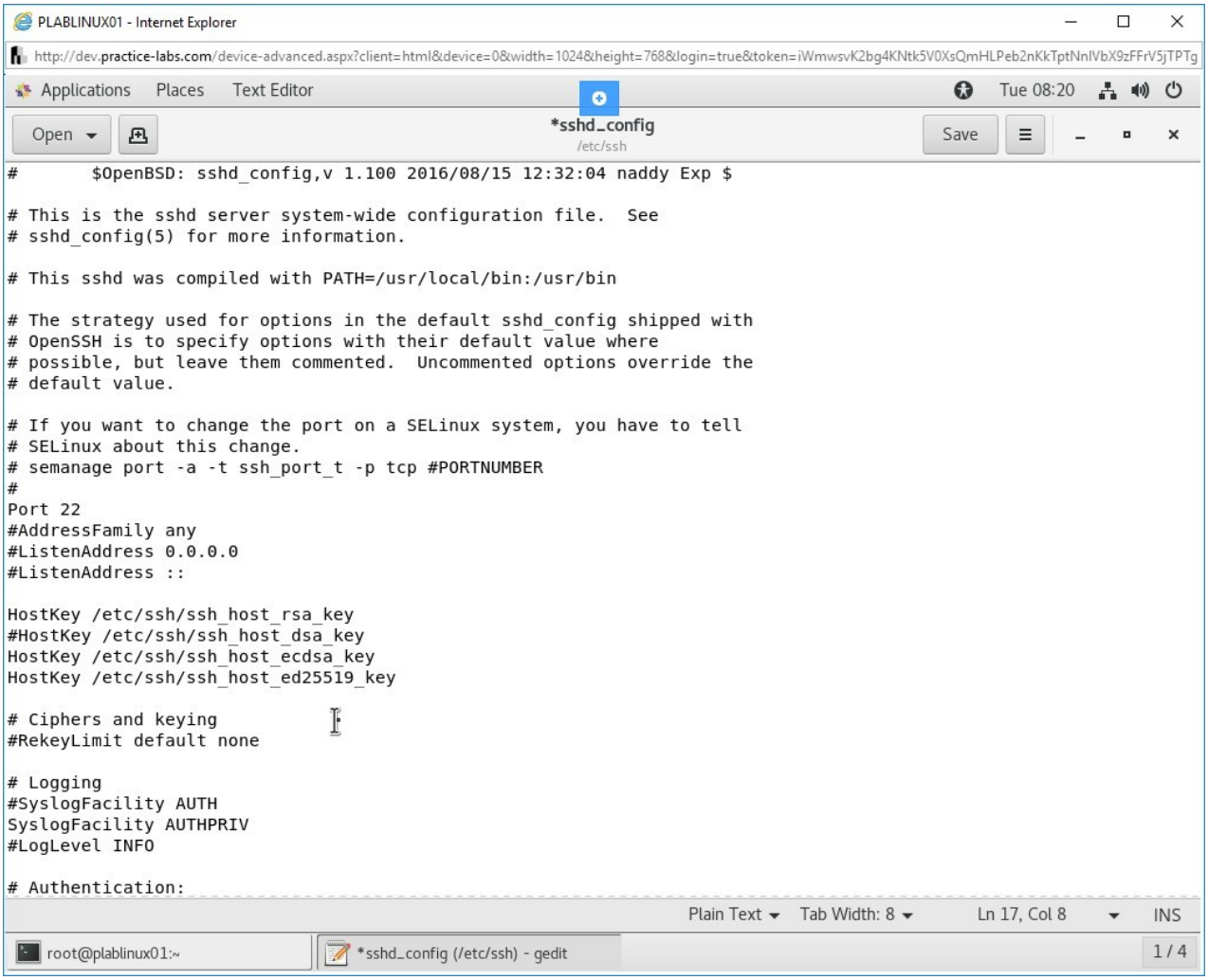


Figure 1.11 Screenshot of PLABLINUX01: Displaying the /etc/ssh/sshd_config file.

Step 3

You should also block the root access. Navigate to the **Authentication** section. From #**PermitRootLogin**, remove #.

Change the following:

From:

```
#PermitRootLogin yes
```

To:

```
PermitRootLogin no
```

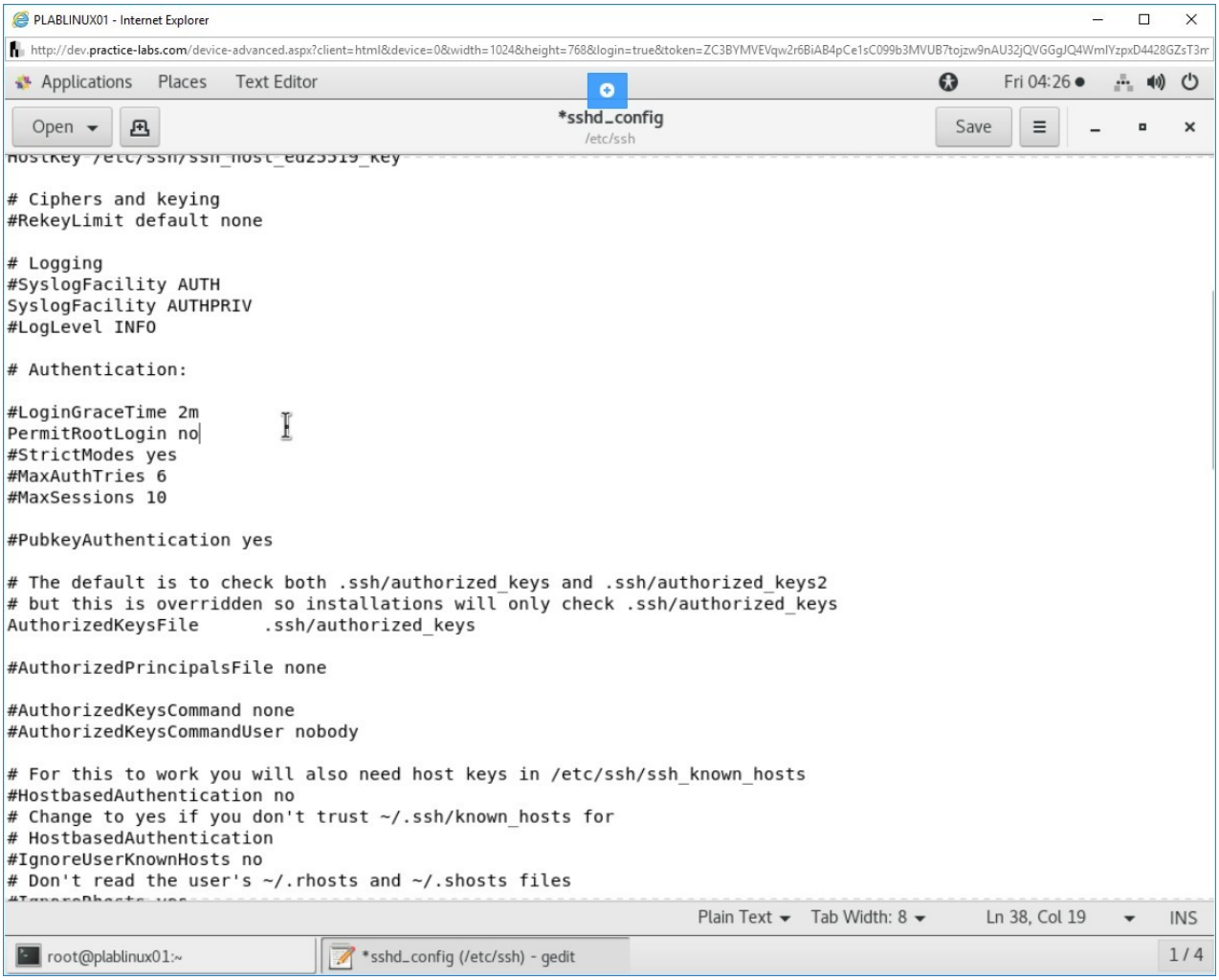


Figure 1.12 Screenshot of PLABLINUX01: Making changes to the /etc/ssh/sshd_config file.

Step 4

In the **Authentication** section, add the following:

```
AllowUsers administrator
AllowGroups administrator
```

With the **AllowUSers** and **AllowGroups**, you can add as many users and groups.

> ***Note:*** *You can also deny users and groups with the DenyUsers and DenyGroups option.*

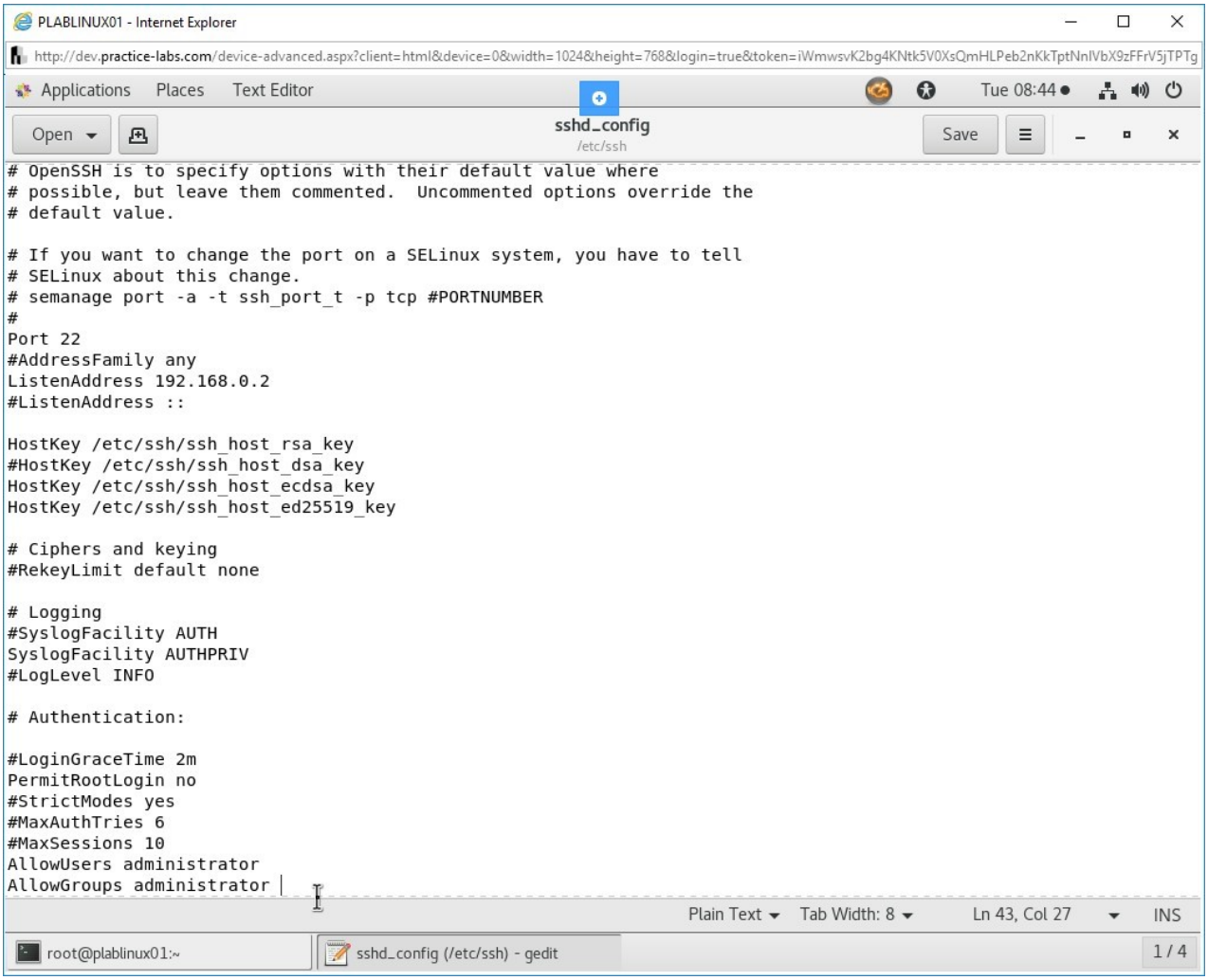


Figure 1.13 Screenshot of PLABLINUX01: Making changes to the /etc/ssh/sshd_config file.

Step 5

Click **Save** to save the file. Then, close the **/etc/ssh/sshd_config** file.

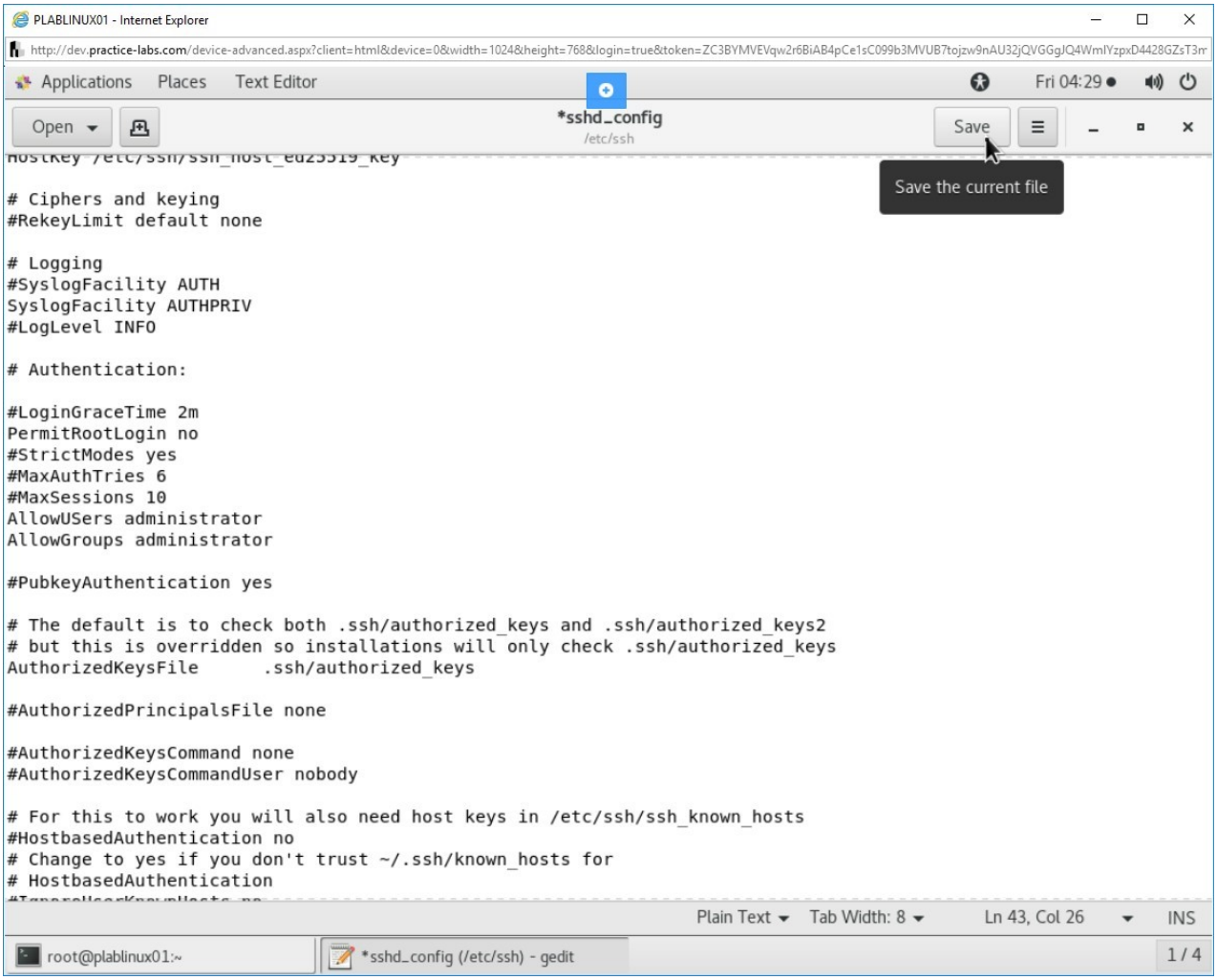


Figure 1.14 Screenshot of PLABLINUX01: Saving and closing the /etc/ssh/sshd_config file.

Step 6

You are now back on the terminal window. To restart the **sshd** service, type the following command:

```
systemctl restart sshd
```

Press **Enter**.

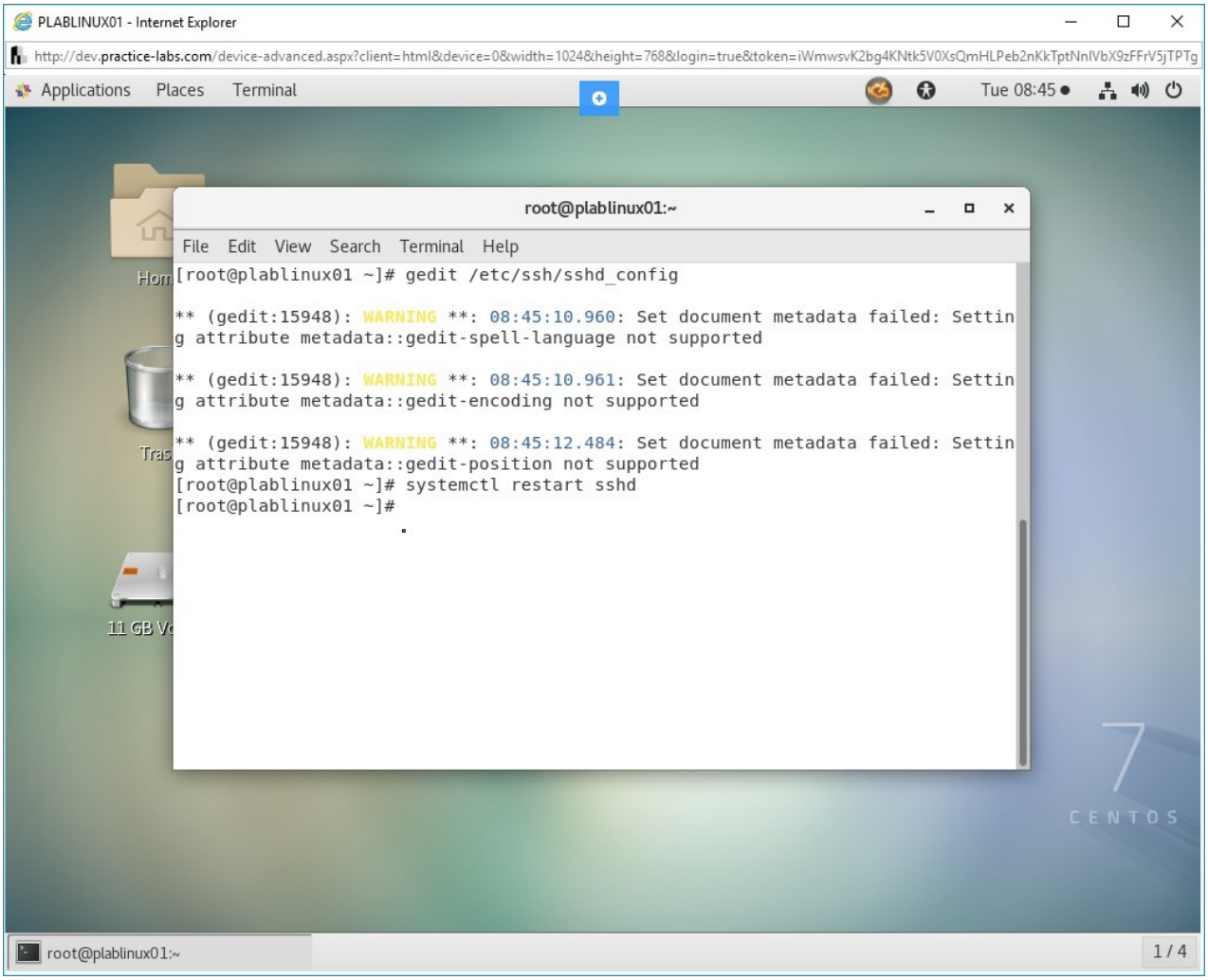


Figure 1.15 Screenshot of PLABLINUX01: Restarting the sshd service.

Step 7

Switch to **PLABSA01**. From the **Putty** window, open an SSH connection to **PLABLINUX01**.

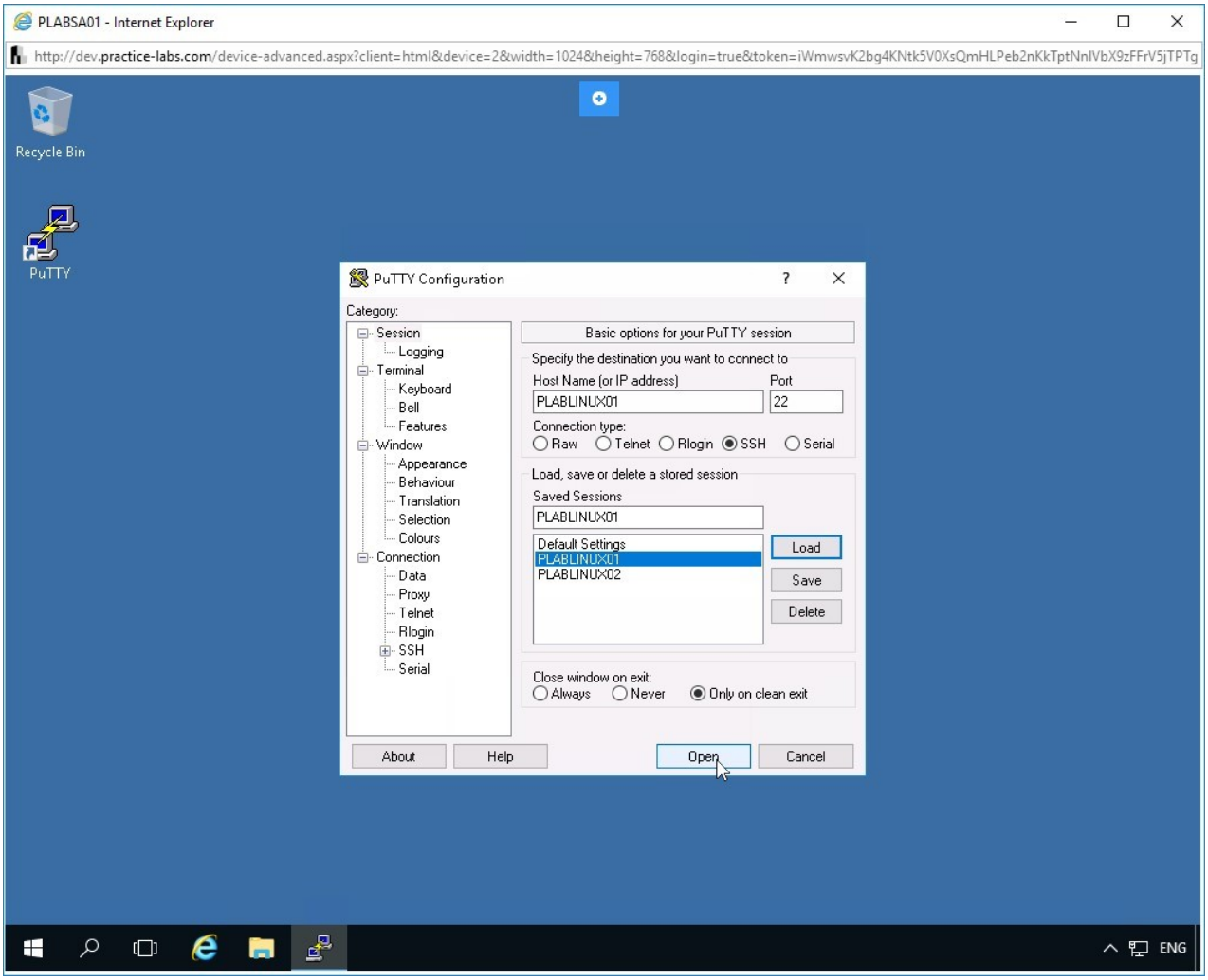


Figure 1.16 Screenshot of PLABLINUX01: Loading required configuration in the PutTTY window.

Step 8

The terminal window is displayed. Enter the following credentials:

login as:

```
root
```

Password:

```
Passw0rd
```

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

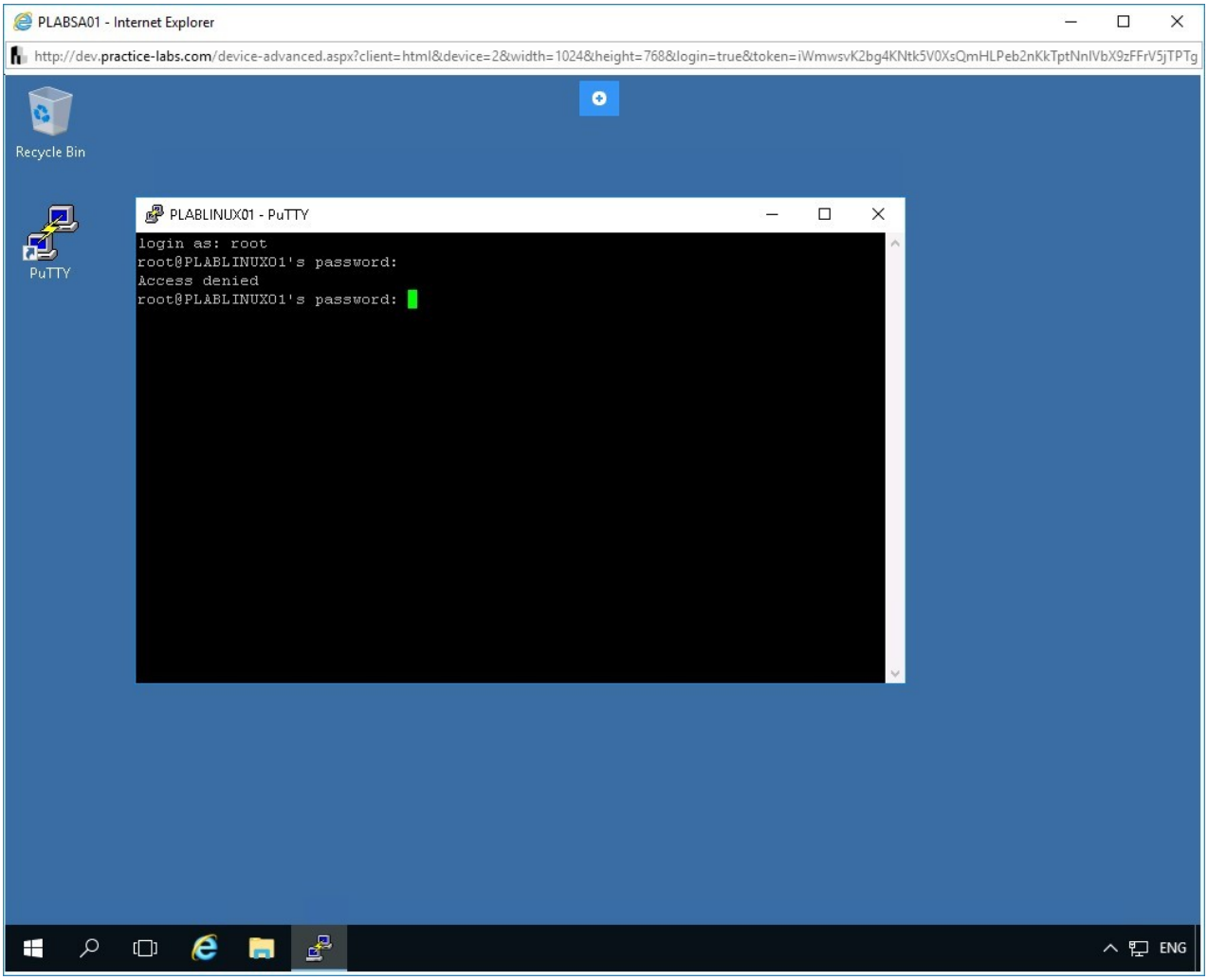


Figure 1.17 Screenshot of PLABLINUX01: Showing the access denied message after entering the credentials.

Step 9

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.

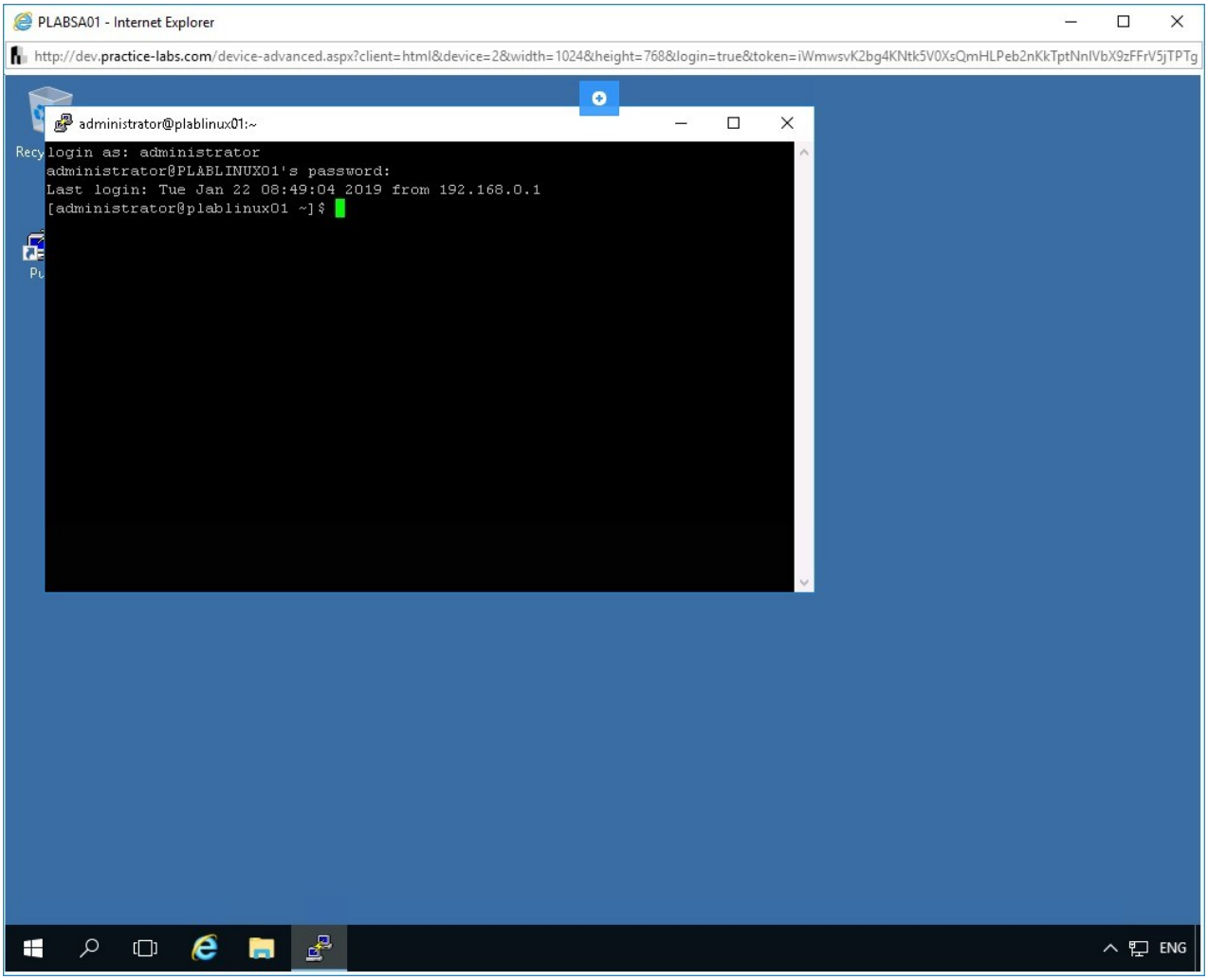


Figure 1.18 Screenshot of PLABLINUX01: Showing a successful connection after entering the credentials.

Task 3 - Change the Default SSH Port

The **/etc/ssh/sshd_config** file contains the configuration settings for the OpenSSH Server. You can tweak the settings in this file to ensure optimal security. To secure the OpenSSH Server, perform the following steps:

Step 1

Switch back to **PLABLINUX01**. Restore the terminal window. Ensure that the **root** prompt is displayed.

Clear the screen by entering the following command:

```
clear
```

To make changes to the OpenSSH Server configuration, you need to edit the **/etc/ssh/sshd_config** file. Type the following command:

```
gedit /etc/ssh/sshd_config
```

Press **Enter**.

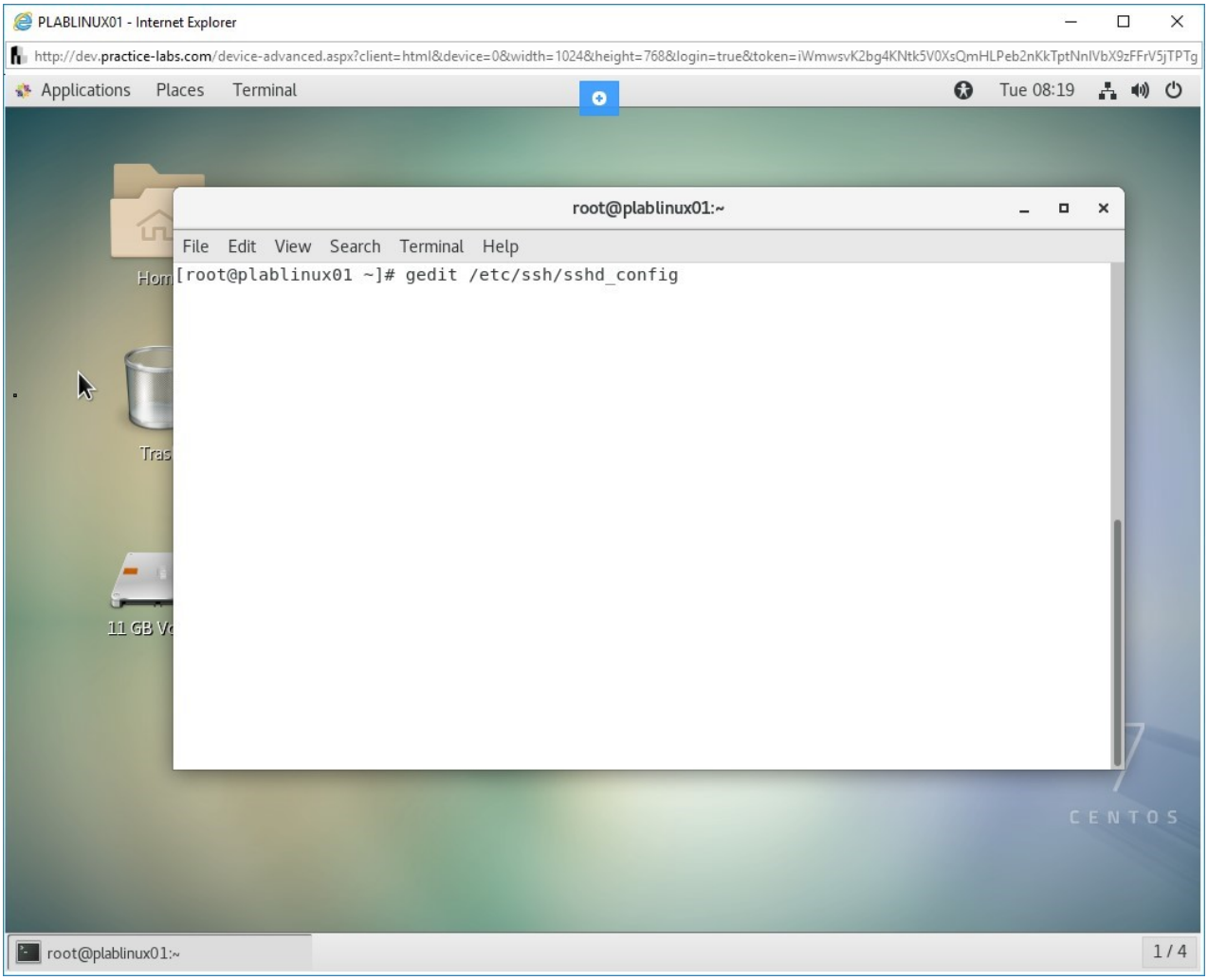


Figure 1.19 Screenshot of PLABLINUX01: Opening the /etc/ssh/sshd_config file.

Step 2

The **/etc/ssh/sshd_config** file is displayed.

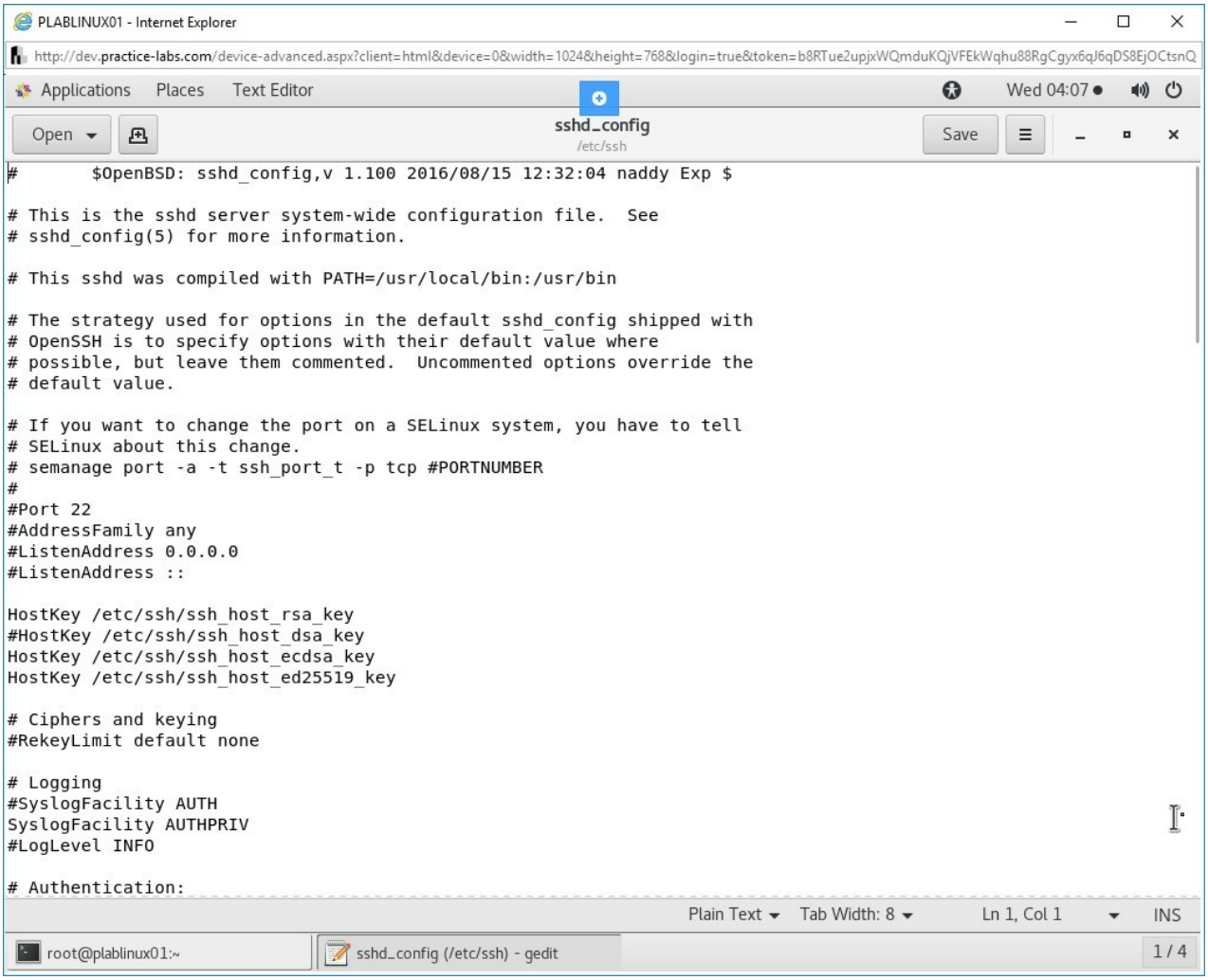


Figure 1.20 Screenshot of PLABLINUX01: Displaying the /etc/ssh/sshd_config file.

Step 3

Notice that the port number line is commented. You will n

Change the following:

From:

```
#Port 22
```

To:

```
Port 1234
```

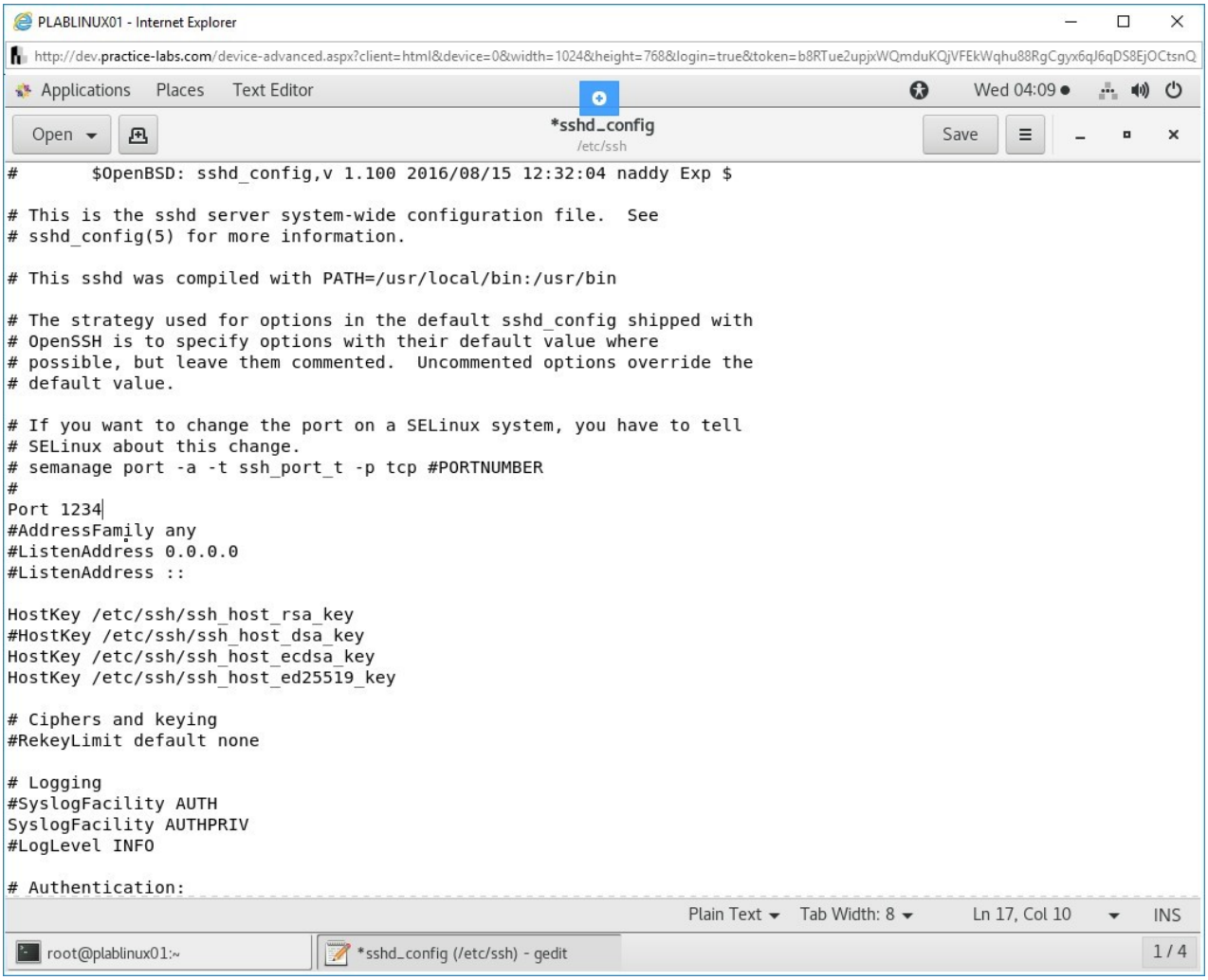


Figure 1.21 Screenshot of PLABLINUX01: Making changes to the /etc/ssh/sshd_config file.

Step 4

Click **Save** to save the file. Then, close the **/etc/ssh/sshd_config** file.

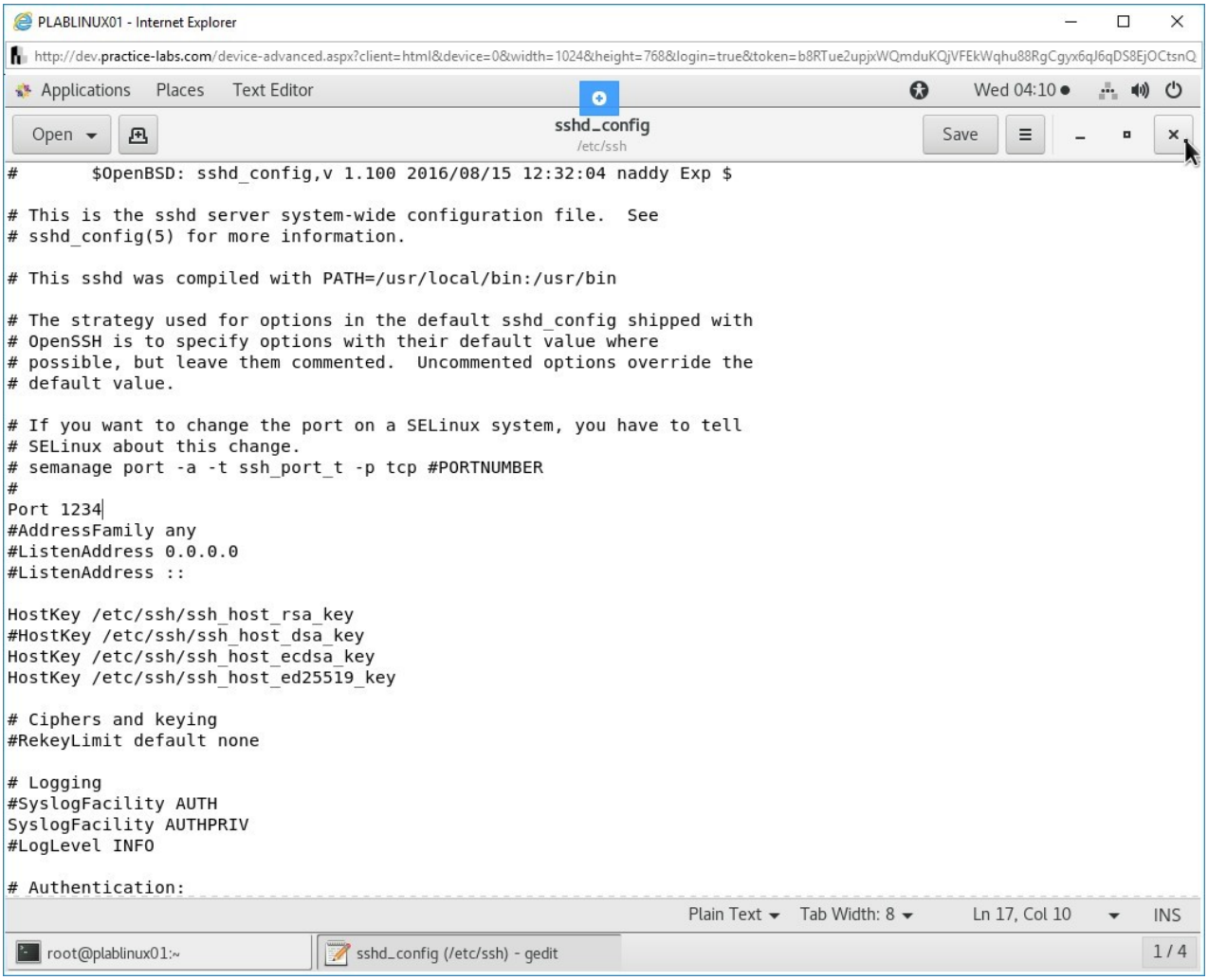


Figure 1.22 Screenshot of PLABLINUX01: Saving and closing the /etc/ssh/sshd_config file.

Step 5

You are now back on the terminal window. To restart the sshd service, type the following command:

```
systemctl restart sshd
```

Press **Enter**. Notice that the service fails to restart. This means that the port that you have chosen is being used by another program. You will need to choose an alternate port. You may have to try this a few times.

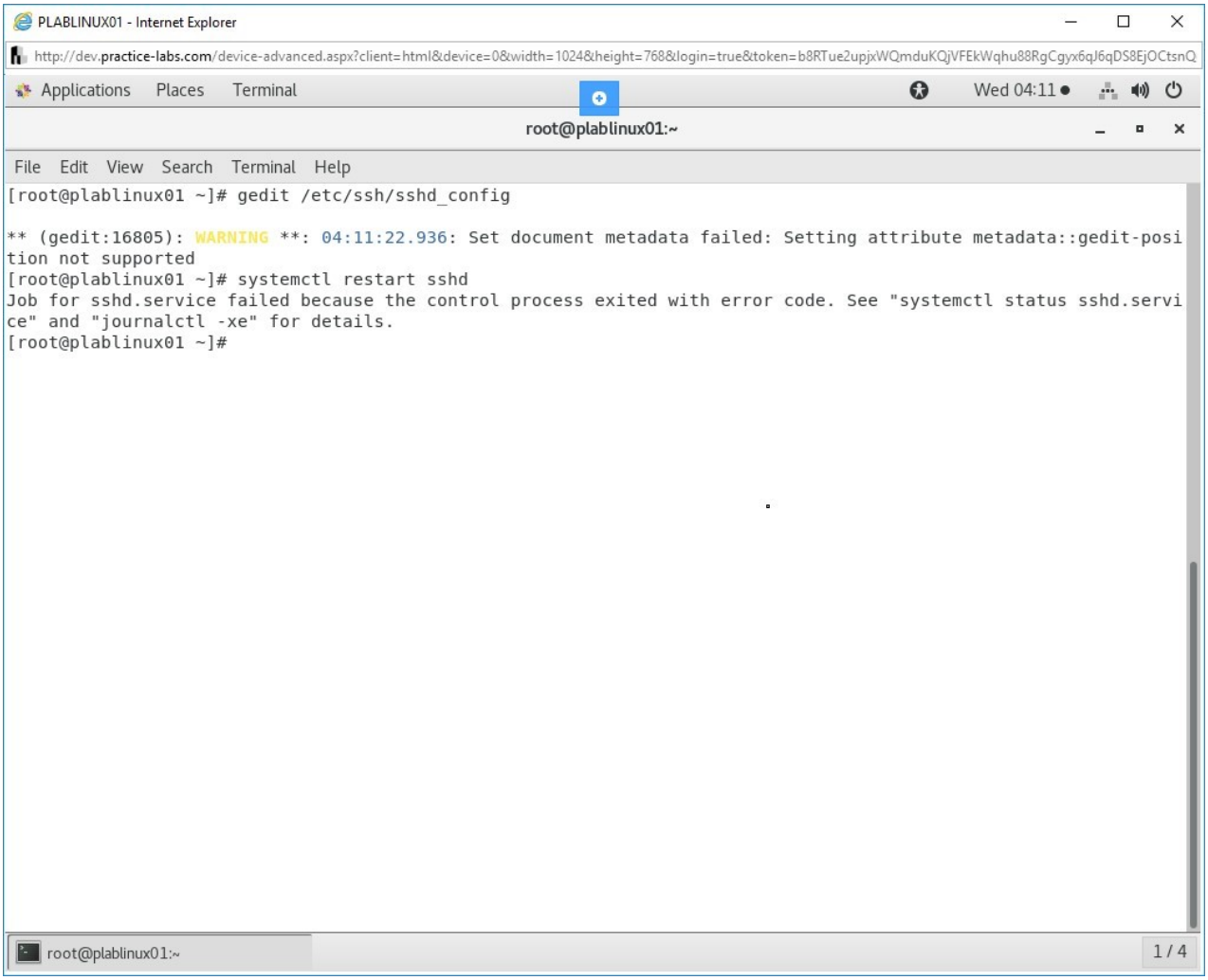


Figure 1.23 Screenshot of PLABLINUX01: Restarting the sshd service.

Task 4 - Verify the Last Logged In Users

There will be situations in which you will need to determine which users have logged on to the system. You can easily determine this on a CentOS system. To verify the last logged in users, perform the following steps:

Step 1

Clear the screen by entering the following command:

```
clear
```

To determine the recent logins on your system, type the following command:

```
last
```

Press **Enter**. Notice that various login entries appear. The listing starts with the most recent logins. It also shows the time user logged in and how long did the user stay connected with the system.

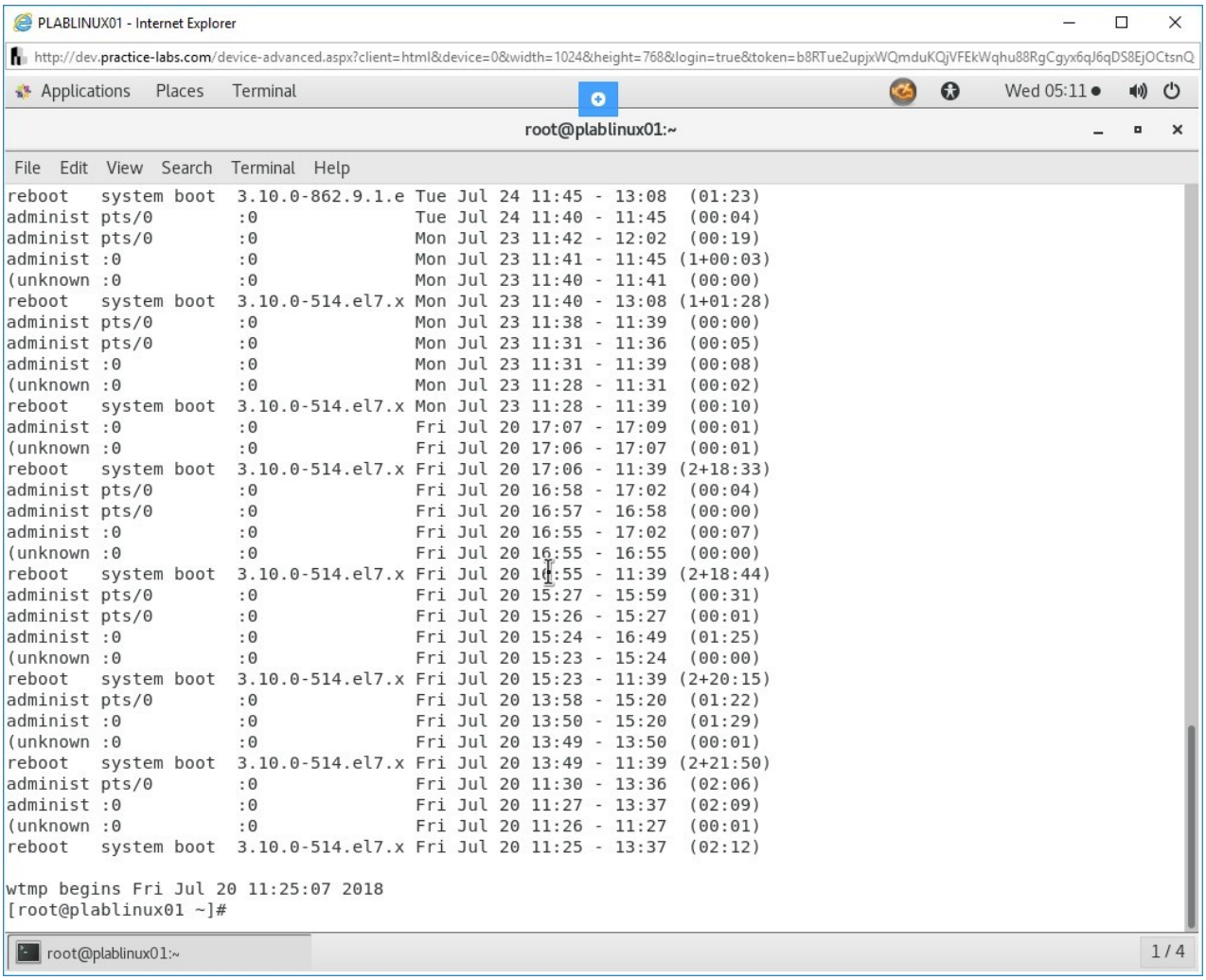


Figure 1.24 Screenshot of PLABLINUX01: Using the last command to verify the list of users who logged into the system.

Step 2

Clear the screen by entering the following command:

```
clear
```

You can also verify the logins for a specific user. Type the following command:

```
last root
```

Press **Enter**. Notice that you receive the **success** message.

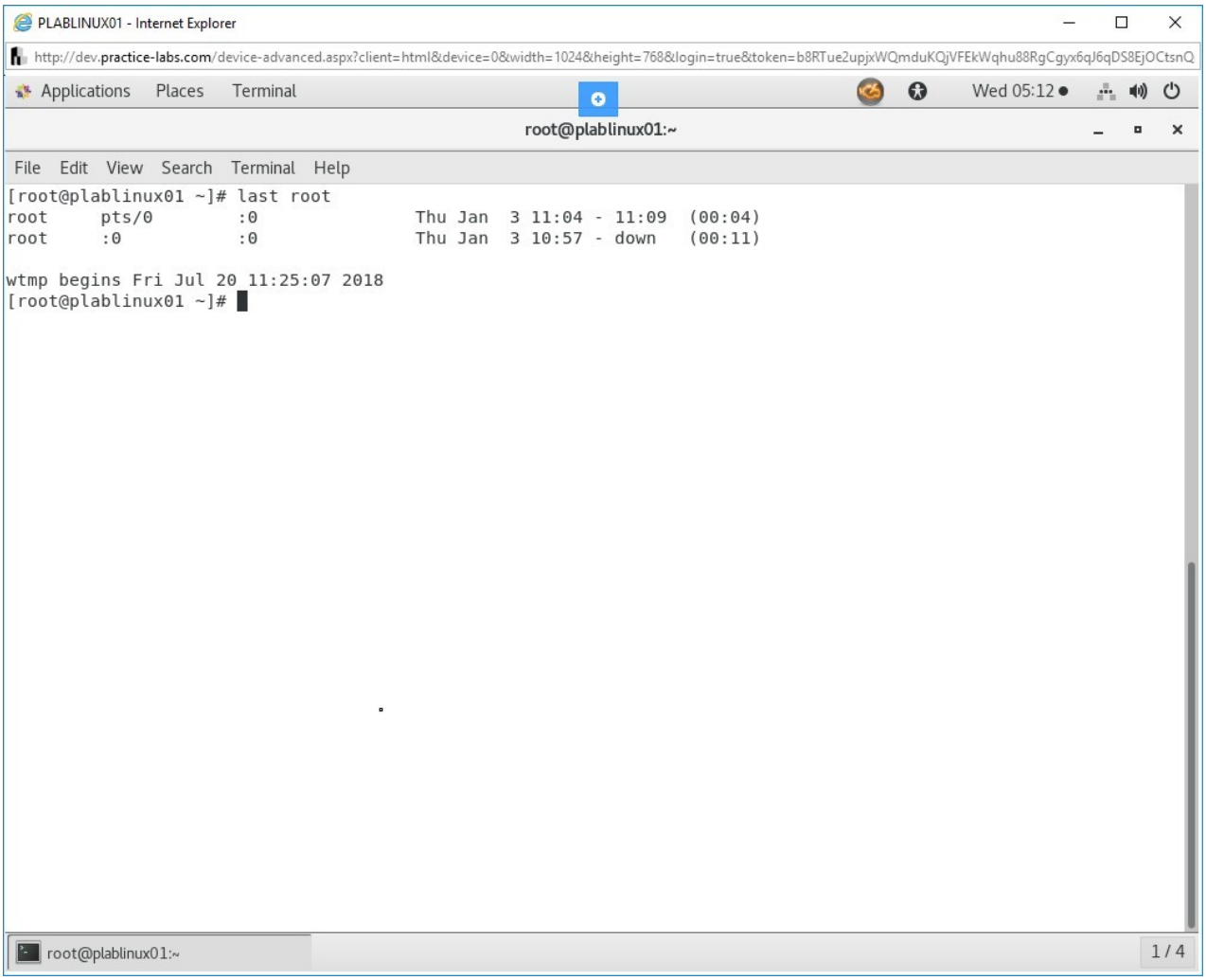


Figure 1.25 Screenshot of PLABLINUX01: Verifying the logins for the root user.

Step 3

The login data is retrieved from the latest **/var/log/wtmp** file. Type the following command:

```
last -f /var/log/wtmp
```

Press **Enter**. Notice that you get the same results as the last command.

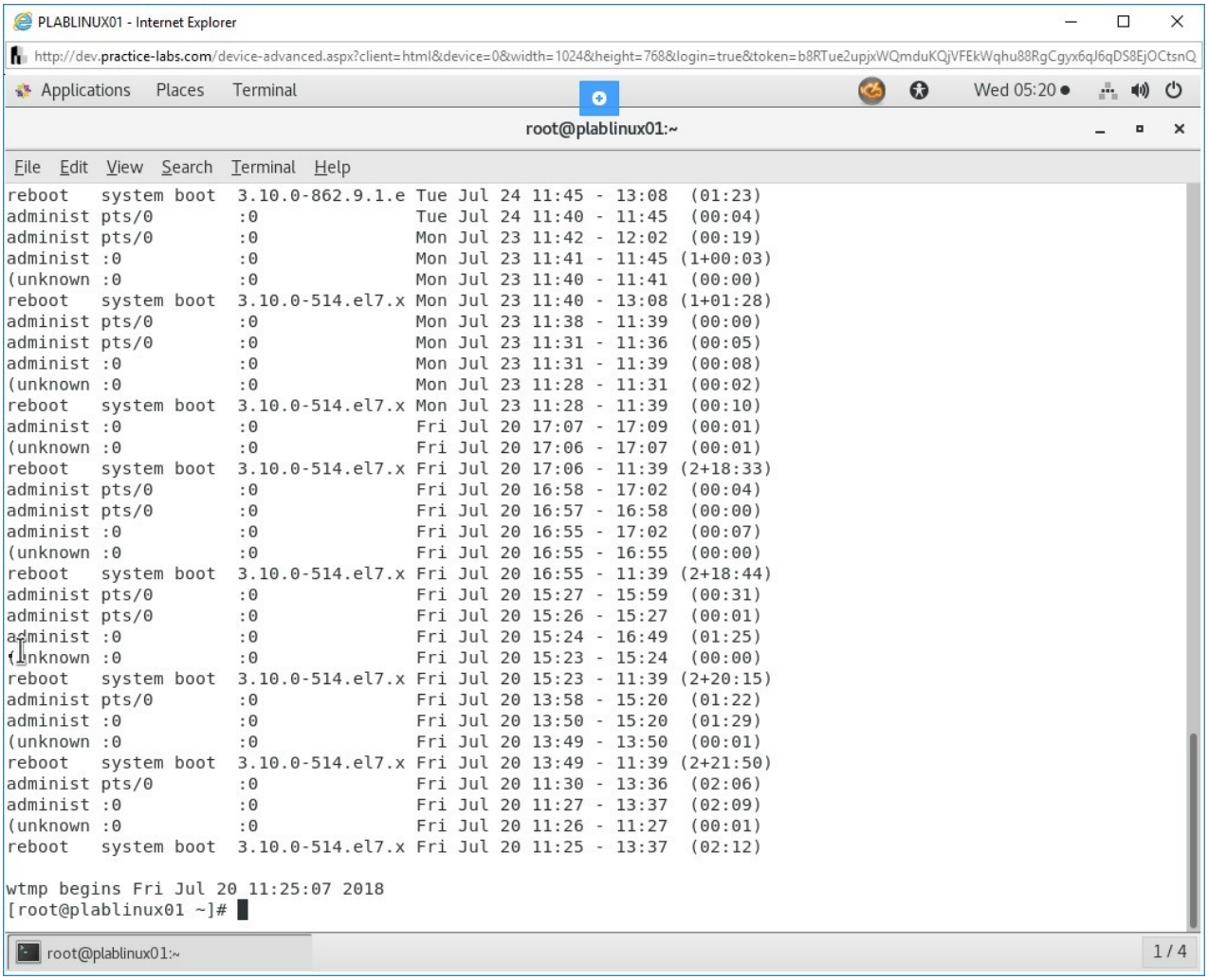


Figure 1.26 Screenshot of PLABLINUX01: Displaying the contents of the /var/log/wtmp file.

Step 4

Clear the screen by entering the following command:

```
clear
```

You can also find the last login for each individual on a system by using the **lastlog** command. Type the following command:

```
lastlog
```

Press **Enter**. Notice that you get the same results as the last command.

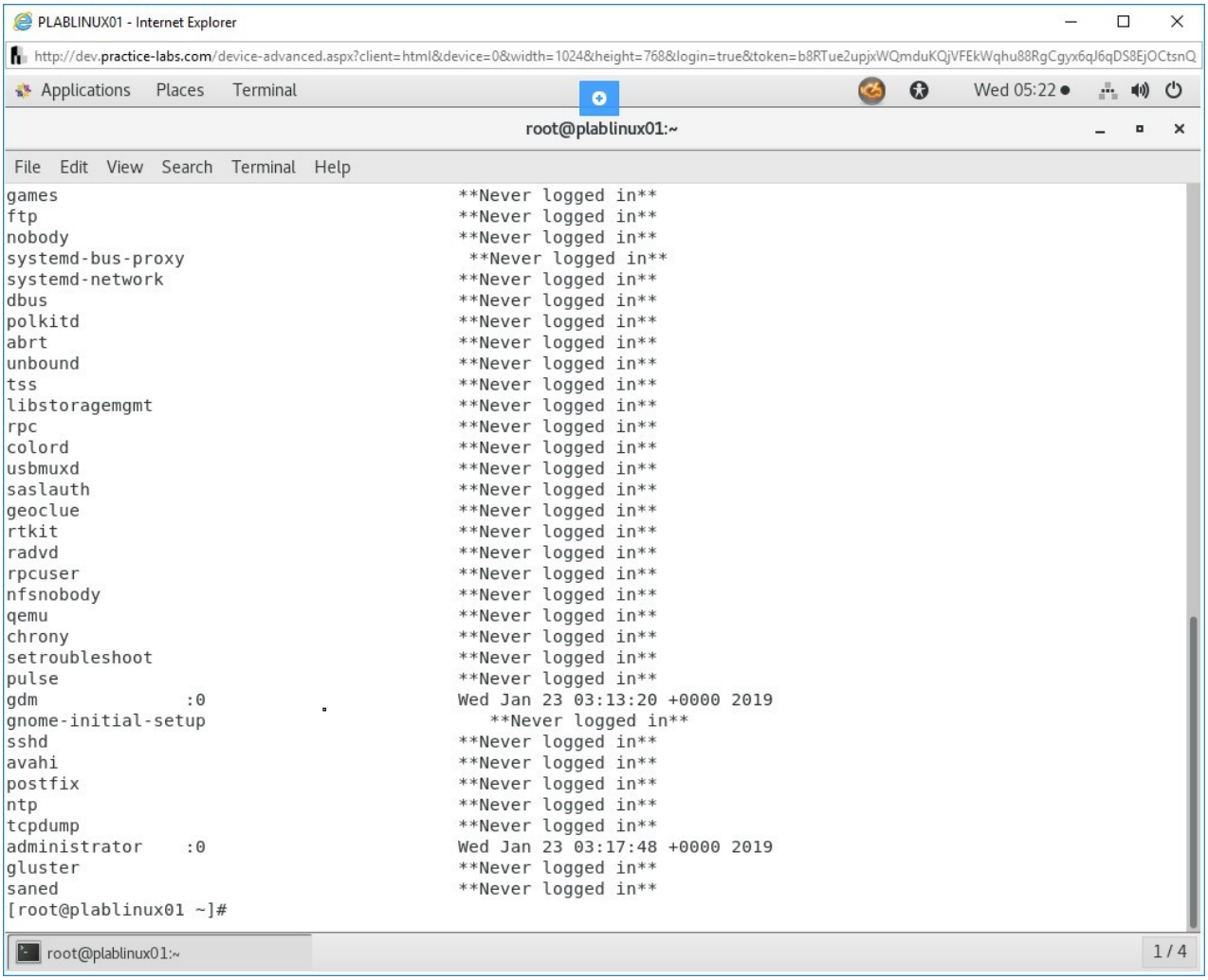


Figure 1.27 Screenshot of PLABLINUX01: Displaying the last login for each individual on a system by using the lastlog command.

Step 5

Clear the screen by entering the following command:

```
clear
```

You can find the users who never logged in using the **lastlog** command. Type the following command:

```
lastlog | grep Never | awk '{print $1}'
```

Press **Enter**. Notice that you get the same results as the last command.

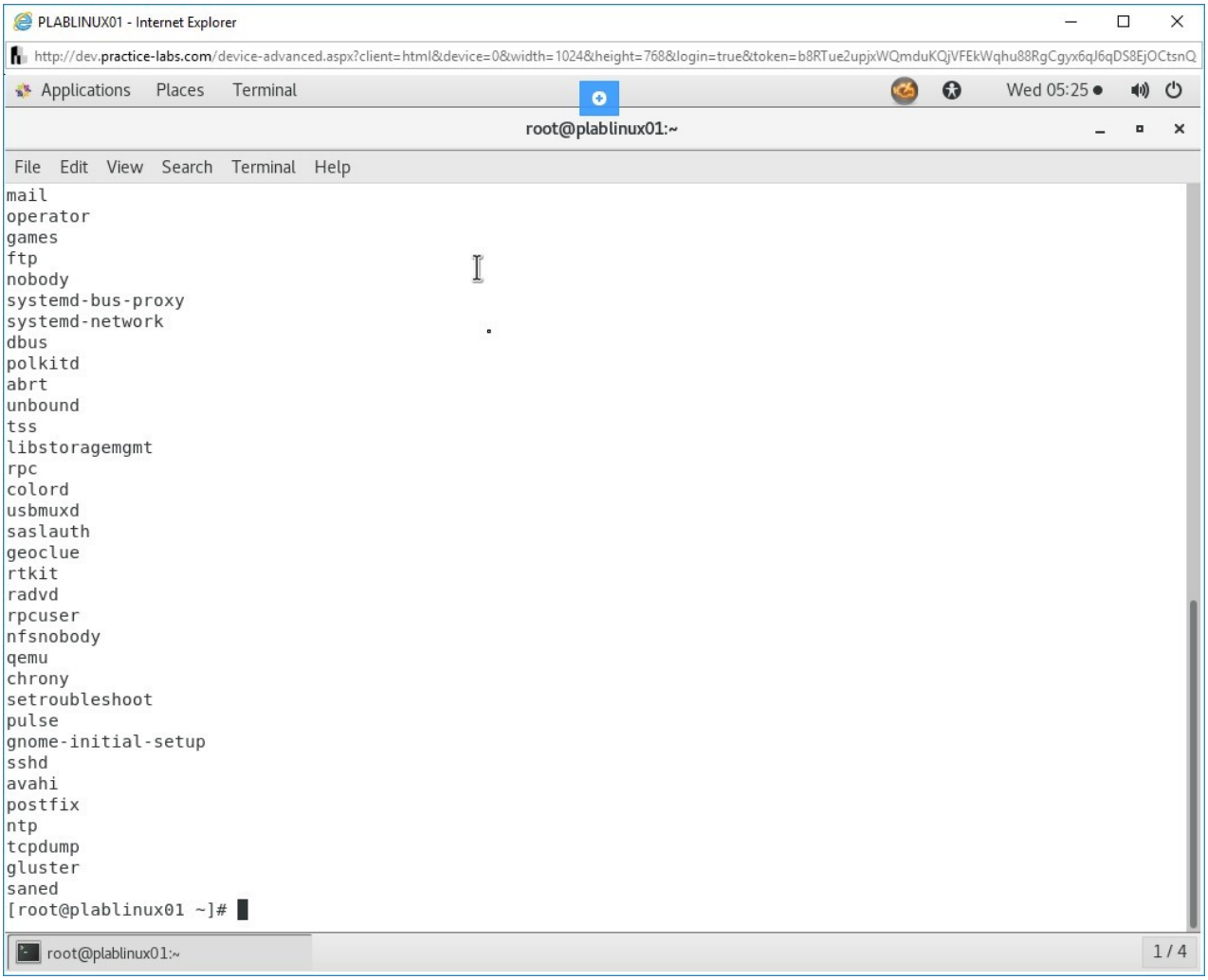


Figure 1.28 Screenshot of PLABLINUX01: Finding the users who never logged in using the lastlog command.

Task 5 - Know the Key Locations for logging

Logs are meant for recording events in a system. In the case of an event, you can refer to the respective log for more details. Logs are stored in the /var/log directory. It is important to note that the number of logs in each system will differ because of the installed applications. For example, if a system has MySQL installed, this directory will have a log pertaining to the MySQL application. On the other hand, a system that does not have MySQL, will not have this log generated. To test the Apache Web Server Traffic, perform the following steps:

Step 1

Clear the screen by entering the following command:

```
clear
```

Let's first list the number of logs in the **/var/log** directory. Type the following command:

```
ls -l /var/log/
```

Press **Enter**.

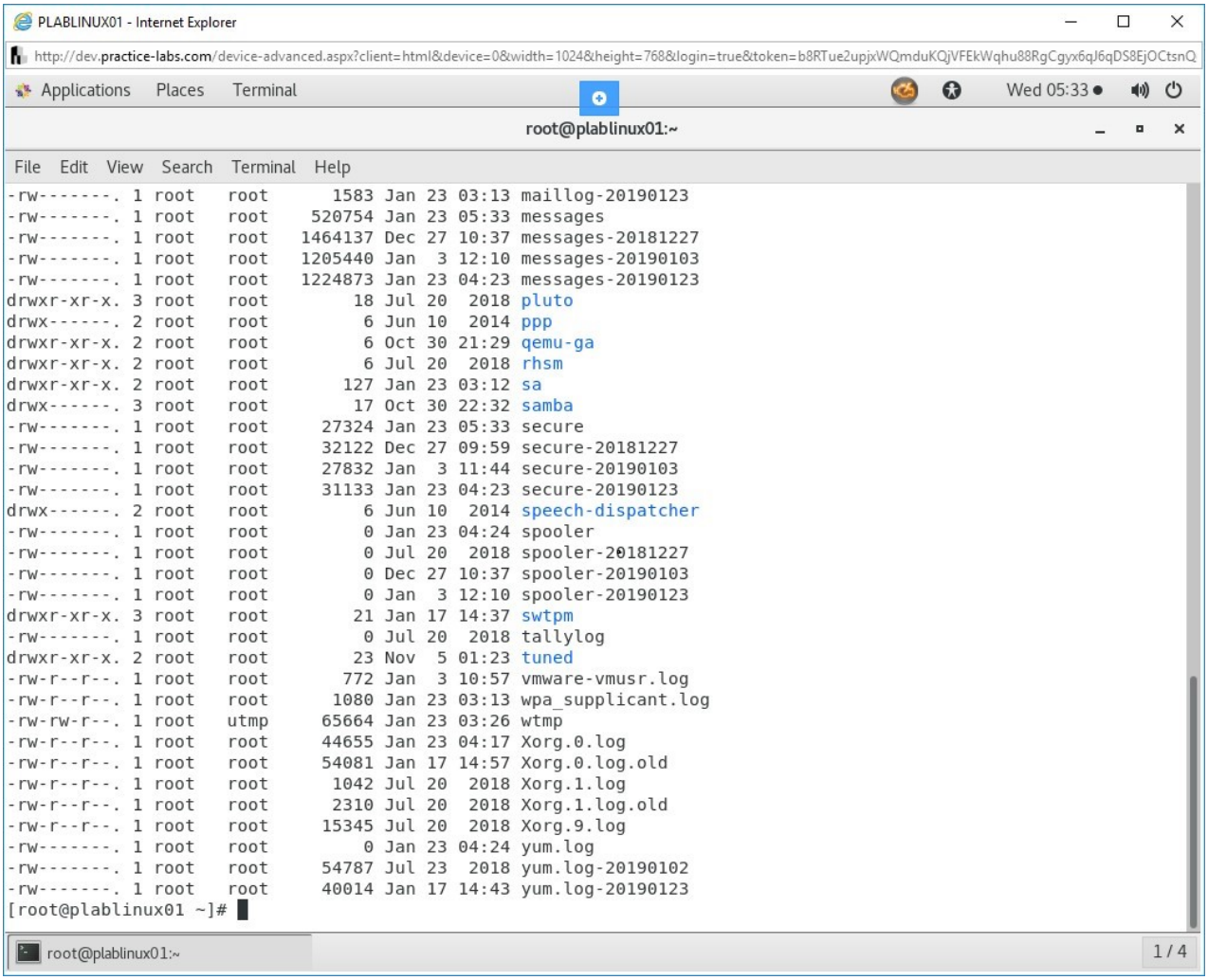


Figure 1.29 Screenshot of PLABLINUX01: Listing the number of logs in the /var/log directory.

Step 2

Clear the screen by entering the following command:

```
clear
```

To view a log file, you can use the **cat** command. Type the following command:

```
cat /var/log/vmware-vmusr.log
```

Press **Enter**.

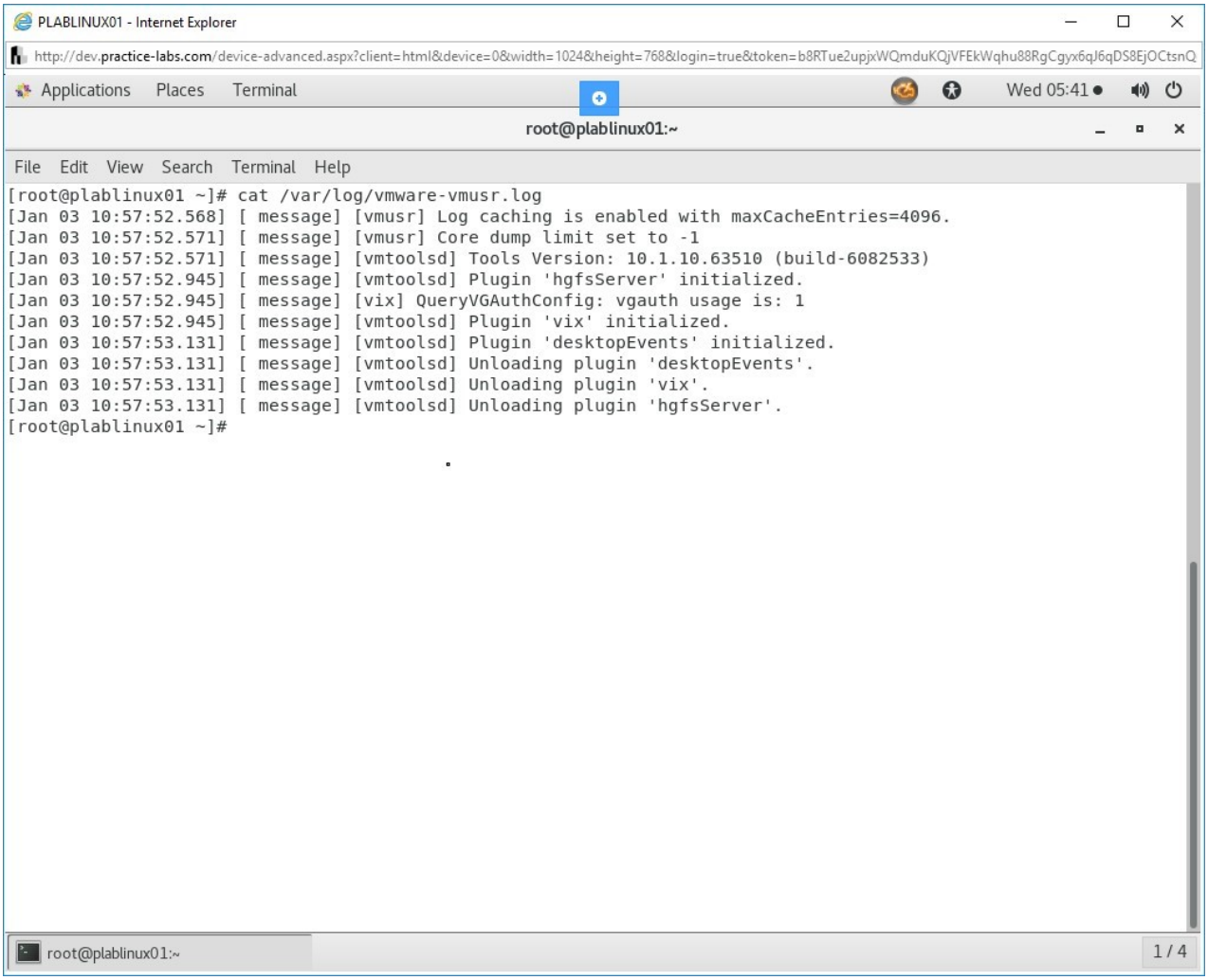


Figure 1.30 Screenshot of PLABLINUX01: Viewing a log file using the cat command.

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

Review

Well done, you have completed the **Secure a Linux Terminal and Implement Logging Services** Practice Lab.

Summary

You completed the following exercise:

- Exercise 1 - Secure a Linux Terminal and Implement Logging Services

You should now be able to:

- Disable Unnecessary Services
- Disable the root Login via SSH
- Change the Default SSH Port
- Verify the Last Logged in Users
- Know the Key Locations for logging

Feedback

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