

Secure Communication using SSH

- **Introduction**
 - **Lab Topology**
 - **Exercise 1 - Secure Communication Using SSH**
 - **Review**
-

Introduction

Welcome to the **Secure Communication using SSH** Practice Lab. In this module you will be provided with the instructions and devices needed to develop your hands-on skills.

Communication

SSH

OpenSSH Server

CentOS

Learning Outcomes

In this module, you will complete the following exercise:

- Exercise 1 - Secure Communication using SSH

After completing this lab, you will be able to:

- Configure Network on CentOS
- Perform Basic Configuration for the OpenSSH Server
- Connect with the OpenSSH Server

Exam Objectives

The following exam objectives are covered in this lab:

- **LPI: 110.1** Perform security administration tasks

- **CompTIA:** 3.1 Given a scenario, apply or acquire the appropriate user and/or group permissions and ownership.
- **CompTIA:** 4.4 Given a scenario, analyse and troubleshoot application and hardware issues.

***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 Communication Using SSH

In the old days, telnet was used to establish remote connectivity with another server. The key problem was that telnet did not secure the communication over an unsecured channel, such as the Internet. SSH secures the communication even if it is taking place over the Internet.

In this exercise, you will learn to secure communication using SSH.

Learning Outcomes

After completing this exercise, you will be able to:

- Log into a Linux System
- Configure Network on CentOS
- Perform Basic Configuration for the OpenSSH Server
- Connect with the OpenSSH Server

Your Devices

You will be using the following device 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**.

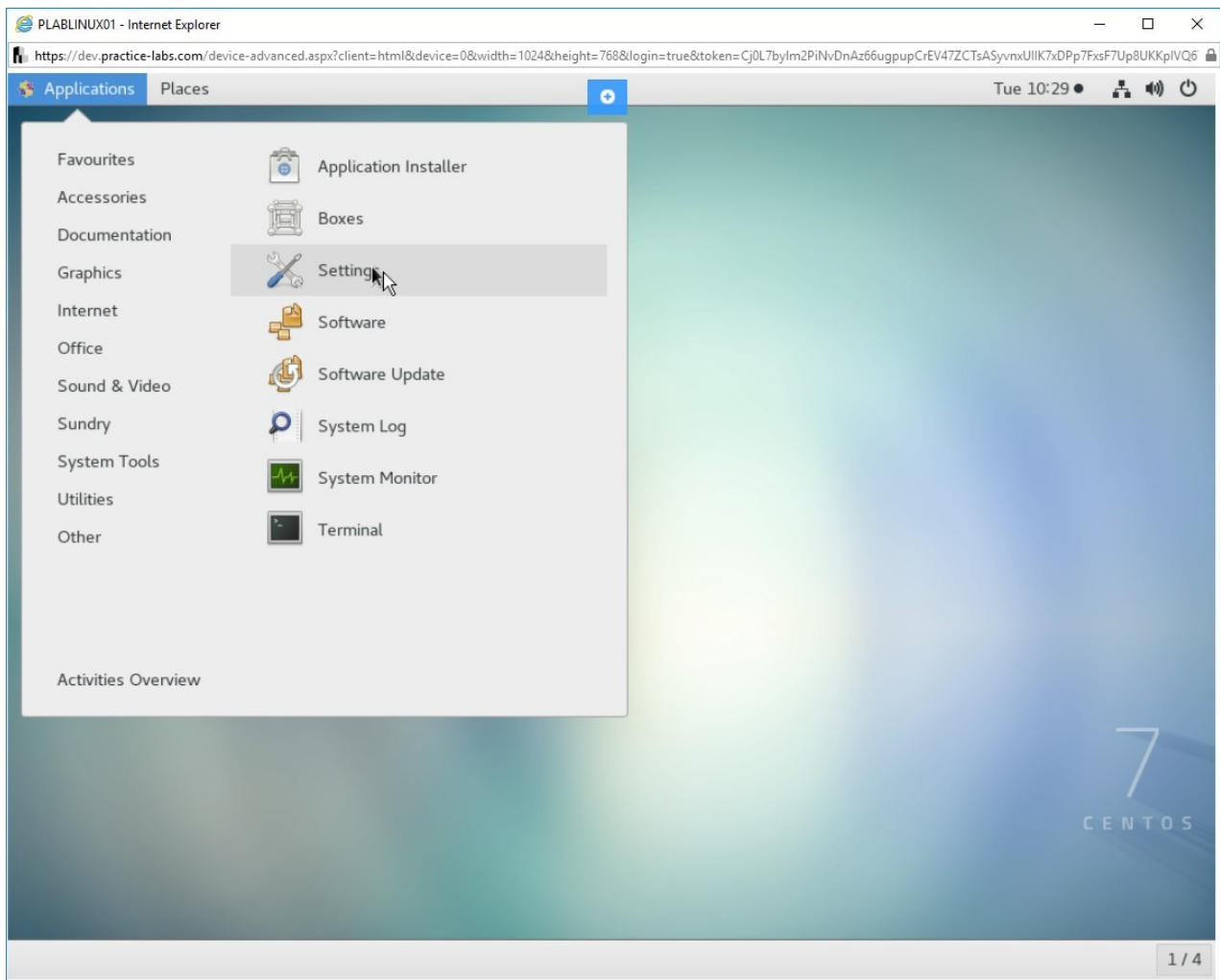


Figure 1.1 Screenshot of PLABLINUX01: Selecting the Settings option from the Applications > System Tools menu.

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.

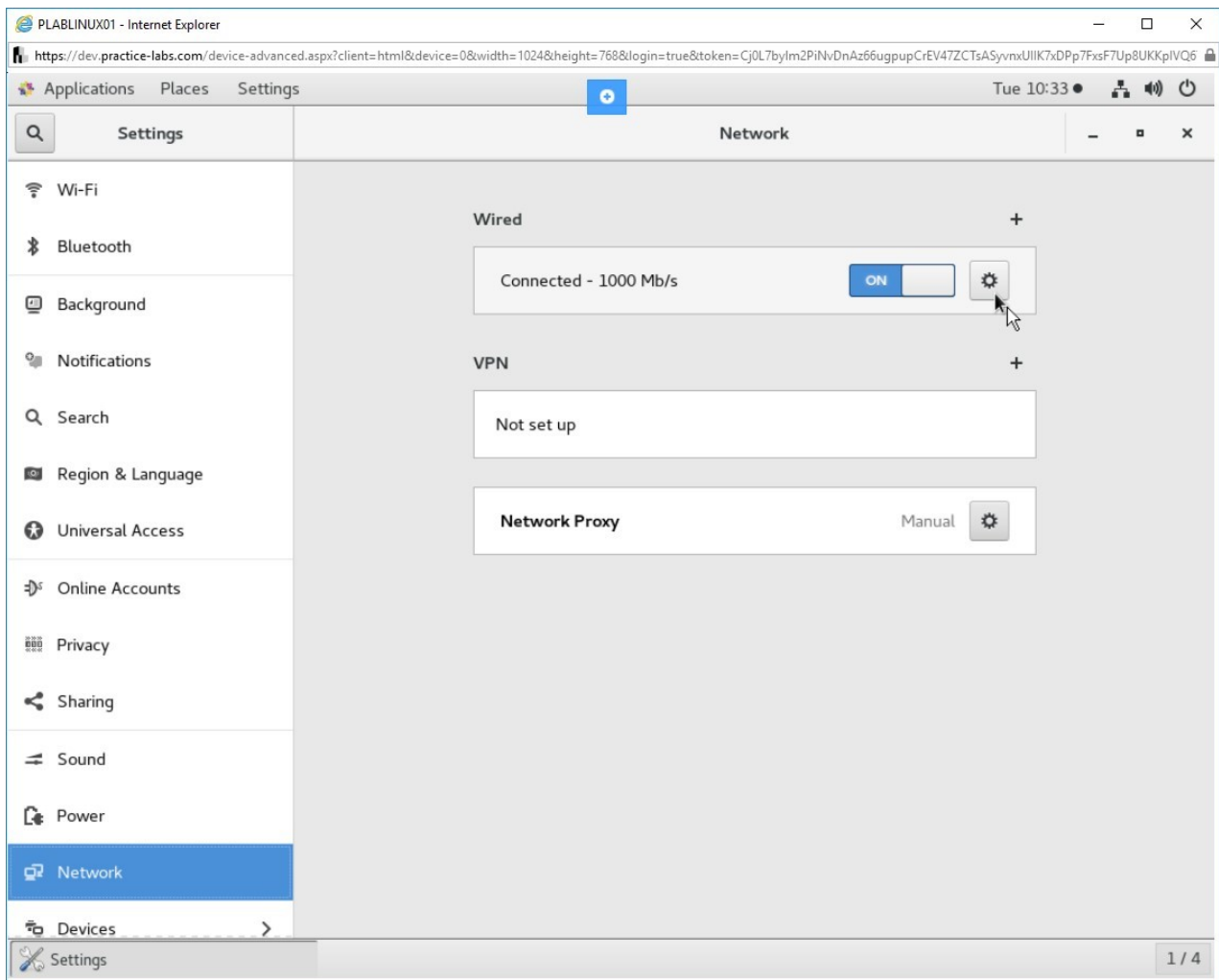


Figure 1.2 Screenshot of PLABLINUX01: Clicking the button to invoke the Wired dialog box.

Step 3

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

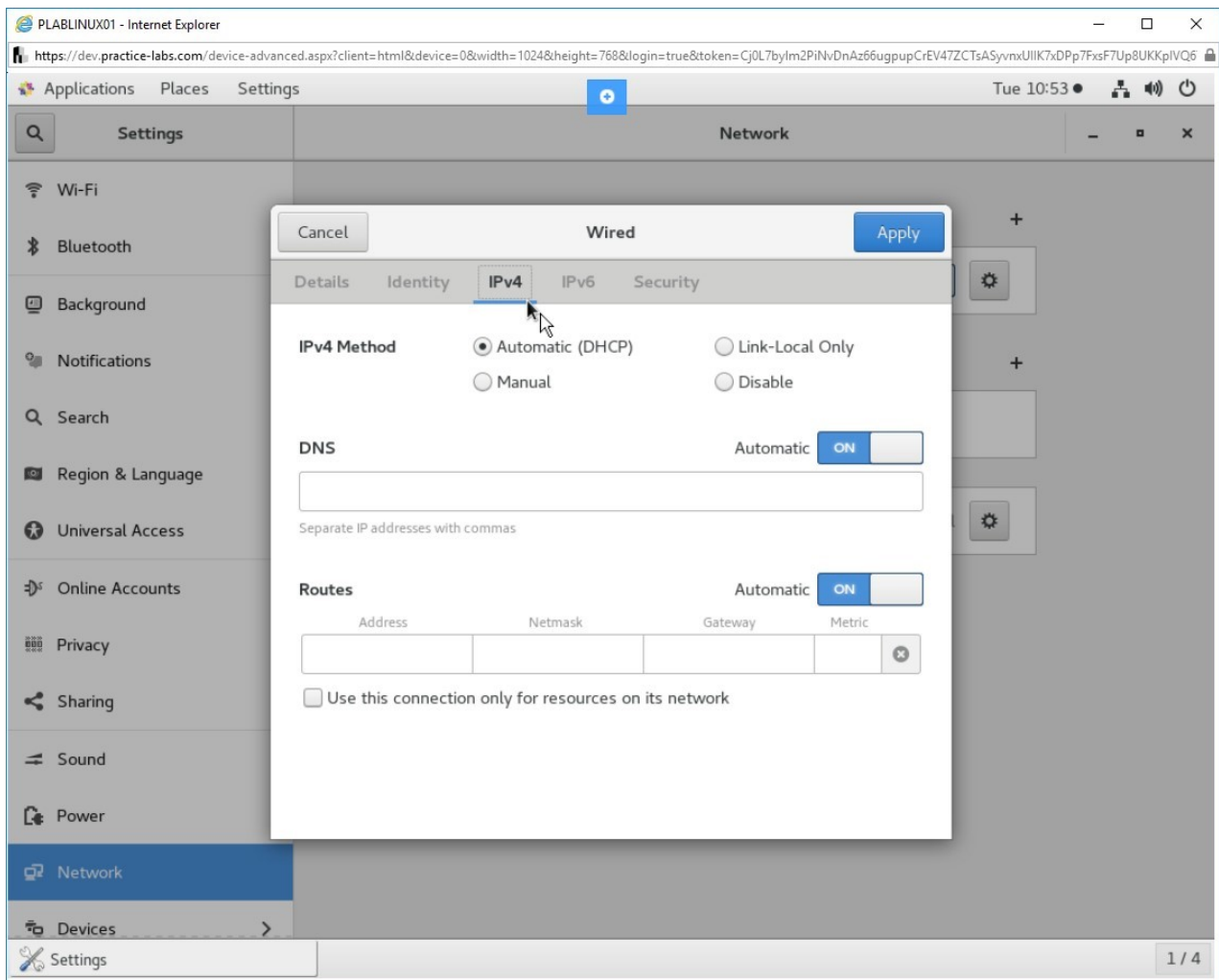


Figure 1.3 Screenshot of PLABLINUX01: Selecting the IPv4 tab in the Wired dialog box.

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**.

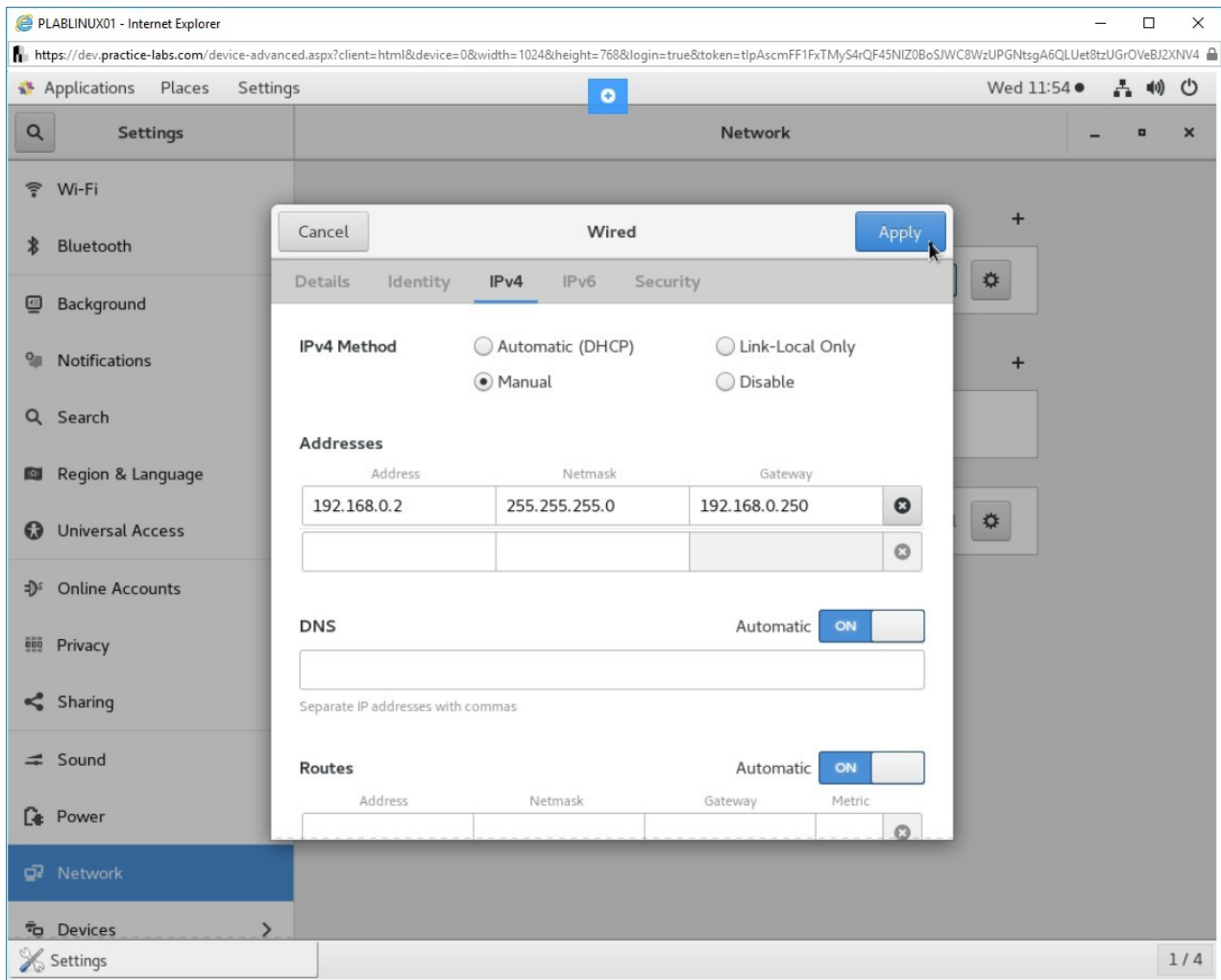


Figure 1.4 Screenshot of PLABLINUX01: Entering the network information and then clicking the Apply button.

Step 5

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

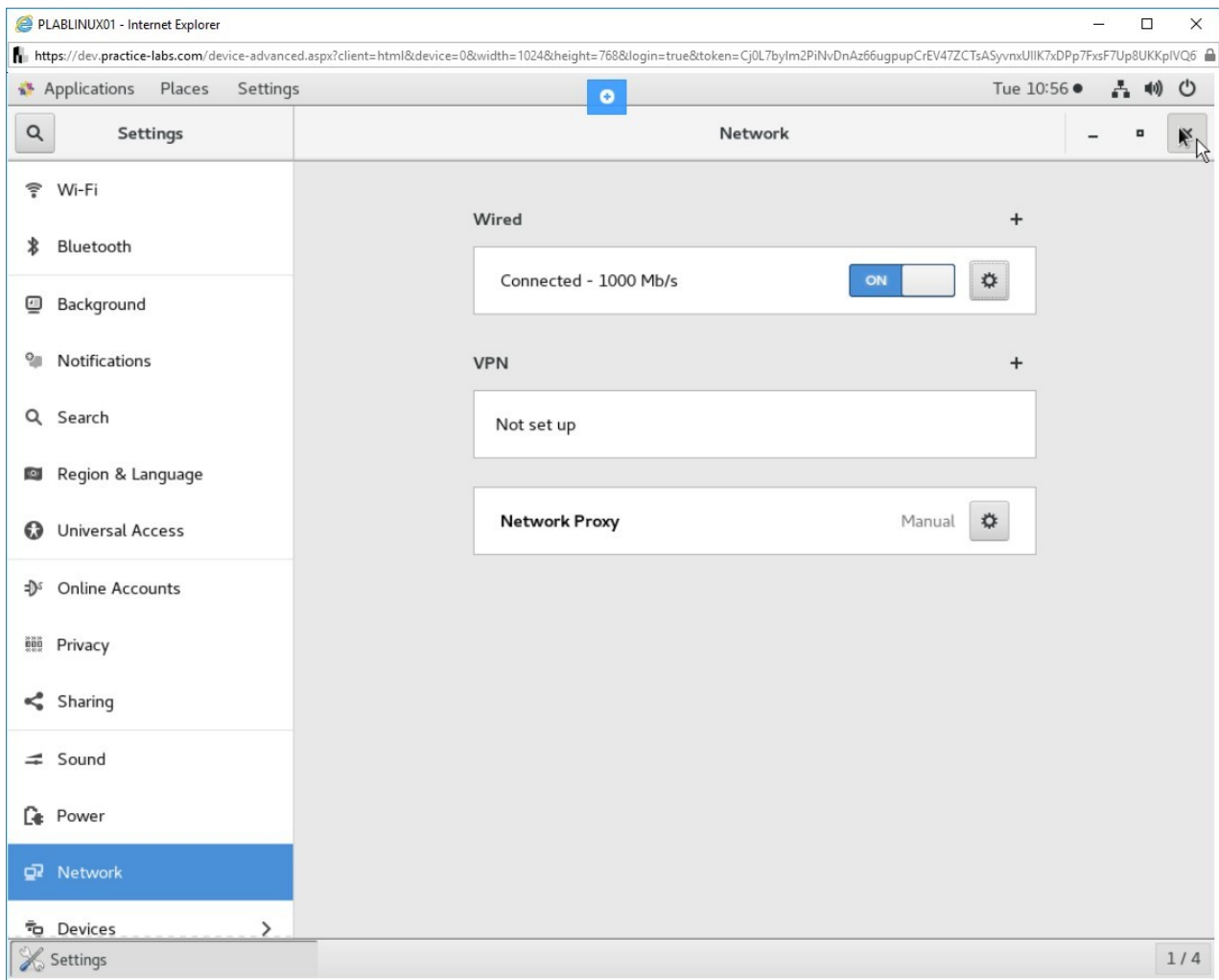


Figure 1.5 Screenshot of PLABLINUX01: Displaying the Settings window.

Task 2 - Perform Basic Configuration for the OpenSSH Server

OpenSSH is available in the Yum repositories. It is widely used for remote administration or remote file transfer. It uses SSH as the underlying protocol for secure communication.

In this task, you will learn to connect with the OpenSSH server. To connect with the OpenSSH server, perform the following steps:

Step 1

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

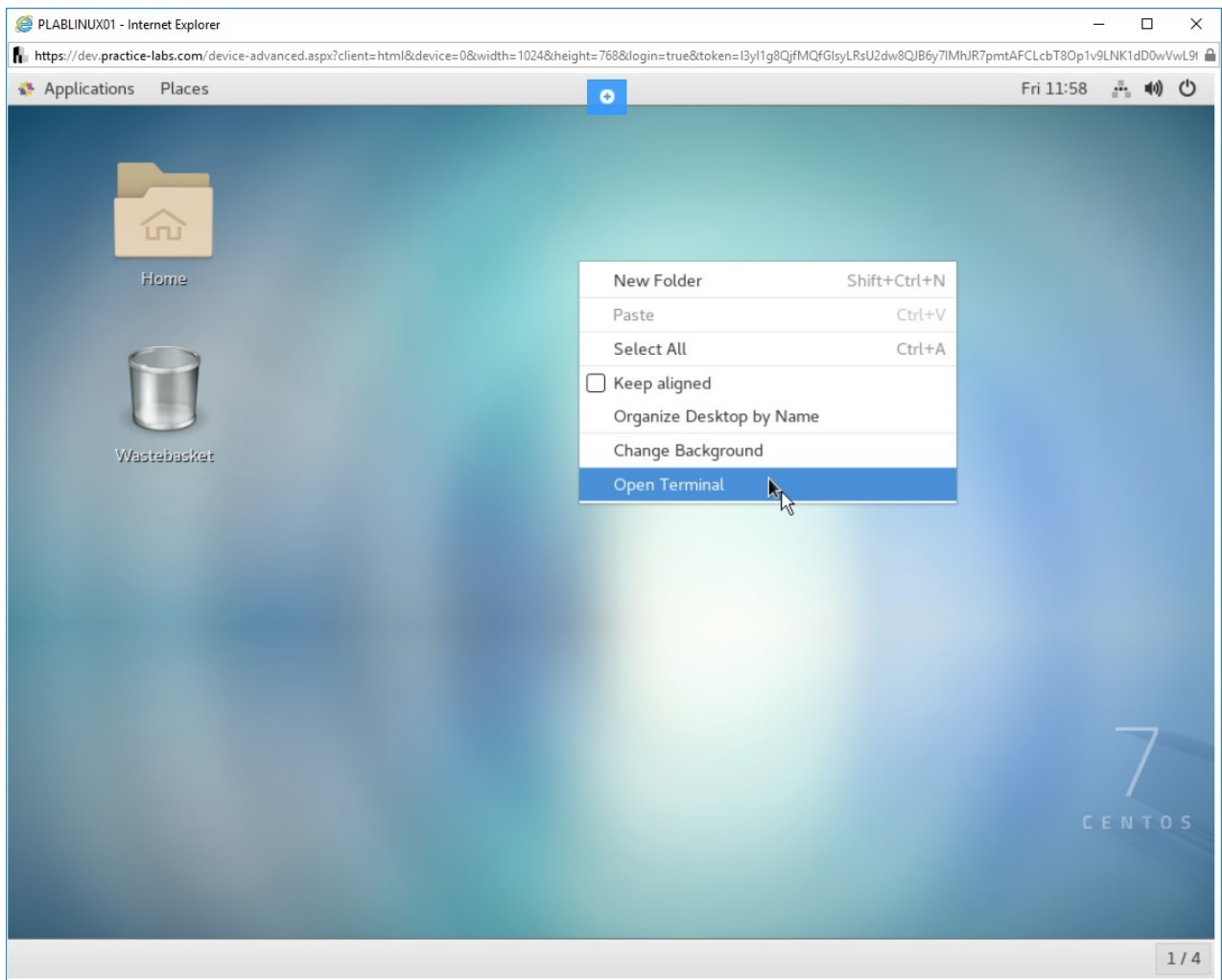


Figure 1.6 Screenshot of PLABLINUX01: Selecting the Open Terminal option from the context menu.

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**.

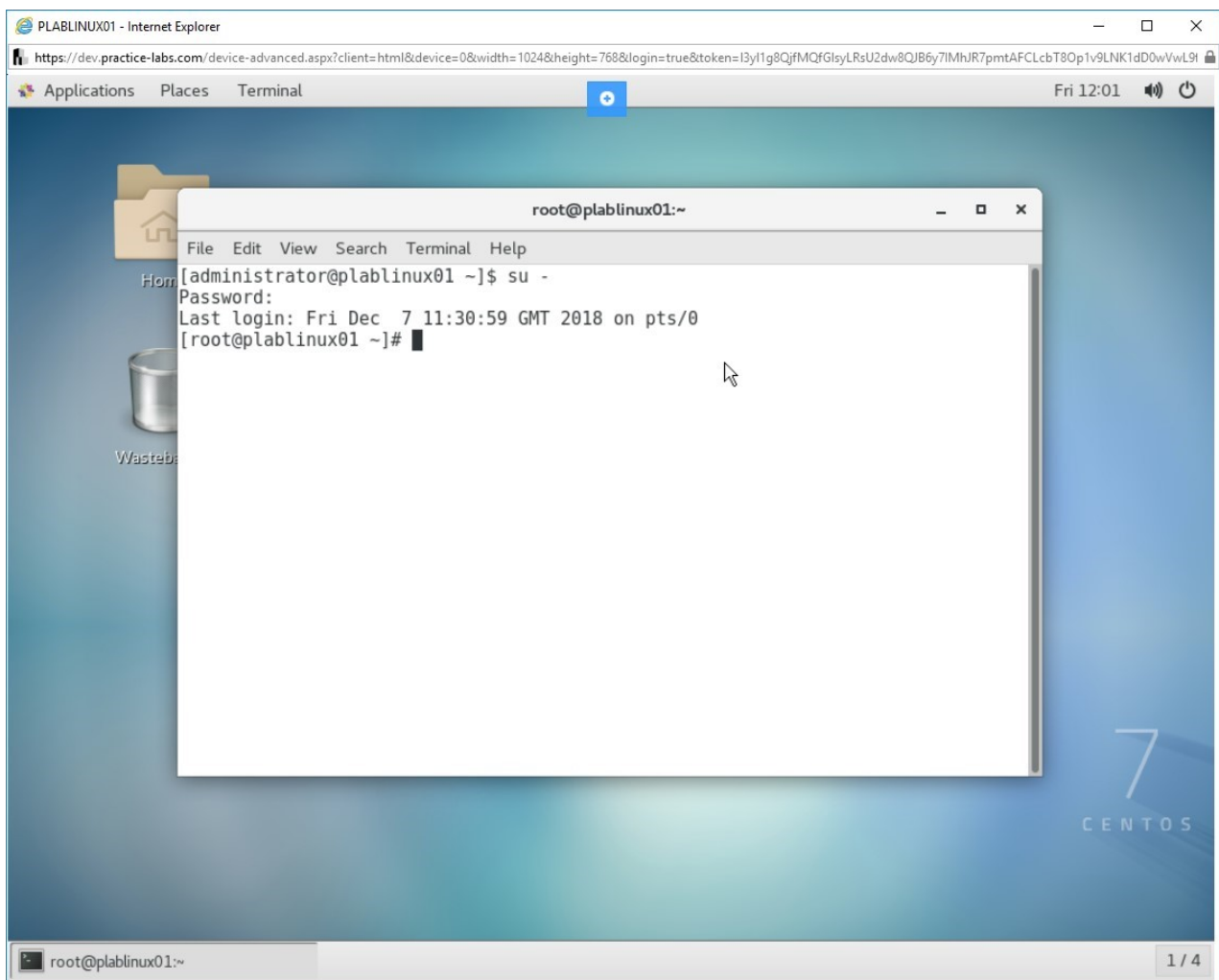


Figure 1.7 Screenshot of PLABLINUX01: Changing the account to the root account with the su command.

Step 3

Clear the screen by entering the following command:

```
clear
```

To check if openssh is already installed, type the following command:

```
rpm -qa | grep openssh
```

Press **Enter**. Notice that the OpenSSH server is already installed. If it is not installed, you should install it using the **yum install openssh** command.

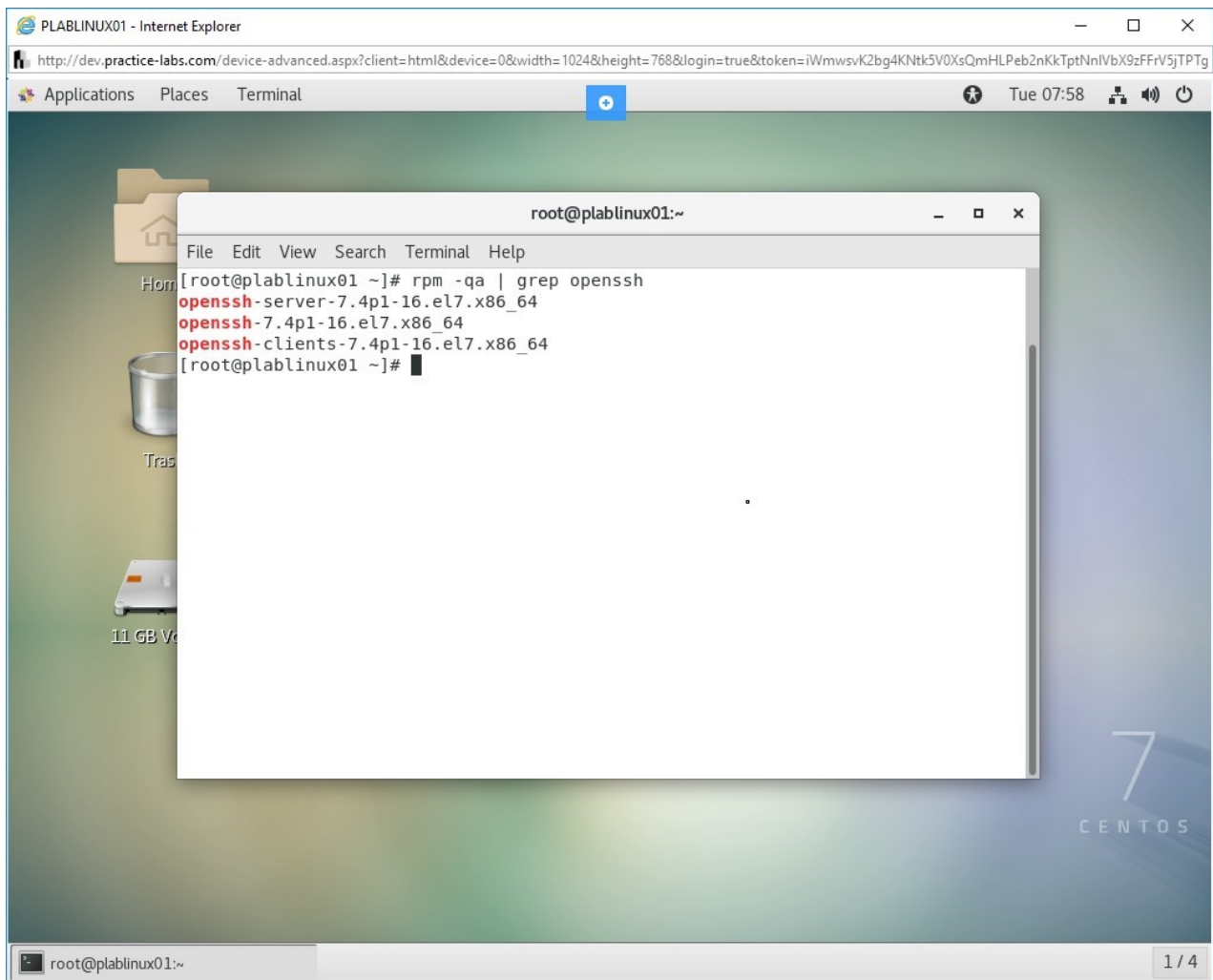


Figure 1.8 Screenshot of PLABLINUX01: Verifying if OpenSSL package is installed.

Step 4

You need to check the status of the OpenSSH server service next. Type the following command:

```
systemctl status sshd
```

Press **Enter**. Notice that the service is **Active** and **running**.

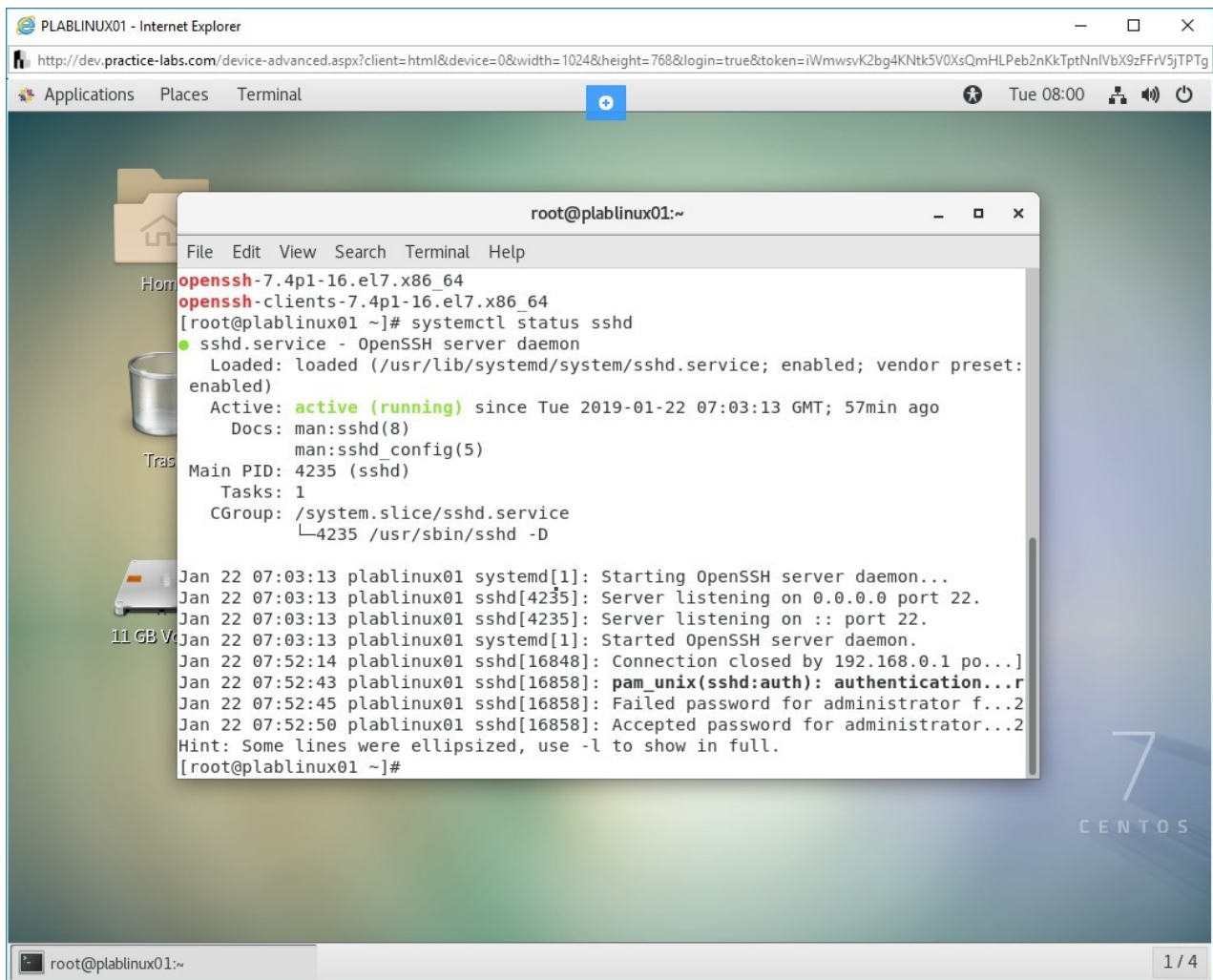


Figure 1.9 Screenshot of PLABLINUX01: Checking the status of sshd service.

Step 5

Clear the screen by entering the following command:

```
clear
```

You need to create a rule in iptables so that connection from a specific range of IP addresses can be established. Type the following command:

```
iptables -A INPUT -s 192.168.0.0/24 -p tcp --dport 22 -j  
ACCEPT
```

Press **Enter**. Notice that there is no error generated, which means that the rule has been added in iptables. Minimize the terminal window.

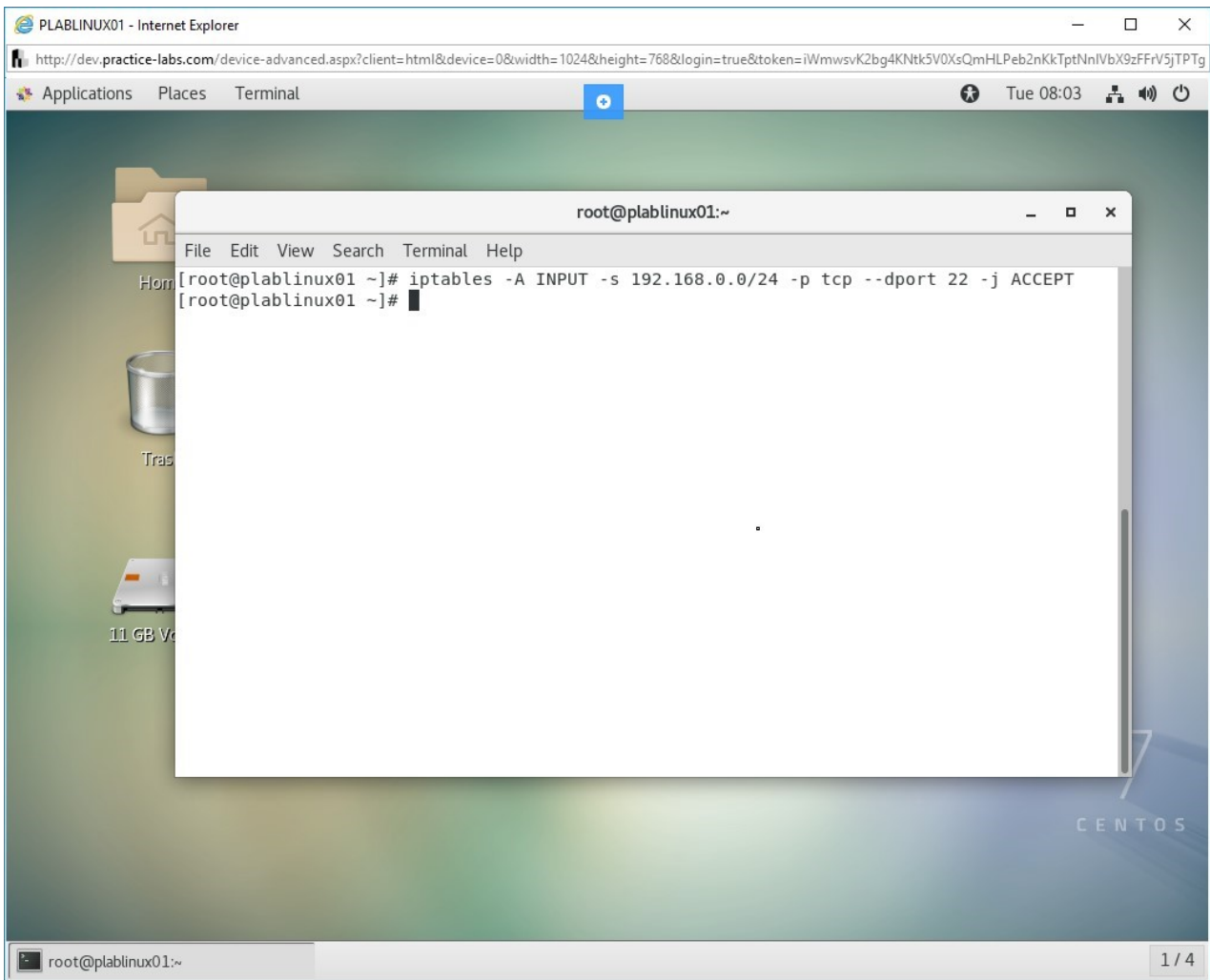


Figure 1.10 Screenshot of PLABLINUX01: Adding a rule in iptables for OpenSSH.

Task 3 - Connect With the OpenSSH Server

After you had performed the basic configuration, you need to test the connection with the OpenSSH server.

In this task, you will learn to connect to the OpenSSH server. To connect to the OpenSSH server, 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.

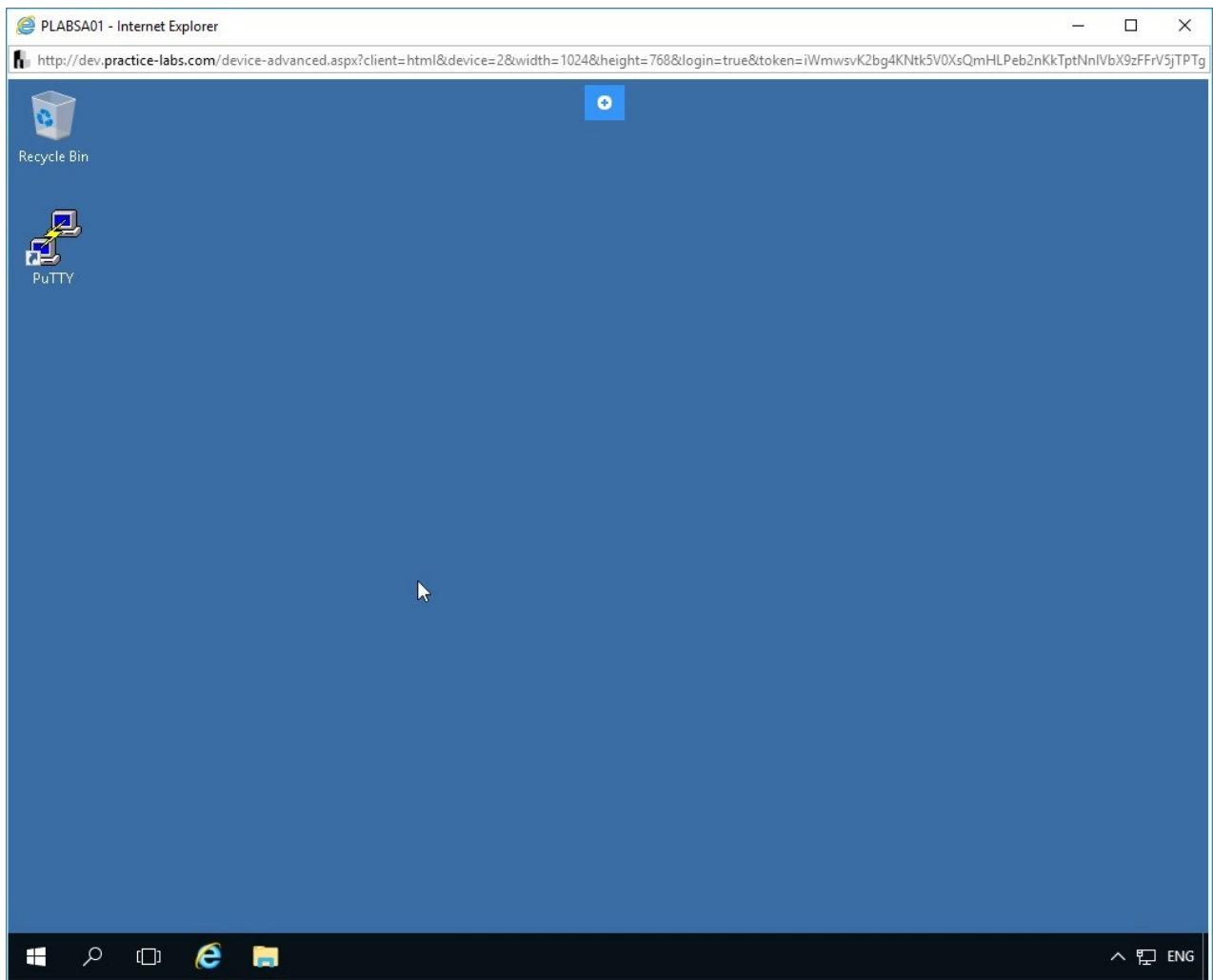


Figure 1.11 Screenshot of PLABSA01: Displaying the PLABSA01 desktop.

Step 2

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

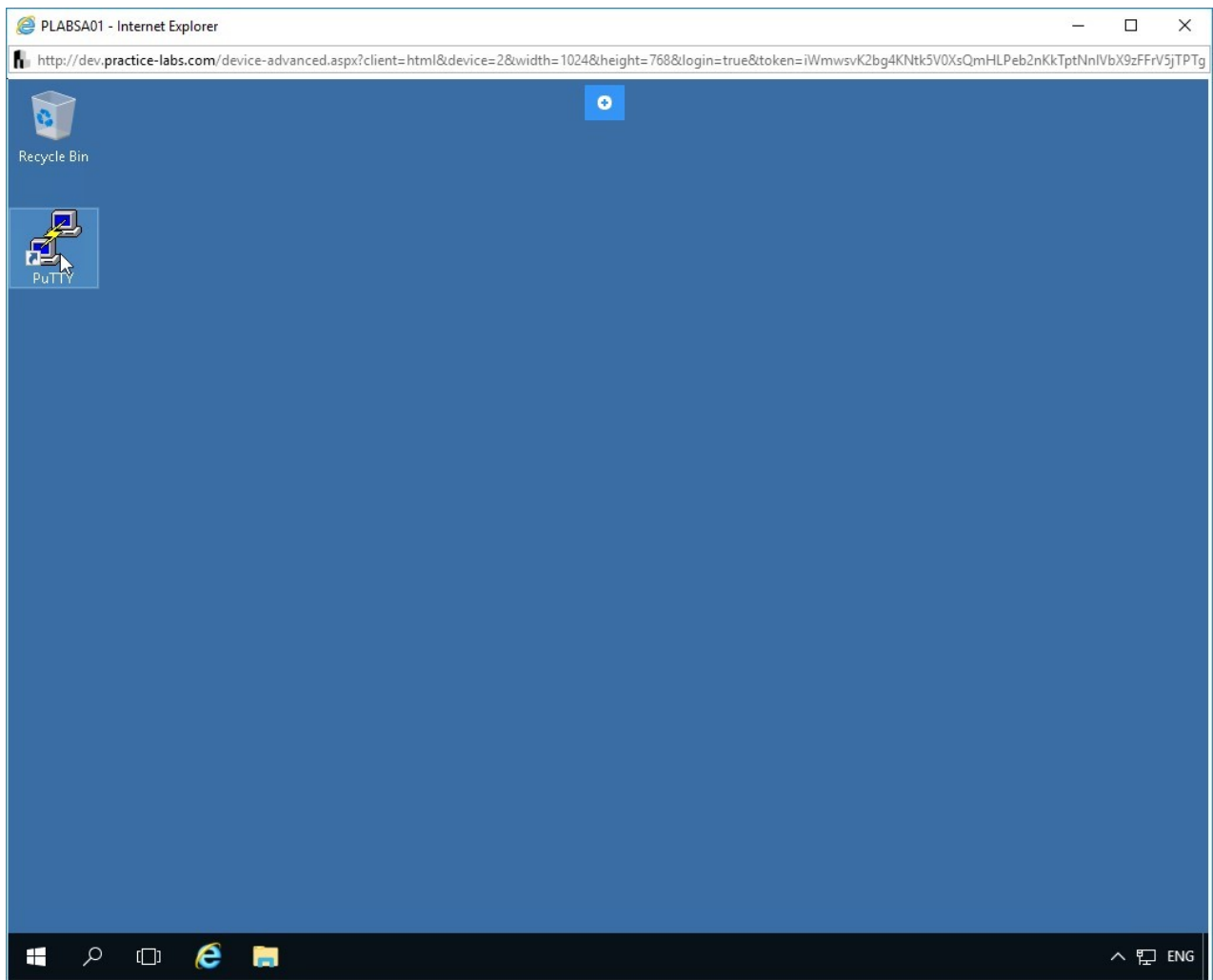


Figure 1.12 Screenshot of PLABSA01: Double-clicking the PuTTY icon.

Step 3

Notice that the **PuTTY Configuration** dialog box appears.

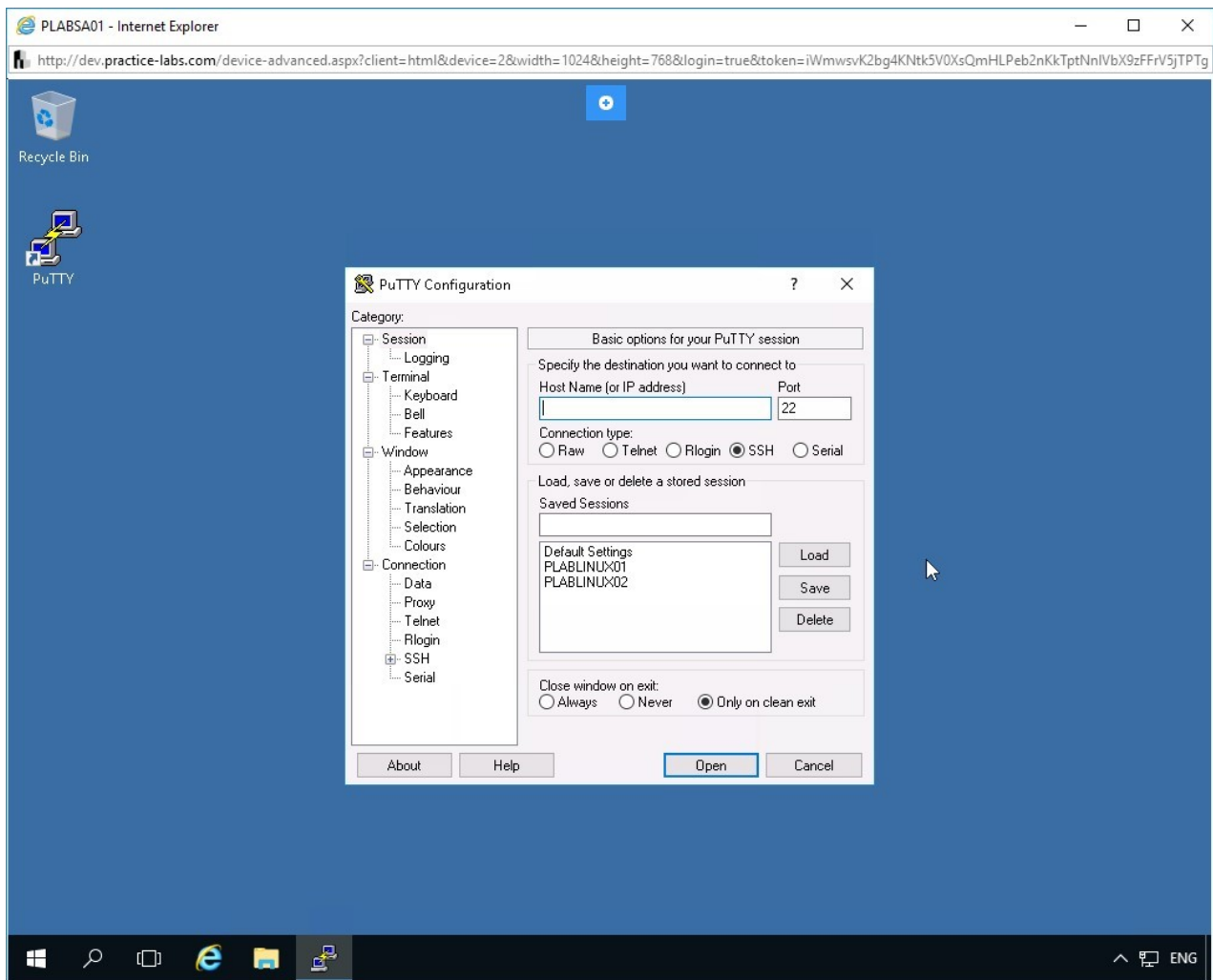


Figure 1.13 Screenshot of PLABSA01: Displaying the PuTTY Configuration dialog box.

Step 4

On the **PuTTY Configuration** dialog box, select **PLABLINUX01** under the **Load, save or delete a stored session** section and click **Load**.

Notice that **PLABLINUX01** now appears in the **Saved Sessions** text box.

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

Click **Open**.

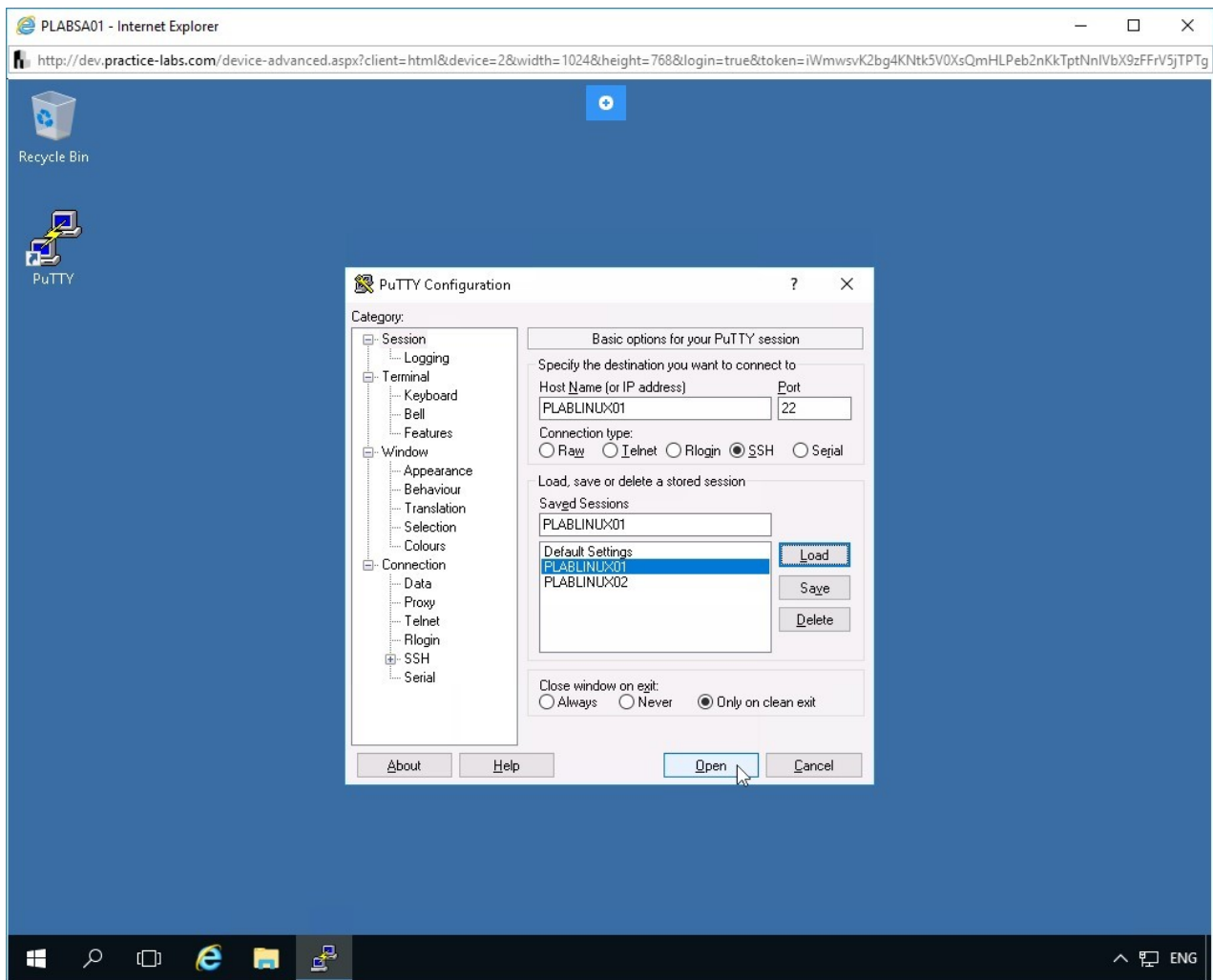


Figure 1.14 Screenshot of PLABSA01: Loading the PLABLINUX01 configuration.

Step 5

Notice that the SSH session window launches.

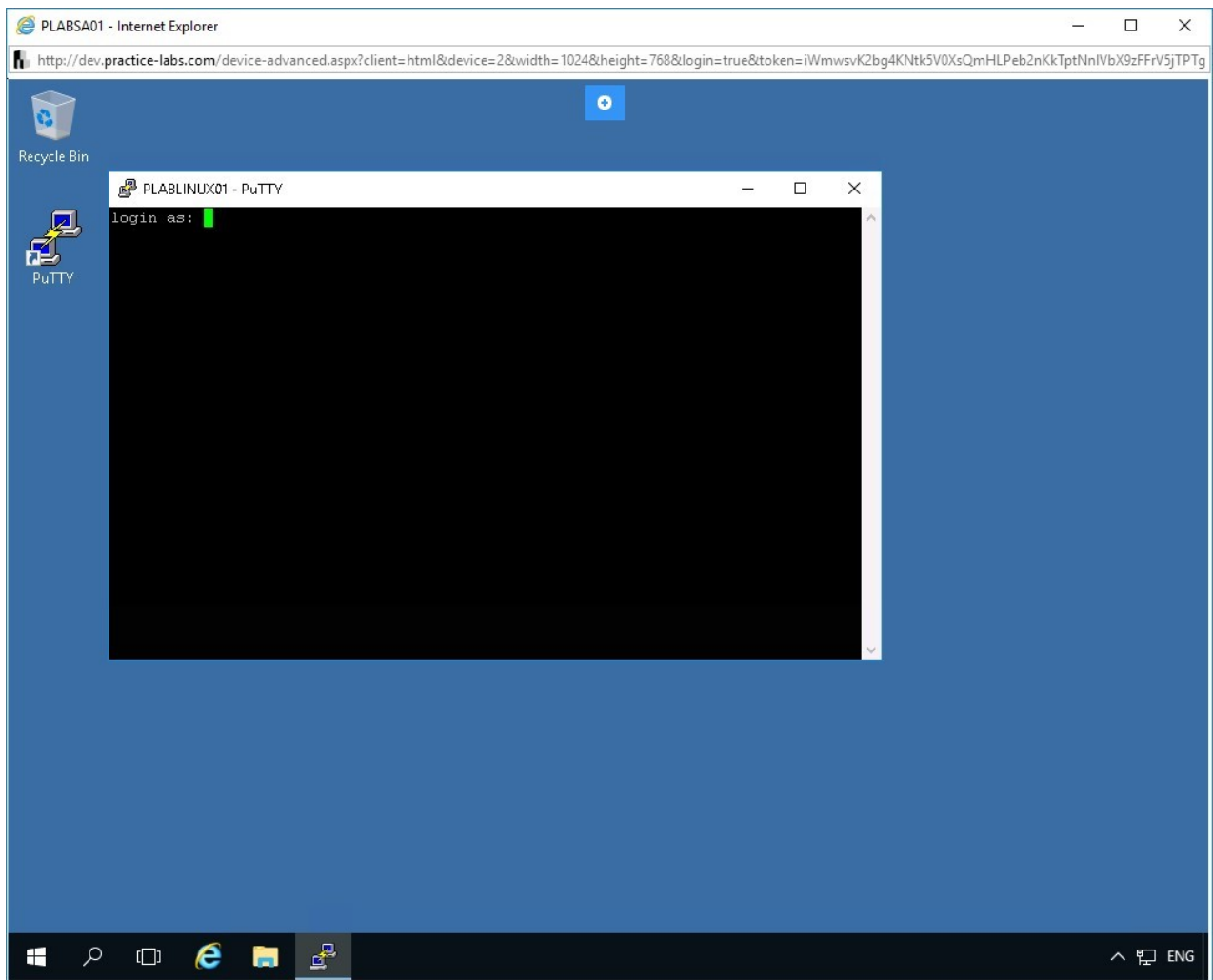


Figure 1.15 Screenshot of PLABSA01: Displaying the SSH session window.

Step 6

On the login screen, enter **root** as the login ID.

Press **Enter**.

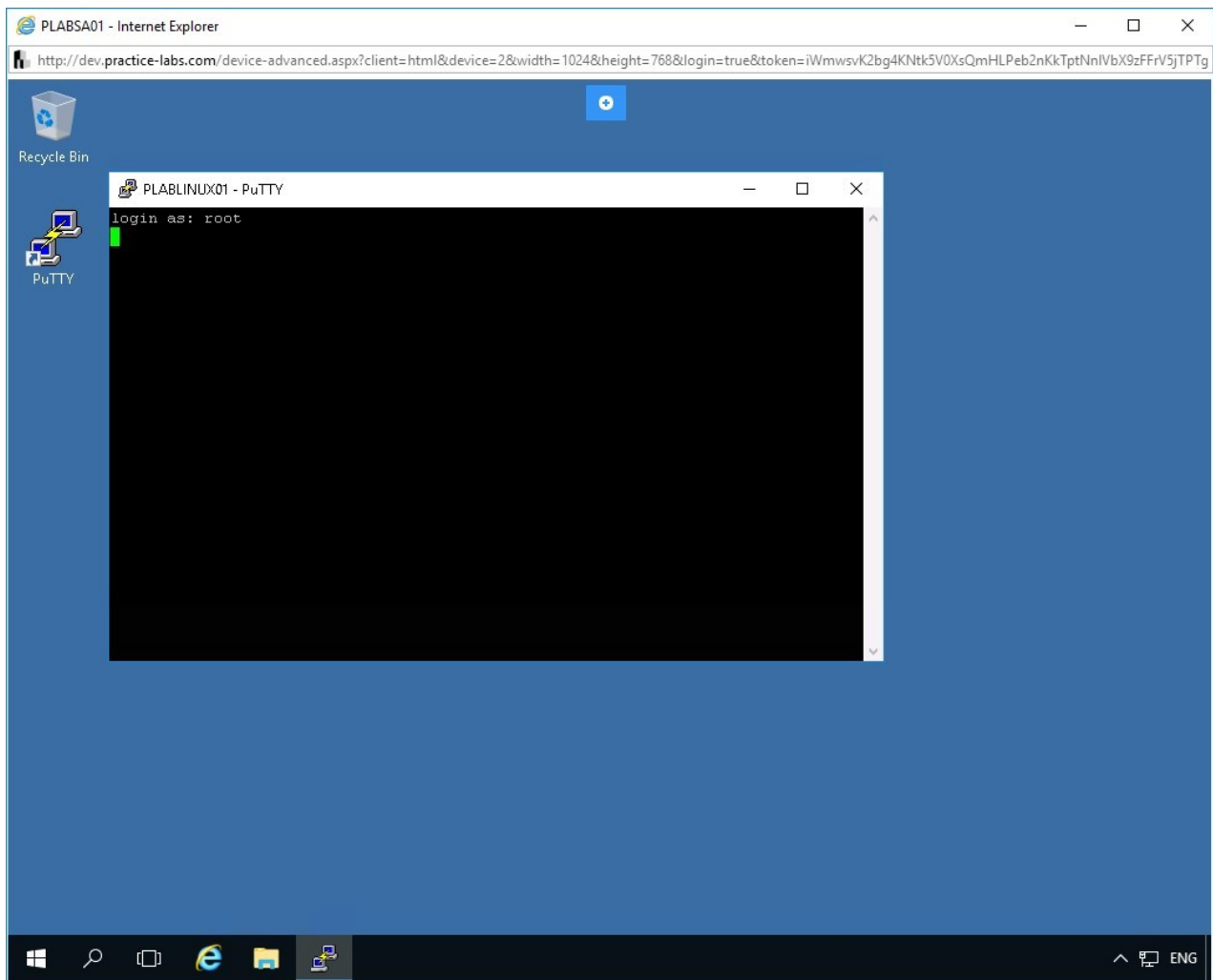


Figure 1.16 Screenshot of PLABSA01: Entering root login ID at the login prompt.

Step 7

Wait for a couple of seconds to let the **root@PLABLINUX01** password prompt appear.

On the prompt, enter **Password**.

Press **Enter**.

Note: Unlike Windows, the username is case-sensitive on Linux systems. Also, the password field does not show any characters, so input the password above and press enter.

You have successfully logged into the **PLABLINUX01** system.

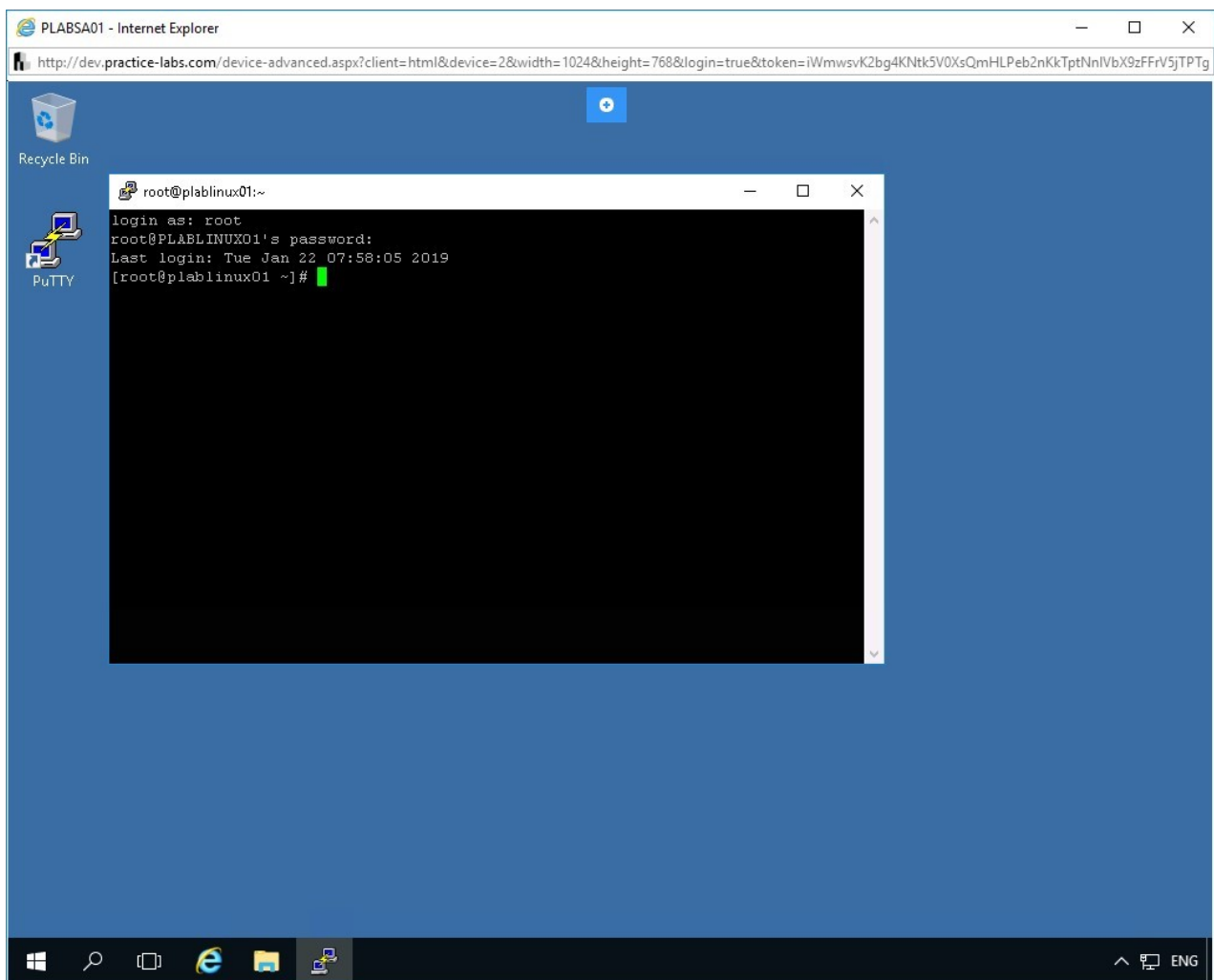


Figure 1.17 Screenshot of PLABSA01: Entering and re-entering the password.

Task 4 - Secure the OpenSSH Server

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**.

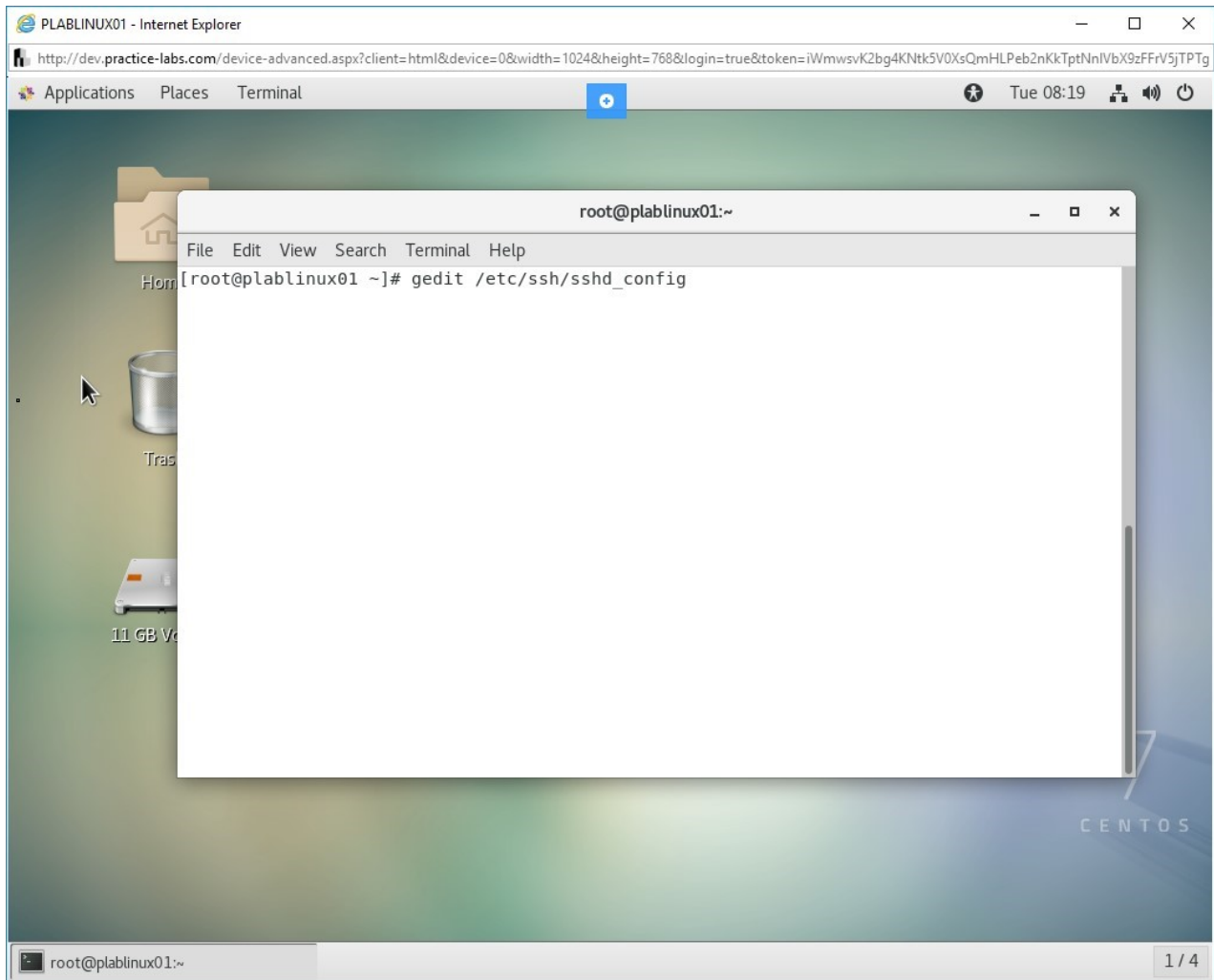
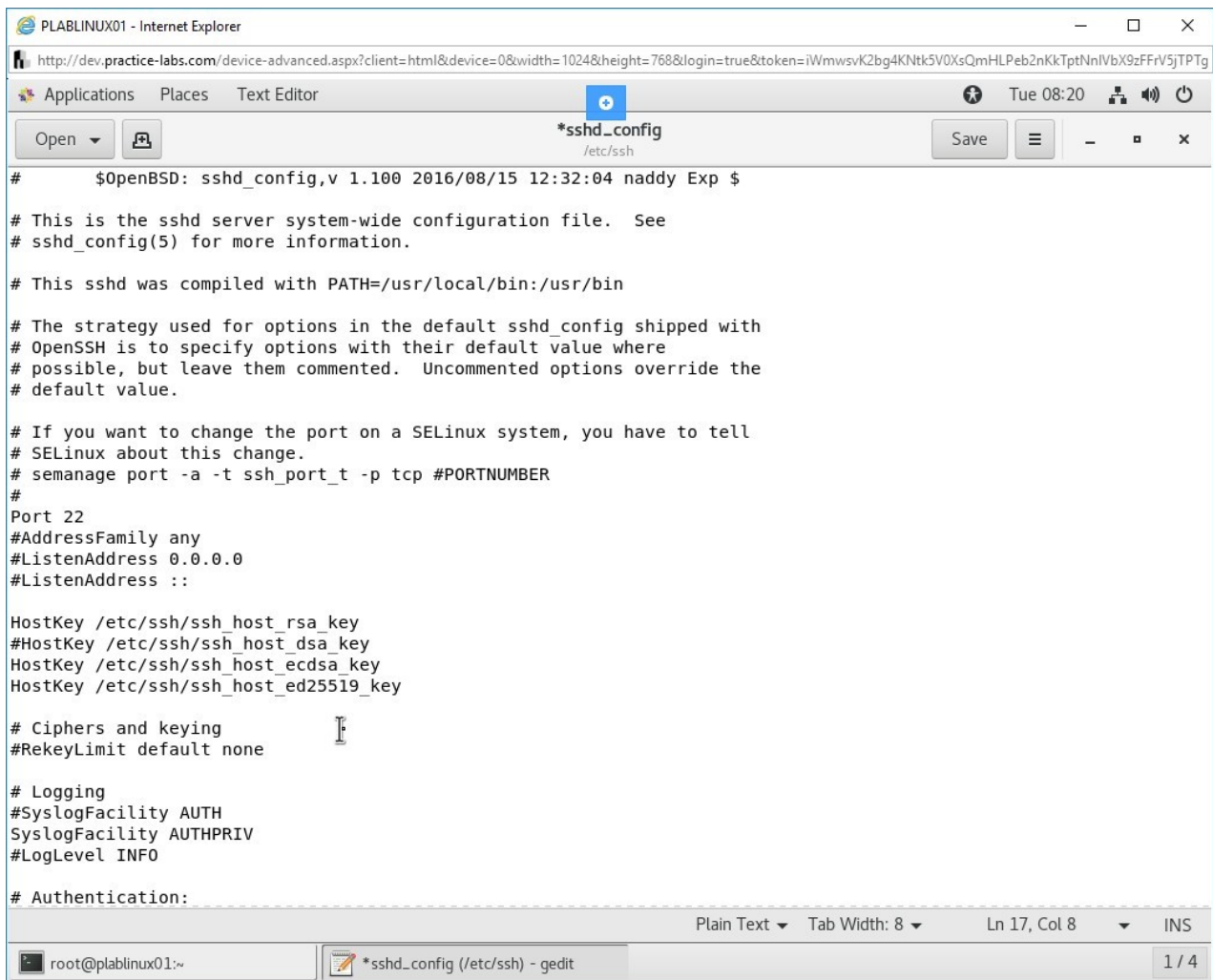


Figure 1.18 Screenshot of PLABLINUX01: Opening the **/etc/ssh/sshd_config** file.

Step 2

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

A screenshot of a web browser window titled 'PLABLINUX01 - Internet Explorer'. The address bar shows a URL from 'dev.practice-labs.com'. The browser has tabs for 'Applications', 'Places', and 'Text Editor'. The active tab is a text editor showing the file '*sshd_config' located at '/etc/ssh'. The editor contains the default OpenSSH configuration file content, including comments about the file's purpose, compilation path, and various settings like 'Port 22', 'HostKey', 'Ciphers', 'Logging', and 'Authentication'. The status bar at the bottom indicates 'root@plablinux01:~' and the file is being edited with 'gedit'.

```
# $OpenBSD: sshd_config,v 1.100 2016/08/15 12:32:04 naddy Exp $

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/bin:/usr/bin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.

# If you want to change the port on a SELinux system, you have to tell
# SELinux about this change.
# semanage port -a -t ssh_port_t -p tcp #PORTNUMBER
#
Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_dsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key
HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
SyslogFacility AUTHPRIV
#LogLevel INFO

# Authentication:
```

Figure 1.19 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 #.

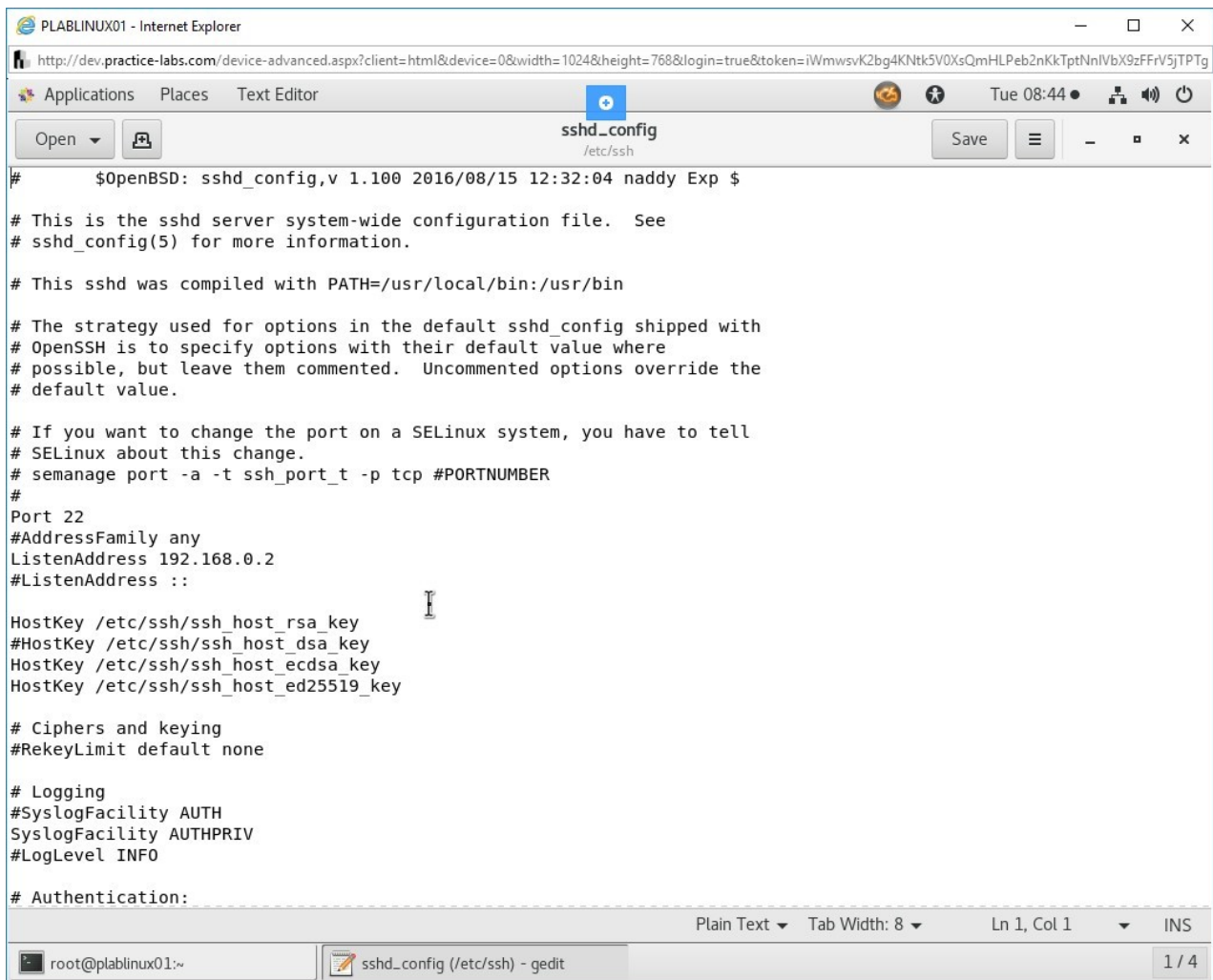
Change the following:

From:

```
#PermitRootLogin yes
```

To:

```
PermitRootLogin no
```

A screenshot of a web browser window titled 'PLABLINUX01 - Internet Explorer'. The address bar shows a URL from 'dev.practice-labs.com'. The browser has tabs for 'Applications', 'Places', and 'Text Editor'. The active tab is 'sshd_config (/etc/ssh)', which is open in a text editor. The text editor shows the contents of the '/etc/ssh/sshd_config' file. The file contains various configuration options for the SSH daemon, including comments, port settings, host keys, ciphers, logging, and authentication. The text is as follows:

```
# $OpenBSD: sshd_config,v 1.100 2016/08/15 12:32:04 naddy Exp $

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/bin:/usr/bin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.

# If you want to change the port on a SELinux system, you have to tell
# SELinux about this change.
# semanage port -a -t ssh_port_t -p tcp #PORTNUMBER
#
Port 22
#AddressFamily any
ListenAddress 192.168.0.2
#ListenAddress ::

HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_dsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key
HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
SyslogFacility AUTHPRIV
#LogLevel INFO

# Authentication:
```

The text editor interface includes a status bar at the bottom showing 'root@plablinux01:~', the file name 'sshd_config (/etc/ssh) - gedit', and the line/col indicator '1 / 4'. The browser's status bar at the very bottom shows 'Plain Text', 'Tab Width: 8', 'Ln 1, Col 1', and 'INS'.

Figure 1.20 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.

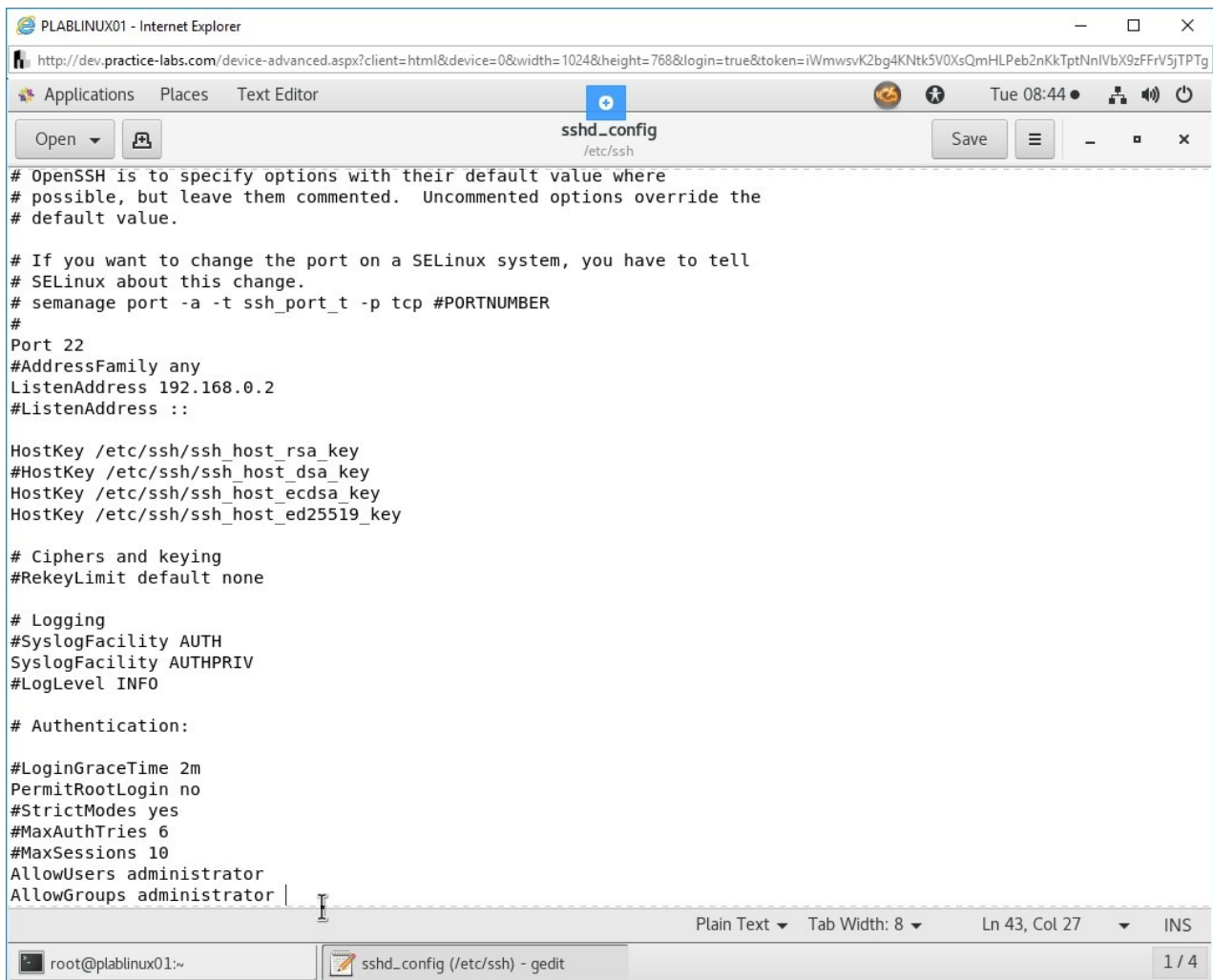


Figure 1.21 Screenshot of PLABLINUX01: Making changes to the /etc/ssh/sshd_config file.

Step 5

You can also configure the OpenSSH Server to listen to one or more interfaces. If the system has more than one interface, one for the Internet and one for the intranet, then you should disable SSH on the Internet interface. You can restrict the interfaces from which SSH should listen.

Change the following:

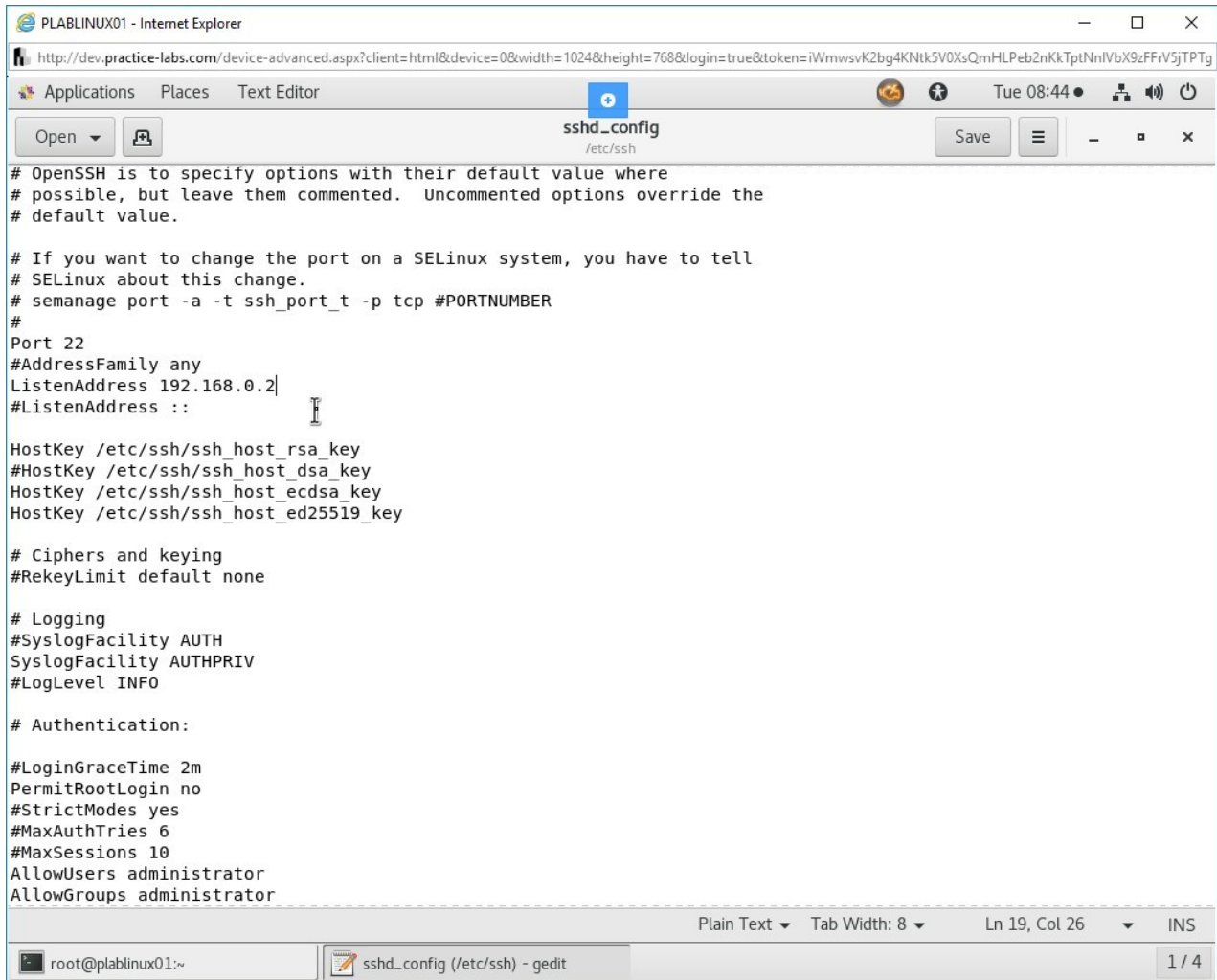
From:

```
#ListenAddress 0.0.0.0
```

To:

ListenAddress 192.168.0.2

You have configured the OpenSSH Server to listen from one IP address only.



The screenshot shows a web browser window titled 'PLABLINUX01 - Internet Explorer'. The address bar displays a URL from 'dev.practice-labs.com'. The browser's top menu bar includes 'Applications', 'Places', and 'Text Editor'. Below the menu bar, there are buttons for 'Open', 'ssh_config (/etc/ssh)', and 'Save'. The main content area shows the text of the '/etc/ssh/sshd_config' file. The file contains various configuration options for the SSH daemon, including port settings, host keys, ciphers, logging, and authentication. The 'ListenAddress 192.168.0.2' line is highlighted. The bottom status bar shows 'root@plablinux01:~' and 'ssh_config (/etc/ssh) - gedit'.

```
# OpenSSH is to specify options with their default value where
# possible, but leave them commented. Uncommented options override the
# default value.

# If you want to change the port on a SELinux system, you have to tell
# SELinux about this change.
# semanage port -a -t ssh_port_t -p tcp #PORTNUMBER
#
Port 22
#AddressFamily any
ListenAddress 192.168.0.2
#ListenAddress ::

HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_dsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key
HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
SyslogFacility AUTHPRIV
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
AllowUsers administrator
AllowGroups administrator
```

Figure 1.22 Screenshot of PLABLINUX01: Making changes to the /etc/ssh/sshd_config file.

Step 6

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

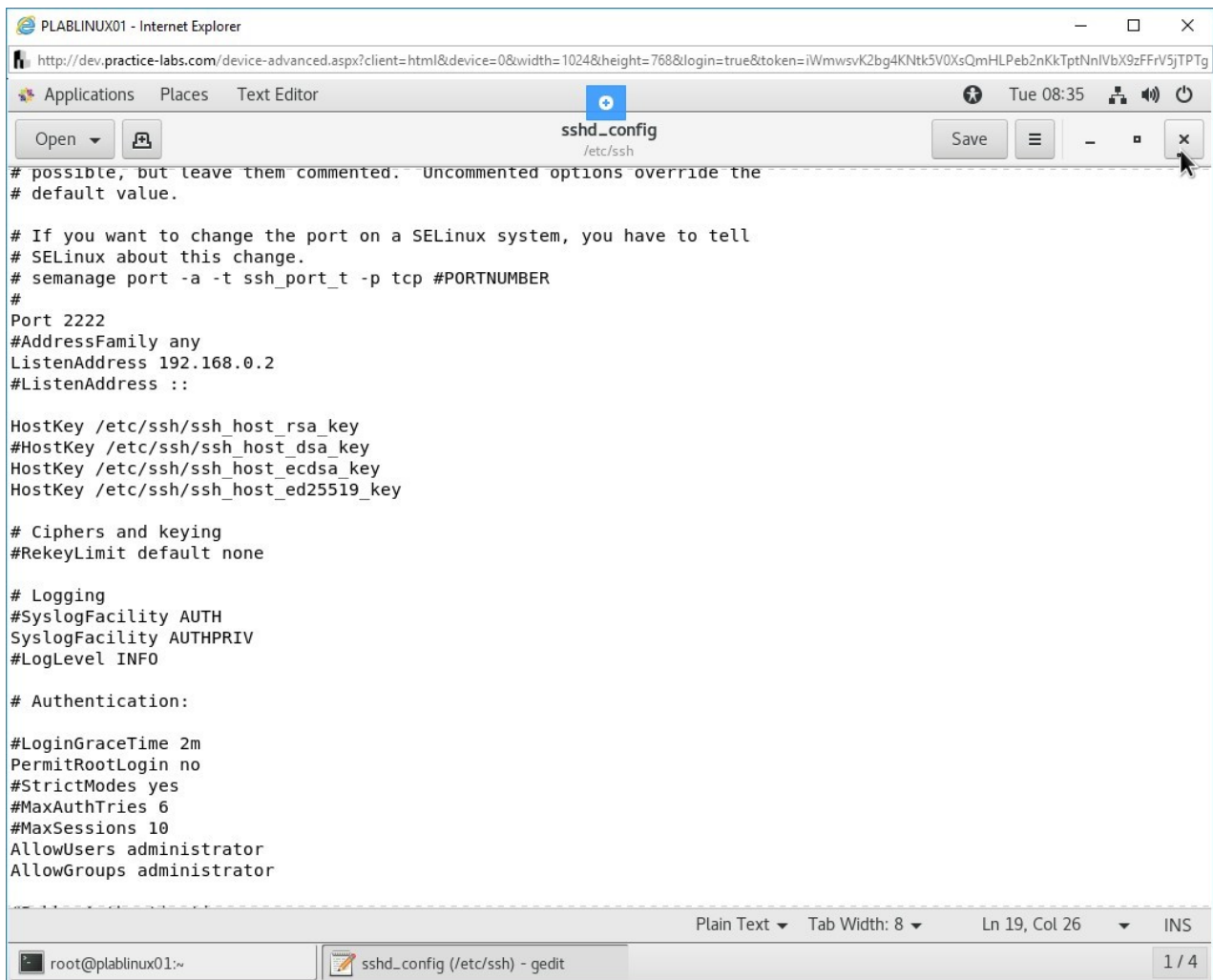


Figure 1.23 Screenshot of PLABLINUX01: Saving and closing the /etc/ssh/sshd_config file.

Step 7

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

```
systemctl restart sshd
```

Press **Enter**.

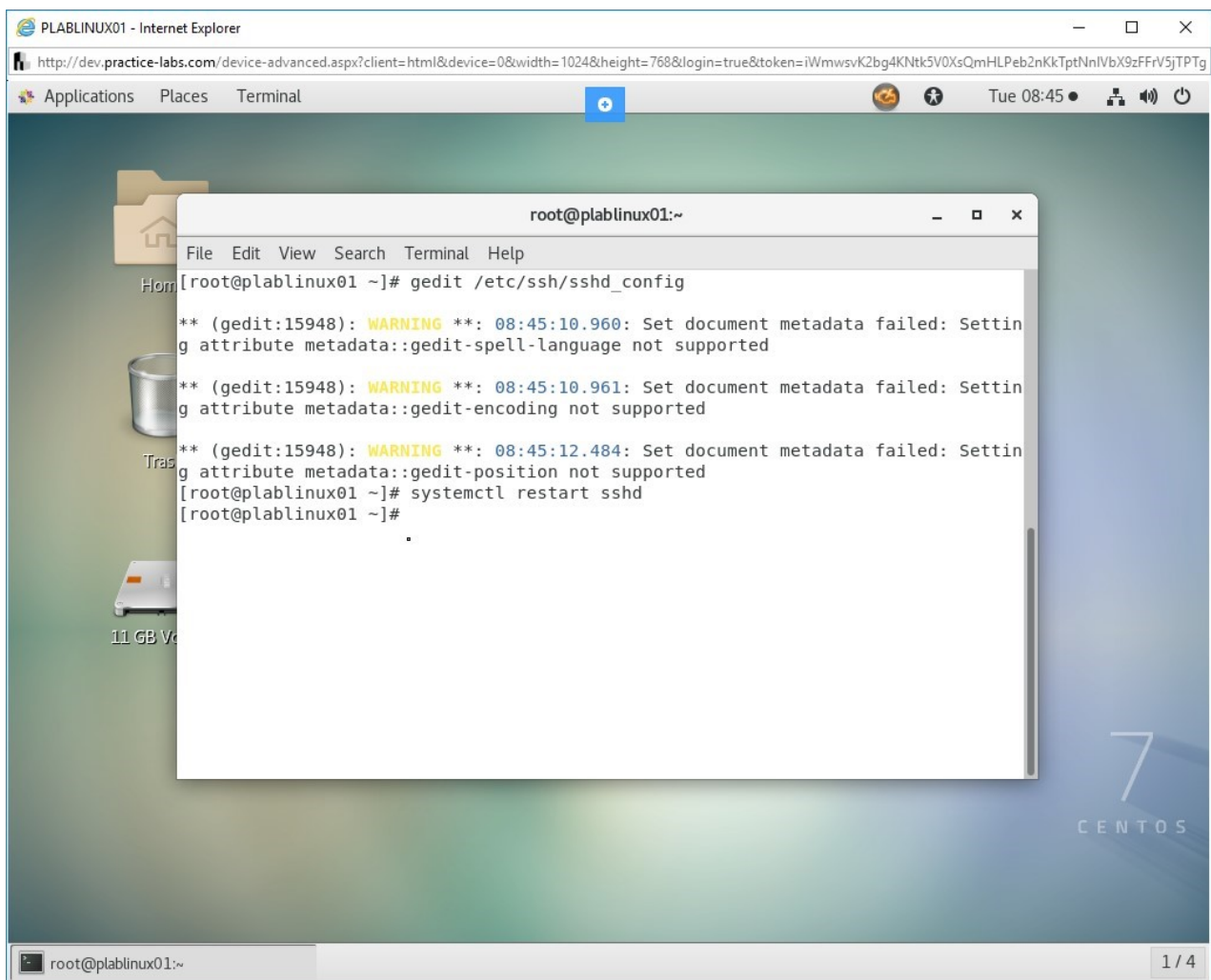


Figure 1.24 Screenshot of PLABLINUX01: Restarting the sshd service.

Step 8

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

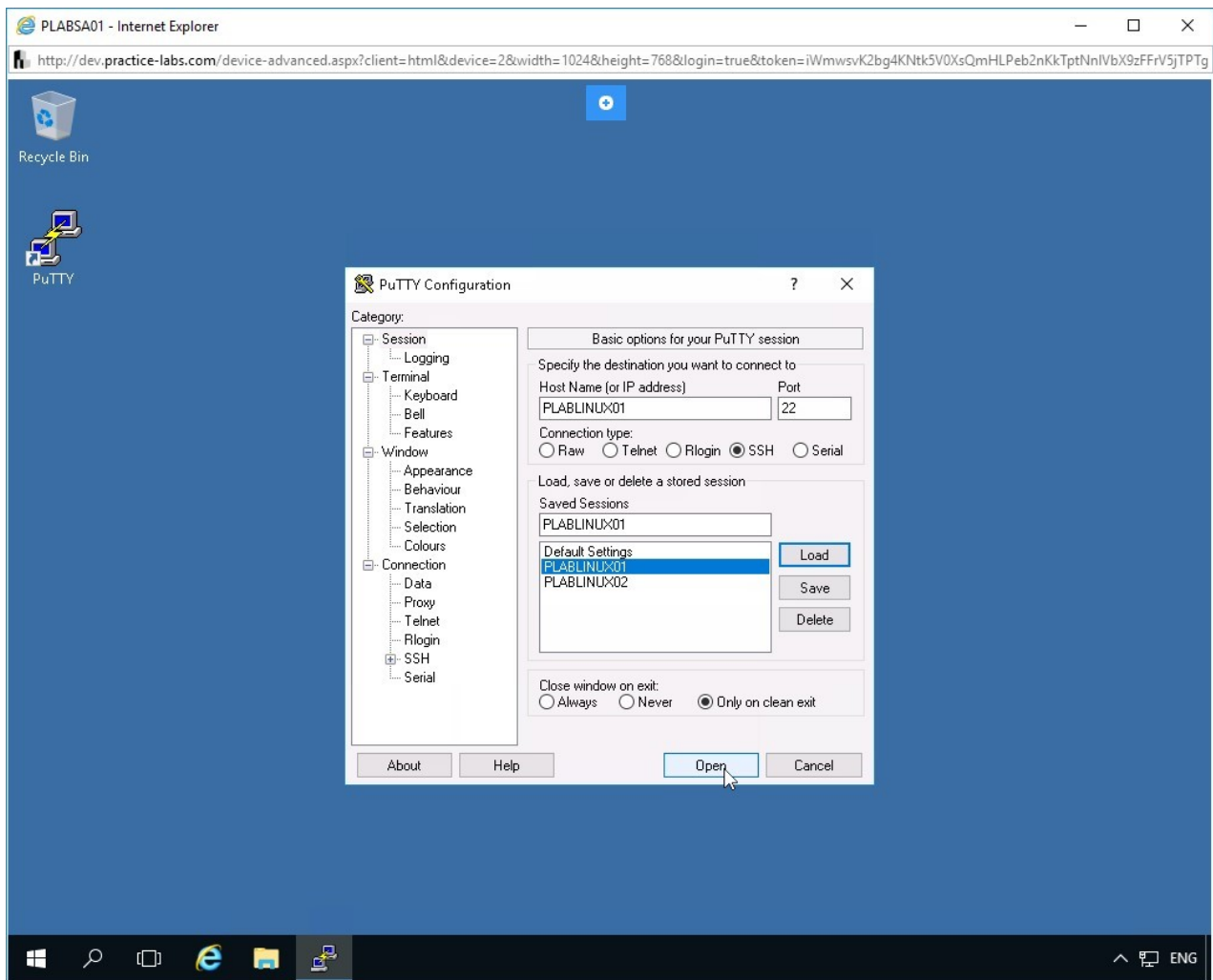


Figure 1.25 Screenshot of PLABSA01: Loading required configuration in the PutTTY window.

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.

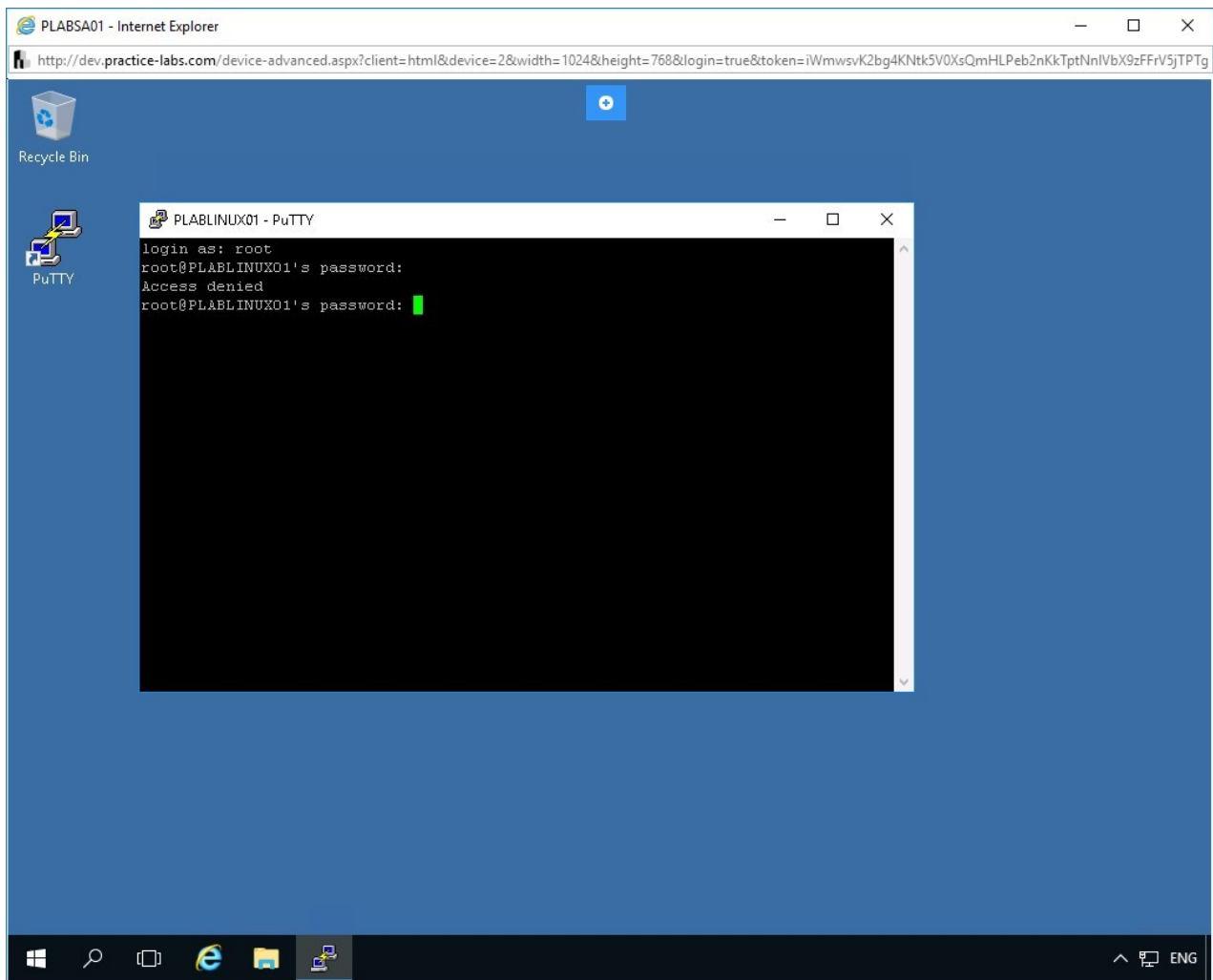


Figure 1.26 Screenshot of PLABINUX01: Showing the access denied message after entering the credentials.

Close the session window. Launch putty again. Load the **PLABINUX01** session. When prompted for the login, use the following credentials:

login as:

administrator

Password:

Passw0rd

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

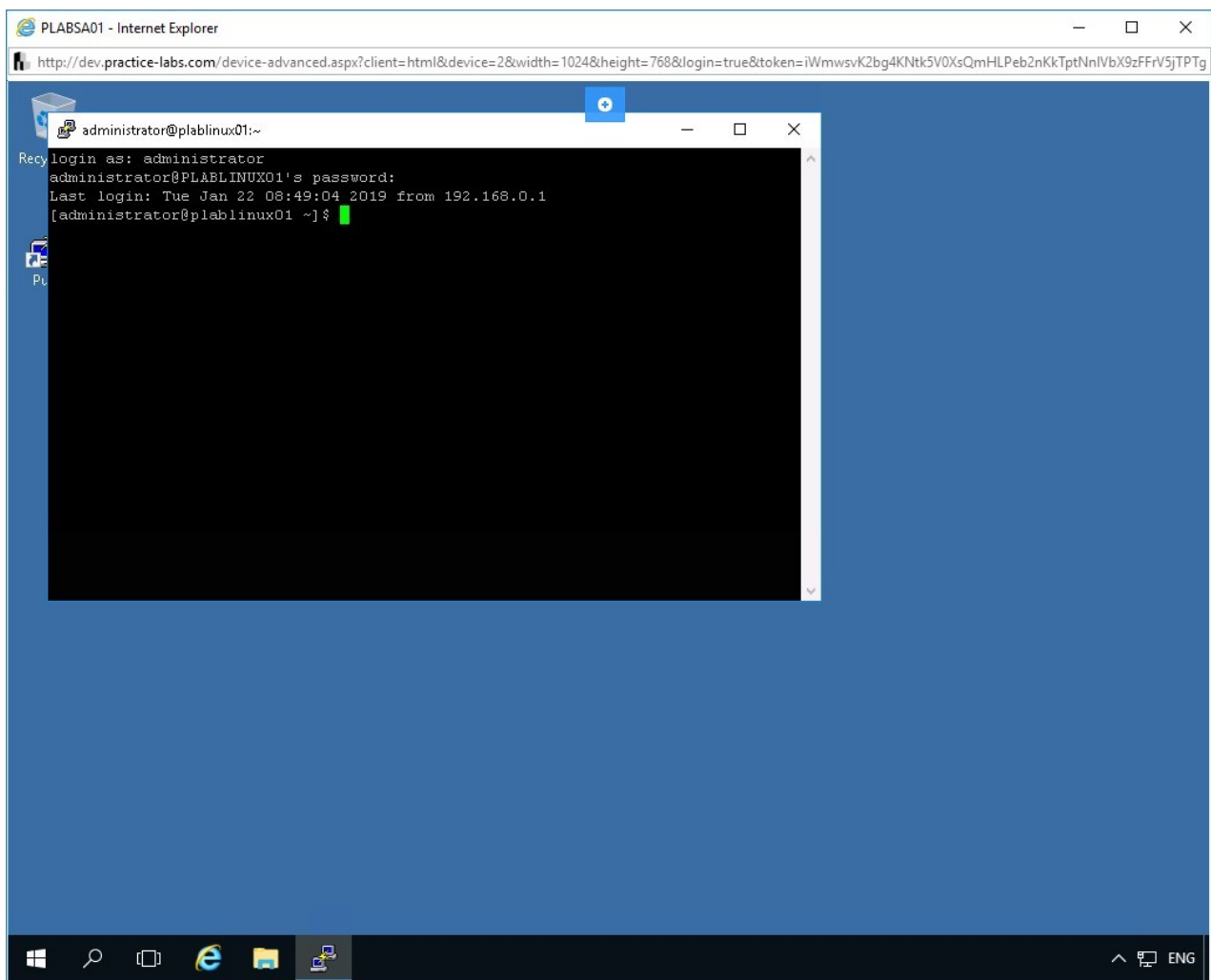


Figure 1.30 Screenshot of PLABINUX01: Showing a successful connection after entering the credentials.

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

Review

Well done, you have completed the **Secure Communication using SSH** Practice Lab.

Summary

You completed the following exercises:

- Exercise 1 - Secure Communication using SSH

You should now be able to:

- Configure Network on CentOS
- Perform Basic Configuration for the OpenSSH Server
- Connect with the OpenSSH Server

Feedback

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