CompTIA Linux+

Configure UFW and DenyHosts

Introduction

Welcome to the **Configure UFW and DenyHosts** Practice Lab. In this module you will be provided with the instructions and devices needed to develop your hands-on skills.

UFW
DenyHosts
ICMP
Ubuntu
CentOS

Learning Outcomes

In this module, you will complete the following exercises:

- Exercise 1 - Install and Configure UFW
- Exercise 2 - Install and Configure DenyHosts

After completing this lab, you will be able to:

- Configure Network on CentOS
- Install UFW
- Set UFW Default Policy
- Configure Advanced UFW Rules
- Block ICMP Requests
- Reset UFW

- Configure Network on Ubuntu
- Install and Configure DenyHosts

Exam Objectives

The following exam objectives are covered in this lab:

- **LPI:** 110.1 Perform security administration tasks
- **CompTIA:** 3.5 Given a scenario, implement and configure Linux firewalls.

> ***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.

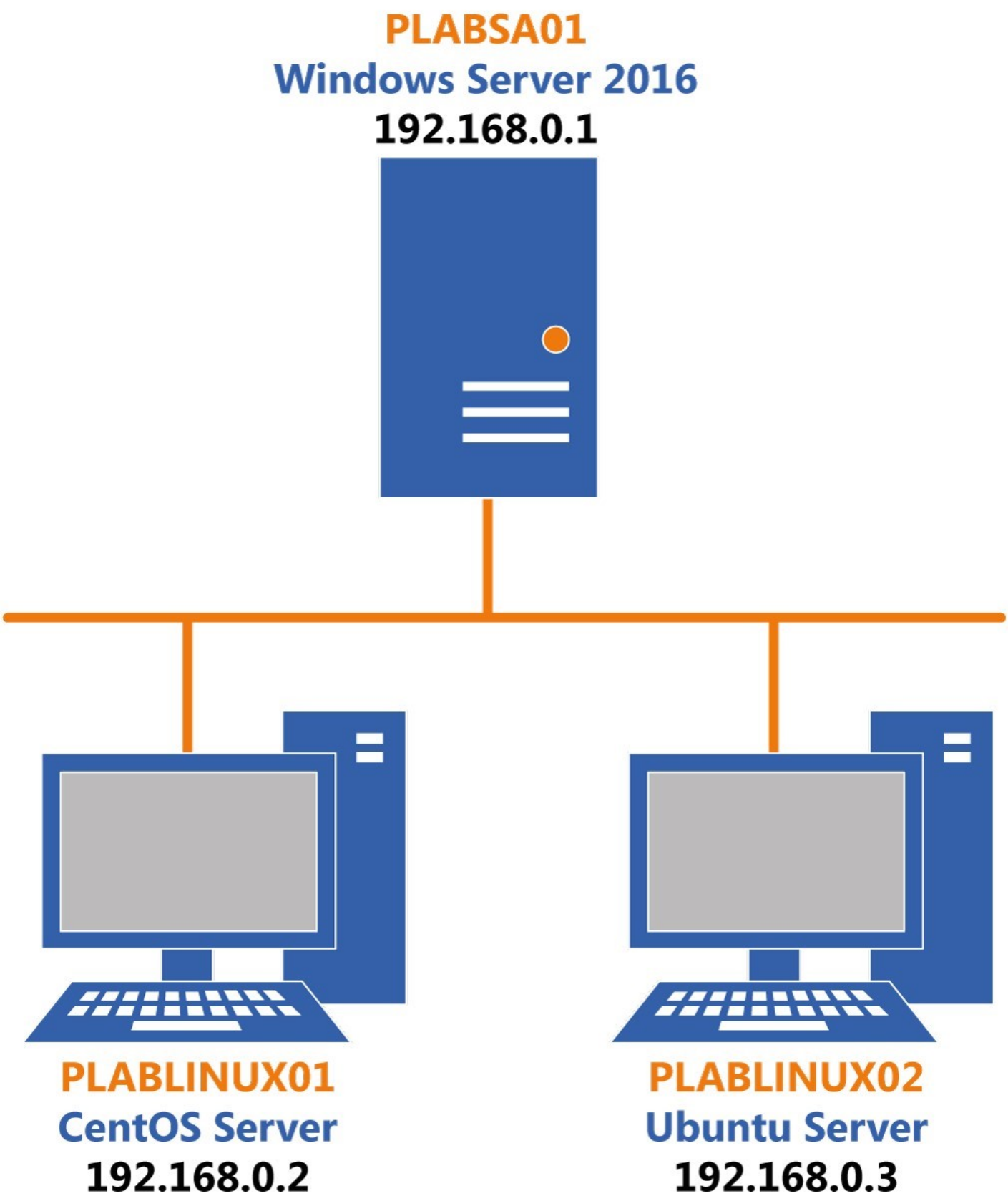
Help and Support

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 - Install and Configure UFW

UFW originated from Ubuntu, and it provides an interface to iptables, which is a host-based firewall. It is also known as Uncomplicated Firewall, which means that the users who are not familiar with the firewall concepts can still use it.

In this exercise, you will learn to install and configure UFW.

Learning Outcomes

After completing this exercise, you will be able to:

- Log into a Linux System
- Configure Network on CentOS
- Install UFW
- Set UFW Default Policy
- Configure Advanced UFW Rules
- Block ICMP Requests
- Reset UFW

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**.

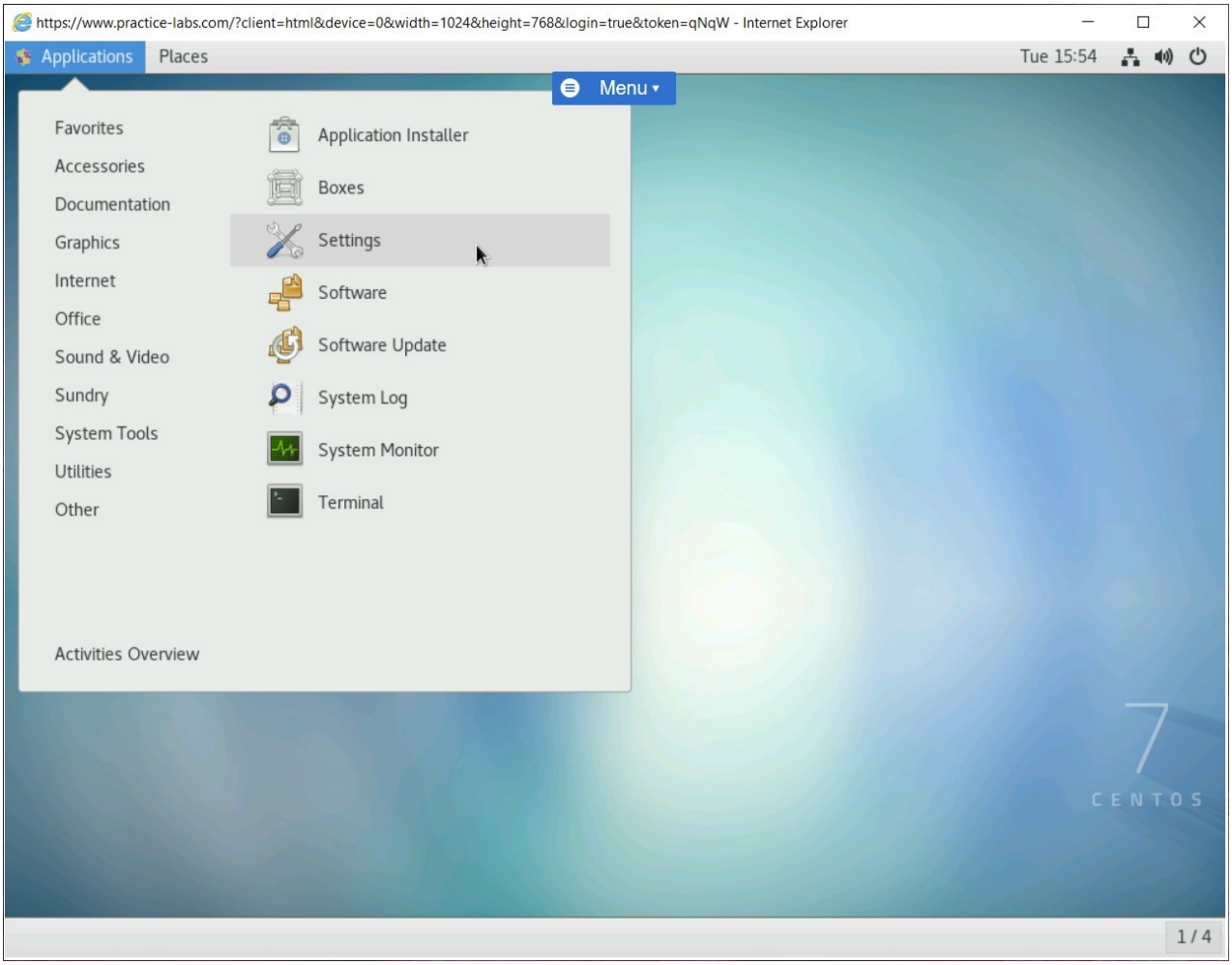


Figure 1.1 Screenshot of PLABLINUX01: Selecting the Settings option from the Applications > System Tools menu.

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 your wired connection is being shown as* ***OFF*** *then click the switch on the left of* ***OFF*** *to switch it to* ***ON.***

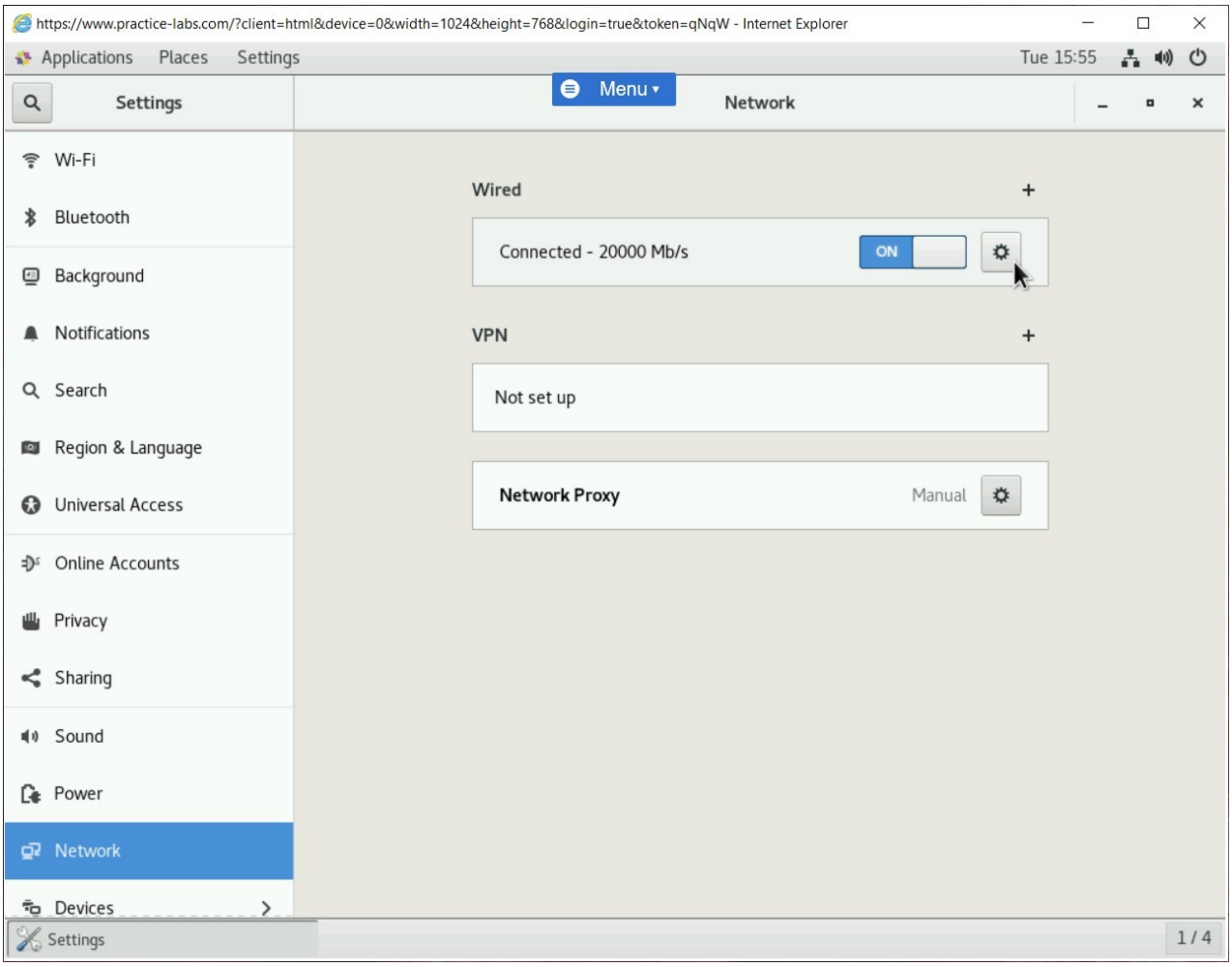


Figure 1.2 Screenshot of PLABLINUX01: Clicking the button to invoke the Wired dialog box.

Step 3

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

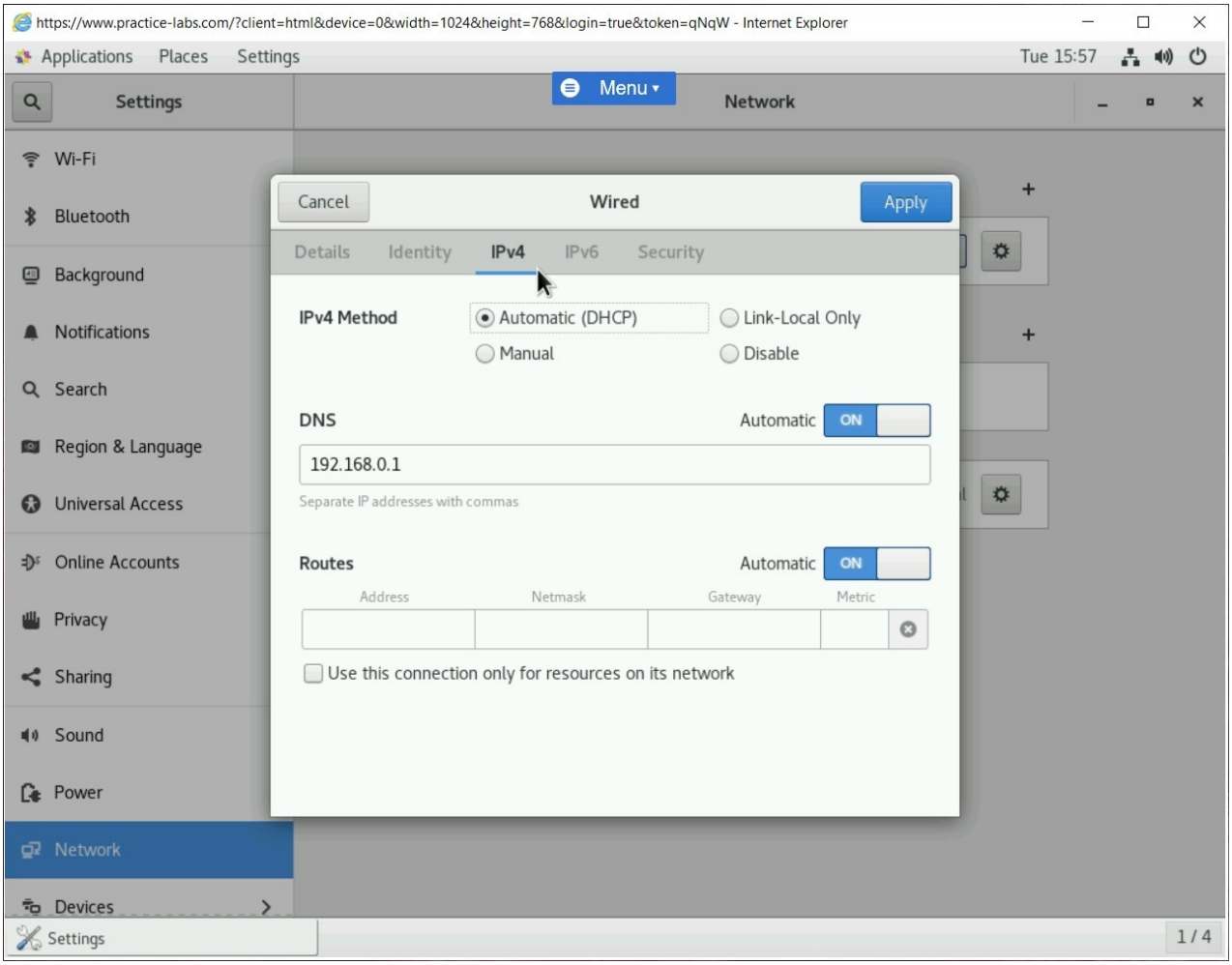


Figure 1.3 Screenshot of PLABLINUX01: Selecting the IPv4 tab in the Wired dialog box.

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**.

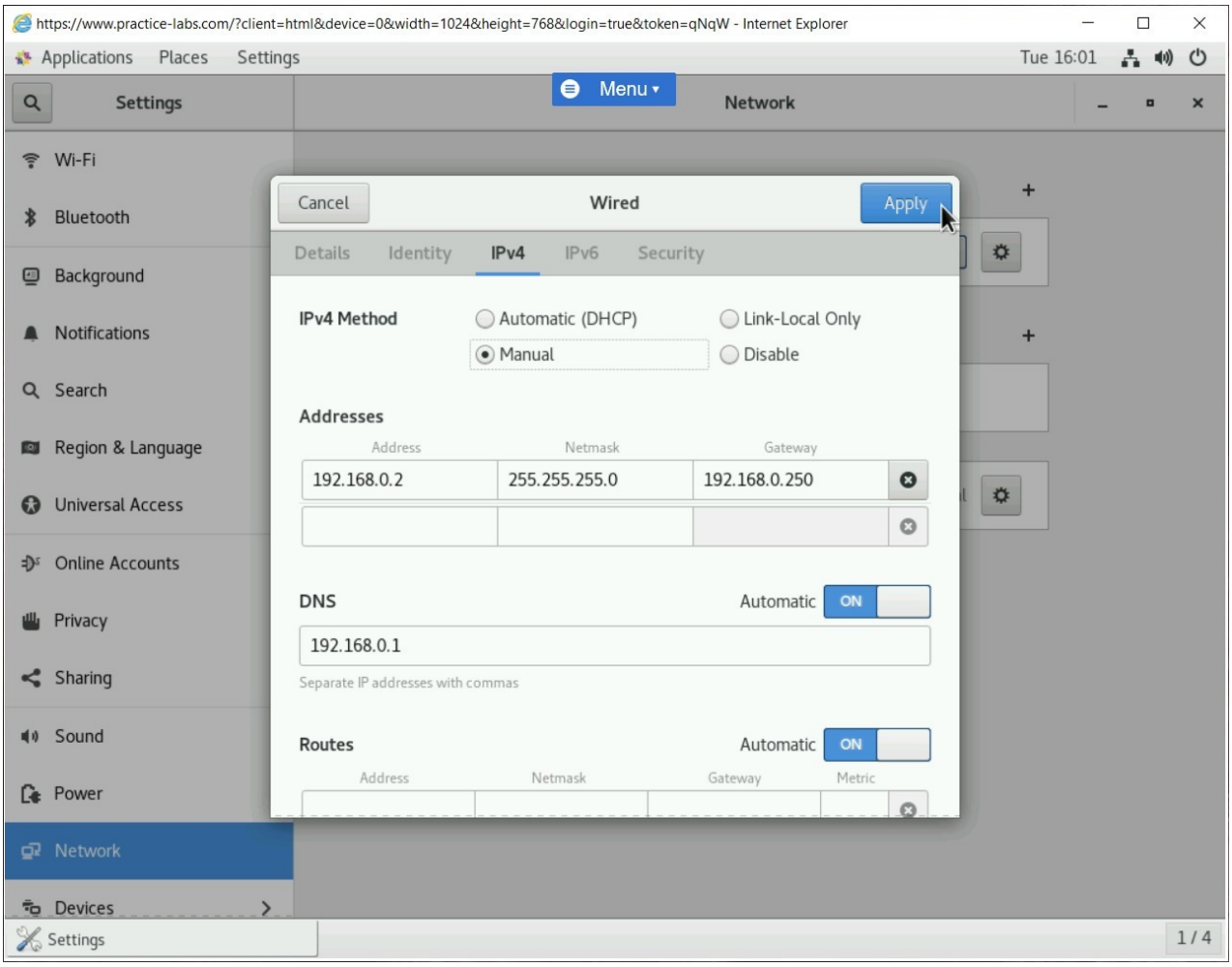


Figure 1.4 Screenshot of PLABLINUX01: Entering the network information and then clicking the Apply button.

Step 5

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

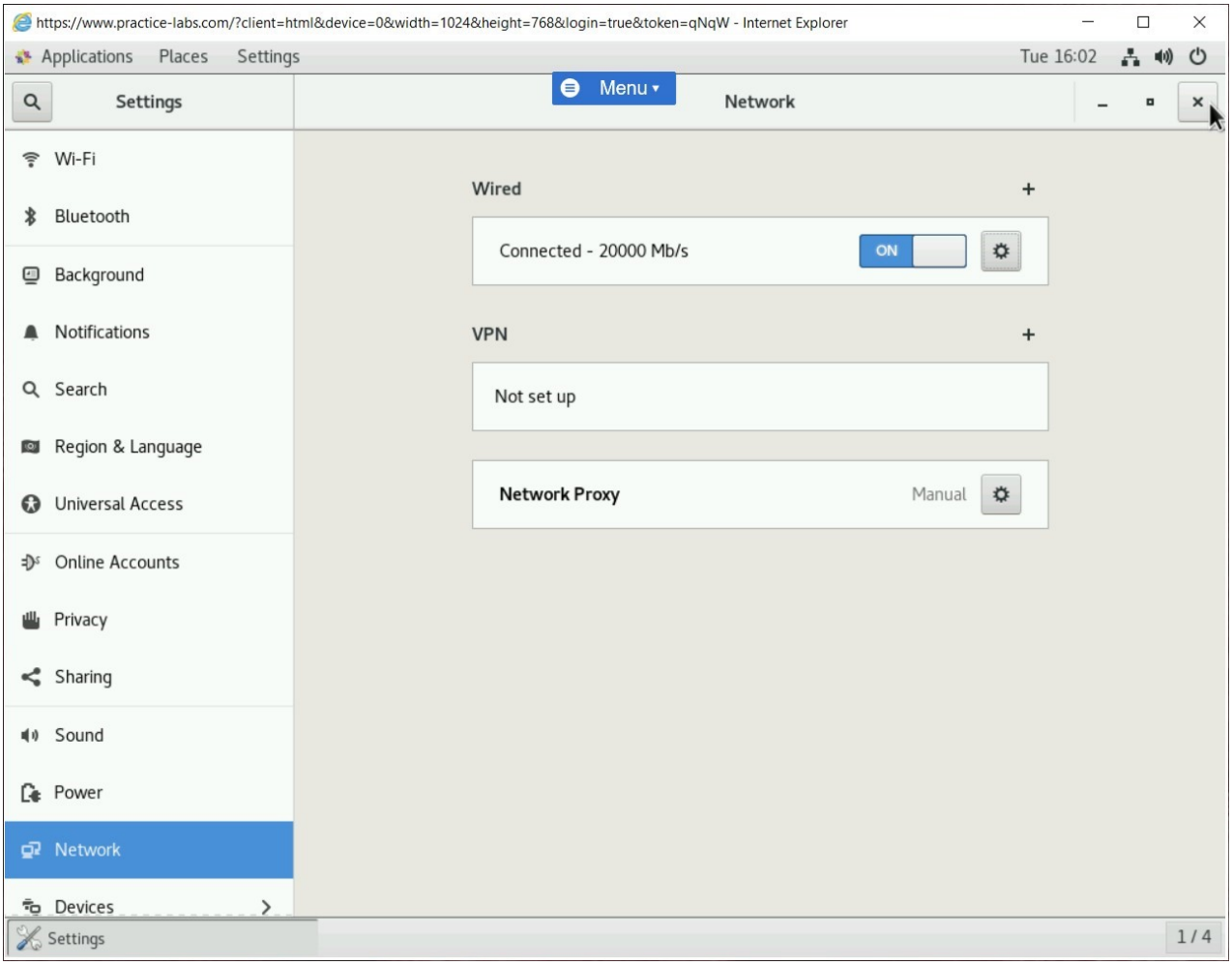


Figure 1.5 Screenshot of PLABLINUX01: Displaying the Settings window.

Task 2 - Install UFW

Before configuring UFW, you need to install it. By default, UFW does not come readily installed on CentOS.

In this task, you will learn to install UFW. To install UFW, perform the following steps:

Step 1

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

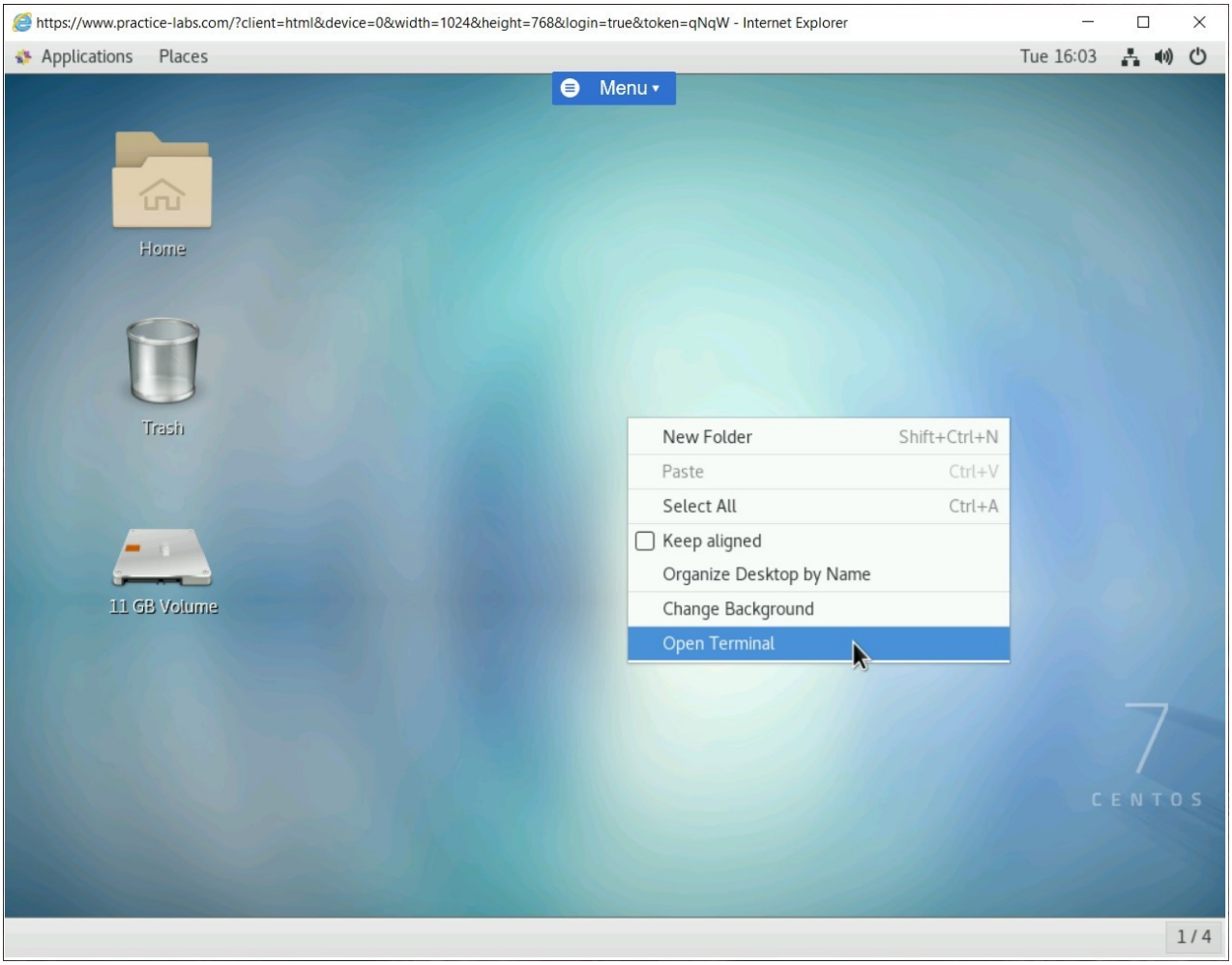


Figure 1.6 Screenshot of PLABLINUX01: Selecting the Open Terminal option from the context menu.

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**.

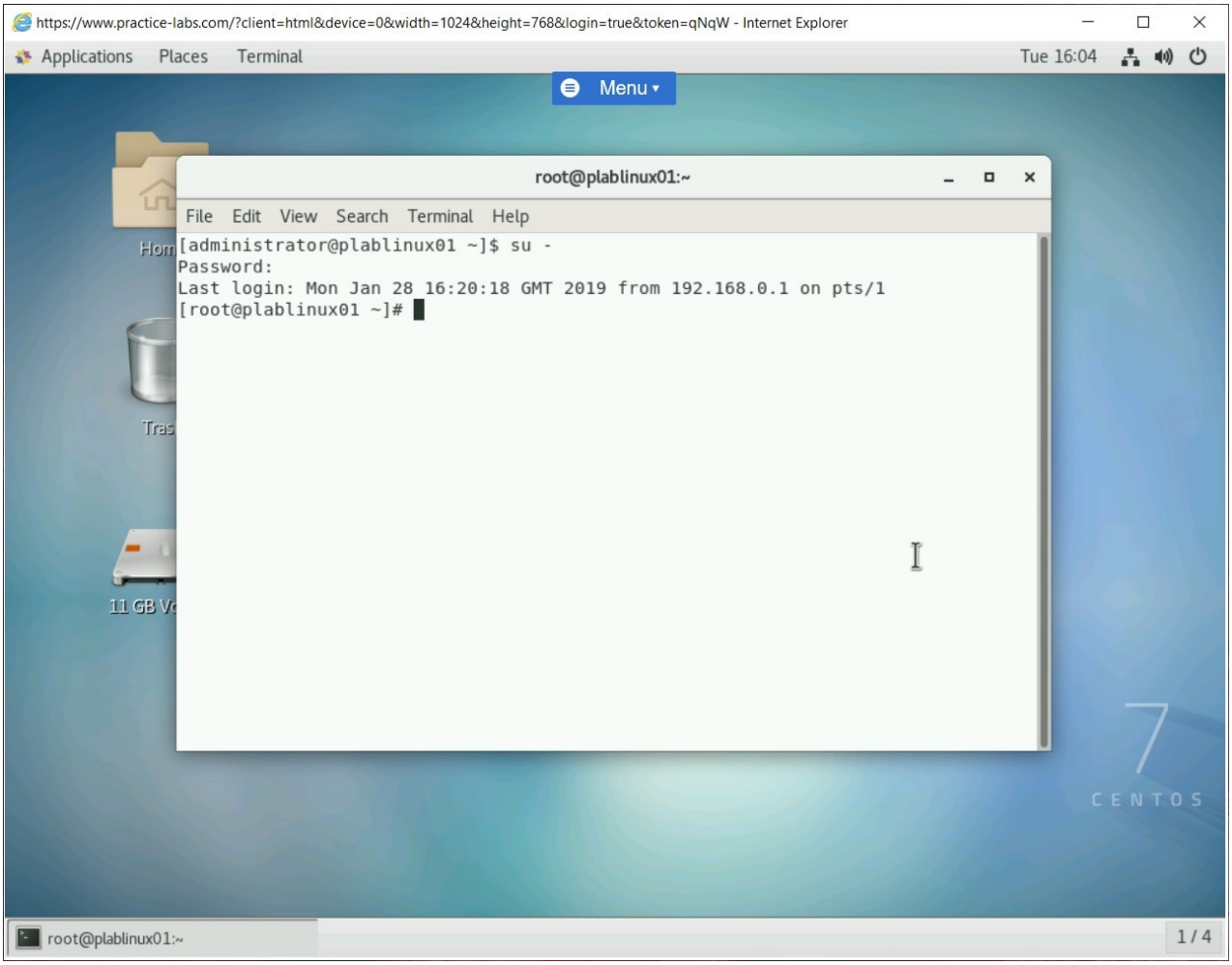


Figure 1.7 Screenshot of PLABLINUX01: Changing the account to the root account with the su command.

Step 3

Clear the screen by entering the following command:

```
clear
```

Before installing UFW, you need to add it to the CentOS repository. For this, you are required to install the **epel** repository on your system. Type the following command:

```
yum install epel-release -y
```

Press **Enter**. Notice that when you add **-y**, the installation does not require any confirmation.

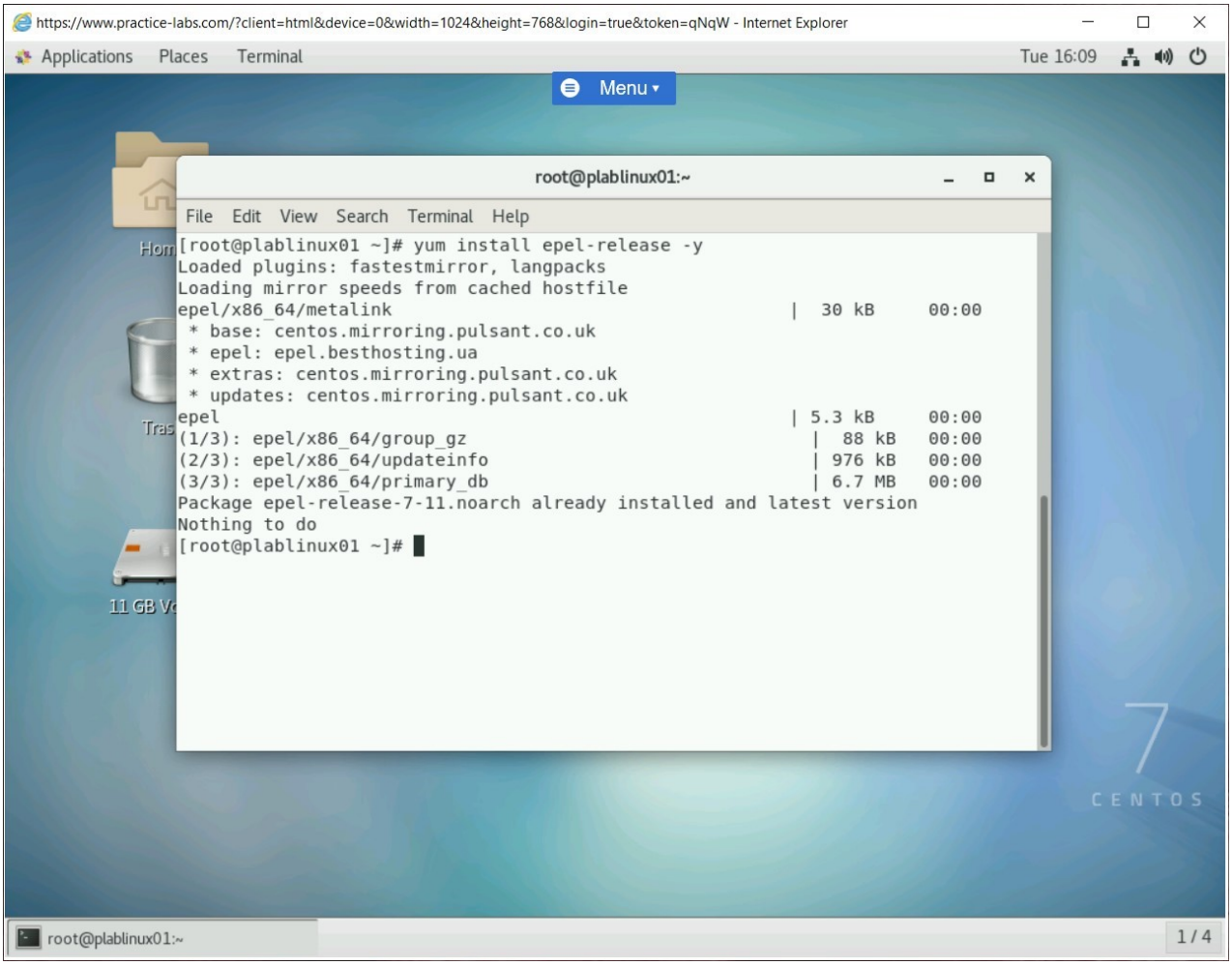


Figure 1.8 Screenshot of PLABLINUX01: Installing the epel repository.

Step 4

When the installation is complete, you will see the **Complete!** message.

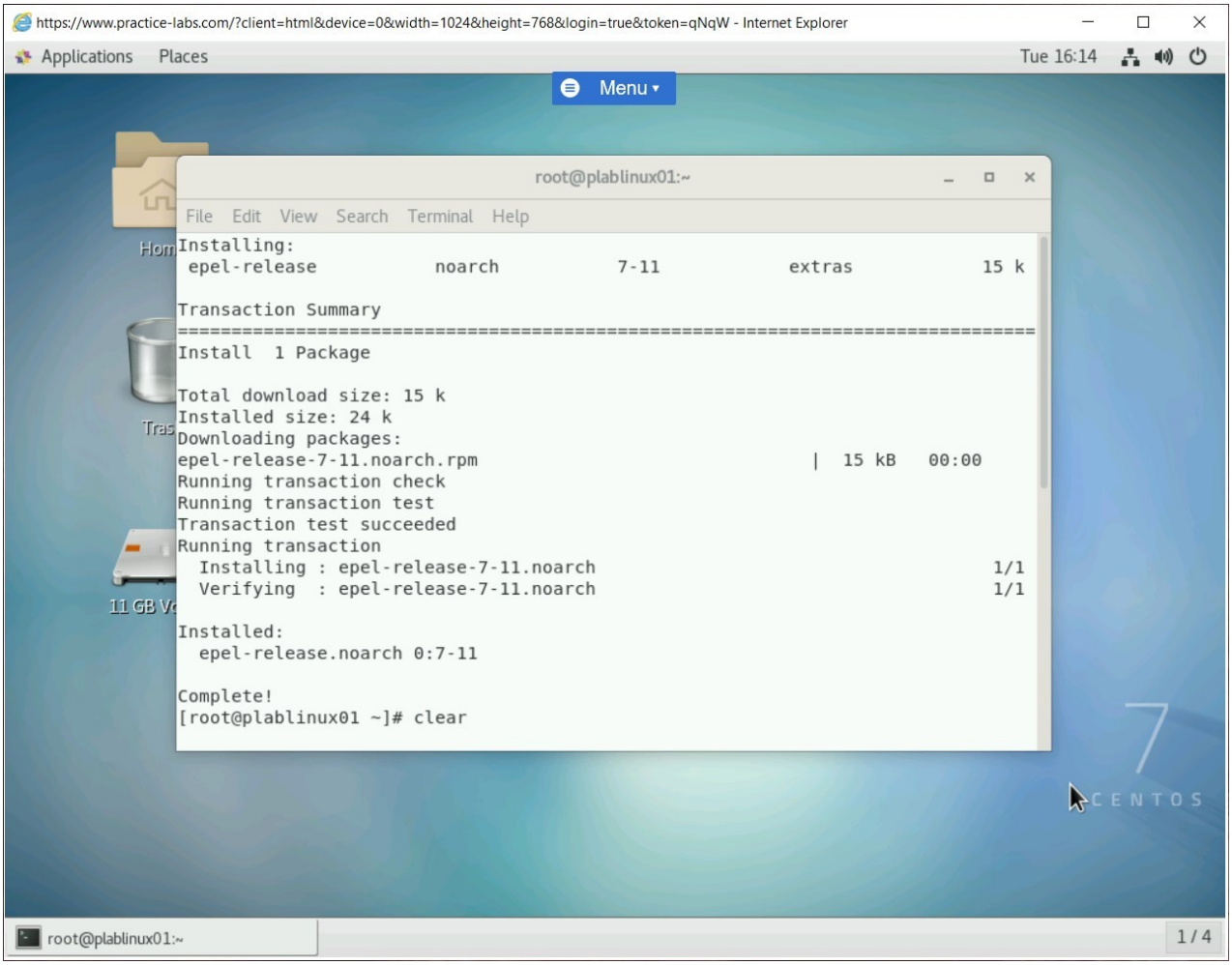


Figure 1.9 Screenshot of PLABLINUX01: Showing the installation completion of the epel repository.

Step 5

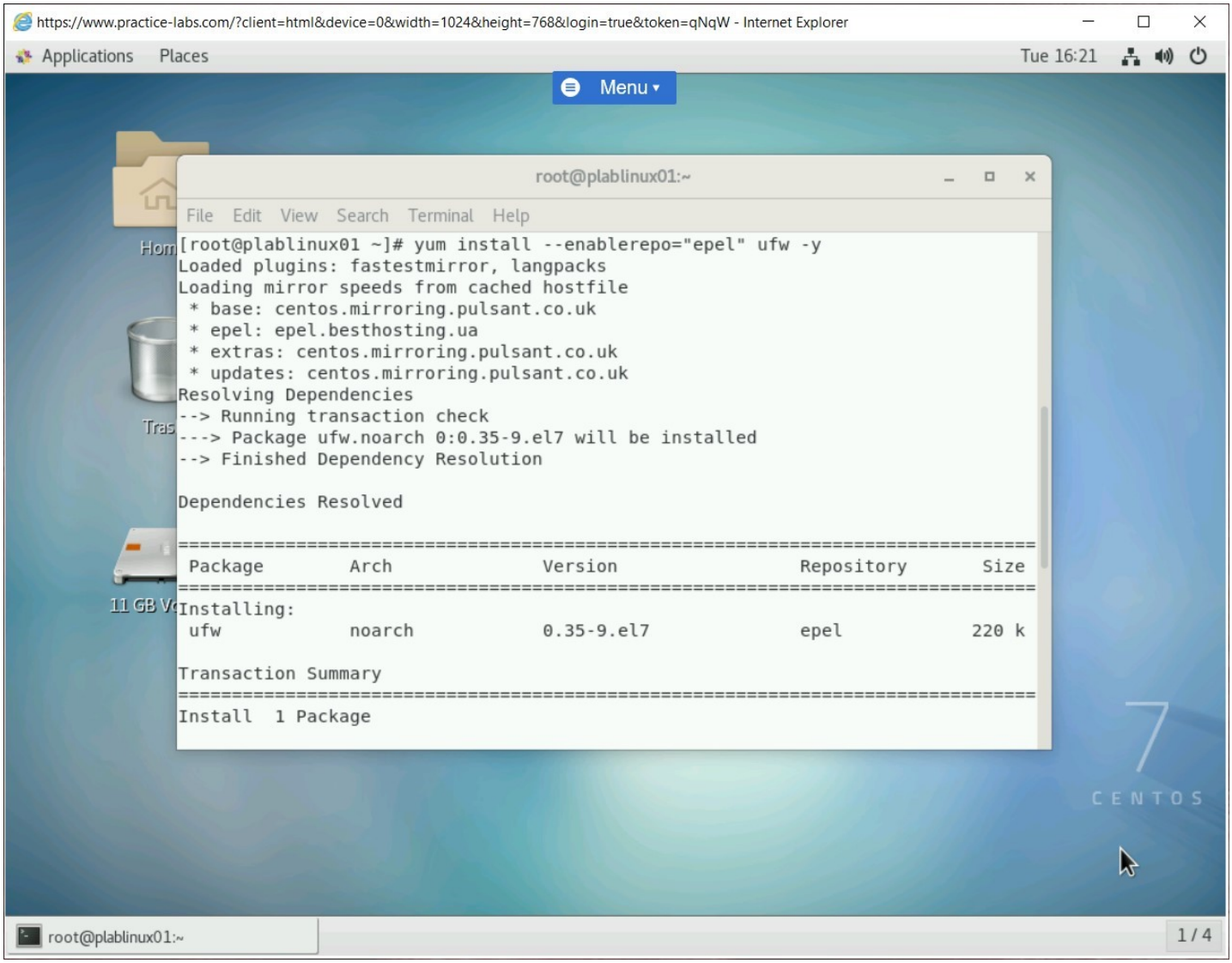
Clear the screen by entering the following command:

```
clear
```

After installing the **epel** repository, you need to install UFW now. Type the following command:

```
yum install --enablerepo="epel" ufw -y
```

Press **Enter**. Notice that you are enabling the epel repository, which will be used for UFW installation.



Step 6

When the installation is complete, you will see the **Complete!** message.

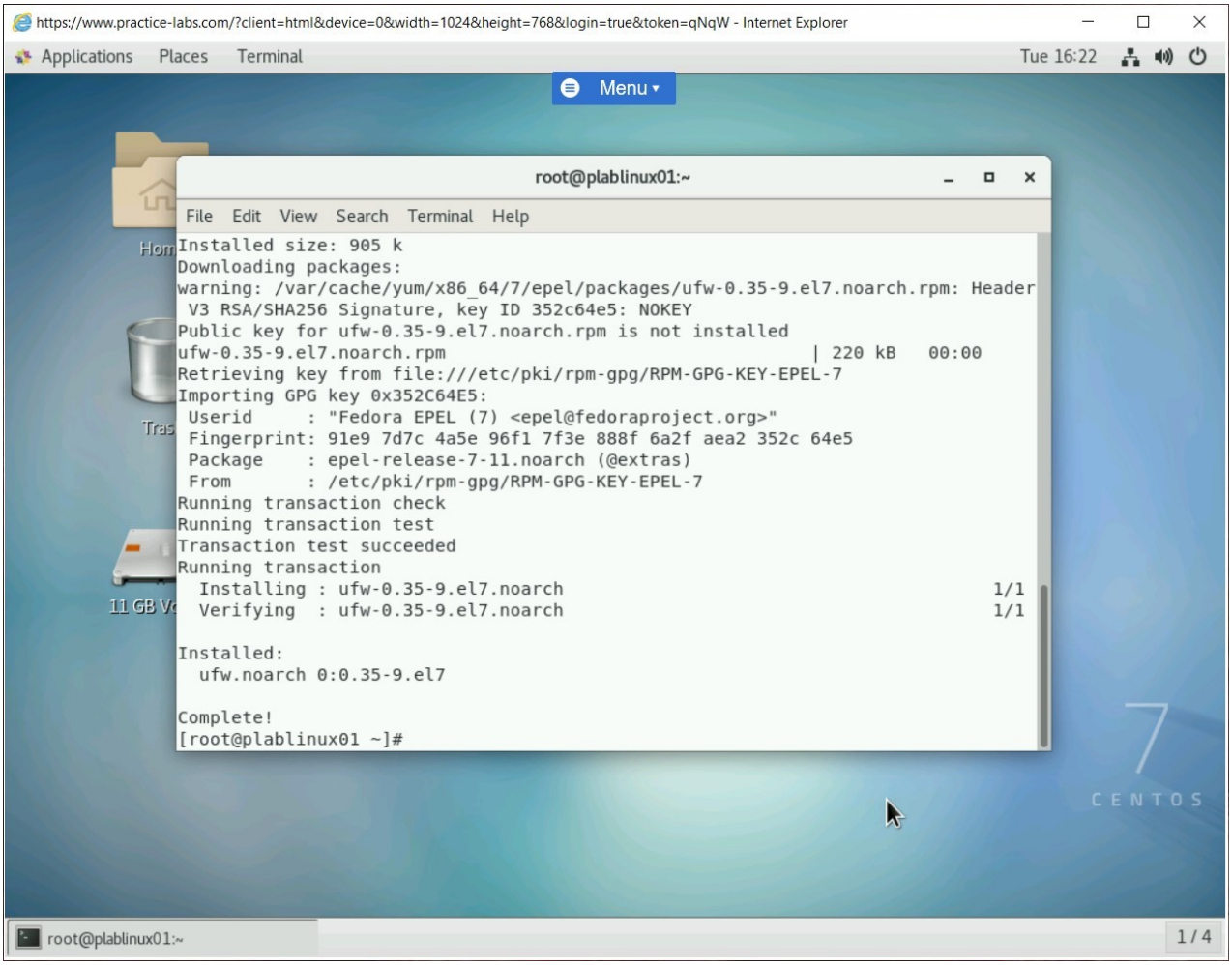


Figure 1.11 Screenshot of PLABLINUX01: Showing the installation completion of UFW firewall.

Step 7

Clear the screen by entering the following command:

```
clear
```

You need to configure UFW to auto start at the system boot. Type the following command:

```
ufw enable
```

Press **Enter**. Notice that UFW is now active and enabled on system startup.

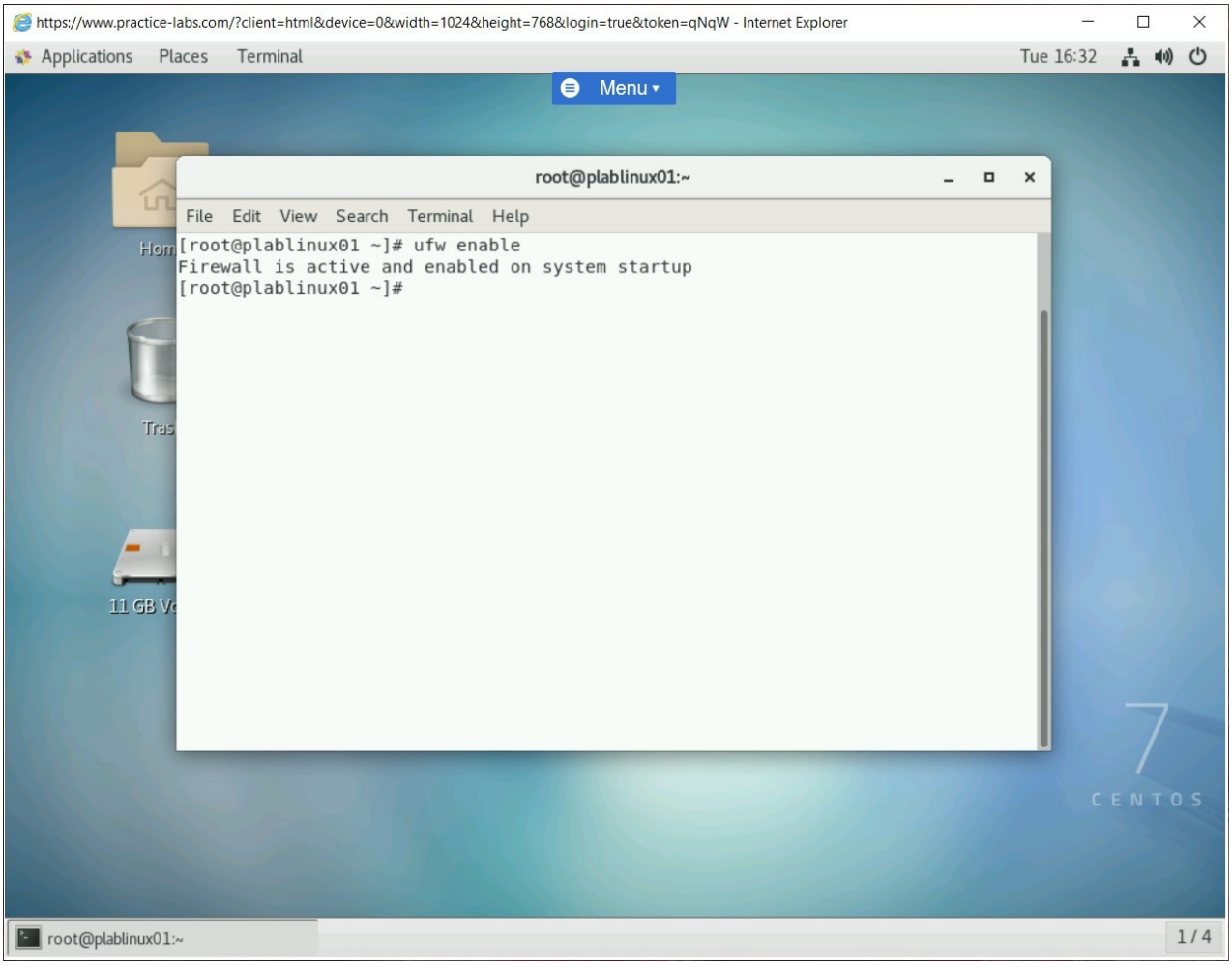


Figure 1.12 Screenshot of PLABLINUX01: Enabling the UFW firewall to start at the bootup.

Step 8

You can now verify the status of UFW. Type the following command:

```
ufw status
```

Press **Enter**. Notice that UFW is now active and enabled on system startup.

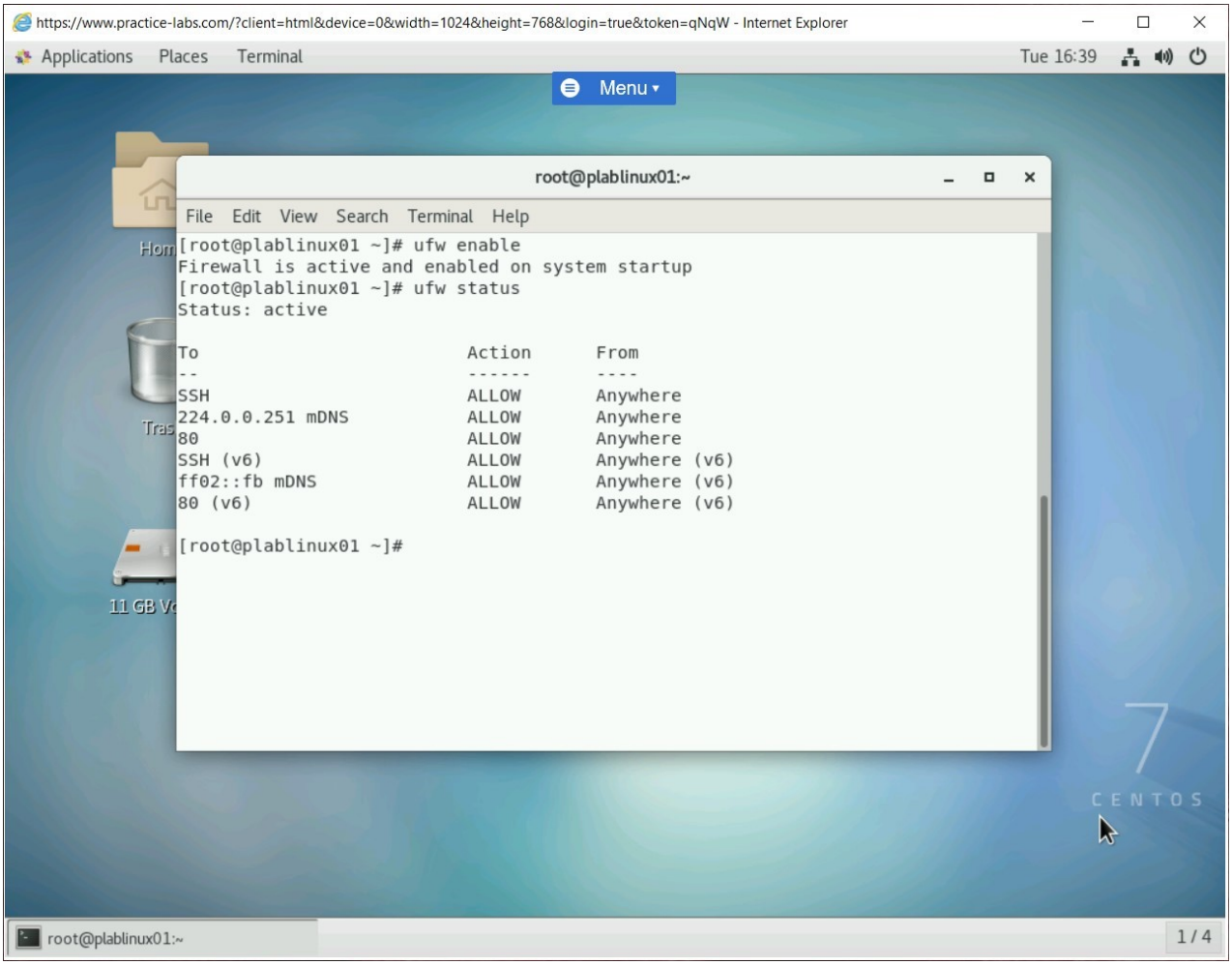


Figure 1.13 Screenshot of PLABLINUX01: Checking the UFW status.

Task 3 - Set UFW Default Policy

Without any configuration, UFW, by default, denies all incoming traffic and allows all outgoing traffic. However, this may not be the requirement in most organizations. You will need to define your own policies.

In this task, you will learn to set UFW default policy. To set the UFW default policy, perform the following steps:

Step 1

Clear the screen by entering the following command:

```
clear
```

There are two different ways in which you can add incoming and outgoing rules.

- Use the service name
- Use the port number

Let's first add a rule with the service name. Type the following command:

```
ufw allow http
```

Press **Enter**. Notice the **HTTP** service is now allowed.

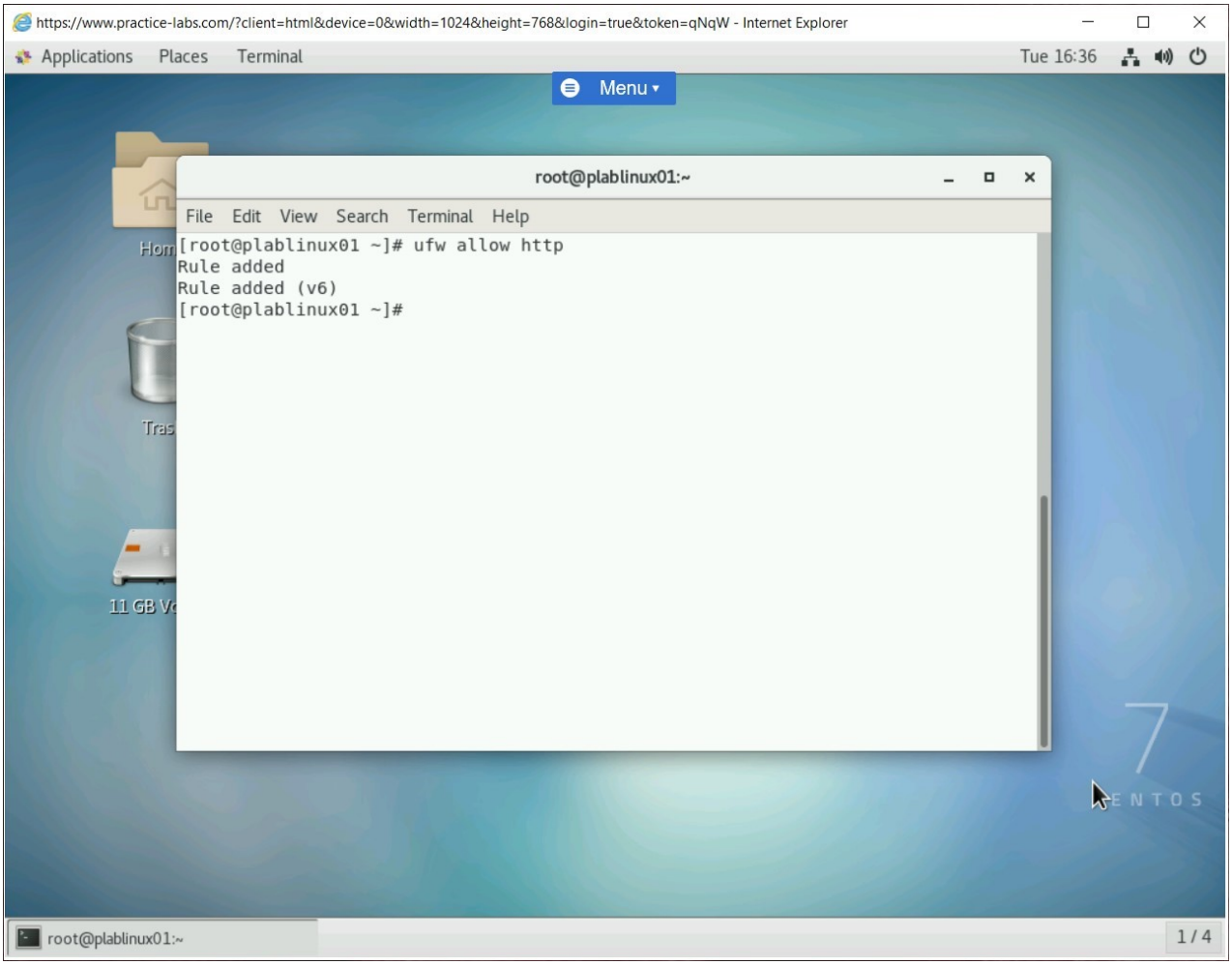


Figure 1.14 Screenshot of PLABLINUX01: Adding a rule in the UFW firewall for HTTP.

Step 2

You can also use the port number to add a rule. Type the following command:

```
ufw allow 80
```

Press **Enter**. Notice that no new rule has been added because its equivalent service rule was added.

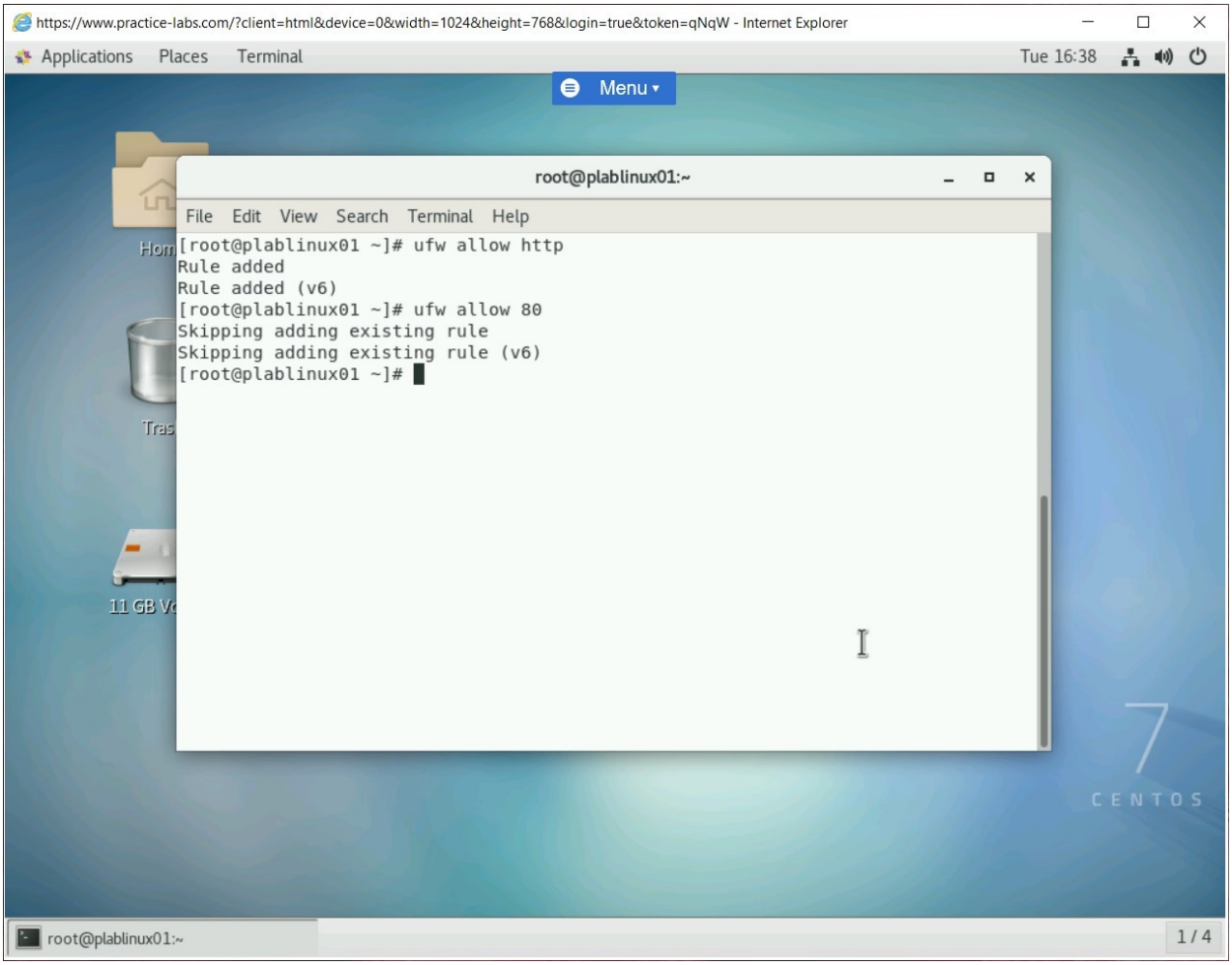


Figure 1.15 Screenshot of PLABLINUX01: Adding a rule in the UFW firewall for the port 80.

Step 3

Clear the screen by entering the following command:

```
clear
```

You can now try to add another rule with a different port number, 443. Type the following command:

```
ufw allow 443
```

Press **Enter**. Notice the **443** port is now allowed.

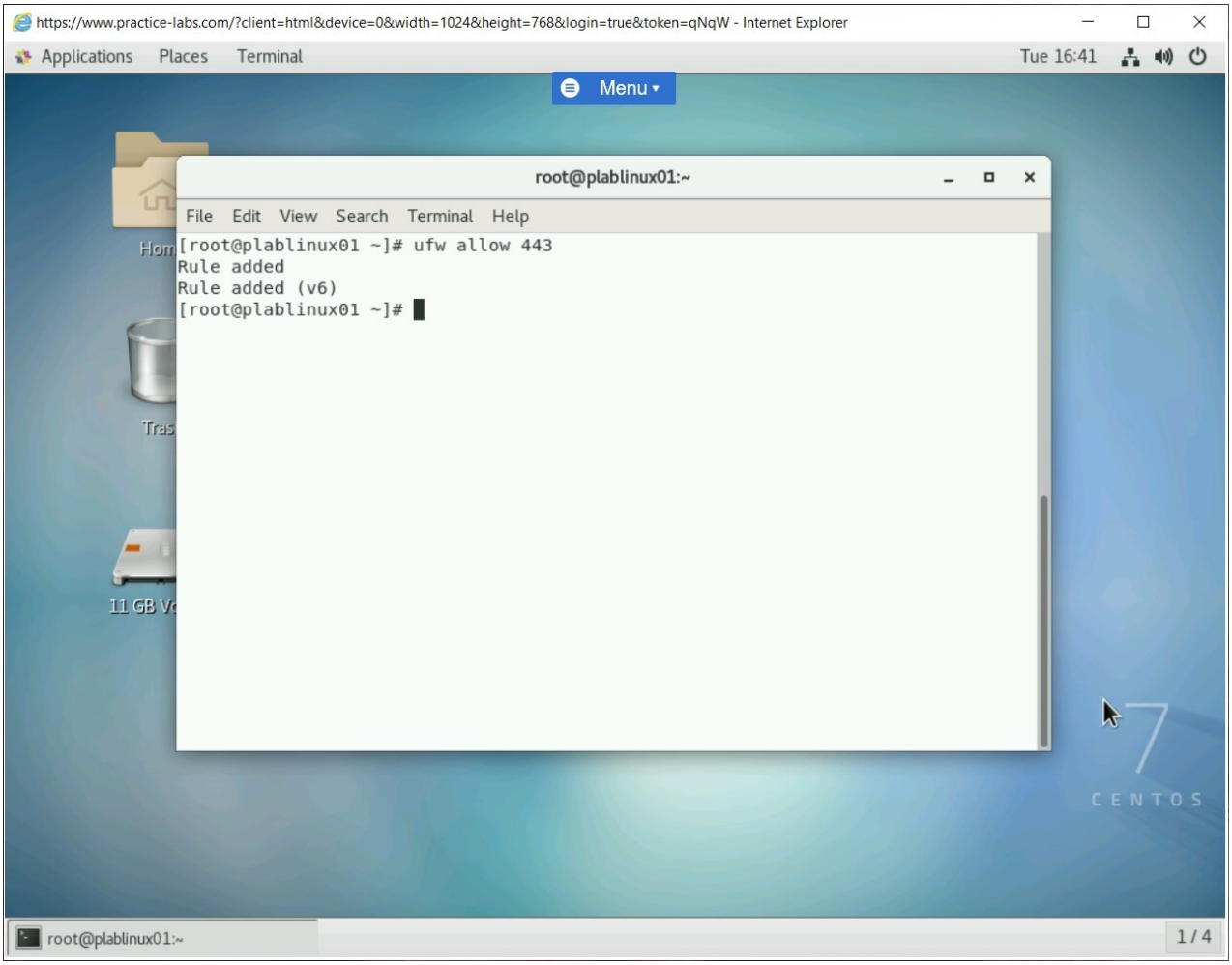


Figure 1.16 Screenshot of PLABLINUX01: Adding a rule in the UFW firewall for port 443.

Step 4

Clear the screen by entering the following command:

```
clear
```

UFW also provides the flexibility of filtering packet with a port and protocol. Type the following command:

```
ufw allow 80/tcp
```

Press **Enter**. Notice that a new rule has been added. Both, the port number and protocol name, have been considered for the rule.

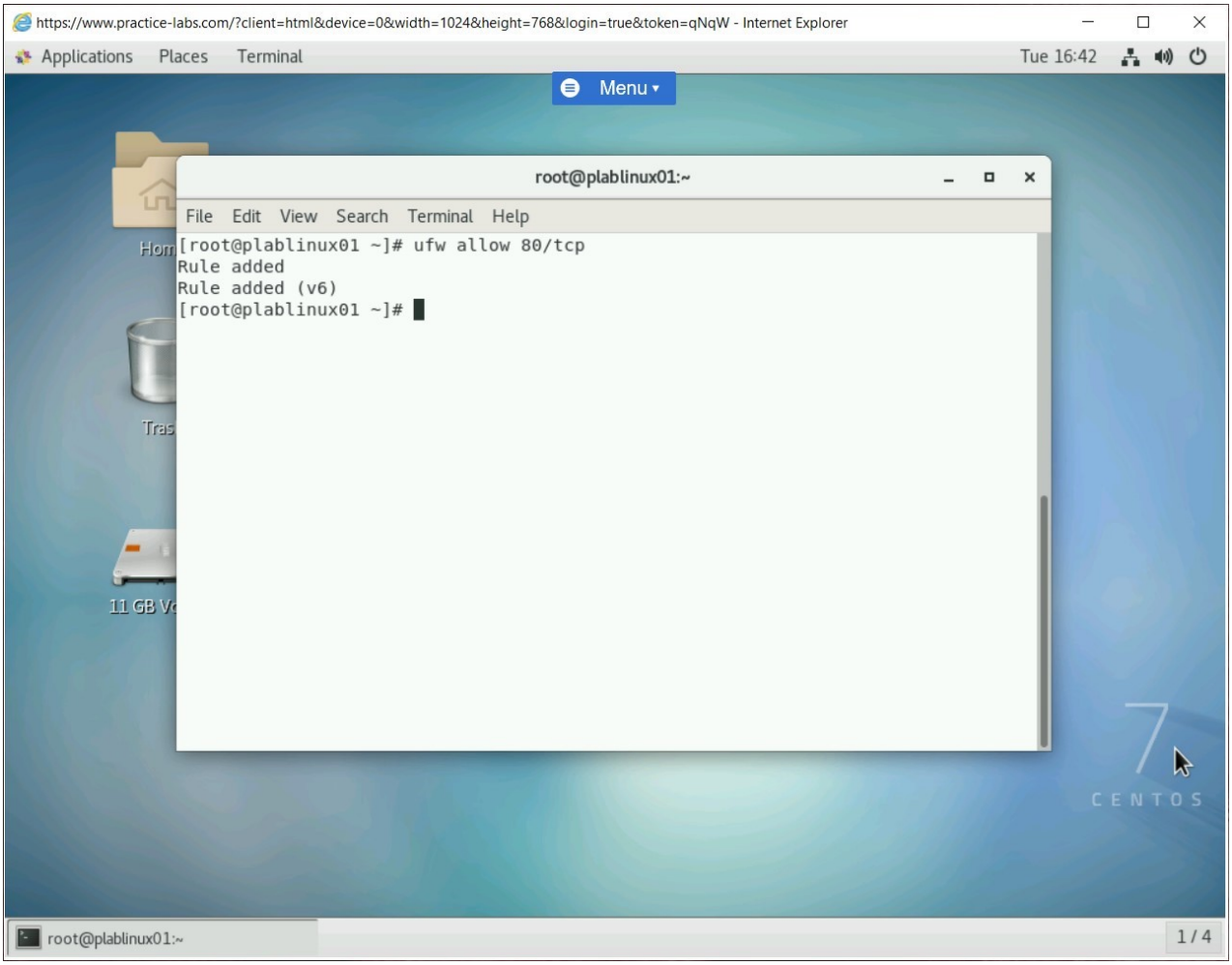


Figure 1.17 Screenshot of PLABLINUX01: Adding a rule for port and protocol.

Step 5

Clear the screen by entering the following command:

```
clear
```

Just like in a rule, you allow a port or service, and it is also possible to deny a port or service. Type the following command:

```
ufw deny 21
```

Press **Enter**. Notice that a rule with the deny condition has been added.

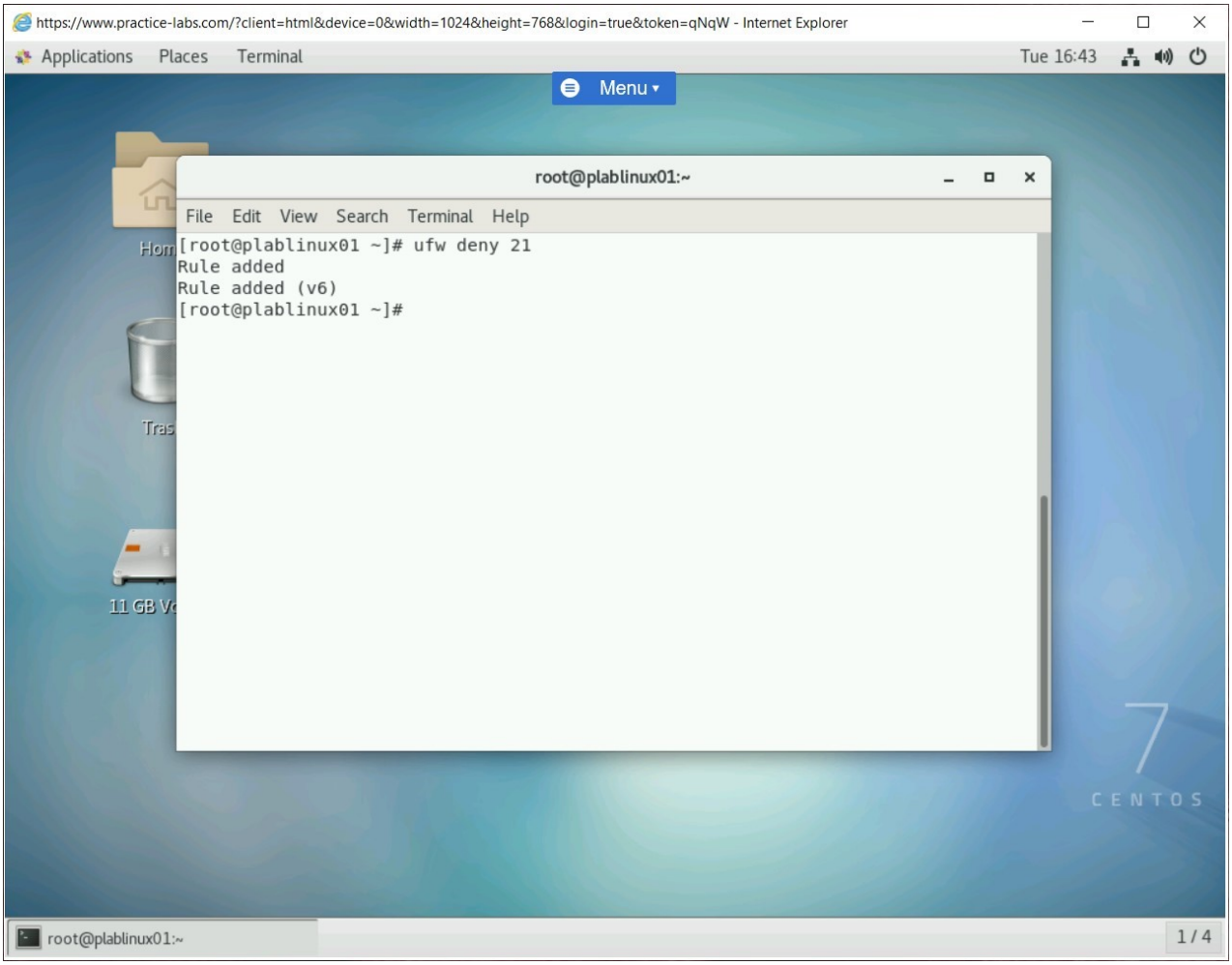


Figure 1.18 Screenshot of PLABLINUX01: Adding a rule to deny port 21.

Step 6

Clear the screen by entering the following command:

```
clear
```

Similar to allowing or denying, it is also simple to delete a rule. Type the following command:

```
ufw delete deny 21
```

Press **Enter**. Notice that the rule with the deny condition is now deleted.

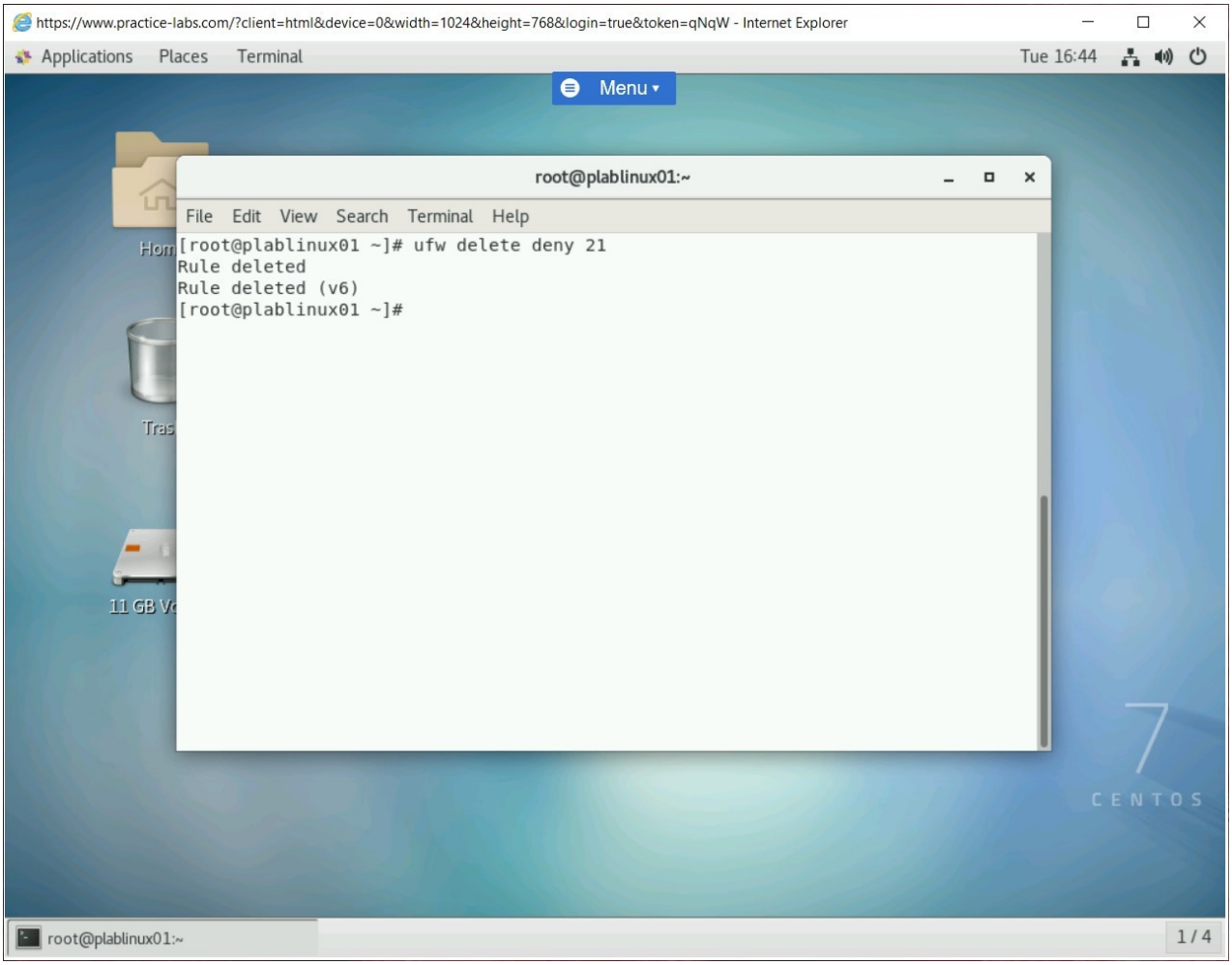


Figure 1.19 Screenshot of PLABLINUX01: Deleting the deny port 21 rule.

Step 7

Clear the screen by entering the following command:

```
clear
```

You can check the status of the rule in UFW. Type the following command:

```
ufw status verbose
```

Press **Enter**. The output will display the existing rules in UFW.

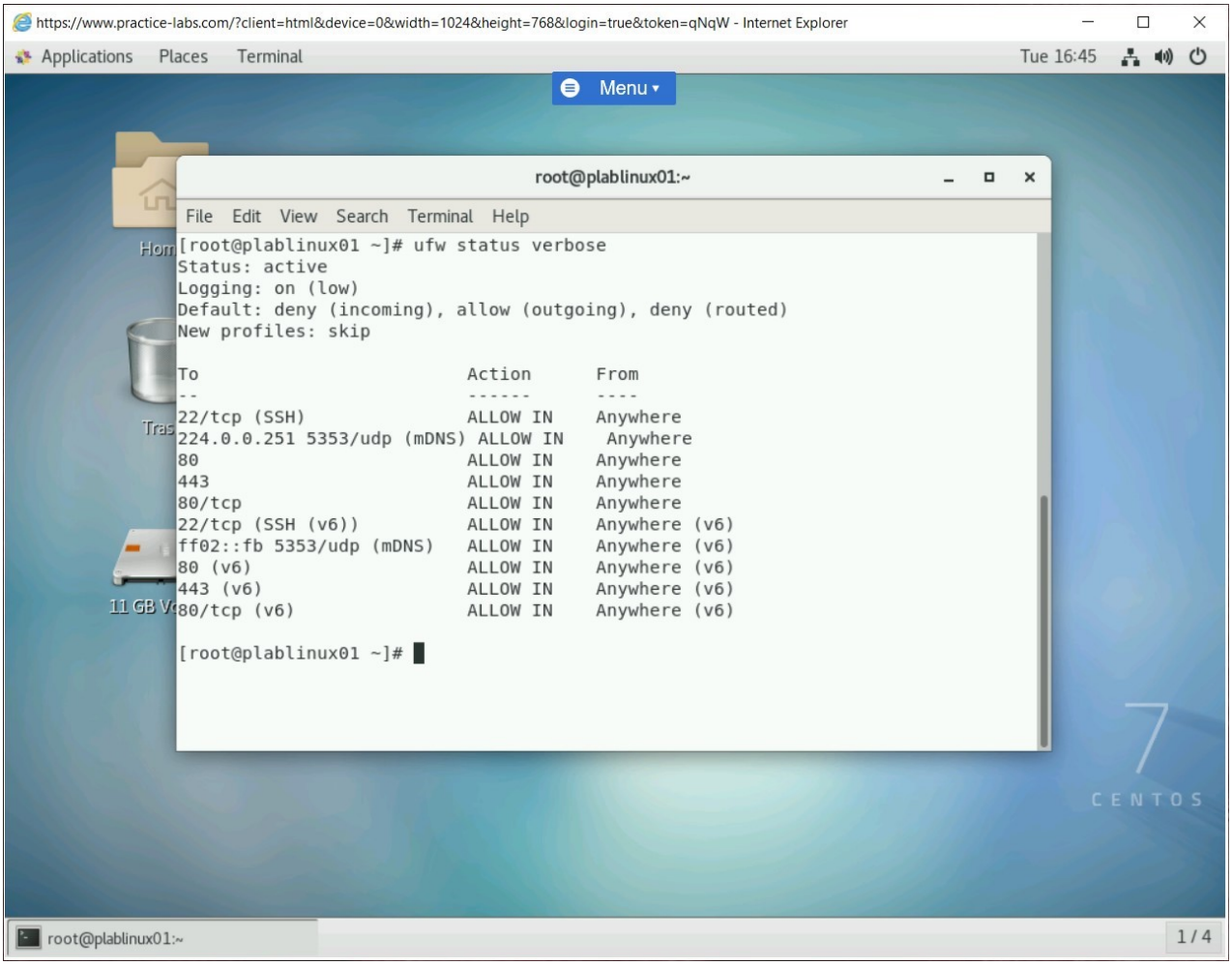


Figure 1.20 Screenshot of PLABLINUX01: Checking the UFW firewall status.

Task 4 - Configure Advanced UFW Rules

Other than adding or deleting simple rules in UFW, you can configure rules for specific IP address or a range of IP addresses. To configure Advanced UFW rules, perform the following steps:

Step 1

Clear the screen by entering the following command:

```
clear
```

You can create a rule in which a specific IP is allowed all services on **PLABLINUX01**. Type the following command:

```
ufw allow from 192.168.0.3
```

Press **Enter**. Notice that a new rule has been added.

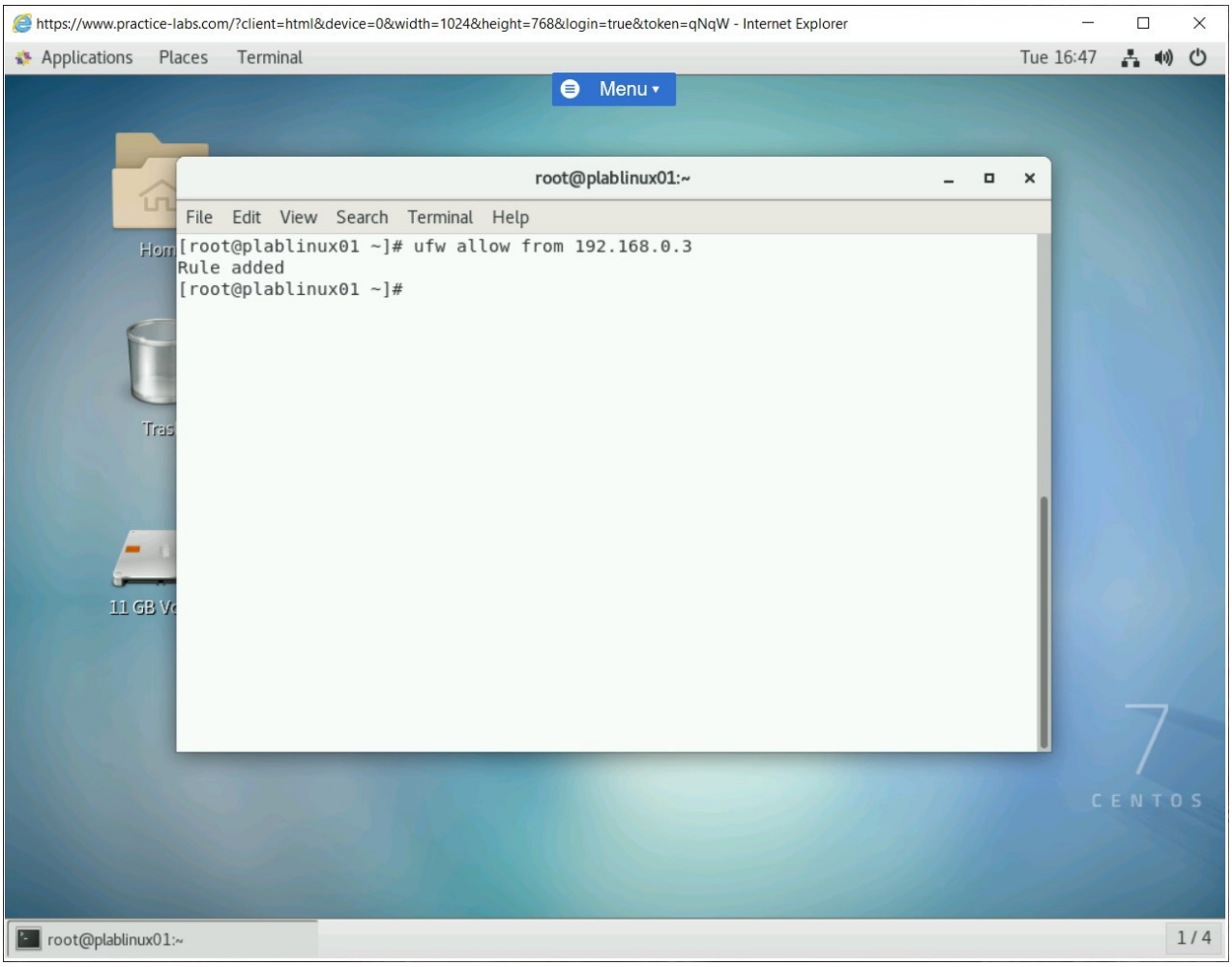


Figure 1.21 Screenshot of PLABLINUX01: Creating a rule to allow a specific IP for all services.

Step 2

Similarly, you can add a rule to allow a complete IP range to access all services on PLABLINUX01. Type the following command:

```
ufw allow from 192.168.0.0/24
```

Press **Enter**. The systems in this IP range will be able to access all services on **PLABLINUX01**.

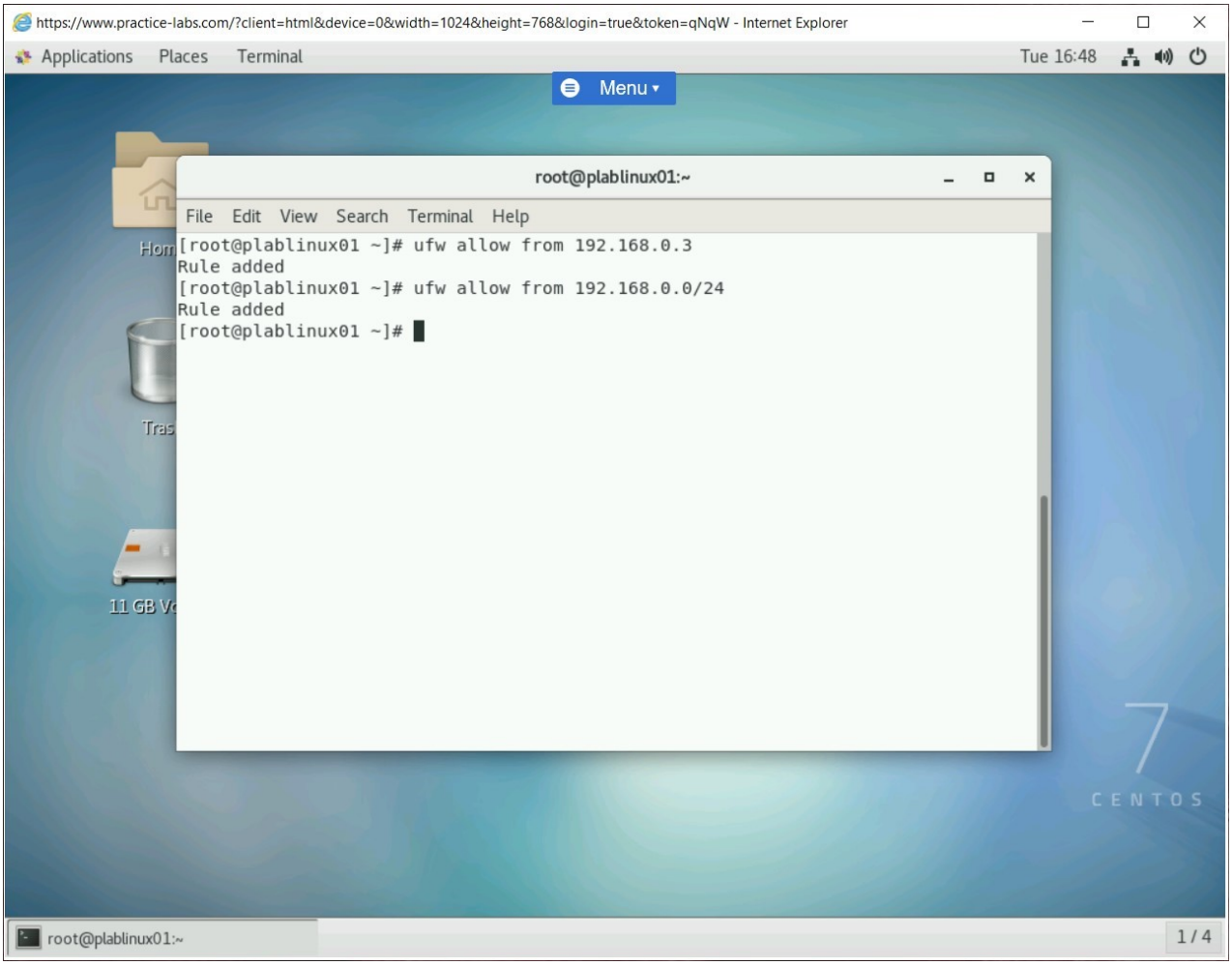


Figure 1.22 Screenshot of PLABLINUX01: Adding a rule to allow a complete IP range to access all services.

Step 3

Instead of providing access to all services on **PLABLINUX01**, you can allow 192.168.0.3 to access only **80/tcp**. Type the following command:

```
ufw allow from 192.168.0.3 to any port 80 proto tcp
```

Press **Enter**. The IP address, 192.168.0.3, is now allowed to access only 80/tcp on **PLABLINUX01**.

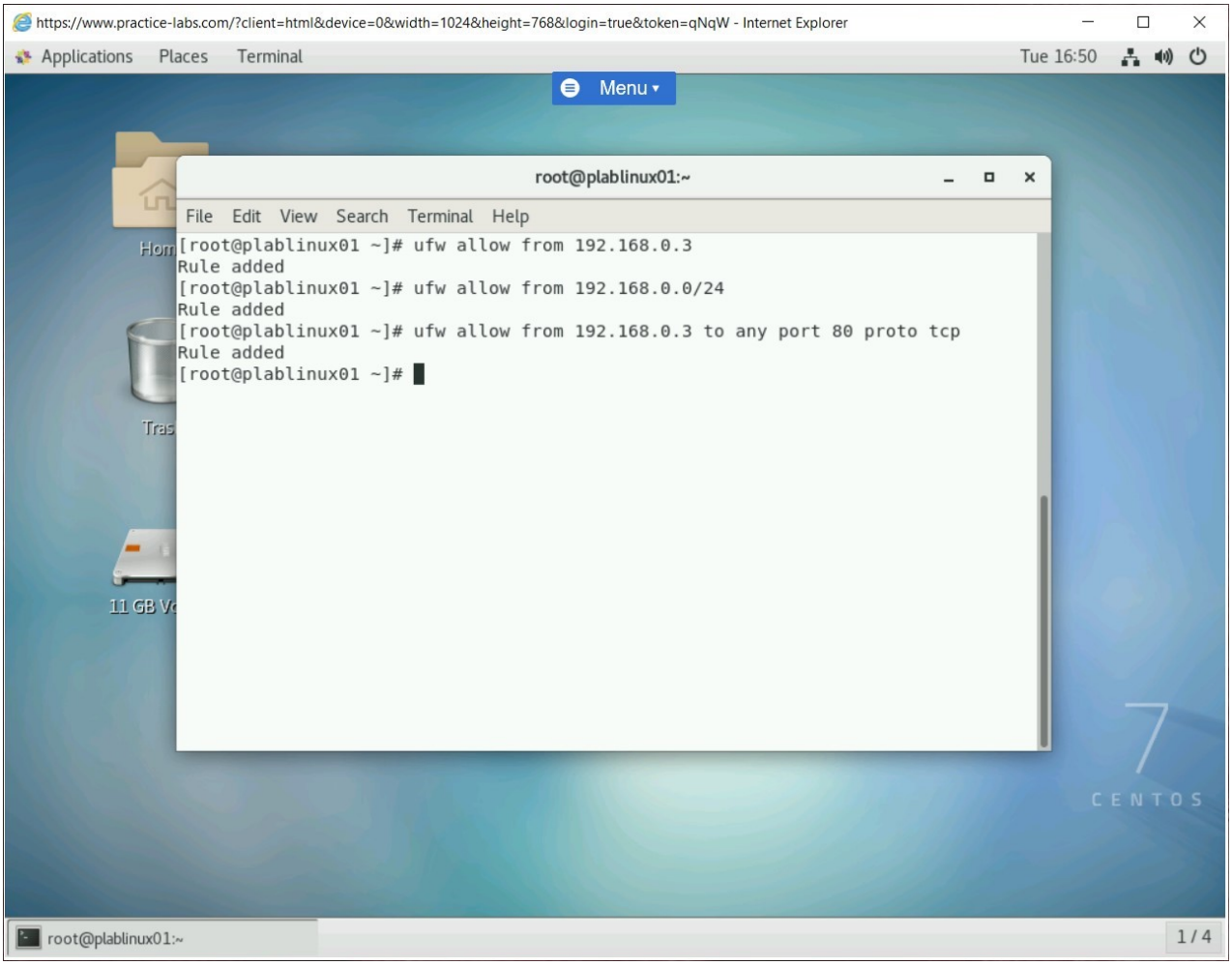


Figure 1.23 Screenshot of PLABLINUX01: Allowing 192.168.0.3 to access only 80/tcp.

Step 4

Assume that you want to disallow 192.168.0.3 from accessing 80/tcp. However, you want to allow other systems to access 80/tcp. Type the following command:

```
ufw deny from 192.168.0.3 to any port 80 proto tcp
```

Press **Enter**. Notice that the existing rule, which allowed access, is now updated.

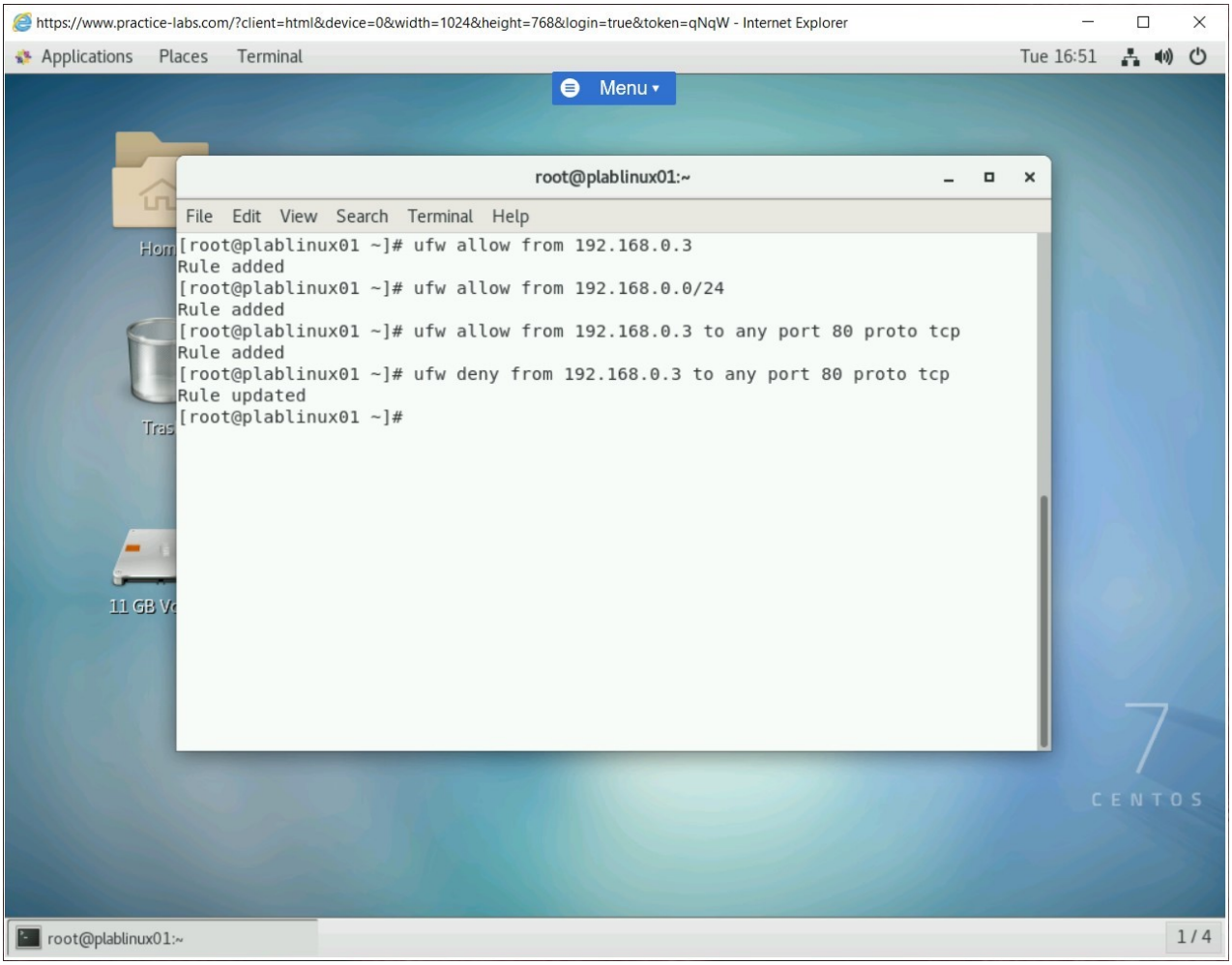


Figure 1.24 Screenshot of PLABLINUX01: Disallowing 192.168.0.3 from accessing 80/tcp.

Task 5 - Block ICMP Requests

By default, UFW is designed to allow the ICMP requests, which means that any system can ping to the system hosting UFW, which is PLABLINUX01 in this case. To block ICMP requests, perform the following steps:

Step 1

Clear the screen by entering the following command:

```
clear
```

To be able to block ping requests, you need to edit the **/etc/ufw/before.rules** file. Type the following command:

```
gedit /etc/ufw/before.rules
```

Press **Enter**. Notice that a new rule has been added.

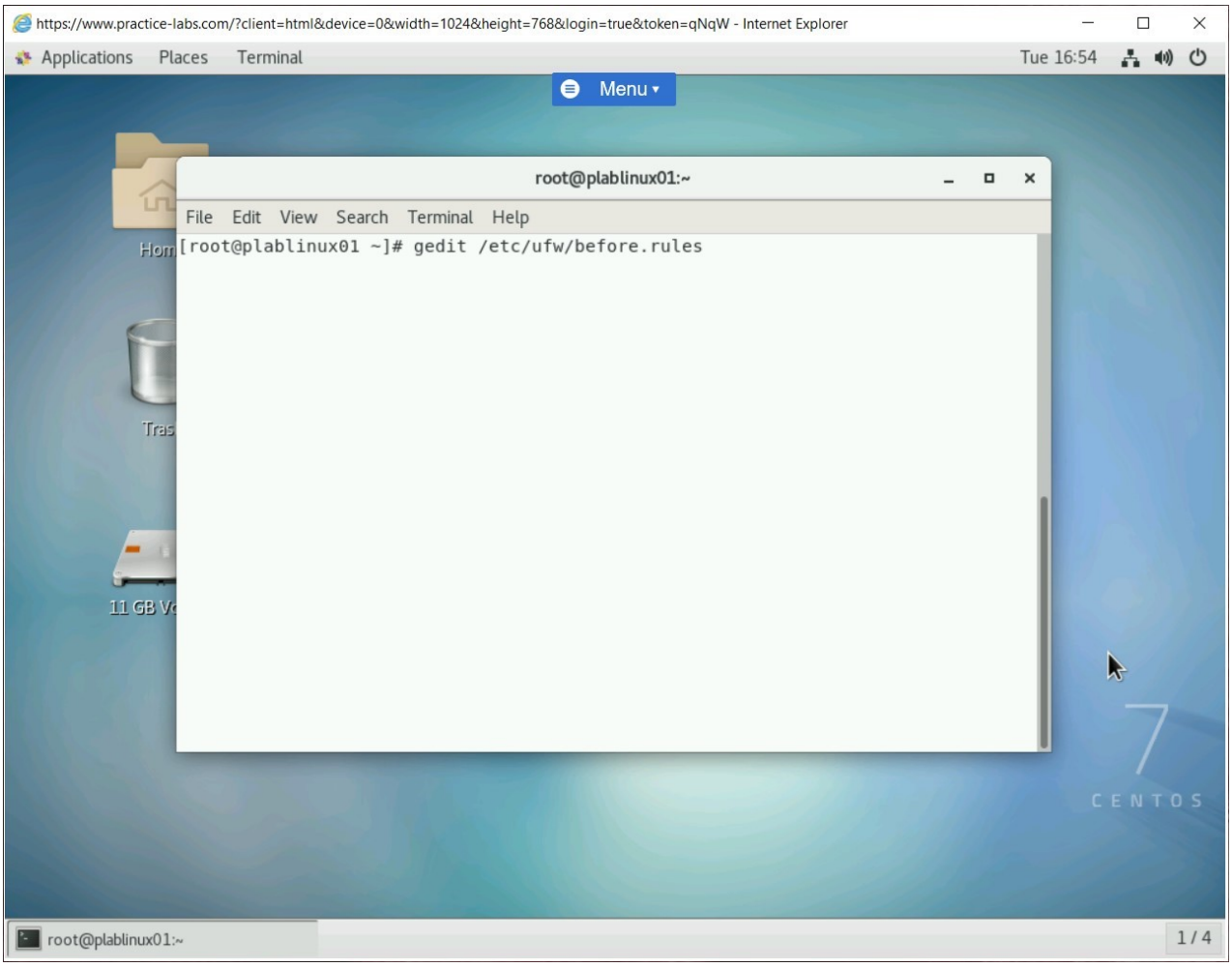


Figure 1.25 Screenshot of PLABLINUX01: Opening the /etc/ufw/before.rules file for editing.

Step 2

The **/etc/ufw/before.rules** file is now opened. Navigate to the following section: **# ok icmp codes for INPUT**

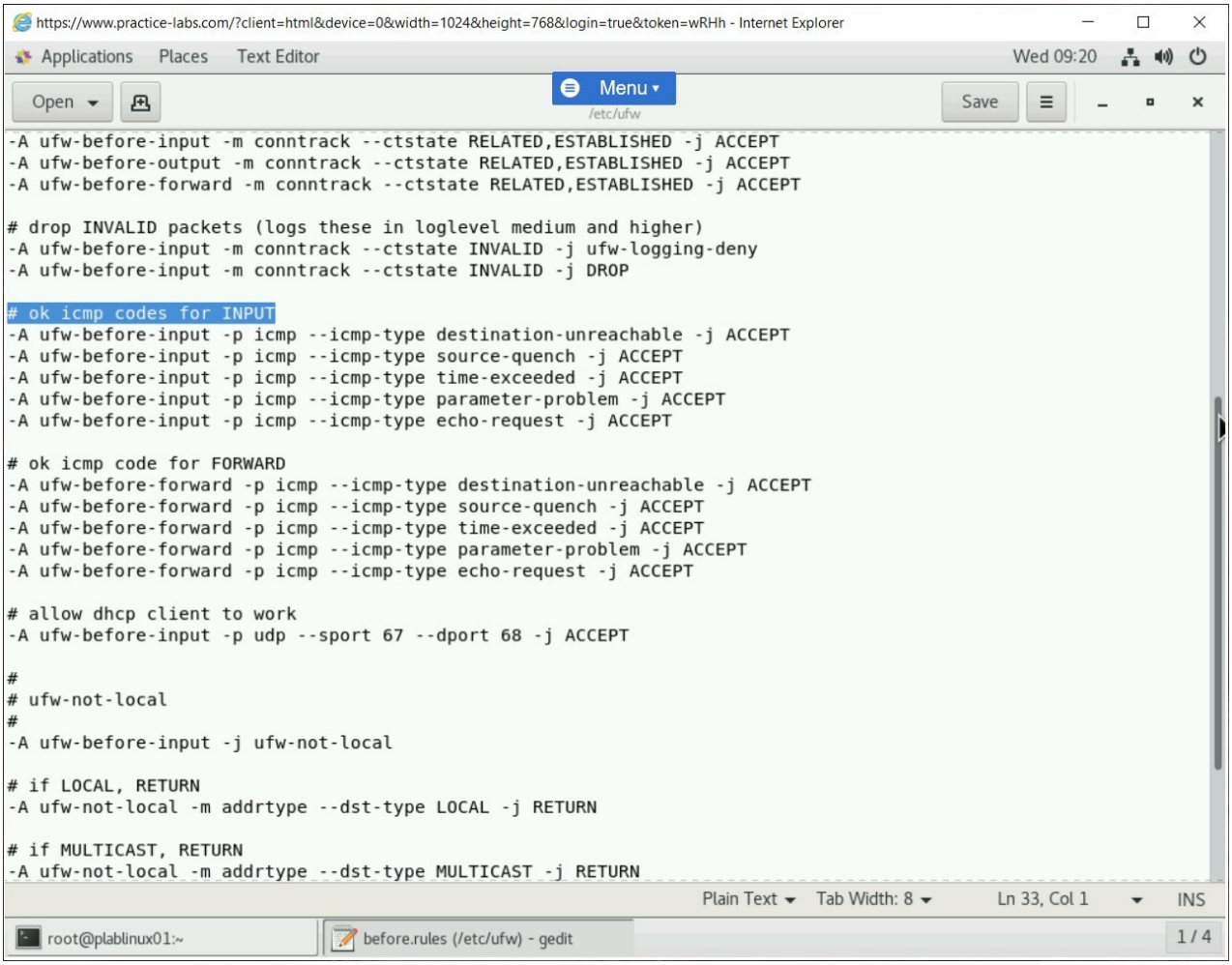


Figure 1.26 Screenshot of PLABLINUX01: Showing the opened /etc/ufw/before.rules file.

Step 3

Comment the following line by prefixing # in front of them:

```
-A ufw-before-input -p icmp --icmp-type destination-
unreachable -j ACCEPT
-A ufw-before-input -p icmp --icmp-type source-quench -j
ACCEPT
-A ufw-before-input -p icmp --icmp-type time-exceeded -j
ACCEPT
-A ufw-before-input -p icmp --icmp-type parameter-problem
-j ACCEPT
-A ufw-before-input -p icmp --icmp-type echo-request -j
ACCEPT
```

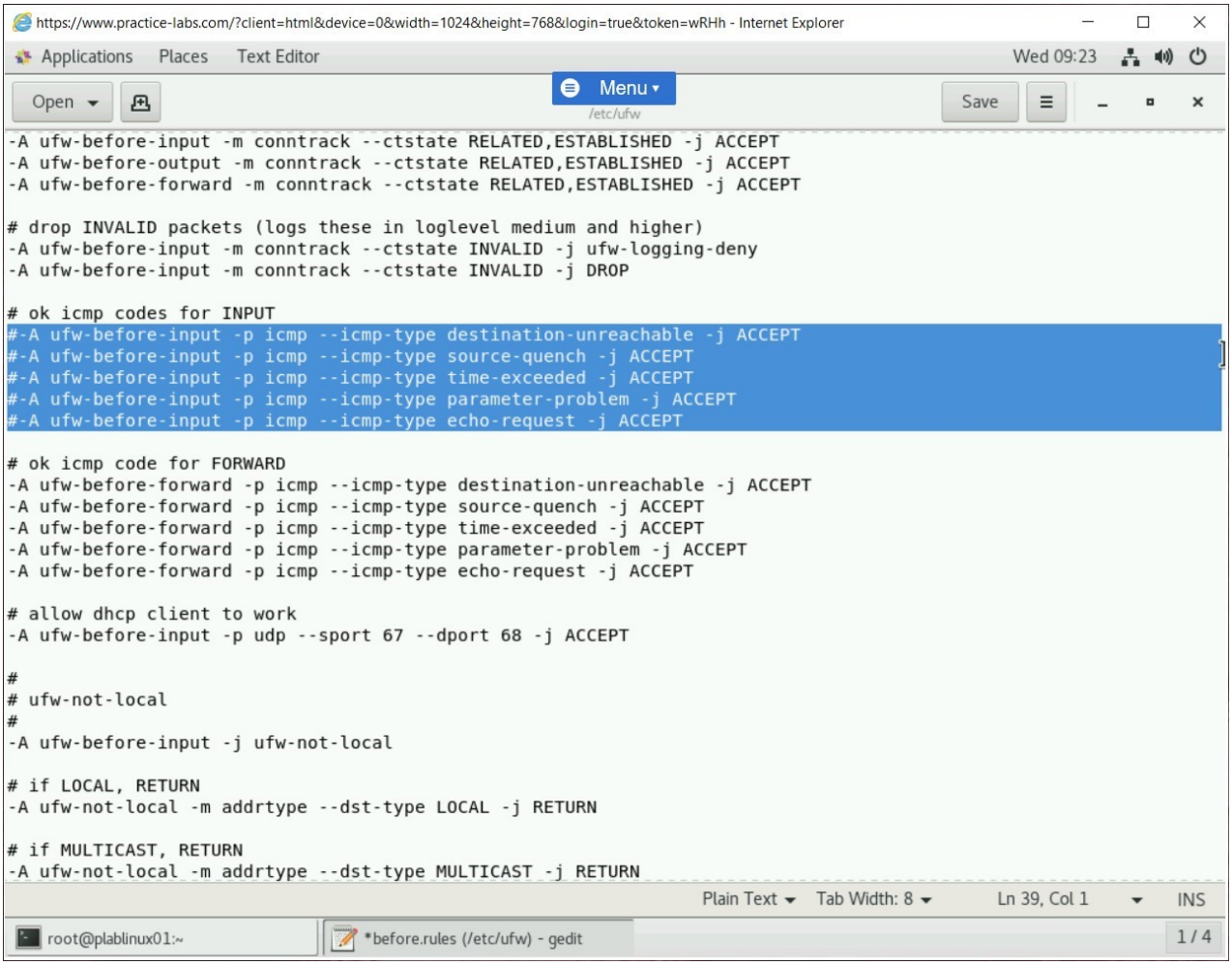


Figure 1.27 Screenshot of PLABLINUX01: Commenting on the ICMP INPUT rules.

Step 4

To save the file, click **Save**. Then, close the file. You have denied ping requests to **PLABLINUX01**.

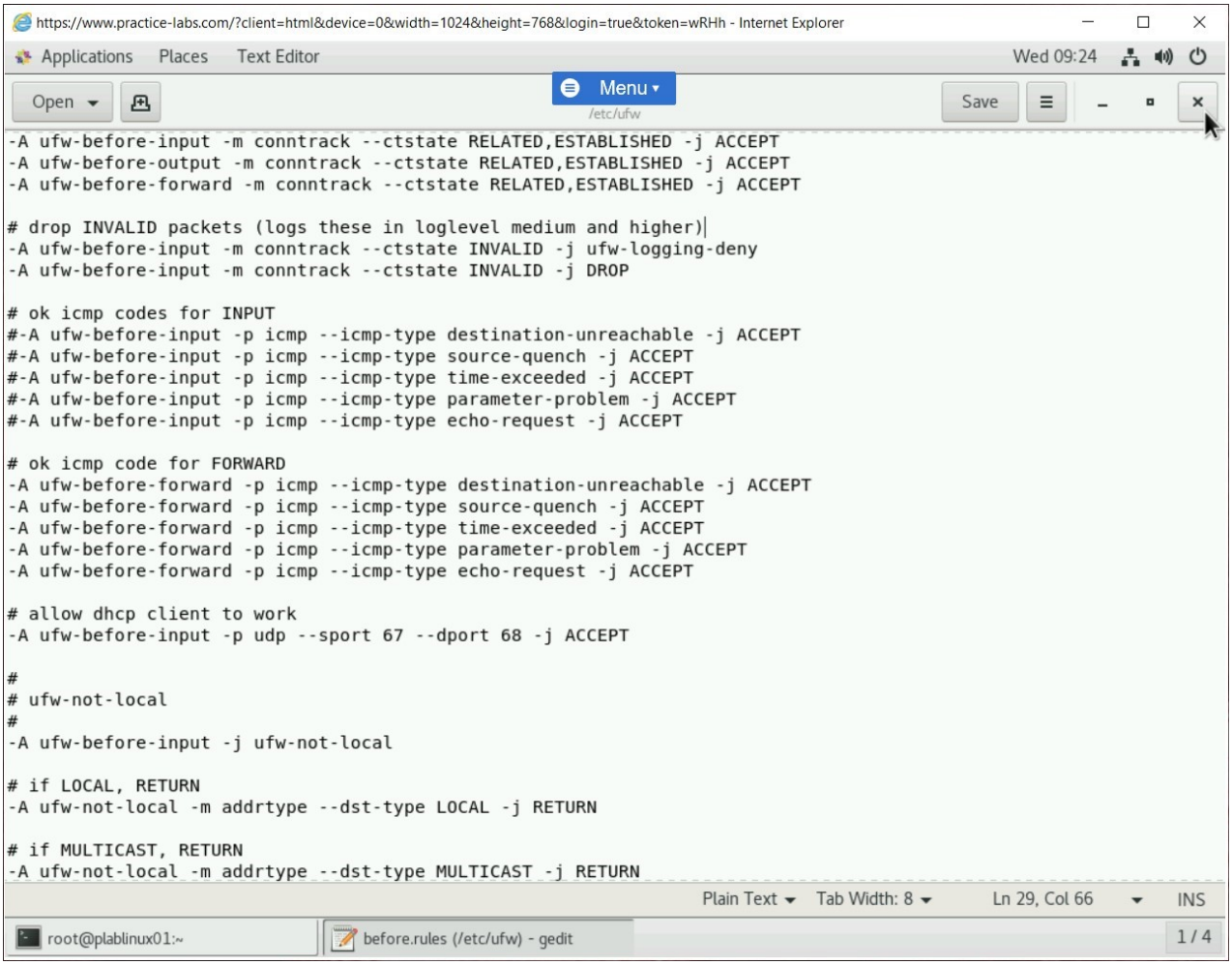


Figure 1.28 Screenshot of PLABLINUX01: Saving and closing the file.

Task 6 - Reset UFW

There may be a scenario in which you need to reset UFW. To reset UFW, perform the following steps:

Step 1

Clear the screen by entering the following command:

```
clear
```

To reset UFW, type the following command:

```
ufw reset
```

Press **Enter**. Notice that you are prompted to confirm the reset, which will remove all rules and the default rules will be configured.

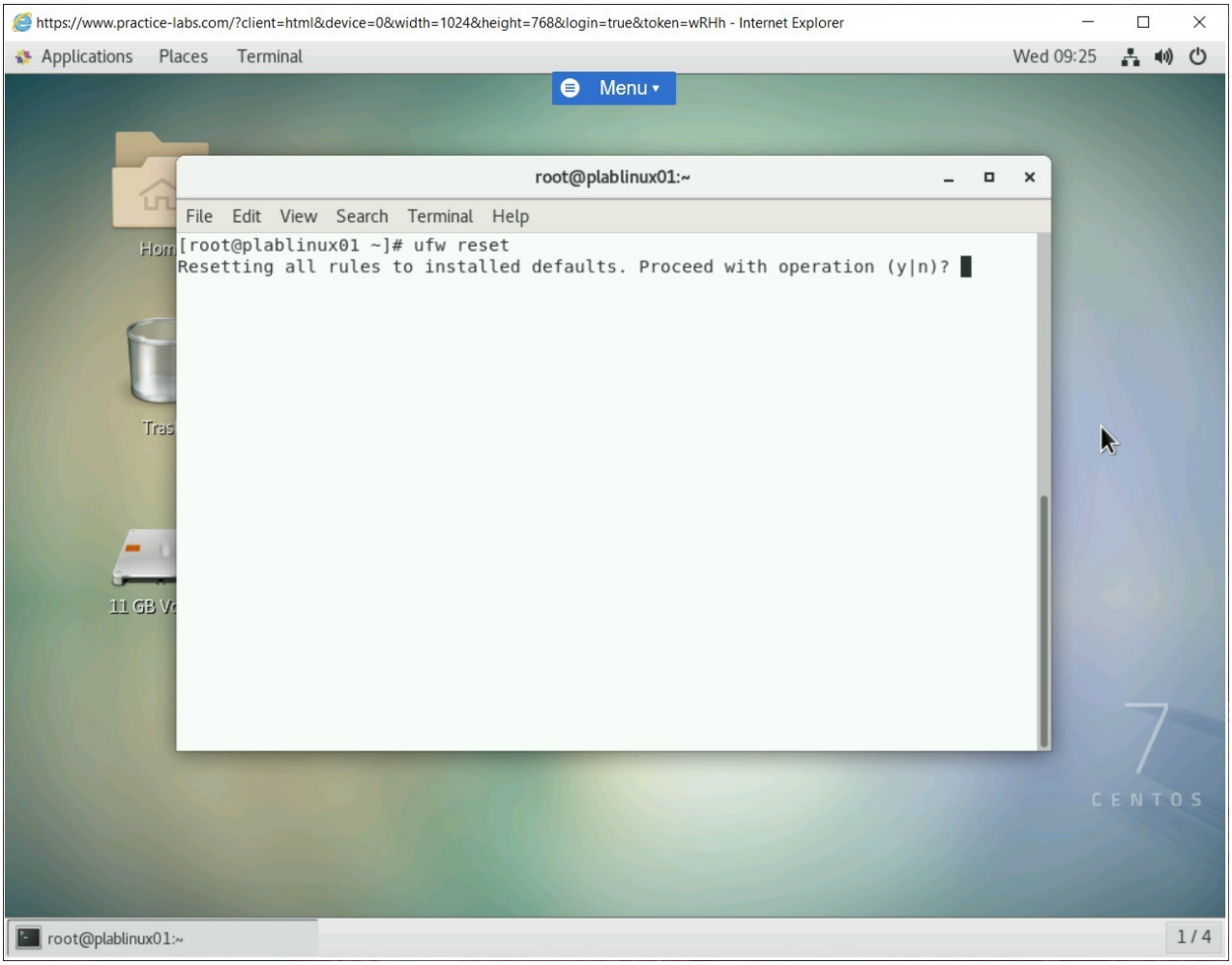


Figure 1.29 Screenshot of PLABLINUX01: Resetting the UFW firewall to the original configuration.

Step 2

To confirm the reset of UFW, type the following command:

```
y
```

Press **Enter**. Notice that before resetting, all rules are backed up automatically.

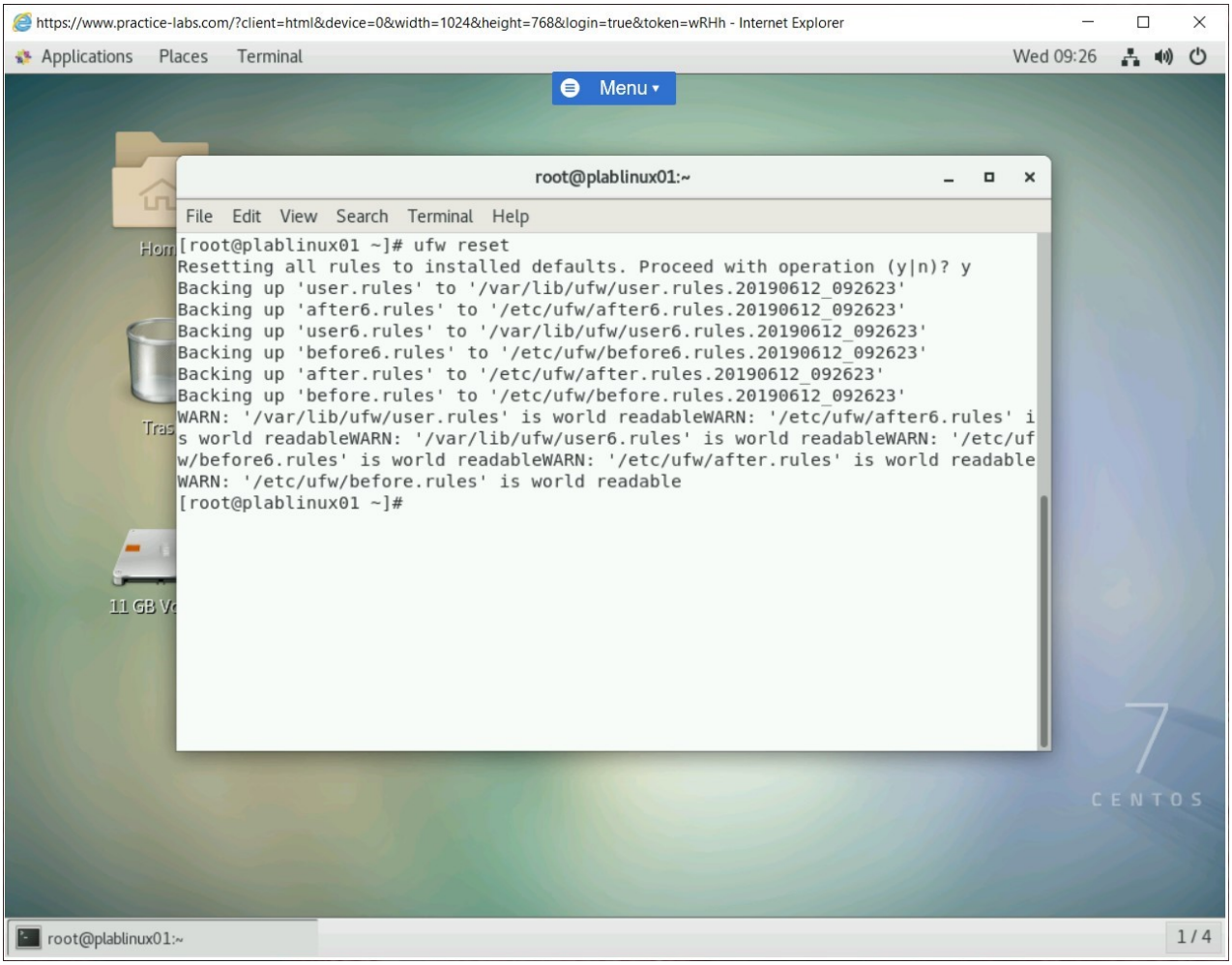


Figure 1.30 Screenshot of PLABLINUX01: Confirming the reset of the UFW firewall.

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

Exercise 2 - Install and Configure DenyHosts

DenyHosts is a Python-based firewall that is mainly used for monitoring the SSH server. It can prevent the SSH server from any intruding IP address by adding it in the /etc/hosts.deny file.

In this exercise, you will learn to install and configure DenyHosts.

Learning Outcomes

After completing this exercise, you will be able to:

- Configure Network on Ubuntu

- Install and Configure DenyHosts

Your Devices

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

- **PLABLINUX02** (Ubuntu Server)

Task 1 - Configure Network on Ubuntu

Similar to CentOS, you will now configure the network on Ubuntu.

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

Step 1

Ensure all the required devices are powered on. Connect to **PLABLINUX02**.

Click **Admin**.

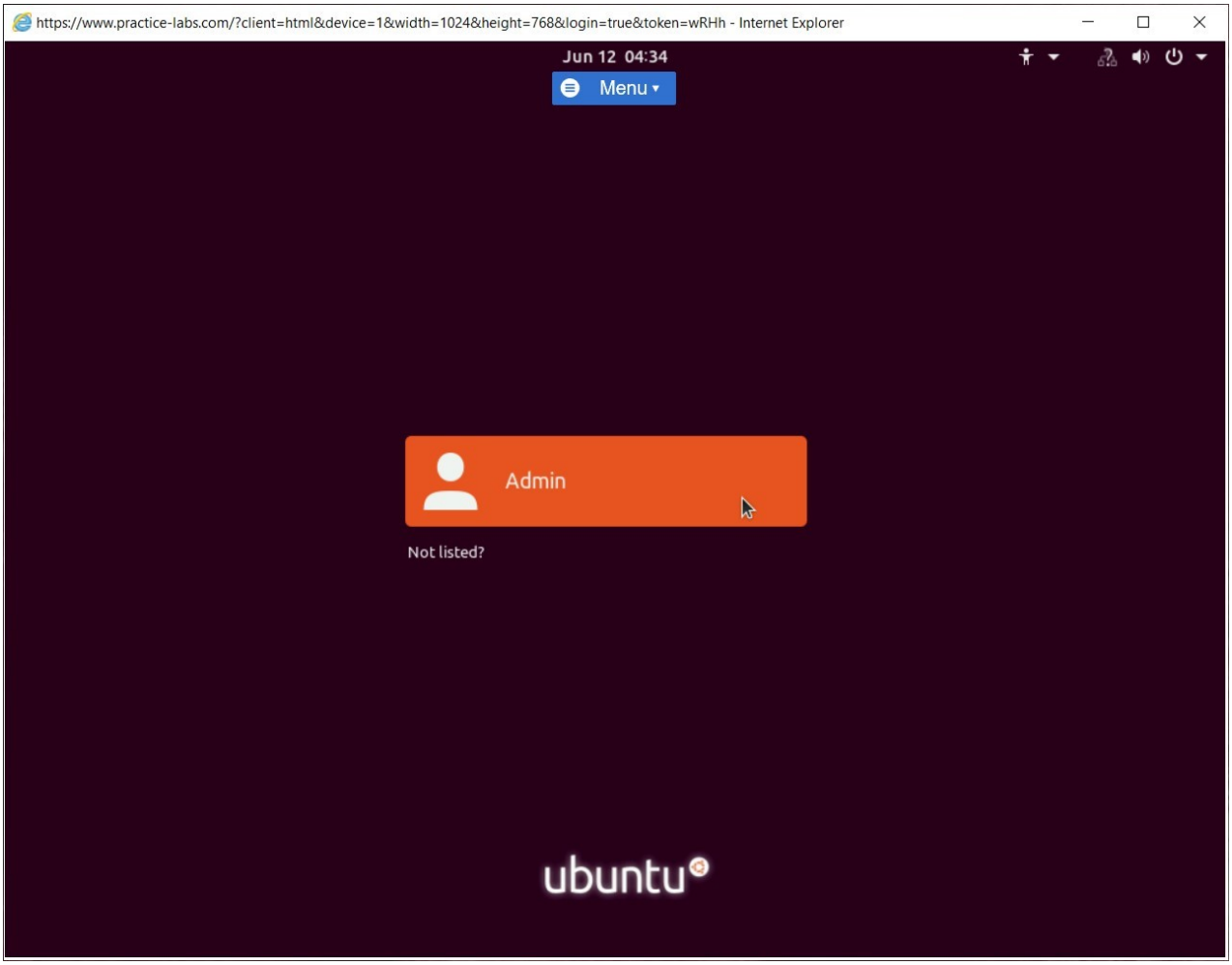


Figure 2.1 Screenshot of PLABLINUX02: Clicking the Administrator account on the login screen.

Step 2

When prompted, type the following password in the **Password** field:

```
Passw0rd
```

Click **Sign In**.

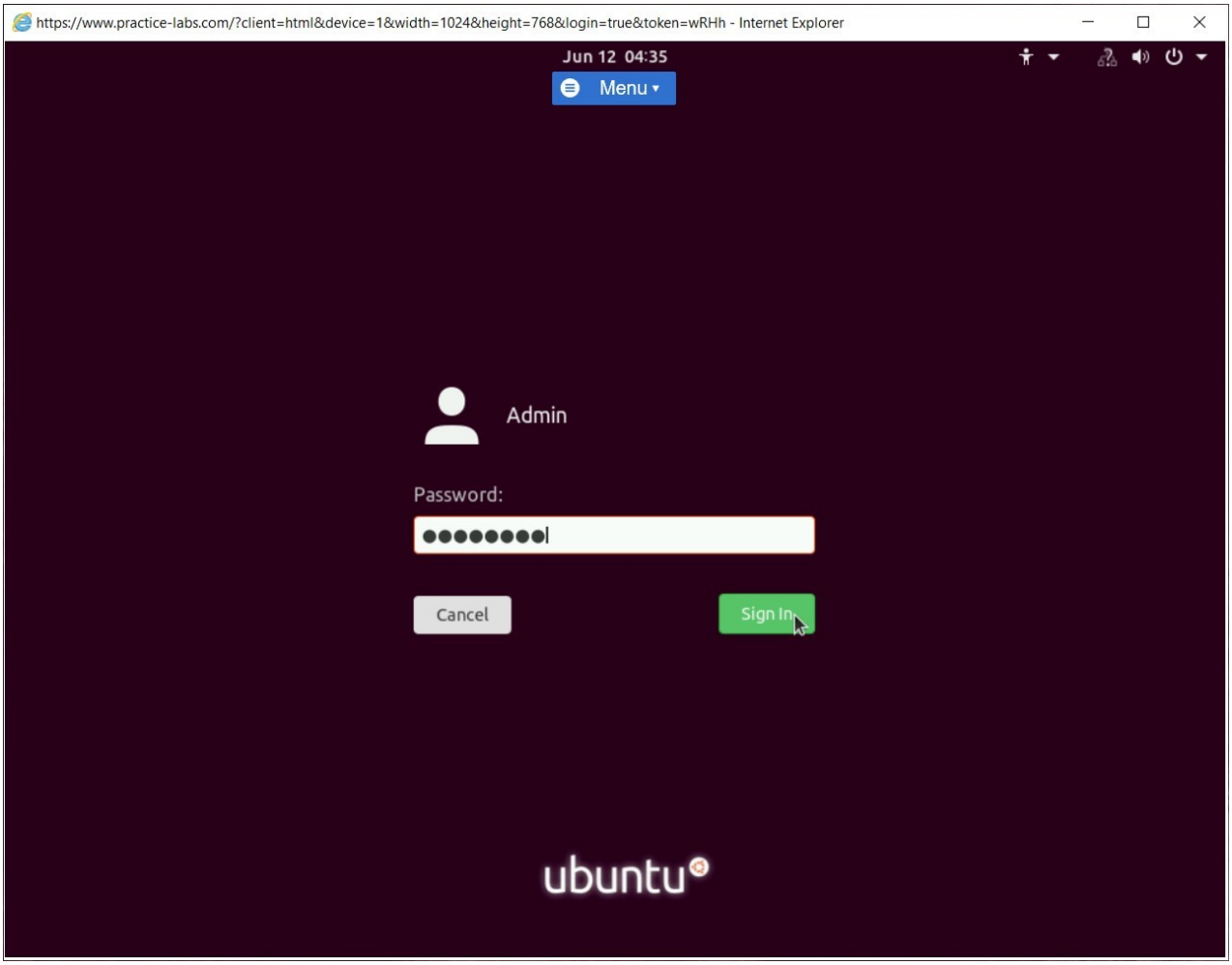


Figure 2.2 Screenshot of PLABLINUX02: Entering the password in the Password text box and then clicking Sign In.

After a successful login, the desktop is displayed.

> ***Note:*** *If you are prompted with Software Updater dialog box, click* ***Remind Me Later****.*

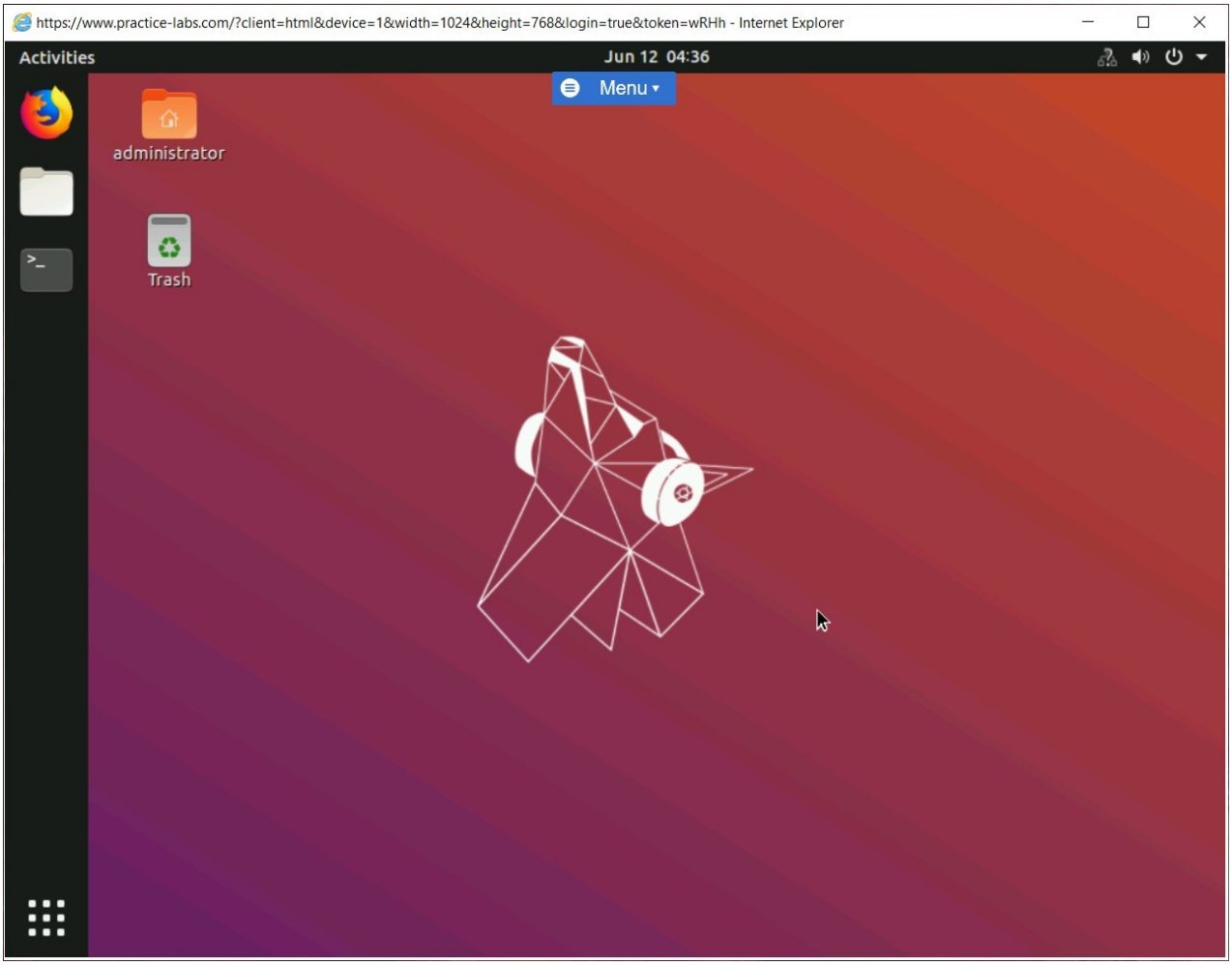


Figure 2.3 Screenshot of PLABLINUX02: Displaying the desktop after the successful login.

Step 3

Click the **Show Applications** icon in the bottom left corner.

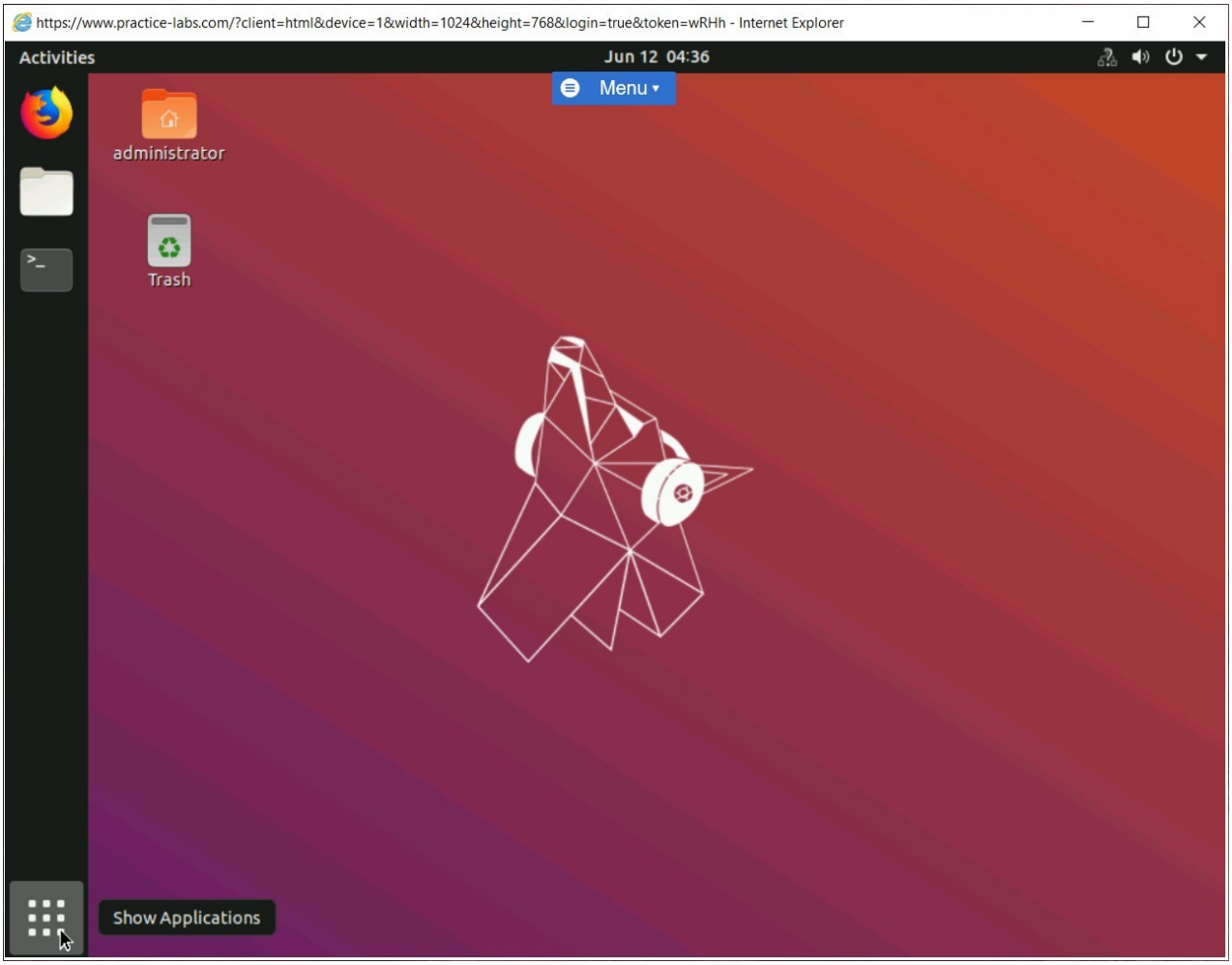


Figure 2.4 Screenshot of PLABLINUX02: Clicking the Show Applications icon.

Step 4

In the middle of the window, click **All**. Then click the second dot in the right corner.

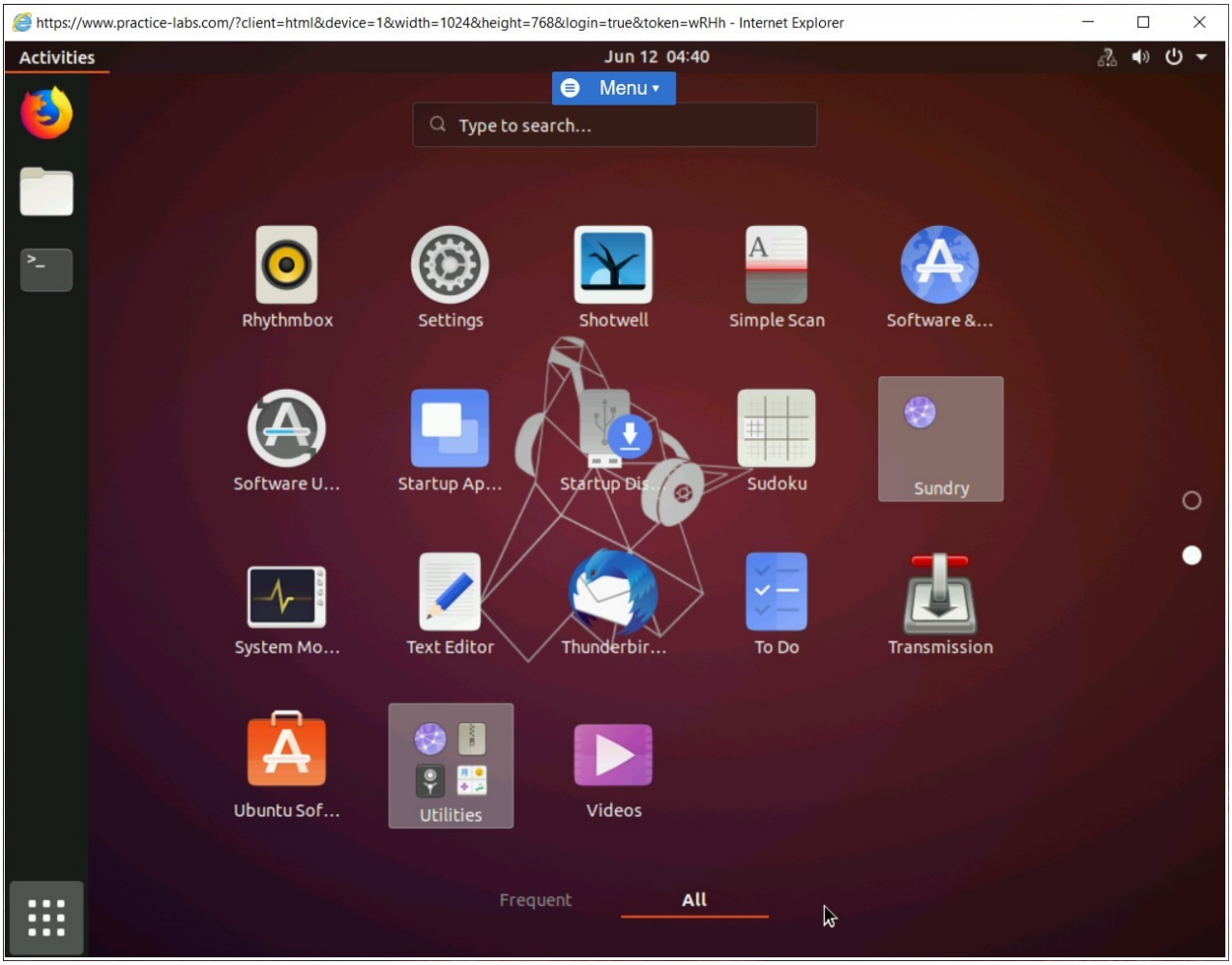


Figure 2.5 Screenshot of PLABLINUX02: Clicking the All button and navigating to the second page.

Step 5

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

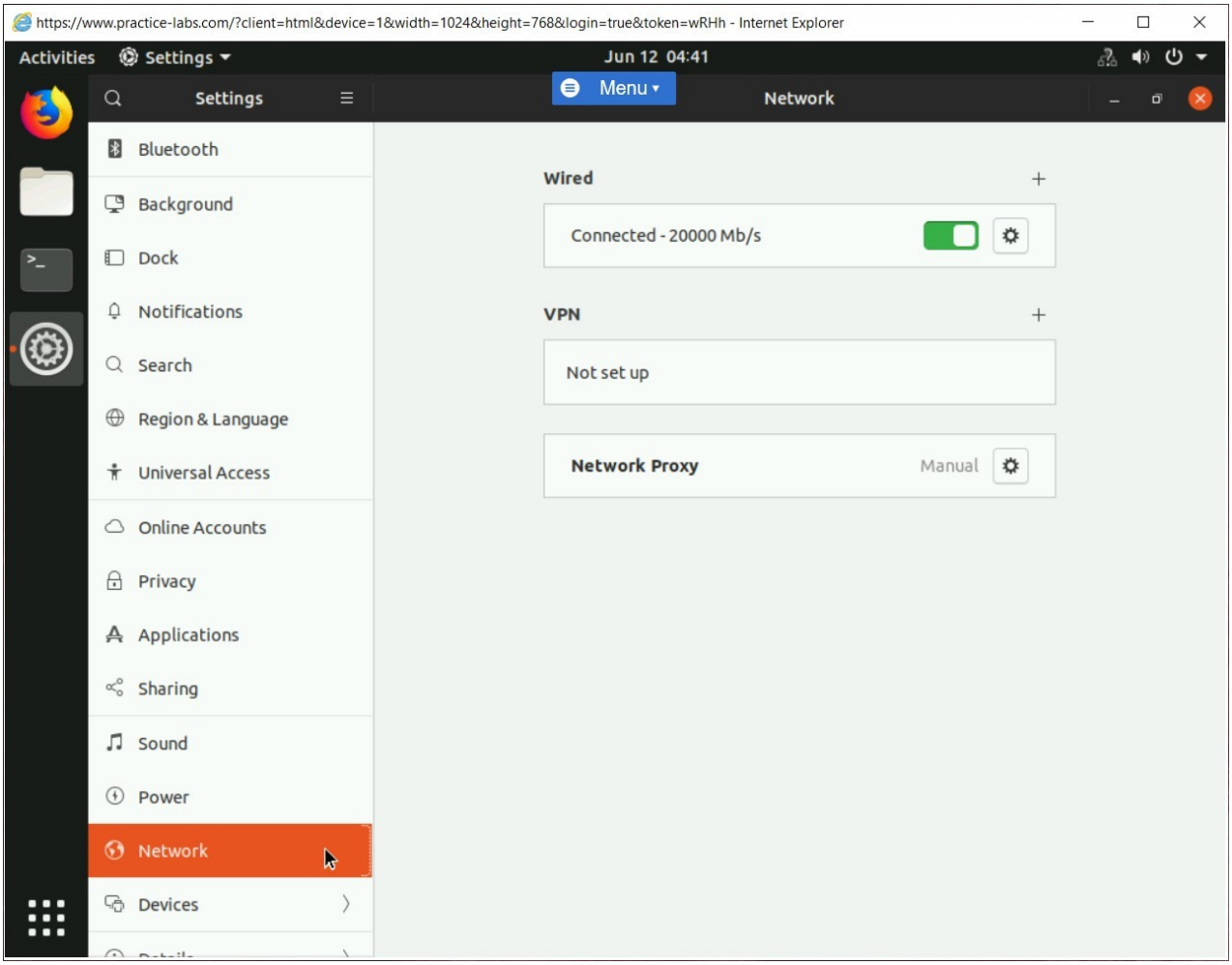


Figure 2.6 Screenshot of PLABLINUX02: Clicking the button to invoke the Wired dialog box.

Step 6

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

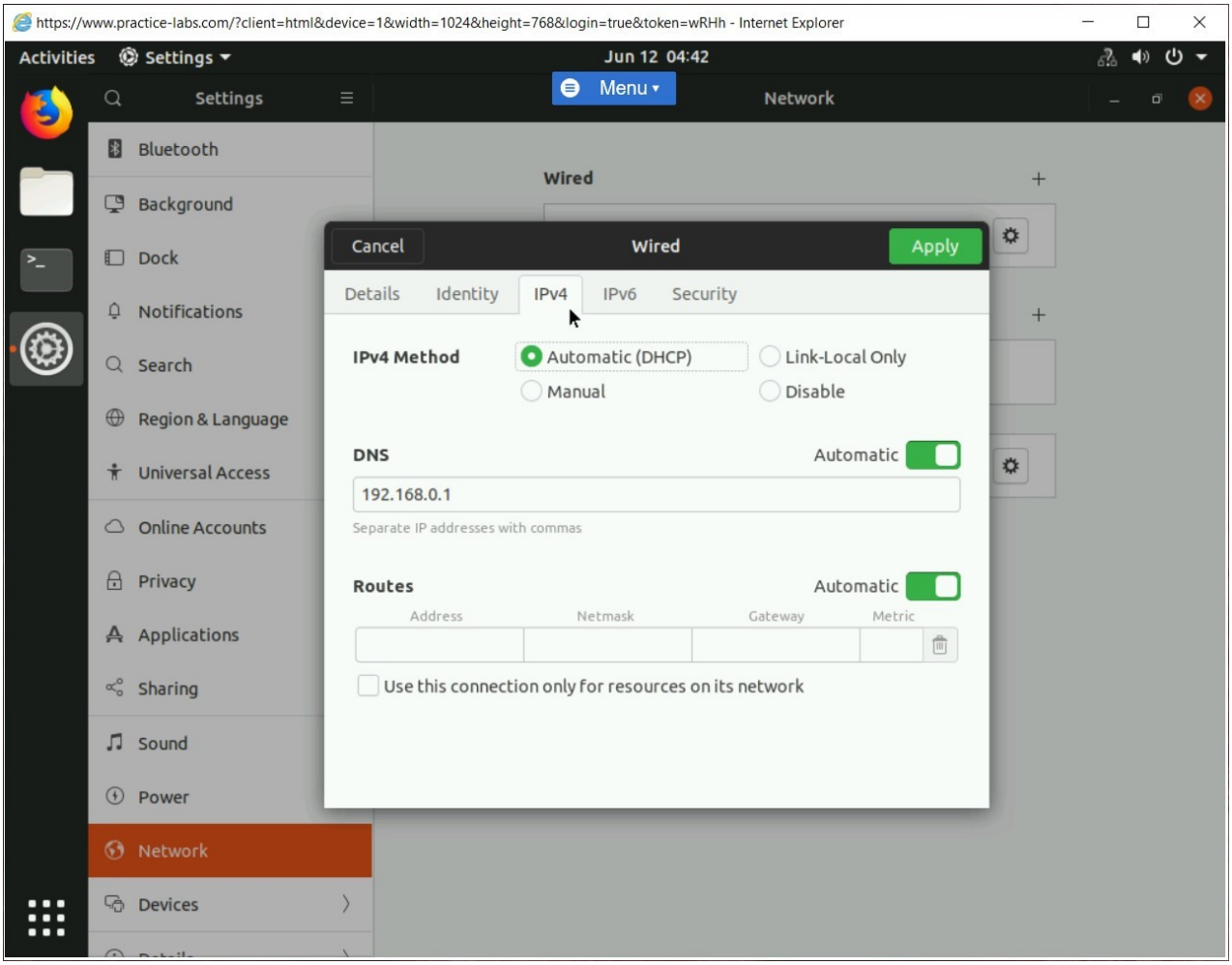


Figure 2.7 Screenshot of PLABLINUX02: Selecting the IPv4 tab in the Wired dialog box.

Step 7

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

Address:

```
192.168.0.3
```

Netmask:

```
255.255.255.0
```

Gateway:

```
192.168.0.250
```

Click **Apply**.

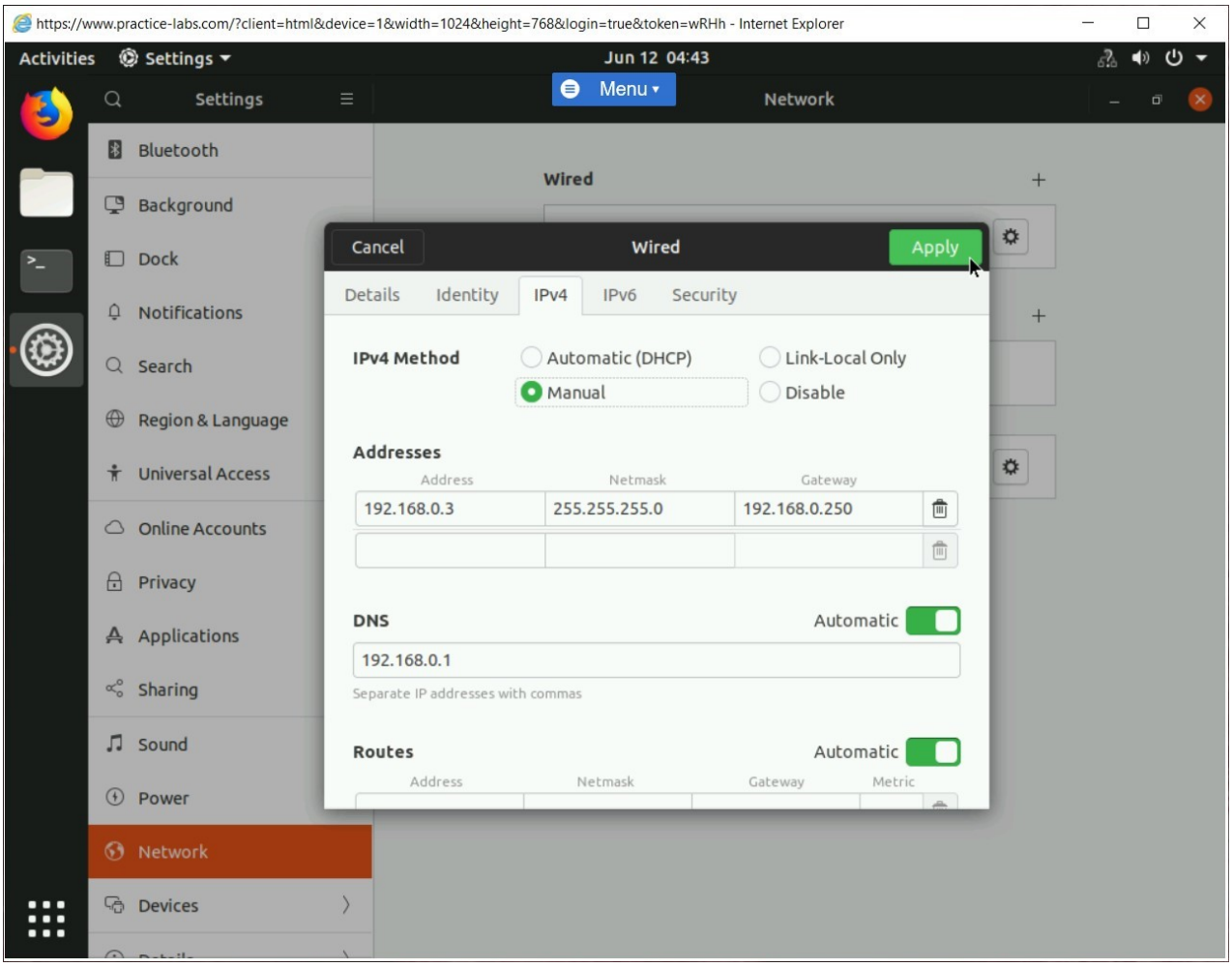


Figure 2.8 Screenshot of PLABLINUX02: Entering the network information and then clicking the Apply button.

Step 8

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

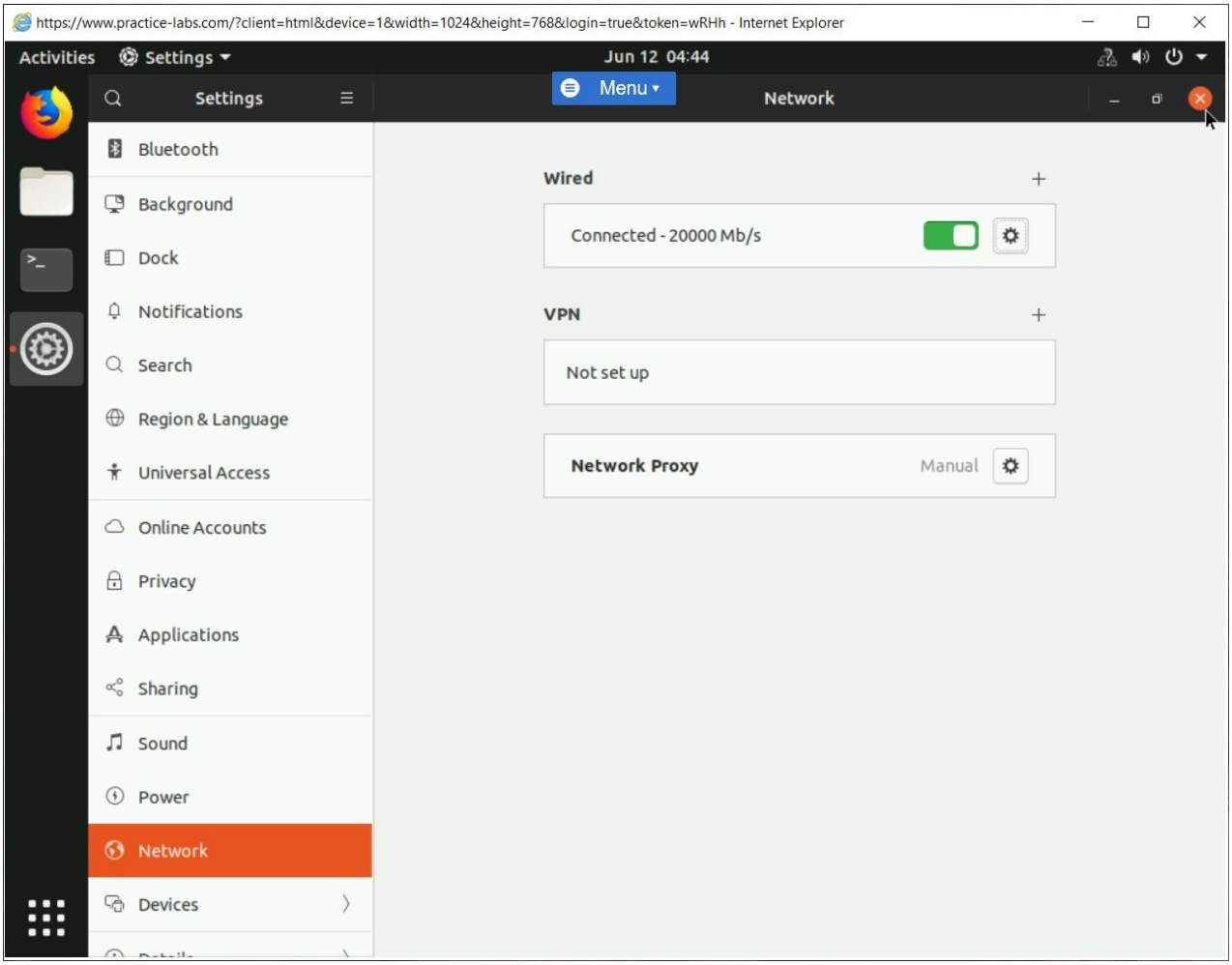


Figure 2.9 Screenshot of PLABLINUX02: Displaying the Settings window.

Task 2 - Install and Configure DenyHosts

Debian packages are operating system and CPU neutral. This means that a Debian package can work with any kind of Debian distribution and CPU type. The extension for Debian packages is **.deb**. In this task, you will install, upgrade, and remove a **gcl** package.

To manage Debian binary packages, perform the following steps:

Step 1

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

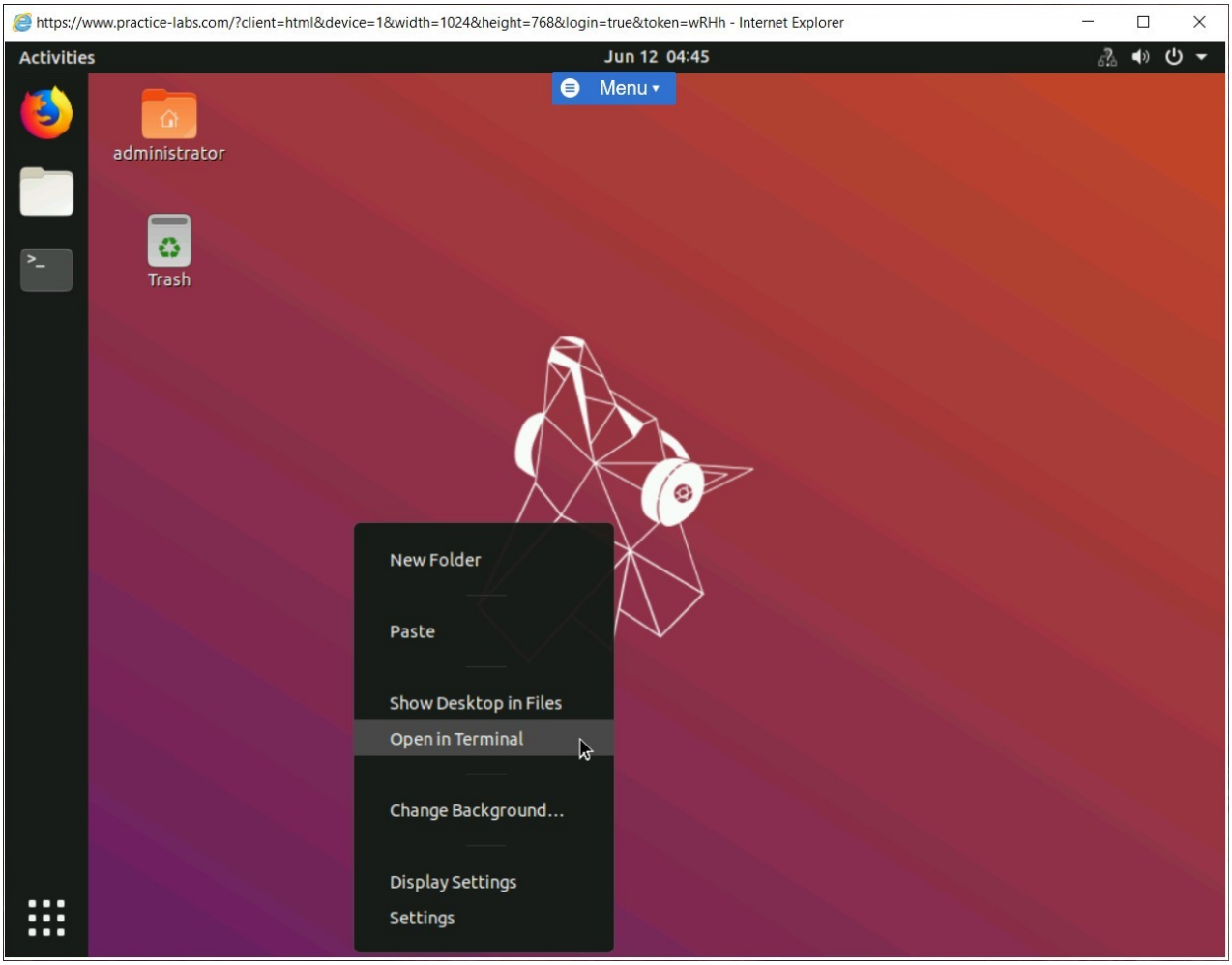


Figure 2.10 Screenshot of PLABLINUX02: Selecting the Open Terminal option from the context menu.

Step 2

You will install DenyHosts on PLABLINUX02. Type the following command:

```
sudo apt-get install denyhosts
```

Press **Enter**.

When prompted, type the following password:

`Passw0rd`

Press **Enter**. The installation will start. You will be prompted for confirmation.

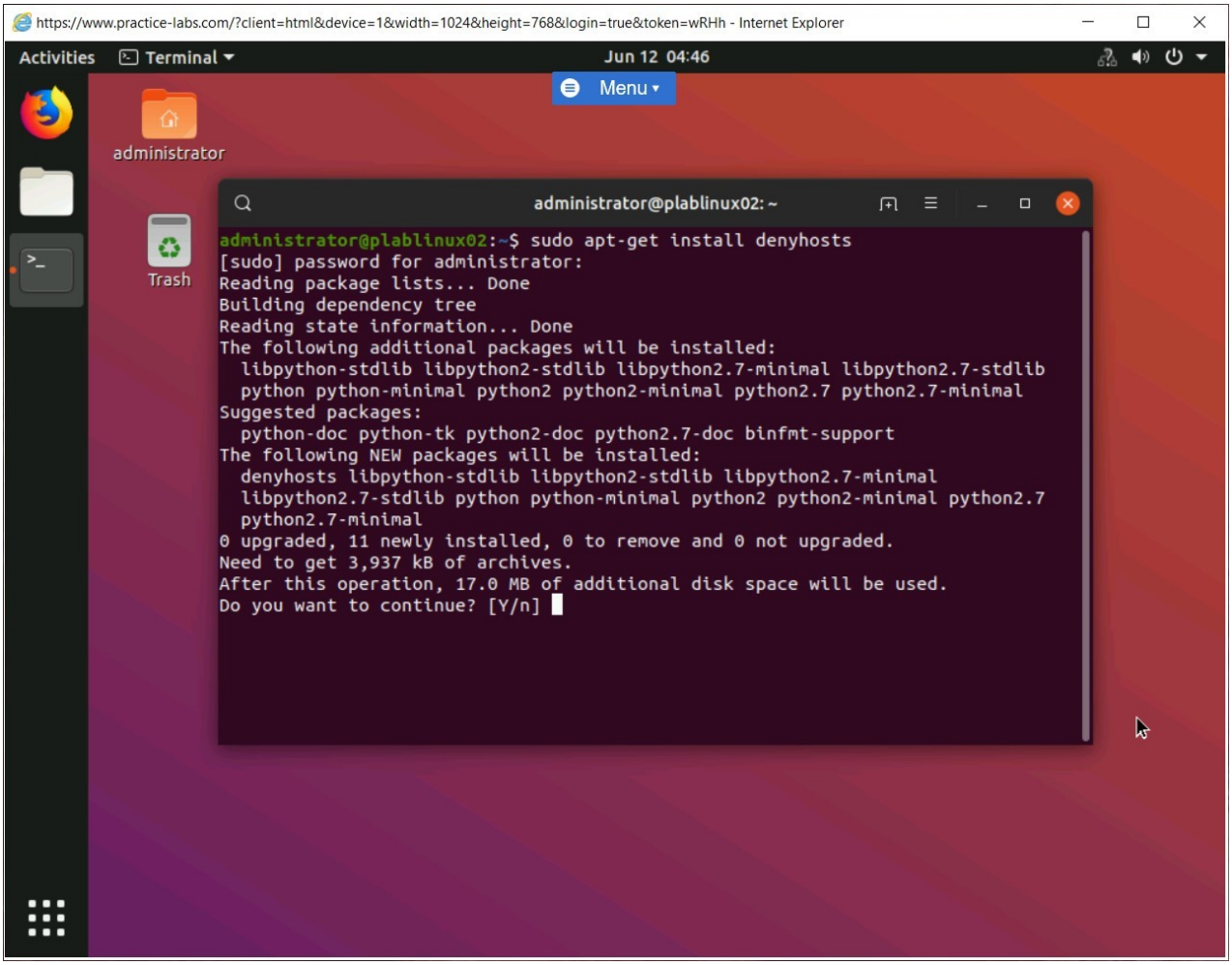


Figure 2.11 Screenshot of PLABLINUX02: Initiating the DenyHosts installation.

Step 3

To confirm the installation, type the following command:

```
Y
```

Press **Enter**. The installation now starts.

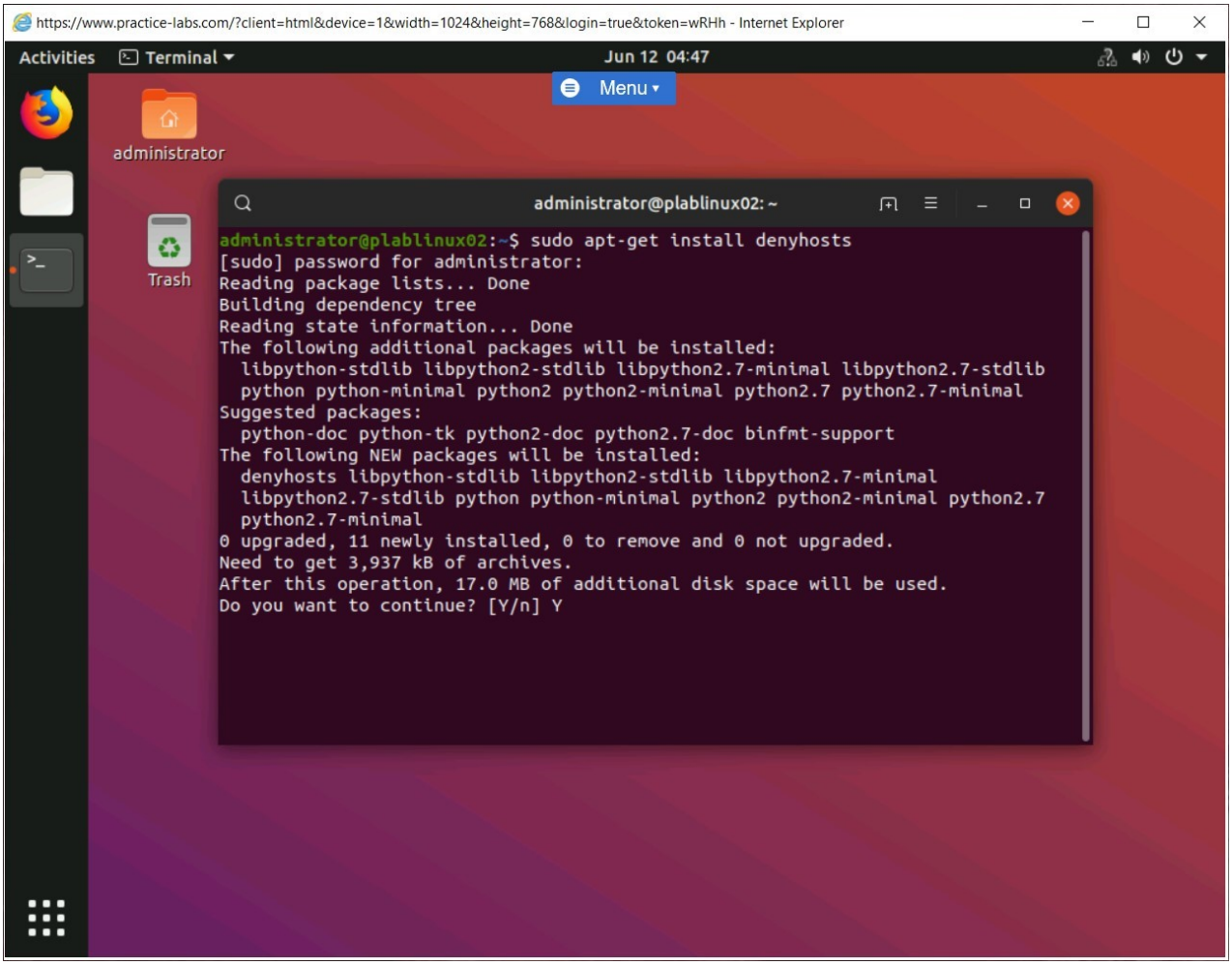


Figure 2.12 Screenshot of PLABLINUX02: Confirming the DenyHosts installation.

Step 4

The installation now starts.

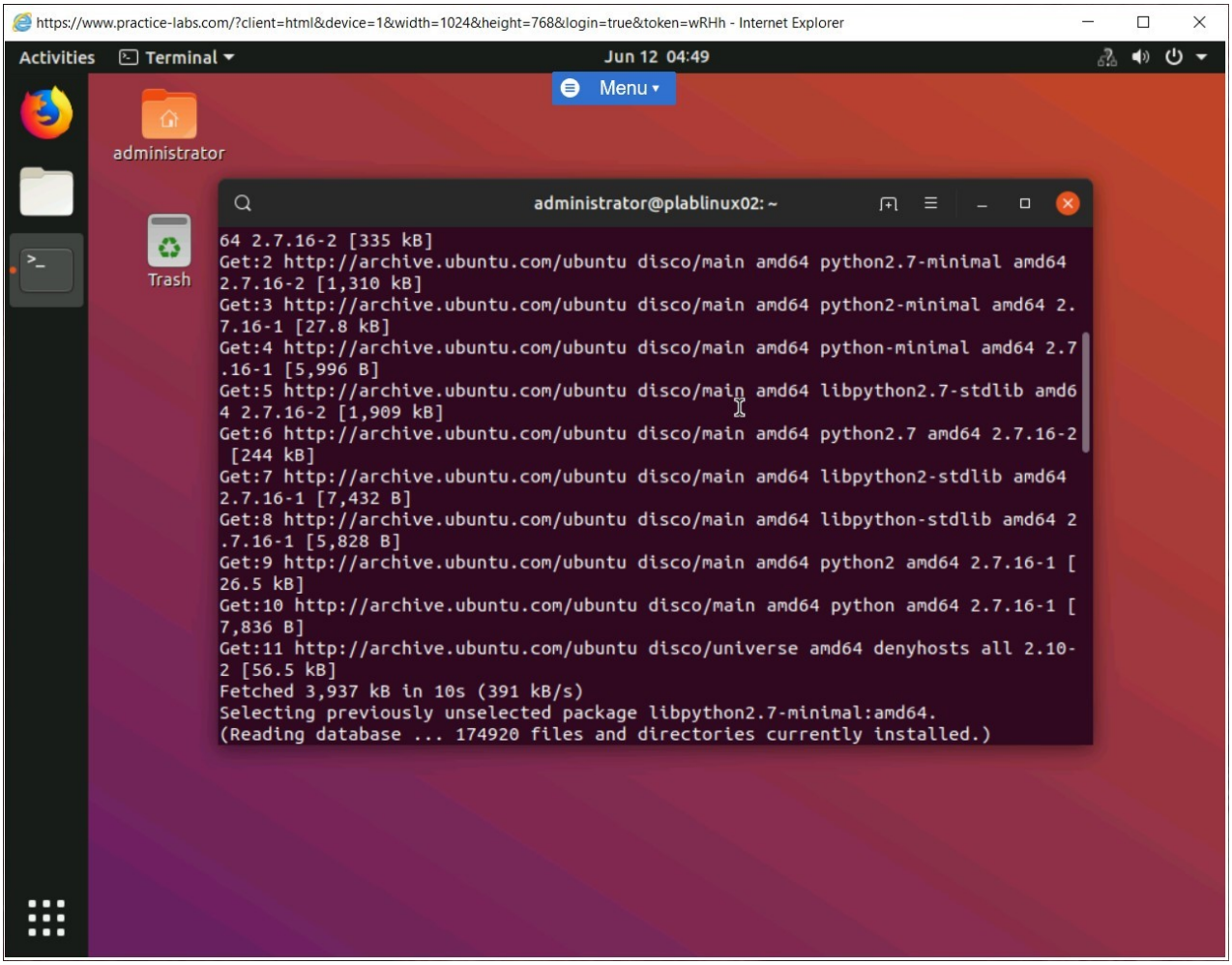


Figure 2.13 Screenshot of PLABLINUX02: Showing the DenyHosts installation progress.

Step 5

After the installation is complete, the command prompt is displayed.

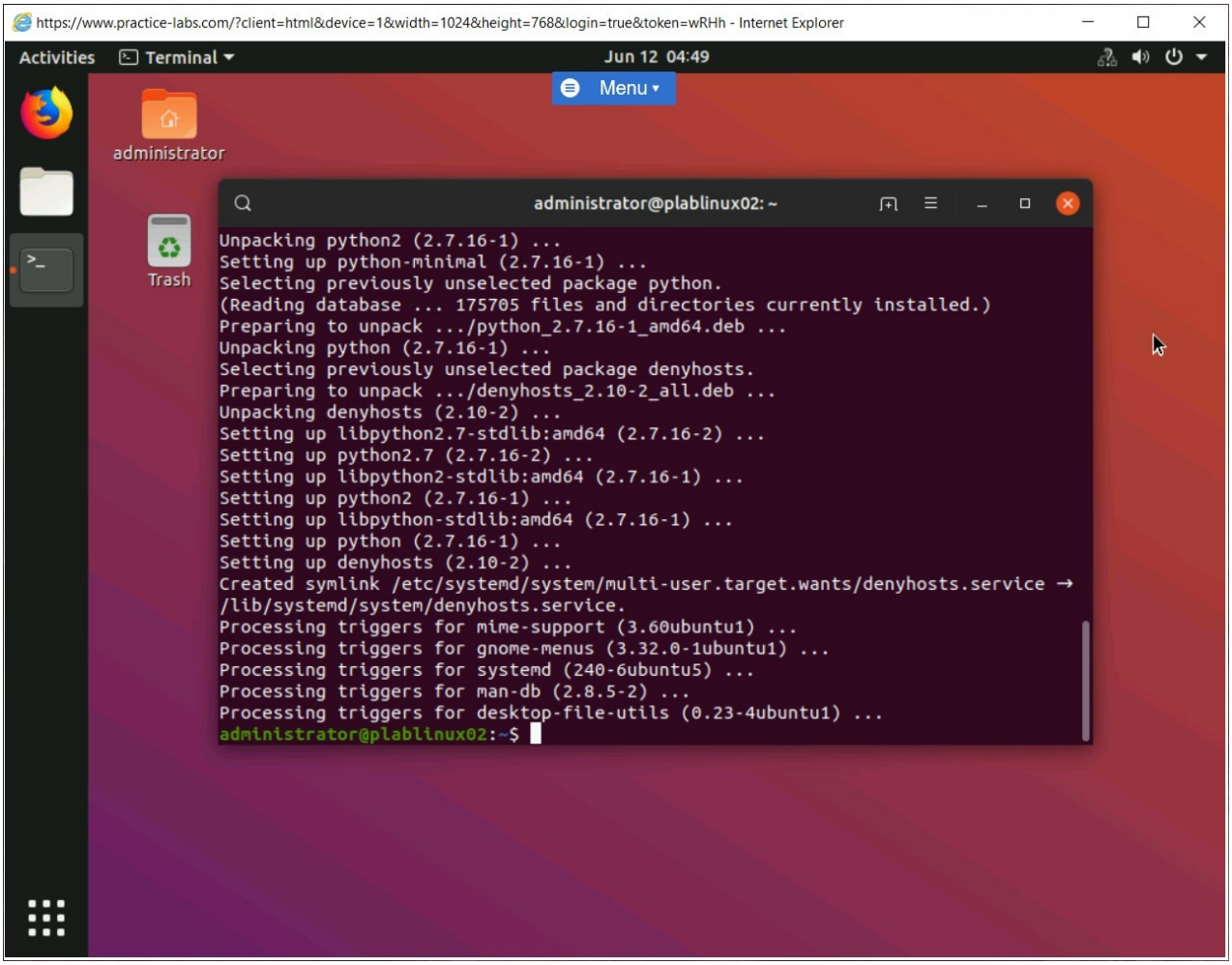


Figure 2.14 Screenshot of PLABLINUX02: Showing the DenyHosts installation completion.

Step 6

Clear the screen by entering the following command:

```
clear
```

Before proceeding ahead, you need to ensure that you whitelist your own IP address, which is **192.168.0.3** in the **/etc/hosts.allow** file. To do this, type the following command:

```
sudo gedit /etc/hosts.allow
```

Press **Enter**.

Note: *If prompted for the password, type Password and press* ***Enter****.*

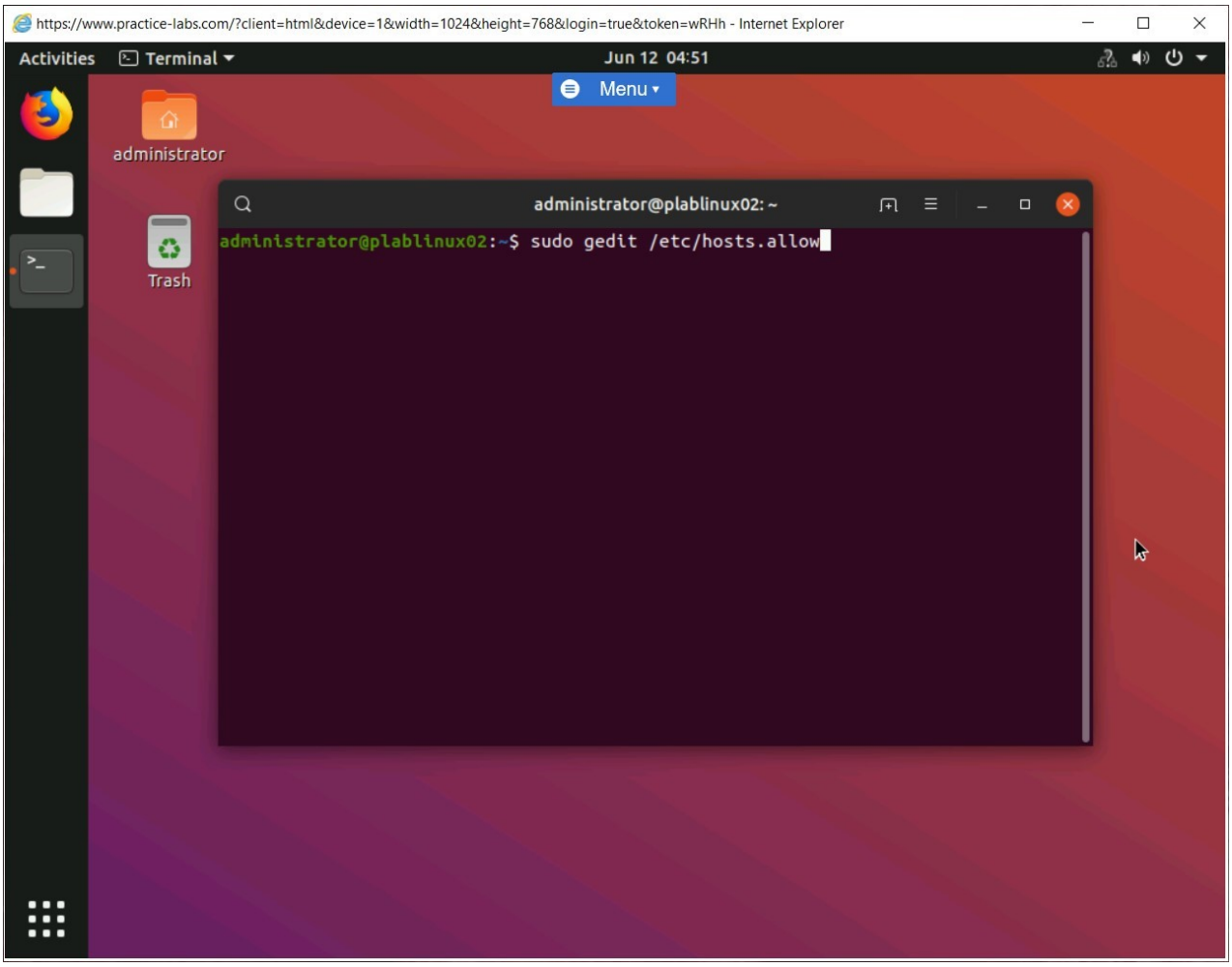


Figure 2.15 Screenshot of PLABLINUX02: Opening the /etc/hosts.allow file for editing.

Step 7

Before proceeding ahead, you need to ensure that you whitelist your own IP address, which is **192.168.0.3** in the **/etc/hosts.allow** file. Also, you can add another IP address, 192.168.0.2, if you want to connect to PLABLINUX02 from this IP address. To do this, type the following command:

```
sshd 192.168.0.3
sshd 192.168.0.2
```

Press **Enter**.

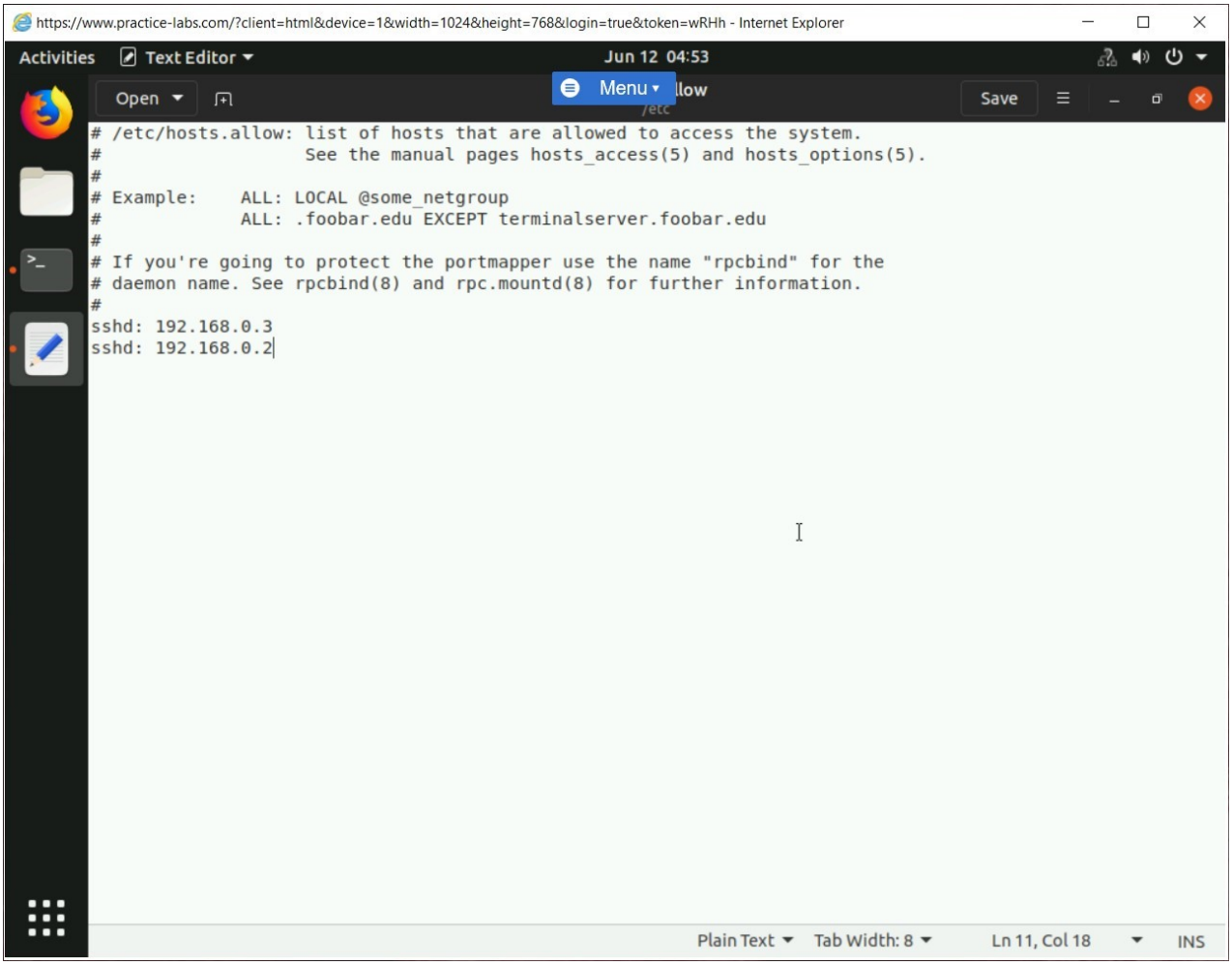


Figure 2.16 Screenshot of PLABLINUX02: Adding the IP addresses to allow SSH connection in the /etc/hosts.allow file.

Step 8

To save the file, click **Save**. Then, close the file.

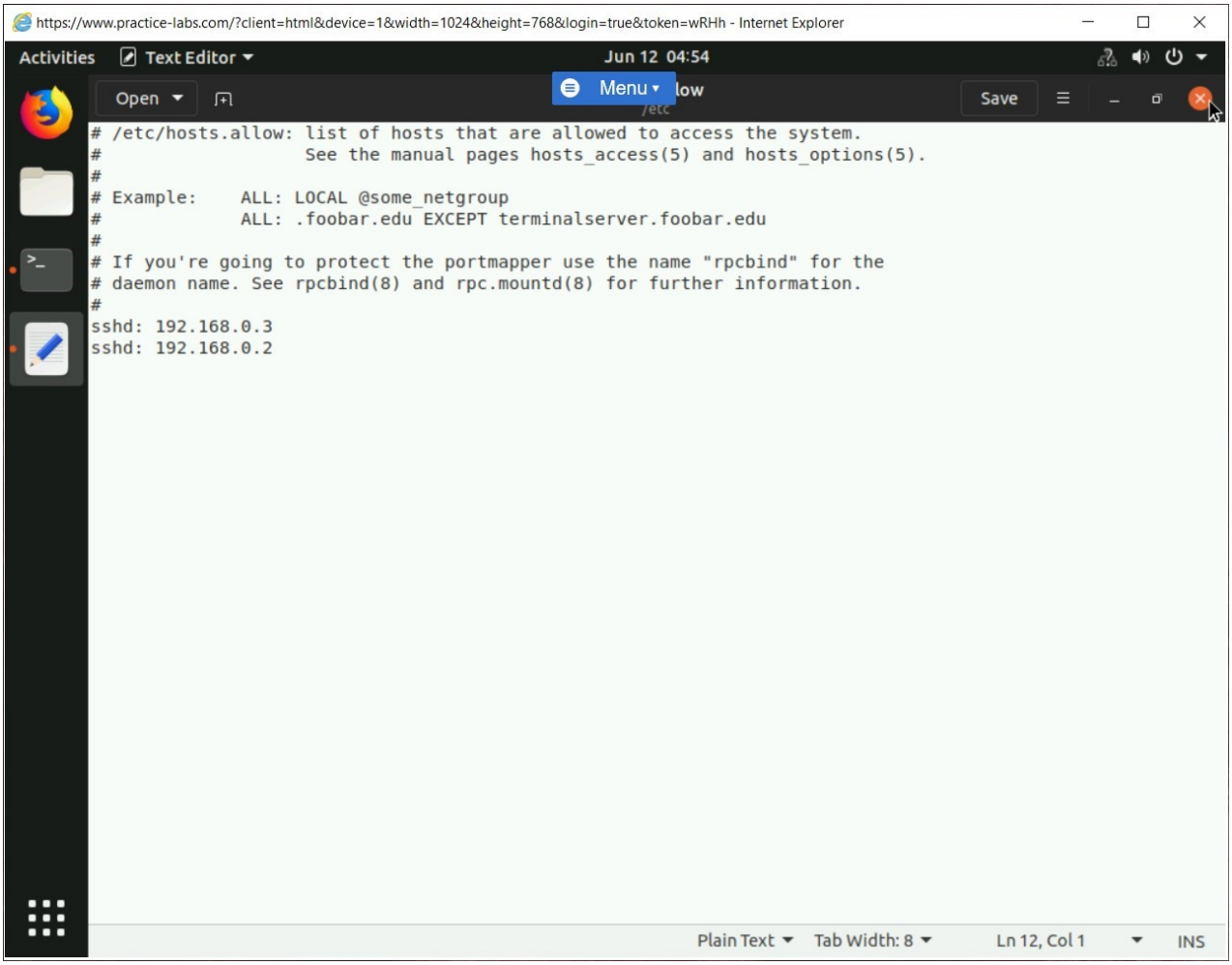


Figure 2.17 Screenshot of PLABLINUX02: Saving and closing the file.

Step 9

You are now back on the terminal window. Clear the screen by entering the following command:

```
clear
```

For the changes to take effect, you need to restart DenyHosts. To do this, type the following command:

```
sudo /etc/init.d/denyhosts restart
```

Press **Enter**.

Note: *If prompted for the password, type Password and press* ***Enter****.*

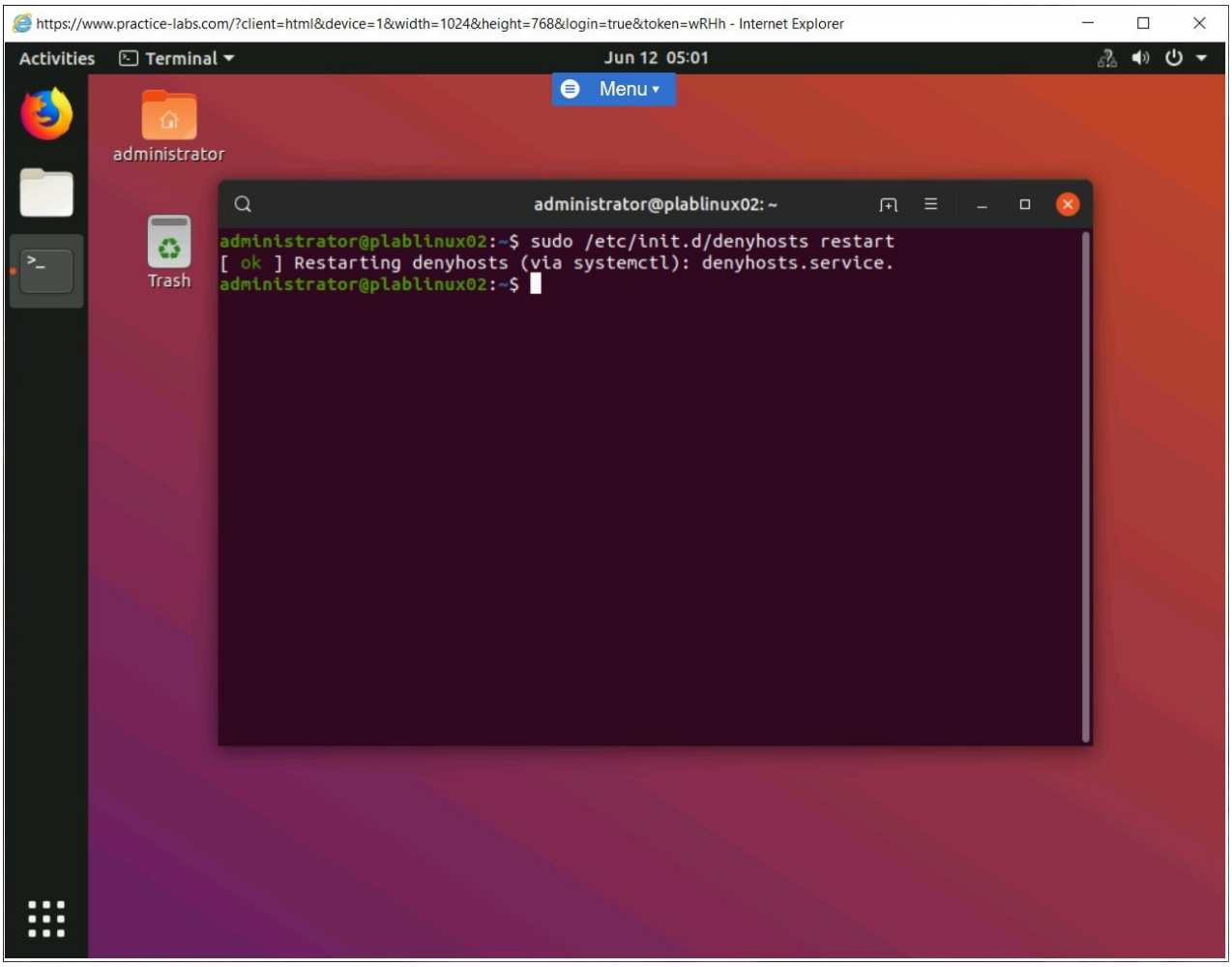


Figure 2.18 Screenshot of PLABLINUX02: Restarting DenyHosts.

Step 10

You should once verify that your own IP address is not in the **/etc/hosts.deny** file. To do this, type the following command:

```
cat /etc/hosts.deny
```

Press **Enter**. Notice that this file currently does not have any IP address listed.

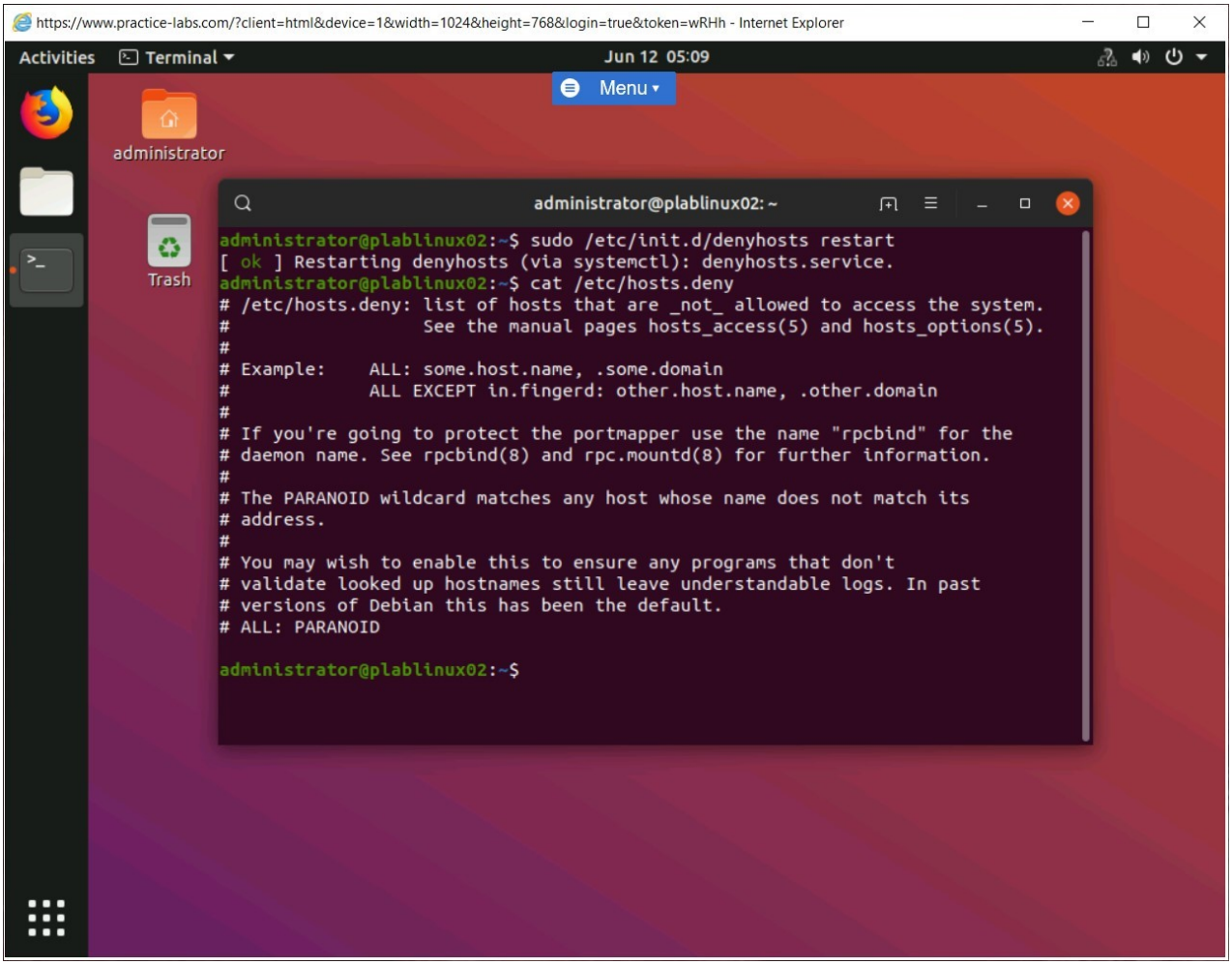


Figure 2.19 Screenshot of PLABLINUX02: Viewing the /etc/hosts.deny file.

Step 11

You are now back on the terminal window. Clear the screen by entering the following command:

```
clear
```

Let's check the status of DenyHosts To do this, type the following command:

```
systemctl status denyhosts
```

Press **Enter**. Press **Ctrl + C** to break the command.

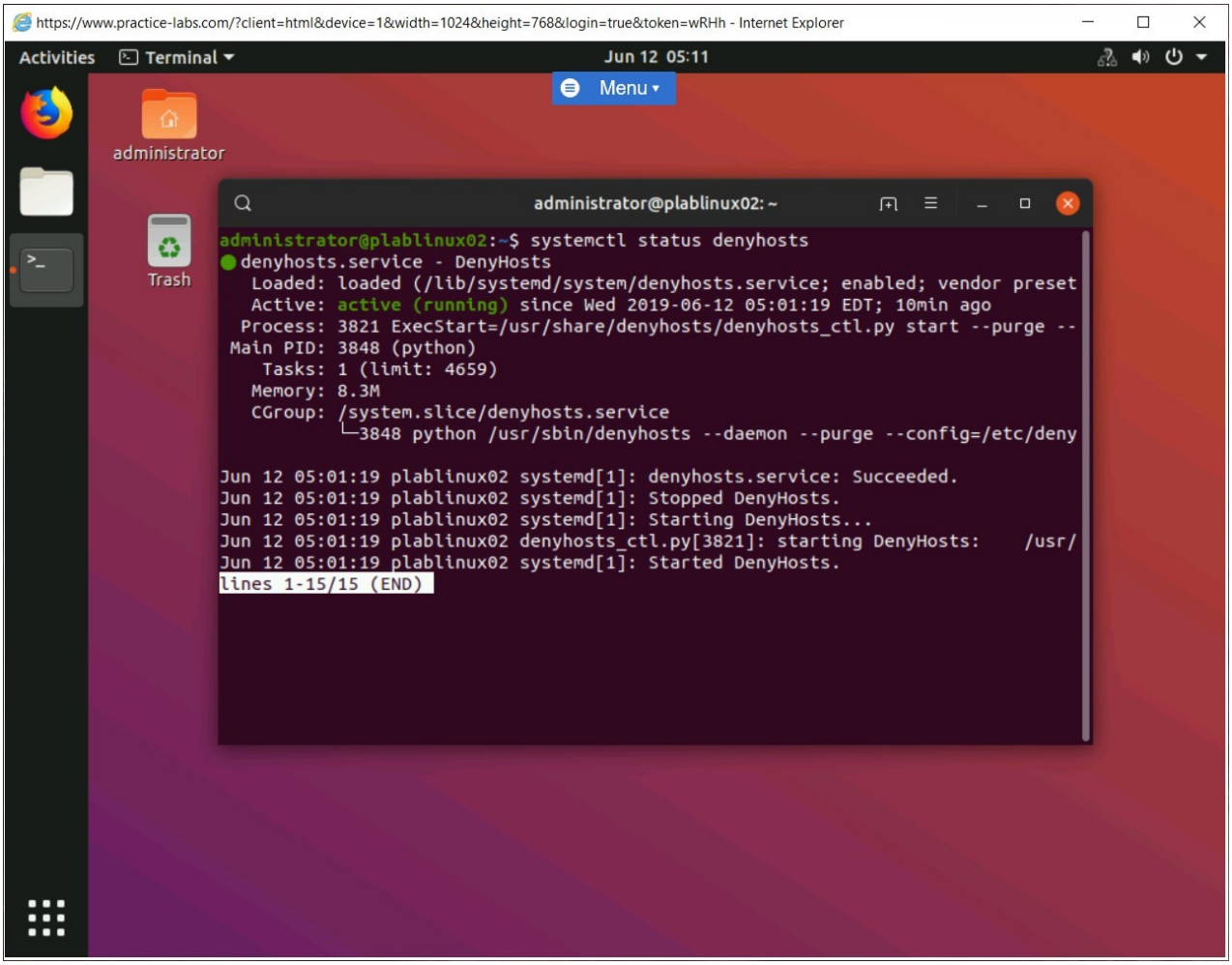


Figure 2.20 Screenshot of PLABLINUX02: Verifying the status of DenyHosts.

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

Review

Well done, you have completed the **Configure UFW and DenyHosts** Practice Lab.

Summary

You completed the following exercises:

- Exercise 1 - Install and Configure UFW
- Exercise 2 - Install and Configure DenyHosts

You should now be able to:

- Configure Network on CentOS
- Install UFW
- Set UFW Default Policy
- Configure Advanced UFW Rules
- Block ICMP Requests
- Reset UFW
- Configure Network on Ubuntu
- Install and Configure DenyHosts

Feedback

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