CompTIA Linux+

Securing Data with Encryption

Introduction

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

Data
Encryption
OpenSSH
GnuPG

Learning Outcomes

In this module, you will complete the following exercise:

- Exercise 1 - Securing Data with Encryption

After completing this lab, you will be able to:

- Perform Basic OpenSSH 2 client configuration and usage
- Understand the role of OpenSSH 2 server host keys
- Perform basic GnuPG management

Exam Objectives

The following exam objectives are covered in this lab:

- **LPI:** 110.3 Securing data with encryption

- **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.

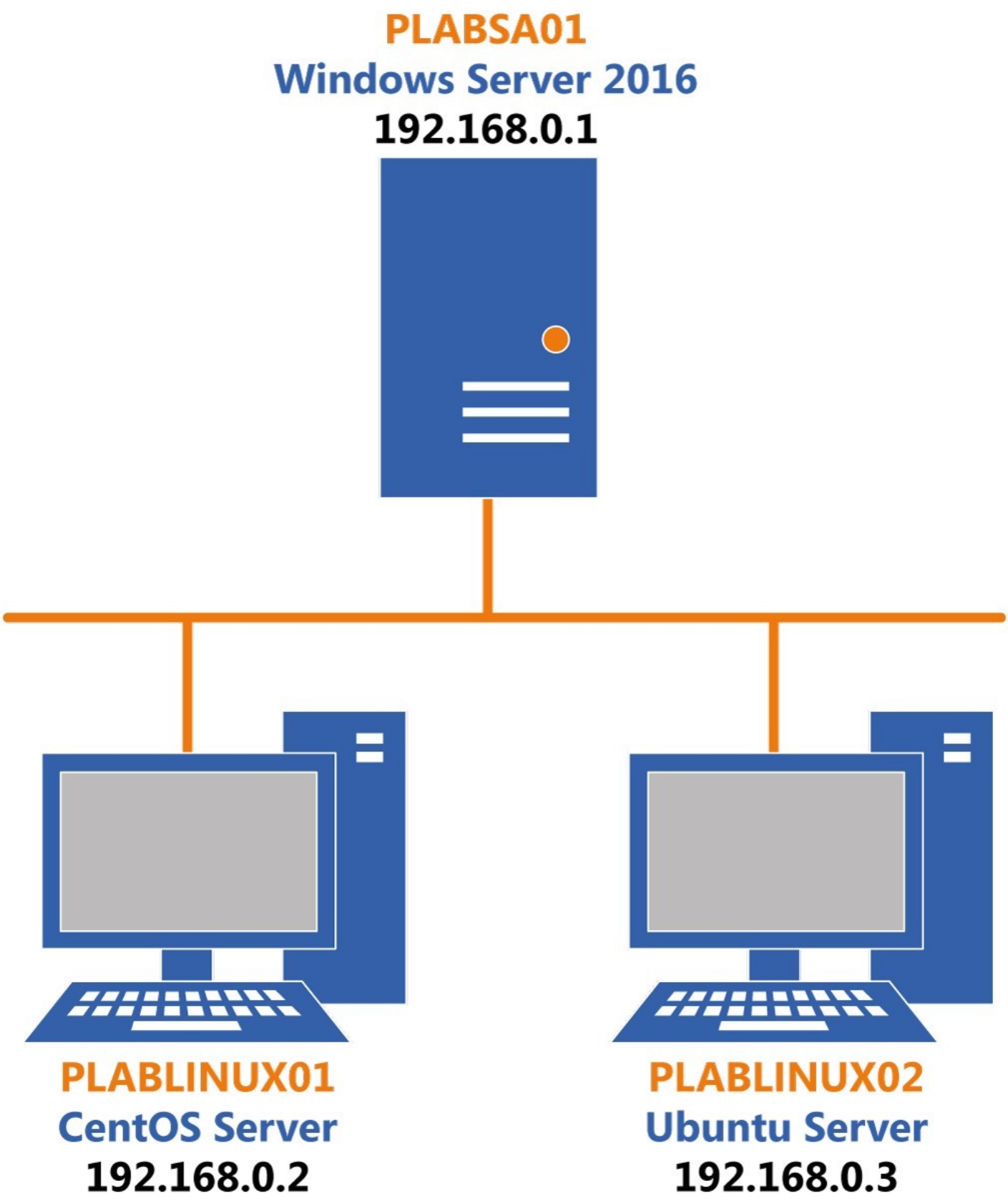
Help and Support

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 - Securing Data with Encryption

Encryption is one of the most effective and most popular techniques to ensure data security. Plain data is processed with a secret key to produce encrypted data, also known as cipher data. To read encrypted data, you must decrypt the data using the relevant secret key. In this exercise, you will understand how to secure data with encryption.

Learning Outcomes

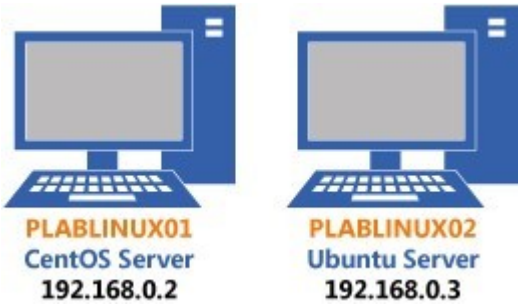
After completing this exercise, you will be able to:

- Log into a Linux System
- Perform Basic OpenSSH 2 client configuration and usage
- Understand the role of OpenSSH 2 server host keys
- Perform basic GnuPG management

Your Devices

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

- **PLABLINUX01** (CentOS Server)
- **PLABLINUX02** (Ubuntu Server)



Task 1 - Basic OpenSSH 2 Client Configuration and Usage

SSH, short for secure shell, is a replacement for the remote connectivity programs, such as telnet and rlogin. Both these programs used to send unencrypted traffic from the host machine to the recipient machine. SSH, on the other hand, sends only

encrypted traffic. SSH implementation in Linux is called **OpenSSH**. In this task, you will view the basic configuration files for the ssh server and client.

To understand basic Open SSH2 client configuration and usage, perform the following steps:

Step 1

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

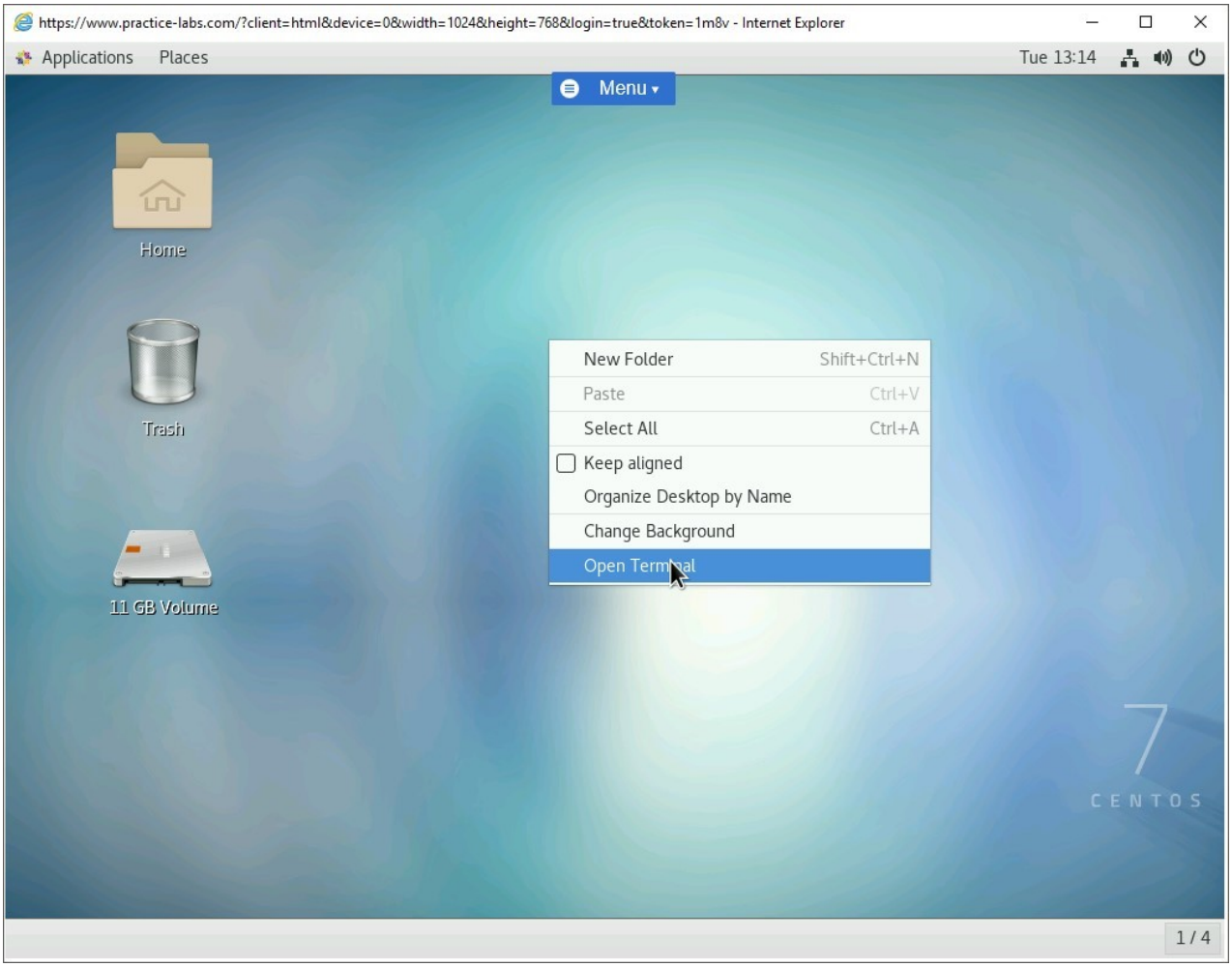


Figure 1.1 Screenshot of PLABLINUX01: Selecting the Open Terminal option from the context menu.

Step 2

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

```
su -
```

Press **Enter**.

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

`Passw0rd`

Press **Enter**.

Step 3

Clear the screen by entering the following command:

```
clear
```

The OpenSSH configuration is stored in two different files:

- Server configuration in sshd_config
- client configuration in ssh_config

Both these files are stored in the **/etc/ssh** directory.

To list both these files in the **/etc/ssh** directory, type the following command:

```
ls -l /etc/ssh/ssh*
```

Press **Enter**.

Notice that the first two files listed are **ssh_config** and **sshd_config**.

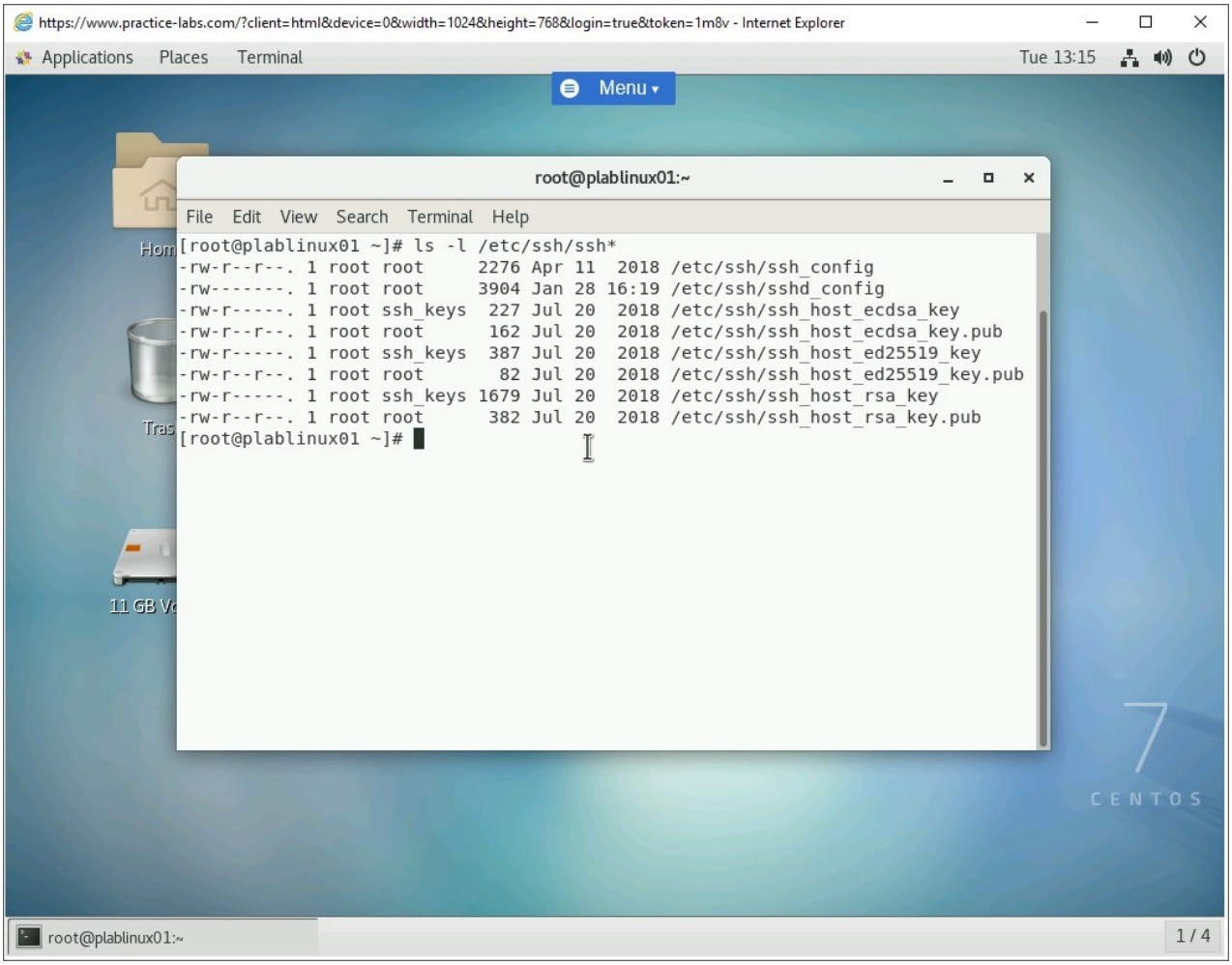


Figure 1.2 Screenshot of PLABLINUX01: Listing the files in the /etc/ssh directory.

Step 4

Clear the screen by entering the following command:

```
clear
```

To view the server configuration file, type the following command:

```
cat /etc/ssh/sshd_config
```

Press **Enter**.

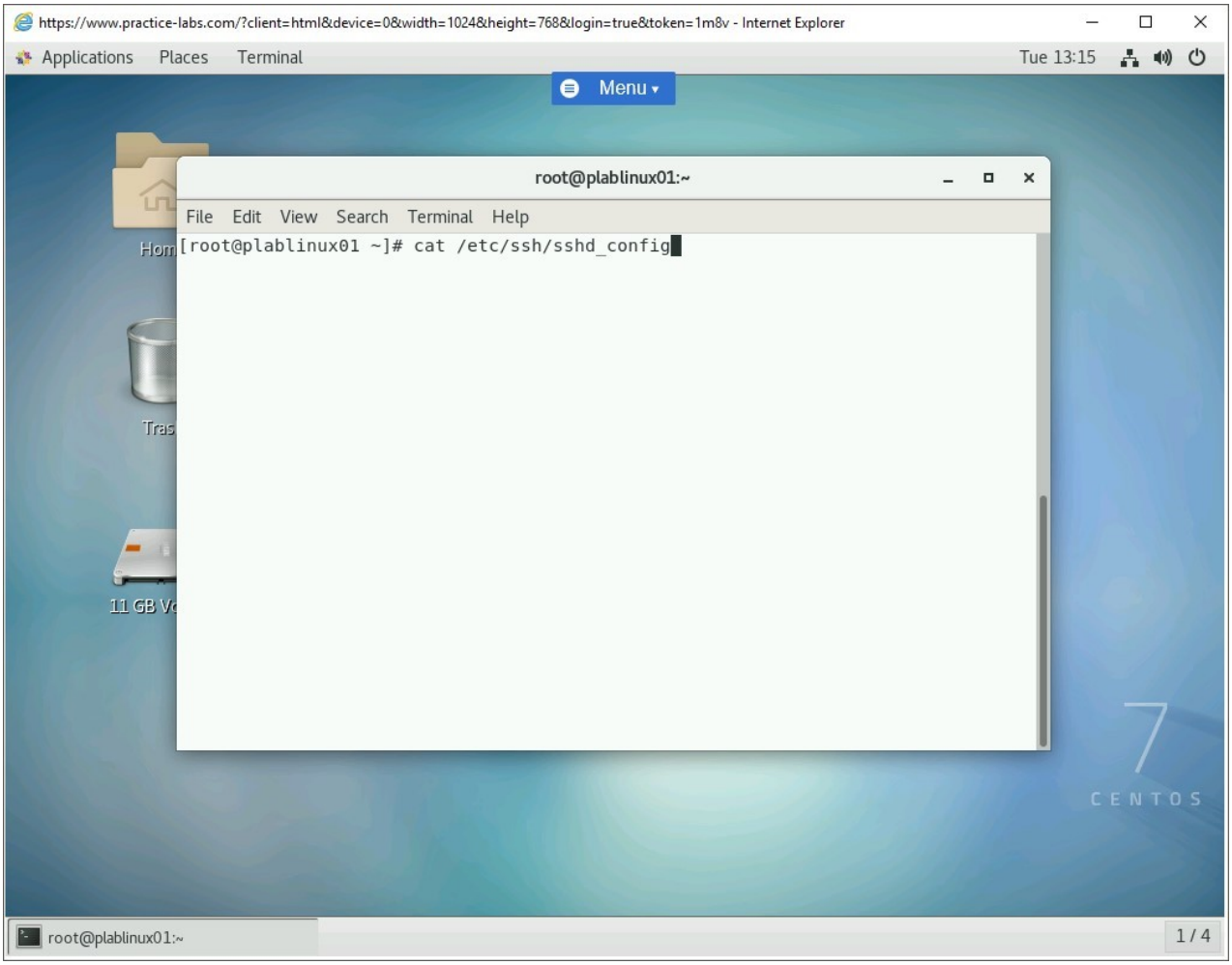


Figure 1.3 Screenshot of PLABLINUX01: Viewing the server configuration file.

Step 5

The output of the file is shown.

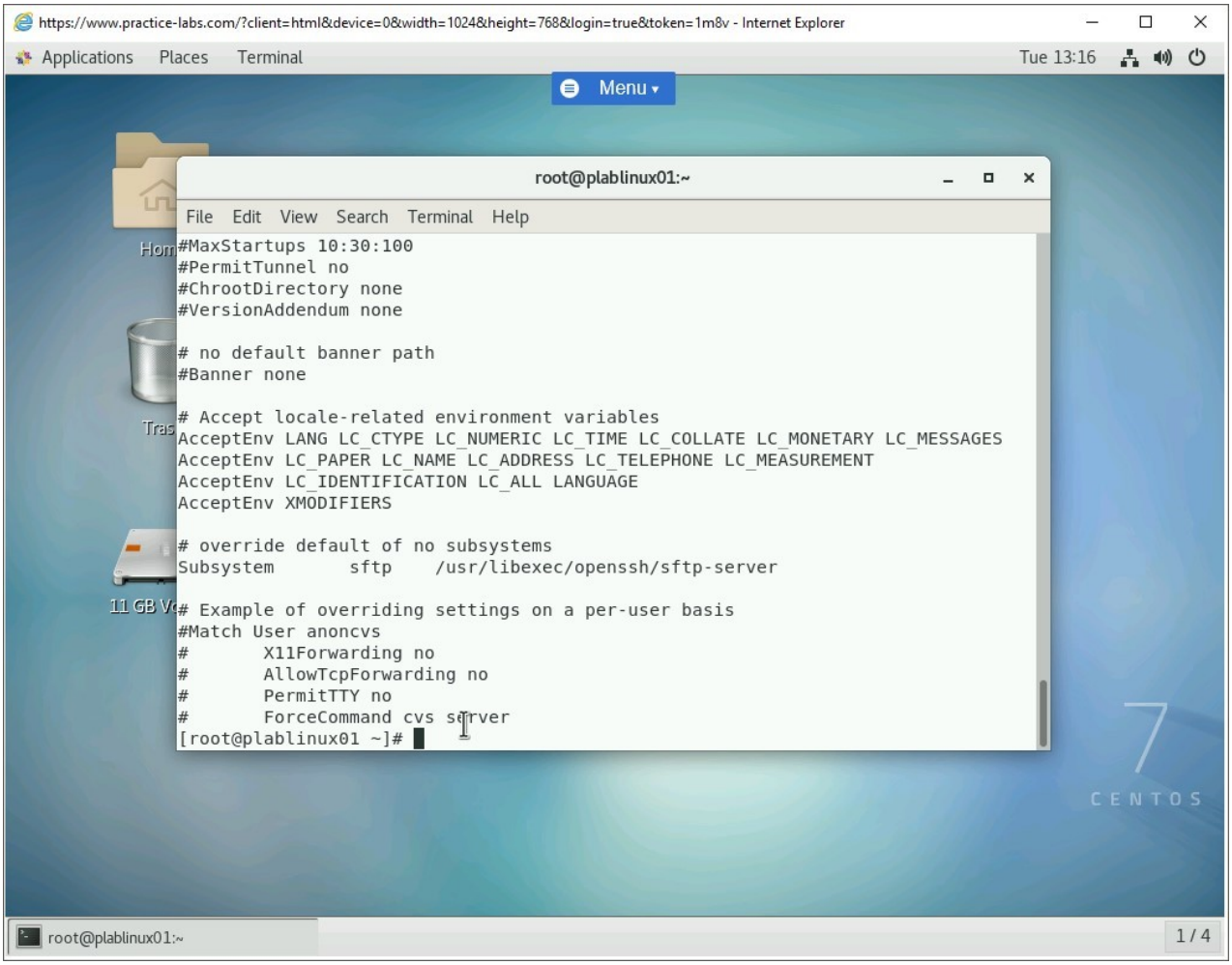


Figure 1.4 Screenshot of PLABLINUX01: Showing the output of the server configuration file.

Step 6

Clear the screen by entering the following command:

```
clear
```

To view the client configuration file, type the following command:

```
cat /etc/ssh/ssh_config
```

Press **Enter**.

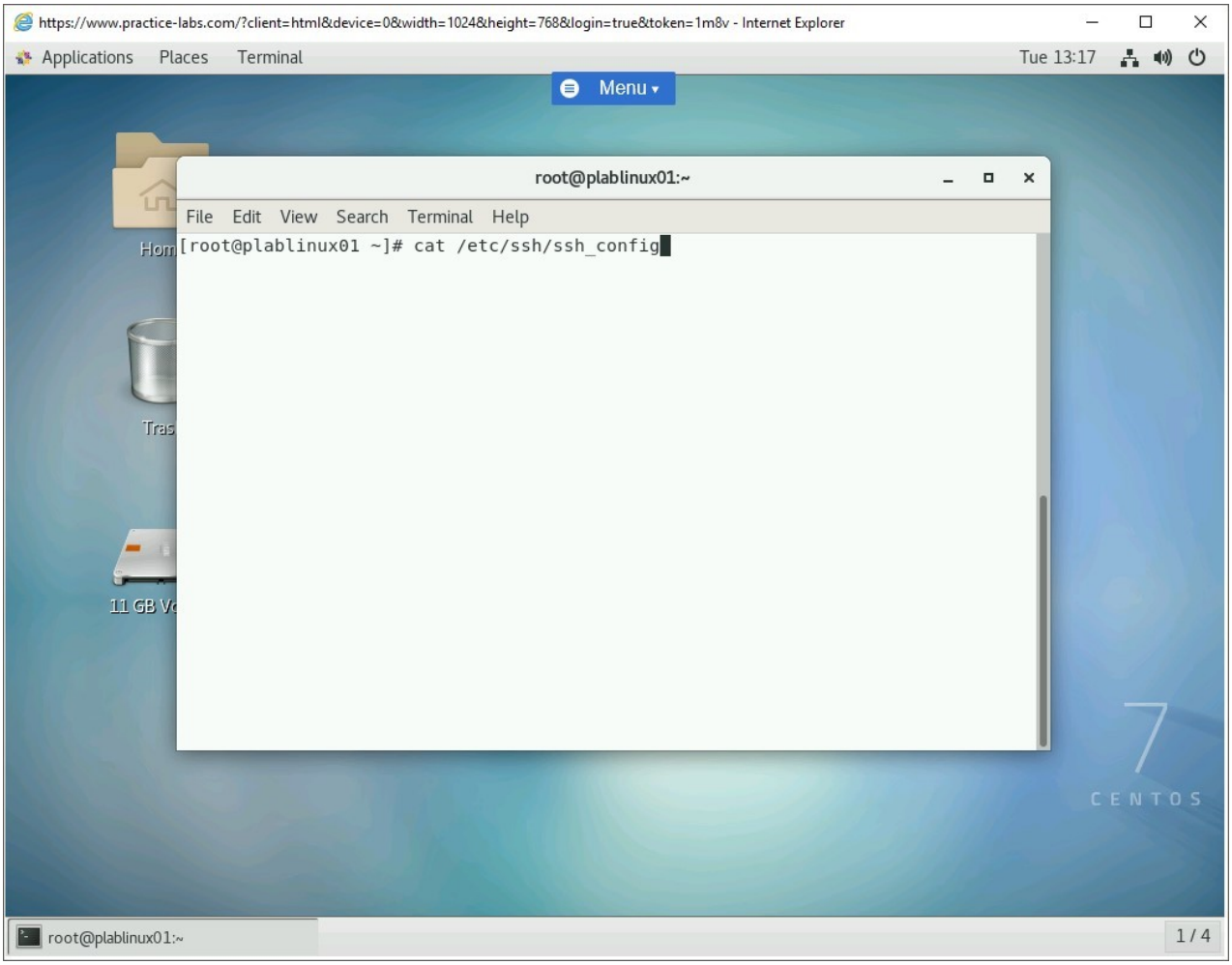


Figure 1.5 Screenshot of PLABLINUX01: Viewing the client configuration file.

Step 7

The output of the file is shown.

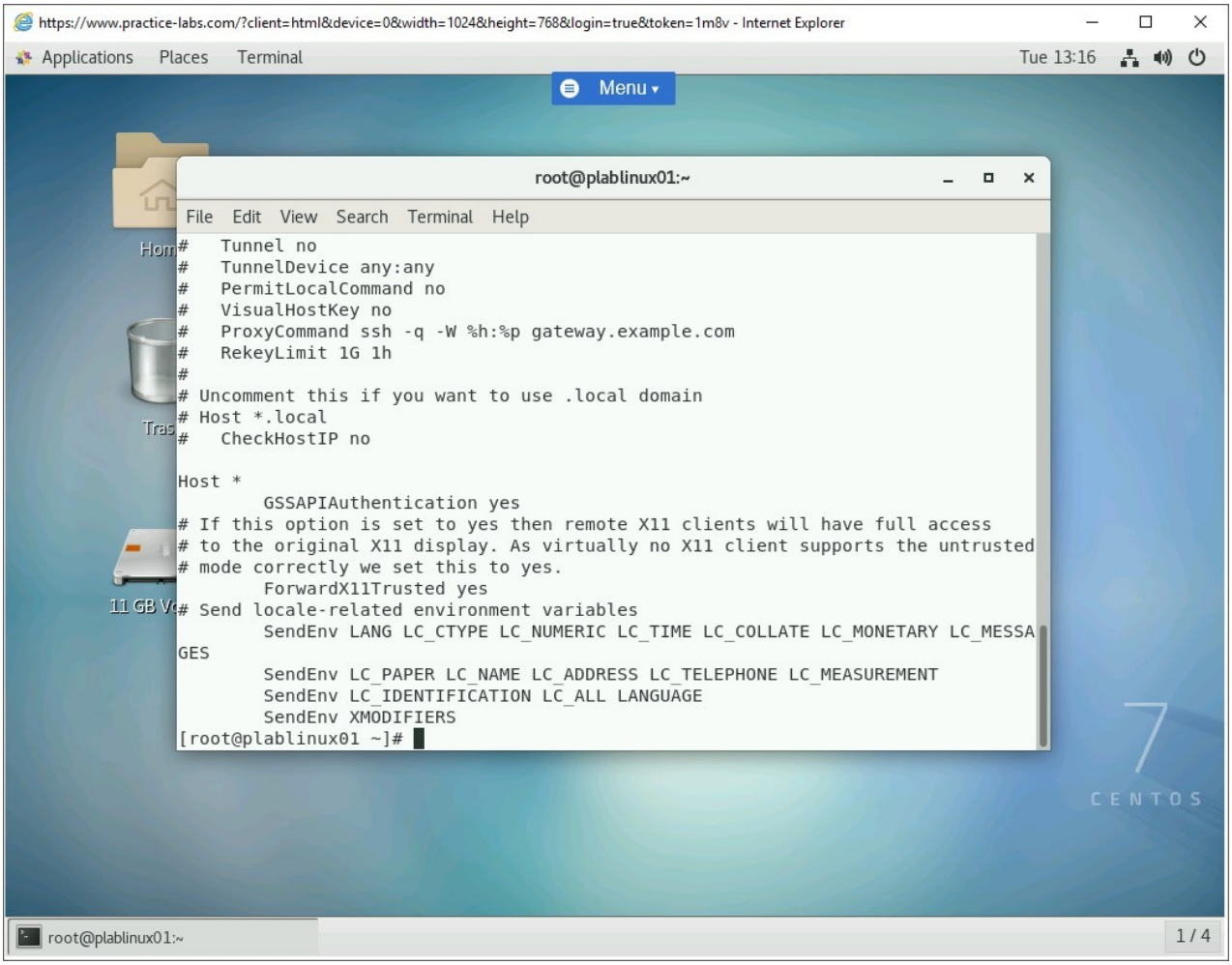


Figure 1.6 Screenshot of PLABLINUX01: Showing the client configuration file.

Task 2 - Role of OpenSSH 2 Server Host Keys

You should generate SSH keys for the login accounts that you use in the Linux environment. You can use the ssh-keygen to generate the keys, which are then stored in **~/.ssd**. In this task, you will generate the public and private keys and then copy them onto a remote system. To generate the keys, perform the following steps:

Step 1

Clear the screen by entering the following command:

```
clear
```

To generate the keys, type the following command:

```
ssh-keygen -t dsa
```

Press **Enter**.

> ***Note**: In the command above, you can either use **dsa** or **rsa**.*

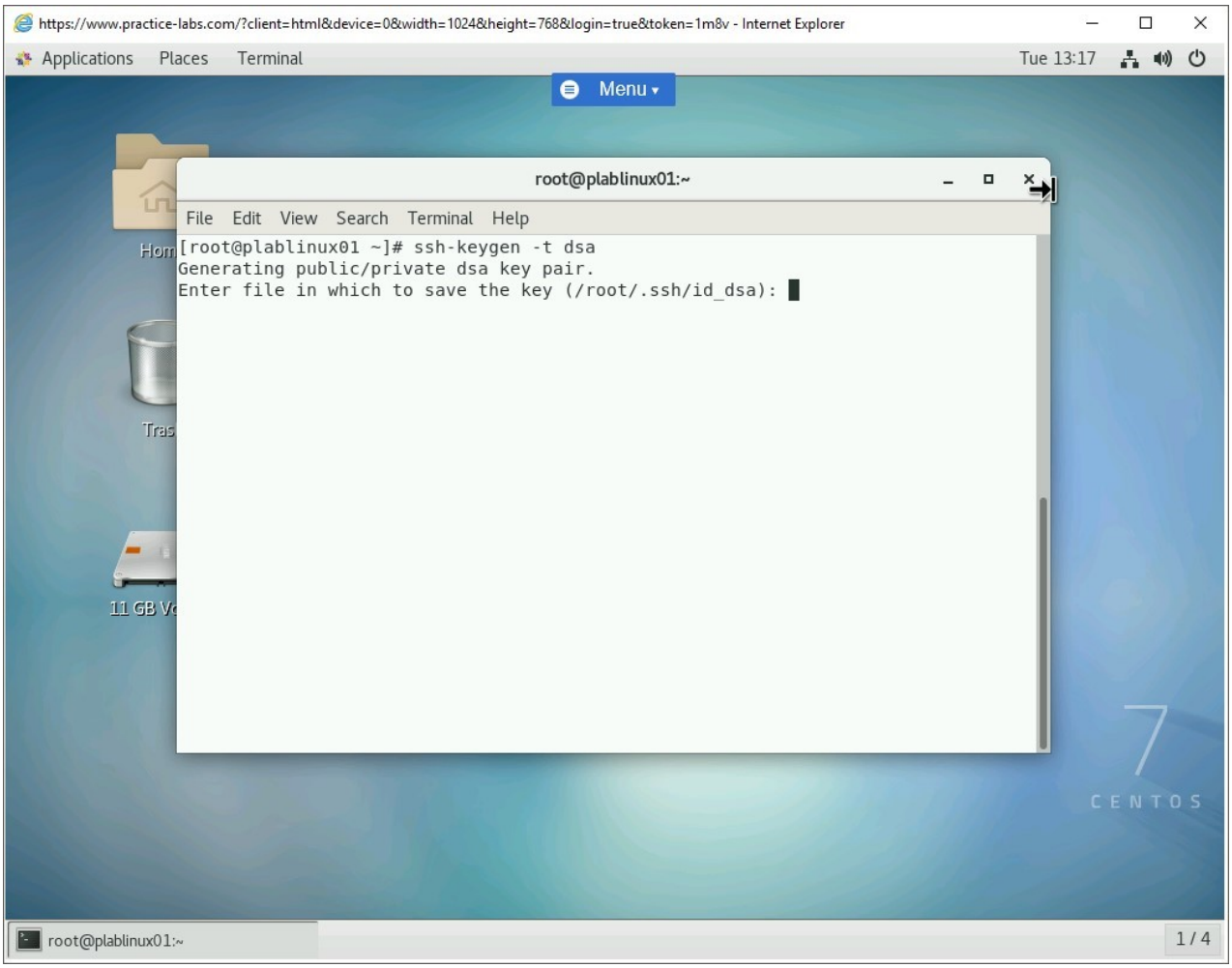


Figure 1.7 Screenshot of PLABLINUX01: Generating the keys.

Step 2

When prompted, press **Enter** to use the default file.

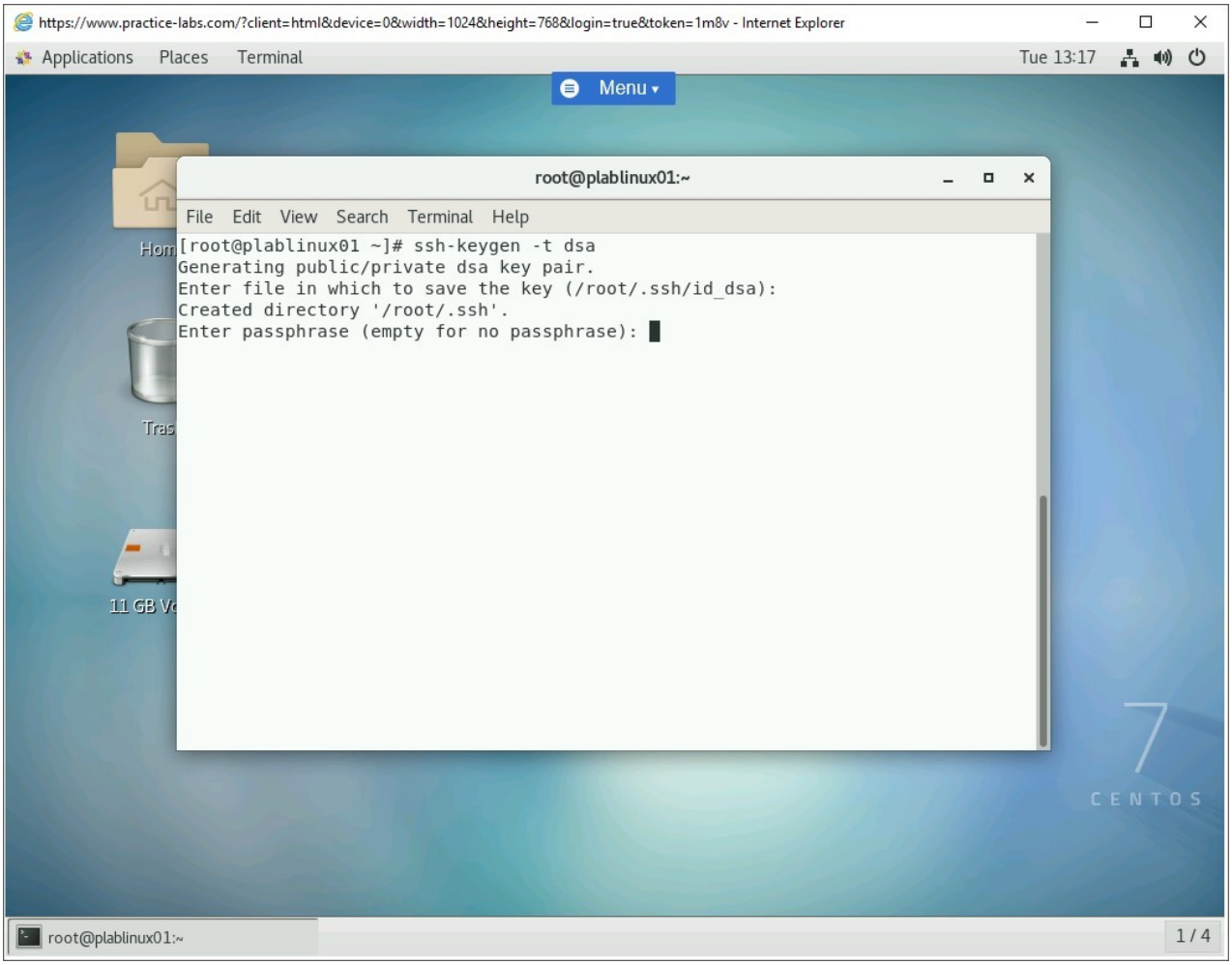


Figure 1.8 Screenshot of PLABLINUX01: Pressing Enter to use the default file.

Step 3

When prompted for a password and confirm the password, type the following password:

`Passw0rd`

Note that the keys are generated.

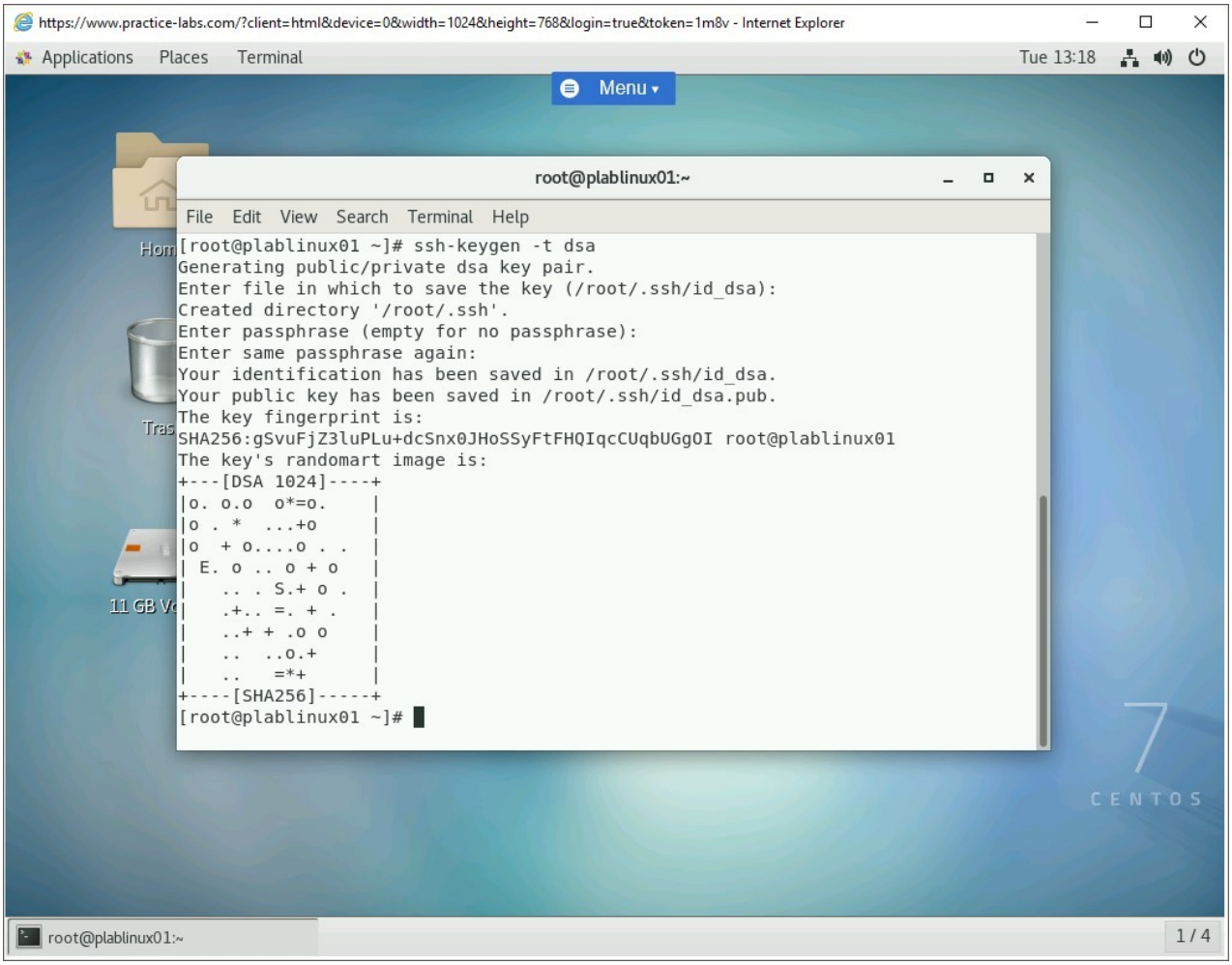


Figure 1.9 Screenshot of PLABLINUX01: Entering and confirming the password.

Step 4

Clear the screen by entering the following command:

```
clear
```

Verify that the public and private keys have been generated. Type the following command:

```
ls -l ~/.ssh/
```

Press **Enter**.

Note that the **id_dsa** (which is the private key) and **id_dsa.pub** (which is the public key) are generated.

> ***Note**: If you use **rsa** instead of **dsa**, the file names will be **id_rsa** and **id_rsa.pub**.*

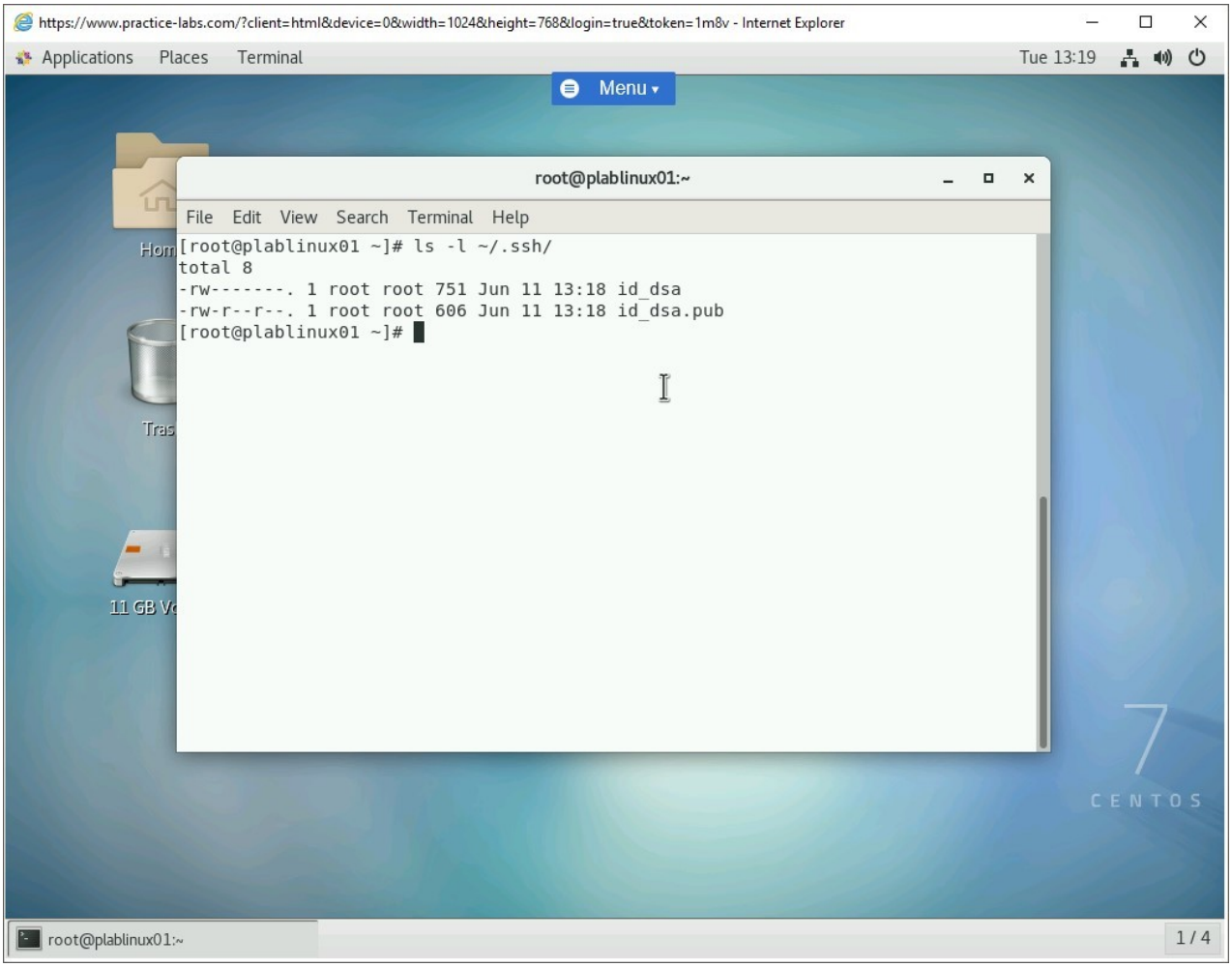


Figure 1.10 Screenshot of PLABLINUX01: Viewing the generated public and private keys.

Step 5

Clear the screen by entering the following command:

```
clear
```

Now, you will need to copy the public key to the remote system. On the host system, navigate to the **.ssh/** directory using the following command:

```
cd .ssh/
```

Press **Enter**.

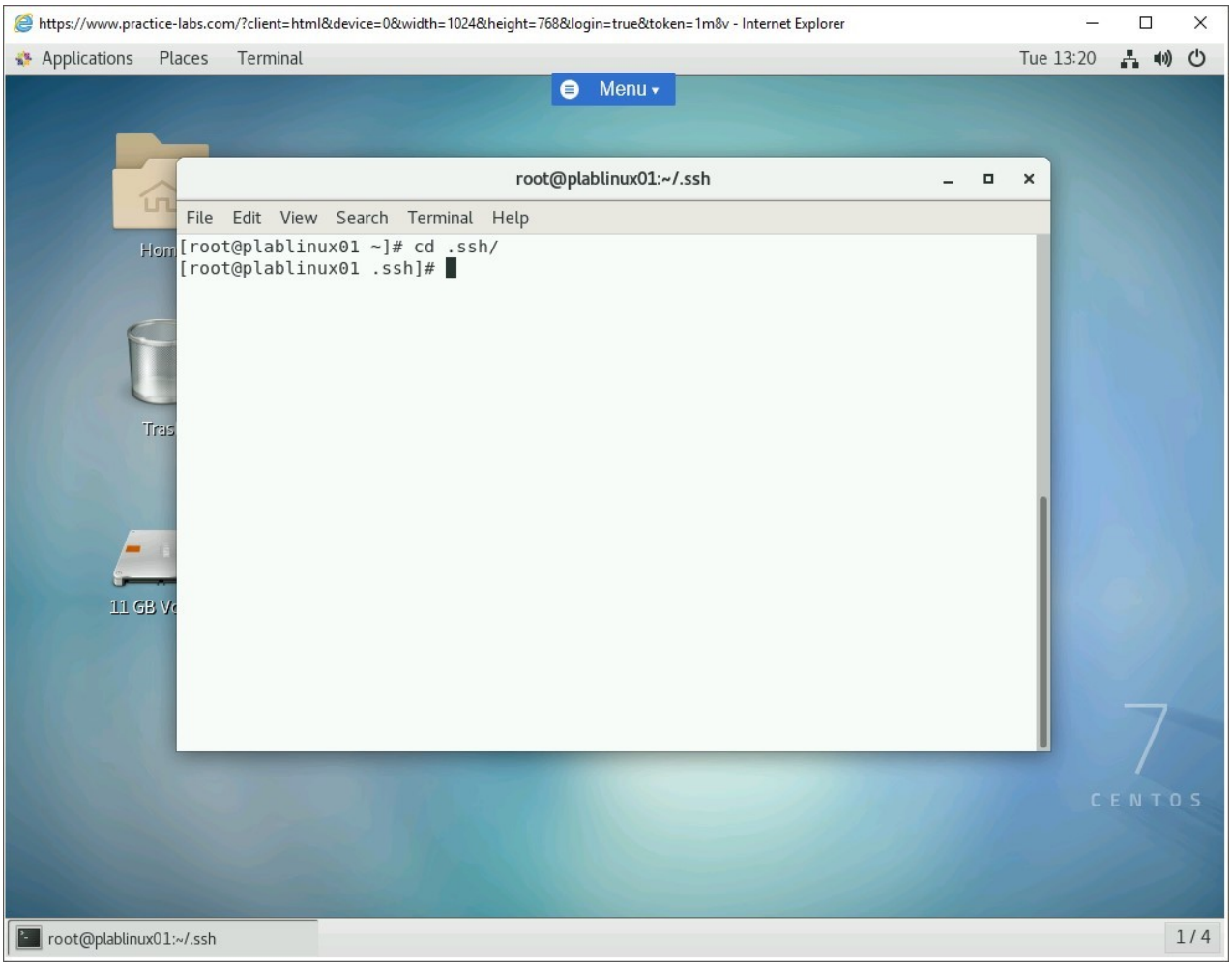


Figure 1.11 Screenshot of PLABLINUX01: Navigating to the .ssh directory.

Step 6

After you have navigated to the ssh directory, copy the file to the remote system. For this task, the remote system is **192.16.0.3**. Type the following command:

```
scp id_dsa.pub administrator@192.168.0.3:./id_dsa.pub
```

Press **Enter**.

When prompted for confirmation, enter **yes**.

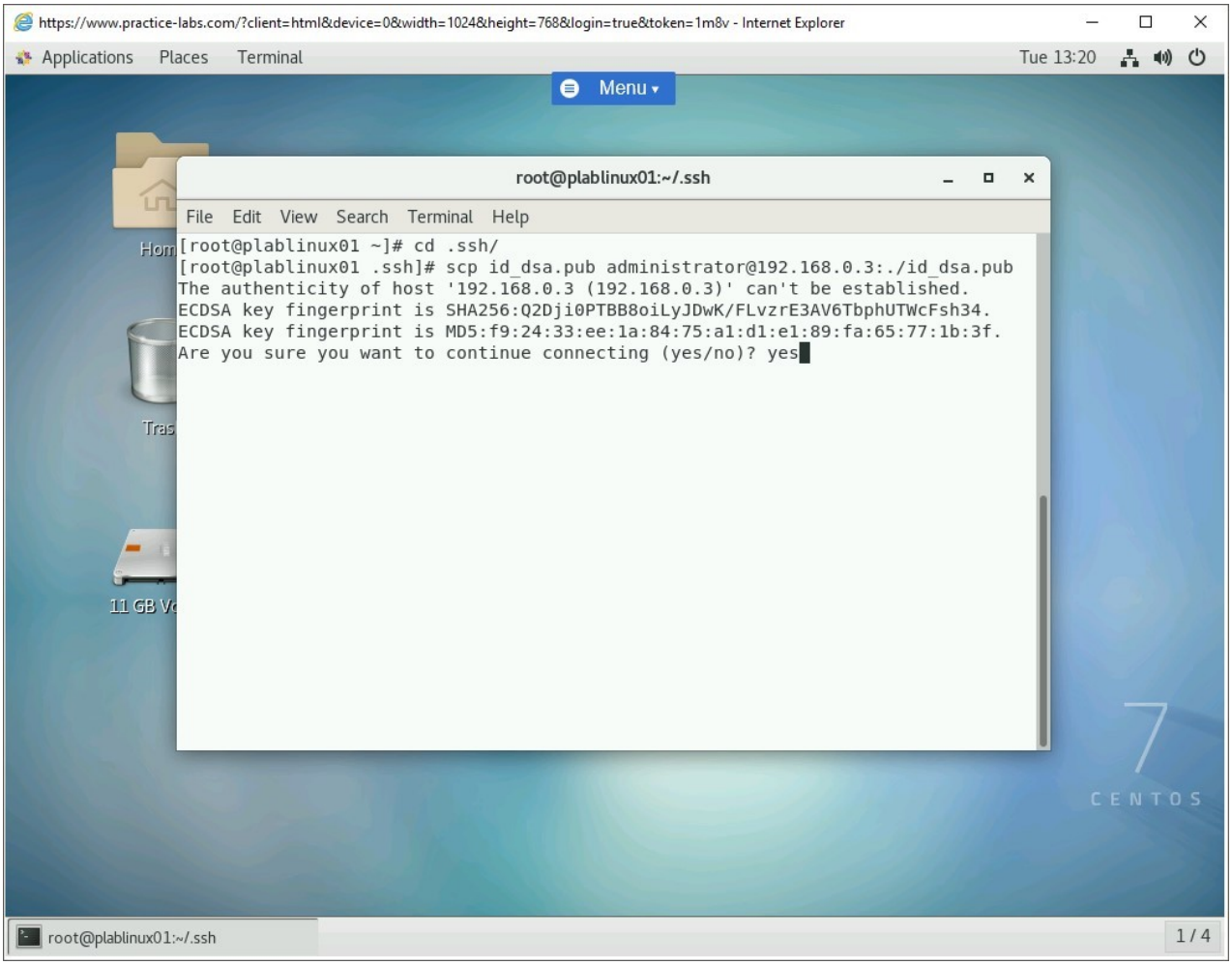


Figure 1.12 Screenshot of PLABLINUX01: Copying the file to the remote system.

Step 7

You will be requested for a password for the username that you used while copying the file. In this case, enter **`Passw0rd`**

The file is now copied to the remote system.

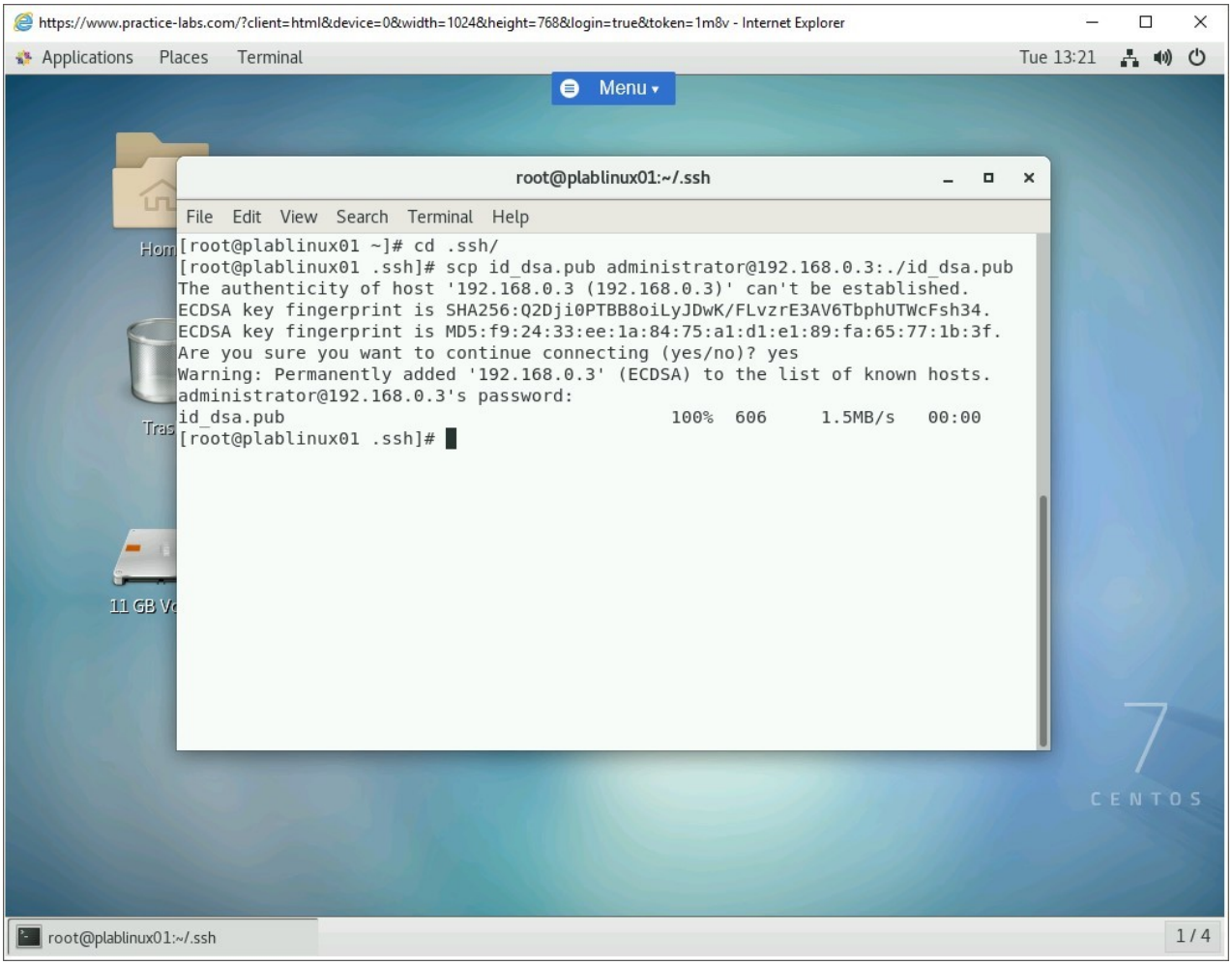


Figure 1.13 Screenshot of PLABLINUX01: Entering the password.

Step 8

Connect to **PLABLINUX02**.

Press **Enter** and click **Admin**.

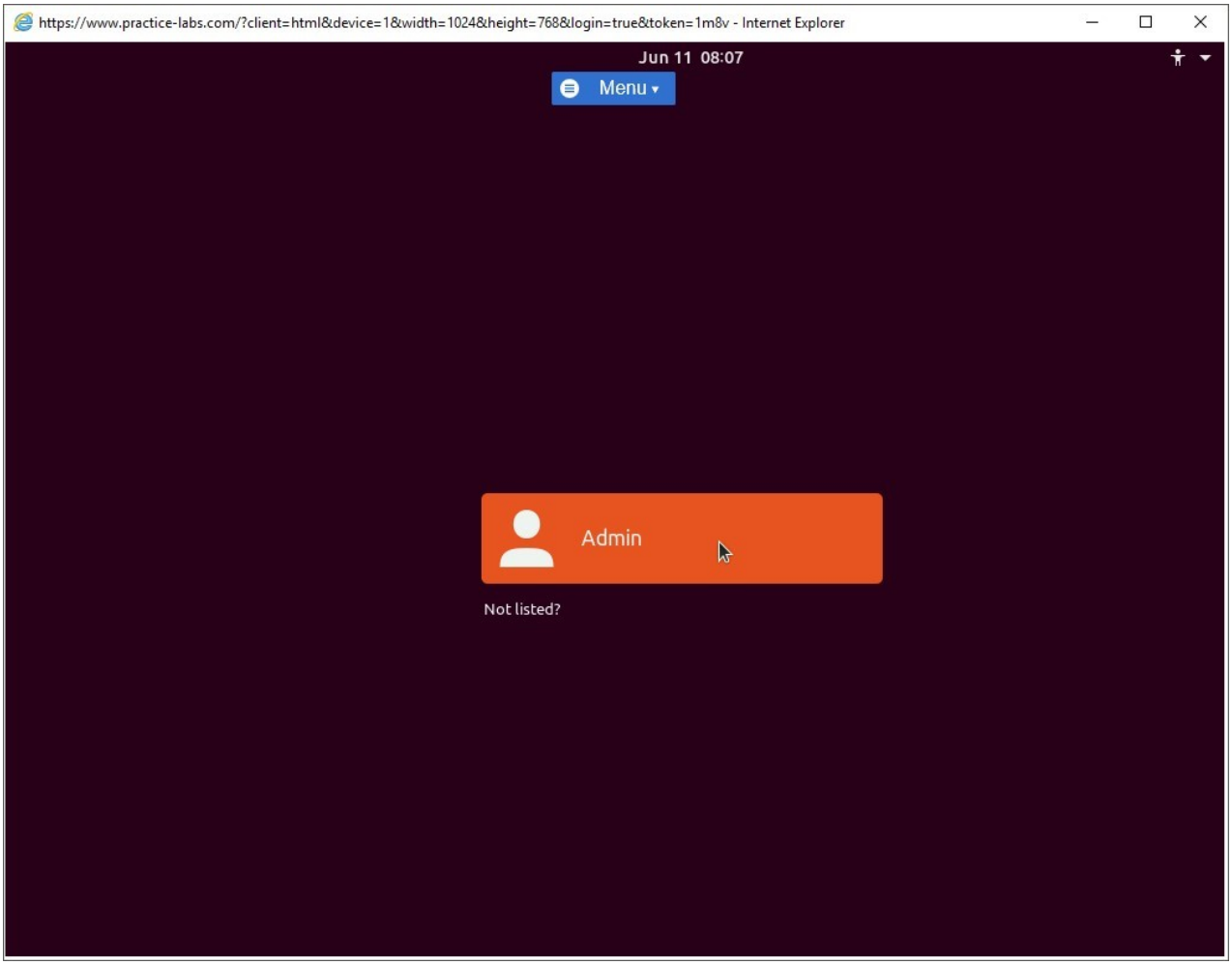


Figure 1.14 Screenshot of PLABLINUX02: Clicking the Administrator account on the login screen.

Step 9

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

```
Passw0rd
```

Click **Sign In**.

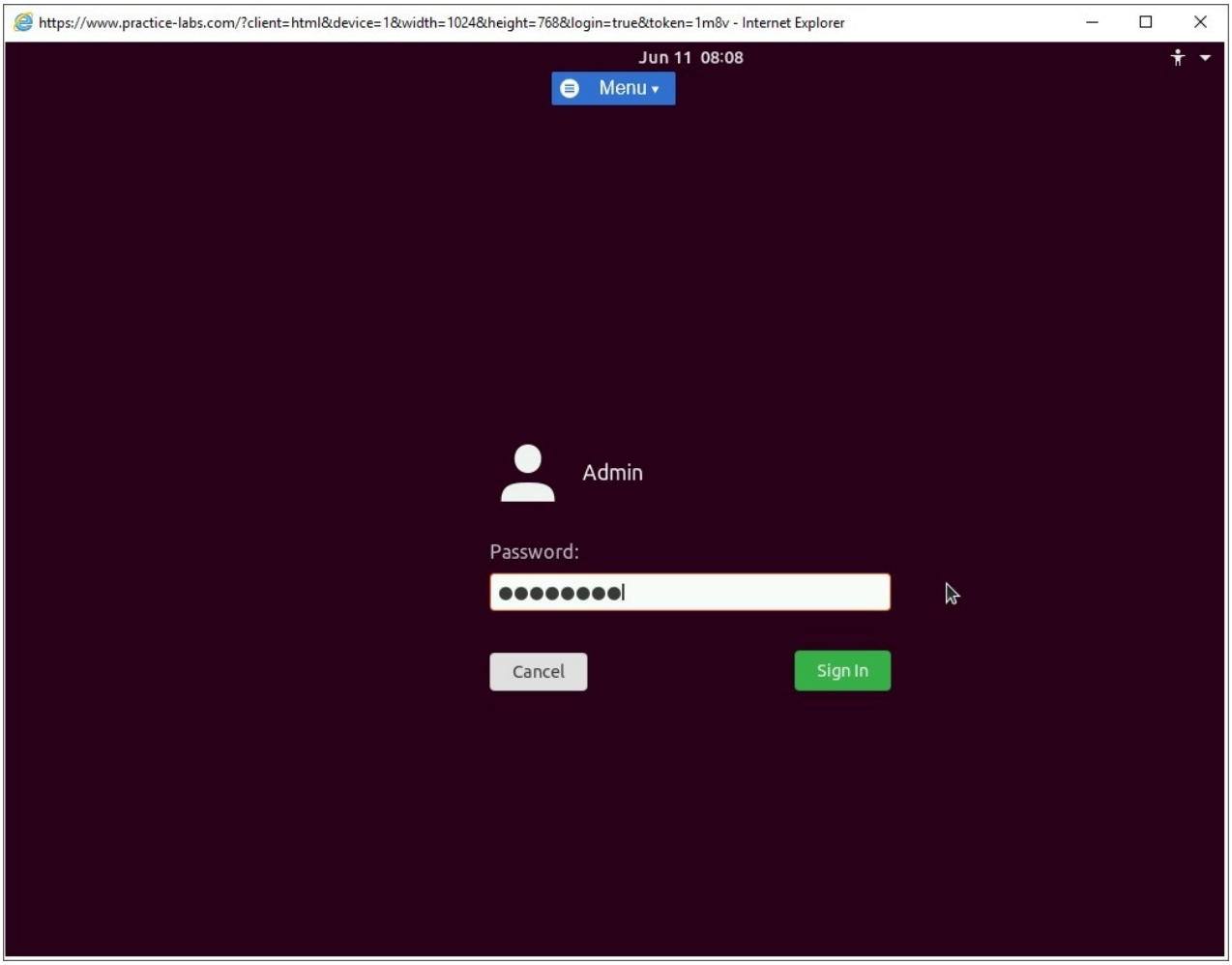


Figure 1.15 Screenshot of PLABLINUX02: Entering the password in the Password text box and then clicking Sign In.

After a successful login, the desktop is displayed.

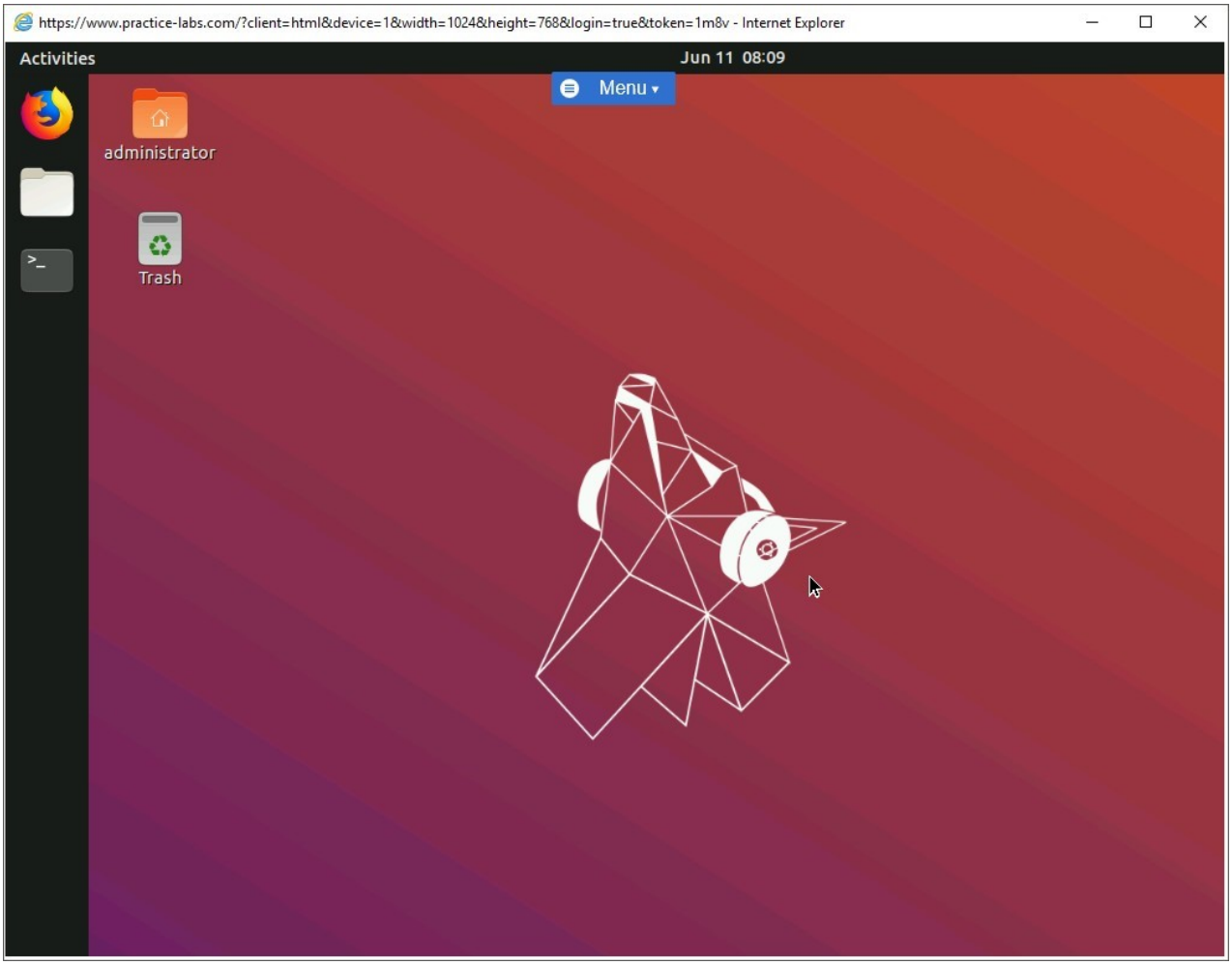


Figure 1.16 Screenshot of PLABLINUX02: Displaying the desktop after the successful login.

Step 10

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

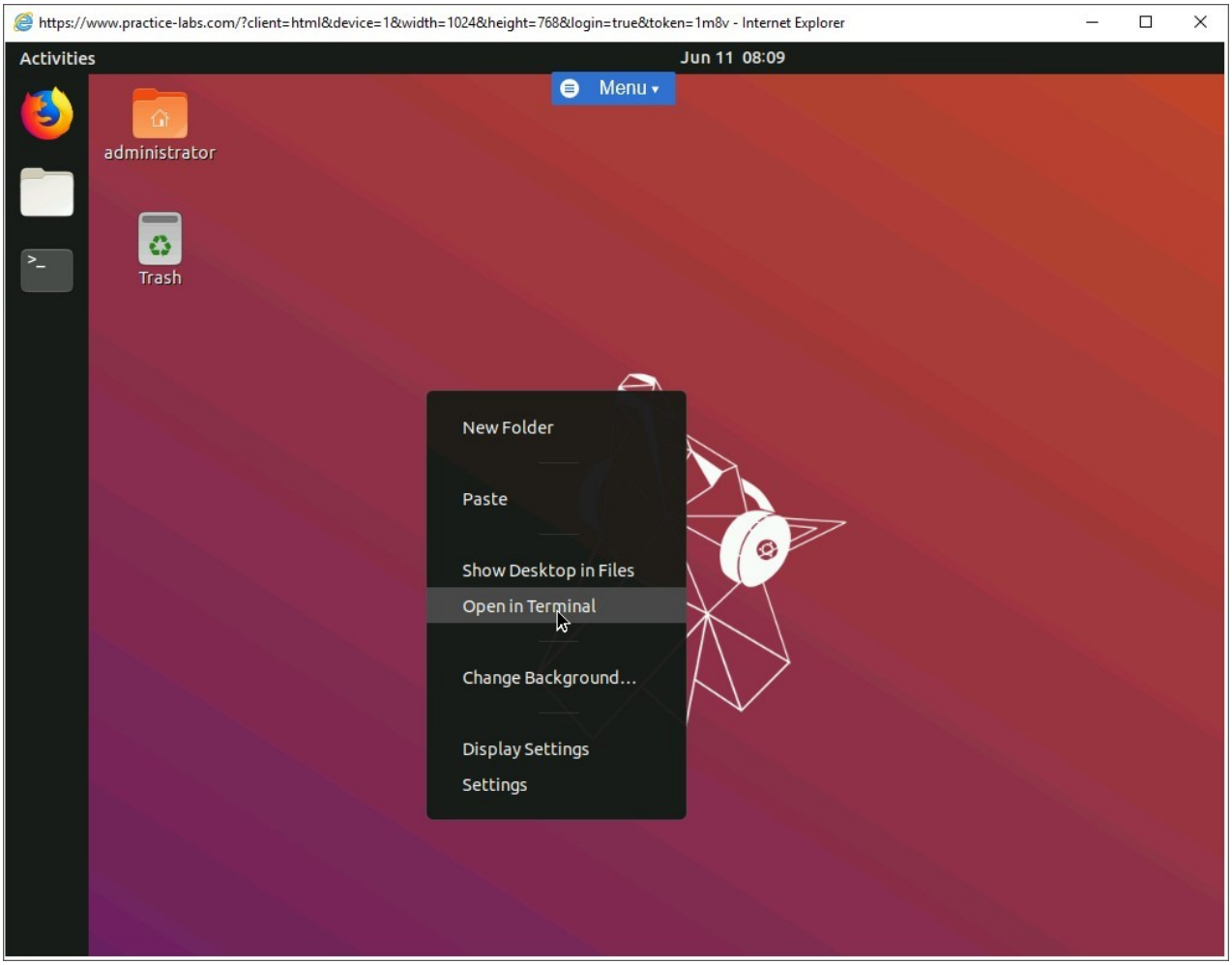


Figure 1.17 Screenshot of PLABLINUX02: Selecting the Open Terminal option from the context menu.

Step 11

If necessary, clear the screen by entering the following command:

```
clear
```

To verify if the **id_dsa.pub** file has been copied, type the following command:

```
ls
```

Press **Enter**.

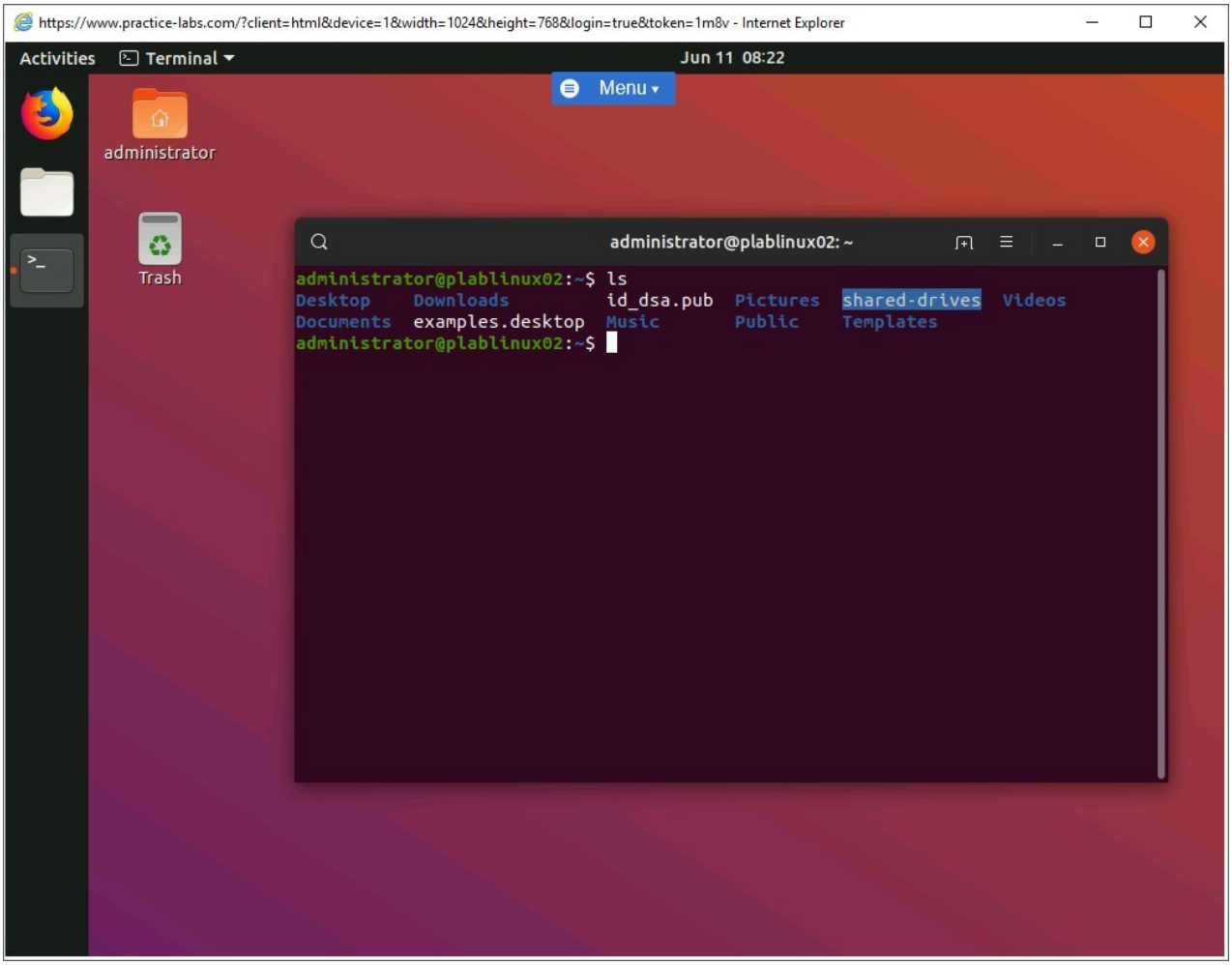


Figure 1.18 Screenshot of PLABLINUX02: Verifying the id_dsa.pub file.

Step 12

Now, create the **ssh** directory. Type the following command:

```
mkdir ssh
```

Press **Enter**.

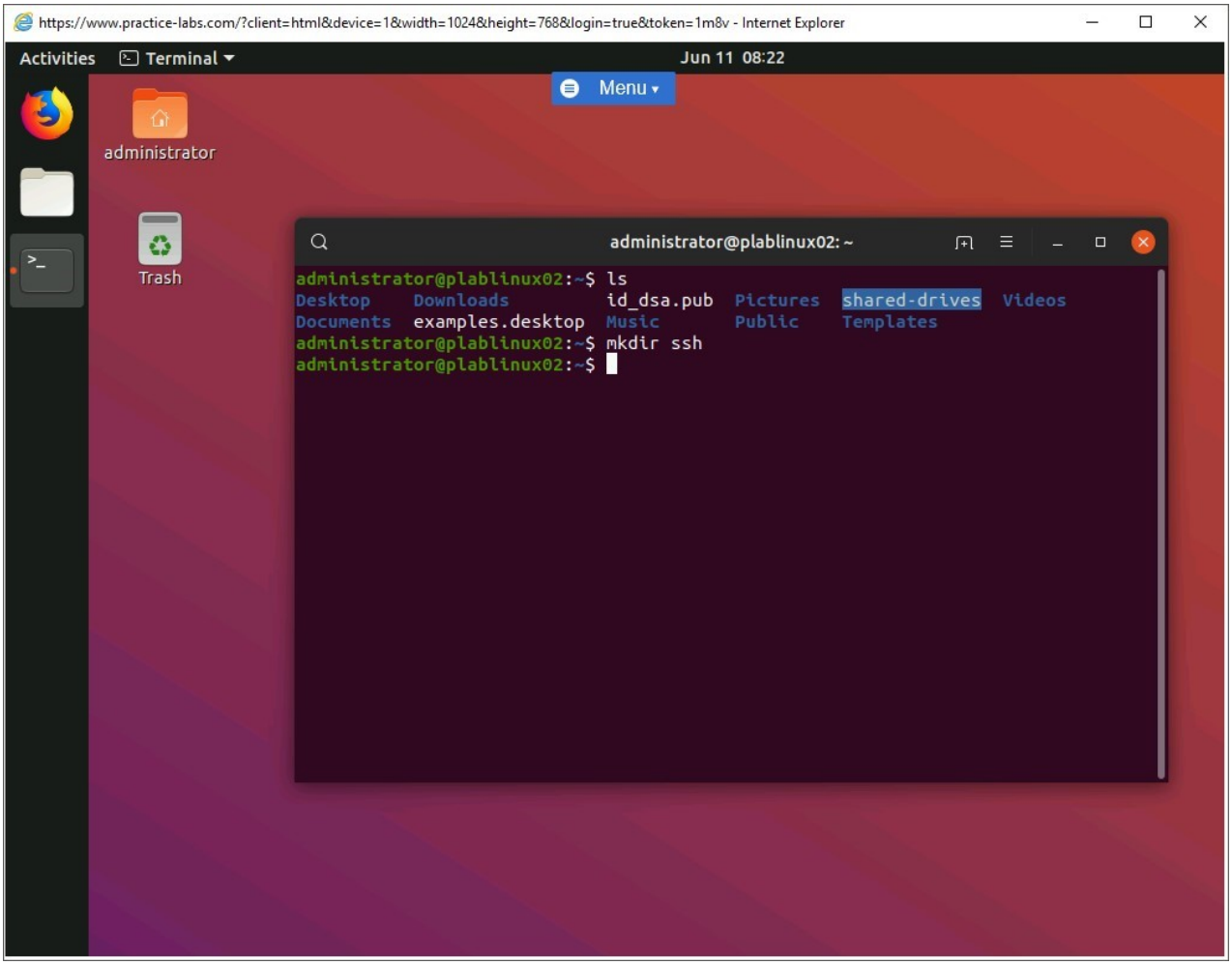


Figure 1.19 Screenshot of PLABLINUX02: Creating the ssh directory.

Step 13

Now, you will need to create an **authorized_keys** file inside the **ssh/** directory and an **authorized_keys2** file and add the public keys to the files.

First, you need to ensure that the **ssh** directory is not writeable.

Type the following command:

```
chmod 700 ssh
```

Press **Enter**.

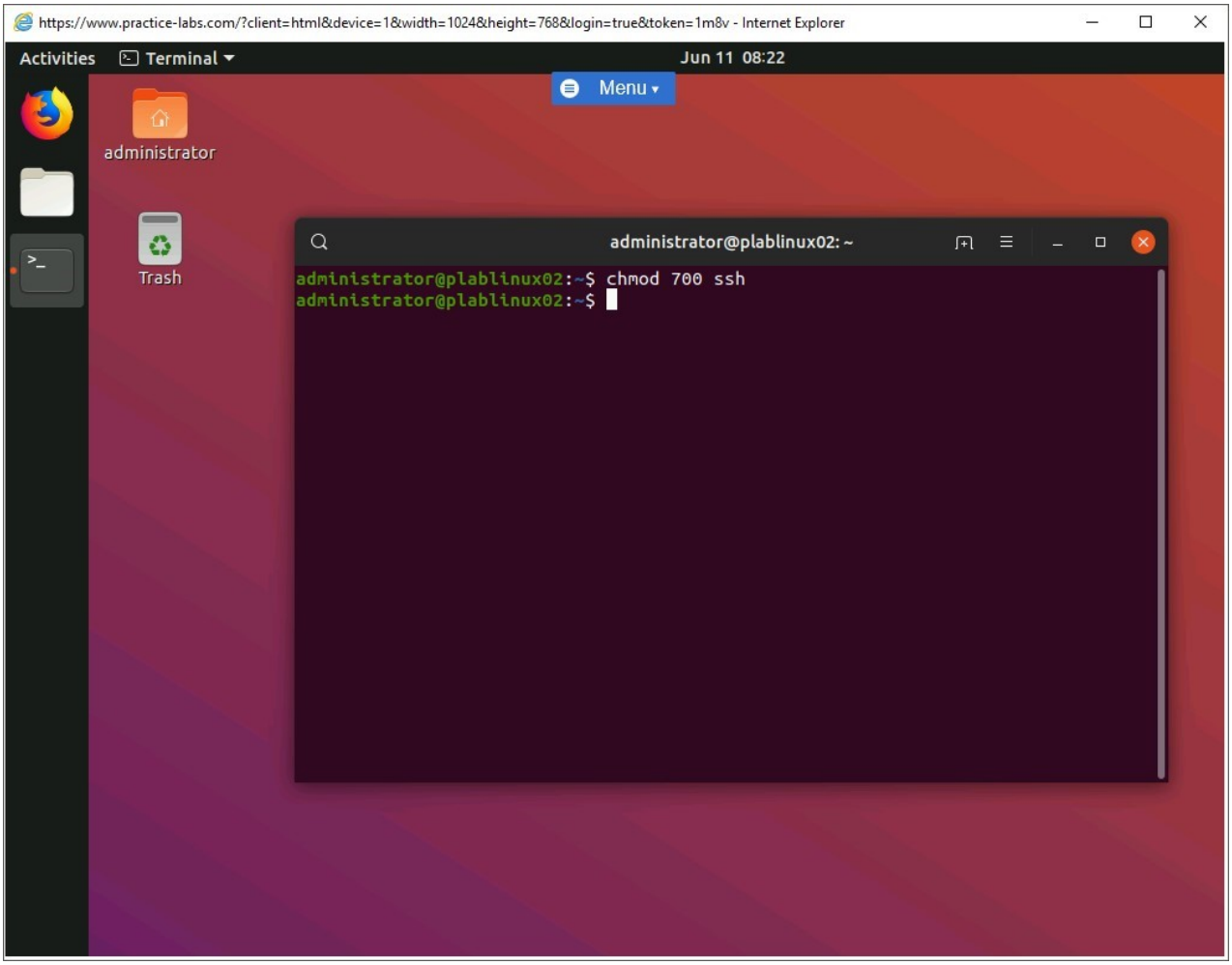


Figure 1.20 Screenshot of PLABLINUX02: Making the ssh directory not writable.

Step 14

Now, navigate to the **ssh** directory. Type the following command:

```
cd ssh
```

Press **Enter**.

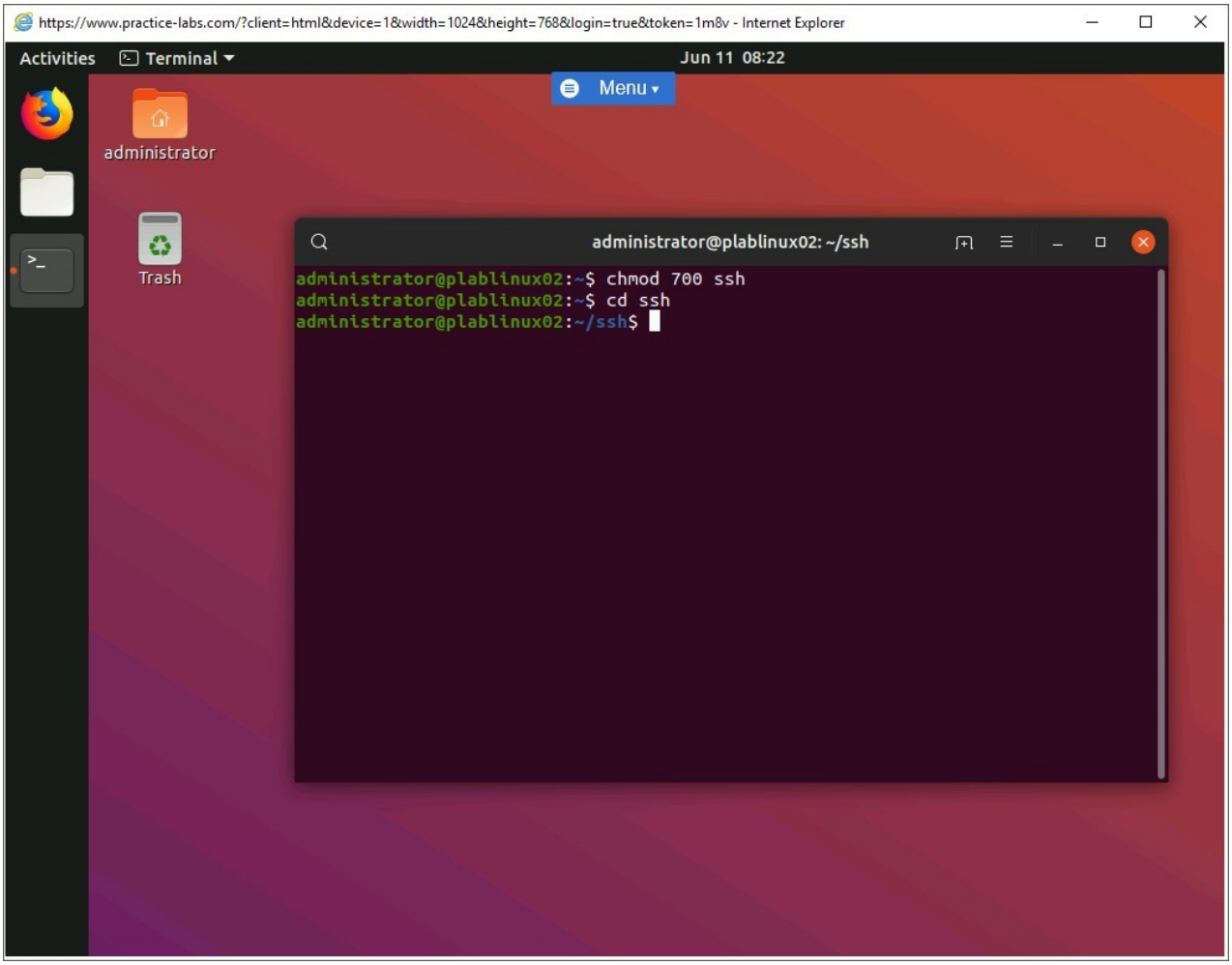


Figure 1.21 Screenshot of PLABLINUX02: Navigating to the ssh directory.

Step 15

Create the **authorized_keys** file. Type the following command:

```
touch authorized_keys
```

Press **Enter**.

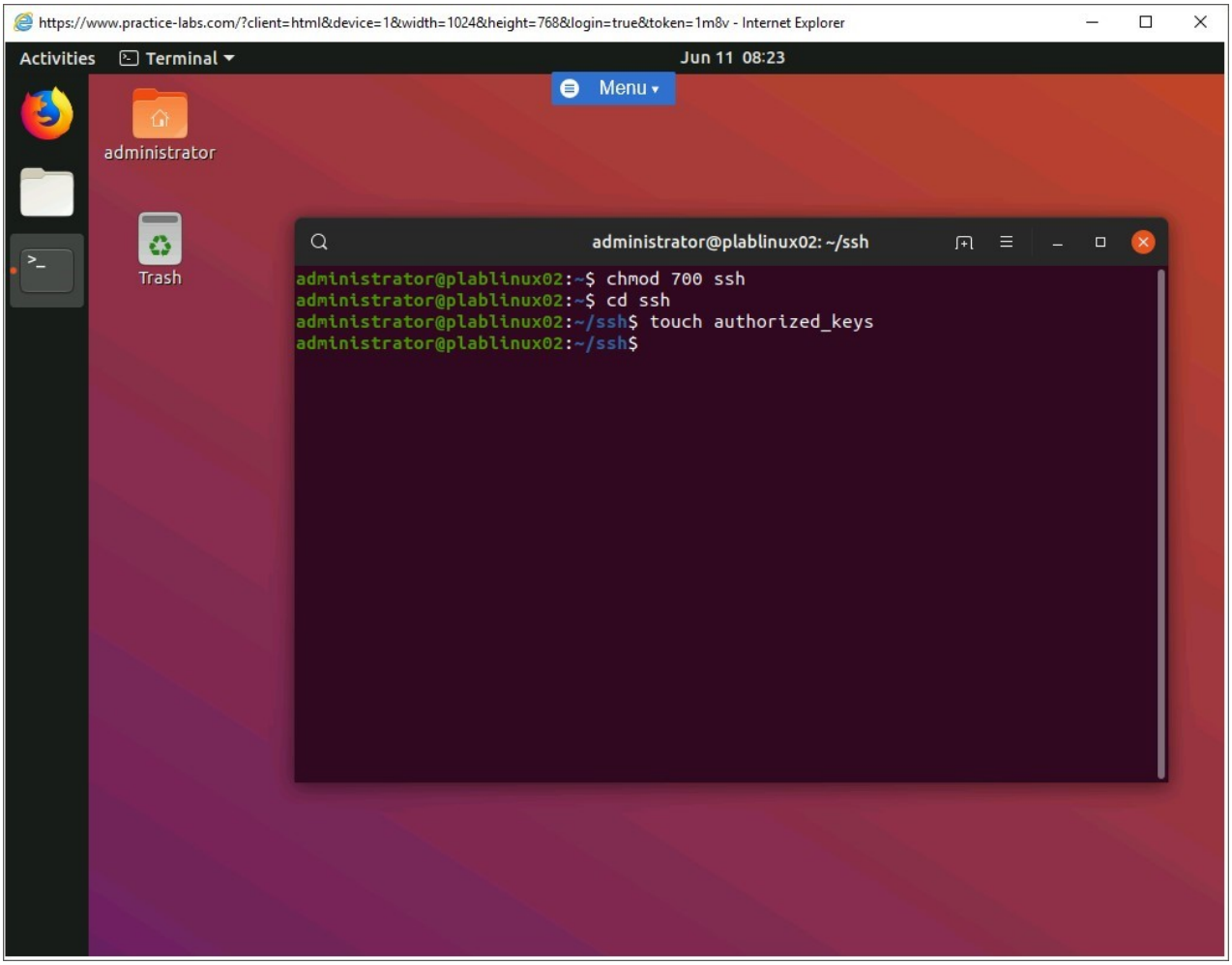


Figure 1.22 Screenshot of PLABLINUX02: Creating the authorized_keys file.

Step 16

Clear the screen by entering the following command:

```
clear
```

Now, change the mode of **authorized_keys** to **600**. Type the following command:

```
chmod 600 authorized_keys
```

Press **Enter**.

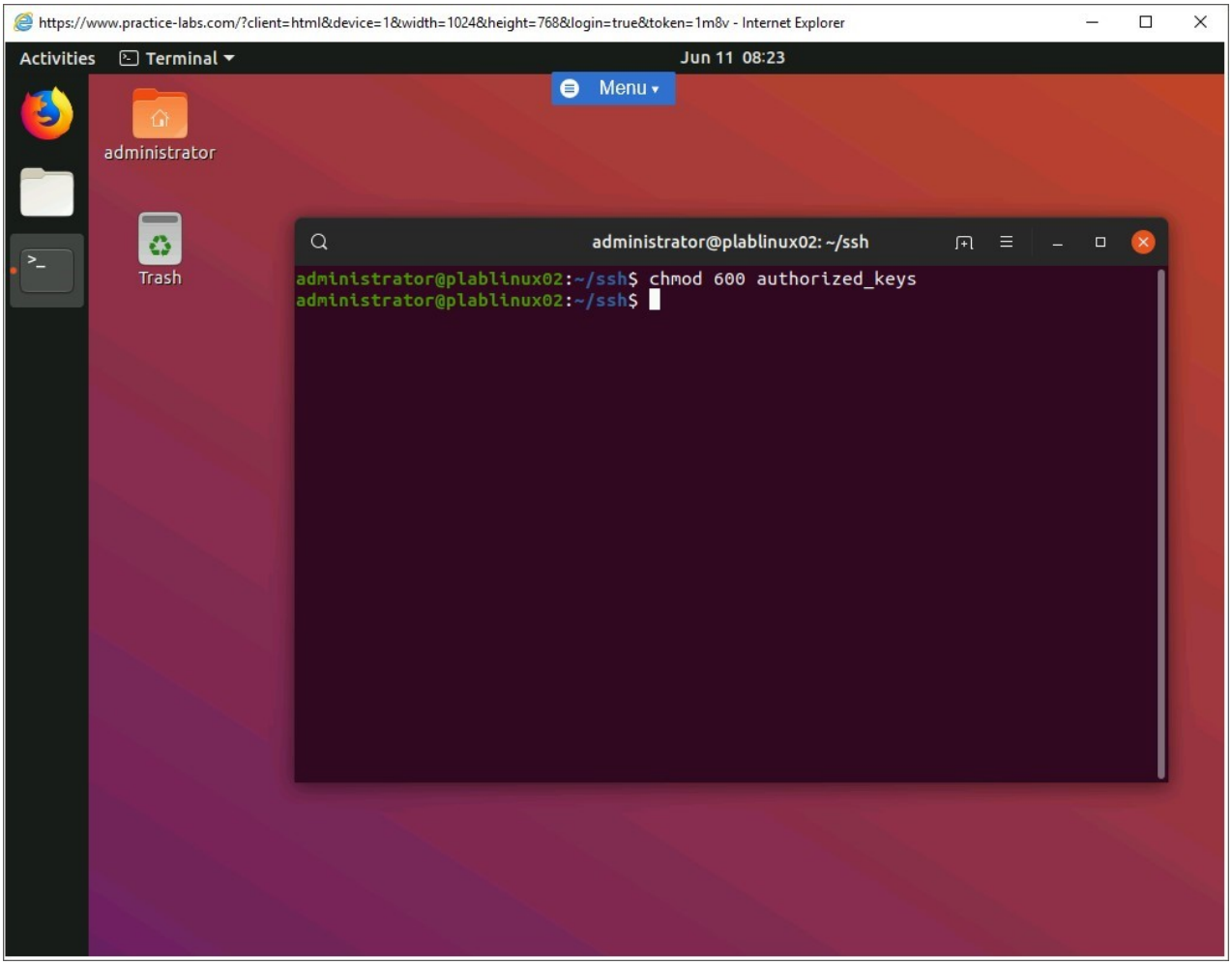


Figure 1.23 Screenshot of PLABLINUX02: Changing the mode of authorized_keys to 600.

Step 17

Add the content of the **id_dsa.pub** file to the **authorized_keys** file. Type the following command:

```
cat ../id_dsa.pub >> authorized_keys
```

Press **Enter**.

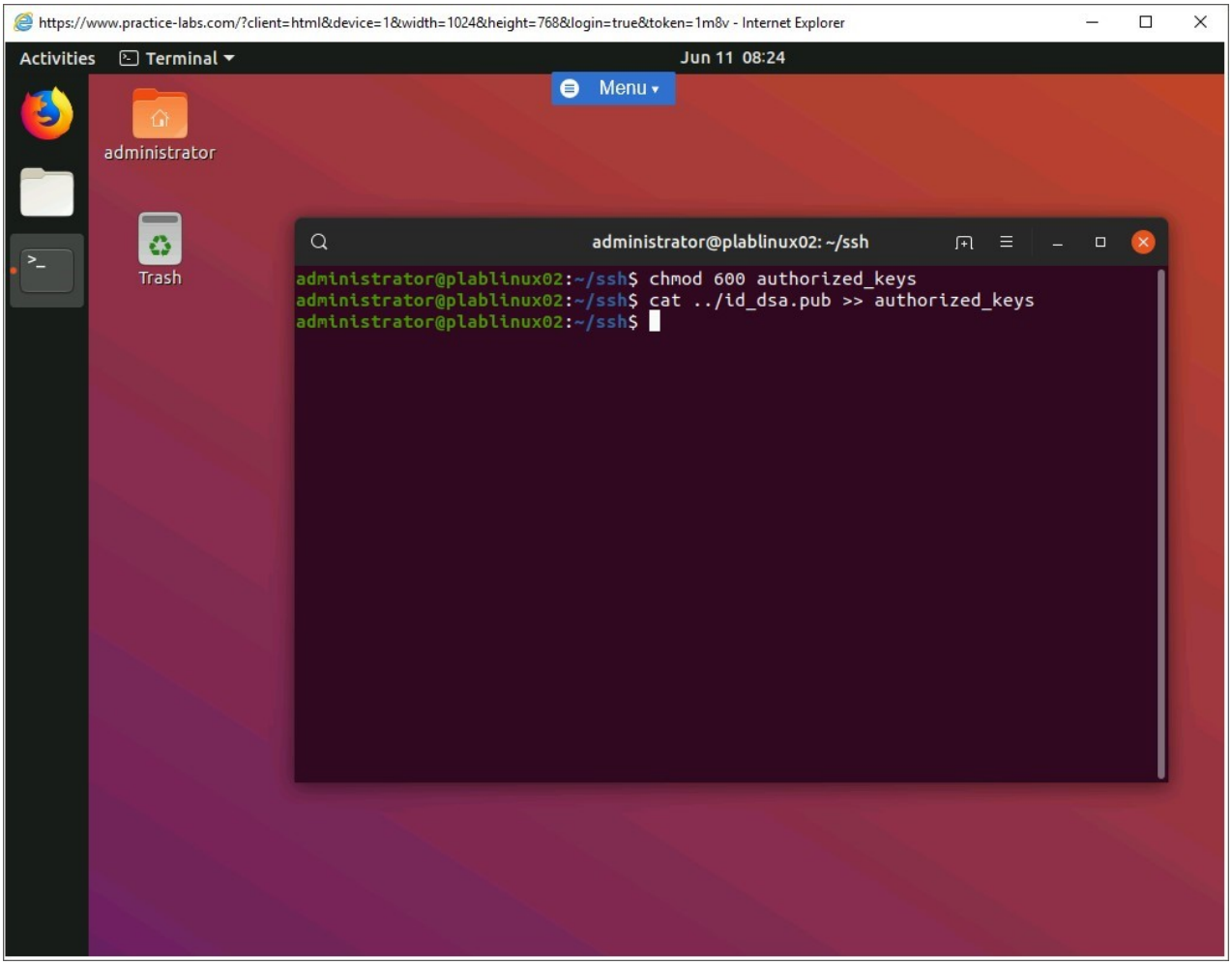


Figure 1.24 Screenshot of PLABLINUX02: Adding the content of the id_dsa.pub file to the authorized_keys file.

Step 18

Now, verify whether the contents have been copied to the **authorized_keys**. Type the following command:

```
cat authorized_keys
```

Press **Enter**.

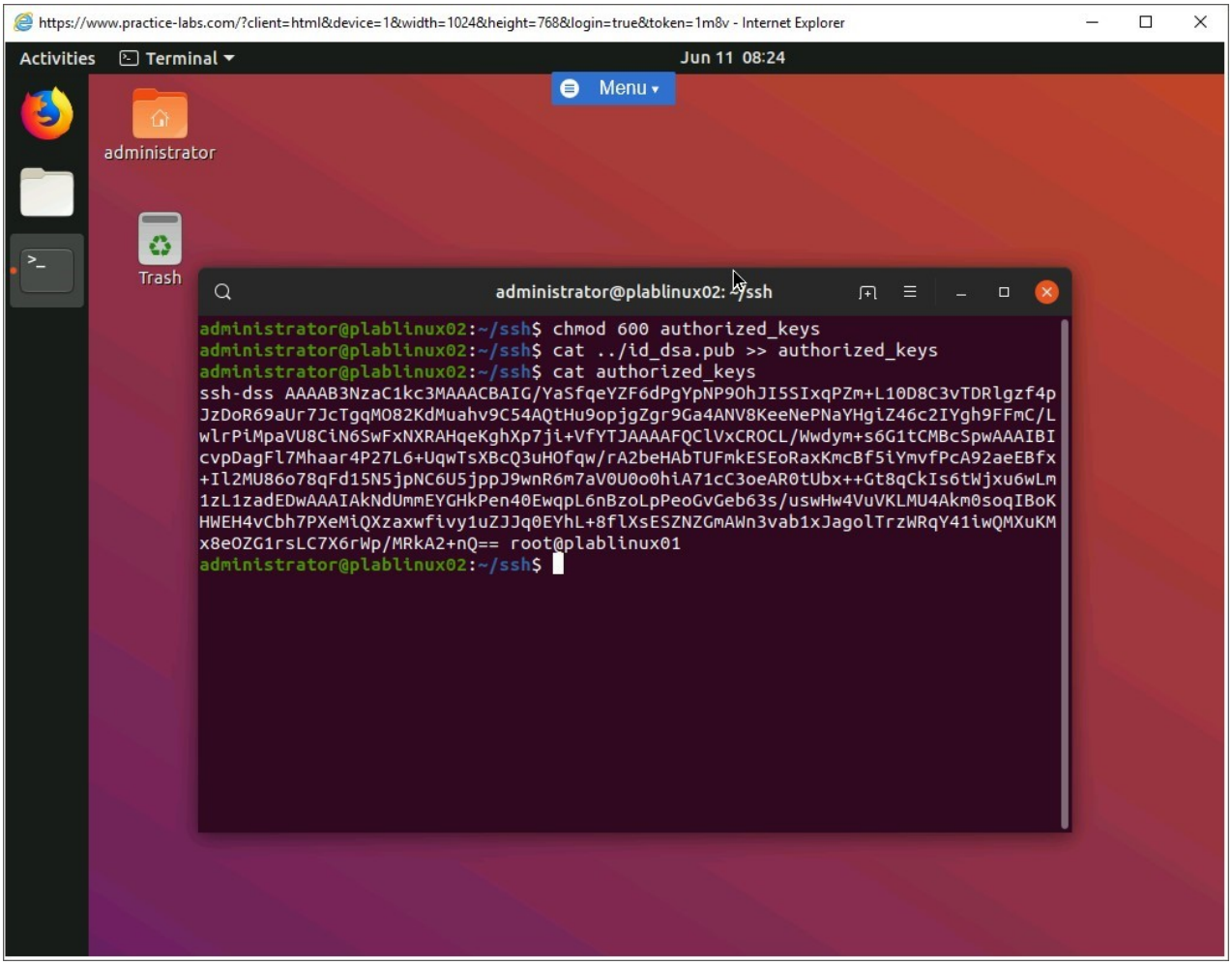


Figure 1.25 Screenshot of PLABLINUX02: Verifying whether the contents have been copied to the authorized_keys.

Task 3 - Basic GnuPG Management

GNU Privacy Guard (**GPG**), just like **SSH**, requires you to make a key pair. The key pair generated is stored in the **~/.gnupg/** directory. In this task, you will generate a secret key for a GnuPG connection.

To perform basic GnuPG management, perform the following steps:

Step 1

Ensure that you are logged on to the **PLABLINUX01**. Clear the screen if required.

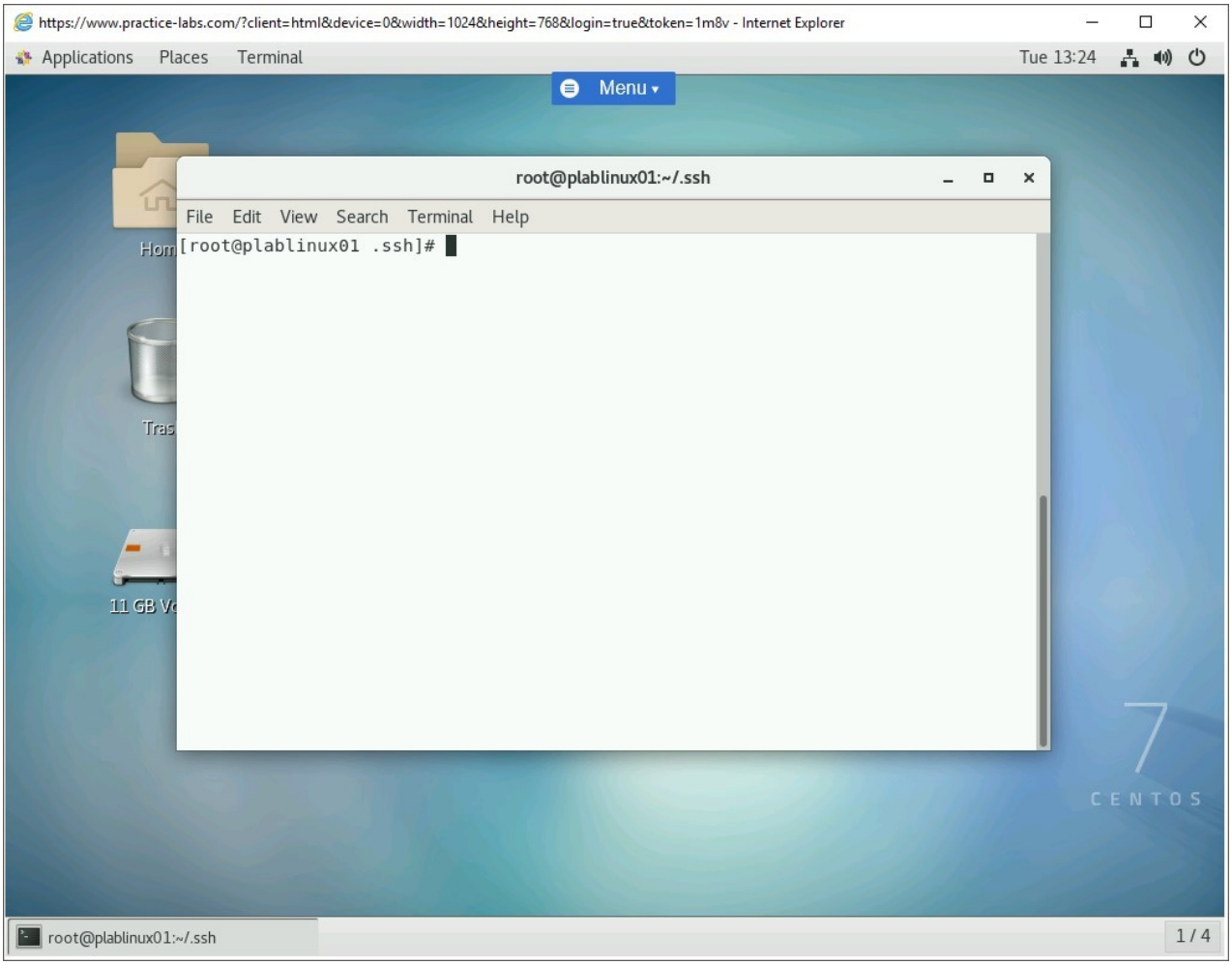


Figure 1.26 Screenshot of PLABLINUX01: Showing the terminal window.

Step 2

First, you will have to generate the key pair. Type the following command:

```
sudo gpg --gen-key
```

Press **Enter**.

When prompted, type the following password:

`Passw0rd`

Press **Enter**.

You will be prompted to select the type of key.

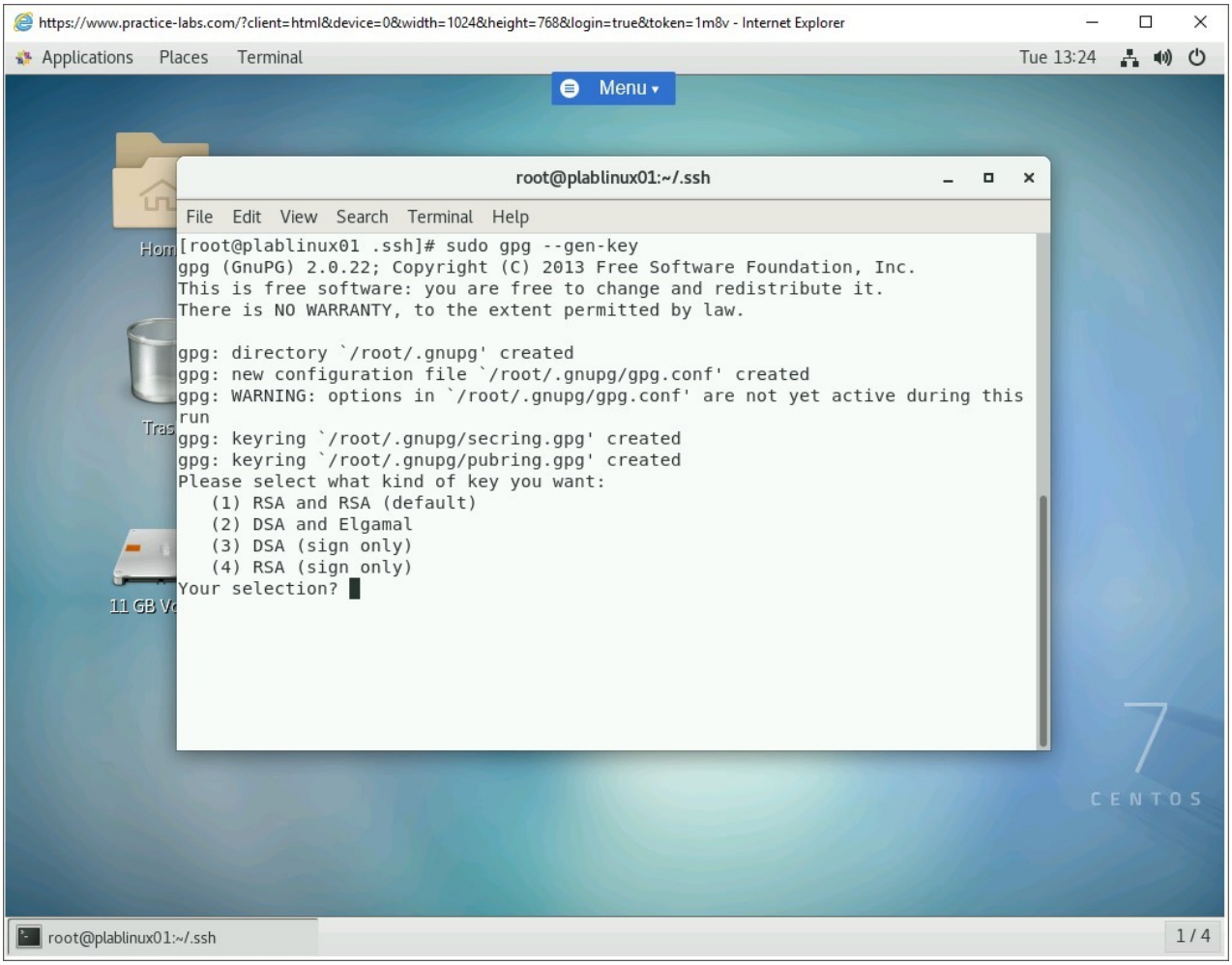


Figure 1.27 Screenshot of PLABLINUX01: Generating the key pair.

Step 3

Type **4**, which is RSA (sign only).

Press **Enter**.

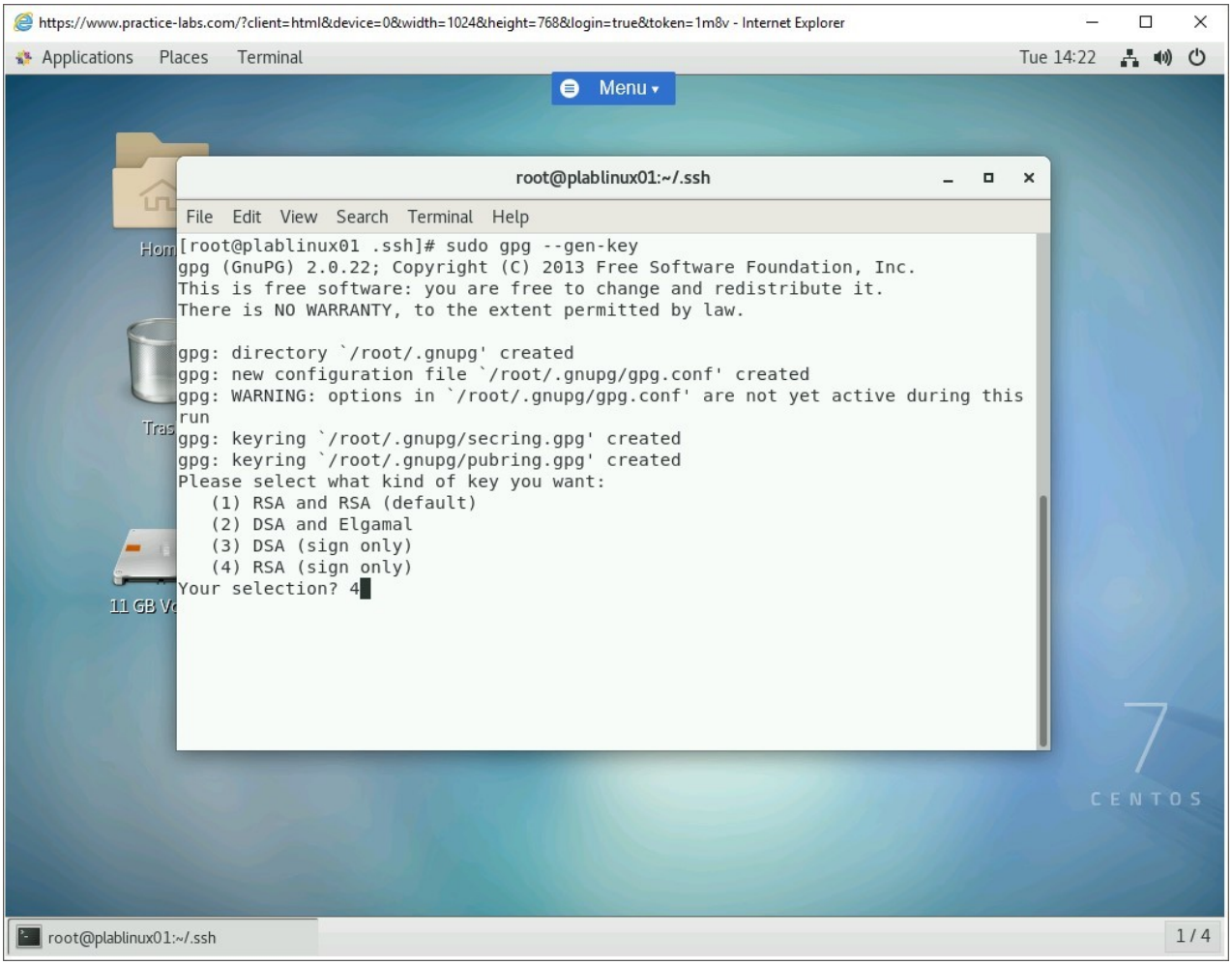


Figure 1.28 Screenshot of PLABLINUX01: Selecting option 4.

Step 4

You are now prompted to type the key size. Enter **1024**. You can choose the default size 2048 or enter 1024.

Press **Enter**.

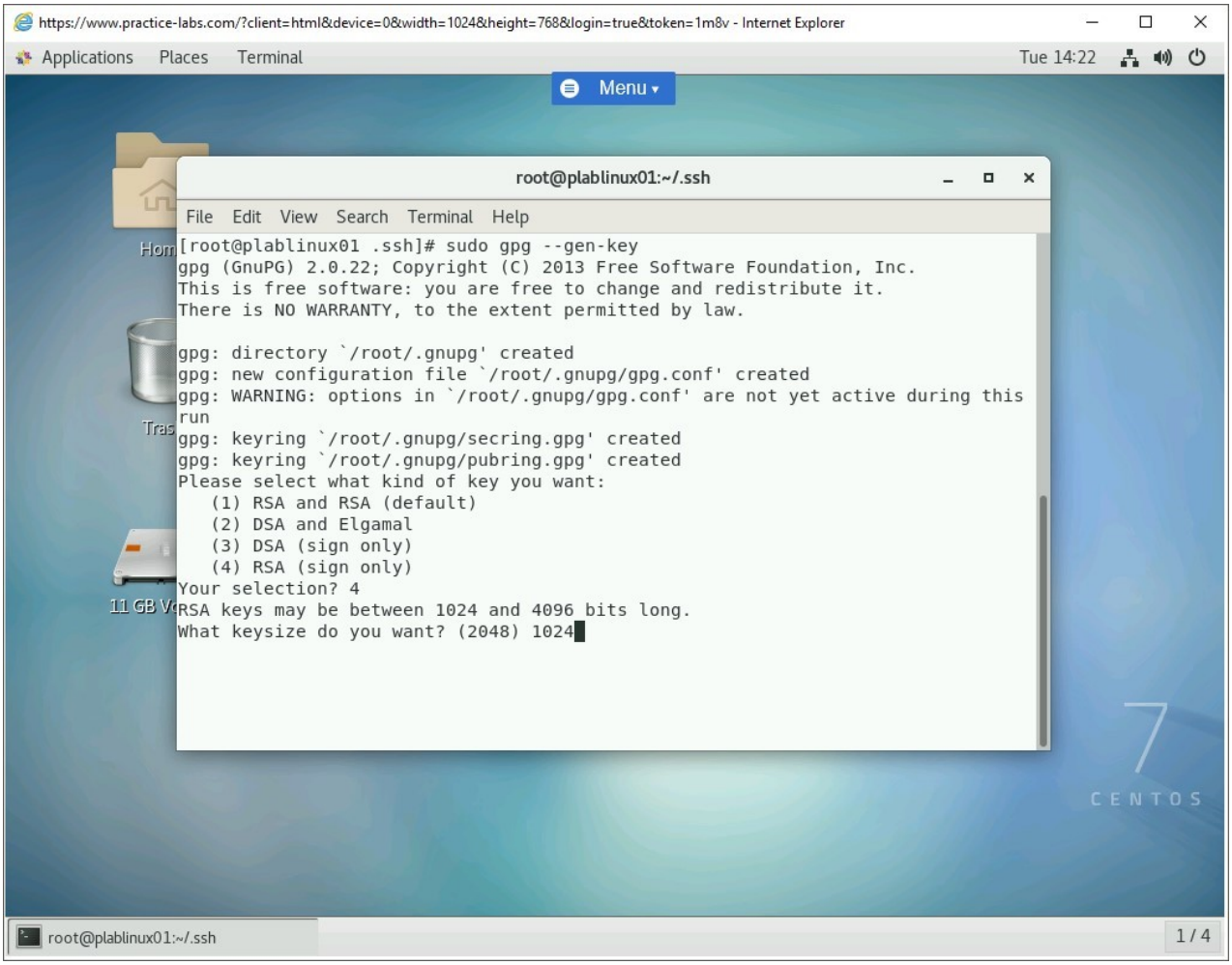


Figure 1.29 Screenshot of PLABLINUX01: Selecting 1024 as the key size.

Step 5

You are now prompted to provide the validity duration of the key. Type **3y**.

Press **Enter**.

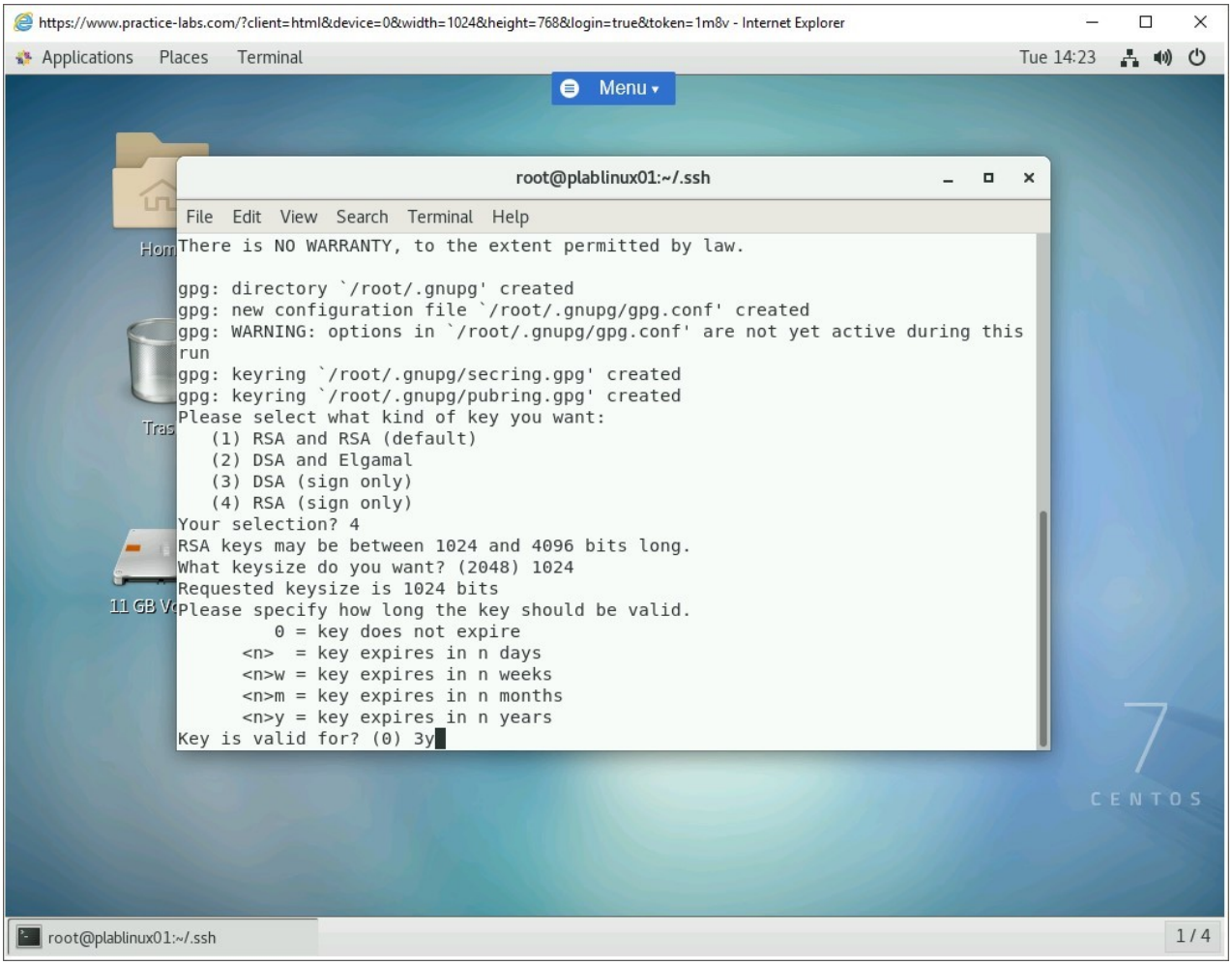


Figure 1.30 Screenshot of PLABLINUX01: Entering the validity duration.

Step 6

You are prompted to provide confirmation for the set duration. Type **y**.

Press **Enter**.

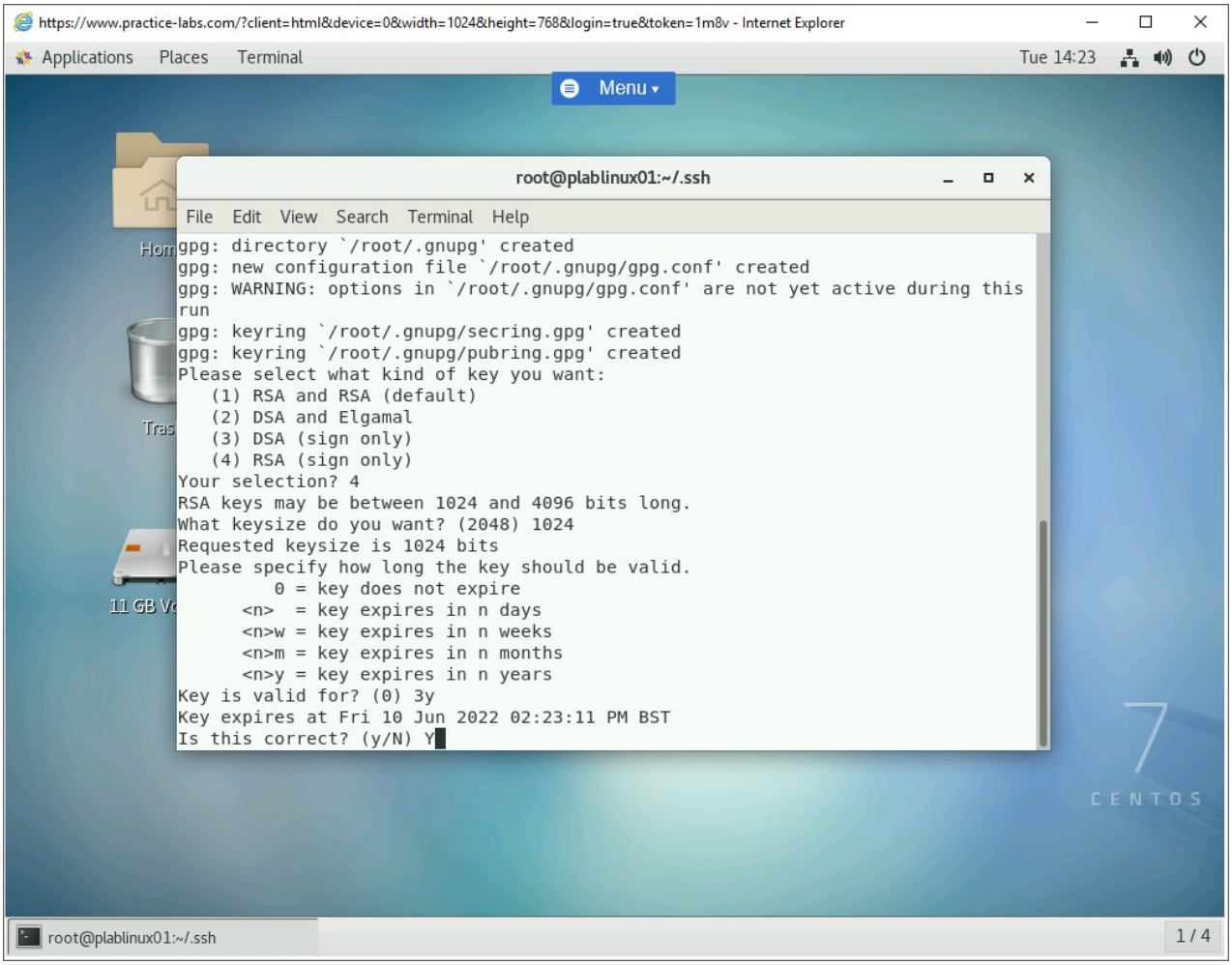


Figure 1.31 Screenshot of PLABLINUX01: Confirming the duration.

Step 7

You are prompted to provide a real name. For this task, enter the following:

```
admin
```

Press **Enter**.

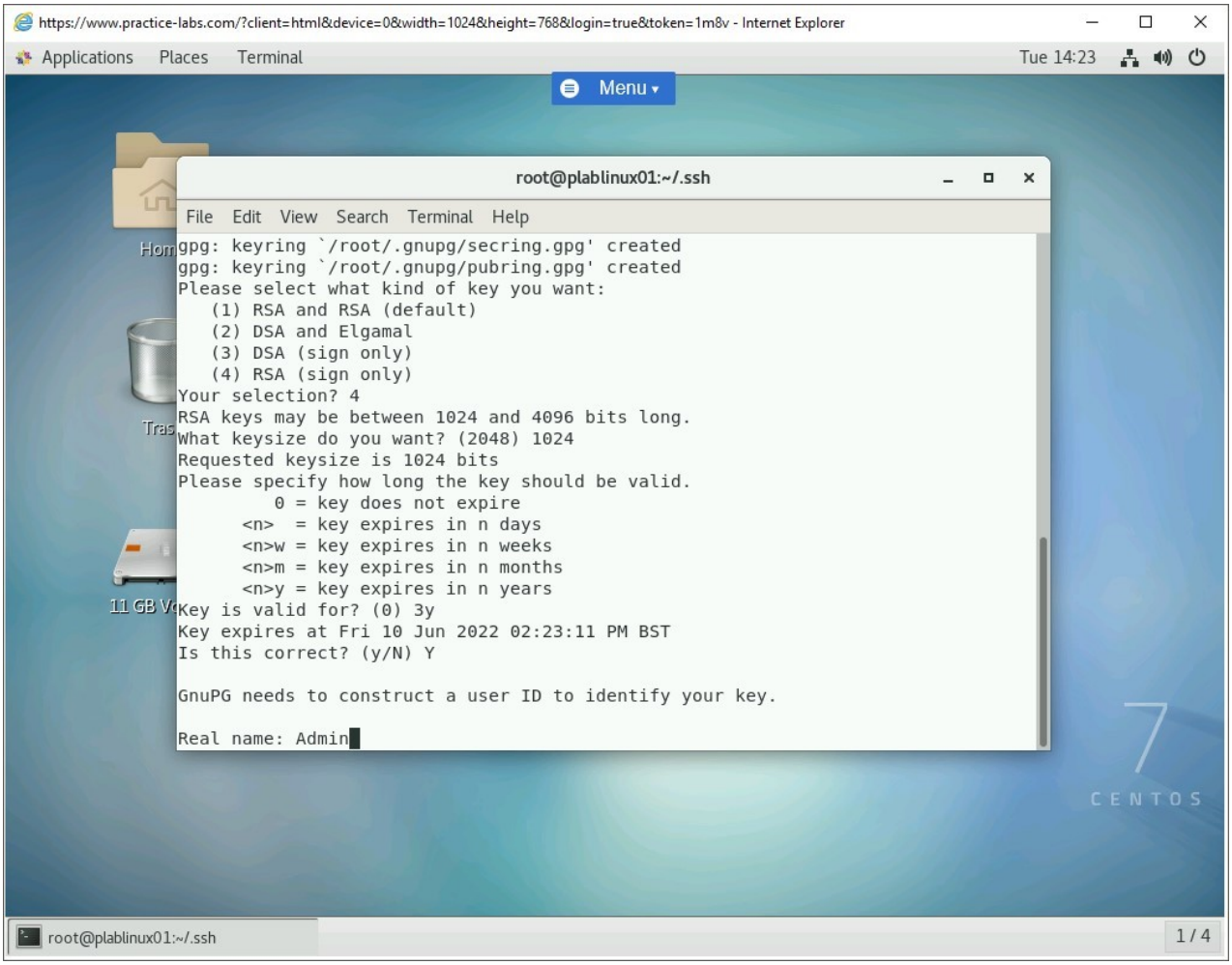


Figure 1.32 Screenshot of PLABLINUX01: Entering a real name.

Step 8

You are now prompted for the E-mail address. Enter the following:

```
admin@practicelabs.com
```

Press **Enter**.

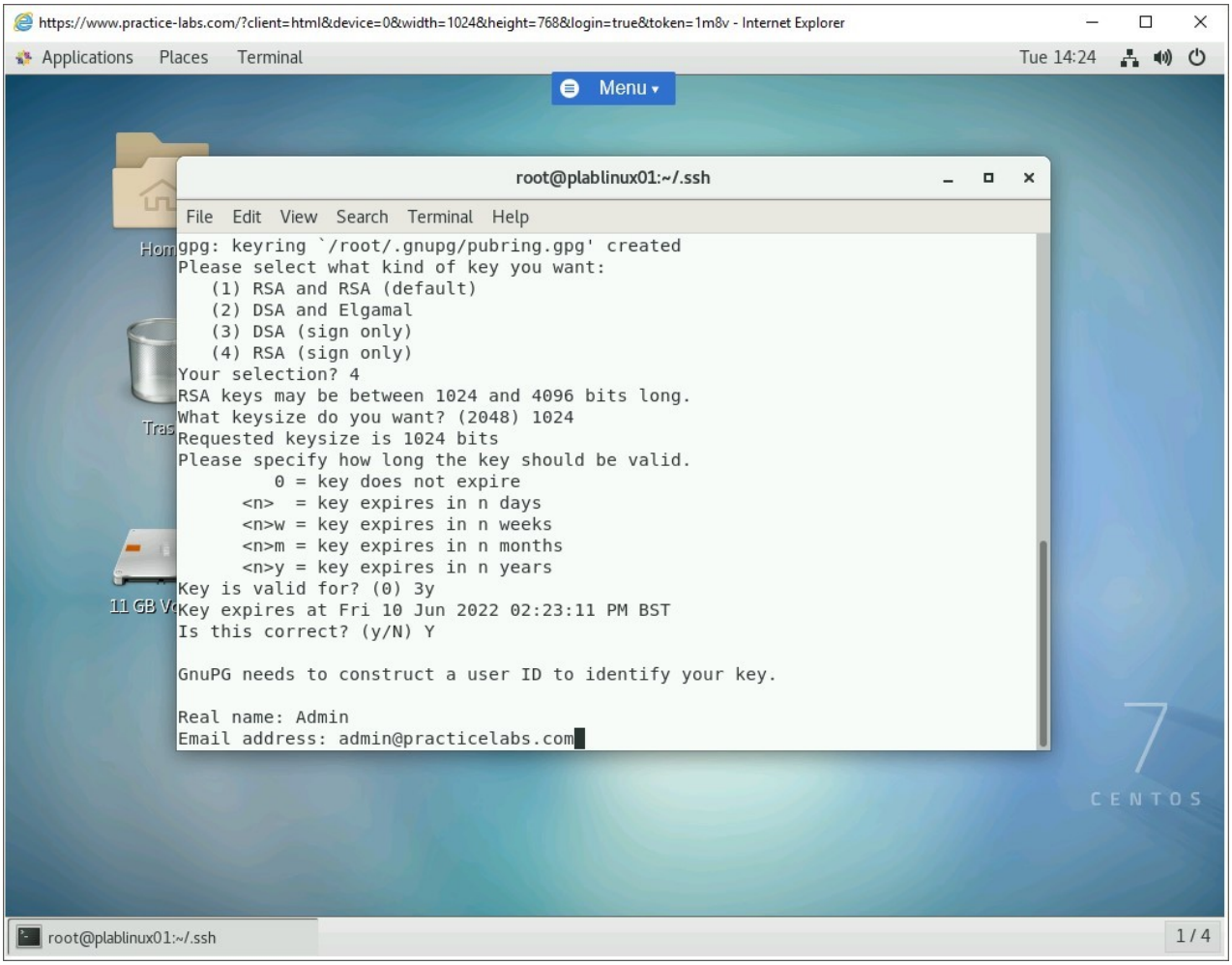


Figure 1.33 Screenshot of PLABLINUX01: Entering the E-mail id.

Step 9

You are now prompted to enter a comment. Enter the following:

```
Administrator
```

Press **Enter**.

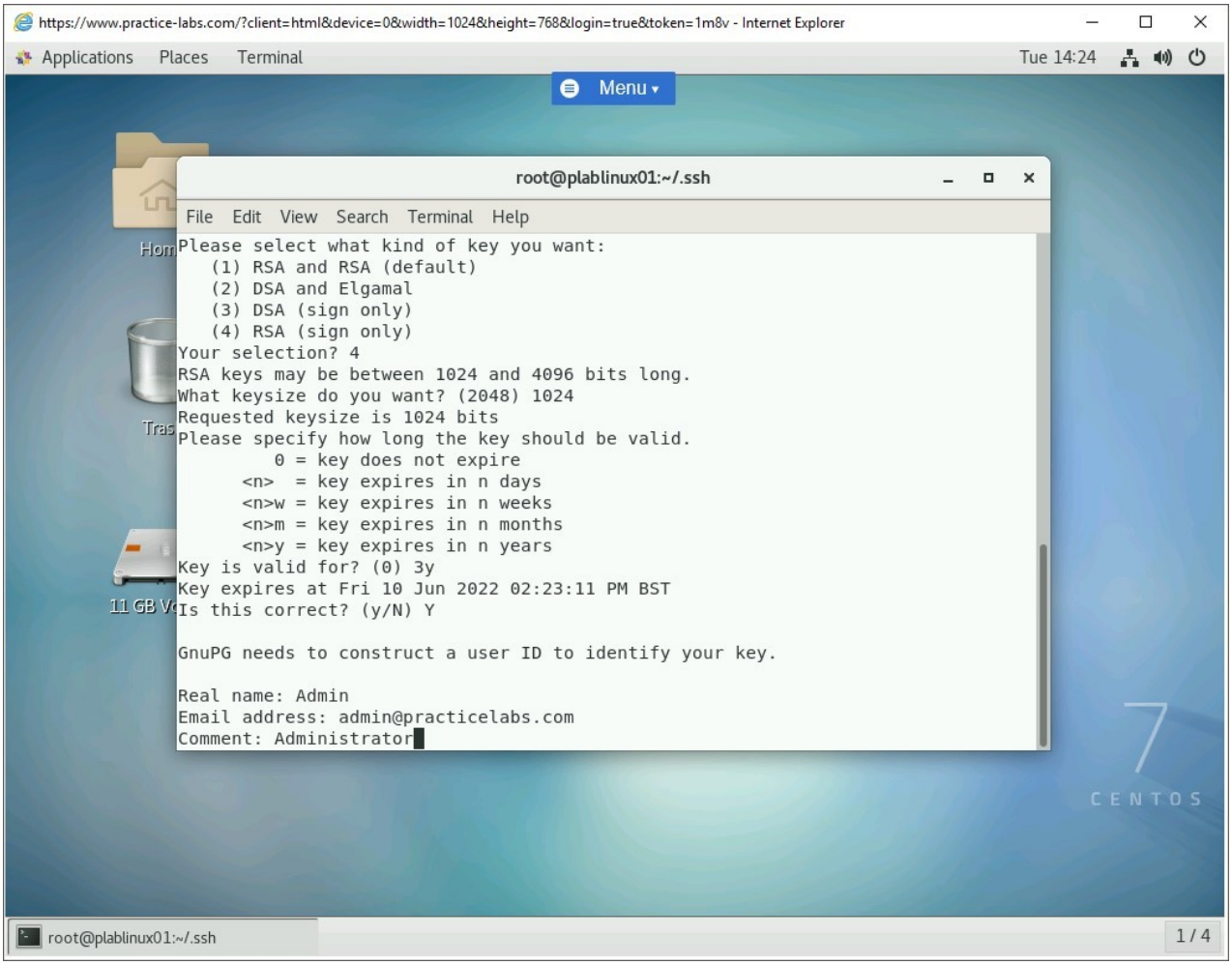


Figure 1.34 Screenshot of PLABLINUX01: Entering text in the Comment prompt.

Step 10

You are prompted for the confirmation. Type **o**.

Press **Enter**.

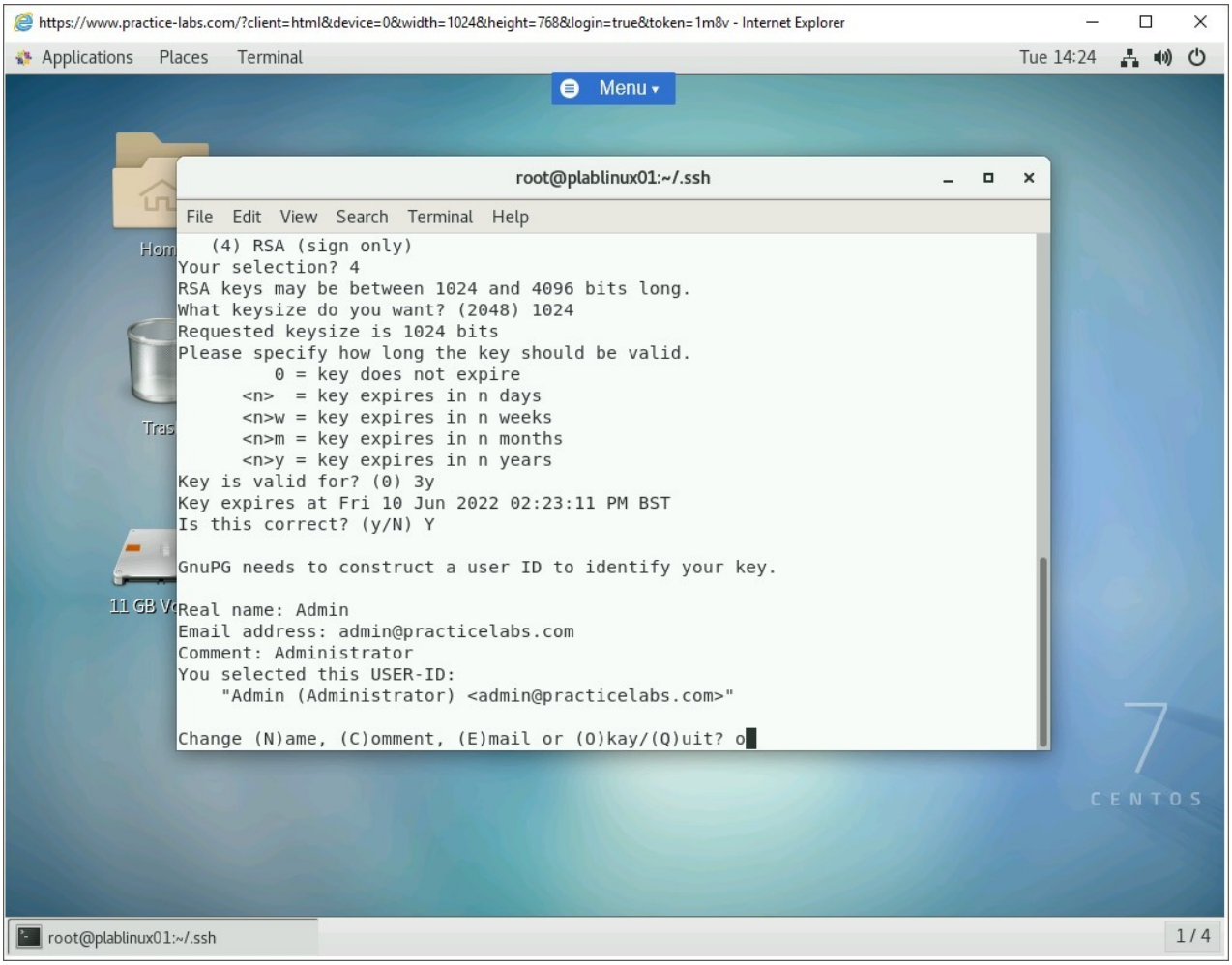


Figure 1.35 Screenshot of PLABLINUX01: Providing confirmation.

Step 11

You need to enter the passphrase now. Enter **`Passw0rd`**

Click **OK**.

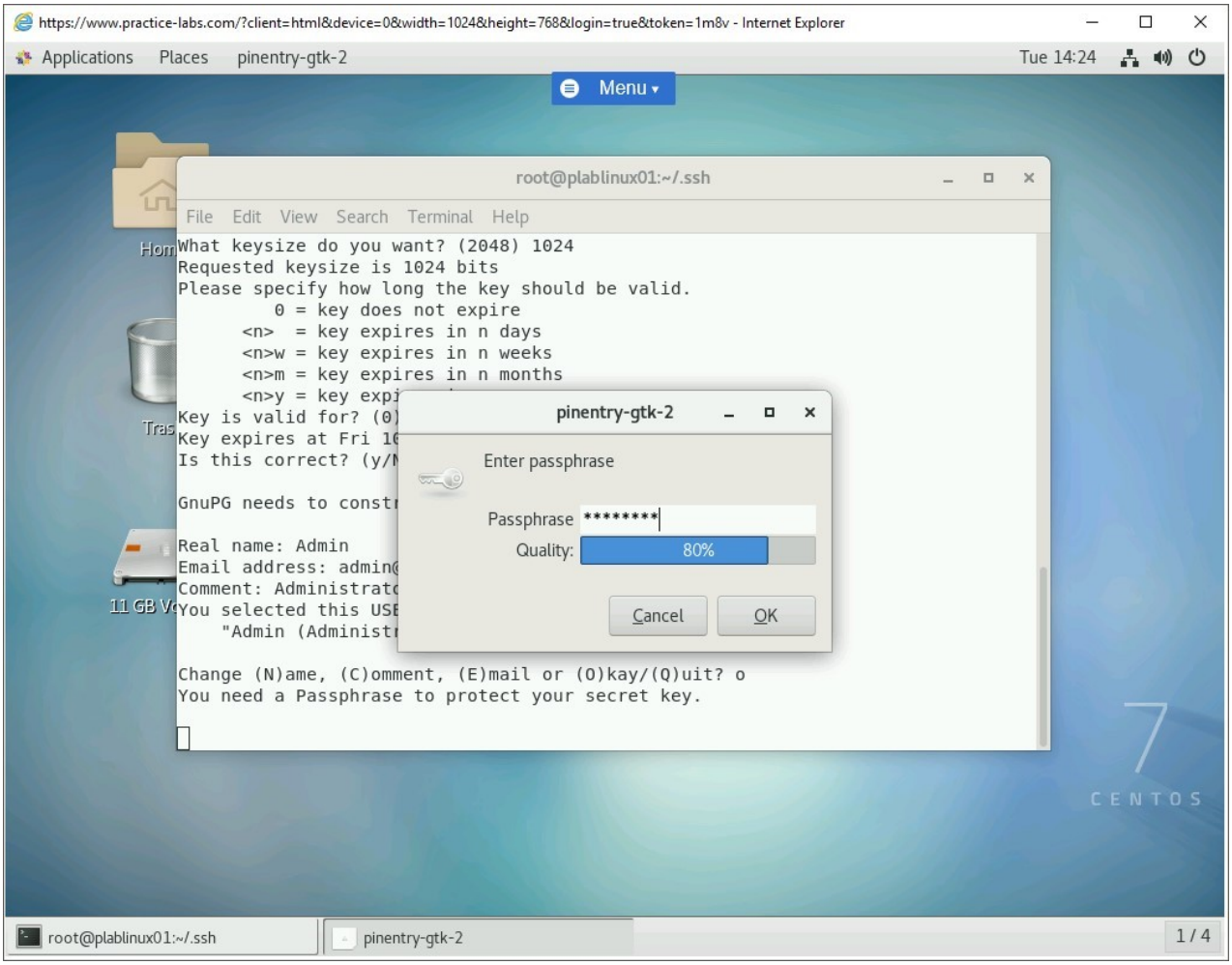


Figure 1.36 Screenshot of PLABLINUX01: Entering a password.

Step 12

You need to now confirmation passphrase. Enter **`Passw0rd`** once again.

Click **OK**.

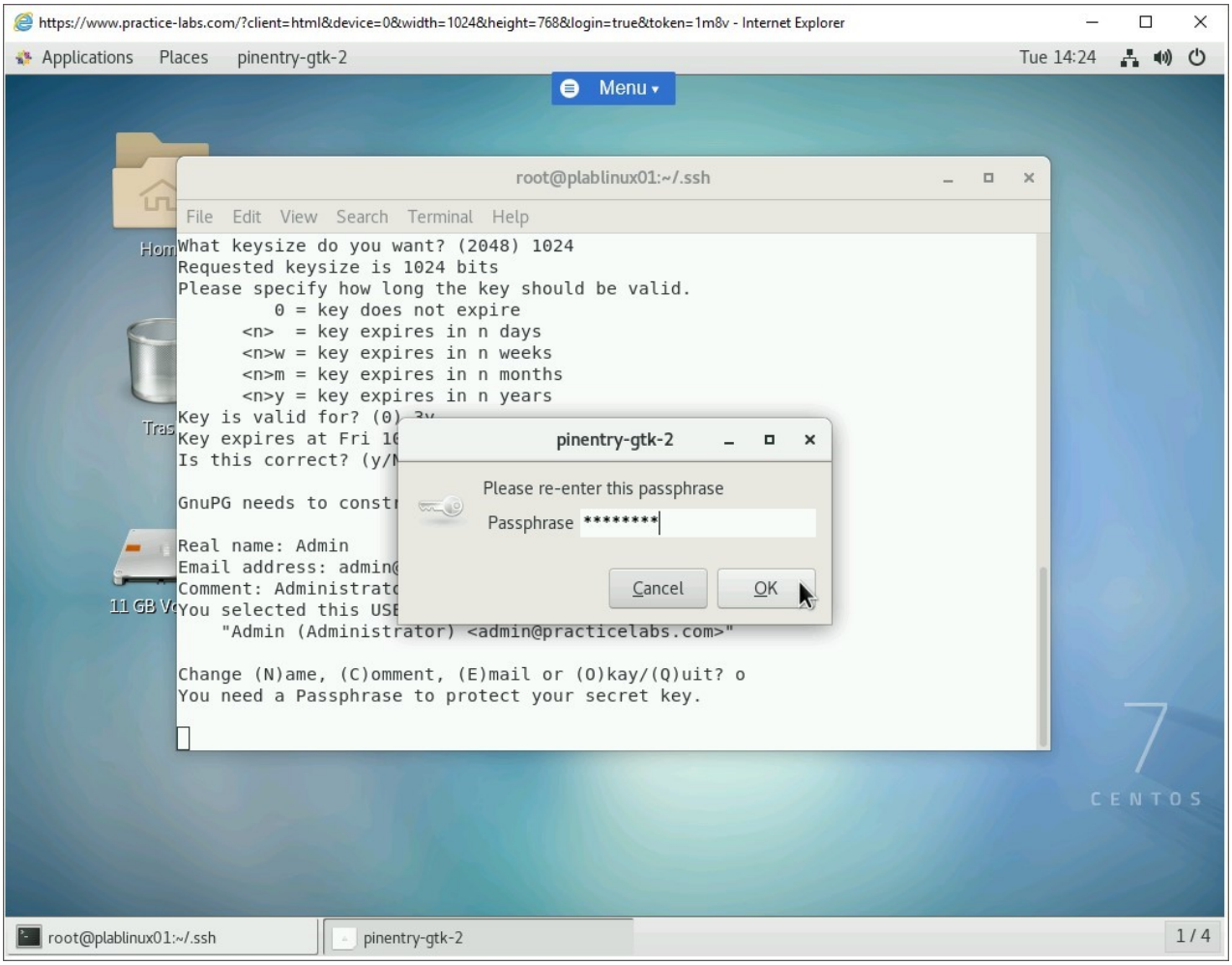


Figure 1.37 Screenshot of PLABLINUX01: Confirming the password.

Step 13

You are prompted that more bytes are required to generate random keys. You will need to do some more tasks in the system. For example, you can ensure some disk utilization by copying files from one directory to another directory. You can open applications or download applications and install them.

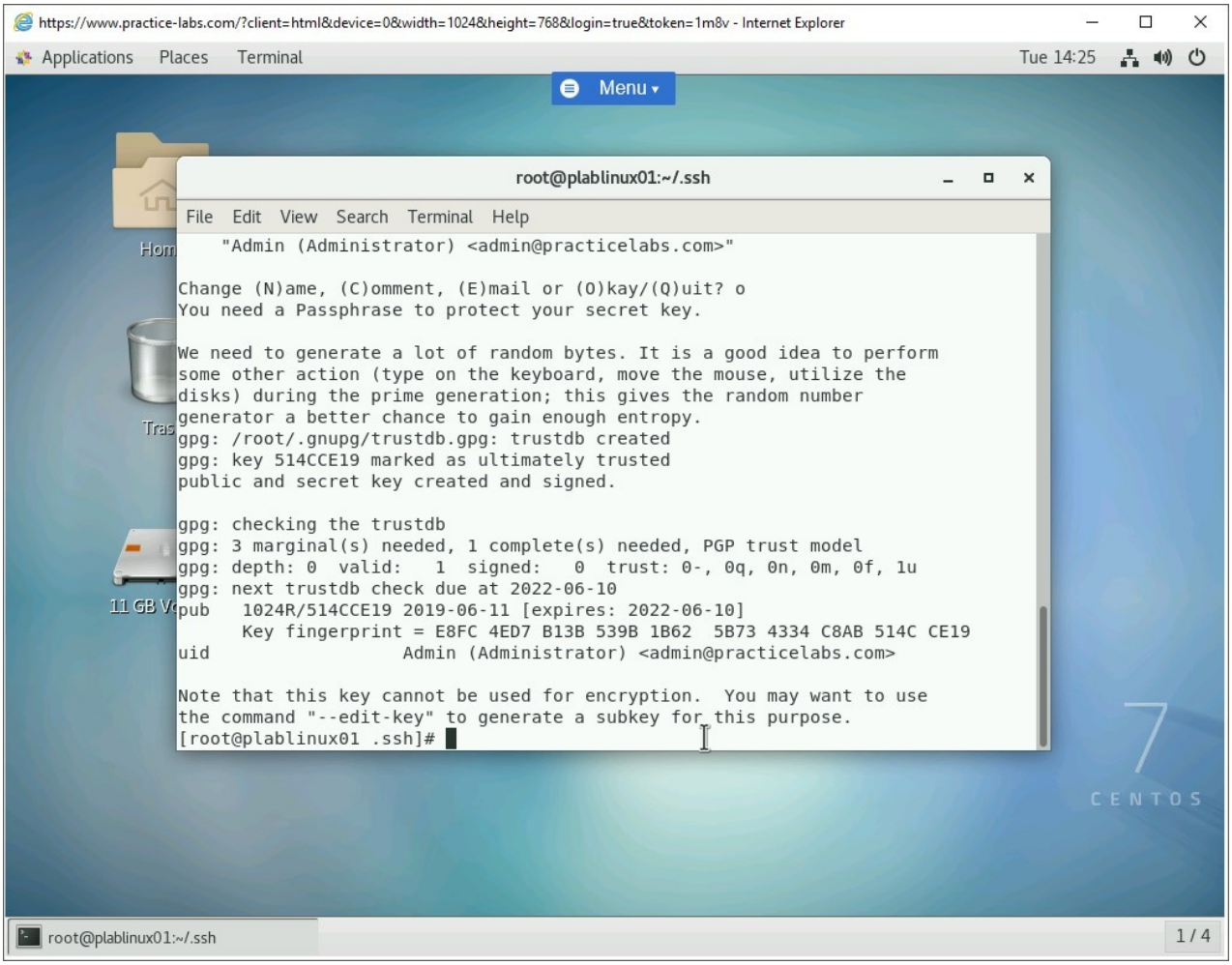


Figure 1.38 Screenshot of PLABLINUX01: Generating random bytes.

Step 14

After doing various activities to generate the bytes, the required number of bytes is generated, the keys are generated.

> ***Note**: This process may take a while depending upon the number of bytes required. In this task, it took a little more than 30 minutes to generate these bytes.*

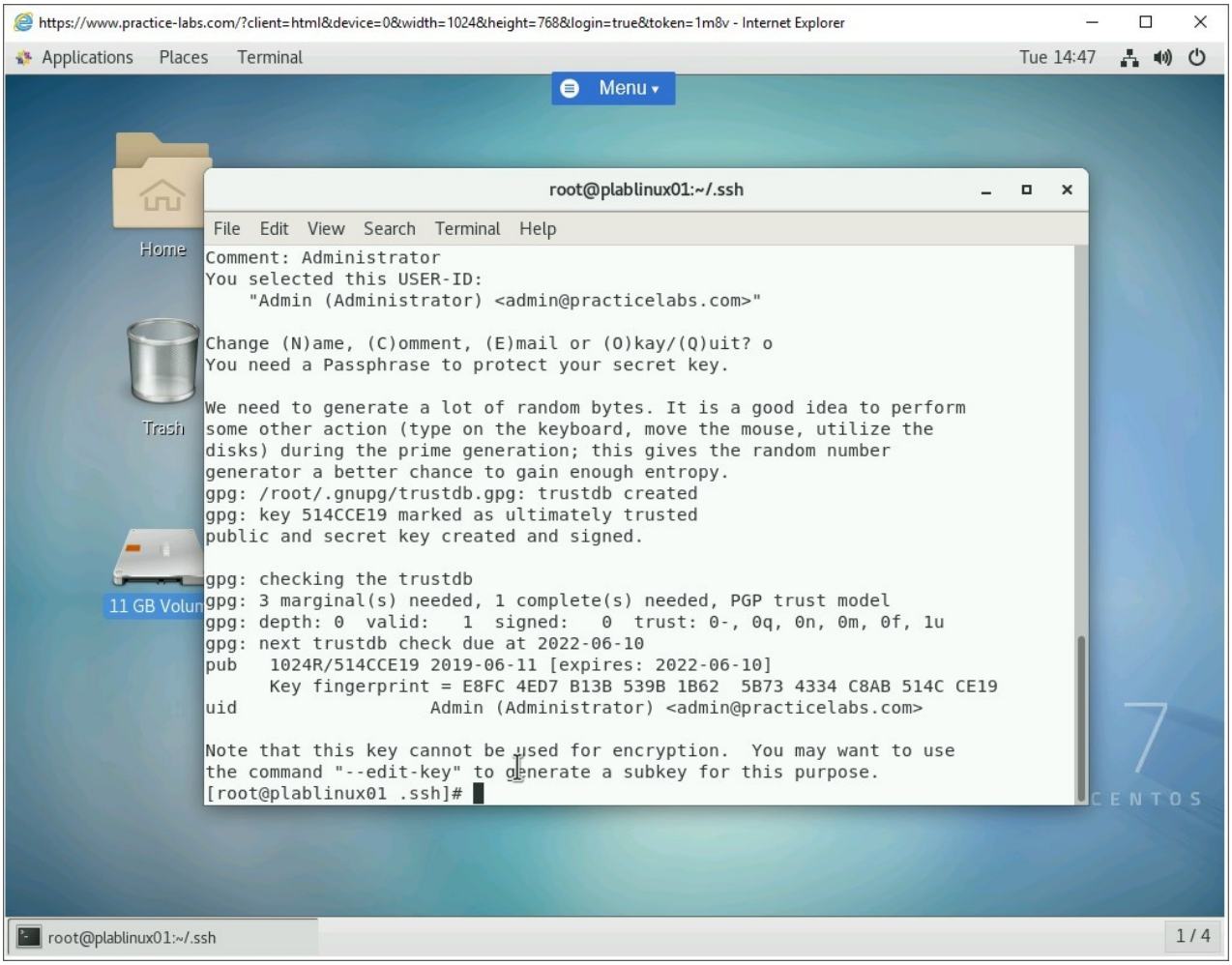


Figure 1.39 Screenshot of PLABLINUX01: Generating random bytes.

Step 15

Clear the screen by entering the following command:

```
clear
```

To verify the fingerprint of the **admin** public key, type the following command:

```
sudo gpg --fingerprint admin
```

Press **Enter**.

If prompted, type the following password:

`Passw0rd`

Press **Enter**.

The details, such as public key and UID of the administrator is displayed.

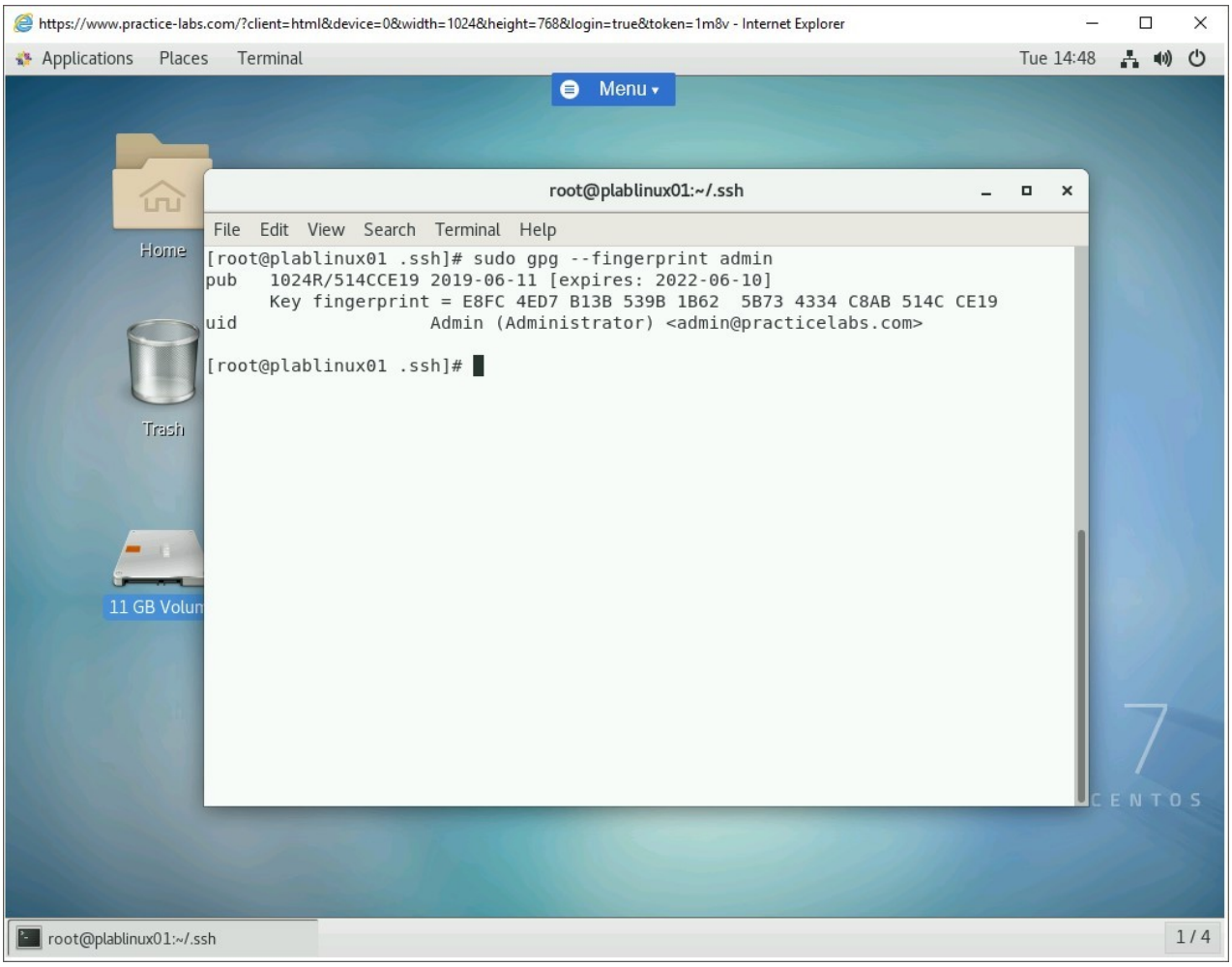


Figure 1.40 Screenshot of PLABLINUX01: Verifying the fingerprint of the admin public key.

Step 16

You can also backup your key. Type the following command to make the backup:

```
sudo gpg --export-secret-keys --armor admin >
admin_private.asc
```

Press **Enter**.

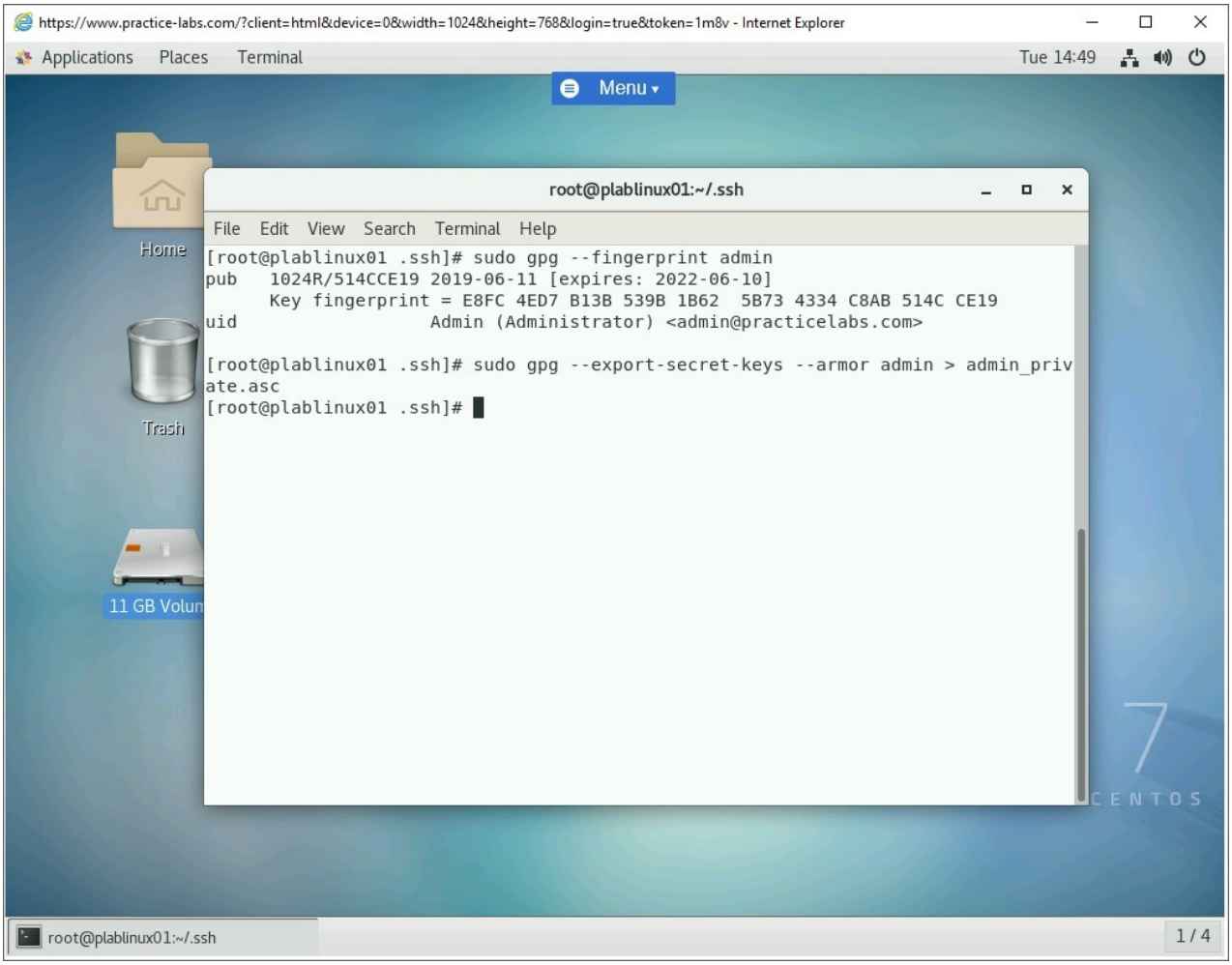


Figure 1.41 Screenshot of PLABLINUX01: Backing up the key pair.

Step 17

You can also share the public key manually, and you can copy it into an ASCII file. Type the following command:

```
sudo gpg --export --armor admin > admin-pub.asc
```

Press **Enter**.

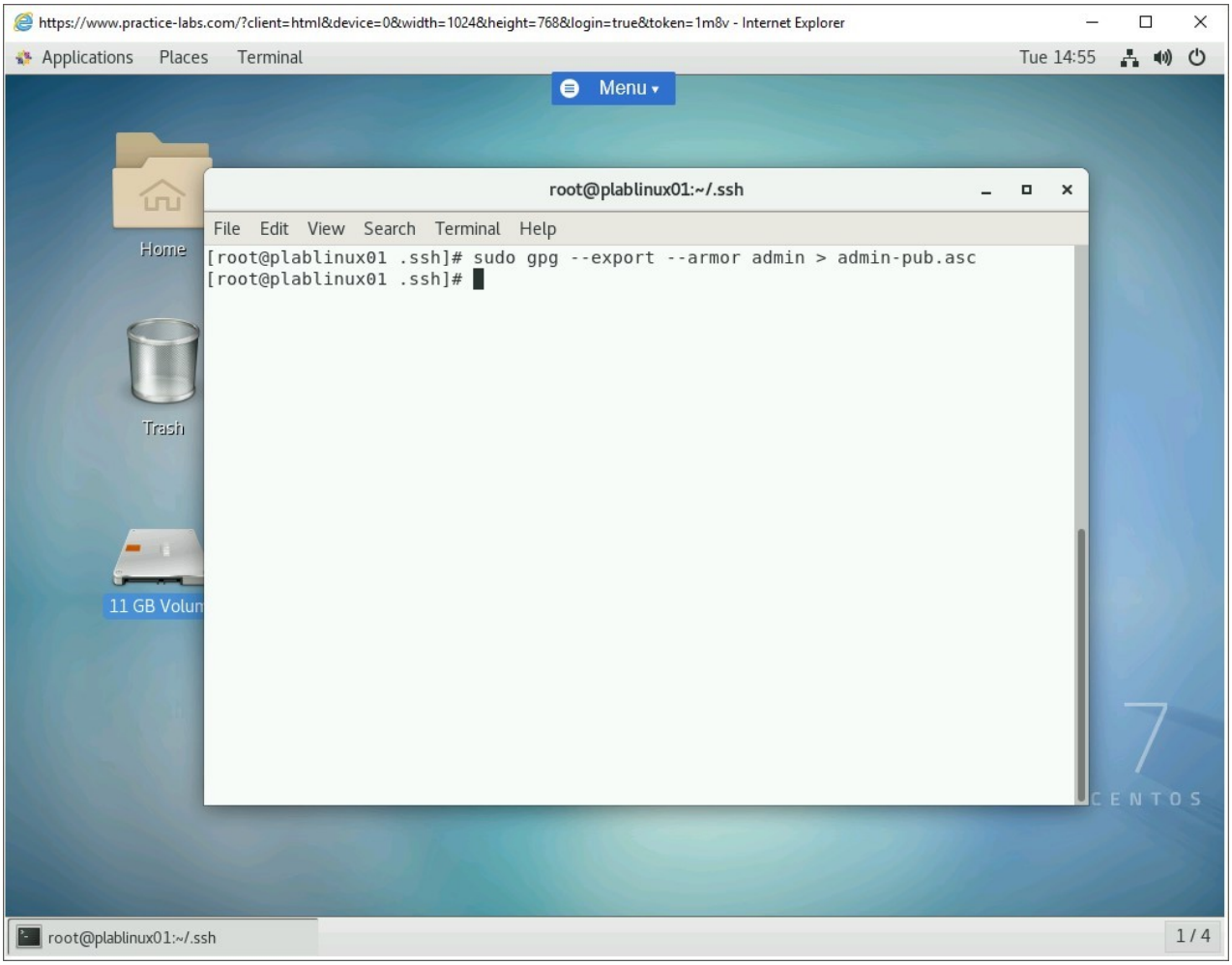


Figure 1.42 Screenshot of PLABLINUX01: Sharing the public key manually and copying it into an ASCII file.

Step 18

When you create the key pair, as a best practice, you should create a key revocation certificate along with it. This certificate notifies the users that the public key is revoked and should not be used.

To create a revocation certificate, type the following command:

```
sudo gpg --output revoke.asc --gen-revoke admin
```

Press **Enter**.

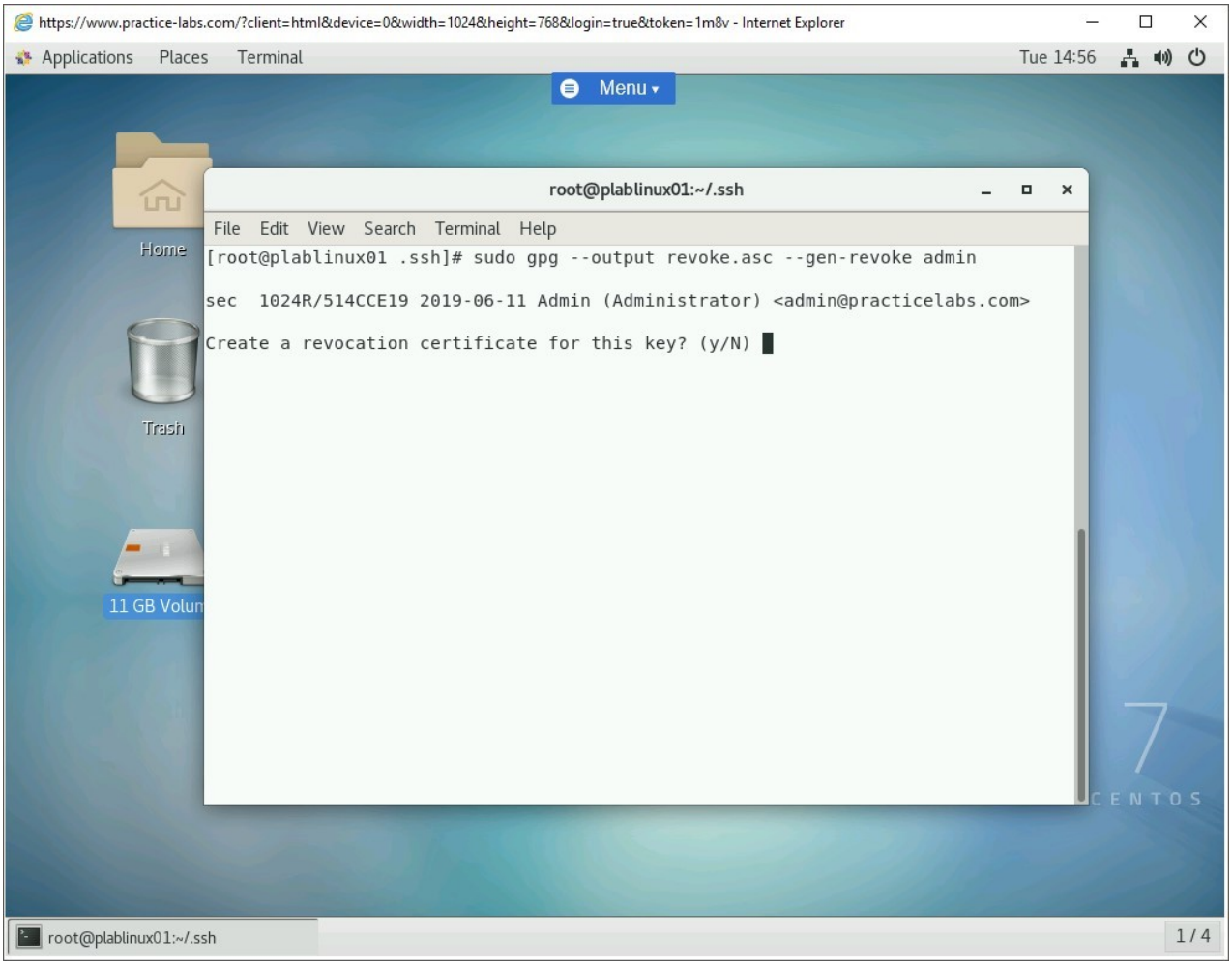


Figure 1.43 Screenshot of PLABLINUX01: Creating a revocation certificate.

Step 19

Type **y** to generate the revocation certificate.

Press **Enter**.

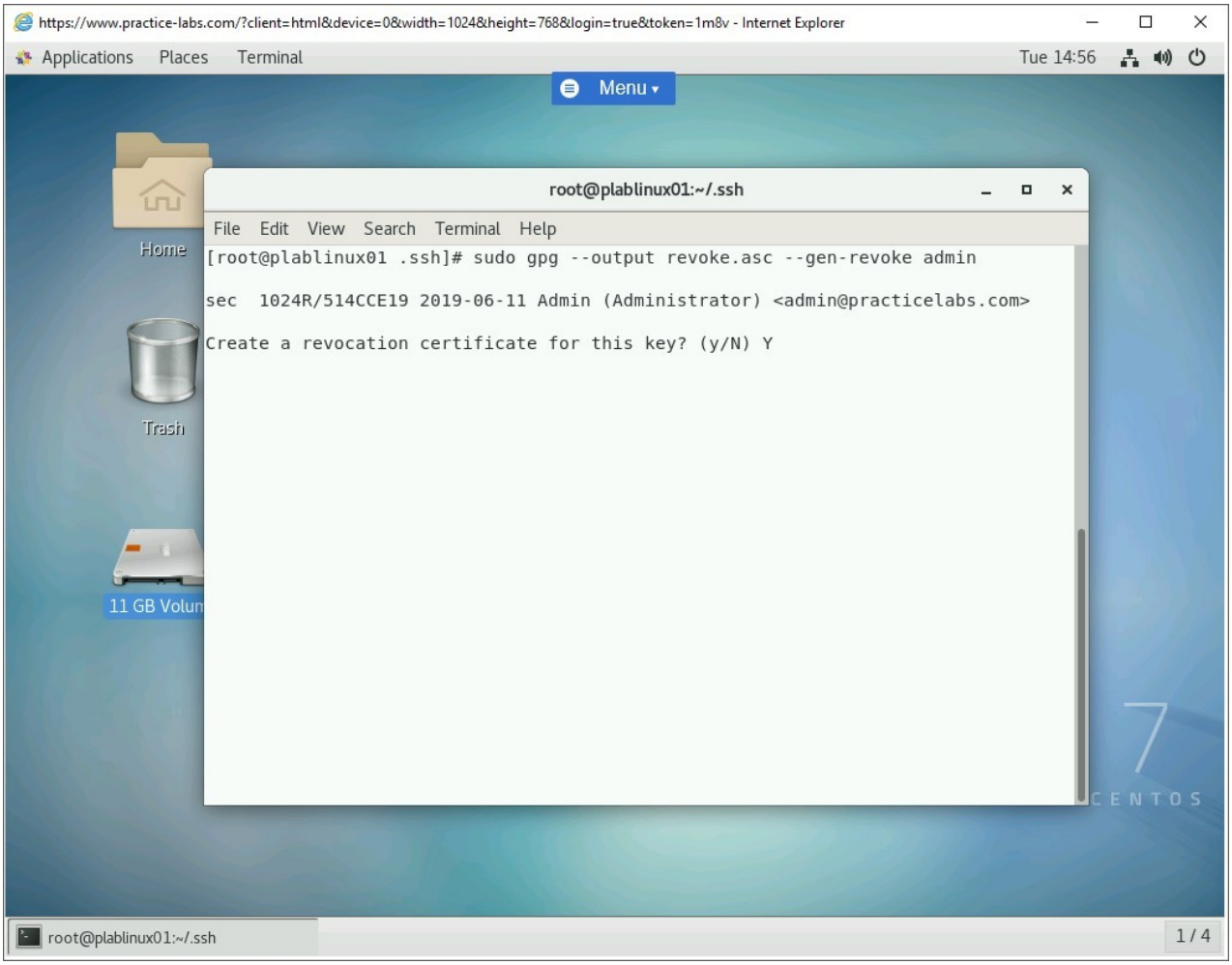


Figure 1.44 Screenshot of PLABLINUX01: Generating the revocation certificate.

Step 20

When prompted to select an option, type **0**.

Press **Enter**.

> ***Note:*** *0 is zero.*

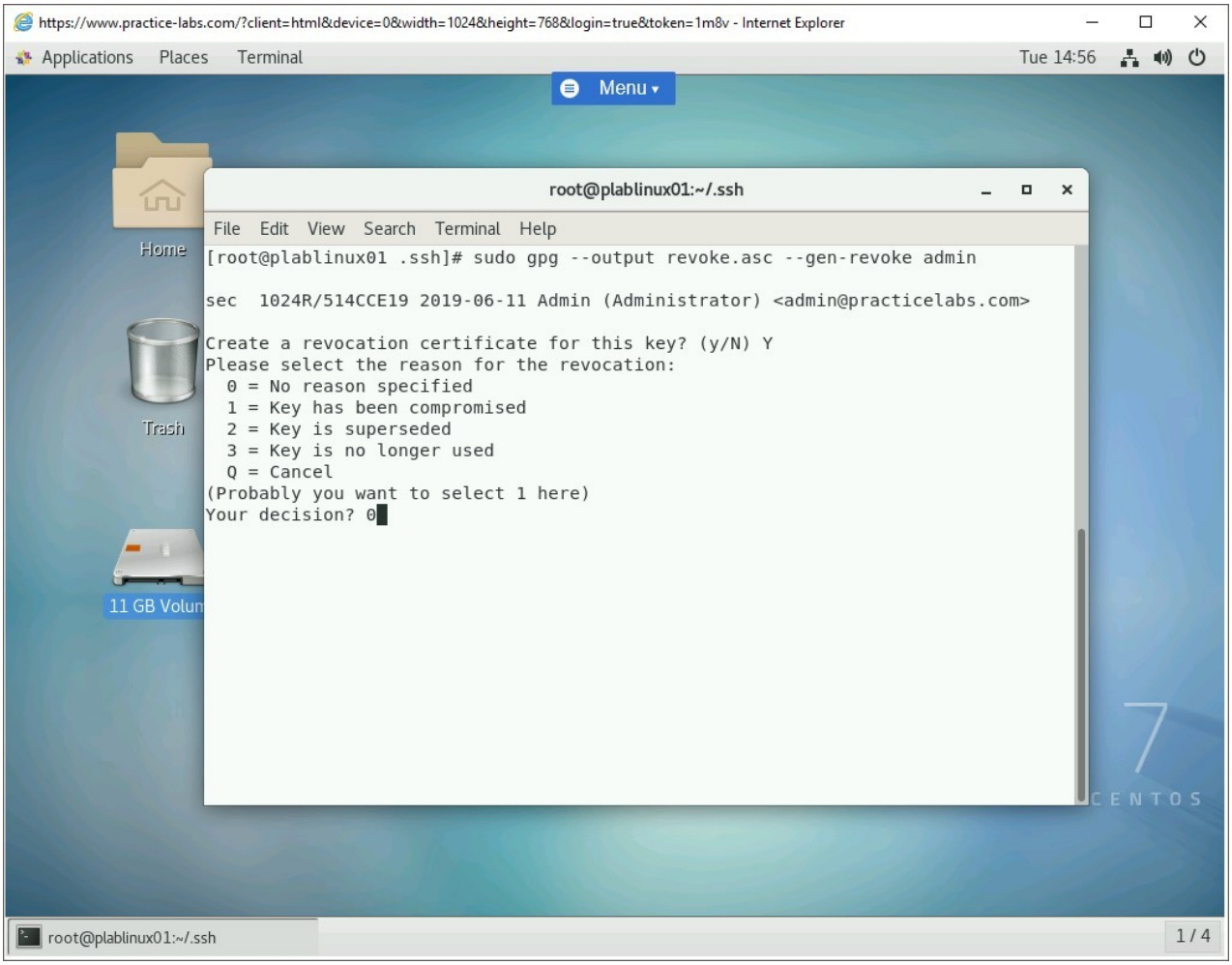


Figure 1.45 Screenshot of PLABLINUX01: Selecting no reason specified.

Step 21

You are prompted to enter a description. Press **Enter**.

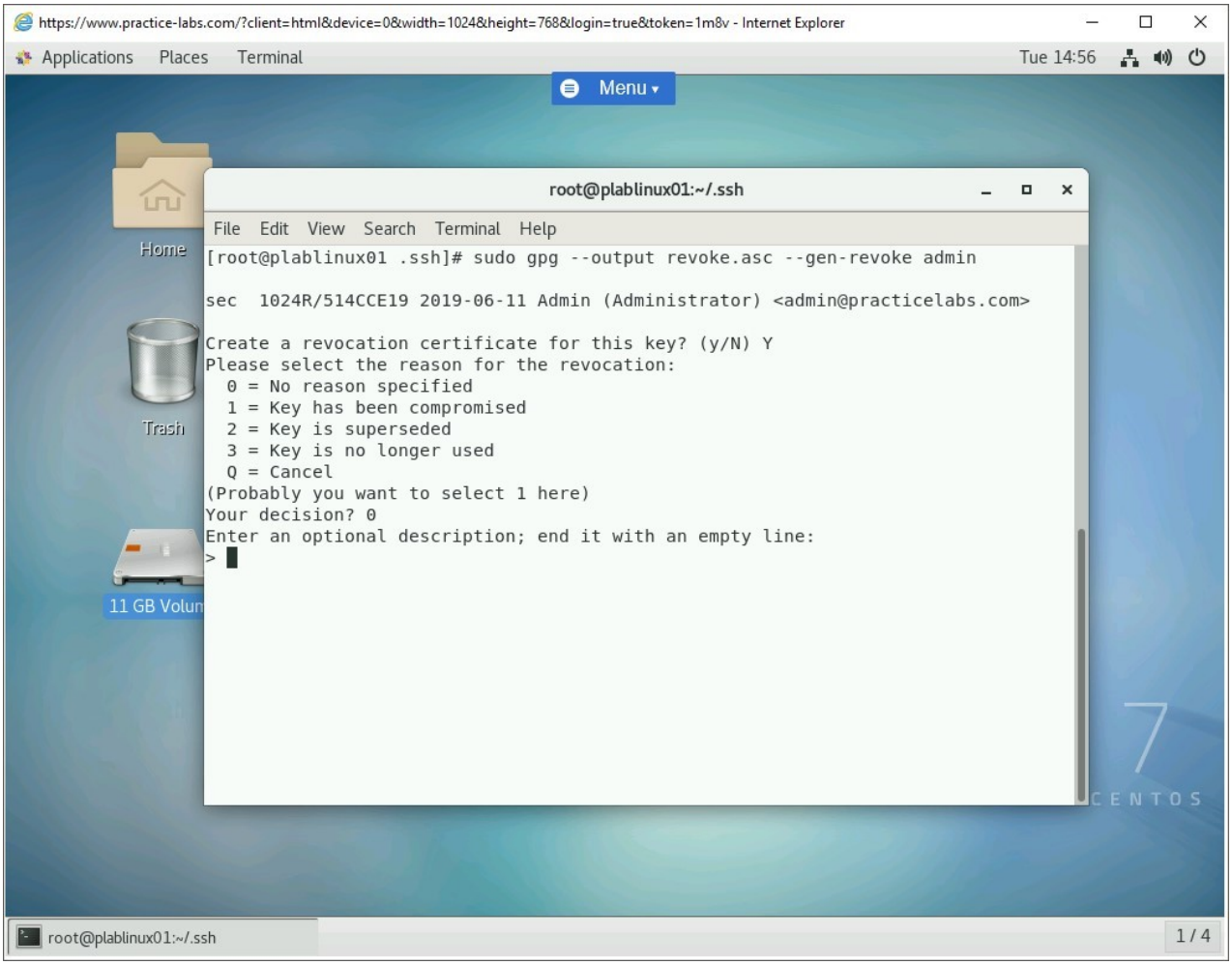


Figure 1.46 Screenshot of PLABLINUX01: Entering the description.

Step 22

Since you have not specified any reason for certificate revocation, Type **y**.

Press **Enter**.

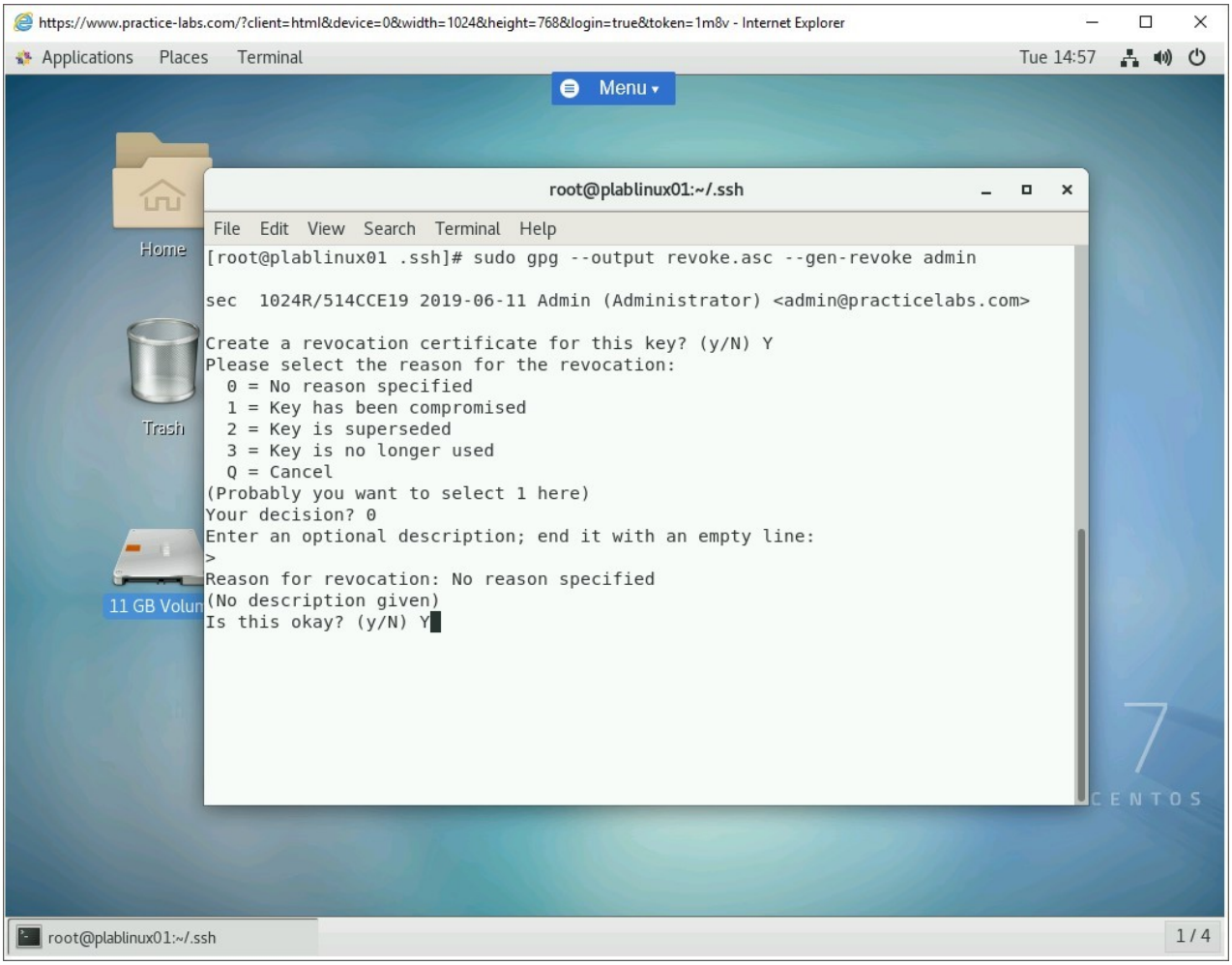


Figure 1.47 Screenshot of PLABLINUX01: Specified the reason for certificate revocation.

Step 23

When a key is generated, it is locked by default. You are prompted to unlock the key with the original password.

When prompted, type the following password:

`Passw0rd`

Click **OK**.

The key will be unlocked.

> ***Note**: Recall that this is the passphrase specified while defining various parameters to create the secret key.*

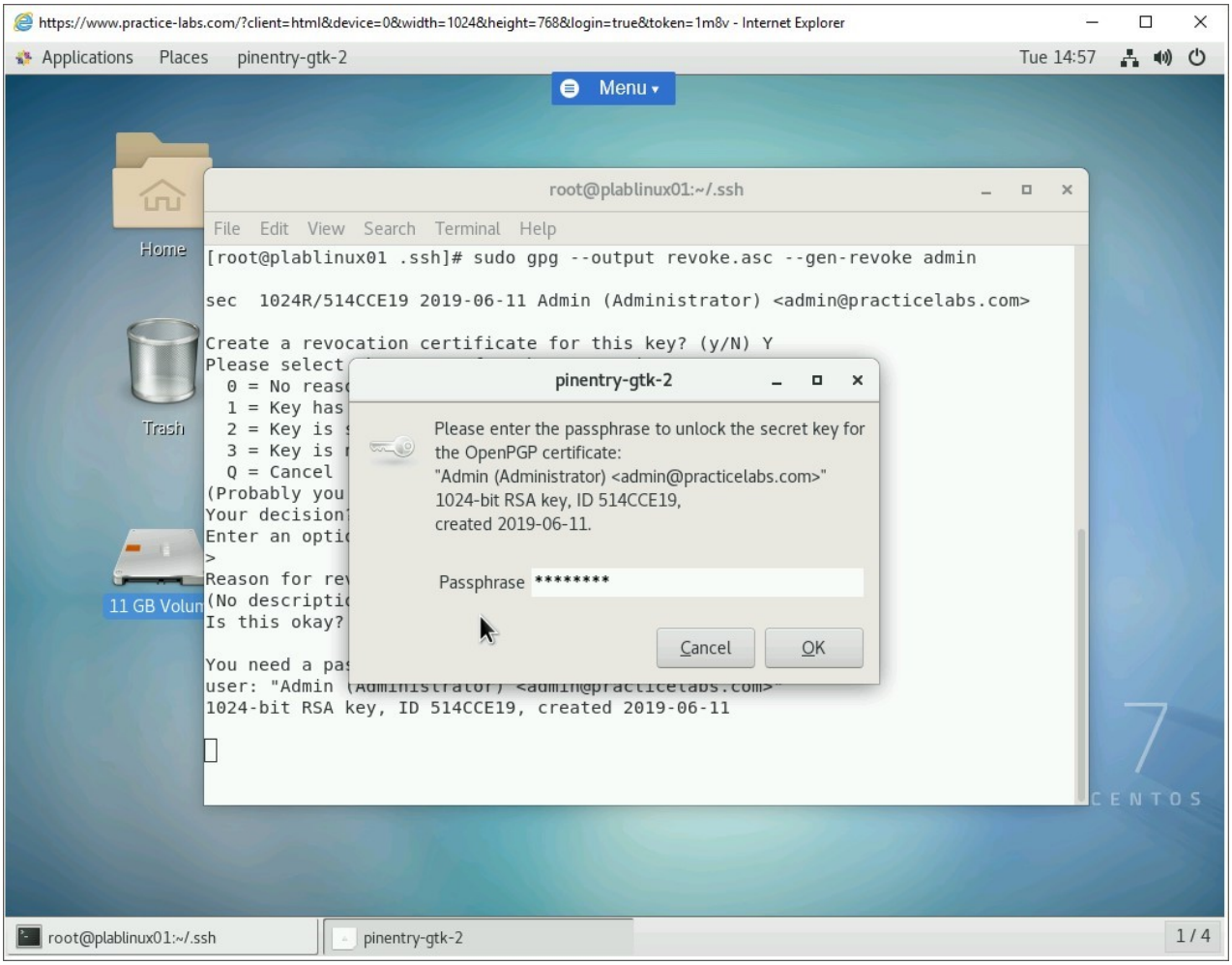


Figure 1.48 Screenshot of PLABLINUX01: Entering the password.

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

Review

Well done, you have completed the **Securing Data with Encryption** Practice Lab.

Summary

You completed the following exercise:

- Exercise 1 - Securing Data with Encryption

You should now be able to:

- Perform Basic OpenSSH 2 client configuration and usage
- Understand the role of OpenSSH 2 server host keys

- Perform basic GnuPG management

Feedback

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