Exercise 1 - Setup Host Security

Setting up host security is all the more relevant and required in the current networked multi-user environment. In this exercise, you will understand how to setup host security.

Learning Outcomes

After completing this exercise, you will be able to:

- Log into a Linux system
- Shadow passwords
- Turn off network services not in use
- Role of TCP wrappers

Task 1 - Shadow Passwords

In a multi-user environment, it is important to encrypt passwords to protect them against unauthorized access. The passwords are moved from the /etc/passwd file to the /etc/shadow file. This file is readable only by the root user. Shadow password is enabled by default by the shadow-utils package. In this task, you will list the contents of both - password file and the shadow file. You will also create a nologin file.

To view the shadow passwords, perform the following steps:

Step 1

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

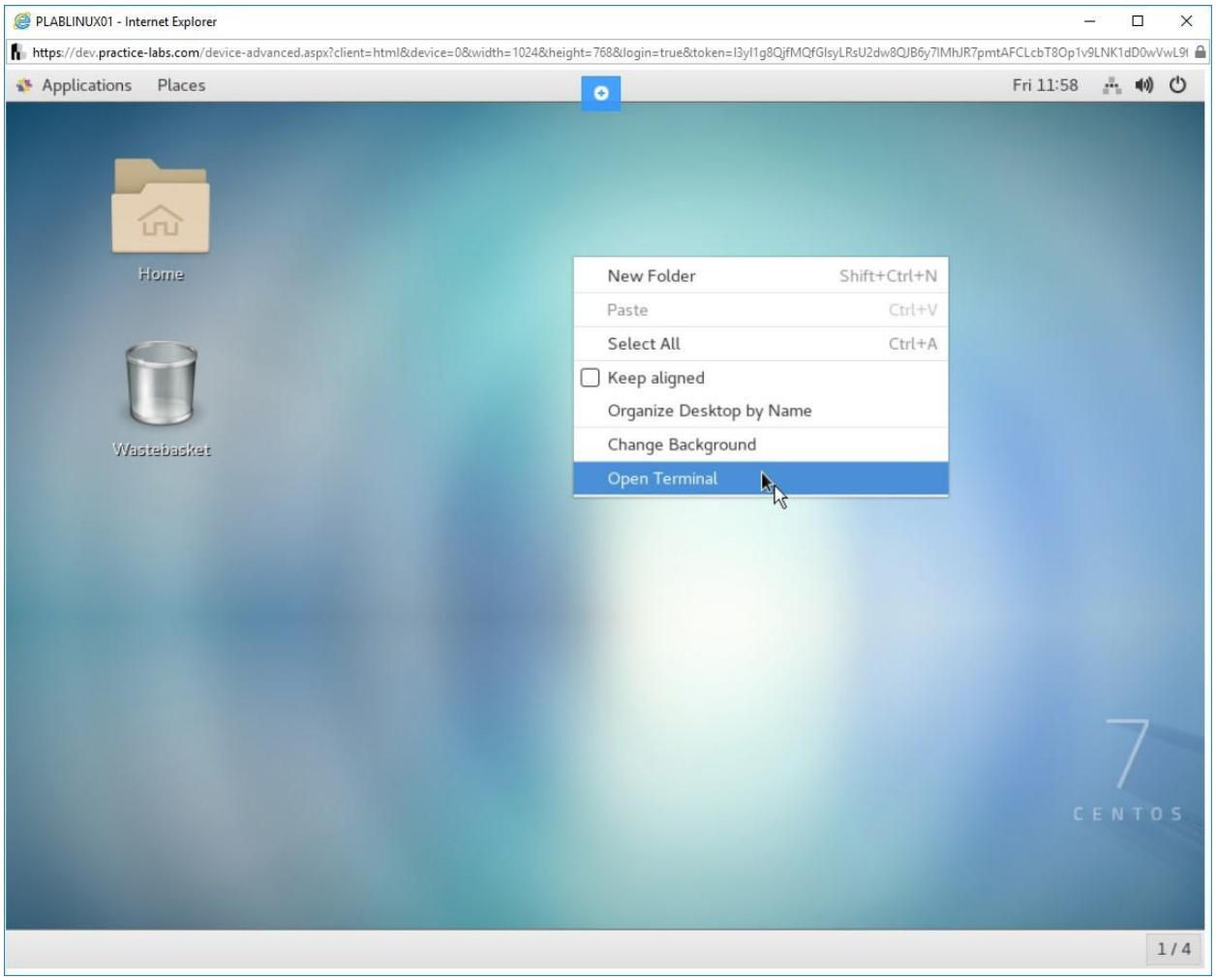

Figure 1.1 Screenshot of PLABLINUX01: Selecting the Open Terminal option from the context menu.

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.

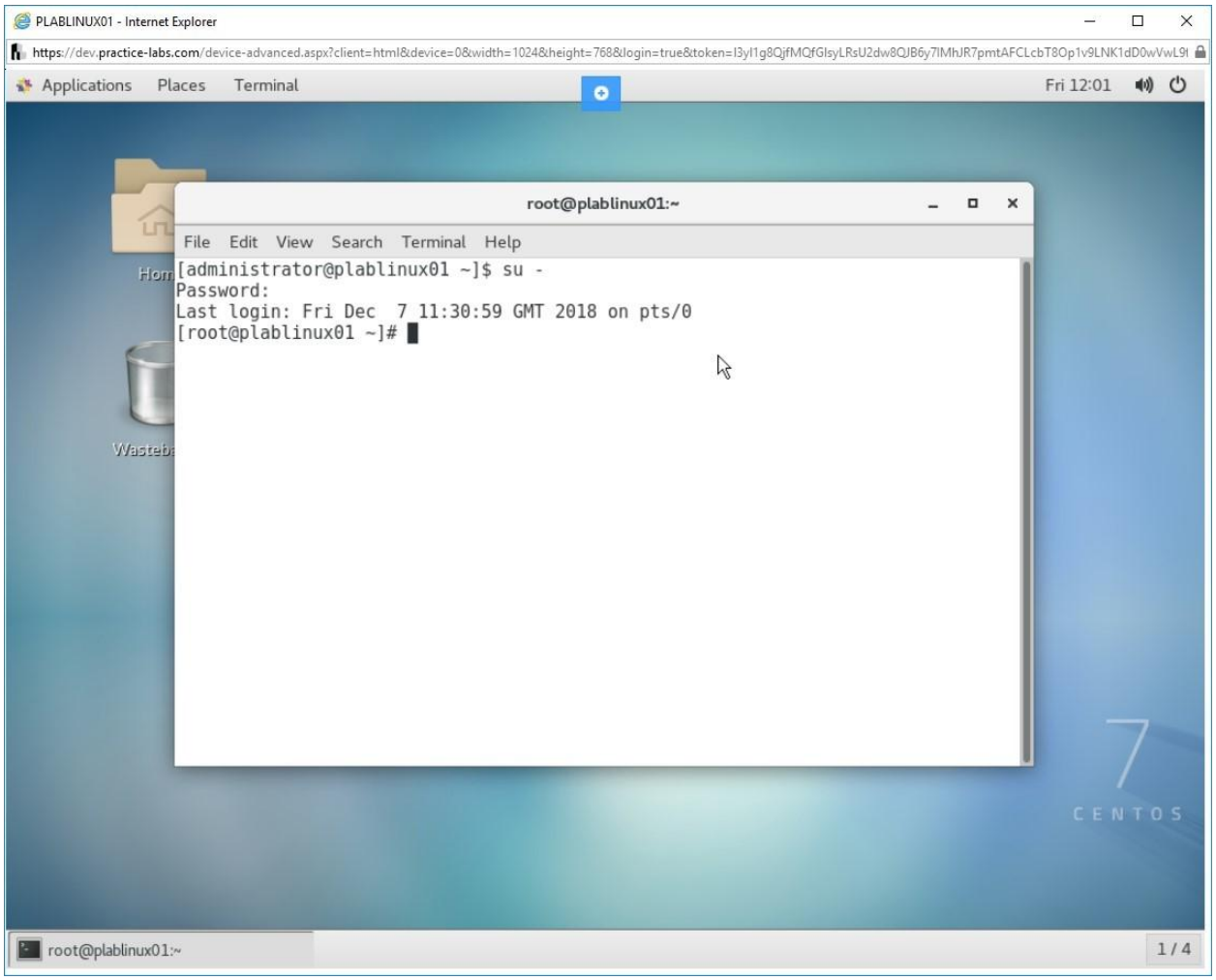

Figure 1.2 Screenshot of PLABLINUX01: Changing the account to the root account with the su command.

Step 3

Clear the screen by entering the following command:

```
clear
```

Press Enter.

Note: The clear command is used before every step to enable the learners to get a clear view of the output of each command. Otherwise, it is not mandatory to use the clear command before every command.

To view the /etc/passwd file, type the following command

```
cat /etc/passwd
```

Press Enter.

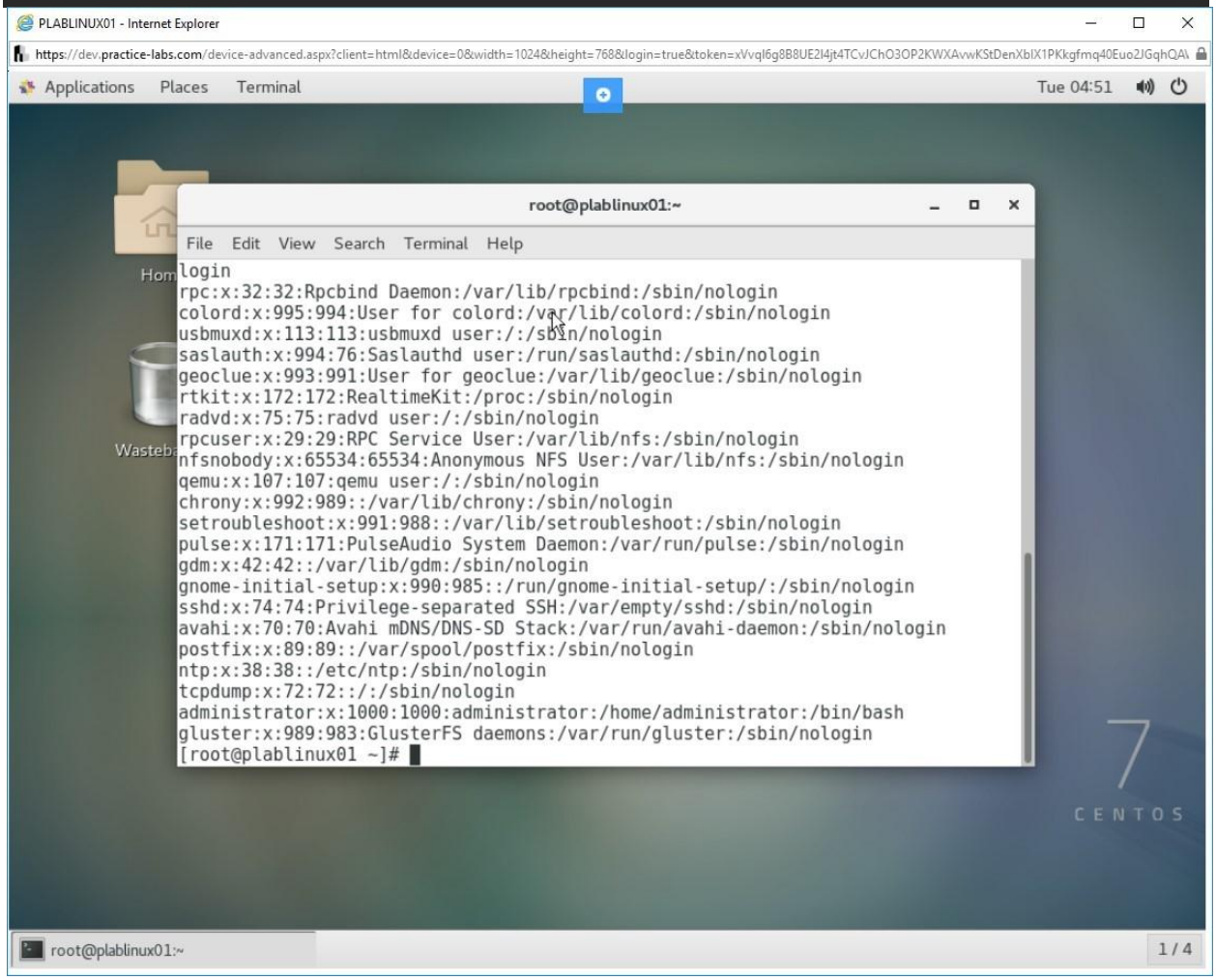

Figure 1.3 Screenshot of PLABLINUX01: Viewing the /etc/passwd file.

Step 4

Clear the screen by entering the following command:

```
clear
```

Press Enter.

To view the /etc/shadow file, type the following command

```
cat /etc/shadow
```

Press Enter.

Note that all passwords are encrypted.

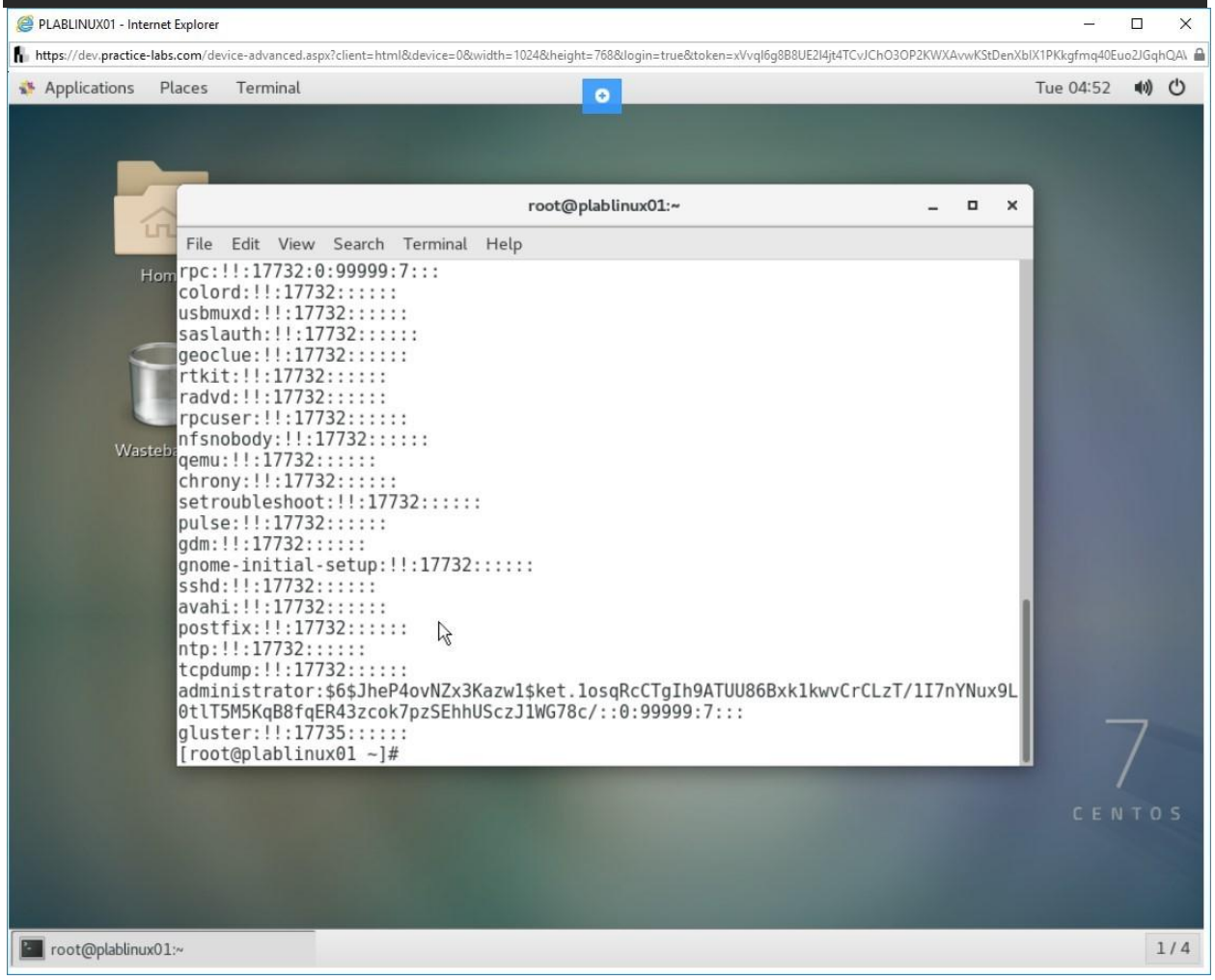

Figure 1.4 Screenshot of PLABLINUX01: Viewing the /etc/shadow file.

Step 5

Clear the screen by entering the following command:

```
clear
```

Press Enter.

You can also disable logins into the system by creating the /etc/nologin file. By default, this file does not exist. If you create this file, only the root user will able to log on to the system. Login access to the remaining users will be disabled. To do this, type the following command:

```
touch /etc/nologin
```

Press Enter.

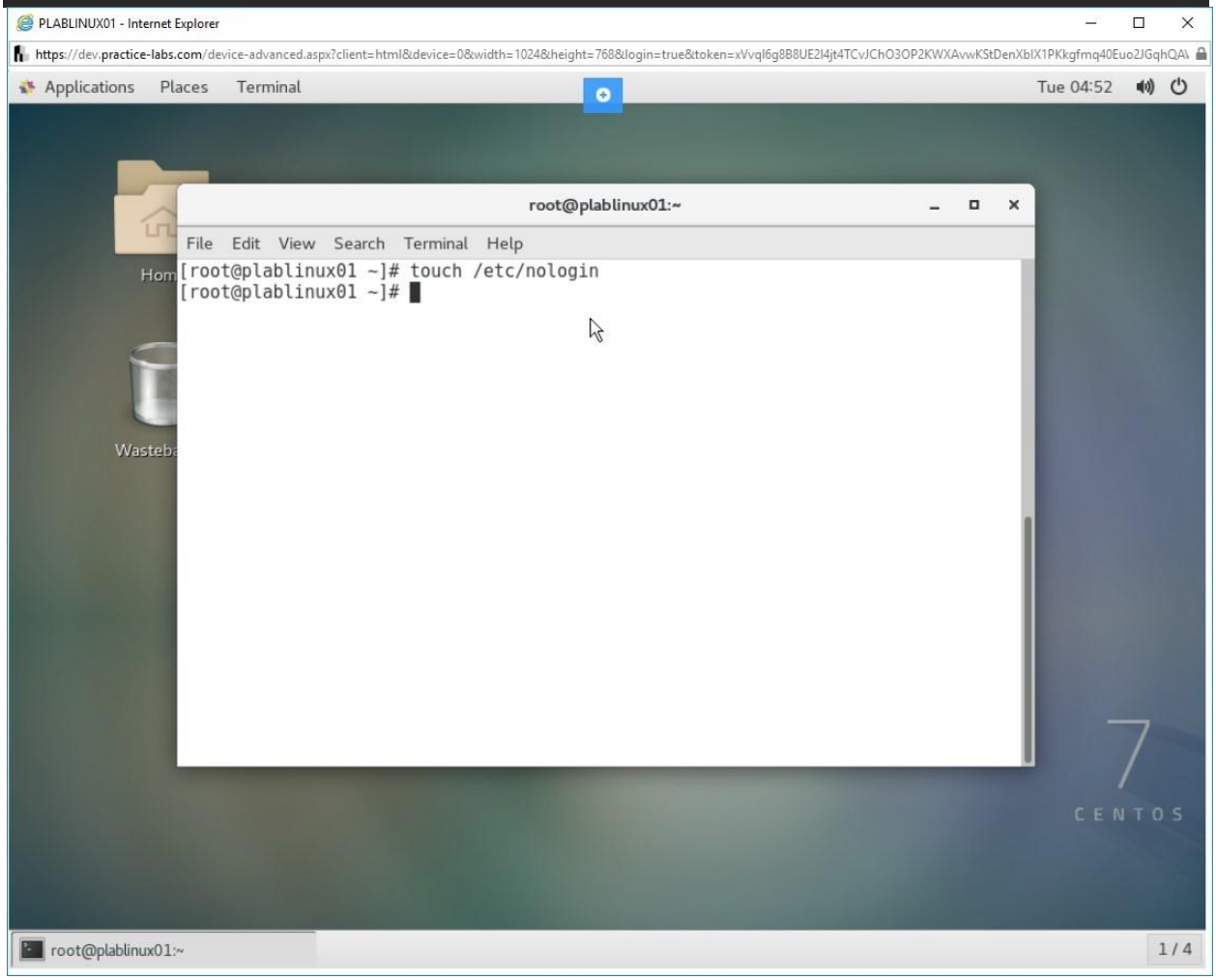

Figure 1.5 Screenshot of PLABLINUX01: Creating a new file named /etc/nologin with the touch command.

Step 6

The /etc/nologin file just needs to be there without anything inside it. To view the file, type the following command:

```
cat /etc/nologin
```

Press Enter.

Note that there are no contents in the file. It is blank.

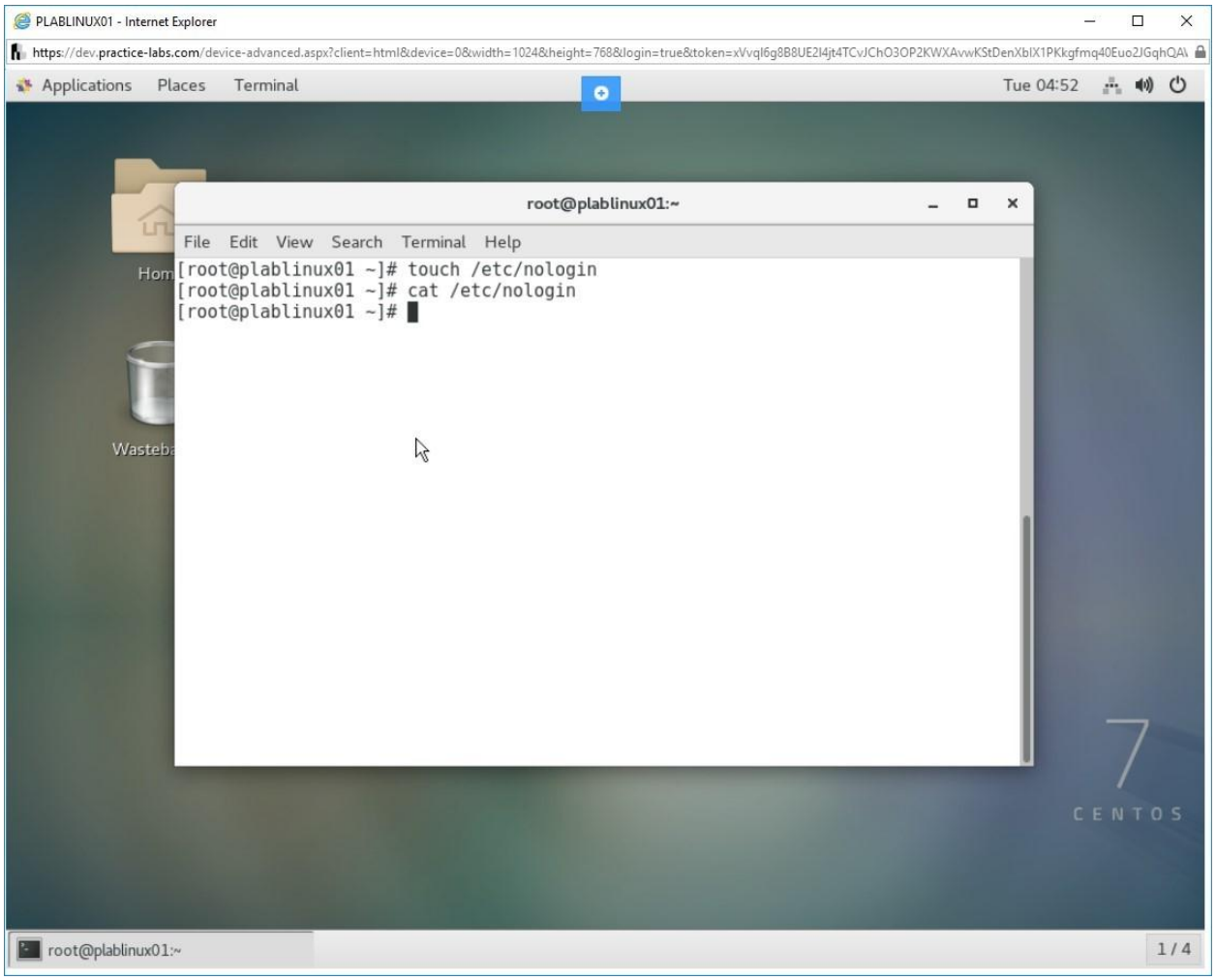

Figure 1.6 Screenshot of PLABLINUX01: Viewing the contents of the /etc/nologin file.

Task 2 - Turn off Network Services Not in Use

For system security sake, you should turn off the network services that are not in use. Turning off unnecessary services helps in two ways: reduces the system overhead and also prevents the system from hackers who may use these services to get into the system. To turn off the network services that are not in use, perform the following steps:

Step 1

Clear the screen by entering the following command:

```
clear
```

Press Enter.

Let's first list the SysV services on Centos. Type the following command:

```
chkconfig --list
```

Press Enter.

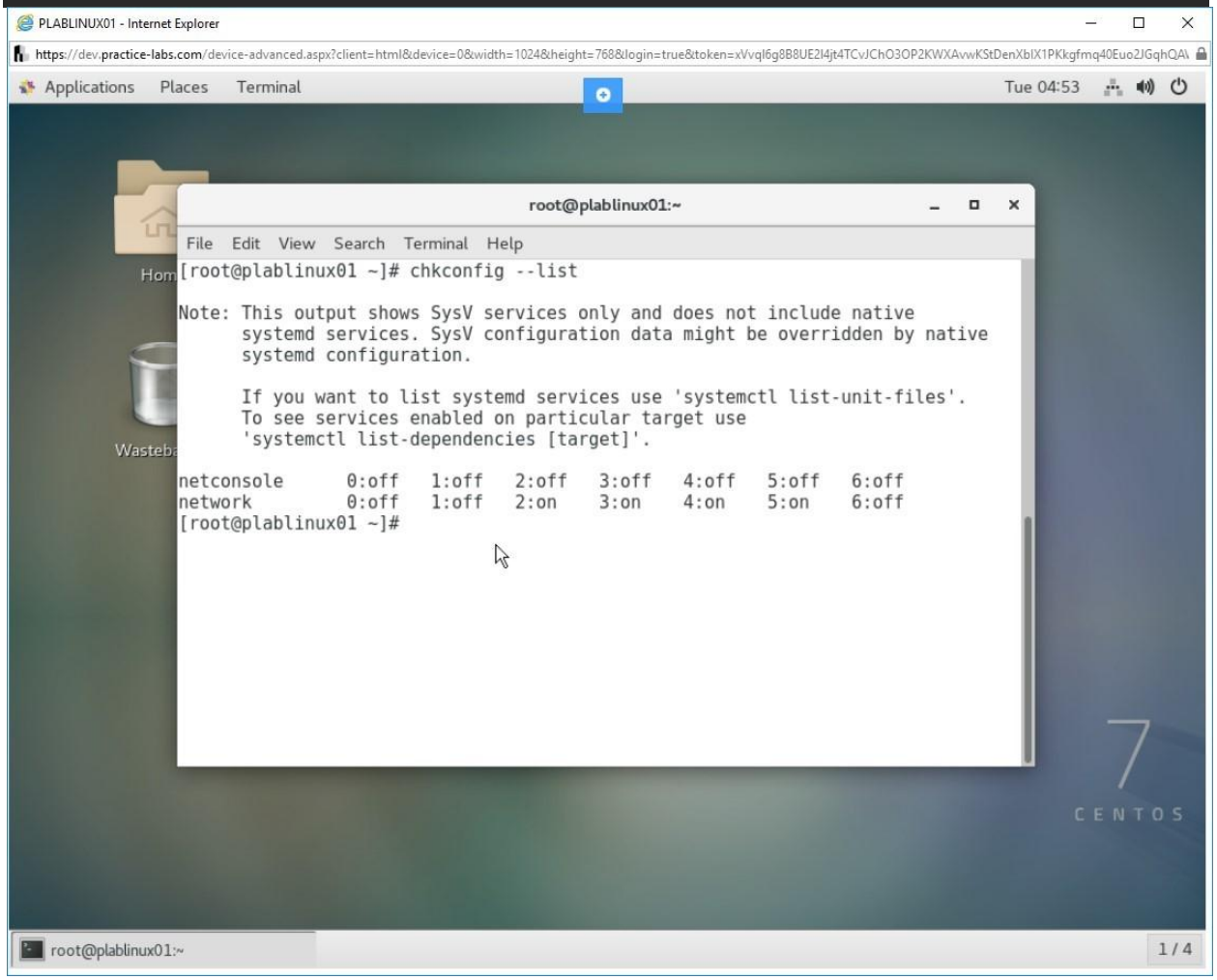

Figure 1.7 Screenshot of PLABLINUX01: Listing the SysV services on Centos.

Step 2

The /etc/init.d directory in a Linux system contains a number of scripts.

These scripts help you start or stop various services and perform some other actions on the services. Using this directory, you can perform the following tasks on a service:

- start
- stop
- reload
- restart
- force-reload

For example, you can stop the netconsole service that you may not require. Type the following command:

```
/etc/init.d/netconsole stop
```

Press Enter.

Note: The service is temporarily stopped for this session. When you log off and log in again, the service will be in the original state that has been defined for it. To define its permanent state, you have to define its runlevel in the /etc/inittab file.

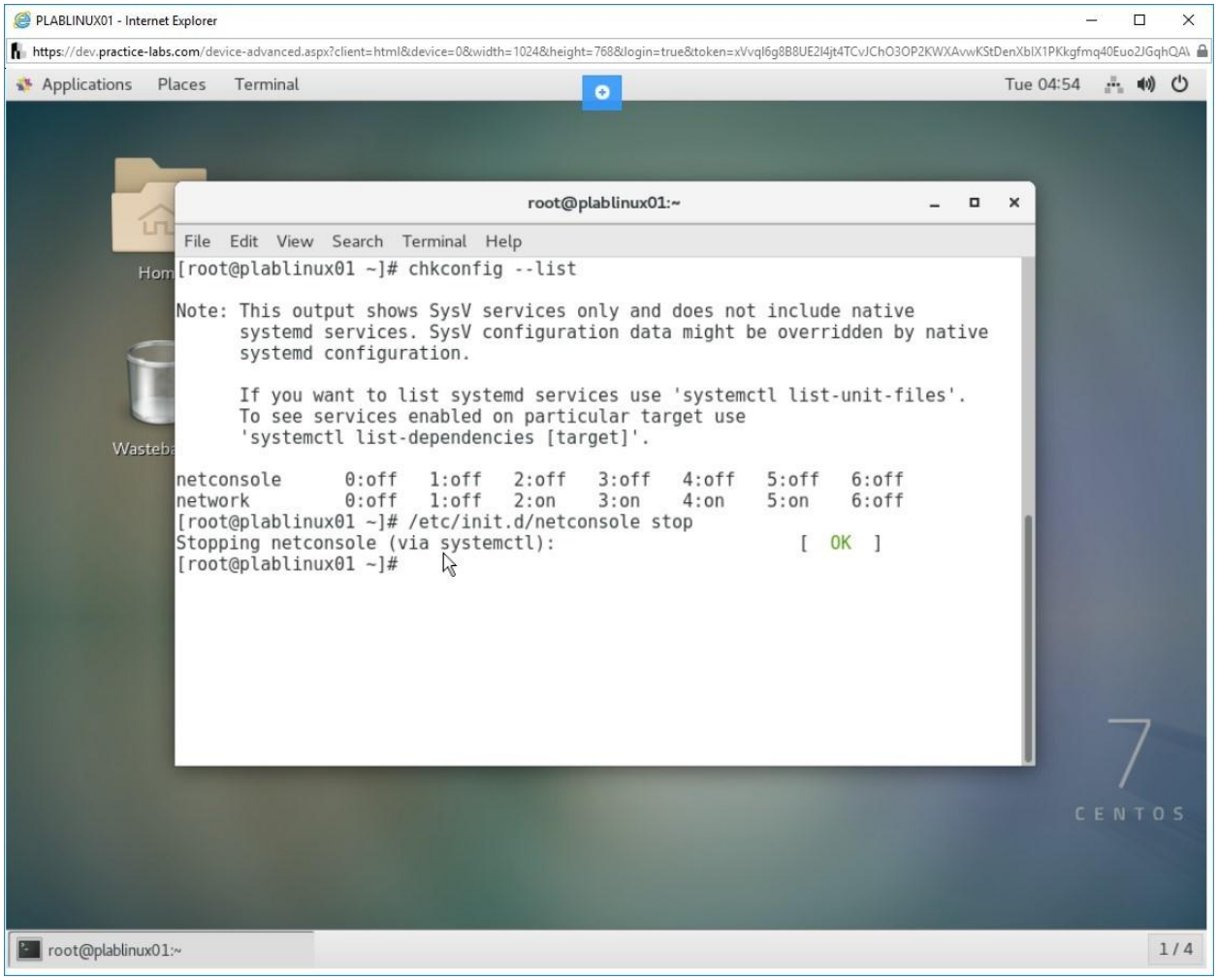

Figure 1.8 Screenshot of PLABLINUX01: Stopping the netconsole service.

Step 3

Clear the screen by entering the following command:

```
clear
```

Press Enter.

You can check whether the inetd daemon is running on your system.

To do this, type the following command:

```
ps aux | grep inetd
```

Press Enter.

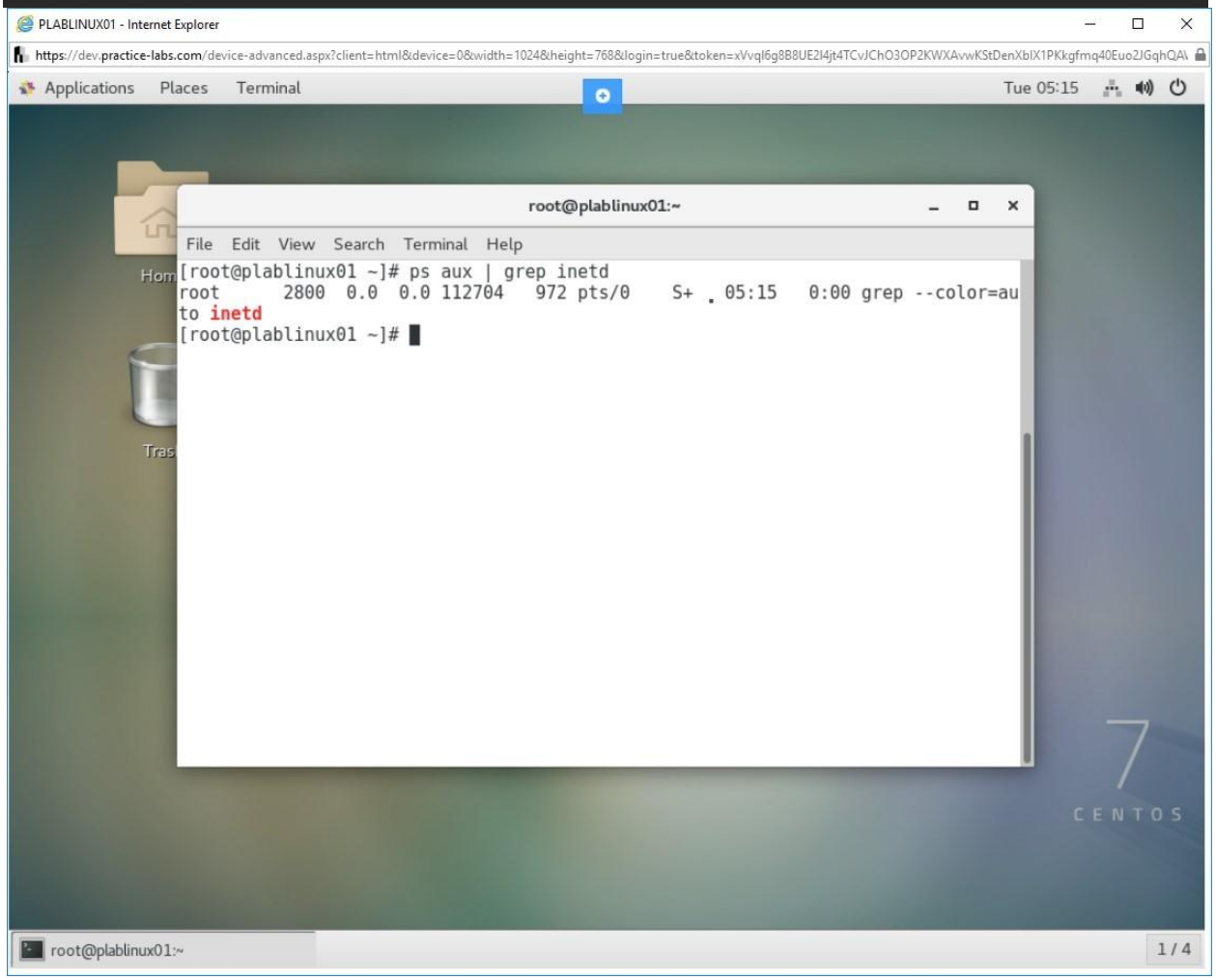

Figure 1.9 Screenshot of PLABLINUX01: Checking the status of the inetd daemon.

Step 4

Clear the screen by entering the following command:

```
clear
```

Press Enter.

To view the runlevel, you can browse through the /etc/inittab file. Type the following command:

```
cat /etc/inittab
```

Press Enter.

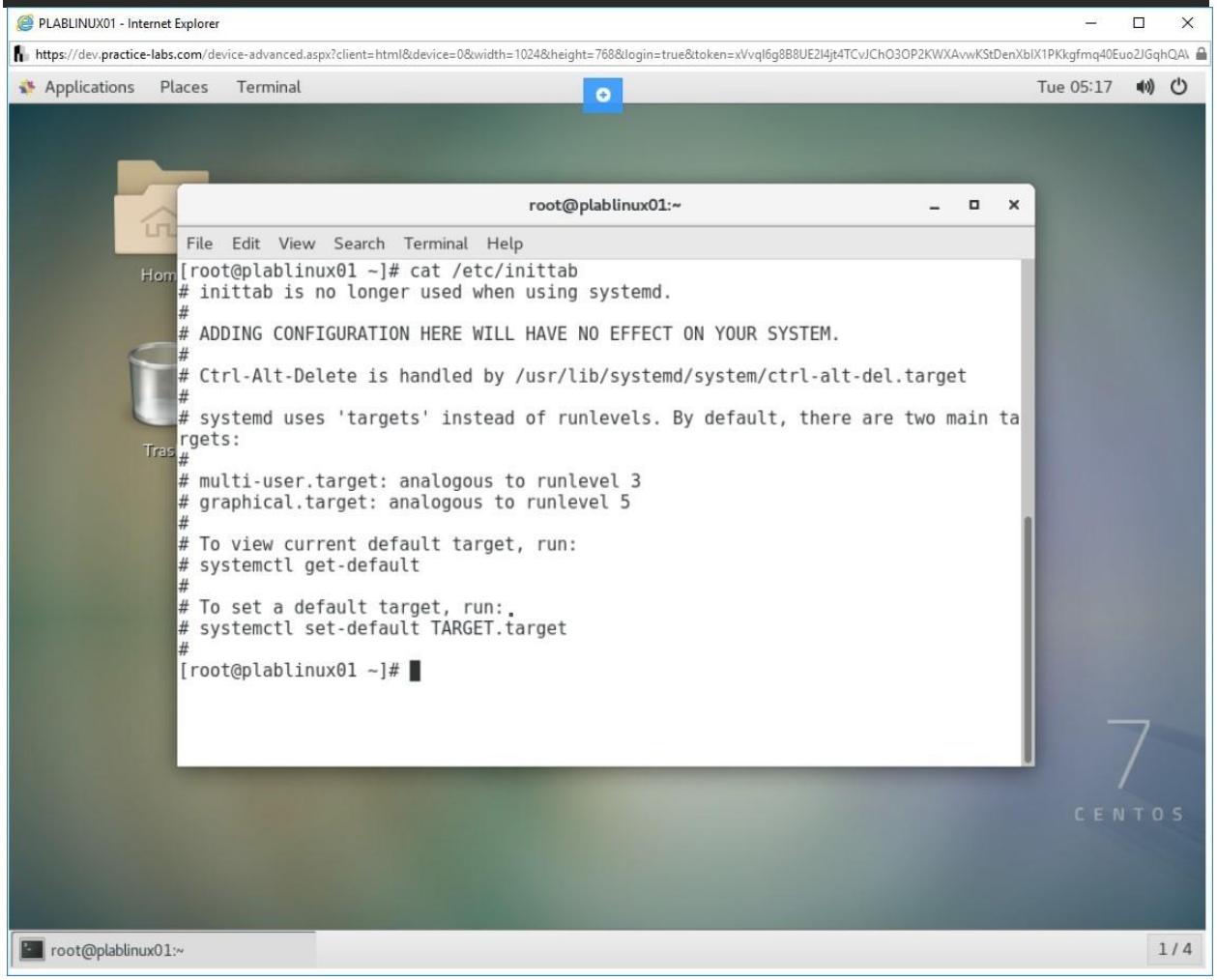

Figure 1.10 Screenshot of PLABLINUX01: Viewing the runlevel configuration in the /etc/inittab file.

Task 3 - Role of TCP Wrappers

For access control, inetd and xinetd files use the TCP_WRAPPER service. The xinetd binary file has built-in support for the TCP_WRAPPERS. TCP_WRAPPERS is configured in two different files. These files are:

- /etc/hosts.allow
- /etc/hosts.deny

By default, the /etc/hosts.allow file does not have any services added. If you add any service, such as sshd in this file, all the users will be able to access the service. However, all the other services will be blocked.

Similarly, no services are added to the /etc/hosts.deny file by default. Any service added to the /etc/hosts.deny file is denied access to all the users. However, the remaining services are available.

In this task, you will view the /etc/hosts.allow file and the /etc/hosts.deny file.

To understand the role of TCP wrappers, perform the following steps:

Step 1

Clear the screen by entering the following command:

```
clear
```

Press Enter.

To view this file, type the following command:

```
more /etc/hosts.allow
```

Press Enter.

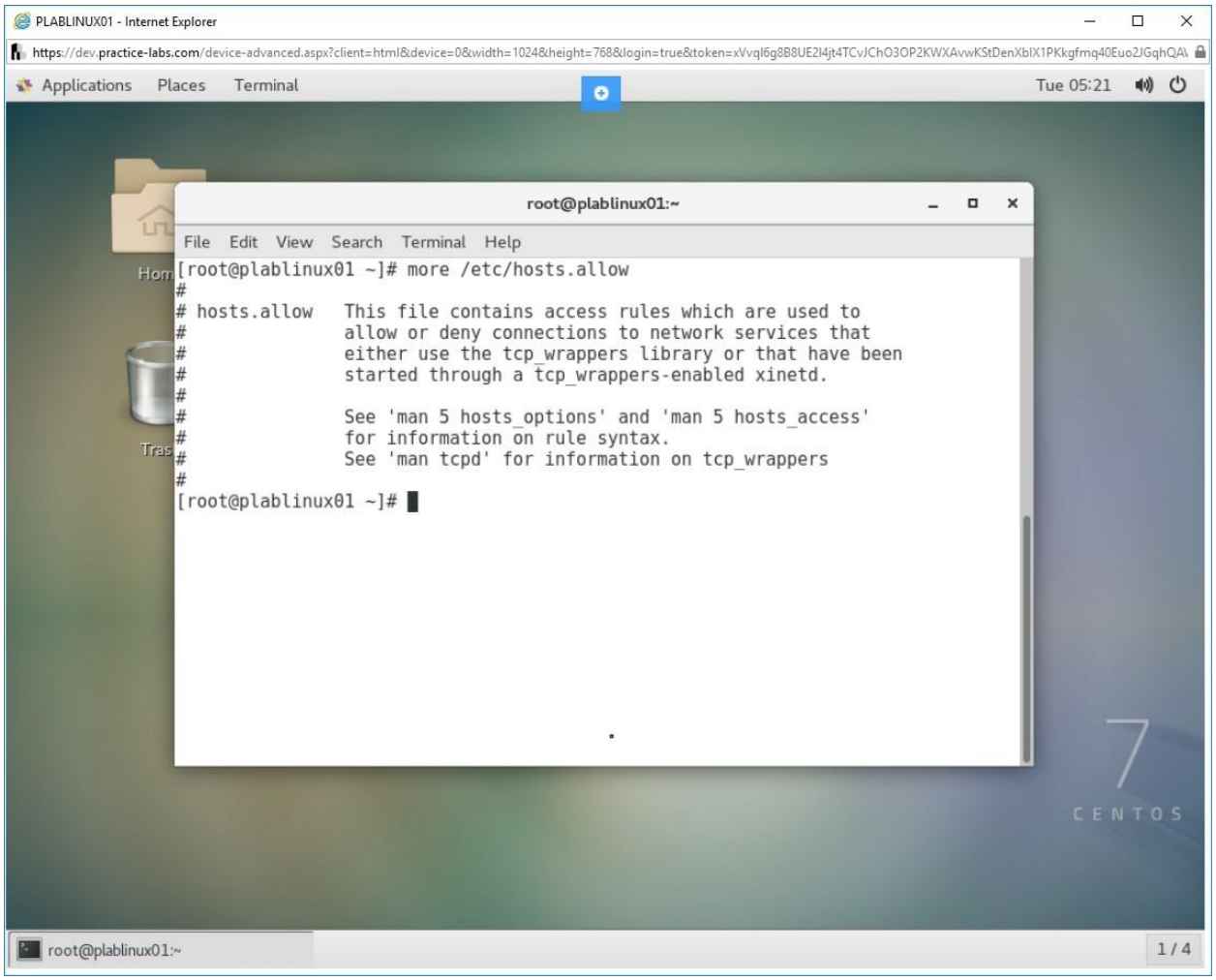

Figure 1.11 Screenshot of PLABLINUX01: Viewing the /etc/hosts.allow file.

Step 2

To view the /etc/hosts.deny file, type the following command:

```
more /etc/hosts.deny
```

Press Enter.

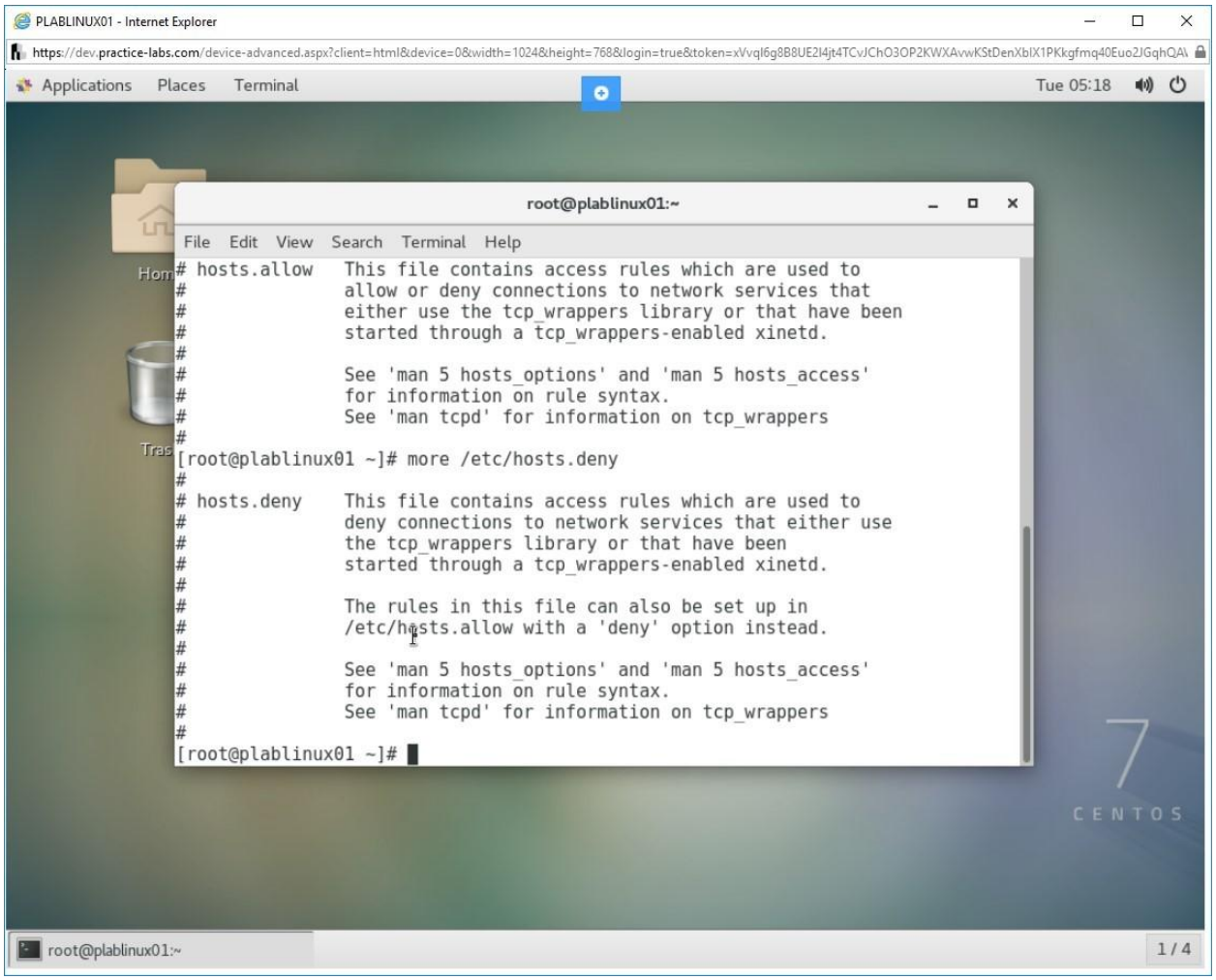

Figure 1.12 Screenshot of PLABLINUX01: Viewing the /etc/hosts.deny file.