

# Secure a Linux Terminal and Implement Logging Services

- **Introduction**
  - **Lab Topology**
  - **Exercise 1 - Secure a Linux Terminal and Implement Logging Services**
  - **Review**
- 

## Introduction

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

Linux Terminal  
Logging Services  
SSH Port  
SSH

## Learning Outcomes

In this module, you will complete the following exercise:

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

After completing this lab, you will be able to:

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

## Exam Objectives

The following exam objectives are covered in this lab:

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

**Note:** Our main focus is to cover the practical, hands-on aspects of the exam objectives. We recommend referring to course material or a search engine to research theoretical topics in more detail.

## Lab Duration

It will take approximately **1 hour** to complete this lab.

## Help and Support

For more information on using Practice Labs, please see our **Help and Support** page. You can also raise a technical support ticket from this page.

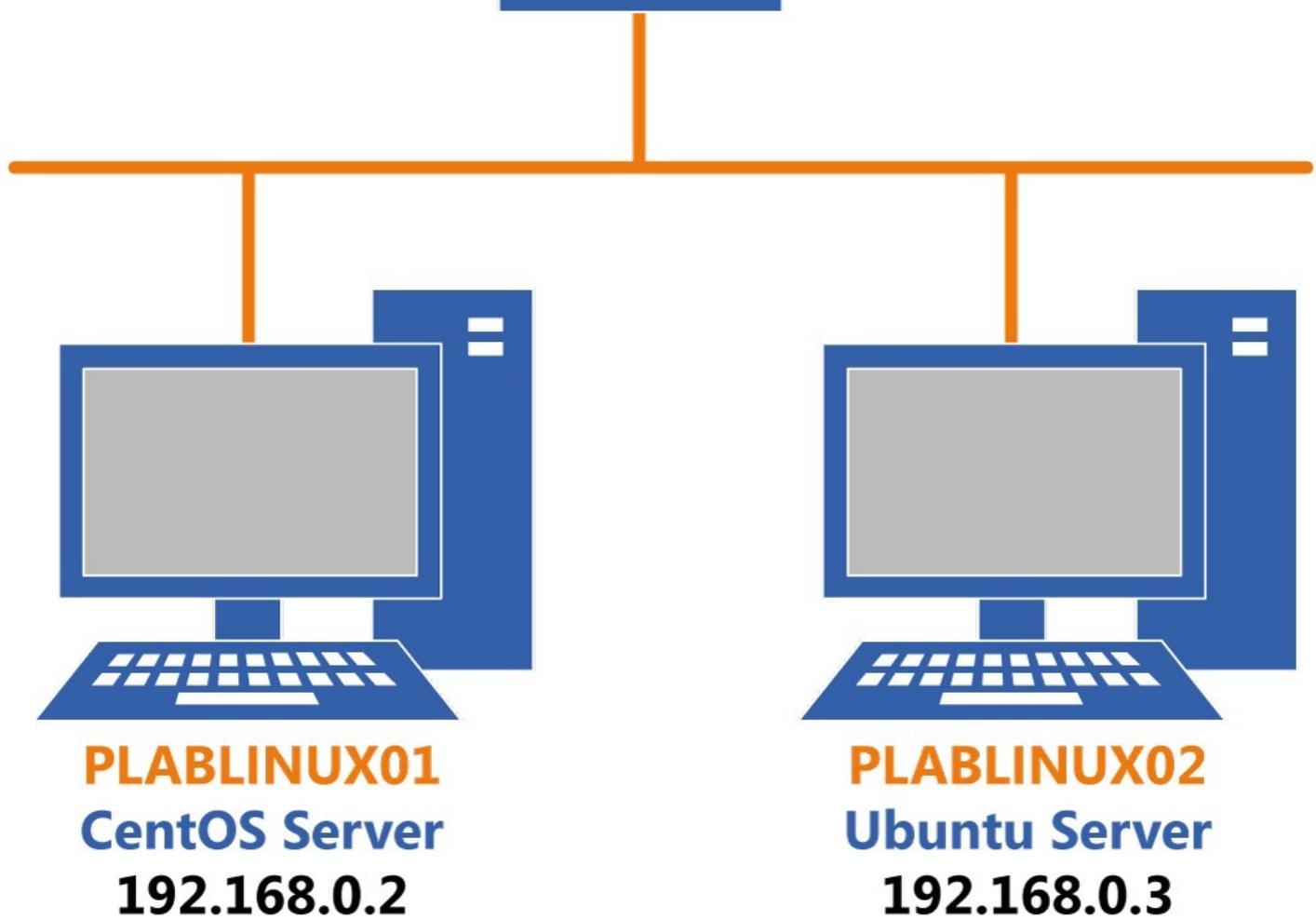
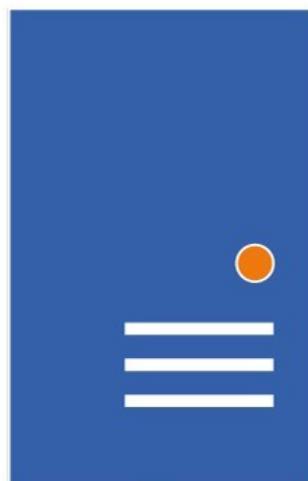
Click Next to view the Lab topology used in this module.

---

## Lab Topology

During your session, you will have access to the following lab configuration.

**PLABSA01**  
**Windows Server 2016**  
**192.168.0.1**



Depending on the exercises you may or may not use all of the devices, but they are shown here in the layout to get an overall understanding of the topology of the lab.

- **PLABSA01** (Windows Server 2016)
- **PLABLINUX01** (CentOS Server)
- **PLABLINUX02** (Ubuntu Server)

Click Next to proceed to the first exercise.

---

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

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

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

### **Learning Outcomes**

After completing this exercise, you will be able to:

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

### **Your Devices**

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

- **PLABLINUX01** (CentOS Server)



## Task 1 - Disable Unnecessary Services

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

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

### **Step 1**

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

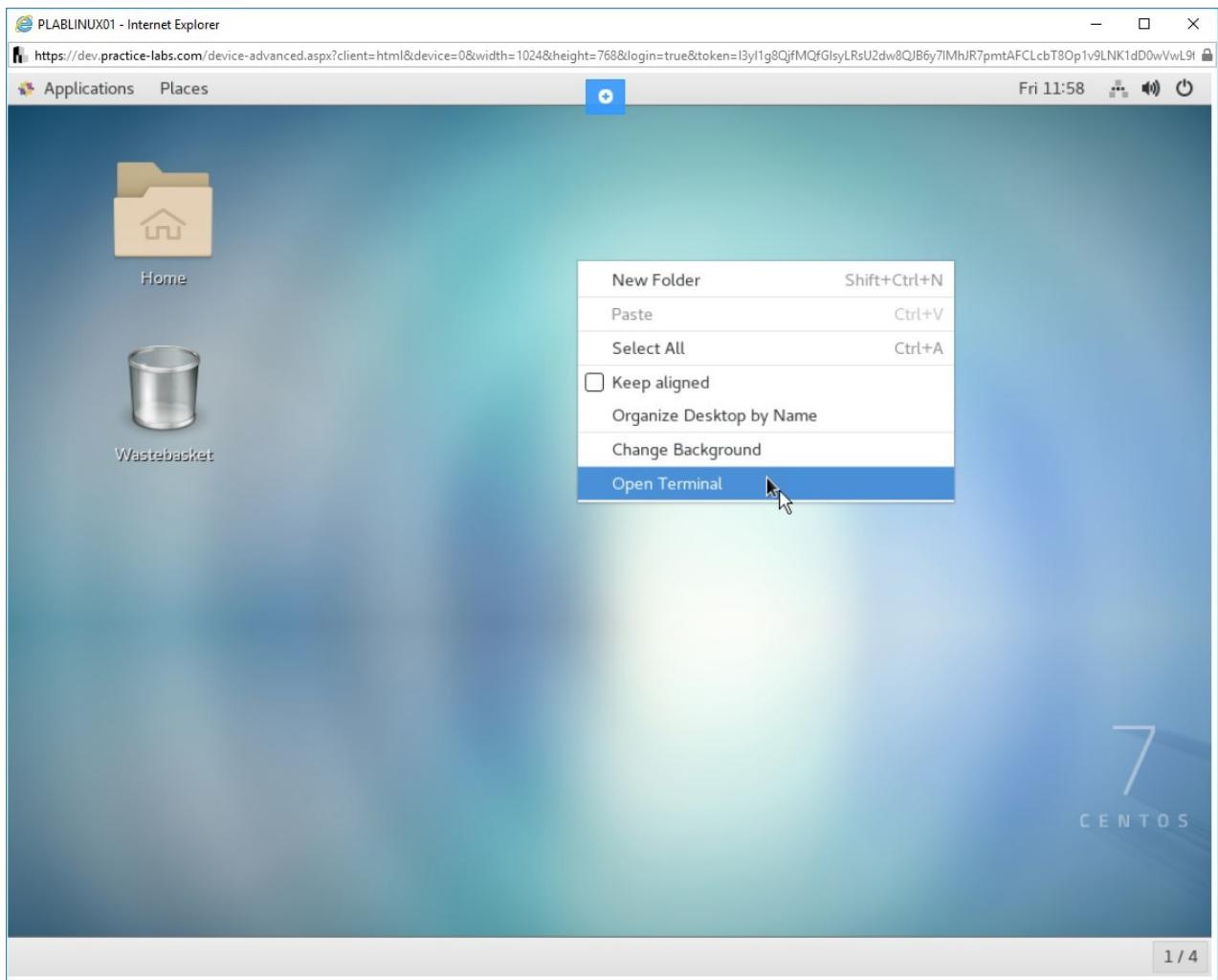


Figure 1.1 Screenshot of PLABLINUX01: Selecting the Open Terminal option from the context menu.

## Step 2

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

```
su -
```

Press **Enter**.

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

Passw0rd

Press **Enter**.

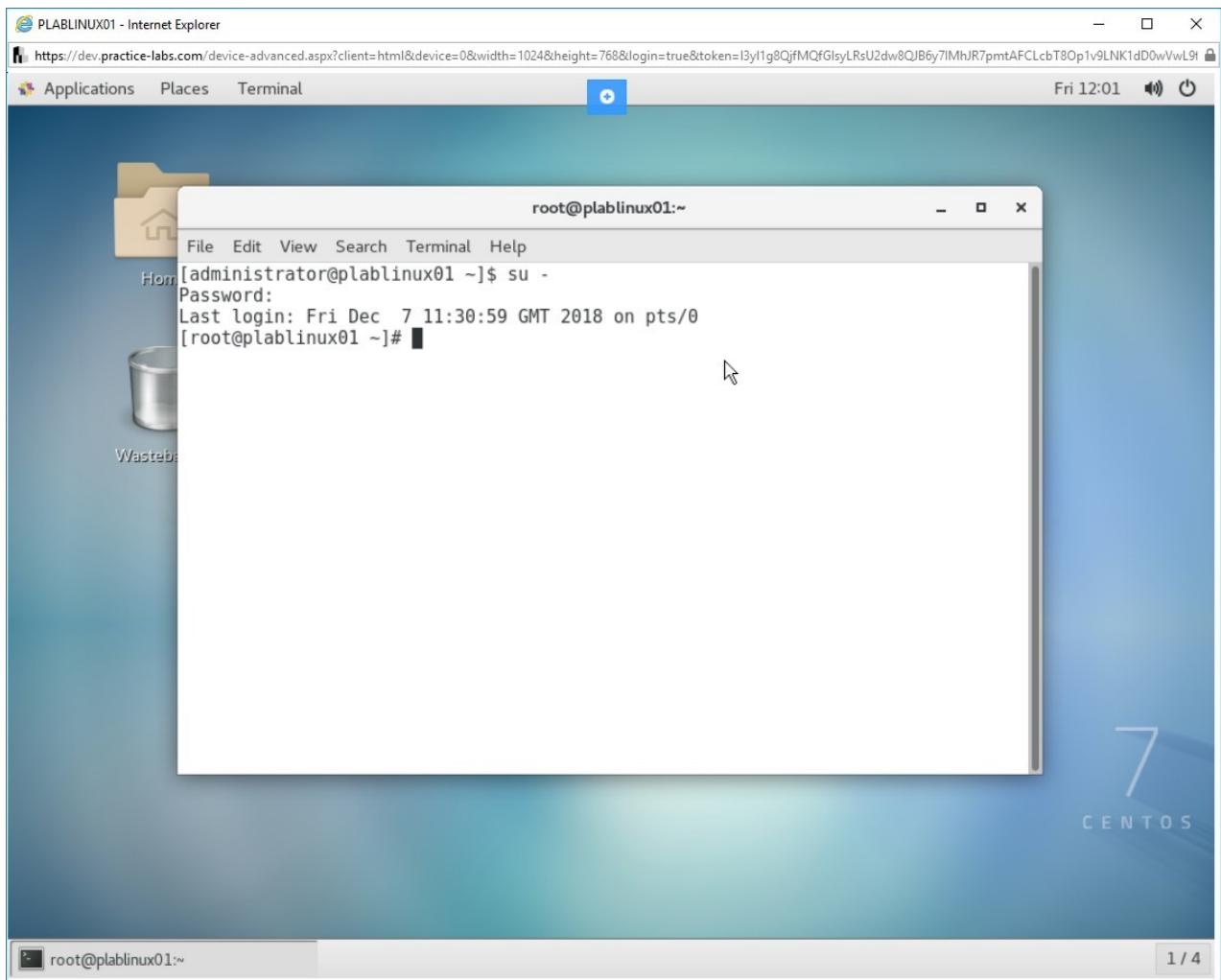


Figure 1.2 Screenshot of PLABLINUX01: Changing the account to the root account with the su command.

## Step 3

Clear the screen by entering the following command:

```
clear
```

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

```
netstat -npl
```

Press **Enter**.

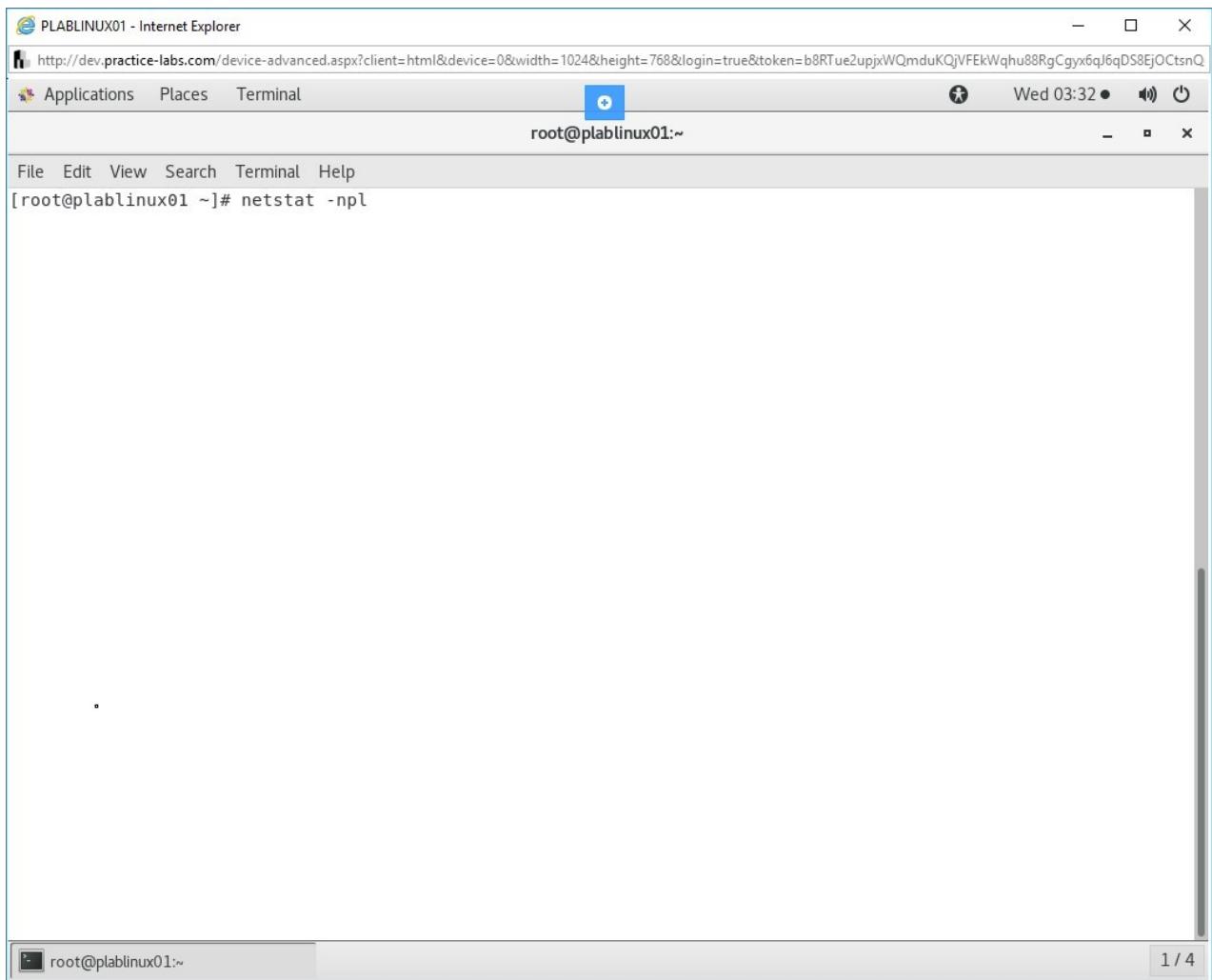


Figure 1.3 Screenshot of PLABLINUX01: Verifying which service is running on which port.

## Step 4

Notice that the command output is now displayed.

```

root@plablinux01:~#
File Edit View Search Terminal Help
unix 2 [ ACC ] STREAM LISTENING 50805 14596/gnome-keyring /run/user/1000/keyring/pkcs11
unix 2 [ ACC ] STREAM LISTENING 50807 14596/gnome-keyring /run/user/1000/keyring/ssh
unix 2 [ ACC ] STREAM LISTENING 37976 4210/gdm @/tmp/dbus-mHwxoABT
unix 2 [ ACC ] STREAM LISTENING 50897 14873/ibus-daemon @/tmp/dbus-GdifbDvU
unix 2 [ ACC ] STREAM LISTENING 17538 1/systemd /run/lvm/lvmetad.socket
unix 2 [ ACC ] STREAM LISTENING 34519 4513/master public/flush
unix 2 [ ACC ] STREAM LISTENING 34534 4513/master public/showq
unix 2 [ ACC ] STREAM LISTENING 29403 3625/gssproxy /var/lib/gssproxy/default.sock
unix 2 [ ACC ] STREAM LISTENING 50626 14791/ssh-agent /tmp/ssh-qxAJJtIfpfWv/agent.1460
5
unix 2 [ ACC ] SEQPACKET LISTENING 17587 1/systemd /run/udev/control
unix 2 [ ACC ] STREAM LISTENING 50760 14605/gnome-session /tmp/.ICE-unix/14605
unix 2 [ ACC ] STREAM LISTENING 26925 1/systemd @ISCSIADM_ABSTRACT_NAMESPACE
unix 2 [ ACC ] STREAM LISTENING 50681 14814/dbus-daemon @/tmp/dbus-Toh0zBrig0
unix 2 [ ACC ] STREAM LISTENING 50883 14860/pulseaudio /run/user/1000/pulse/native
unix 2 [ ACC ] STREAM LISTENING 50759 14605/gnome-session @/tmp/.ICE-unix/14605
unix 2 [ ACC ] STREAM LISTENING 8399 1/systemd /run/systemd/journal/stdout
unix 2 [ ACC ] STREAM LISTENING 34525 4513/master private/proxywrite
unix 2 [ ACC ] STREAM LISTENING 34528 4513/master private/smtp
unix 2 [ ACC ] STREAM LISTENING 34531 4513/master private/relay
unix 2 [ ACC ] STREAM LISTENING 34537 4513/master private/error
unix 2 [ ACC ] STREAM LISTENING 29404 3625/gssproxy /run/gssproxy.sock
unix 2 [ ACC ] STREAM LISTENING 27612 3564/abrtd /var/run/abrt/abrt.socket
unix 2 [ ACC ] STREAM LISTENING 17886 1/systemd /run/lvm/lvmpolld.socket
unix 2 [ ACC ] STREAM LISTENING 34540 4513/master private/retry
unix 2 [ ACC ] STREAM LISTENING 50881 14860/pulseaudio /tmp/.esd-1000/socket
unix 2 [ ACC ] STREAM LISTENING 34543 4513/master private/discard
unix 2 [ ACC ] STREAM LISTENING 34546 4513/master private/local
unix 2 [ ACC ] STREAM LISTENING 34549 4513/master private/virtual
unix 2 [ ACC ] STREAM LISTENING 34552 4513/master private/lmtp
unix 2 [ ACC ] STREAM LISTENING 31992 3676/NetworkManager /var/run/NetworkManager/private-
dhcp
unix 2 [ ACC ] STREAM LISTENING 34555 4513/master private/anvil
unix 2 [ ACC ] STREAM LISTENING 34558 4513/master private/scache
[root@plablinux01 ~]#

```

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

## Step 5

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

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

```

root@plablinux01:~#
File Edit View Search Terminal Help
Active UNIX domain sockets (only servers)
Proto RefCnt Flags Type State I-Node PID/Program name Path
unix 2 [ ACC ] STREAM LISTENING 29697 3647/mcelog /var/run/mcelog-client
unix 2 [ ACC ] STREAM LISTENING 29442 3609/lsmd /var/run/lsm ipc/simc
unix 2 [ ACC ] STREAM LISTENING 34501 4513/master private/tlsmgr
unix 2 [ ACC ] STREAM LISTENING 29444 3609/lsmd /var/run/lsm ipc/sim
unix 2 [ ACC ] STREAM LISTENING 34062 4189/libvirt /var/run/libvirt/libvirt-sock
unix 2 [ ACC ] STREAM LISTENING 34064 4189/libvirt /var/run/libvirt/libvirt-sock-ro
unix 2 [ ACC ] STREAM LISTENING 34066 4189/libvirt /var/run/libvirt/libvirt-admin-s
ock
unix 2 [ ACC ] STREAM LISTENING 34504 4513/master private/rewrite
unix 2 [ ACC ] STREAM LISTENING 34507 4513/master private/bounce
unix 2 [ ACC ] STREAM LISTENING 34510 4513/master private/defer
unix 2 [ ACC ] STREAM LISTENING 37975 4210/gdm @/tmp/dbus-s2a9MvqF
unix 2 [ ACC ] STREAM LISTENING 37850 5553/X @/tmp/.X11-unix/X0
unix 2 [ ACC ] STREAM LISTENING 26915 1/systemd /var/run/libvirt/virtlockd-sock
unix 2 [ ACC ] STREAM LISTENING 26918 1/systemd /var/run/cups/cups.sock
unix 2 [ ACC ] STREAM LISTENING 26920 1/systemd /var/run/avahi-daemon/socket
unix 2 [ ACC ] STREAM LISTENING 34513 4513/master private/trace
unix 2 [ ACC ] STREAM LISTENING 26923 1/systemd /var/run/libvirt/virtlogd-sock
unix 2 [ ACC ] STREAM LISTENING 34516 4513/master private/verify
unix 2 [ ACC ] STREAM LISTENING 34522 4513/master private/proxymap
unix 2 [ ACC ] STREAM LISTENING 26926 1/systemd /var/run/rpcbind.sock
unix 2 [ ACC ] STREAM LISTENING 26932 1/systemd /run/dbus/system_bus_socket
unix 2 [ ACC ] STREAM LISTENING 49091 14615/dbus-daemon @/tmp/dbus-N3AA2RLVW0
unix 2 [ ACC ] STREAM LISTENING 37851 5553/X /tmp/.X11-unix/X0
unix 2 [ ACC ] STREAM LISTENING 26935 1/systemd @ISCSID_UIP_ABSTRACT_NAMESPACE
unix 2 [ ACC ] STREAM LISTENING 17482 1/systemd /run/systemd/private
unix 2 [ ACC ] STREAM LISTENING 34490 4513/master public/pickup
unix 2 [ ACC ] STREAM LISTENING 48996 14596/gnome-keyring /run/user/1000/keyring/control
unix 2 [ ACC ] STREAM LISTENING 34494 4513/master public/cleanup
unix 2 [ ACC ] STREAM LISTENING 34497 4513/master public/qmgr
unix 2 [ ACC ] STREAM LISTENING 50805 14596/gnome-keyring /run/user/1000/keyring/pkcs11
unix 2 [ ACC ] STREAM LISTENING 50807 14596/gnome-keyring /run/user/1000/keyring/ssh
unix 2 [ ACC ] STREAM LISTENING 37976 4210/gdm @/tmp/dbus-mHwxoABT
unix 2 [ ACC ] STREAM LISTENING 50007 14073/dibus_daemon @/tmp/dbus_Gdifh0uL

```

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

## Step 6

Clear the screen by entering the following command:

```
clear
```

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

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

Press **Enter**.

The screenshot shows a Linux terminal window titled "PLABLINUX01 - Internet Explorer". The window has a standard title bar with icons for minimize, maximize, and close. Below the title bar is a menu bar with "File", "Edit", "View", "Search", "Terminal", and "Help". The main area of the window is a terminal session. The prompt "root@plablinux01:~" is visible at the top of the terminal. A command is being typed into the terminal: "[root@plablinux01 ~]# systemctl list-unit-files --type=service | grep enabled". The terminal window is set against a light gray background. At the bottom of the screen, there is a horizontal bar with the text "root@plablinux01:~" on the left and "1 / 4" on the right.

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

## Step 7

Notice that the command output is now displayed.

The screenshot shows a terminal window titled 'PLABLINUX01 - Internet Explorer'. The URL in the address bar is 'http://dev.practice-labs.com/device-advanced.aspx?client=html&device=0&width=1024&height=768&login=true&token=b8RTue2upjxWQmduKQjVFEkWqhu88RgCgyx6qJ6qDS8EjOCTsnQ'. The window title bar includes icons for Applications, Places, Terminal, and a power button. The status bar at the top right shows 'root@plablinux01:~' and the date/time 'Wed 03:42'. The main content area displays a list of system services and their current status:

Service	Status
libstoragemgmt.service	enabled
libvirdt.service	enabled
lvm2-monitor.service	enabled
mcelog.service	enabled
mdmonitor.service	enabled
microcode.service	enabled
ModemManager.service	enabled
multipathd.service	enabled
netcf-transaction.service	enabled
NetworkManager-dispatcher.service	enabled
NetworkManager-wait-online.service	enabled
NetworkManager.service	enabled
postfix.service	enabled
qemu-guest-agent.service	enabled
rhel-autorelabel-mark.service	enabled
rhel-autorelabel.service	enabled
rhel-configure.service	enabled
rhel-dmesg.service	enabled
rhel-domainname.service	enabled
rhel-import-state.service	enabled
rhel-loadmodules.service	enabled
rhel-readonly.service	enabled
rngd.service	enabled
rsyslog.service	enabled
rtkit-daemon.service	enabled
smartd.service	enabled
spice-vdagentd.service	enabled
sshd.service	enabled
sysstat.service	enabled
systemd-readahead-collect.service	enabled
systemd-readahead-drop.service	enabled
systemd-readahead-replay.service	enabled
tuned.service	enabled
vmtoolsd.service	enabled

[root@plablinux01 ~]#

At the bottom left is a small icon of a terminal window with the text 'root@plablinux01:~'. At the bottom right is the page number '1 / 4'.

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

## Step 8

Clear the screen by entering the following command:

```
clear
```

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

```
systemctl disable vmtoolsd.service
```

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

The screenshot shows a terminal window titled "PLABLINUX01 - Internet Explorer". The URL in the address bar is "http://dev.practice-labs.com/device-advanced.aspx?client=html&device=0&width=1024&height=768&login=true&token=b8RTue2upjxWQmduKQjVFEkWqhu88RgCgyx6qJ6qDS8EjOCTsnQ". The window title bar includes icons for Applications, Places, Terminal, a blue plus sign, a user icon, and system status indicators. The status bar at the bottom shows "root@plablinux01:~". The terminal content shows the command "systemctl disable vmtoolsd.service" being run, with the output "Removed symlink /etc/systemd/system/multi-user.target.wants/vmtoolsd.service." The bottom status bar also shows "root@plablinux01:~". A small navigation bar at the bottom right indicates "1 / 4".

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

## Step 9

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

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

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

The screenshot shows a terminal window titled "PLABLINUX01 - Internet Explorer" running on a Linux system. The window title bar includes the URL "http://dev.practice-labs.com/device-advanced.aspx?client=html&device=0&width=1024&height=768&login=true&token=b8RTue2upjxWQmduKQjVFEkWqhu88RgCgyx6qJ6qDS8EjOCtsnQ". The window has standard Linux desktop icons in the top right corner. The terminal window itself has a light gray header bar with tabs for "Applications", "Places", and "Terminal". The main area displays a command-line session where the user is listing system services using the command "ls /etc/systemd/system/\*.service". The output shows numerous services listed with their status as "enabled".

```
root@plablinux01:~# ls /etc/systemd/system/*.service
ksmtuned.service                                enabled
libstoragemgmt.service                          enabled
libvirtd.service                               enabled
lvm2-monitor.service                           enabled
mcelog.service                                 enabled
mdmonitor.service                            enabled
microcode.service                            enabled
ModemManager.service                         enabled
multipathd.service                           enabled
netcf-transaction.service                    enabled
NetworkManager-dispatcher.service           enabled
NetworkManager-wait-online.service          enabled
NetworkManager.service                        enabled
postfix.service                                enabled
qemu-guest-agent.service                     enabled
rhel-autorelabel-mark.service                enabled
rhel-autorelabel.service                     enabled
rhel-configure.service                      enabled
rhel-dmesg.service                           enabled
rhel-domainname.service                     enabled
rhel-import-state.service                   enabled
rhel-loadmodules.service                    enabled
rhel-readonly.service                       enabled
rngd.service                                  enabled
rsyslog.service                             enabled
rtkit-daemon.service                        enabled
smartd.service                               enabled
spice-vdagentd.service                     enabled
sshd.service                                 enabled
sysstat.service                            enabled
systemd-readahead-collect.service          enabled
systemd-readahead-drop.service             enabled
systemd-readahead-replay.service           enabled
tuned.service                                enabled
[root@plablinux01 ~]#
```

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

## Task 2 - Disable the root Login via SSH

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

### Step 1

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

Clear the screen by entering the following command:

```
clear
```

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

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

Press **Enter**.

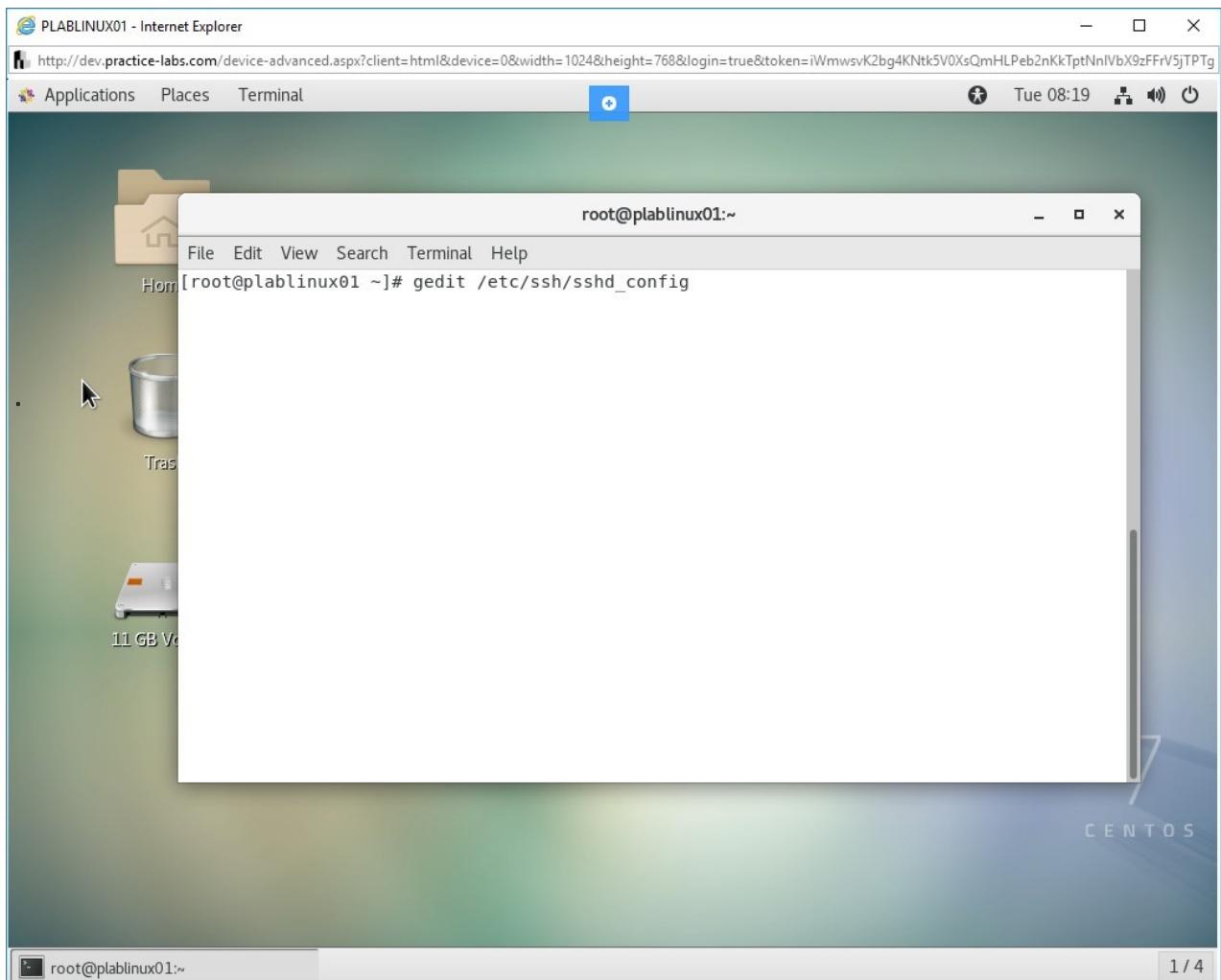


Figure 1.10 Screenshot of PLABLINUX01: Opening the /etc/ssh/sshd\_config file.

## Step 2

The **/etc/ssh/sshd\_config** file is displayed.

The screenshot shows a terminal window titled 'PLABLINUX01 - Internet Explorer' with the URL 'http://dev.practice-labs.com/device-advanced.aspx?client=html&device=0&width=1024&height=768&login=true&token=iWmwsvK2bg4KNtk5V0sQmHLPeb2nKkTptNnlVbX9zFFrV5jTPTg'. The window contains the contents of the /etc/ssh/sshd\_config file. The file includes comments about the configuration, port settings (port 22), host keys, ciphers, logging, and authentication sections. The terminal interface shows standard Linux navigation commands like 'root@plablinux01:~\$' and file operations like 'gedit \*sshd\_config (/etc/ssh)'. The status bar at the bottom indicates 'Plain Text' mode, a tab width of 8, line 17, column 8, and an 'INS' key state.

```
#      $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 1.11 Screenshot of PLABLINUX01: Displaying the /etc/ssh/sshd\_config file.

## Step 3

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

Change the following:

From:

```
#PermitRootLogin yes
```

To:

```
PermitRootLogin no
```

The screenshot shows a terminal window titled 'PLABLINUX01 - Internet Explorer' displaying the contents of the '/etc/ssh/sshd\_config' file. The file contains various configuration options for the SSH daemon, including sections for ciphers, logging, authentication, and host-based authentication. The terminal window includes standard Linux navigation keys like F1-F12 and a status bar at the bottom.

```
# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
SyslogFacility AUTHPRIV
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

# The default is to check both .ssh/authorized_keys and .ssh/authorized_keys2
# but this is overridden so installations will only check .ssh/authorized_keys
AuthorizedKeysFile      .ssh/authorized_keys

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#TunnelOptionsUser
```

Figure 1.12 Screenshot of PLABLINUX01: Making changes to the /etc/ssh/sshd\_config file.

## Step 4

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

```
AllowUsers administrator
AllowGroups administrator
```

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

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

The screenshot shows a terminal window titled 'PLABLINUX01 - Internet Explorer' with the URL 'http://dev.practice-labs.com/device-advanced.aspx?client=html&device=0&width=1024&height=768&login=true&token=iWmwsvK2bg4KNtk5V0XsQmHLPeb2nKkTptNnlVbX9zFFrV5jTPTg'. The window contains the contents of the /etc/ssh/sshd\_config file. The configuration includes port 22, host keys, ciphers, logging, authentication, and root login settings. The file is currently being edited in 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 1.13 Screenshot of PLABLINUX01: Making changes to the /etc/ssh/sshd\_config file.

## Step 5

Click **Save** to save the file. Then, close the **/etc/ssh/sshd\_config** file.

The screenshot shows a terminal window titled 'PLABLINUX01 - Internet Explorer' displaying the contents of the '/etc/ssh/sshd\_config' file. The file contains various SSH configuration parameters, including cipher settings, logging levels, authentication methods, and host-based authentication. A cursor is hovering over the 'Save' button at the top right of the text editor window. The terminal prompt at the bottom left shows 'root@plablinux01:~\$'. The status bar at the bottom right indicates 'Plain Text' mode, a tab width of 8, line 43, column 26, and an 'INS' key state.

```
# 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

#PubkeyAuthentication yes

# The default is to check both .ssh/authorized_keys and .ssh/authorized_keys2
# but this is overridden so installations will only check .ssh/authorized_keys
AuthorizedKeysFile      .ssh/authorized_keys

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#FingerprintHashSHA256
```

Figure 1.14 Screenshot of PLABLINUX01: Saving and closing the /etc/ssh/sshd\_config file.

## Step 6

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

```
systemctl restart sshd
```

Press **Enter**.

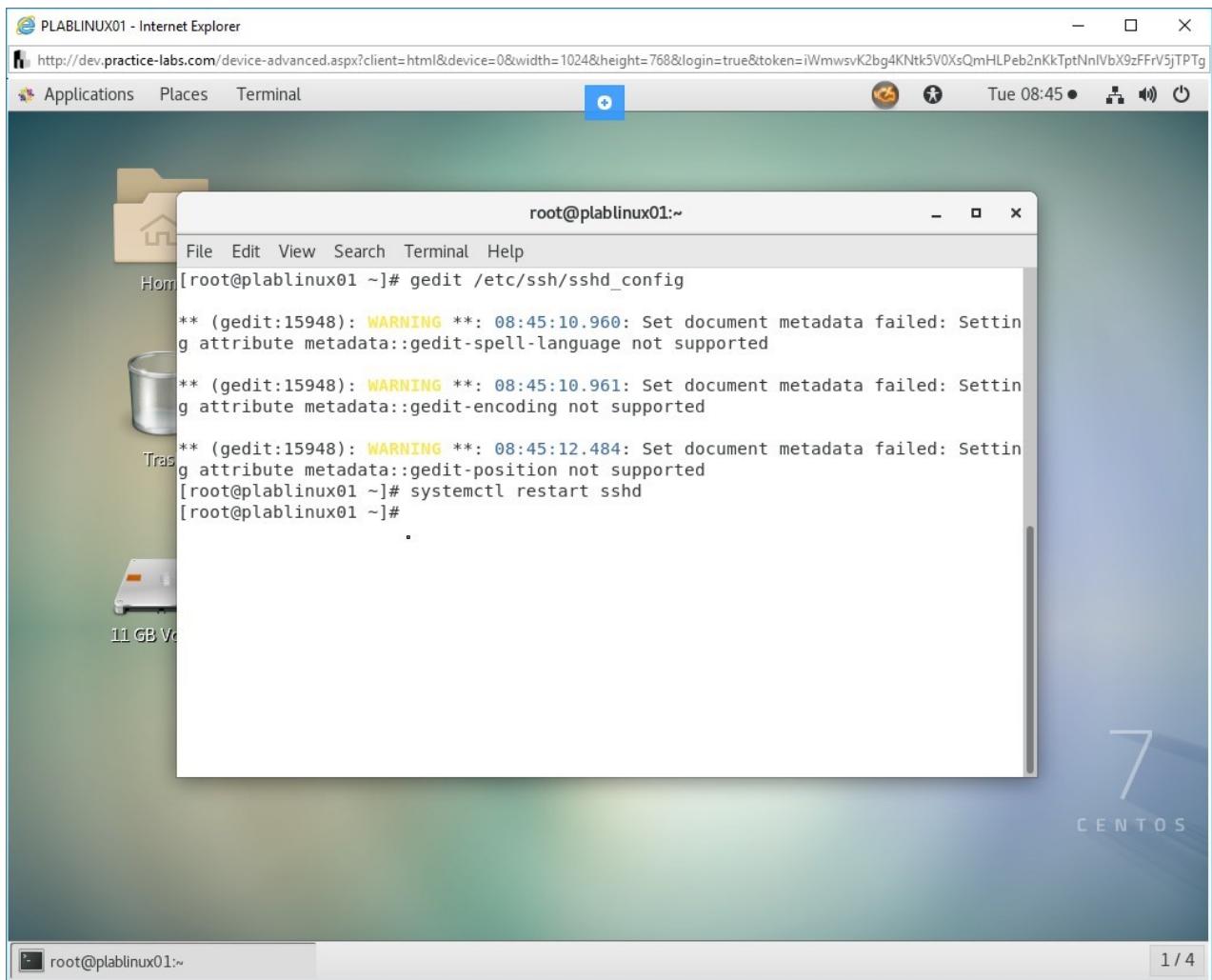


Figure 1.15 Screenshot of PLABLINUX01: Restarting the sshd service.

## Step 7

Switch to **PLABSAo1**. From the **Putty** window, open an SSH connection to **PLABLINUX01**.

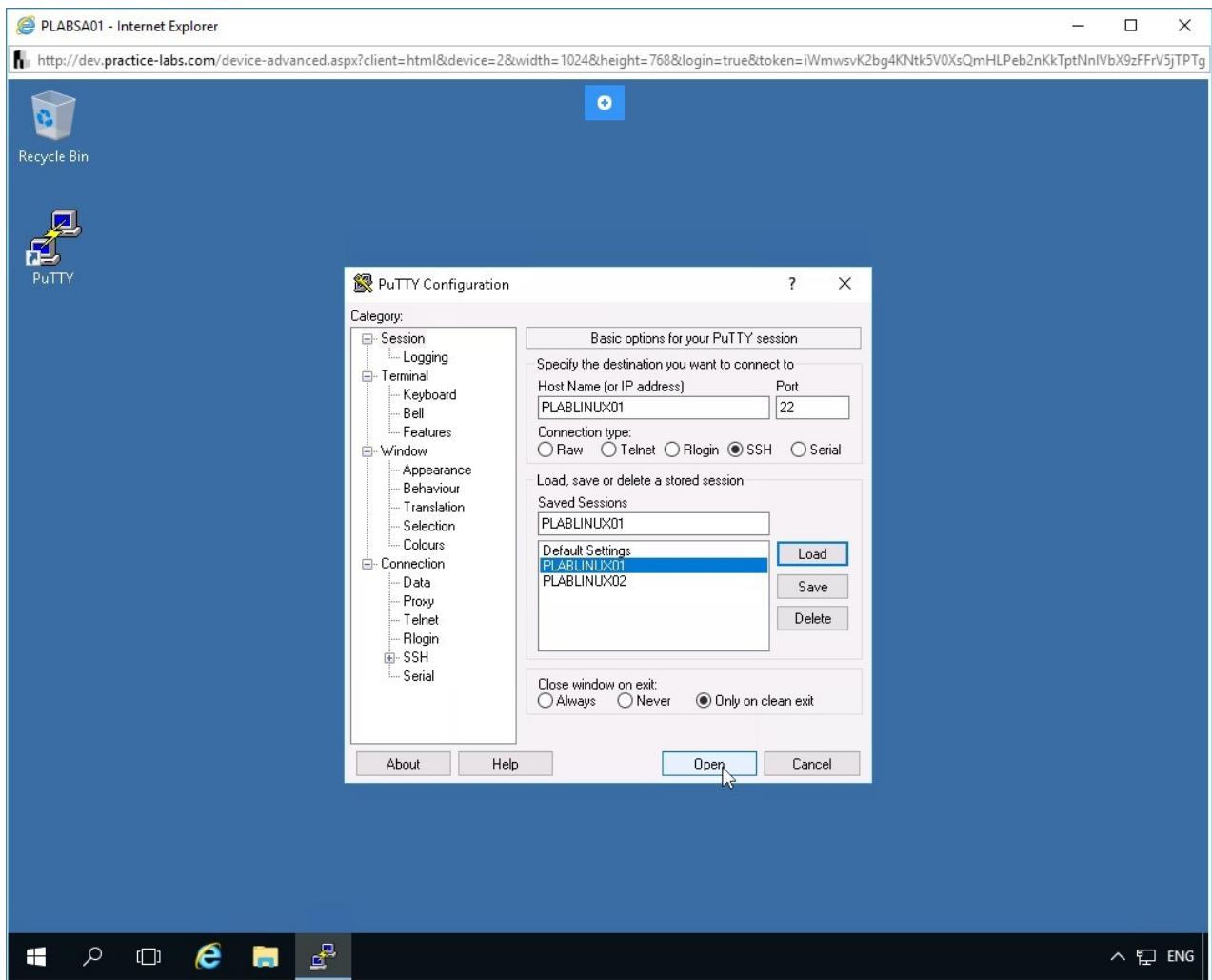


Figure 1.16 Screenshot of PLABLINUX01: Loading required configuration in the PutTTY window.

## Step 8

The terminal window is displayed. Enter the following credentials:

**login as:**

root

**Password:**

Passw0rd

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

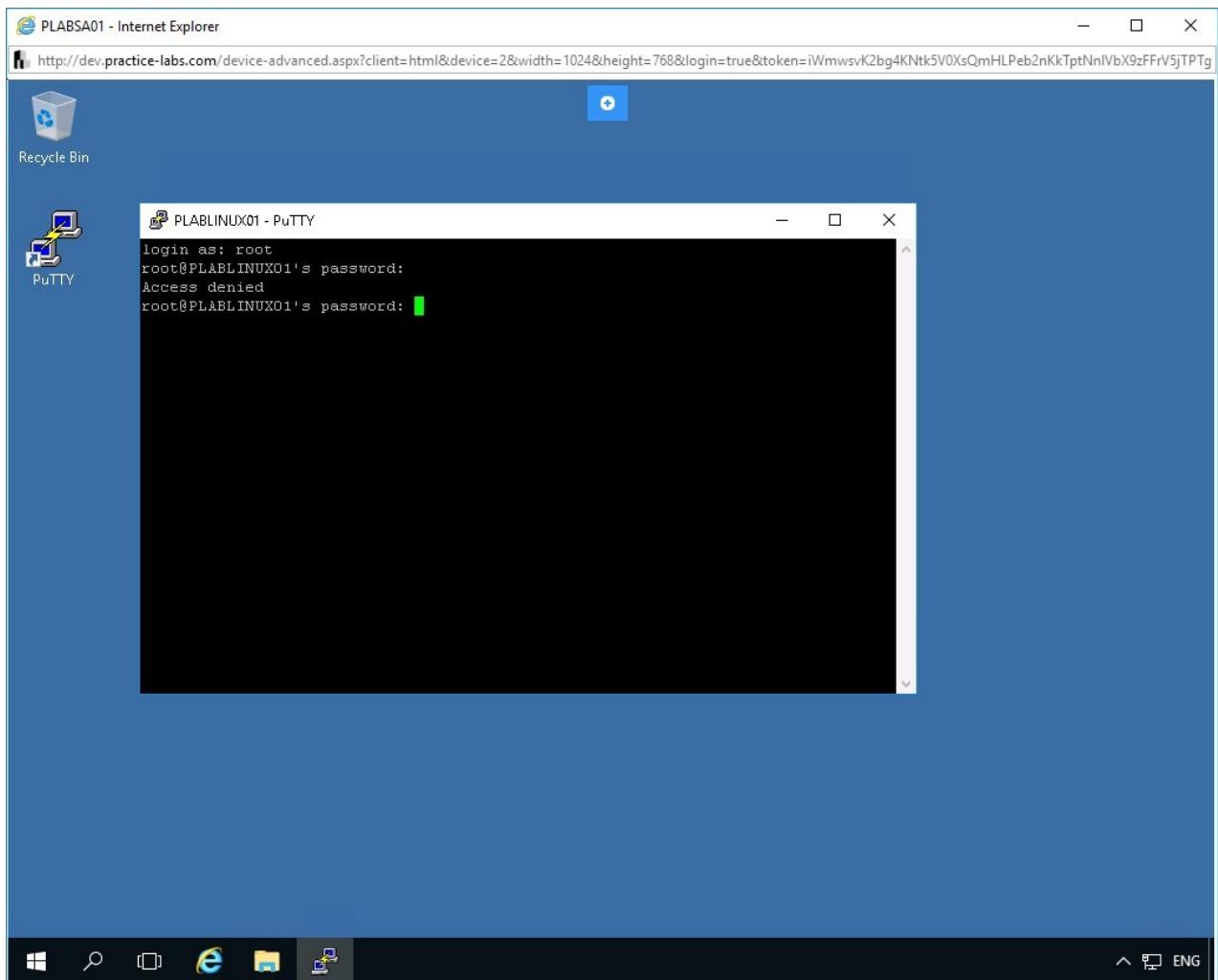


Figure 1.17 Screenshot of PLABLINUX01: Showing the access denied message after entering the credentials.

## Step 9

Close the session window. Launch putty again. Load the **PLABLINUX01** session. When prompted for the login, use the following credentials:

**login as:**

administrator

**Password:**

Passw0rd

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

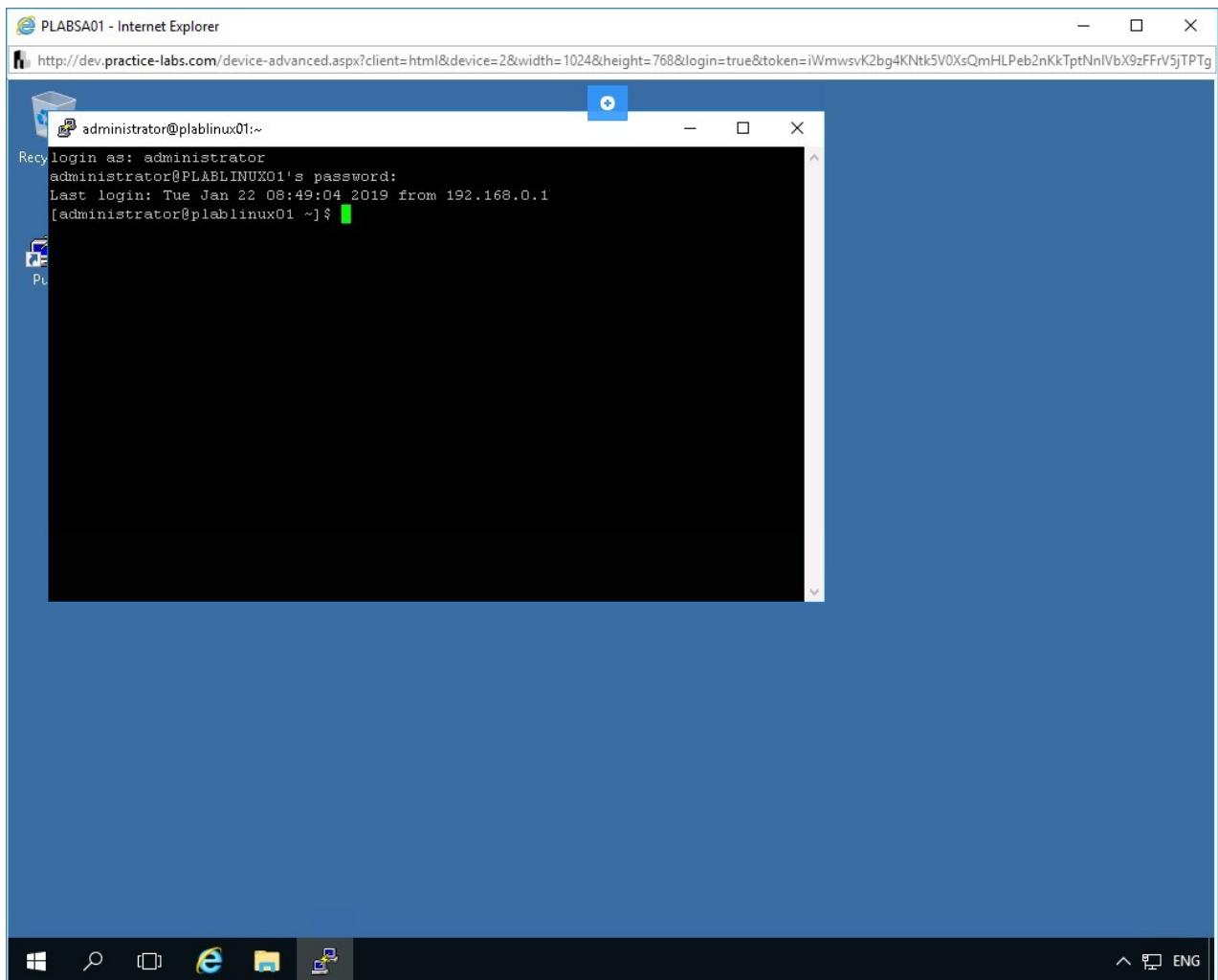


Figure 1.18 Screenshot of PLABLINUX01: Showing a successful connection after entering the credentials.

## Task 3 - Change the Default SSH Port

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

### Step 1

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

Clear the screen by entering the following command:

```
clear
```

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

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

Press **Enter**.

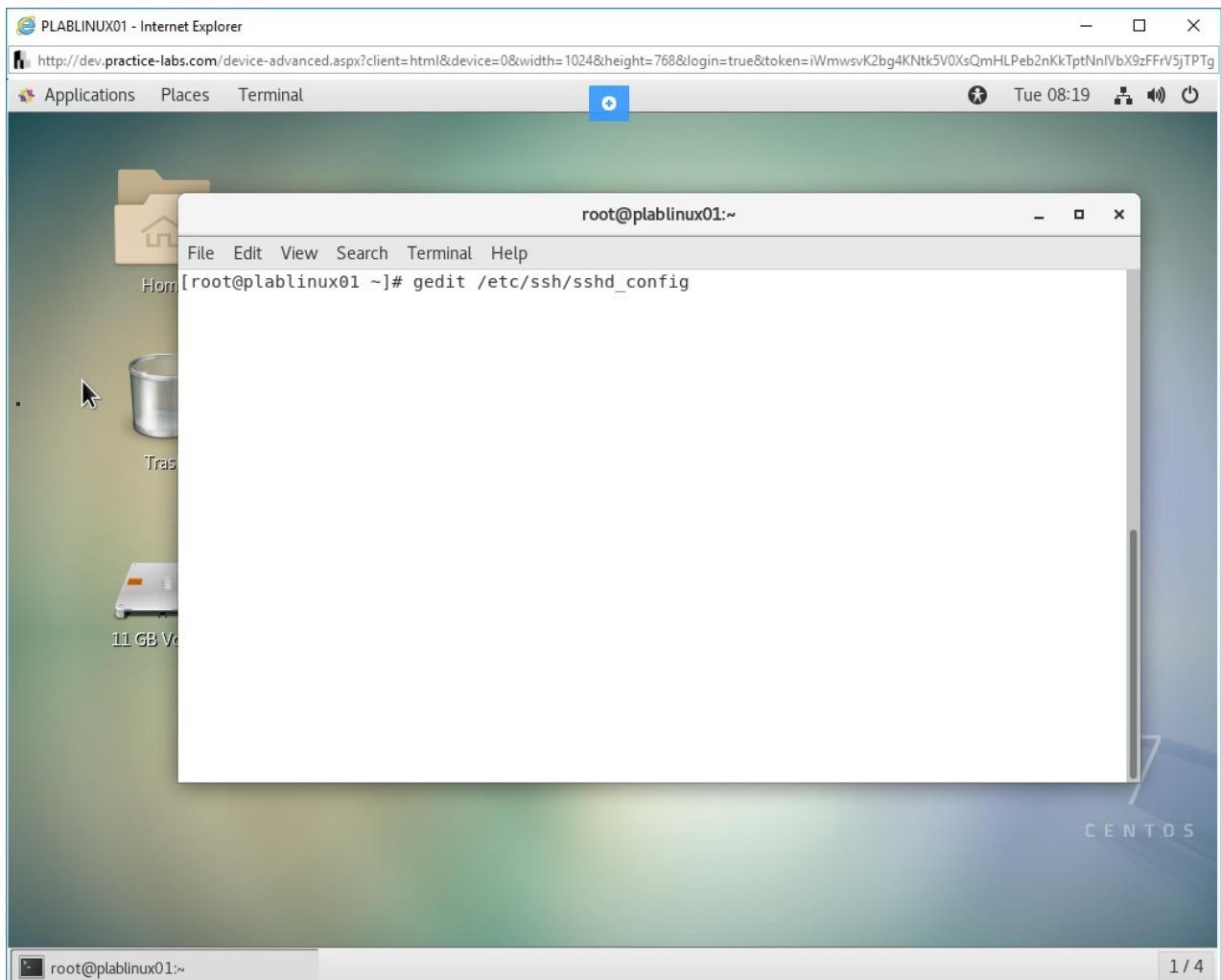


Figure 1.19 Screenshot of PLABLINUX01: Opening the /etc/ssh/sshd\_config file.

## Step 2

The **/etc/ssh/sshd\_config** file is displayed.

The screenshot shows a Windows-style window titled "PLABLINUX01 - Internet Explorer". Inside, a tab labeled "ssh\_config" is open, showing the contents of the file "/etc/ssh/sshd\_config". The file contains configuration options for the SSH daemon, including port settings, host keys, ciphers, logging, and authentication methods. A status bar at the bottom indicates 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:  
Plain Text ▾ Tab Width: 8 ▾ Ln 1, Col 1 ▾ INS  
root@plablinux01:~ | sshd_config (/etc/ssh) - gedit | 1 / 4
```

Figure 1.20 Screenshot of PLABLINUX01: Displaying the /etc/ssh/sshd\_config file.

## Step 3

Notice that the port number line is commented. You will now change the following:

From:

```
#Port 22
```

To:

```
Port 1234
```

The screenshot shows a terminal window titled 'PLABLINUX01 - Internet Explorer' with the URL 'http://dev.practice-labs.com/device-advanced.aspx?client=html&device=0&width=1024&height=768&login=true&token=b8RTue2upjxWQmduKQjVFEkWqhu88RgCgyx6qJ6qDS8EjOCtsnQ'. The window contains the contents of the /etc/ssh/sshd\_config file. The configuration includes port 1234, host keys, ciphers, logging, and authentication settings. The file is currently 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 1234
#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 1.21 Screenshot of PLABLINUX01: Making changes to the /etc/ssh/sshd\_config file.

## Step 4

Click **Save** to save the file. Then, close the **/etc/ssh/sshd\_config** file.

```
#      $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 1234
#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 1.22 Screenshot of PLABLINUX01: Saving and closing the /etc/ssh/sshd\_config file.

## Step 5

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

```
systemctl restart sshd
```

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

The screenshot shows a terminal window titled 'PLABLINUX01 - Internet Explorer' running on a Linux system. The window title bar includes the URL 'http://dev.practice-labs.com/device-advanced.aspx?client=html&device=0&width=1024&height=768&login=true&token=b8RTue2upjxWQmduKQjVFEkWqhu88RgCgyx6qJ6qDS8EjOCtsnQ'. The menu bar has options like File, Edit, View, Search, Terminal, and Help. The command line at the bottom shows the root user's session: [root@plablinux01 ~]# gedit /etc/ssh/sshd\_config. The terminal output shows a warning message from gedit about setting document metadata and then a command to restart the sshd service: [root@plablinux01 ~]# systemctl restart sshd. A message indicates that the job failed because the control process exited with an error code. The status of the sshd.service is shown as failed. The bottom status bar shows the user as 'root@plablinux01'.

Figure 1.23 Screenshot of PLABLINUX01: Restarting the sshd service.

## Task 4 - Verify the Last Logged In Users

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

### Step 1

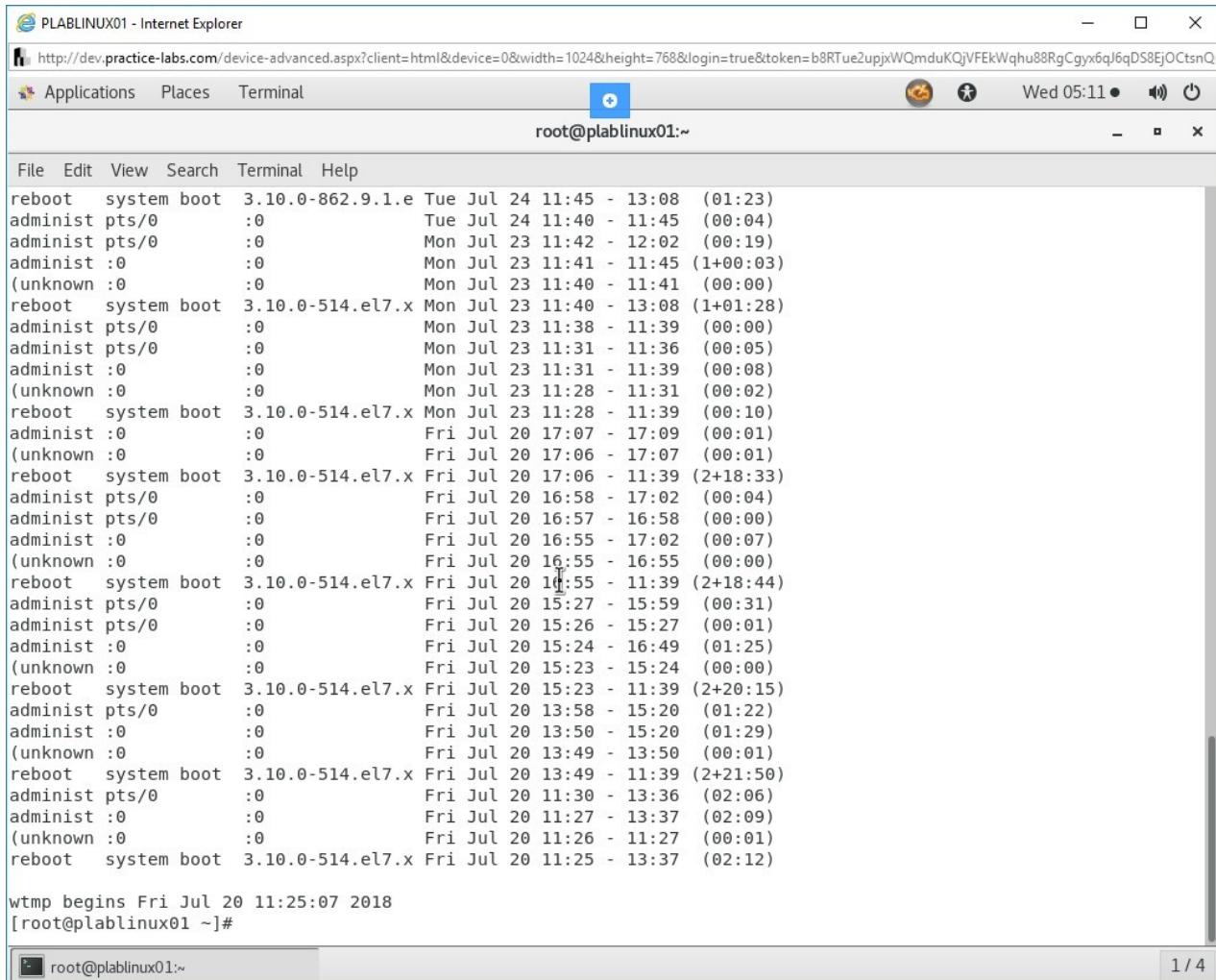
Clear the screen by entering the following command:

```
clear
```

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

```
last
```

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



The screenshot shows a terminal window titled "root@plablinux01:~". The window displays the output of the "last" command, which lists user logins. The output includes columns for the user, terminal, IP address, date, and time of login, along with the duration of the session. The terminal window has a standard Linux-style interface with a menu bar, tabs, and status icons.

User	Terminal	IP Address	Date	Time	Duration	
reboot	system boot	3.10.0-862.9.1.e	Tue Jul 24	11:45	- 13:08 (01:23)	
administ	pts/0	:	Tue Jul 24	11:40	- 11:45 (00:04)	
administ	pts/0	:	Mon Jul 23	11:42	- 12:02 (00:19)	
administ	:0	:	Mon Jul 23	11:41	- 11:45 (1+00:03)	
(unknown	:0	:	Mon Jul 23	11:40	- 11:41 (00:00)	
reboot	system boot	3.10.0-514.el7.x	Mon Jul 23	11:40	- 13:08 (1+01:28)	
administ	pts/0	:	Mon Jul 23	11:38	- 11:39 (00:00)	
administ	pts/0	:	Mon Jul 23	11:31	- 11:36 (00:05)	
administ	:0	:	Mon Jul 23	11:31	- 11:39 (00:08)	
(unknown	:0	:	Mon Jul 23	11:28	- 11:31 (00:02)	
reboot	system boot	3.10.0-514.el7.x	Mon Jul 23	11:28	- 11:39 (00:10)	
administ	:0	:	Fri Jul 20	17:07	- 17:09 (00:01)	
(unknown	:0	:	Fri Jul 20	17:06	- 17:07 (00:01)	
reboot	system boot	3.10.0-514.el7.x	Fri Jul 20	17:06	- 11:39 (2+18:33)	
administ	pts/0	:	Fri Jul 20	16:58	- 17:02 (00:04)	
administ	pts/0	:	Fri Jul 20	16:57	- 16:58 (00:00)	
administ	:0	:	Fri Jul 20	16:55	- 17:02 (00:07)	
(unknown	:0	:	Fri Jul 20	16:55	- 16:55 (00:00)	
reboot	system boot	3.10.0-514.el7.x	Fri Jul 20	16:55	- 11:39 (2+18:44)	
administ	pts/0	:	Fri Jul 20	15:27	- 15:59 (00:31)	
administ	pts/0	:	Fri Jul 20	15:26	- 15:27 (00:01)	
administ	:0	:	Fri Jul 20	15:24	- 16:49 (01:25)	
(unknown	:0	:	Fri Jul 20	15:23	- 15:24 (00:00)	
reboot	system boot	3.10.0-514.el7.x	Fri Jul 20	15:23	- 11:39 (2+20:15)	
administ	pts/0	:	Fri Jul 20	13:58	- 15:20 (01:22)	
administ	:0	:	Fri Jul 20	13:50	- 15:20 (01:29)	
(unknown	:0	:	Fri Jul 20	13:49	- 13:50 (00:01)	
reboot	system boot	3.10.0-514.el7.x	Fri Jul 20	13:49	- 11:39 (2+21:50)	
administ	pts/0	:	Fri Jul 20	11:30	- 13:36 (02:06)	
administ	:0	:	Fri Jul 20	11:27	- 13:37 (02:09)	
(unknown	:0	:	Fri Jul 20	11:26	- 11:27 (00:01)	
reboot	system boot	3.10.0-514.el7.x	Fri Jul 20	11:25	- 13:37 (02:12)	
wtmp begins Fri Jul 20 11:25:07 2018						
[root@plablinux01 ~]#						

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

## Step 2

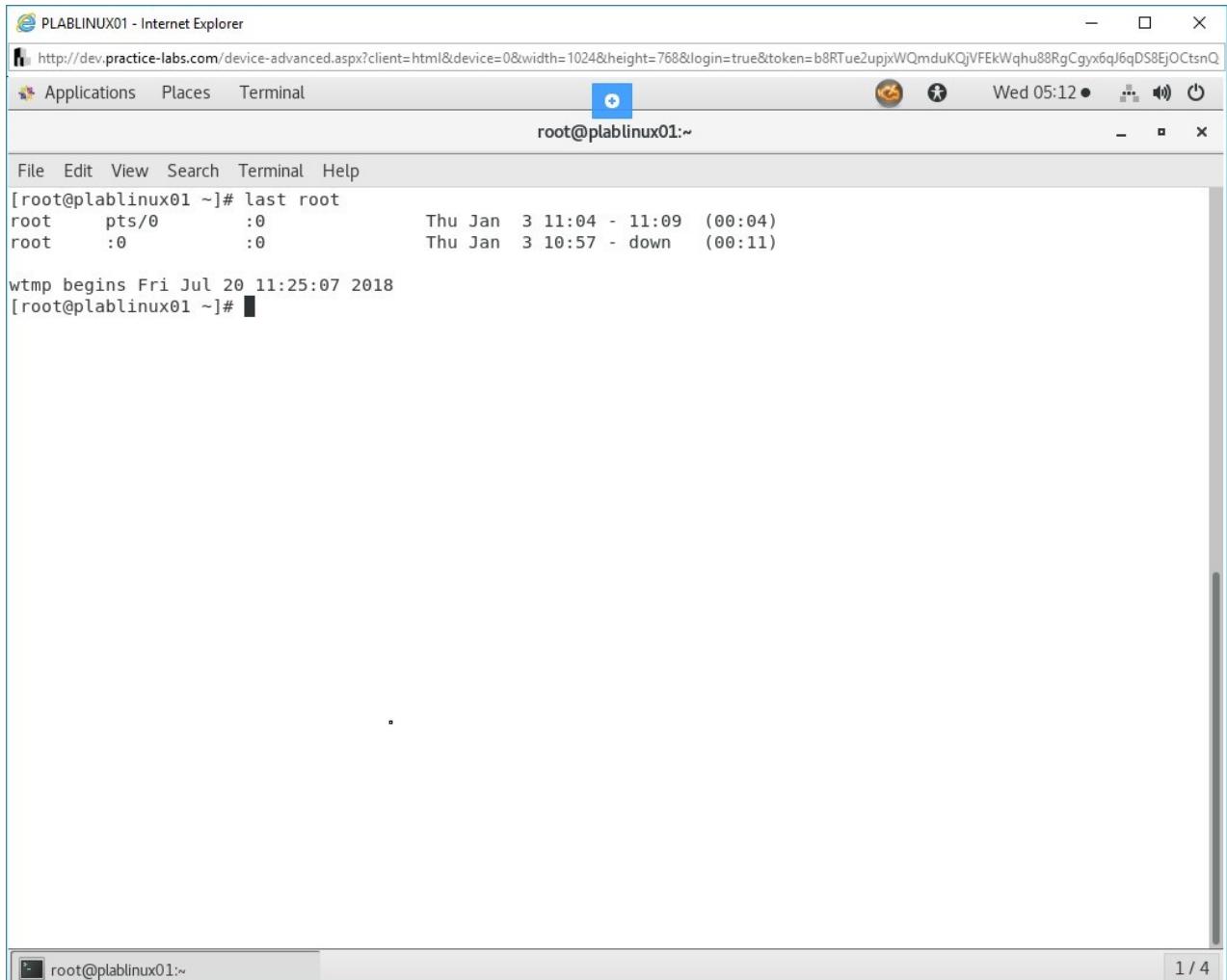
Clear the screen by entering the following command:

```
clear
```

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

**last root**

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



The screenshot shows a terminal window titled "PLABLINUX01 - Internet Explorer" running on a Linux system. The window title bar includes the URL "http://dev.practice-labs.com/device-advanced.aspx?client=html&device=0&width=1024&height=768&login=true&token=b8RTue2upjxWQmduKQjVFEkWqhu88RgCgyx6ql6qDS8EjO CtsnQ". The window has a standard Linux desktop interface with icons for Applications, Places, Terminal, and a power button. The status bar at the bottom shows "root@plablinux01:~" and the date/time "Wed 05:12". The terminal window itself displays the command "last root" followed by a log of user sessions:

```
[root@plablinux01 ~]# last root
root pts/0 :0 Thu Jan 3 11:04 - 11:09 (00:04)
root :0 :0 Thu Jan 3 10:57 - down (00:11)

wtmp begins Fri Jul 20 11:25:07 2018
[root@plablinux01 ~]#
```

The status bar at the bottom of the terminal window also shows "root@plablinux01:~". In the bottom right corner of the terminal window, there is a small thumbnail preview labeled "1 / 4".

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

## Step 3

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

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

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

```
root@plablinux01:~# cat /var/log/wtmp
reboot system boot 3.10.0-862.9.1.e Tue Jul 24 11:45 - 13:08 (01:23)
administ pts/0 :0 Tue Jul 24 11:40 - 11:45 (00:04)
administ pts/0 :0 Mon Jul 23 11:42 - 12:02 (00:19)
administ :0 :0 Mon Jul 23 11:41 - 11:45 (1+00:03)
(unknown :0 :0 Mon Jul 23 11:40 - 11:41 (00:00)
reboot system boot 3.10.0-514.el7.x Mon Jul 23 11:40 - 13:08 (1+01:28)
administ pts/0 :0 Mon Jul 23 11:38 - 11:39 (00:00)
administ pts/0 :0 Mon Jul 23 11:31 - 11:36 (00:05)
administ :0 :0 Mon Jul 23 11:31 - 11:39 (00:08)
(unknown :0 :0 Mon Jul 23 11:28 - 11:31 (00:02)
reboot system boot 3.10.0-514.el7.x Mon Jul 23 11:28 - 11:39 (00:10)
administ :0 :0 Fri Jul 20 17:07 - 17:09 (00:01)
(unknown :0 :0 Fri Jul 20 17:06 - 17:07 (00:01)
reboot system boot 3.10.0-514.el7.x Fri Jul 20 17:06 - 11:39 (2+18:33)
administ pts/0 :0 Fri Jul 20 16:58 - 17:02 (00:04)
administ pts/0 :0 Fri Jul 20 16:57 - 16:58 (00:00)
administ :0 :0 Fri Jul 20 16:55 - 17:02 (00:07)
(unknown :0 :0 Fri Jul 20 16:55 - 16:55 (00:00)
reboot system boot 3.10.0-514.el7.x Fri Jul 20 16:55 - 11:39 (2+18:44)
administ pts/0 :0 Fri Jul 20 15:27 - 15:59 (00:31)
administ pts/0 :0 Fri Jul 20 15:26 - 15:27 (00:01)
administ :0 :0 Fri Jul 20 15:24 - 16:49 (01:25)
(unknown :0 :0 Fri Jul 20 15:23 - 15:24 (00:00)
reboot system boot 3.10.0-514.el7.x Fri Jul 20 15:23 - 11:39 (2+20:15)
administ pts/0 :0 Fri Jul 20 13:58 - 15:20 (01:22)
administ :0 :0 Fri Jul 20 13:50 - 15:20 (01:29)
(unknown :0 :0 Fri Jul 20 13:49 - 13:50 (00:01)
reboot system boot 3.10.0-514.el7.x Fri Jul 20 13:49 - 11:39 (2+21:50)
administ pts/0 :0 Fri Jul 20 11:30 - 13:36 (02:06)
administ :0 :0 Fri Jul 20 11:27 - 13:37 (02:09)
(unknown :0 :0 Fri Jul 20 11:26 - 11:27 (00:01)
reboot system boot 3.10.0-514.el7.x Fri Jul 20 11:25 - 13:37 (02:12)

wtmp begins Fri Jul 20 11:25:07 2018
[root@plablinux01 ~]#
```

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

## Step 4

Clear the screen by entering the following command:

```
clear
```

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

```
lastlog
```

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

The screenshot shows a terminal window titled 'root@plablinux01:~'. The window displays the output of the 'lastlog' command, which lists various system users and their login history. Most users are listed as 'Never logged in'. Some users like 'gdm' and 'administrator' have specific login details shown. The terminal window has a standard Linux-style interface with a menu bar and a status bar at the bottom.

```
File Edit View Search Terminal Help
games          **Never logged in**
ftp           **Never logged in**
nobody        **Never logged in**
systemd-bus-proxy    **Never logged in**
systemd-network     **Never logged in**
dbus           **Never logged in**
polkitd        **Never logged in**
abrt           **Never logged in**
unbound        **Never logged in**
tss            **Never logged in**
libstoragemgmt   **Never logged in**
rpc             **Never logged in**
colord          **Never logged in**
usbmuxd         **Never logged in**
saslauth        **Never logged in**
geoclue         **Never logged in**
rtkit           **Never logged in**
radvd           **Never logged in**
rpcuser         **Never logged in**
nfsnobody       **Never logged in**
qemu            **Never logged in**
chrony          **Never logged in**
setroubleshoot  **Never logged in**
pulse           **Never logged in**
gdm              :0      Wed Jan 23 03:13:20 +0000 2019
gnome-initial-setup  **Never logged in**
sshd            **Never logged in**
avahi           **Never logged in**
postfix         **Never logged in**
ntp              **Never logged in**
tcpdump         **Never logged in**
administrator   :0      Wed Jan 23 03:17:48 +0000 2019
gluster         **Never logged in**
saned           **Never logged in**
[root@plablinux01 ~]#
```

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

## Step 5

Clear the screen by entering the following command:

```
clear
```

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

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

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

The screenshot shows a terminal window titled "PLABLINUX01 - Internet Explorer". The URL in the address bar is "http://dev.practice-labs.com/device-advanced.aspx?client=html&device=0&width=1024&height=768&login=true&token=b8RTue2upjxWQmduKQjVFEkWqhu88RgCgyx6qJ6qDS8EjOCtsnQ". The window title bar also displays "root@plablinux01:~". The terminal window has a menu bar with "File", "Edit", "View", "Search", "Terminal", and "Help". Below the menu is a toolbar with icons for Applications, Places, Terminal, and a blue plus sign. The status bar at the bottom right shows "Wed 05:25". The main area of the terminal displays the output of the "lastlog" command, which lists various system users and their last logins. The output includes:

```
mail
operator
games
ftp
nobody
systemd-bus-proxy
systemd-network
dbus
polkitd
abrt
unbound
tss
libstoragemgmt
rpc
colord
usbmuxd
saslauth
geoclue
rtkit
radvd
rpcuser
nfsnobody
qemu
chrony
setroubleshoot
pulse
gnome-initial-setup
sshd
avahi
postfix
ntp
tcpdump
gluster
saned
[root@plablinux01 ~]#
```

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

## Task 5 - Know the Key Locations for logging

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

### Step 1

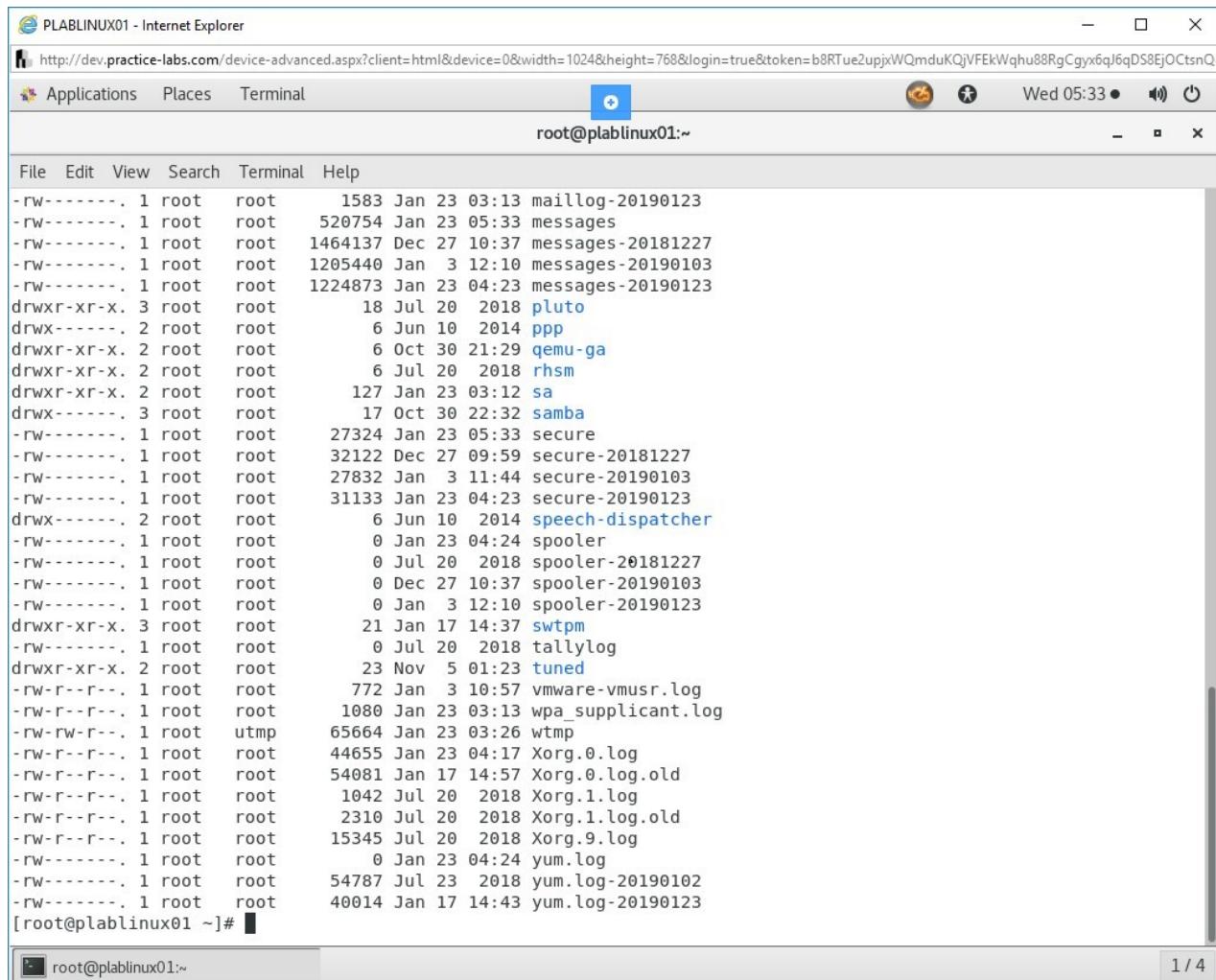
Clear the screen by entering the following command:

```
clear
```

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

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

Press **Enter**.



The screenshot shows a terminal window titled "PLABLINUX01 - Internet Explorer". The URL in the address bar is "http://dev.practice-labs.com/device-advanced.aspx?client=html&device=0&width=1024&height=768&login=true&token=b8RTue2upjxWQmduKQjVFEkWqhu88RgCgyx6qJ6qDS8EjOCtsnQ". The terminal window has tabs for "Applications", "Places", and "Terminal". The title bar shows "root@plablinux01:~". The terminal content displays a long list of log files in the /var/log directory, including "maillog-20190123", "messages", "messages-20181227", "messages-20190103", "messages-20190123", "pluto", "ppp", "qemu-ga", "rhsm", "sa", "samba", "secure", "secure-20181227", "secure-20190103", "secure-20190123", "speech-dispatcher", "spooler", "spooler-20181227", "spooler-20190103", "spooler-20190123", "swtpm", "tallylog", "tuned", "vmware-vmusr.log", "wpa\_supplicant.log", "utmp", "wtmp", "Xorg.0.log", "Xorg.0.log.old", "Xorg.1.log", "Xorg.1.log.old", "Xorg.9.log", "yum.log", "yum.log-20190102", and "yum.log-20190123". The command prompt at the bottom is "[root@plablinux01 ~]#".

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

## Step 2

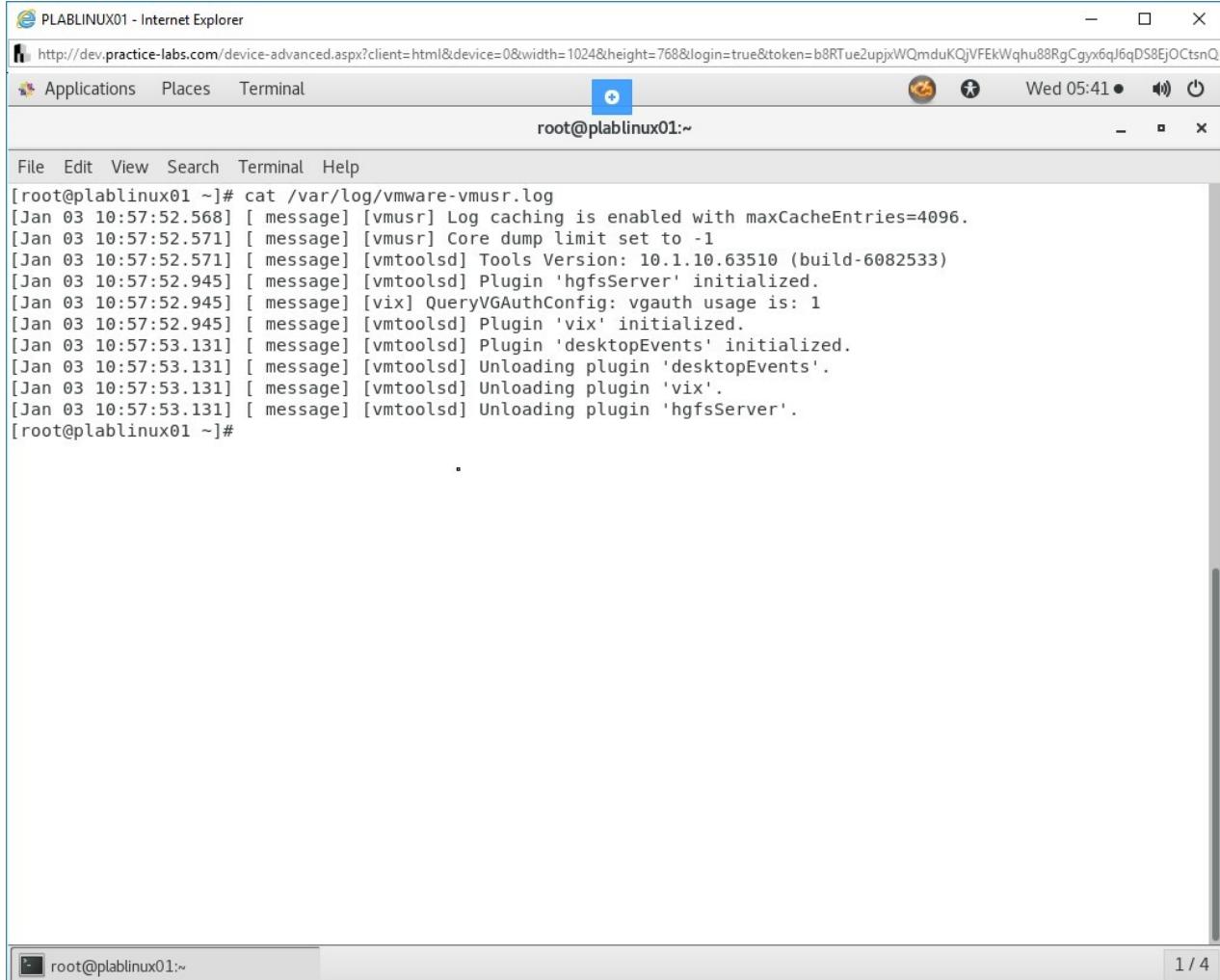
Clear the screen by entering the following command:

```
clear
```

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

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

Press **Enter**.



The screenshot shows a terminal window titled "PLABLINUX01 - Internet Explorer". The URL in the address bar is "http://dev.practice-labs.com/device-advanced.aspx?client=html&device=0&width=1024&height=768&login=true&token=b8RTue2upjxWQmduKQjVFEkWqhu88RgCgyx6qJ6qDS8EjOOctsnQ". The window title bar also displays "root@plablinux01:~". The terminal content shows the output of the "cat /var/log/vmware-vmusr.log" command, which logs various initialization messages for the vmtoolsd service. The log entries include:

```
[root@plablinux01 ~]# cat /var/log/vmware-vmusr.log
[Jan 03 10:57:52.568] [ message] [vmusr] Log caching is enabled with maxCacheEntries=4096.
[Jan 03 10:57:52.571] [ message] [vmusr] Core dump limit set to -1
[Jan 03 10:57:52.571] [ message] [vmtoolsd] Tools Version: 10.1.10.63510 (build-6082533)
[Jan 03 10:57:52.945] [ message] [vmtoolsd] Plugin 'hgfsServer' initialized.
[Jan 03 10:57:52.945] [ message] [vix] QueryVGAAuthConfig: vgauth usage is: 1
[Jan 03 10:57:52.945] [ message] [vmtoolsd] Plugin 'vix' initialized.
[Jan 03 10:57:53.131] [ message] [vmtoolsd] Plugin 'desktopEvents' initialized.
[Jan 03 10:57:53.131] [ message] [vmtoolsd] Unloading plugin 'desktopEvents'.
[Jan 03 10:57:53.131] [ message] [vmtoolsd] Unloading plugin 'vix'.
[Jan 03 10:57:53.131] [ message] [vmtoolsd] Unloading plugin 'hgfsServer'.
[root@plablinux01 ~]#
```

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

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

## Review

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

## Summary

You completed the following exercise:

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

You should now be able to:

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

## Feedback

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