JONES & BARTLETT LEARNING | INFORMATION SYSTEMS SECURITY & ASSURANCE SERIES

LABORATORY MANUAL TO ACCOMPANY

Security Strategies in Linux Platforms and Applications

INSTRUCTOR EDITION

VERSION 2.0

JONES & BARTLETT
LEARNING

World Headquarters
Jones & Bartlett Learning
5 Wall Street
Burlington, MA 01803
978-443-5000
info@jblearning.com
www.jblearning.com

Jones & Bartlett Learning books and products are available through most bookstores and online booksellers. To contact Jones & Bartlett Learning directly, call 800-832-0034, fax 978-443-8000, or visit our website, www.jblearning.com.

Substantial discounts on bulk quantities of Jones & Bartlett Learning publications are available to corporations, professional associations, and other qualified organizations. For details and specific discount information, contact the special sales department at Jones & Bartlett Learning via the above contact information or send an email to specialsales@jblearning.com.

Production Credits

Chief Executive Officer: Ty Field
President: James Homer
Chief Product Officer: Eduardo Moura
SVP, Curriculum Solutions: Christopher Will
Author: vLab Solutions, LLC, David Kim, President
Editorial Management: High Stakes Writing, LLC, Lawrence J. Goodrich, Editor and Publisher
Product Manager, Custom and Curriculum Solutions: Rainna Erikson
Product Management Assistant: Ned Hinman
Associate Production Editor: Kristen Rogers
Director of Marketing: Alisha Weisman
Senior Marketing Manager: Andrea DeFronzo
VP, Manufacturing and Inventory Control: Therese Connell
Manufacturing and Inventory Control Supervisor: Amy Bacus
Composition: vLab Solutions, LLC
Cover Design: Scott Moden
Manager of Photo Research, Rights & Permissions: Lauren Miller
Cover Image: © ErickN/ShutterStock, Inc.

ISBN: 978-1-284-07490-1

6048

Printed in the United States of America
18 17 16 15 14 10 9 8 7 6 5 4 3 2 1

Contents

Acceptable Use Policy & Usage Restrictions

The hardware, software, tools, and applications described and discussed in this lab manual and as provided by the Virtual Security Cloud Labs/OnDemand Workbench (VSCL) are intended to be used to perform the labs and learning activities described in this lab manual. No other use of these resources is authorized or permitted.

►Warning:
Downloading software or software distribution packages from the VCSL is strictly prohibited. If you wish to obtain a personal copy of an open source software tool or demo version of an application, you must obtain it directly from the vendor (developer) or from an authorized Internet downloads Web site.

Your subscription to and use of the VSCL is restricted to instructional and/or educational purposes as part of an academic program of study at an educational institution. No other use is authorized. Violations of this restriction will result in termination of your lab access without refund.

You are responsible for compliance with all laws governing your access and use of this resource. All applicable federal, state, and local laws govern your access to the VSCL. All information available on the VSCL is subject to U.S. export control laws to the extent applicable and may also be subject to the laws of the country in which you reside.

Your use of the hardware, software, tools, and applications provided in the VSCL is subject to your academic institution's *Code of Student Conduct* and *Acceptable Use Policies* for information technology resources. Suspected violations of the usage restrictions for the VSCL will be reported to your institution's Dean of Students or equivalent academic officer for investigation and action.

Ethics and Your Personal Responsibilities

The material presented in this course is designed to give you a real-life look at the use of various tools and systems that are at the heart of every cybersecurity practitioner's daily responsibilities. During this course, you will have access to software and techniques used by professionals to investigate and test the security of critical infrastructures and information technology systems and devices. With this access come certain ethical responsibilities:

1. Do not exceed your authorized level of access. This includes remaining within your authorized level of access when using lab provided software tools to scan or attack computers and software applications as directed within the lab procedures.
2. Do not attempt to use your authorized access for unauthorized purposes either inside or outside of the VSCL environment.
3. Do not attempt to attack or otherwise compromise the confidentiality, integrity, or availability of *any* IT systems, services, or infrastructures outside of the VSCL.
4. Comply with your academic institution's *Code of Student Conduct* and all other applicable policies and regulations.
5. Comply with applicable federal, state, and local laws regarding the use and misuse of information technology systems and services.
6. Comply with applicable laws regarding intellectual property rights including patents and trademarks and copyrights.

Preface

Welcome! This lab manual is your step-by-step guide to completing the laboratory exercises for this course. You will have an opportunity to gain valuable hands-on experience with professional-grade tools and techniques as you work through the lab activities and answer the lab questions found at the end of each lab.

Virtual Security Cloud Lab

You will use the Virtual Security Cloud Lab (VSCL) resource to complete the learning activities in this lab manual.

▶Note:
The Virtual Security Cloud Lab requires Java, Adobe Flash, and a compatible Web browser. The list of compatible browsers and required version numbers for Java and Flash is available on the VSCL Web site (*http://campus.toolwire.com/b4ubegin/start.asp*). The Technical Support Help Desk will *not* be able to assist you in the use of unsupported Web browsers. If you use an unsupported browser, you may not be able to complete the labs as directed in the lab procedures.

You will need to download and install the Citrix® ICA Web client before you access the VSCL for the first time. This download package is also vailable from the VSCL Web site.

The heart of the VSCL is a virtual Workstation desktop (the vWorkstation) configured to give you access to the tools and resources you need for each lab. The VSCL is a collection of virtual resources that includes Windows and Linux servers, Cisco routers, and well-known applications like Wireshark®, FileZilla®, Nessus®, and Zenmap/Nmap Security Scanner®.

The use of virtualization enables you to perform all of the tasks in this lab manual as if you were performing them in a live production environment without putting your institution's assets at risk. This environment is isolated within self-contained private network that, except for the browser session you use to connect to it, is not connected to the Internet. Some of the lab exercises require the use of the Internet. To successfully complete these steps, you will need to use a workstation with Internet access, such as your local computer.

Capabilities are provided within the VSCL which enable transfer of files between systems within this private network. There is also a capability for downloading lab results files from the vWorkstation to student computers.

How to Use This Lab Manual

This lab manual features step-by-step instructions for completing the following hands-on lab exercises:

Lab #	Lab Title
1	Installing a Core Linux Operating System on a Server
2	Configuring Basic Security Controls on a CentOS Linux Server
3	Hardening Security with User Account Management and Security Controls
4	Applying Hardened Linux Filesystem Security Controls
5	Hardening Security for Linux Services and Applications
6	Hardening Security by Controlling Access
7	Hardening Security for the Linux Kernel
8	Applying Best Practices for Secure Software Management
9	Applying Best Practices for Security Logging and Monitoring
10	Defining Linux OS and Application Backup and Recovery Procedures

Step-by-Step Instructions

For each lab, you are provided with detailed, step-by-step instructions and screen captures showing the results of key steps within the lab. All actions that you are required to take are shown in **bold** font. The screen captures will also help you identify menus, dialog boxes, and input locations.

In each lab, you will perform identical steps, such as opening the virtual lab, logging in to another server, taking screen captures, and transferring files to your local computer. To avoid repeating steps in the lab itself, those common steps have been collected in a separate file, Common Lab Steps.pdf. The file is located on the student landing, the vWorkstation desktop. You may use the instructions within the file to download it and refer to it throughout the lab.

Web References

URLs for Web resources listed in this laboratory manual are subject to change without prior notice. These links were last verified on July 20, 2014. Many times, you can find the required resource by using an Internet search engine and a partial URL or keywords. You may also search the Internet Archives (also referred to as the "Wayback Machine") for a given URL that is no longer available at the original Web site (*http://www.archive.org*).

Technical Support

If you need help completing a lab in this manual, contact the Jones Bartlett Learning Help Desk using the information below. Remember to include the name of your institution and reference the course name and number in your ticket details

Phone: 1-866-601-4525

Online: http://www.jblcourses.com/techsupport

Monday-Thursday:	8AM – 10PM
Friday:	8AM – 8PM
Saturday:	8AM – 5PM
Sunday:	10AM – 11PM
(All hours are EST)	

If you need help outside of these hours, submit an online ticket or leave a message on our toll-free phone line, and someone from the help desk will get back to you as soon as possible.

Credits

Adobe© Reader© is a registered trademark of Adobe Systems Incorporated in the United States and/or other countries. Active Directory©, Excel©, Microsoft©, Windows©, and Windows Server© are registered trademarks of Microsoft Corporation in the United States and/or other countries. Linux© is a registered trademark of Linus Torvalds. Citrix© is a trademark of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the United States Patent and Trademark Office and in other countries. FileZilla© is a registered trademark of Tim Kosse. Firefox© is a registered trademark of the Mozilla Foundation. Nessus© is a registered trademark of Tenable Network Security. Nmap Security Scanner© and Zenmap© are either registered trademarks or trademarks of Insecure.com LLC. Wireshark© is a registered trademark of the Wireshark Foundation. pfSense© is a federally registered trademark of Electric Sheep Fencing LLC. Debian© is a registered trademark of Software in the Public Interest, Inc. Openswan™ is an unregistered trademark of Xelerance. Sam Spade© is a copyright of Steve Atkins. PowerBroker™ is a trademark in the United States and certain other countries of BeyondTrust Software. ClamWin™ is a trademark of ClamWin Pty Ltd. GnuPG© is a copyright of Free Software Foundation, Inc. Snort® is a Registered Trademark owned by Sourcefire, Inc. WinHex© is a copyright of Stefan Fleischmann. P2 Commander™ is a trademark of Paraben© Corporation. Oracle® is a registered trademark of Oracle Corporation. UNIX® is a registered trademark licensed through X/Open Company, Ltd. 1010. Python© is a copyright of Python Software Foundation. Tripwire is a copyright of Tripwire, Inc.

All other product names are the property of their respective owners.

Lab #1 Installing a Core Linux Operating System on a Server

Introduction

Network security best practice mandates that Windows systems and Linux systems be installed on a secure network subnet and updated (patched) using trusted sources. Only the minimum services required should be installed, and unneeded services should be disabled. While this axiom remains true, it can be very difficult to find the right balance between a functional system and a secure system.

On UNIX and Linux systems, program dependencies can make it very hard for new administrators to find this balance. Many administrators simply install GUI-driven servers with standard services (SMTP, HTTP, DNS, X-Window, etc.) and put their faith in the firewall to keep attackers out.

The foundation of host-based security starts with the installation of the operating system (OS). Contrary to popular opinion, there is no such thing as a *secure* operating system, but in this lab, you will learn how to install the Linux CentOS operating system in a secure manner. You will create a new virtual machine, partition the hard drive, and install the Linux operating system. You also will create a non-root user account and verify that key services are (or are not) running.

This lab has four parts, which should be completed in the order specified.

1. In the first part of the lab, you will create a virtual machine and attach installation media.
2. In the second part of this lab, you will begin the Linux operating system installation and partition a virtual hard drive.
3. In the third part of this lab, you will complete the Linux OS installation, and then complete a number of post installation steps on a system that is already installed.
4. Finally, if assigned by your instructor, you will answer a set of challenge questions that allow you to use the skills you learned in the lab to conduct independent, unguided work, similar to what you will encounter in a real-world situation.

Learning Objectives

Upon completing this lab, you will be able to:

- Create a virtual machine and mount an installation ISO file
- Partition a Linux hard disk for security hardening, performance, and application support
- Install Linux in the most secure manner

- Create a non-privileged user account for system administration access as a secure alternative to logging in as a root user

Tools and Software

The following software and/or utilities are required to complete this lab. Students are encouraged to explore the Internet to learn more about the products and tools used in this lab.

- Oracle VM Virtual Box
- CentOS Linux

Deliverables

Upon completion of this lab, you are required to provide the following deliverables to your instructor:

1. Lab Report file including screen captures of the following steps: Part 1, Steps 13 and 26; Part 2, Steps 14 and 42; Part 3, Step 26;
2. Lab Assessments file;
3. Optional: Challenge Questions file, if assigned by your instructor.

Hands-On Steps

▶Note:
This lab contains detailed lab procedures, which you should follow as written. Frequently performed tasks are explained in the Common Lab Tasks document on the vWorkstation desktop. You should review these tasks *before* starting the lab.

1. From the vWorkstation desktop, **open** the **Common Lab Tasks file**.

   If you desire, use the File Transfer button to transfer the file to your local computer and print a copy for your reference.

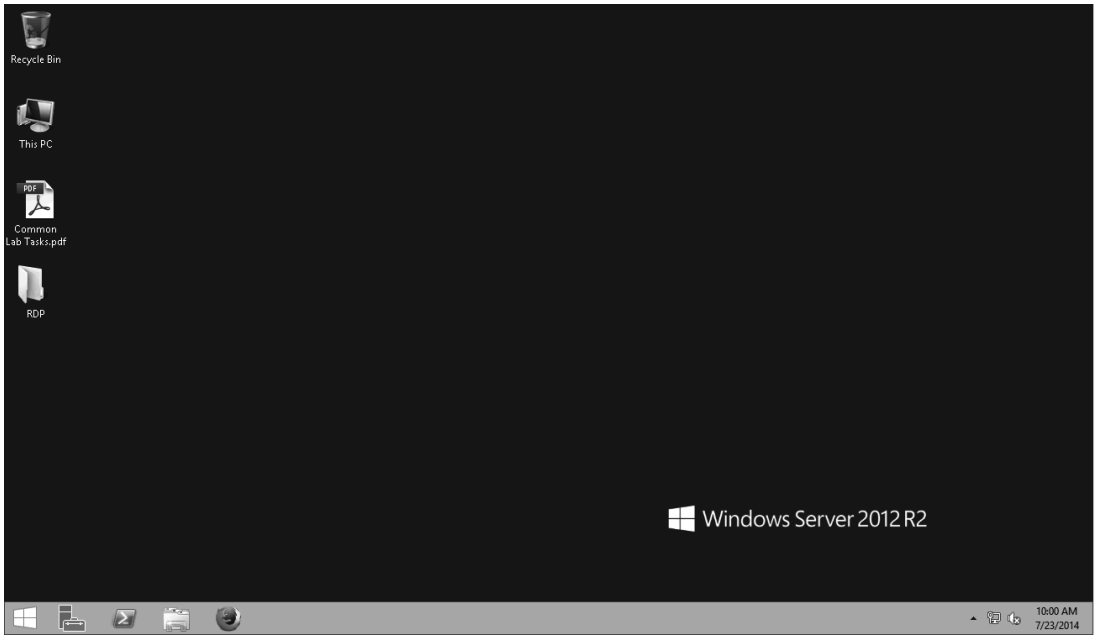


Figure 1 "Student Landing" vWorkstation

2. On your local computer, **create** the **lab deliverable files**.
3. **Review** the **Lab Assessment Worksheet** at the end of this lab. You will find answers to these questions as you proceed through the lab steps.

Part 1: Create a Virtual Machine

▶Note:
In the next steps, you will use the Oracle VM VirtualBox Manager console to create a new virtual machine.

1. **Double-click** the **RDP Folder** on the vWorkstation desktop.
2. **Double-click** the **TargetWindows01 file** to connect to the remote server.

   The remote desktop opens with the IP address of the remote machine (172.30.0.23) in the title bar at the top of the window.

3. On the TargetWindows01 desktop, **double-click** the **Oracle VM VirtualBox icon** to open the Oracle VM VirtualBox hypervisor.

   The left pane of the new window indicates that there is already a completed installation. You will use that image in another part of this lab.

Figure 2 Oracle VM VirtualBox

4. From the Oracle VM VirtualBox Manager toolbar, **click** the **New icon** to begin the process of creating a new virtual machine.

5. In the Create Virtual Machine Wizard, in the Name and operating system window, **type *yourname***, replacing *yourname* with your own name, in the Name text box.

6. From the Type drop-down list, **select Linux**.

7. From the Version drop-down list, **select Other Linux (32 bit)** and **click Next** to continue.

8. On the Memory size page, **slide** the memory handle to **1024 MB** and **click Next**.

9. In the Hard drive page, accept the default (Create a virtual hard drive now) and **click Create** to continue.

10. On the Hard drive file type page, accept the default VDI (VirtualBox Disk Image) and **click Next** to continue.

11. On the Storage on physical hard drive page, accept the default (Dynamically allocated) and **click Next** to continue.

12. On the File location and size page, **type 20GB** in the hard drive size box and **click Create** to specify a size.

The new virtual machine appears in the left pane of the Oracle VM VirtualBox Manager console in a powered-off state.

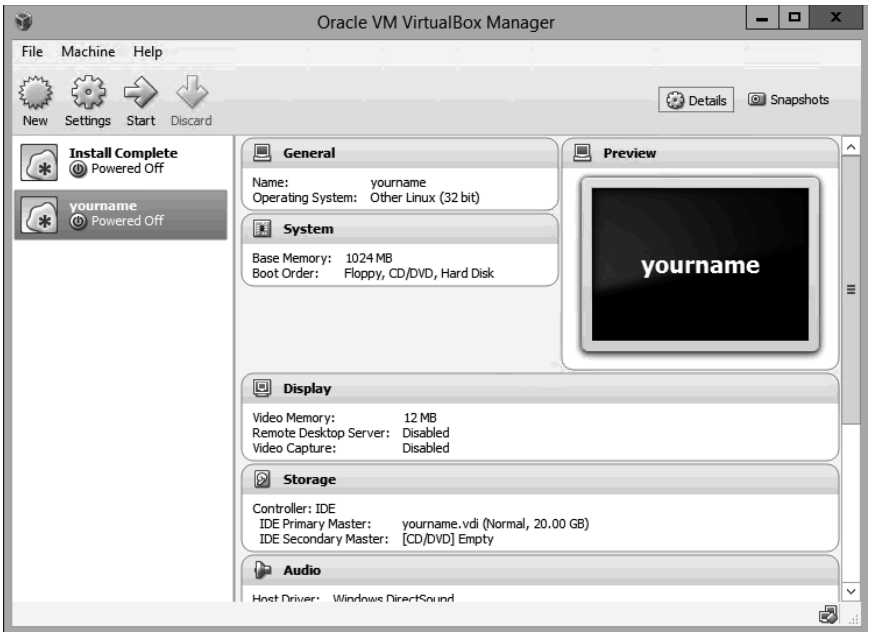


Figure 3 New virtual machine

13. **Make a screen capture** showing the **new virtual machine** and **paste** it into the Lab Report file.

14. In the Oracle VM VirtualBox Manager console, **click** the **Settings icon** to configure the new machine.

15. In the *yourname* Settings window, **click Storage** in the left pane.

16. In the Storage Tree pane, **click** the **Empty CD icon** (in the Controller: IDE tree).

17. In the Attributes pane, **click** the **CD icon** to expand the drop-down list, and **select Choose a virtual CD/DVD disk file** to add an ISO to the virtual CD.

    An ISO file, also called an ISO image, is a single file that contains all of the files or folders necessary for installation.

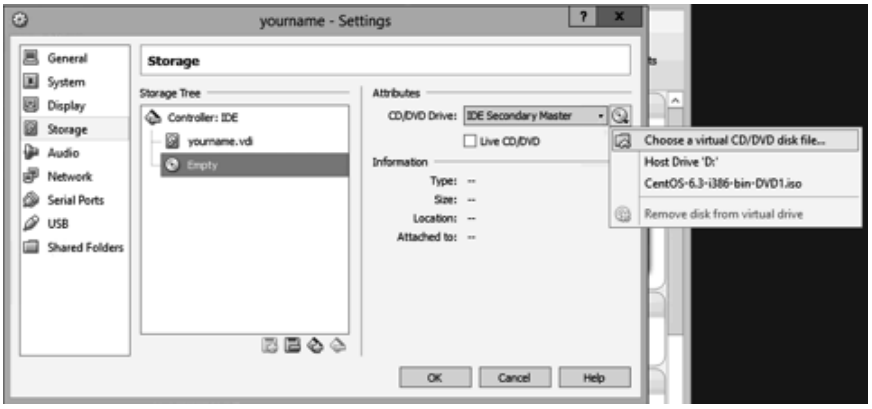


Figure 4 Choose a virtual CD

18. In the Please choose a virtual optical disk file dialog box, **click** the **Desktop icon**, **click** the **CentOS-6.5-i366-bin-DVD1.iso file**, and **click Open** to identify the location of the ISO file.

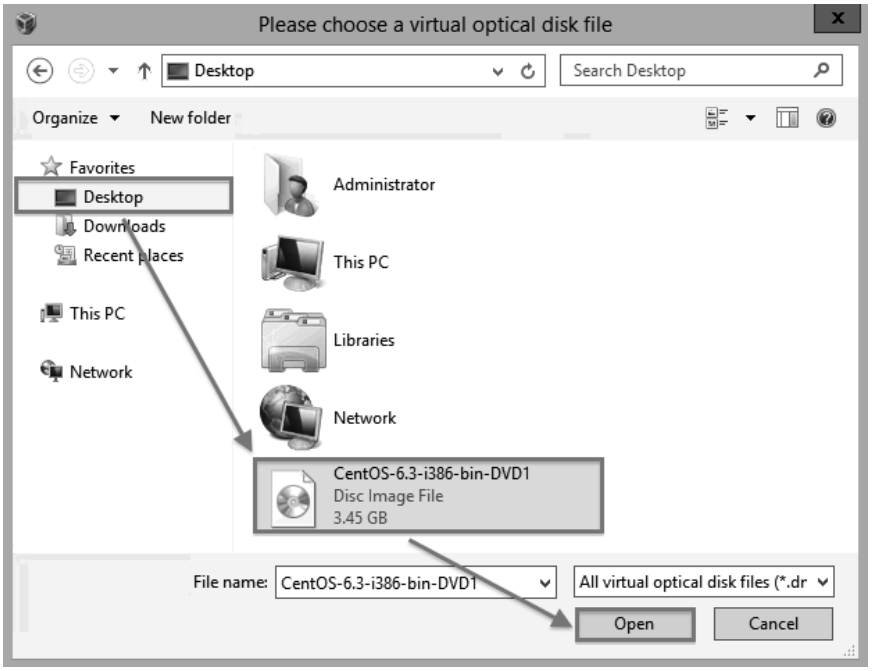


Figure 5 Add an ISO to the virtual CD

19. In the Settings window, **click System** in the left pane.

20. **Click** the **Processor tab** to continue.

21. **Click** the **Enable PAE/NX checkbox** to enable the physical address extension (PAE).

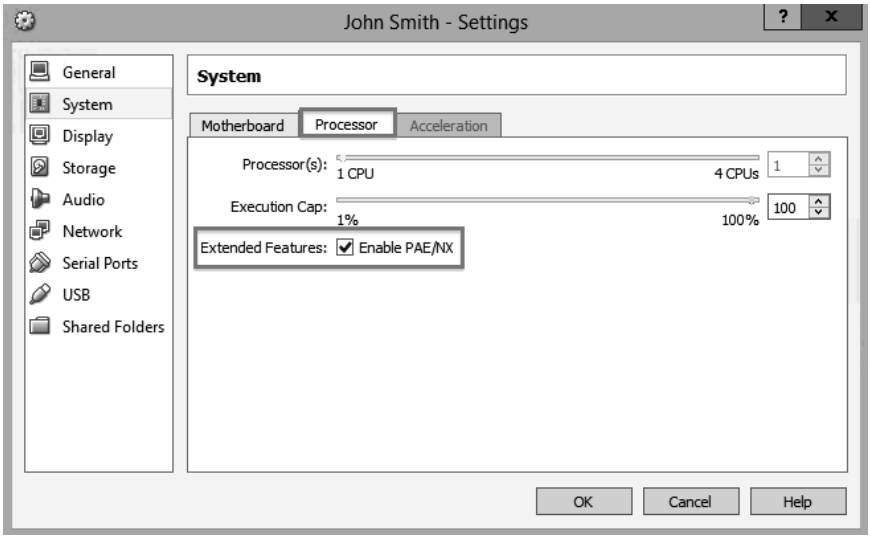


Figure 6 Enable PAE

22. In the Settings window, **click Network** in the left pane.

23. In the Attached to drop-down list, **select Bridged Adapter** to allow the new virtual machine full access to the network.

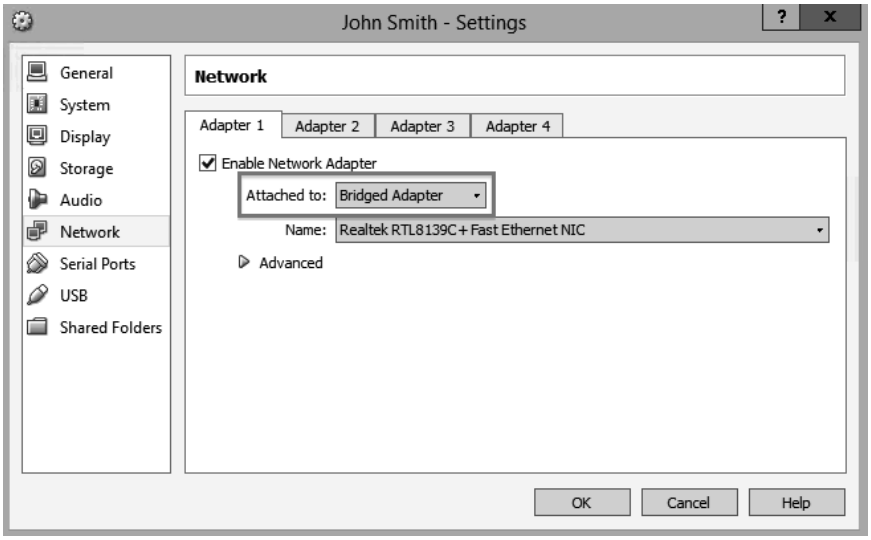


Figure 7 Network adapter settings

24. **Click OK** to close the Settings window.

25. From the Oracle VM VirtualBox Manager toolbar, **click** the **Start icon** to turn on the new virtual machine.

    The new machine will open in a new window and the status in the left pane of the Oracle VM VirtualBox Manager console will change to Running.

26. **Make a screen capture** showing the **status of the new virtual machine** and **paste** it into the Lab Report file.

Part 2: Partition the Virtual Drive

▶Note:
In the next steps, you will begin the installation process of the CentOS operating system on the virtual server you created in Part 1 of this lab. You also will partition the virtual hard drive.

1. When prompted, **click** the **blue x icon** to acknowledge that the auto capture is running.

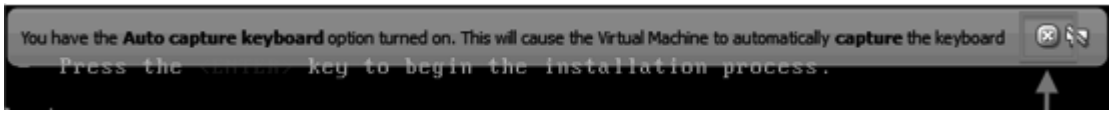


Figure 8 Starting the Linux Install

2. When prompted, **click** the **blue x icon** to acknowledge mouse integration.
3. When prompted, on the Welcome to CentOS for i386 screen, **press** the **Tab key** to move the highlight to the Skip button and **press** the **spacebar** to skip the media test.

   From this point forward the Anaconda graphical installer will take over.

Figure 9 Welcome screen

4. In the resulting window's menu, **click View** and **select Switch to Scaled Mode**.
5. In the VirtualBox - Information dialog box**, click Switch**.
6. On the CentOS splash screen, **click Next** to continue the installation process.
7. On the language selection screen, accept the default selection *English (English)* and **click Next**.

8. On the keyboard layout screen, accept the default keyboard layout *U.S. English* and **click Next**.

9. On the storage devices screen, accept the default selection *Basic Storage Devices* and **click Next**.

   Click the **Yes, discard any data button** to dismiss the Storage Device Warning pop-up.

10. In the hostname screen, **type *yourname***, replacing *yourname* with your own name (all in lowercase and with no spaces) in the Hostname text box, and **click Next**.

Figure 10 Set the Hostname

11. In the time zone page, **select America/Los Angeles** from the drop-down list, **click** the **System Clock uses UTC checkbox** to deselect it, and **click Next**.

12. In the password page, **type qw1290op1** in the Root Password box, **type qw1290op1** in the Confirm box, and **click Next**.

▶Note:
The root user is the system's *super user*. This user account has access to any and everything on the system. Therefore, extreme care should be taken when using this account.

13. On the installation type page, **click** the **Create Custom Layout radio button**.

    You will customize this installation.

14. **Make a screen capture** showing the **installation types** and **paste** it into your Lab Report file.

15. **Click Next** to continue.
16. In the Please Select A Device page, **click** the **Create button** to create a partition.
17. In the Create Storage dialog box, accept the default *Standard Partition*, and **click Create**.
18. In the Add Partition dialog box, **type /boot** in the Mount Point box.
19. In the Size (MB) box, **type 500** to change the size of the /boot partition and **click OK** to continue.

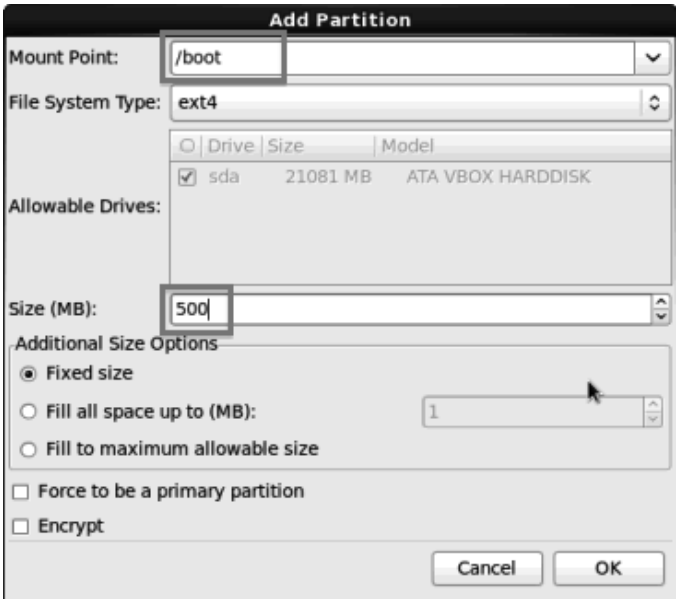


Figure 11 Create a boot partition

20. In the Please Select A Device window, **click** the **Create button** to create a second partition.
21. In the Create Storage dialog box, accept the default *Standard Partition*, and **click Create**.
22. In the Add Partition window, **select swap** from the Filesystem Type drop-down list.
23. In the Size (MB) box, **type 4000** to change the size of the swap partition and **click OK** to continue.

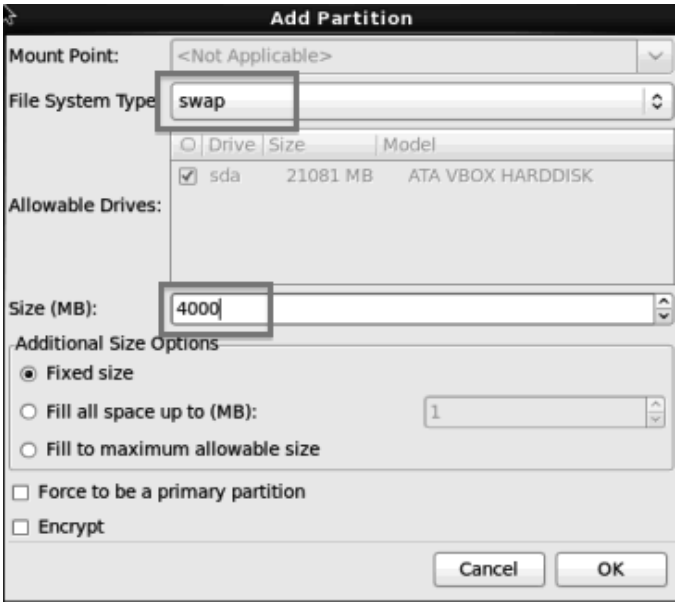


Figure 12 Create a swap partition

▶Note:

Linux has two forms of swap space: the swap partition and the swap file. The swap partition is an independent section of the hard disk used solely for swapping; no other files can reside there. The swap file is a special file in the filesystem that resides among your system and data files. As an independent partition, swap space can be dedicated and improves performance when swapping data from one disk or partition to another.

Swapping is necessary for two important reasons. First, when the system requires more memory than is physically available, the kernel swaps out less frequently used pages and gives memory to the current application (or process) that needs the memory immediately. Second, a significant number of the pages used by an application during its startup phase may only be used for initialization and then never used again. The system can swap out those pages to free up the memory for other applications or even for the disk cache.

The swap partition in Linux should be partitioned separately from the root (/) partition for performance reasons.

24. In the Please Select A Device window, **click** the **Create button** to create a new partition.
25. In the Create Storage window, **click** the **LVM Physical Volume radio button** and **click Create**.
26. In the Size (MB) box, **type 15000** to change the size of the partition and **click OK** to continue.
27. Your new Linux system should have the same partitions (ignore any leftover free space) as in the following figure.

Figure 13 Verify existing partitions

28. In the Please Select A Device window, **click** the **Create button** to create a new partition.

29. In the Create Storage window, **click** the **LVM Volume Group radio button** and **click Create**.

▶Note:
LVM creates a logical physical volume and then a logical volume as a group on top of the physical volume. From LVM, several partitions can be created, such as those for /tmp, /home, and /var. If disk space becomes an issue, LVM can allocate more disk space to volumes from other partitions within the LVM without risking disk loss. Additional hard drives can be added and can immediately become part of the LVM as well.

30. In the Make LVM Volume Group window, **type vg_*yourname***, replacing *yourname* with your own name (all in lowercase and with no spaces) in the Volume Group Name box, and **click Add**.

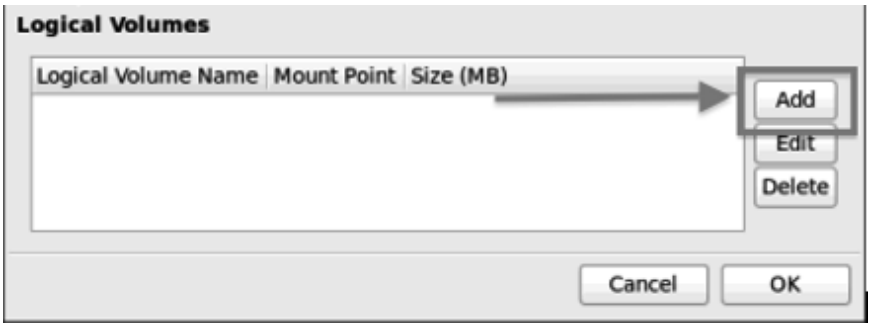


Figure 14 Add logical volumes to a Volume Group

31. In the Make Logical Volume dialog box, **type /var** in the Mount Point box.

32. In the Size (MB) box, **type 2000** to change the size of the volume and **click OK**.

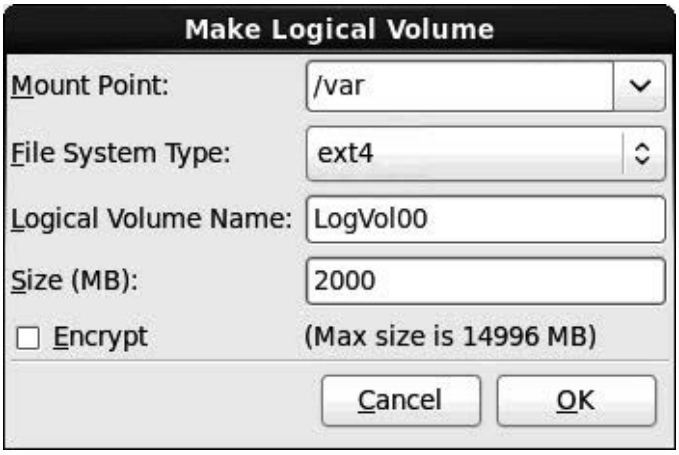


Figure 15 Add /var to volume group

33. In the Make LVM Volume Group box, **click** the **Add button** to add a new volume.
34. In the Make a Logical Volume dialog box, **type /tmp** in the Mount Point box.
35. In the Size (MB) box, **type 2000** to change the size of the volume and **click OK**.
36. In the Make LVM Volume Group box, **click** the **Add button** to add a new volume.
37. In the Make a Logical Volume dialog box, **type /home** in the Mount Point box.
38. In the Size (MB) box, **type 2000** to change the size of the volume and **click OK**.
39. In the Make LVM Volume Group box, **click** the **Add button** to add a new volume.
40. In the Make a Logical Volume dialog box, **type /** in the Mount Point box to add a root drive.
41. In the Size (MB) box, **type 8000** to change the size of the volume and **click OK** to view the completed volumes.

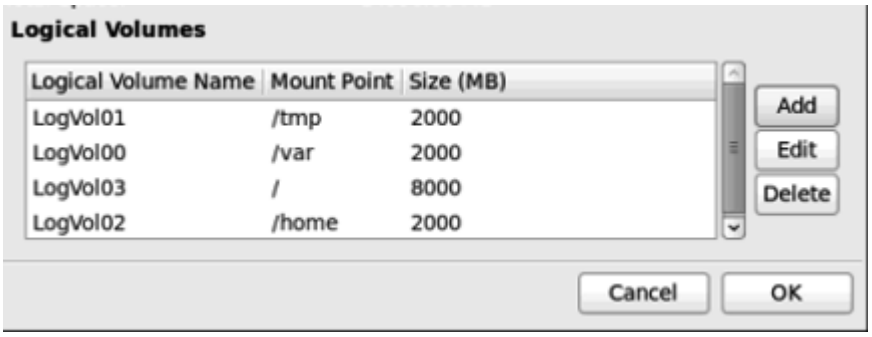


Figure 16 Completed volume group

42. In the Make LVM Volume Group windows, **click OK** to return to the Please Select A Device page.

43. **Make a screen capture** showing the **completed partition in the Please Select A Device page** and **paste** it into the Lab Report file.

44. In the Please Select A Device page, **click Next** to continue.

45. In the Format Warnings window, **click** the **Format button** to dismiss the pop-up.

46. In the Writing storage configuration to disk window, **click** the **Write changes to disk button** to continue.

    The virtual hard drive will be formatted and partitioned based on your selection in the previous lab parts; this process can take several (2–5) minutes.

Part 3: Complete the Installation and Configure Linux

▶Note:
In the next steps, you will complete the CentOS installation process.

1. On the boot loader page, **click** the **Use a boot loader password checkbox** to select it.

2. When prompted, **type qw1290op1** to set the boot loader password, **type qw1290op1** to confirm the boot loader password, and **click OK**.

3. On the boot loader page, **click Next** to continue.

4. In the default installation screen, **click** the **Minimal radio button**, **click** the **Customize now radio button** (at the bottom of the screen), and **click Next**.

   In the next window, you will see software categories (on the left) and software packages (on the right). Because this is a Minimal installation, all optional packages are unchecked by default. Select each category on the left (one at a time) and make note of which software packages on the right are affected. In a production installation, you would uncheck any packages that are not required for your environment.

▶Note:
The Minimal installation option will not include an X-Window system for GUI-driven administration. In other labs, you will be able to connect to the Linux server using an XRDP GUI to make the learning experience more clear; but in a production environment, it is recommended that you *not* run the X-Window environment because it is not needed, and X-Window adds both overhead and an increased security risk. In a production environment, a desktop environment may be helpful in certain situations; however, best practice recommends setting the default runlevel to 3 in this case. Runlevel 3 is a multi-user mode without running X-Window or any GUI services.

5. When you are done reviewing the software packages, **verify** that **no checkboxes** are selected and **click Next** to start the installation.

Figure 17 Deselect all software packages

6. **Close** the **installation window**, *without* waiting for the installation process to complete.

   To ensure that all students have the same starting point, you will use the existing Install Complete virtual machine to complete the rest of this lab, so it is not necessary to complete the installation on this machine.

7. When prompted, **click** the **Power off the machine radio button** and **click OK** to stop the process.

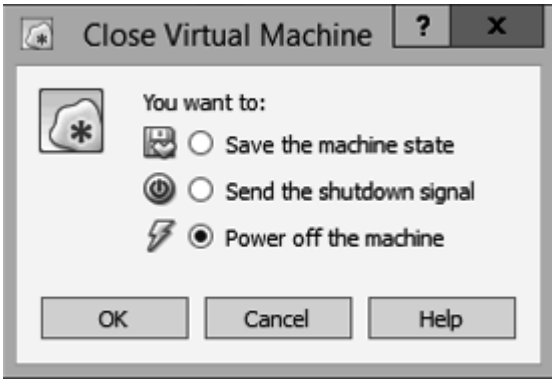


Figure 18 Power off the machine

8. In the Oracle VM VirtualBox Manager console, **click** the **Install Complete virtual machine** to select it and **click** the **Start icon** to open that machine in a new window.

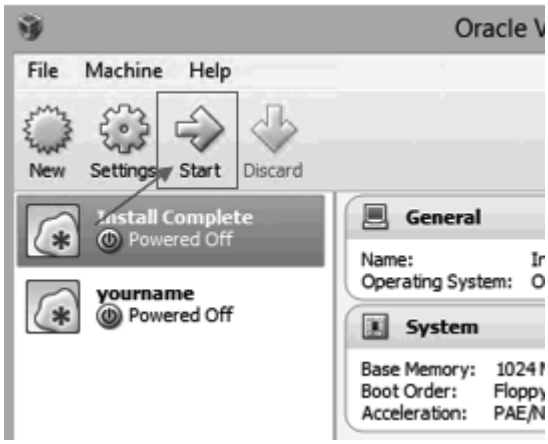


Figure 19 Start the Install Complete machine

9. When prompted, **click Switch** to switch to Scale mode.

10. When prompted, **click** the **blue x icon** to acknowledge that the auto capture is running.

11. When prompted, **click** the **blue x icon** to acknowledge mouse integration, and wait while the Linux server boots up (approximately 2-5 minutes).

    When the server is ready, the system will display a prompt that states *installcomplete login:*.

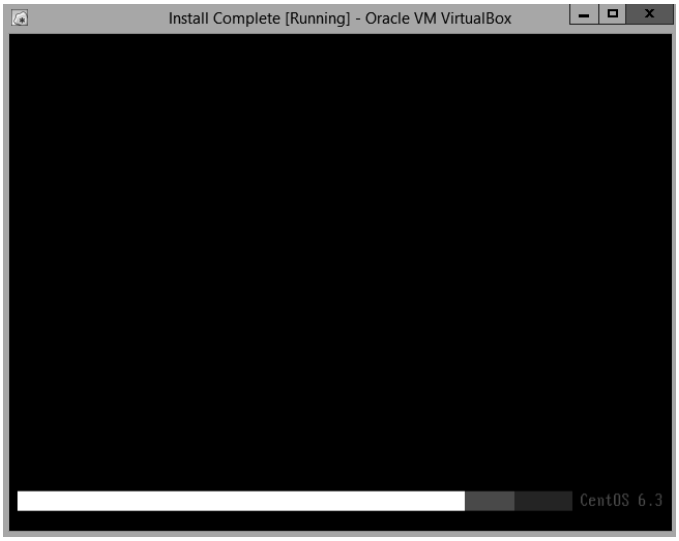


Figure 20 Boot up the CentOS Linux machine

12. When prompted, **type root** and **press Enter** to log in as the root user.

13. At the password prompt, **type qw1290op1** (the same password you used for the new server you created earlier in this lab) and **press Enter**.

    The login prompt will change to *[root@installcomplete ~]#*. At this time, the only user created on the machine is the root user. You will need to add a non-root user and set a password for that account.

14. At the prompt, **type adduser student** and **press Enter** to add the *student* account.

15. At the prompt, **type passwd student** and **press Enter** to access the password information for the student account.

▶Note:
In Linux operating systems, the /etc/passwd file is a text-based database of information about users who may log into the system or other operating system identities that own running processes. The /etc/passwd file is a text file with one record per line, each describing a user account. Each record consists of seven fields separated by colons. An example record may be:

jsmith:x:1001:1000:Joe Smith,Room 1007,(234)555-8910,(234)555-0044,email:/home/jsmith:/bin/sh

The ordering of the records within the file is generally unimportant, but in this example, the second field stores information used to validate a user's password. Rather than using the actual password in a location that is so widely known, best practice usually sets this field to "x" (or some other indicator) as shown in this example. The actual password information is stored in a separate shadow password file. A common practice for deactivating an account to prevent it being used is to set the field to an asterisk (*).

16. When prompted for the new password, **type pass=7890** and **press Enter** to change the password for the student account to *pass=7890*.

17. When prompted to confirm the password, **type pass=7890** and **press Enter**.

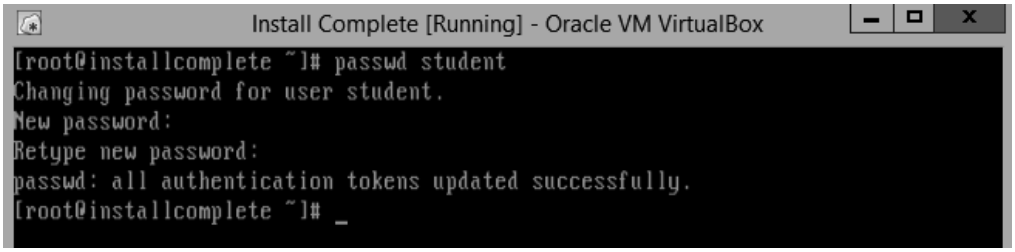


Figure 21 Change the student account password

18. At the prompt, **type exit** and **press enter** to log off the root account.

19. At the login prompt, **type student** and **press Enter** to log in as the student account.

20. At the password prompt, **type pass=7890** and **press Enter**.

    You will be logged in as the student user. The login prompt will change to *[student@installcomplete ~]$*.

21. At the prompt, **type sudo vi /etc/sysconfig/network-scripts/ifcfg-eth0** and **press Enter** to configure networking in the vi Editor with the elevated privileges of the sudo command.

    You will be prompted with a "lecture" reminding you that elevated privilege come with elevated responsibility. Each user is given this lecture the first time they try to use the sudo command.

22. At the password prompt, **type pass=7890** (the password for the student account) and **press Enter**.

    The student account has not been added to the sudoers configuration file, so the student user cannot elevate their privilege. You will configure the sudoers file in another lab.

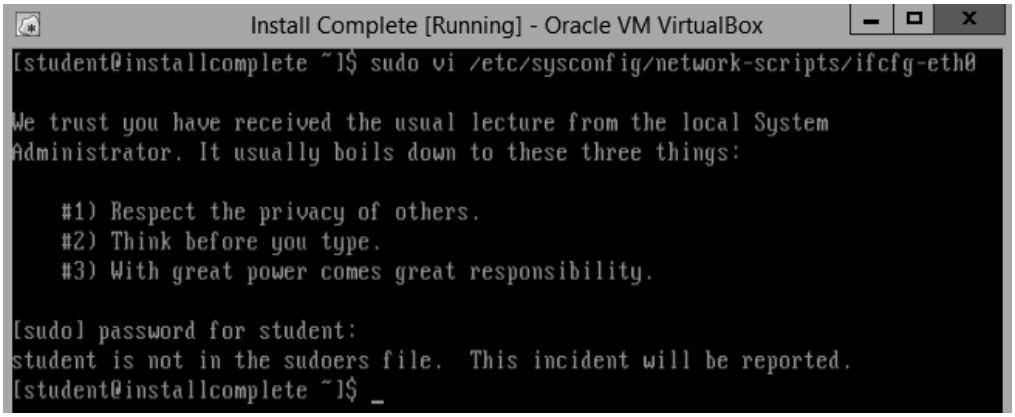


Figure 22 Attempt to use sudo user

23. At the prompt, **type su** and **press Enter** to log in as the root user.

24. When prompted, **type qw1290op1** and **press Enter**.

25. At the prompt, **type whoami** and **press Enter** to confirm the root account is logged in.

26. **Make as screen capture** showing the **result of the whoami command** and **paste** it into the Lab Report file.

27. At the prompt, **type sestatus** and **press Enter** to verify that SELinux (Security Enhanced Linux) is enabled and the current mode is *enforcing*.

▶Note:
Security Enhanced Linux is a mandatory access control system designed to help a Linux system adhere to the principle of least privilege. You will configure and test SELinux in other labs.

28. At the prompt, **type iptables –L** and **press Enter** to see if the iptables firewall is running.

    While the output of the L (list) command can be daunting, in this instance it is simply indicating that all inbound and outbound traffic is allowed (ACCEPT). You will configure iptables in another lab.

29. At the prompt, **type ntpd –q** and **press Enter** to set the Network Time Protocol (NTP).

The system should display an error because it cannot find the ntpd command. NTP is an important service that ensures the clock on the Linux systems stays current. If this was a production server, the ntpd service would need to be installed.

▶Note:
System time must be synchronized with other network servers and/or an atomic-time server on the Internet for consistent operations and valid chronology of events. Synchronized timestamps aid in searching logs for errors and potential security breaches. Certain network services also rely on synchronized system clocks to verify security and other network tokens across the network. If the clocks are out of sync, many services may malfunction.

30. **Close** the **virtual lab**, or proceed with Part 4 to answer the challenge question for this lab.

Part 4: Challenge Questions

▶Note:
The following challenge questions are provided to allow independent, unguided work, similar to what you will encounter in a real situation. You should aim to improve your skills by getting the correct answer in as few steps as possible. Use screen captures in your lab document where possible to illustrate your answers.

1. In Part 3, Step 21, you tried to configure networking on the virtual machine by typing sudo vi /etc/sysconfig/network-scripts/ifcfg-eth0 and pressing Enter. However, student was not configured in the /etc/sudoers file at that time. For this challenge, you will configure and test networking. While logged in as the root user, repeat Part 3, Step 21 and modify the ifcfg-eth0 file (as shown in the following figure) to give the Linux VM an IP address (172.30.0.21).

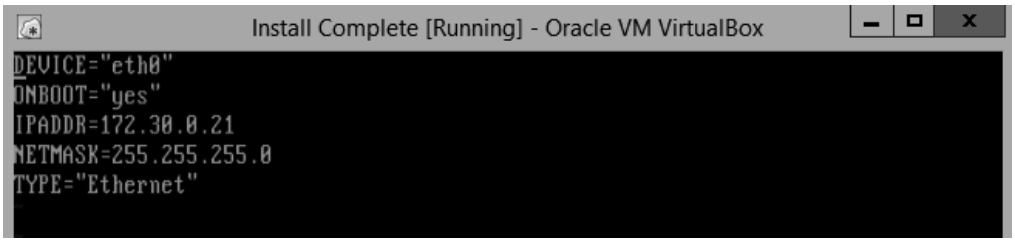


Figure 23 Modify the existing file to match this version

   a. If not root already, **type su** and **press Enter**.
   b. At the password prompt, **type qw1290op1** and **press Enter**.
   c. At the prompt, **type vi /etc/sysconfig/network-scripts/ifcfg-eth0** and **press Enter** to open the file in the vi Editor.
   d. **Press I** to enter the Insert mode and modify the file to match Figure 20.
   e. **Press ESC** to exit the Insert mode and **type :wq!** and **press Enter** to save the file.
   f. At the prompt, **type /etc/init.d/network restart** and **press Enter** to restart networking.

2. Confirm your configuration by pinging the vWorkstation (172.30.0.2). Make a screen capture showing the Ping results and paste it into your Challenge Questions file.

   At the prompt, **type ping 172.30.0.2** and **press Enter** to test the network configuration. **Press CTRL+C** to stop the Ping.

▶Note:
This completes the lab. **Close** the **virtual lab**, if you have not already done so.

Evaluation Criteria and Rubrics

The following are the evaluation criteria for this lab that students must perform:

1. Create a virtual machine and mount an installation ISO file – [**25%**]
2. Partition a Linux hard disk for security hardening, performance, and application support – [**25%**]
3. Install Linux in the most secure manner – [**25%**]
4. Create a non-privileged user account for system administration access as a secure alternative to logging in as a root user – [**25%**]

Lab # 1 – Assessment Worksheet

Installing a Core Linux Operating System on a Server

Course Name and Number: _____

Student Name: _____

Instructor Name: _____

Lab Due Date: _____

Overview

The foundation of host-based security starts with the installation of the operating system (OS). Contrary to popular opinion, there is no such thing as a *secure* operating system, but in this lab, you learned how to install the Linux CentOS operating system in a secure manner. You created a new virtual machine, partitioned the hard drive, and installed the Linux operating system. You also created a non-root user account and verified that key services were (or were not) running.

Lab Assessment Questions & Answers

1. During the Minimal install, NTP (Network Time Protocol) server was not installed. From a security perspective, why is it important for a system to keep accurate time?

   Note following Part 3, Step 29. System time must be synchronized with other network servers and/or an atomic-time server on the Internet for consistent operations and valid chronology of events. Synchronized timestamps aid in searching logs for errors and potential security breaches. Certain network services also rely on synchronized system clocks to verify security and other network tokens across the network. If the clocks are out of sync, many services may malfunction.

2. During the install, you set a password for the root user. What is the root user, and when is it appropriate to use this account?

   Note following Part 2, Step 12. The root user is the system's super user. This user account has access to anything and everything on the system. Therefore, extreme care should be taken when using this account.

3. The Minimal installation process that was used in the lab did not include an X-Window interface. Why is it best practice *not* to run X-Window in a production environment?

   Note following Part 3 Step 4. In a production environment, it is recommended that you not run the X-Window environment because it is not needed and X-Window adds both overhead and an increased security risk. In a production environment, a desktop environment may be helpful in certain situations; however, best practice recommends setting the default runlevel to 3 in this case. Runlevel 3 is a multi-user mode without running X-Window or any GUI services.

4. What partitioning options are available when installing CentOS?

   Part 2, Step 14. Use All Space, Replace Existing Linux System(s), Shrink Current System, Use Free Space, and Create Custom Layout.

5. Why is it important to put the swap file on a separate partition from the root (/) partition?

   Note following Figure 12. The swap partition in Linux should be partitioned separate from the root (/) partition for performance reasons.

6. What is the significance of the swap partition in a Linux system?

   Note following Figure 12. Swapping is necessary for two important reasons. First, when the system requires more memory than is physically available, the kernel swaps out less frequently used pages and gives memory to the current application (or process) that needs the memory immediately. Second, a significant number of the pages used by an application during its startup phase may only be used for initialization and then never used again. The system can swap out those pages to free up the memory for other applications or even for the disk cache.

7. How is the passwd file used, and what fields make up its content? Explain.

   Note following Part 3, Step 15. In Linux operating systems, the /etc/passwd file is a text-based database of information about users who may log into the system or other operating-system identities that own running processes. The /etc/passwd file is a text file with one record per line, each describing a user account. Each record consists of seven fields separated by colons.

8. Why create a Logical Volume Manager (LVM) partition?

   Note following Part 2, Step 28. LVM creates a logical physical volume and then a logical volume as a group on top of the physical volume. From LVM, several partitions can be created, such as those for /tmp, /home, and /var. If disk space becomes an issue, LVM can allocate more disk space to volumes from other partitions within the LVM without risking disk loss. Additional hard drives can be added and can immediately become part of the LVM as well.

Lab #2 Configuring Basic Security Controls on a CentOS Linux Server

Introduction

To some extent, information security on Linux systems is no different from information security on Microsoft or Apple systems. As an administrator, you'll take many of the same steps as you would in any other system. You'll create firewalls, set up bastions, manage users, encrypt filesystems, configure servers, customize applications, and work with intrusion prevention and detection systems. The Linux paradigm is different in some ways, however. With Linux, you can customize the kernel and set up mandatory access with Application Armor (AppArmor) or Security Enhanced Linux (SELinux), a set of security enhancements built into the Linux kernel.

In this lab, you will secure a Linux server system. You will secure the bootloader, enable iptables firewall, and run SELinux to help lock down the Linux OS. By securing the bootloader you can prevent access to single user mode and the GRUB (Grand Unified Bootloader) Console during the boot of the system. Enabling iptables and applying firewall rules can ensure that only the applications you want have the ability to reach or reach out from your computer. You also will apply access control lists (ACLs) to directories and files within the lab to secure the file and data access and then verify those permissions on the system.

This lab has seven parts, which should be completed in the order specified.

1. In the first part of the lab, you will harden the GRUB bootloader, which can load a variety of free and proprietary operating systems.
2. In the second part of the lab, you will confirm SELinux is enabled.
3. In the third part of the lab, you will enable iptables to help lock down services on a Linux system to only those who require network access and deny external connections to any other unnecessary port or service.
4. In the fourth part of the lab, you will create a new group, *web*, and enable sudo user access for the existing *wheel* group.
5. In the fifth part of the lab, you will experiment with the immutable permission extended file attribute.
6. In the sixth part of the lab, you will set access control list permissions on a file.
7. Finally, if assigned by your instructor, you will explore the virtual environment on your own to answer a set of challenge questions that allow you to use the skills you learned in the lab to conduct independent, unguided work, similar to what you will encounter in a real-world situation.

Learning Objectives

Upon completing this lab, you will be able to perform the following:

- Configure the bootloader with the timeout set to 0 and password credential to mitigate tampering with the GRUB loader and the boot sequence of the server
- Enable SELinux on a CentOS Linux Server and set it to enforcing mode
- Create a student user account and add it to a user group for managing permissions and applying access controls across the system
- Configure user groups with limited sudo access (with password credentials) to log and properly monitor access across the system
- Create iptables set to "on" for runlevels 2 and 5 to enable an internal, host-based IP stateful firewall
- Set restrictions and permissions for user access to files and system log files

Tools and Software

The following software and/or utilities are required to complete this lab. Students are encouraged to explore the Internet to learn more about the products and tools used in this lab.

- None

Deliverables

Upon completion of this lab, you are required to provide the following deliverables to your instructor:

1. Lab Report file including screen captures of the following steps: Part 1, Steps 15 and 22; Part 2, Step 3; Part 3, Step 5; Part 4, Step 5; Part 5, Steps 4 and 11; and Part 6, Step 4;
2. Lab Assessments file;
3. Optional: Challenge Questions file, if assigned by your instructor.

Hands-On Steps

▶Note:
This lab contains detailed lab procedures, which you should follow as written. Frequently performed tasks are explained in the Common Lab Tasks document on the vWorkstation desktop. You should review these tasks *before* starting the lab.

1. From the vWorkstation desktop, **open** the **Common Lab Tasks file**.

   If you desire, use the File Transfer button to transfer the file to your local computer and print a copy for your reference.

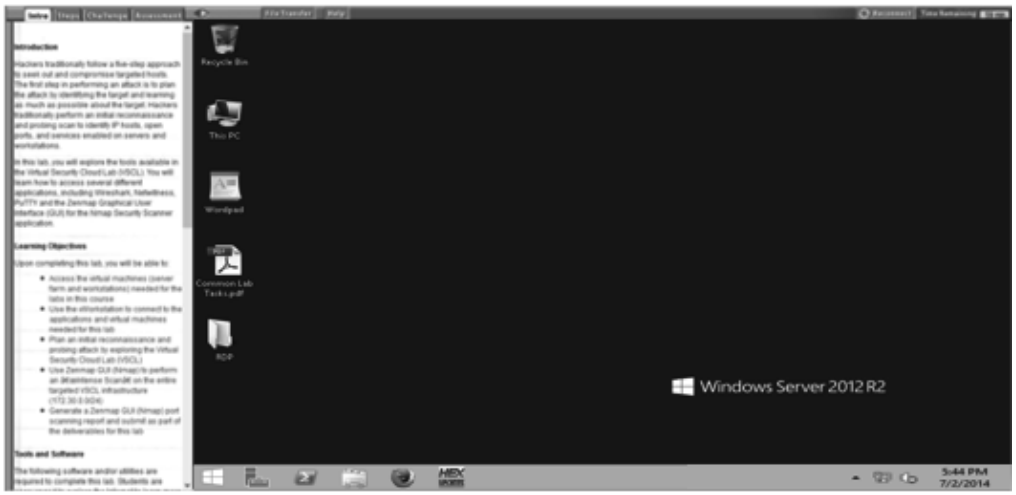


Figure 1 "Student Landing" vWorkstation

2. On your local computer, **create** the **lab deliverable files**.
3. **Review** the **Lab Assessment Worksheet** at the end of this lab. You will find answers to these questions as you proceed through the lab steps.

Part 1: Harden the GRUB Boot Loader

▶Note:
In the next steps, you will apply harden security measures on this server by modifying GRUB, the Grand Unified Bootloader, so that it will boot into the default operating system without displaying the boot loader menu. A boot loader is a program that allows the user or administrator to choose which operating system or kernel to load when the computer starts. GRUB can load a variety of free operating systems, as well as proprietary operating systems with chain-loading. It is important to lock down GRUB with a short delay and a password to avoid tampering with the operating system's boot sequence. Securing the bootloader also provides a layer of security from those who may have physical access to the machine.

1. **Double-click** the **RDP folder** on the vWorkstation desktop to open the folder.
2. **Double-click** the **TargetCentOS01.rdp file** to start a remote desktop connection to that machine.

3. If prompted, **type** the following credentials and **click OK** to open the remote connection.

   - User name: **root** and **press Enter**
   - Password: **toor** and **press Enter**

   The remote GNOME desktop, the graphical user interface (GUI) for the virtual Linux server, opens with the IP address of the remote machine (172.30.0.21) in the title bar at the top of the window.

Figure 2 The GNOME desktop

4. **Double-click** the **Terminal icon** on the GNOME desktop to open the terminal emulator and access the Linux server command line.

5. At the command prompt, **type su –** and **press Enter** to become the root user.

6. When prompted for the password, **type P@ssw0rd!** and **press Enter**.

   The command prompt will change to *[root@centos ~]#*.

7. At the command prompt, **type vi /boot/grub/grub.conf** and **press Enter** to load the grub configuration file into the VI Editor.

   The grub.conf file appears in the VI Editor window.

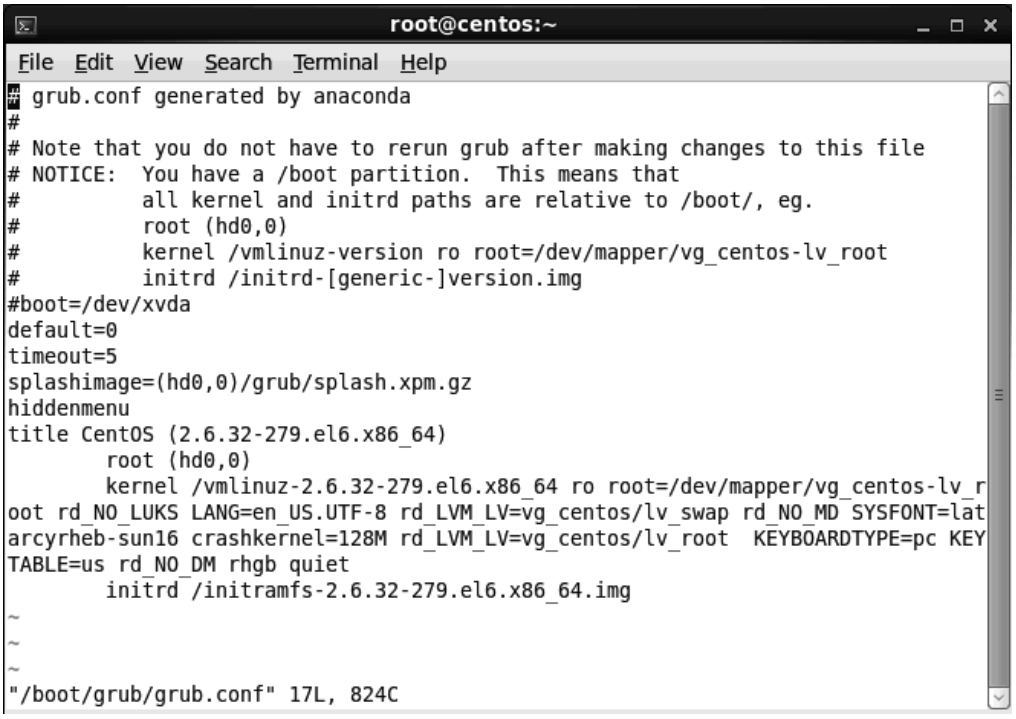


Figure 3 grub.conf within the VI Editor

8. **Hold** the **Shift key** and **press** the **R key** to enter the Replace mode used to edit the file.
9. Use the arrow keys to **locate** the **timeout=5 line** in the editor and **change** the 5 to a **0**.

   This will change the length of the timeout from 5 seconds to zero, which forces grub to skip the edit menu when it loads.
10. **Press** the **Esc key** to exit the Replace mode and **hold** the **Shift key** and **press** the **: key** to return to the command line mode.

    A colon with a solid cursor at the bottom of the window indicates that you are in the command line mode.
11. **Type wq** (write quit) and **press Enter** to save your changes and exit the VI Editor.
12. At the command prompt, **type /sbin/grub** and **press Enter** to open the Grub Console for editing.

    In the Grub Console, the command prompt appears as *grub*>.
13. At the command prompt, **type md5crypt** and **press Enter** to attach a hash string-encrypted password to the grub menu so that it can only be edited by an authorized user.
14. When prompted for a password, **type linuxlab** and **press Enter** to create a password.

    The hash string that appears is the encryption for the password you just created.

15. **Make a screen capture** showing the **newly generated hash string** and **paste** it into the Lab Report file.

16. **Highlight** the hash string and **right-click**, and **select Copy** from the context menu to copy the hash string for use in a later step.

17. At the command prompt, **type quit** and **press Enter** to exit the grub console and return to the root prompt.

18. At the command prompt, **type vi /boot/grub/grub.conf** and **press Enter** to load the grub configuration file into the VI Editor.

    The grub.conf file appears in the VI Editor window.

19. **Press** the **i key** to enter the Insert mode.

20. Use the arrow keys to **locate** the **timeout=0** line in the editor and **press Enter** at the beginning of the next line to start a new line below the timeout=0 line.

21. Use the **up arrow** to move to the **empty line** and **type password --md5**, **press** the **spacebar**, and then **right-click** and **select Paste** from the context menu to paste the hash string you copied in step 16 above.

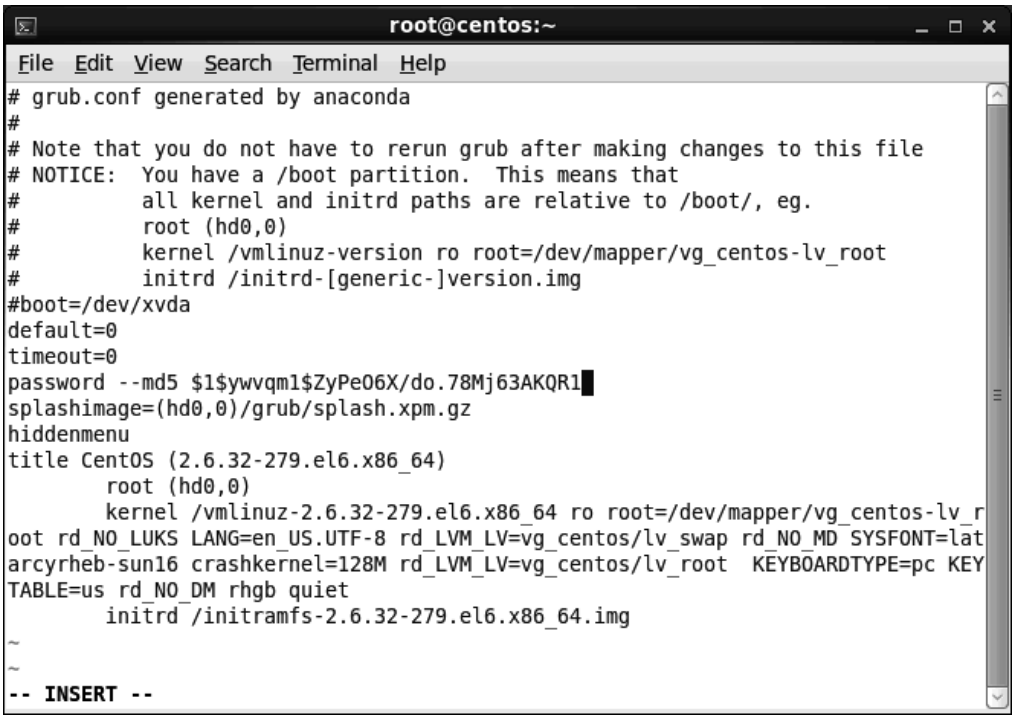


Figure 4 Add an encrypted password to the GRUB

22. **Make a screen capture** showing the **hash string in the VI Editor window** and **paste** it into the Lab Report file.

23. **Press** the **Esc key** to exit the Insert mode and **hold** the **Shift key** and **press** the **: key** to return to the command line mode.

    A colon with a solid cursor at the bottom of the window indicates that you are in the command line mode.

24. **Type wq** (write quit) and **press Enter** to save your changes and exit the VI Editor.

Part 2: Confirm Security-Enhanced Linux is Enabled

▶Note:
In the next steps, you will apply harden security measures on this server by verifying that this CentOS SELinux (Security-Enhanced Linux) server is set to enforcing mode. SELinux is a set of security enhancements built in to the Linux kernel and should be set to enforcing mode by default.

1. At the terminal command prompt, **type cat /etc/selinux/config** and **press Enter** to check the SELinux configuration.

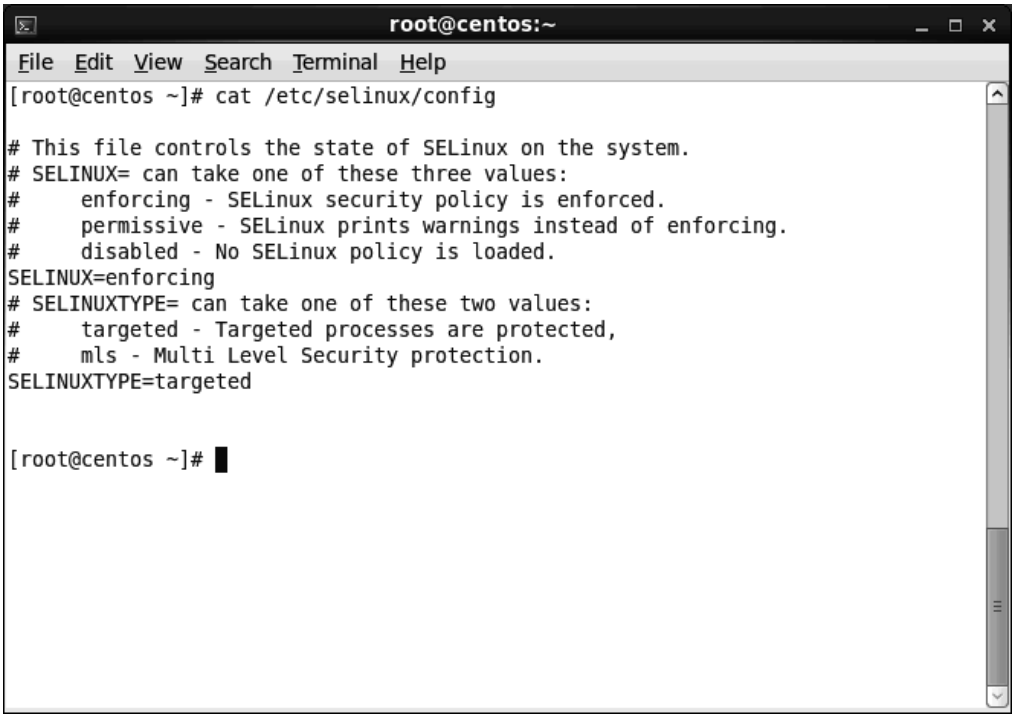


Figure 5 SELinux configuration settings

2. At the command prompt, **type /usr/sbin/sestatus** and **press Enter** to see which mode that SELinux is running.

3. **Make a screen capture** showing the **current mode line** of the SELinux configuration and **paste** it into the Lab Report file.

Part 3: Enable iptables Firewall

▶Note:
In the next steps, you will apply hardened security measures on this server by enabling the internal host-based IP stateful firewall. You will set the firewall to start when it enters runlevels 2 through 5; iptables is the current host-based, Linux IP stateful firewall and routing service that can be enabled in your CentOS Linux Server. It controls incoming and outgoing network connections and either allows, disallows, or forwards requests based on a set of defined rule sets you configure within the firewall application itself.

1. At the command line prompt, **type /sbin/chkconfig --level 2345 iptables on** and **press Enter**.

   The command prompts changes behind the scenes. There will be no visible feedback apart from the reappearance of the command line prompt.

2. At the command line prompt, **type /sbin/service iptables start** and **press Enter** to start the firewall.

   The command prompts changes behind the scenes. There will be no visible feedback apart from the reappearance of the command line prompt.

3. At the command line prompt, **type /sbin/chkconfig iptables --list** and **press Enter** to verify that your changes have been made on the server.

   This command lists the current settings for the iptables firewall and should show that runlevels 2-5 are on, and runlevels 0, 1, and 6 are off.

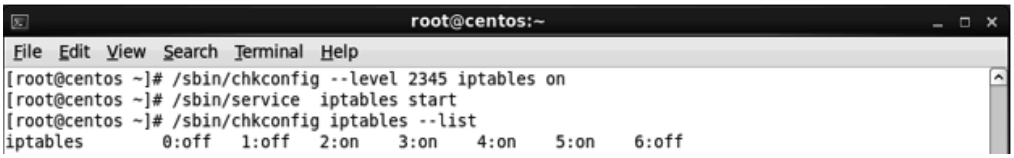


Figure 6 iptables runlevels settings

4. At the command line prompt, **type /sbin/service iptables status** and **press Enter** to view the current iptables configuration.

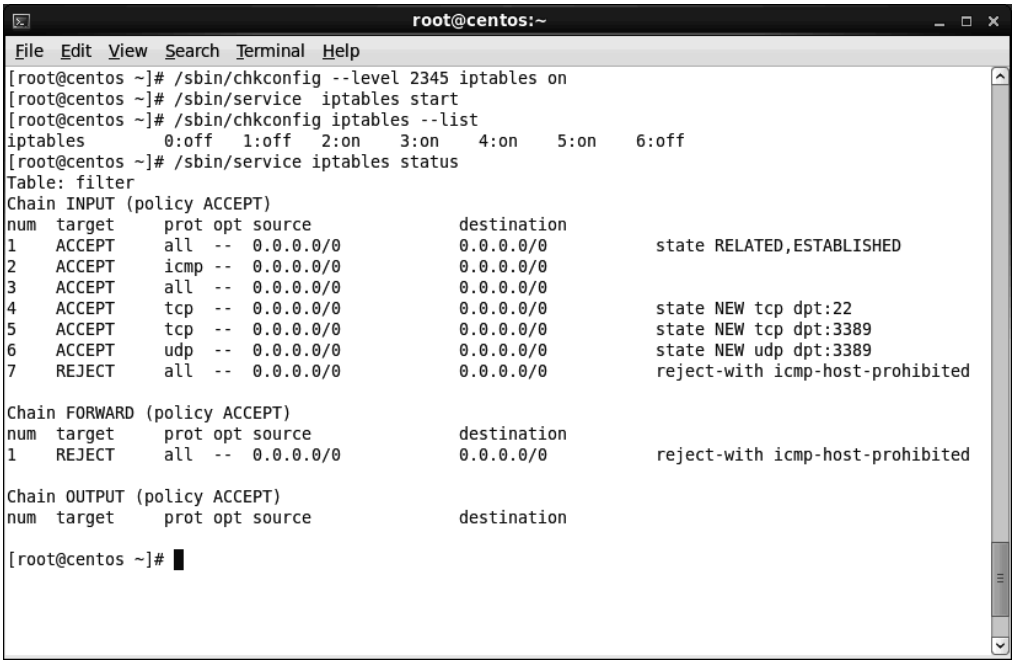


Figure 7 Firewall configuration

5. **Make a screen capture** showing the **iptables status** and **paste** it into the Lab Report file.

Part 4: Enable sudo User

▶Note:
In the next steps, you will apply hardened security measures on this server by allowing the sudo user. Administrators may choose to grant authorized users limited root-level access for a specific purpose. Sudo access also can be used to allow the administrator to audit the actions that authorized users take on the server. Any actions not specifically granted to the sudo user will require the actual root password. Sudo access allows a user to perform actions beyond his or her normal privileges. It is a way to provide these privileges to a user without requiring him to log in as root. A compromised root user account will allow an attacker to compromise an entire Linux server and system. If you do not log in as root user, your IP packets cannot be compromised, and it's not possible for a hacker to conduct a man-in-the-middle attack.

1. At the command line prompt, **type /usr/sbin/visudo** and **press Enter** to edit the sudoers file, the configuration file for the sudo users.

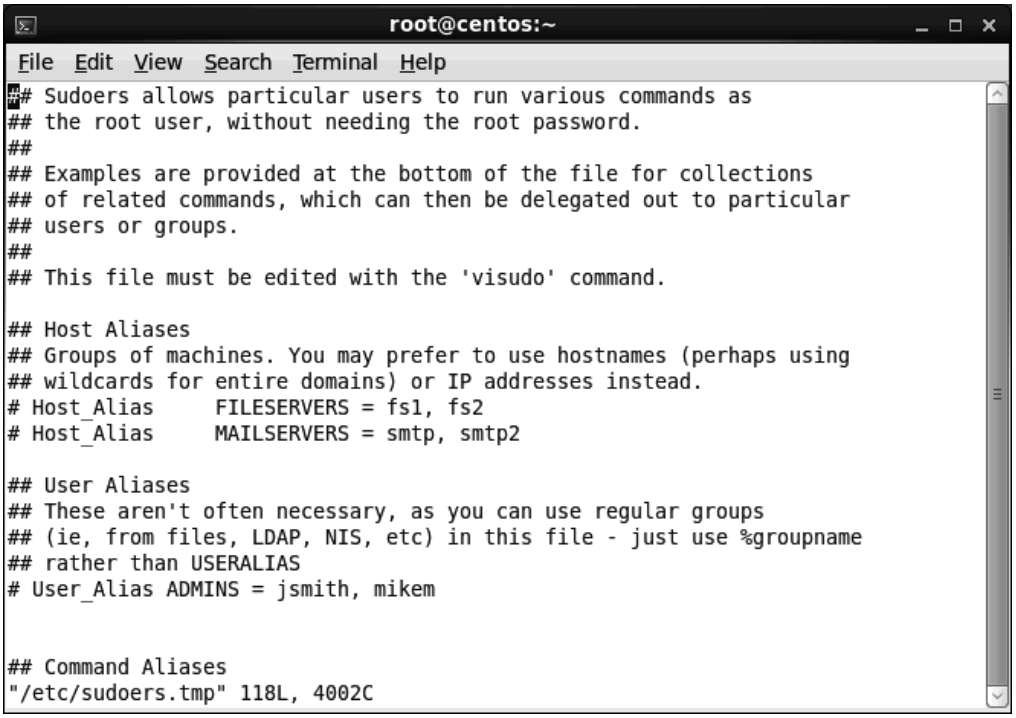


Figure 8 The sudoers file

2. **Press** the **i key** to enter the Insert mode.

3. Use the arrow keys to **locate** the **%wheel ALL = NETWORKING, SOFTWARE, SERVICES, STORAGE, DELEGATING, PROCESSES, LOCATE, DRIVERS line** in the editor and **press Enter** at the beginning of the next line to start a new line.

   The TargetCentOS01 machine is pre-configured to allow anyone in the *wheel* group to have sudo access for each of the commands listed in this step.

4. Use the **up arrow** to move to the **empty line** and **type %web ALL = NETWORKING, SOFTWARE, SERVICES, STORAGE, DELEGATING, PROCESSES, LOCATE, DRIVERS**.

   This step creates a new group called *web* that will have sudo access for each of the commands listed here.

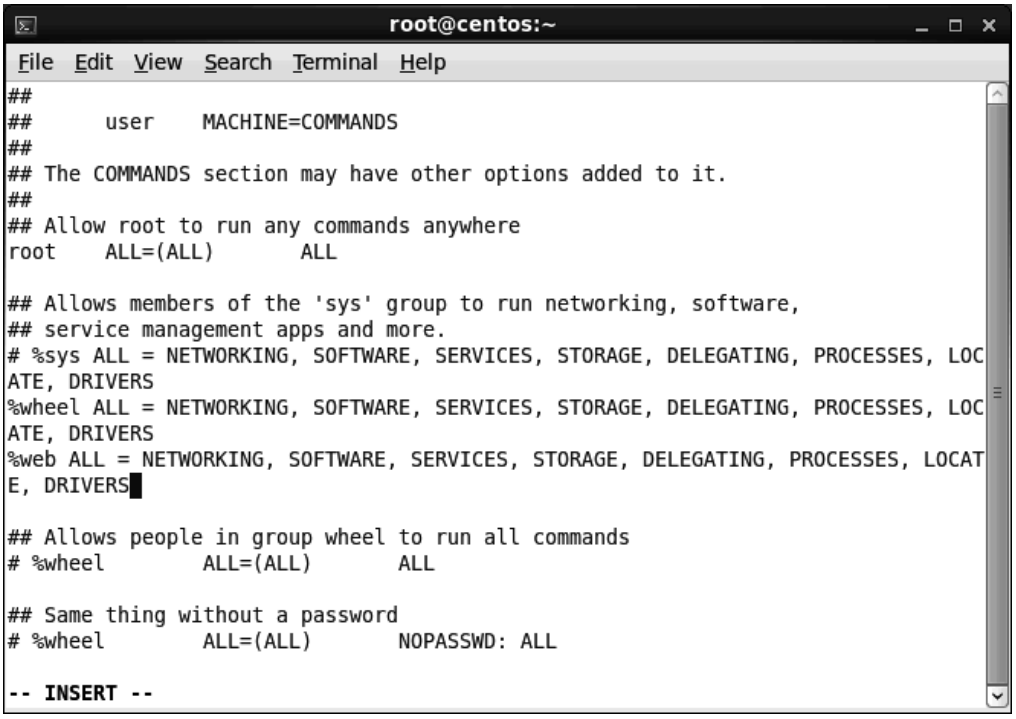


Figure 9 Add the web group

5. **Make a screen capture** showing the **new web group** and **paste** it into the Lab Report file.

6. **Press** the **Esc key** to exit the Insert mode and **hold** the **Shift key** and **press** the **: key** to return to the command line mode.

   A colon with a solid cursor at the bottom of the window indicates that you are in the command line mode.

7. **Type wq** (write quit) and **press Enter** to save your changes and exit the VI Editor.

▶Note:
In the next steps, you will add the user student01 and place the user in the wheel group. Traditionally, this group contains the system administrators.

8. At the command line prompt, **type useradd -G wheel student01** and **press Enter**.

   This creates the student user and places him or her in the wheel group.

9. At the command line prompt, **type passwd student01** and **press Enter**.

10. When prompted for the new password, **type pass=7890** and **press Enter**.

11. **Repeat step 10** when prompted.

Part 5: Extended File Attributes: Set Immutable Permission

▶Note:
In this next steps, you will apply hardened security measures on this server by setting the immutable permission on a temporary file. An immutable designation means the file cannot be manipulated. The file becomes a read-only file that cannot be deleted, moved, or edited, even by someone with root-level access. The immutable permission is an extended file attribute, beyond the usual read/write sort of access. Other extended file attributes include: append only (a), secure deletion (s).

1. At the command line prompt, **type touch /tmp/mytest** and **press Enter** to create a temp file.
2. At the command line prompt, **type chattr +i /tmp/mytest** and **press Enter** to change the file attributes and add the immutable flag (i) to the file permissions.
3. At the command line prompt, **type lsattr /tmp/mytest** and **press Enter** to list the file attributes and verify that the immutable flag has been added to the file permissions.

   The results should include a lowercase i (for example, ---i---) indicating that the file attributes have been changed and the immutable permission has been set.
4. **Make a screen capture** showing the **new file attributes** and **paste** it into the Lab Report file.
5. At the command line prompt, **type rm /tmp/mytest** and **press Enter**.

   This command attempts to remove the file.
6. When prompted, **type yes** and **press Enter**.

   You should see that the operation is not permitted.
7. At the command line prompt, **type mv /tmp/mytest /tmp/file1** and **press Enter**.

   This command attempts to move the file; this operation is not permitted either.
8. At the command line prompt, **type cp /tmp/mytest /tmp/file2** and **press Enter**.

   This command attempts to copy the file. This operation is allowed.

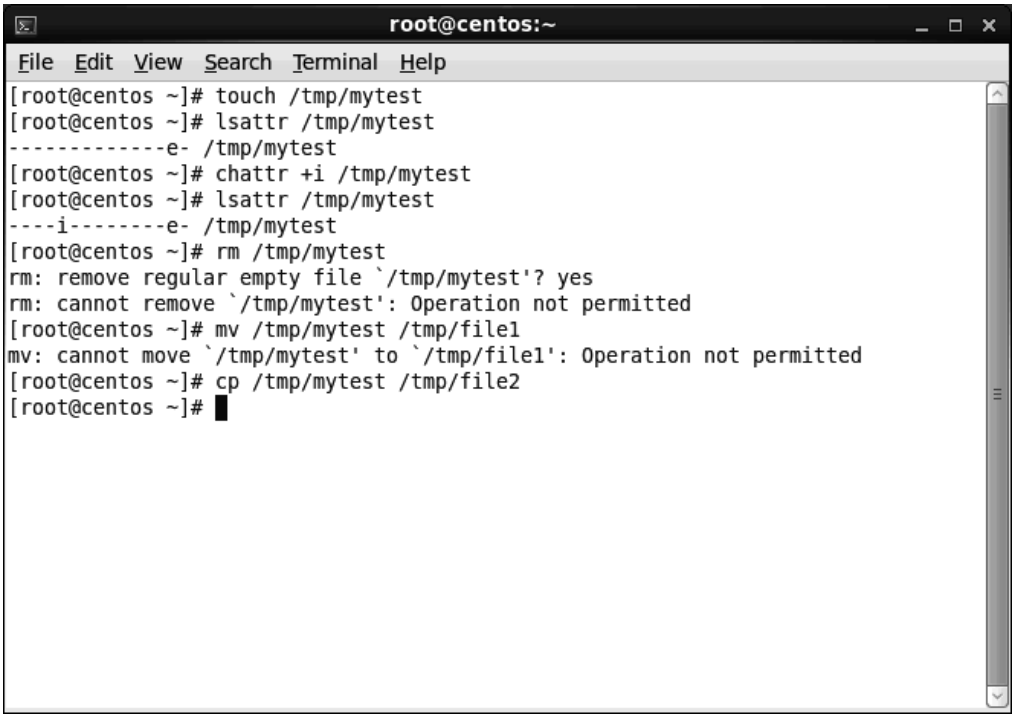


Figure 10 Confirm immutable permissions

9. At the command prompt, **type vi /tmp/mytest** and **press Enter** to open the file in the VI Editor.

10. **Press** the **i key** to enter the Insert mode.

    A warning at the bottom of the screen confirms that the edit operation is not allowed.

11. **Make a screen capture** showing the **warning message** and **paste** it into the Lab Report file.

12. **Press** the **Esc key** to exit the Insert mode and **hold** the **Shift key** and **press** the **: key** to return to the command line mode.

    A colon with a solid cursor at the bottom of the window indicates that you are in the command line mode.

13. **Type q!** (quit without saving) and **press Enter** to exit the VI Editor.

Part 6: Access Control List Permissions

▶Note:
In the next steps, you will apply harden security measures on this server by granting special permissions to allow a user access to the server's log file. You will assign access control list permissions (ACL) to the wheel group. This will be done using the set file access control lists (setfacl) command and the get file access control lists (getfacl) commands. The setfacl command provides an extra layer of security defense by setting permissions for specific users or groups of users regarding access to files on the system. Setfacl helps system administrators define stringent access controls to specific files for ensuring confidentiality. The get file access control lists (getfacl) command displays existing ACLs.

1. At the command prompt, **type getfacl /var/log/messages** and **press Enter** to view the current ACL permissions for the log file.

2. At the command prompt, **type setfacl –m g:wheel:r /var/log/messages** and **press Enter** to add read ACL permissions to the wheel group for the log file.

   There will be no visible feedback apart from the reappearance of the command line prompt.

3. At the command prompt, **type getfacl /var/log/messages** and **press Enter** to get the current ACL permissions for the log file and verify that they were set properly in the previous step.

   The wheel group now has read access to the log file.

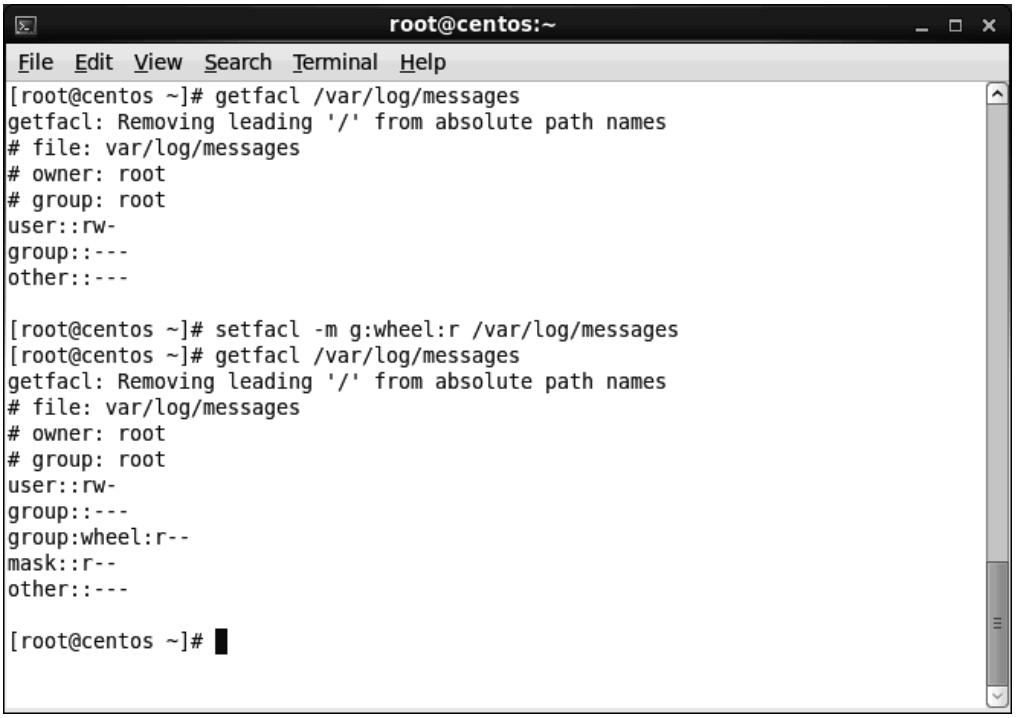


Figure 11 Set ACL permissions on the log file

4. **Make a screen capture** showing the **permissions for the log file** and **paste** it into the Lab Report file.
5. **Close** the **terminal window**.
6. **Close** the **remote Linux connection**.
7. **Close** the **virtual lab**, or proceed with Part 7 to answer the challenge question for this lab.

Part 7: Challenge Question

▶Note:
The following challenge question is provided to allow independent, unguided work, similar to what you will encounter in a real situation. You should aim to improve your skills by getting the correct answer in as few steps as possible. Use screen captures in your lab document where possible to illustrate your answers.

1. Research Linux permissions on the Internet and describe how you would go about deleting the immutable file /tmp/mytest you created in Part 6 of the lab.

   First, remove the immutable permission **chattr -i /tmp/mytest**, then delete the file **rm /tmp/mytest**.

▶Note:
This completes the lab. **Close** the **virtual lab**, if you have not already done so.

Evaluation Criteria and Rubrics

The following are the evaluation criteria for this lab that students must perform:

1. Configure the bootloader with the timeout set to 0 and password credential to mitigate tampering with the GRUB loader and the boot sequence of the server – **[10%]**
2. Enable SELinux on a CentOS Linux Server and set it to enforcing mode – **[10%]**
3. Create a student user account and add it to a user group for managing permissions and applying access controls across the system – **[20%]**
4. Configure user groups with limited sudo access (with password credentials) to log and properly monitor access across the system – **[20%]**
5. Create iptables set to "on" for runlevels 2 and 5 to enable an internal, host-based IP stateful firewall – **[20%]**
6. Set restrictions and permissions for user access to files and system log files – **[20%]**

Lab #2 – Assessment Worksheet

Configuring Basic Security Controls on a CentOS Linux Server

Course Name and Number: _____

Student Name: _____

Instructor Name: _____

Lab Due Date: _____

Overview

In this lab, you secured a Linux server system. You secured the bootloader, enabled iptables firewall, and ran SELinux to help lock down the Linux OS. By securing the bootloader, you prevented access to single-user mode and the GRUB Console during the boot of the system. Enabling iptables and applying firewall rules ensured that only the applications you wanted can reach or reach out from your computer. You also applied access control lists (ACLs) to directories and files within the lab to secure the file and data access and then verified those permissions on the system.

Lab Assessment Questions & Answers

1. What is GRUB and why is it important to lock it down?

   Note introducing Part 1. GRUB, the Grand Unified Bootloader, is a program that allows the user or administrator to choose which operating system or kernel to load when the computer starts. GRUB can load a variety of free operating systems, as well as proprietary operating systems with chain-loading. It is important to lock down GRUB with a short delay and a password to avoid tampering with the operating system's boot sequence. Securing the bootloader also provides a layer of security from those who may have physical access to the machine.

2. Discuss the purpose of granting sudo access. Why is it a good idea not to log in as a root user?

   Note introducing Part 4. Sudo access can also let the administrator audit the actions authorized users take on the server. Any actions not specifically granted to the sudo user will require the actual root password. Sudo access lets a user perform actions beyond his or her normal privileges. It is a way to provide these privileges to a user without requiring him or her to log in as root. A compromised root user account will allow an attacker to compromise an entire Linux server and system. If you do not log in as root user, your IP packets cannot be compromised, and a hacker cannot conduct a man-in-the-middle attack.

3. If a file is set with the immutable flag, what security controls does this provide for the file?

   Note introducing Part 5. An immutable designation means the file cannot be manipulated. The file becomes a read-only file that cannot be deleted, moved, or edited; even by someone with root level access. The immutable permission is an extended file attribute, beyond the usual read/write sort of access.

4. Besides immutable, what are some of the other extended file attributes?

   Note introducing Part 5. Other extended file attributes include: append only (a); secure deletion (s).

5. What is the difference between access control list permissions and sudo?

   Note introducing Part 4. Sudo access allows a user to perform actions beyond his or her normal privileges assigned by the ACLs.

6. What is iptables and how does this help harden the CentOS Linux Server?

   Note introducing Part 3. Iptables is the current host-based, Linux IP stateful firewall and routing service that can be enabled in your CentOS Linux Server. It controls incoming and outgoing network connections and either allows, disallows, or forwards requests based on a set of defined rule sets you configure within the firewall application itself.

7. Why is it important to configure and enable iptables on your CentOS Linux Server?

   Introduction. Iptables is the built-in firewall available within the CentOS Linux system. It will help lock down services on a Linux system to only those who require network access and deny external connections to any other unnecessary port or service.

8. What is the difference between setfacl and getfacl? How can setfacl help achieve security hardening?

   Note introducing Part 6. The setfacl command provides an extra layer of security defense by setting permissions for specific users or groups of users regarding access to files on the system. Setfacl helps system administrators define stringent access controls for specific files to ensure confidentiality. The get file access control lists (getfacl) command displays existing ACLs.

Lab #3 Hardening Security with User Account Management and Security Controls

Introduction

This lab is an extension of the previous labs. Computer security is a series of disparate systems that will each play a key role in the protection of resources and information. However, just about every security policy begins with and is centrally focused on the company's password policy. Every auditor walking in to gauge the worth of the company's accounting systems will ask to see the password policy and the logs for change control. In most cases, the passwords to the system are the keys to the vault.

Any effective password policy will have several elements. The passwords will expire regularly; they will have a certain complexity requirement for length and special characters, and will also have a minimum age requirement. In addition, every organization has "guest users," be they auditors, contractors, temps, or other types of transient users on the system. Having a password system that can deal with these varieties of conditions requires intelligent design and well-trained and capable system administrators.

In this lab, you will harden user accounts on a Linux system with a secure password policy definition. This definition will include the use of user groups to better manage large numbers of users. You also will create temporary user accounts and apply automatic account and password deletion after 90 days.

This lab has six parts, which should be completed in the order specified.

1. In the first part of the lab, you will set password controls on a Linux system.
2. In the second part of the lab, you will create several user accounts on the system and change the password properties for one of those accounts.
3. In the third part of the lab, you will create two new security groups on the system and add the new user accounts to their corresponding groups.
4. In the fourth part of the lab, you will create temporary user accounts that will expire in a set period of time.
5. In the fifth part of the lab, you will edit the .pam file to restrict the use of the su command.
6. Finally, if assigned by your instructor, you will explore the virtual environment on your own to answer a of challenge question that allows you to use the skills you learned in the lab to conduct independent, unguided work, similar to what you will encounter in a real-world situation.

Learning Objectives

Upon completing this lab, you will be able to perform the following:

- Configure a password policy by editing the /etc/login.defs file and implementing stringent password security measures on a CentOS Linux Server
- Enforce a password change every 60 days showing a warning 14 days prior to the password's expiration across the system for all users
- Configure a minimum password length of eight characters with stringent complexity requirements
- Create users and groups with the proper permissions and restrictions to enforce role-based access controls
- Create a temporary user account that expires in 90 days to enforce the proper principle of least privilege with contractors and temporary workers/consultants

Tools and Software

The following software and/or utilities are required to complete this lab. Students are encouraged to explore the Internet to learn more about the products and tools used in this lab.

- vi Editor

Deliverables

Upon completion of this lab, you are required to provide the following deliverables to your instructor:

1. Lab Report file including screen captures of the following steps: Part 1, Step 9; Part 3, Step 11; Part 4, Step 13; Part 5, Step 6;
2. Lab Assessments file;
3. Optional: Challenge Questions file, if assigned by your instructor.

Hands-On Steps

> **▶Note:**
> This lab contains detailed lab procedures, which you should follow as written. Frequently performed tasks are explained in the Common Lab Tasks document on the vWorkstation desktop. You should review these tasks *before* starting the lab.

1. From the vWorkstation desktop, **open** the **Common Lab Tasks file**.

   If you desire, use the File Transfer button to transfer the file to your local computer and print a copy for your reference.

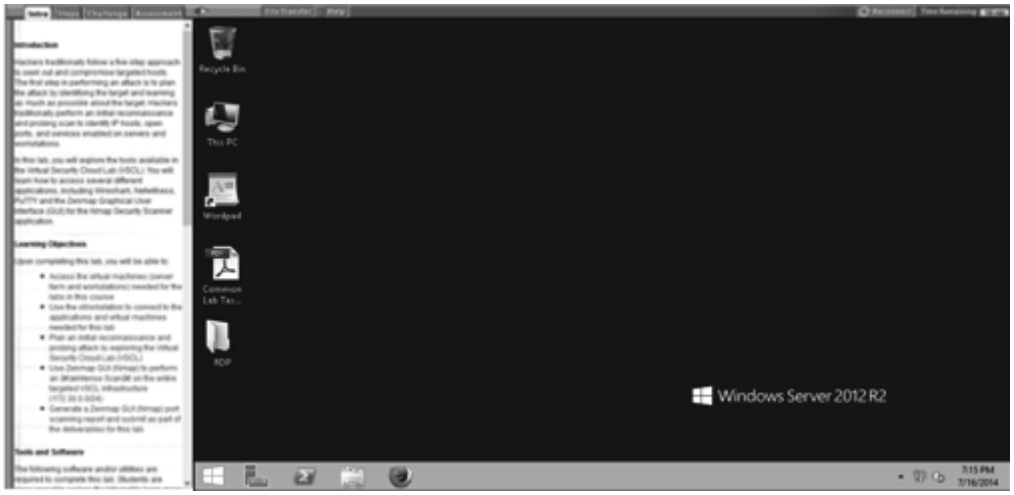


Figure 1 "Student Landing" vWorkstation

2. On your local computer, **create** the **lab deliverable files**.
3. **Review** the **Lab Assessment Worksheet** at the end of this lab. You will find answers to these questions as you proceed through the lab steps.

Part 1: Establish System Password Controls

> **▶Note:**
> In the next steps, you will apply harden security measures on this server by configuring stringent passwords according to a policy definition. You will edit the login definitions (login.defs) file in the vi Editor.

1. **Double-click** the **RDP folder** on the vWorkstation desktop to open the folder.
2. **Double-click** the **TargetCentOS.rdp file** to open a remote connection to the Linux server.

   The remote GNOME desktop, the graphical user interface (GUI) for the virtual Linux server, opens with the IP address of the remote machine (172.30.0.21) in the title bar at the top of the window.

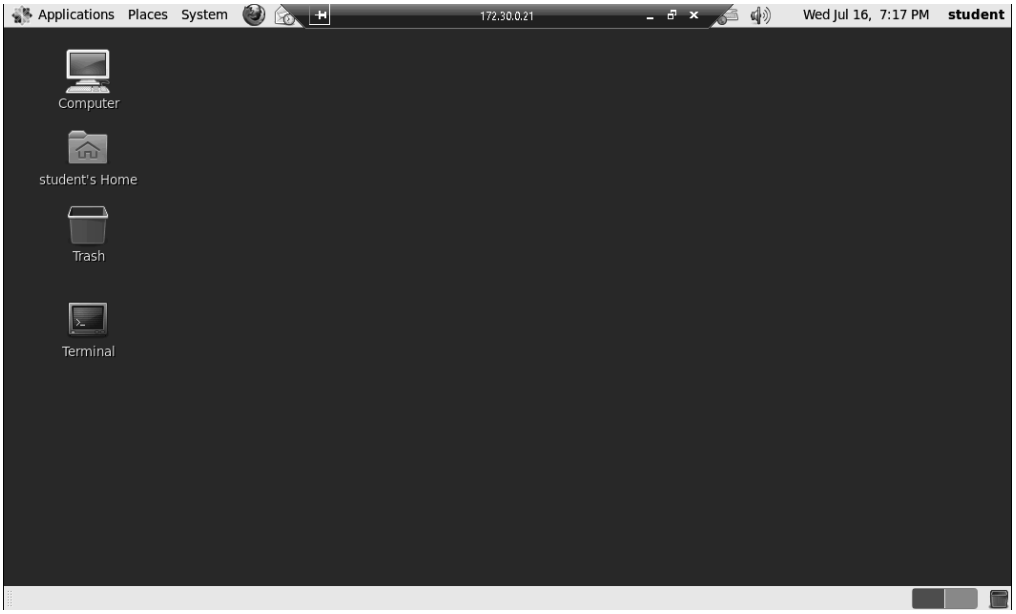


Figure 2 The GNOME desktop

3. **Double-click** the **Terminal icon** on the GNOME desktop to open the terminal emulator and access the Linux server command line.

4. At the command prompt, **type su -c 'vi /etc/login.defs'** and **press Enter** to load the grub configuration file into the vi Editor.

5. When prompted, **type P@ssw0rd!**, the root password, and **press Enter** to open the configuration file.

   The login.defs file appears in the vi Editor window. The login.defs file is used to define the configuration associated with logins into the local Linux system.

▶Note:
You are required to enter a mixed-case password. If you are not using the Citrix Receiver to access this lab, please use the CAPS LOCK button or the On-Screen Keyboard to input the password.

6. **Press** the **i key** to enter the Insert mode.

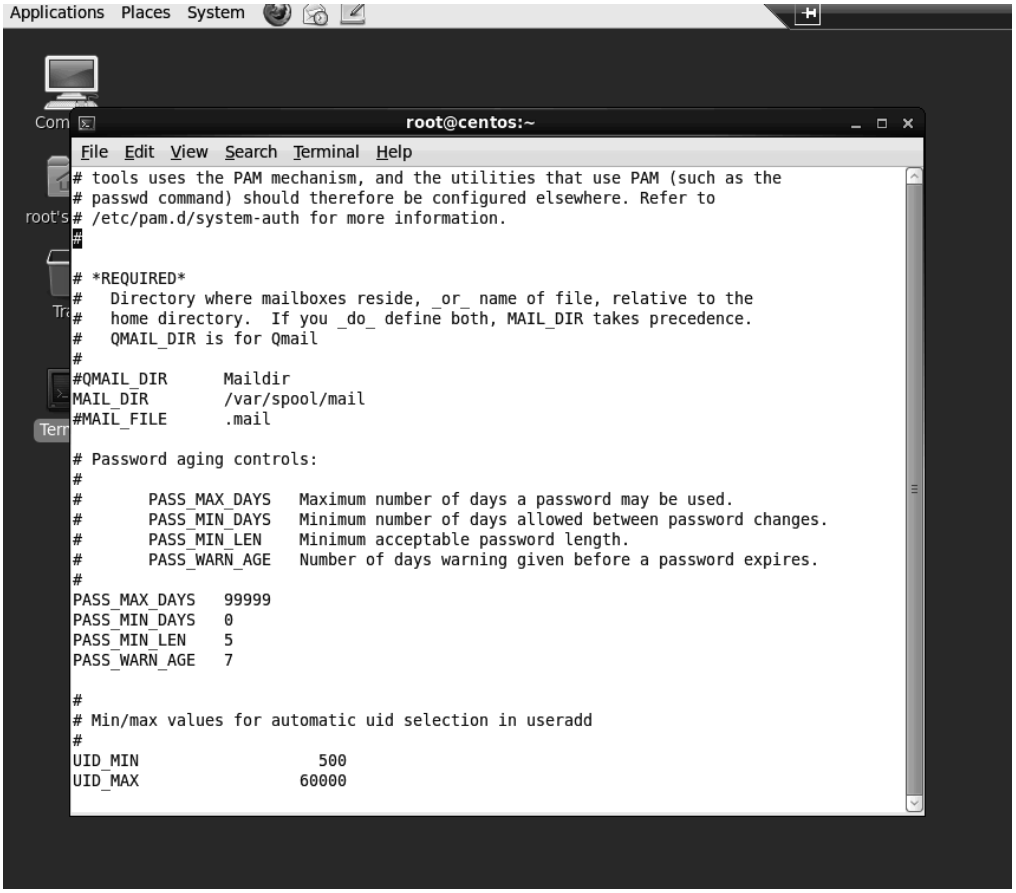


Figure 3 login.defs within the vi Editor

7. Use the arrow keys to **locate** the **Password aging controls** section of the file.

▶Note:

Changes to the Password aging controls section of the login.defs file affect the requirements for user account passwords, including the length of the password and the number of days before a password expires. Requiring users to change passwords on a scheduled basis will, at least, keep hackers guessing and force them to work harder to crack passwords all over again each time they are changed. This is time-consuming and off-putting. If your passwords are difficult to guess and change regularly, you are already well ahead of the skills of many rudimentary hackers.

The section includes a number of password settings. Changes to any of these settings will not affect existing accounts.

- PASS_MAX_DAYS is the maximum number of days a password can be used before a change of password is forced.
- PASS_MIN_DAYS is the minimum number of days a password must be set on an account before it can be changed again. This is to prevent users from trying to revert back to the original password soon after being forced to change.
- PASS_MIN_LEN is the minimum number of characters the password must contain.
- PASS_WARN_AGE is the number of days a warning is sent to an account before the password expires.

8. **Edit** the **password aging controls section** to match the following definition:

    - PASS_MAX_DAYS **60**
    - PASS_MIN_DAYS **0**
    - PASS_MIN_LEN **8**
    - PASS_WARN_AGE **14**

9. **Make a screen capture** showing **your changes in the vi Editor window** and **paste** it into the Lab Report File.

10. **Press** the **Esc key** to exit the Insert mode.

11. **Type :wq!** and **press Enter** to save your changes and exit the vi Editor.

Part 2: Create User Accounts

▶Note:
In the next steps, you will harden security measures on this server by creating several new users accounts using the useradd command and set an initial password for one of the accounts, then require that password to be changed at the first login attempt.

1. At the command prompt, **type su -c '/usr/sbin/useradd dbadmin1'** and **press Enter** to create a new database administrator user account (dbadmin1).

2. When prompted, **type P@ssw0rd!**, the root password, and **press Enter** to create the new account.

▶Note:
You are required to enter a mixed-case password. If you are not using the Citrix Receiver to access this lab, please use the CAPS LOCK button or the On-Screen Keyboard to input the password.

3. **Repeat steps 1-2** to add the following additional users:

    - **dbadmin2**
    - **webadmin1**
    - **webadmin2**

Figure 4 Create new user accounts

4. At the command prompt, **type su -c 'passwd dbadmin1'** and **press Enter** to set a password for the dbadmin1 user account you just created.

5. When prompted, **type P@ssw0rd!**, the root password, and **press Enter** to set the password for the new account.

▶Note:
You are required to enter a mixed-case password. If you are not using the Citrix Receiver to access this lab, please use the CAPS LOCK button or the On-Screen Keyboard to input the password.

6. When prompted for the new password for this account, **type harden** and **press Enter**.

   The system will display a warning indicating that the password is too simple, and that it is based on a dictionary word. However, users with root access (as you have assumed with the su command) will be able to set the password after seeing the warnings.

7. When prompted to retype the password for this account, **type harden** and **press Enter**.

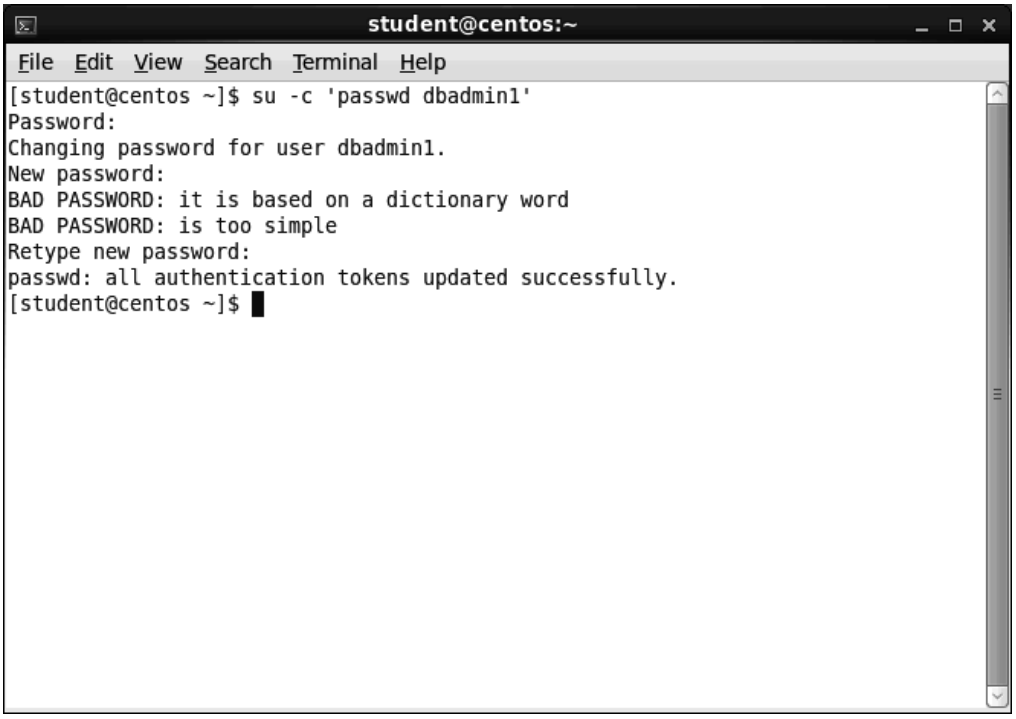


Figure 5 Set a user account password

8. At the command prompt, **type su -c 'chage -d 0 dbadmin1'** and **press Enter** to force the password you just set to change at the next login attempt.

   The command *chage* stands for *change aging*, and is not a misspelling of the word *change*.

9. When prompted, **type P@ssw0rd!**, the root password, and **press Enter** to change the aging of the password.

▶Note:
You are required to enter a mixed-case password. If you are not using the Citrix Receiver to access this lab, please use the CAPS LOCK button or the On-Screen Keyboard to input the password.

Part 3: Manage Security Groups

▶Note:
In the next steps, you will harden security measures on this server by creating two new security groups. You will add the new users to those groups and verify user group membership. The intelligent design and deployment of security groups greatly eases security management, change control, and access tightening. Putting users into groups and then applying the group to a resource is the best way to manage that resource. Changes to the control only need to be made to the group property, instead of possibly dozens if not hundreds of individual users.

1. At the command prompt, **type su -c '/usr/sbin/groupadd dba'** and **press Enter** to add a new group called dba (database administrators).
2. When prompted, **type P@ssw0rd!**, the root password, and **press Enter** to add the new group.

▶Note:
You are required to enter a mixed-case password. If you are not using the Citrix Receiver to access this lab, please use the CAPS LOCK button or the On-Screen Keyboard to input the password.

3. **Repeat steps 1-2** to add a new group called **web**.

Figure 6 Create new group accounts

4. At the command prompt, **type su -c '/usr/sbin/usermod -g dba dbadmin1'** and **press Enter** to add the dbadmin1 user account to the new dba group.
5. When prompted, **type P@ssw0rd!**, the root password, and **press Enter** to add the user to the group.

▶Note:
You are required to enter a mixed-case password. If you are not using the Citrix Receiver to access this lab, please use the CAPS LOCK button or the On-Screen Keyboard to input the password.

6. **Repeat steps 4-5** to add the **dbadmin2** user account to the **dba** group.

7. At the command prompt, **type su -c '/usr/sbin/usermod -g web webadmin1'** and **press Enter** to add the webadmin1 user account to the new web group.

8. When prompted, **type P@ssw0rd!**, the root password, and **press Enter** to add the user to the web group.

▶Note:
You are required to enter a mixed-case password. If you are not using the Citrix Receiver to access this lab, please use the CAPS LOCK button or the On-Screen Keyboard to input the password.

9. **Repeat steps 7-8** to add the **webadmin2** user account to the **web** group.

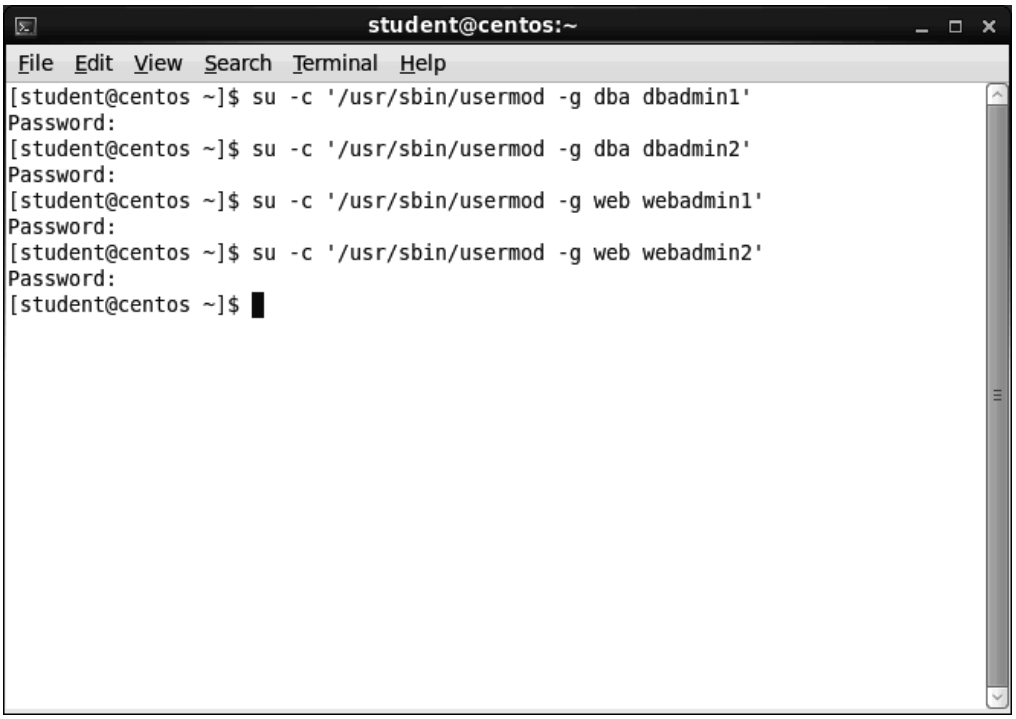


Figure 7 Add user accounts to group accounts

10. At the command prompt, **type groups dbadmin1** and **press Enter** to display all of the groups to which the dbadmin1 user is a member.

    So far in this lab, you have added the dbadmin1 user only to the dba group. However, this command illustrates how either the user or the administrator can easily and quickly determine the groups to which a user is assigned.

Figure 8 Output from the groups command

11. **Make a screen capture** showing the **output from the groups command** and **paste** it into the Lab Report file.

Part 4: Manage Temporary User Accounts

▶Note:
In the next steps, you will apply harden security measures on this server by creating temporary user accounts that will automatically expire in 90 days. This type of action is common in a business that frequently hires contractors or others that will need temporary access to their network.

1. At the terminal command prompt, **type su -c '/usr/sbin/useradd jtemp'** and **press Enter** to create a new database administrator user account (jtemp).

2. When prompted, **type P@ssw0rd!**, the root password, and **press Enter** to create a new account.

▶Note:
You are required to enter a mixed-case password. If you are not using the Citrix Receiver to access this lab, please use the CAPS LOCK button or the On-Screen Keyboard to input the password.

3. At the command prompt, **type su -c 'passwd jtemp'** and **press Enter** to set a password for the jtemp user account you just created.

4. When prompted, **type P@ssw0rd!**, the root password, and **press Enter** to set a password.

▶Note:
You are required to enter a mixed-case password. If you are not using the Citrix Receiver to access this lab, please use the CAPS LOCK button or the On-Screen Keyboard to input the password.

5. When prompted for the new password, **type tempuser!** and **press Enter**.

   The system will display a warning indicating that the password is a dictionary, but users with root access, as you have in this lab, will be able to set the password anyway.

6. When prompted, **type tempuser!** and **press Enter** to confirm the new password.

7. At the command prompt, **type su -c 'chage -d 0 jtemp'** and **press Enter** to force the jtemp user to change the password you just set at the next login attempt.

8. When prompted, **type P@ssw0rd!**, the root password, and **press Enter** to force a password change.

▶Note:
You are required to enter a mixed-case password. If you are not using the Citrix Receiver to access this lab, please use the CAPS LOCK button or the On-Screen Keyboard to input the password.

9. At the command prompt, **type su -c 'chage -E *date* jtemp'** and **press Enter** to force the jtemp user to change the password you just set on the required date.

   For this command, the ***date*** should be entered in the format of YYYY-MM-DD. For this lab, replace the ***date*** in the command line, with an actual date 90 days from the date you perform this hands-on activity.

10. When prompted, **type P@ssw0rd!**, the root password, and **press Enter** to force a password change for the jtemp user.

▶Note:
You are required to enter a mixed-case password. If you are not using the Citrix Receiver to access this lab, please use the CAPS LOCK button or the On-Screen Keyboard to input the password.

11. At the command prompt, **type su -c 'chage --list jtemp'** and **press Enter** to review the password settings for the jtemp user account.

12. When prompted, **type P@ssw0rd!**, the root password, and **press Enter** to review the password settings.

▶Note:
You are required to enter a mixed-case password. If you are not using the Citrix Receiver to access this lab, please use the CAPS LOCK button or the On-Screen Keyboard to input the password.

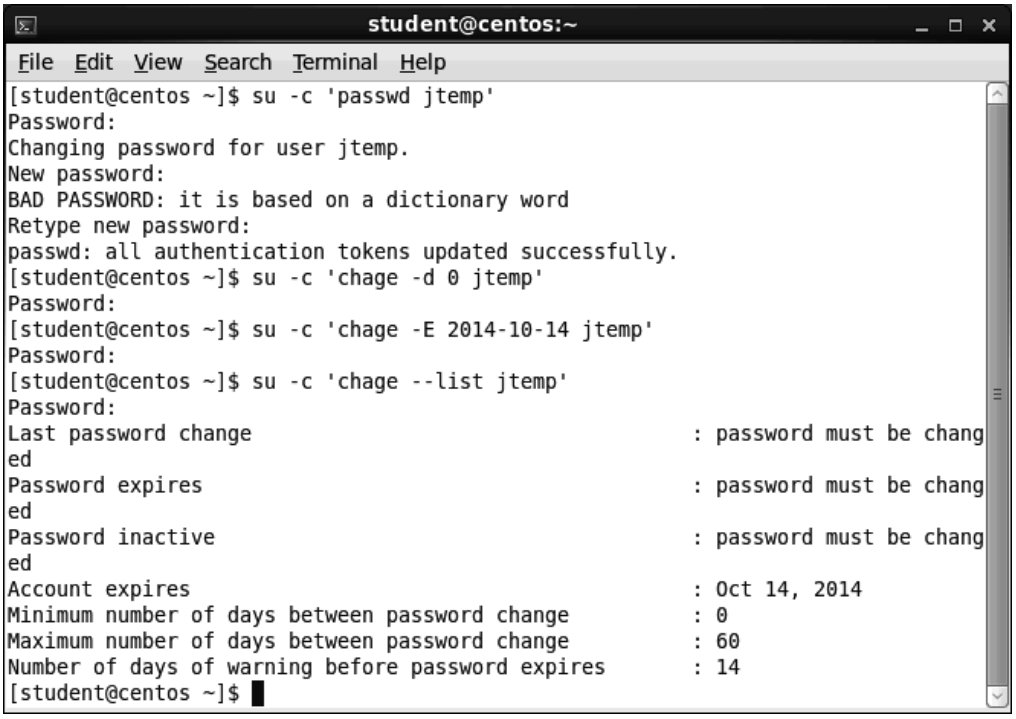


Figure 9 Output from the jtemp user account configuration

13. **Make a screen capture** showing the **output of the –list command** and **paste** it into the Lab Report file.

Part 5: Restrict Access

▶Note:
In the next steps, you will harden security measures on this server by restricting the use of the su command which grants the user root level access. You will edit the pam.d file to restrict the wheel group from using the su command.

1. At the command line prompt, **type su -c 'vi /etc/pam.d/su'** and **press Enter** to edit the access for the su command in the pluggable authentication module file.

2. When prompted, **type P@ssw0rd!**, the root password, and **press Enter** to open the pam.d file opens in the vi Editor.

▶Note:
You are required to enter a mixed-case password. If you are not using the Citrix Receiver to access this lab, please use the CAPS LOCK button or the On-Screen Keyboard to input the password.

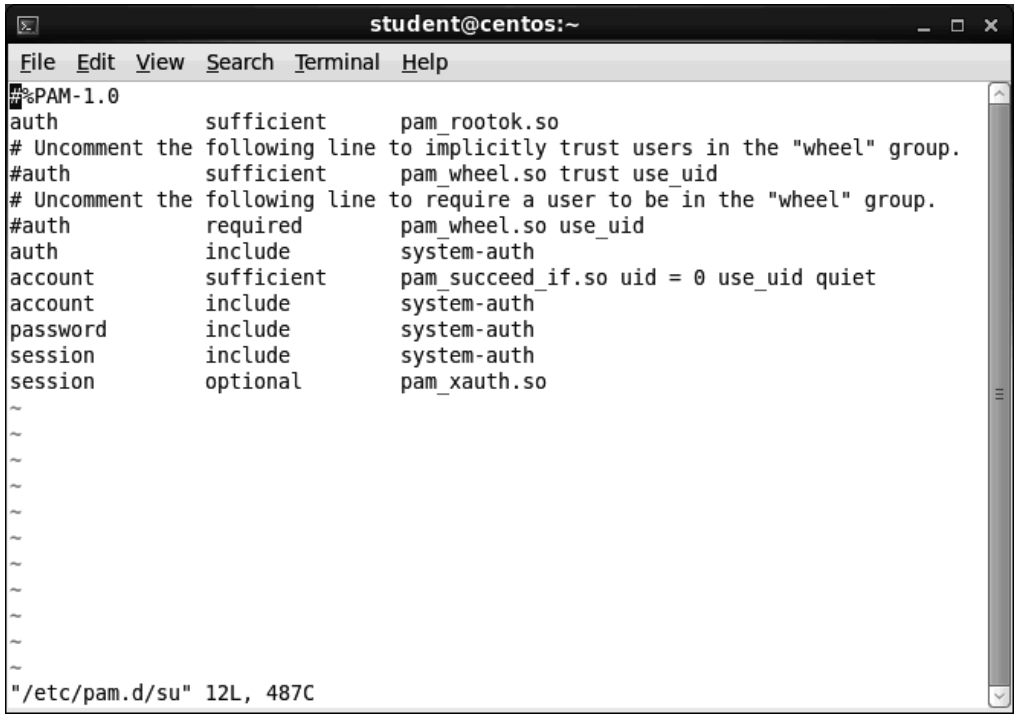


Figure 10 The pam.d file

3. **Press** the **i key** to enter the Insert mode.

4. Use the arrow keys to **locate** the **#auth required pam_wheel.so use_uid line** in the editor.

5. **Replace** the **hash tag (#)** at the beginning of the line with an **x** so that the entire line now reads *xauth required pam_wheel.so use_uid*.

   This action cancels the statements and removes the wheel group from those authorized to use the su command.

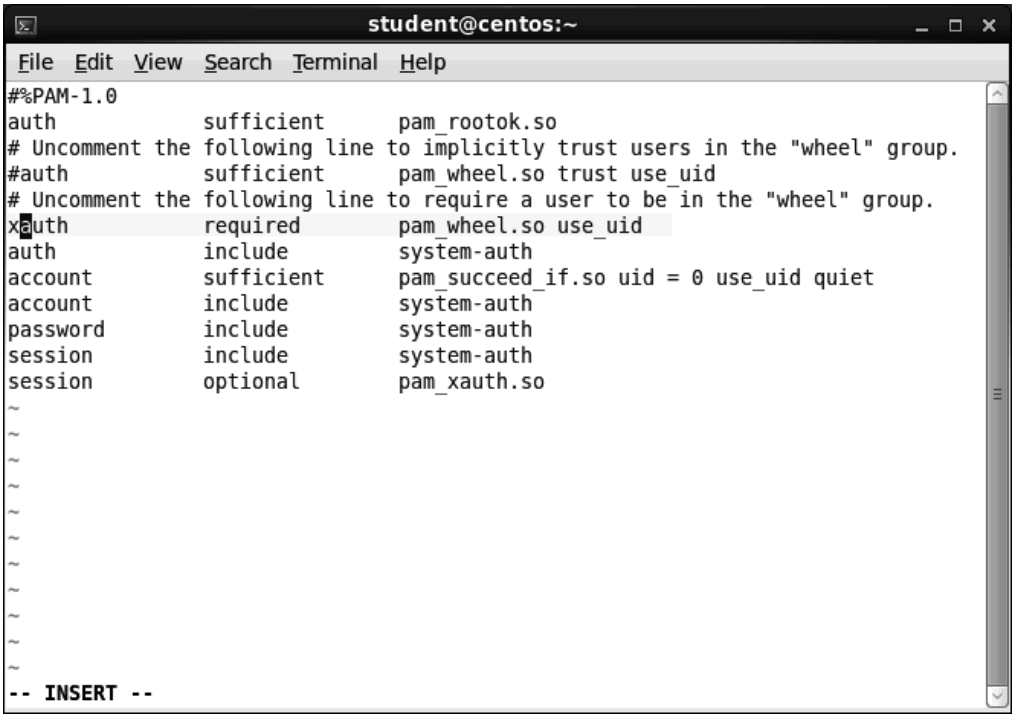


Figure 11 Edit the su command

6. **Make a screen capture** showing the **edits from step 5** and **paste** it into the Lab Report file.
7. **Press** the **Esc key** to exit the Insert mode and **type :wq!** and **press Enter** to save your changes and exit the pluggable authentication module file.
8. At the prompt, **type exit** and **press Enter** to close the terminal window.
9. **Close** the **remote Linux connection**.
10. **Close** the **virtual lab**, or proceed with Part 6 to answer the challenge question for this lab.

Part 6: Challenge Question

▶Note:
The following challenge question is provided to allow independent, unguided work, similar to what you will encounter in a real situation. You should aim to improve your skills by getting the correct answer in as few steps as possible. Use screen captures in your lab document where possible to illustrate your answers.

1. You are the SysAdmin for a local company. You have been instructed to create access to the network for an outside auditing agency who will be coming on-site to perform a financial audit. The audit will last for eight weeks, and the lead auditor is to be given user creation rights to track the use of temps that he is bringing on-site to perform some of the auditing tasks. Your boss is understandably concerned about someone outside the IT group having user admin rights. Given the set of hardening rules you worked with in this lab, describe the policy you would recommend to best meet the needs of the auditors and ease your boss' concerns. For additional consideration, investigate and explain any further reasonable steps you would consider to safeguard data and administer this request.

   (Answers will be unique to each student, but should include some form of the following.)
   The lead auditor is given two accounts, one would be his work account, and the second would be an account relegated to user admin only. The lead auditor would have to su to the user account to administer any of the new accounts he desires, and then log out to his main account do any other work.

   The auditor's accounts and the other temp accounts would be set to expire in eight weeks, and new users would have to immediately change their passwords upon first login. No minimum password days would be needed, as these users would not be on-site long enough to go through a password change cycle. Maximum password days is set at eight weeks, and the warning is set to 0 days to turn it off. Passwords must be a minimum of 8 characters in length.

   Further steps to consider not covered by this lab: Depending on the environment and the need for the temporary auditors' access, create a DMZ and allow the temporary auditors access to the DMZ, but not the internal network. Very often, all that many people need is communication capability in the form of Internet access. A DMZ provides that. In the absence of a DMZ, set time controls on the temp accounts to be valid only during work hours. Do not allow their accounts to be used when the lead auditor is not present or is not sanctioning work. In all of these instances, I would set up logging on all of the accounts and set ACLs to prevent access to any areas that the temps in particular should not be allowed. Auditors often request, and are granted, unrestricted access, but you must clear that with your supervisor before providing it.

▶Note:
This completes the lab. **Close** the **virtual lab**, if you have not already done so.

Evaluation Criteria and Rubrics

The following are the evaluation criteria and rubrics that the students must perform:

1. Configure a password policy by editing the /etc/login.defs file and implementing stringent password security measures on a CentOS Linux Server – [**20%**]
2. Enforce a password change every 60 days showing a warning 14 days prior to the password's expiration across the system for all users – [**20%**]
3. Configure a minimum password length of eight characters with stringent complexity requirements – [**20%**]
4. Create users and groups with the proper permissions and restrictions to enforce role-based access controls – [**20%**]
5. Create a temporary user account that expires in 90 days to enforce the proper principle of least privilege with contractors and temporary workers/consultants – [**20%**]

Lab #3 – Assessment Worksheet

Hardening Security with User Account Management and Security Controls

Course Name and Number: _____

Student Name: _____

Instructor Name: _____

Lab Due Date: _____

Overview

In this lab, you hardened user accounts on a Linux system with a secure password policy definition. This definition included the use of user groups to better manage large numbers of users. You also created temporary user accounts and applied automatic account and password deletion after 90 days.

Lab Assessment Questions & Answers

1. What is the significance of creating groups and adding users to groups? Explain.

   Note introducing Part 3. The intelligent design and deployment of security groups greatly eases security management, change control, and access tightening. Putting users into groups and then applying the group to a resource is the best way to manage that resource. Changes to the control need to be made only to the group property, instead of possibly dozens, if not hundreds, of individual users.

2. Given a scenario where there are five database administrators who may periodically need access to a given system, discuss a concept to better manage these administrators' access permissions.

   Part 3, Step1. Create a group and add the DBAs to the group. Then give the necessary permissions to the group.

3. The new Web administrator's account (webadmin1) has been set up and a password provided to the user. What is the command to force the user to change the password upon first login?

   Part 2, Step 8. Use the command **su -c 'chage –d 0 webadmin1'**

4. How can the use of the su command be restricted?

   Note introducing Part 5. Edit the pam.d file to restrict users or groups from using the su command.

5. What is the purpose of the login.defs file? Explain the contents and configuration options.

   Part 1 Step 5. The login.defs file is used to define the configuration associated with logins into the local Linux system.

6. What is the PASS_MIN_DAYS setting? Why would it be a good idea to specify a PASS_MIN_DAYS setting?

   Note following Part 1, Step 7. It shows the minimum number of days a password must be set on an account before it can be changed again. This is to prevent users from trying to revert back to the original password soon after being forced to change.

7. Will changes to the PASS_MAX_DAYS, PASS_MIN_DAYS, and PASS_WARN_AGE commands in /etc/login.defs settings affect existing accounts?

   Note following Part 1, Step 7. Changes to any of these settings will not affect existing accounts.

8. Describe the password and account settings you would configure if you were told that a few contractors needed accounts on the Linux system for the next 14 days.

   Part 4. Create temporary accounts that expire in 14 days. Possibly, edit the pam.d file to restrict the su command.

Lab #4 Applying Hardened Linux Filesystem Security Controls

Introduction

Server hardening is the process of securing a system by reducing its surface of vulnerability. It is an important task, especially if you realize that the default configuration of most operating systems is not designed with security as the primary focus. Instead, default setups focus more on usability, communications, and functionality. Protection is provided in various layers and often referred to as defense in depth. The idea behind the defense in depth approach is to defend a system against any particular attack using several independent methods. Defense in depth measures should not only prevent security breaches, but also buy an organization time to detect and respond to an attack, thereby reducing and mitigating the consequences of a breach.

This lab, an extension of the previous labs, incorporates security hardening for filesystems and user access to mounted filesystems. In this lab, you will mount a filesystem that does not have execute permissions on the CentOS Linux Server. You also will mount a remote filesystem and set quotas for users of mounted filesystems.

This lab has three parts, which should be completed in the order specified. There is no challenge question for this lab.

1. In the first part of the lab, you will mount a filesystem, apply permissions, test it, and report your findings.
2. In the second part of the lab, you will set user account quotas on filesystem partitions and report your findings.
3. In this part of the lab, you will test your quota configuration and report your findings.

Learning Objectives

Upon completing this lab, you will be able to:

- Mount a filesystem without execute permissions, so you can safely read the data contained in the disk without executing any unexpected programs
- Mount a remote filesystem and configure the system to be mounted at boot time for an automatic network share on a Linux system
- Set user quotas on disk to protect the availability and security on the Linux system and to prevent users from taking up all the disk drive space on the system
- Edit and modify the /etc/fstab file to manage local and remote network file shares as well as the necessary disk mounting configurations required
- Configure and use the repquota command to verify usage of disk space by users and manage quotas

Tools and Software

The following software is required to complete this lab. Students are encouraged to explore the Internet to learn more about the products and tools used in this lab.

- vi Editor

Deliverables

Upon completion of this lab, you are required to provide the following deliverables to your instructor:

1. Lab Report file including screen captures of the following steps: Part 1, Steps 12, 20, and 24; Part 2, Step 9; Part 3, Steps 5 and 9;
2. Lab Assessments file.

Hands-On Steps

1. From the vWorkstation desktop, **open** the **Common Lab Tasks file**.

   If you desire, use the File Transfer button to transfer the file to your local computer and print a copy for your reference.

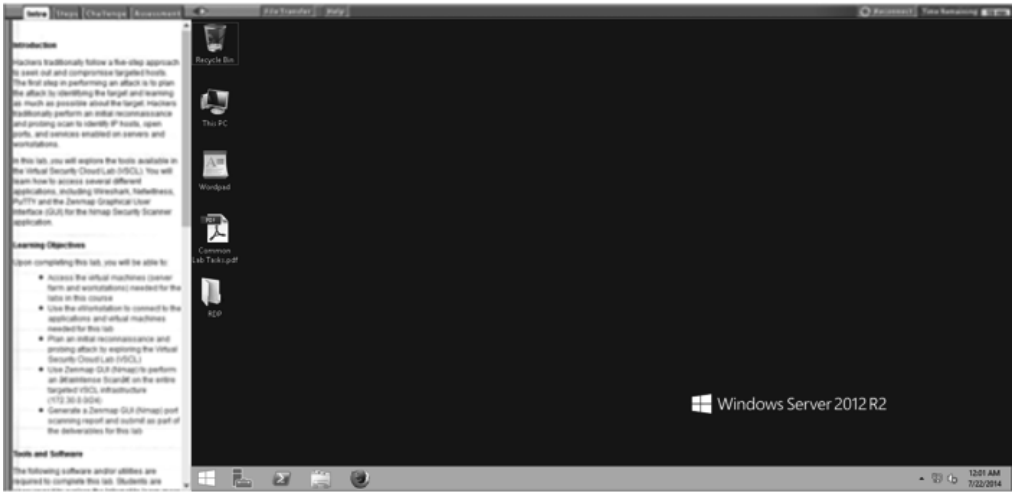


Figure 1 "Student Landing" vWorkstation

2. On your local computer, **create** the **lab deliverable files**.

3. **Review** the **Lab Assessment Worksheet** at the end of this lab. You will find answers to these questions as you proceed through the lab steps.

Part 1: Filesystem Permissions

▶Note:
In the next steps, you will apply hardened security measures on this server by mounting a filesystem with read-only permissions. You will modify the /etc/fstab file and perform several tests to make sure that your changes were effective.
The /etc/fstab file (or filesystems table) is a system configuration file commonly found on UNIX systems. This file usually lists all available disks and disk partitions, and indicates how they are to be initialized or otherwise integrated into the overall system's filesystem.

```
# device name    mount point     fs-type         options          dump-freq pass-num
tmp               /tmp            ext3            defaults,ro       0 0
proc              /proc           swap            defaults          0 0
devpts            /dev/pts        devpts          gid=5,mode=620    0 0
```

Figure 2 Typical fstab file

In a typical fstab file, the columns are separated by spaces or tabs and defined in the following manner.

- **device name:** The device name or other means of locating the partition or data source.
- **mount point:** The mount point, where the data is to be attached to the filesystem. For swap files & devices, this should be set to none.
- **fs-type:** The filesystem type, or the algorithm used to interpret the filesystem.
- **options:** This column indicates whether or not the filesystem should be mounted at boot or whether it can be written to, with *rw* (read-write) or not, with *ro* (read-only).
- **dump-freq:** This indicator adjusts the archiving schedule for the partition (used by dump).
- **pass-num:** This indicator controls the order in which fsck checks the device/partition for errors at boot time. The root device should be 1. Other partitions should be either 2 (to check after root) or 0 (to disable checking for that partition altogether).
- A value of 0 in either of the last two columns disables the corresponding feature.

The /etc/fstab file is most commonly used by the mount command. The mount command instructs the operating system that a filesystem is ready to use, and it becomes associated with a particular point in the filesystem's hierarchy.

1. **Double-click** the **RDP folder** icon on the desktop.
2. **Double-click** the **TargetCentOS01.rdp file** to open the Linux server.

   The remote GNOME desktop, the graphical user interface (GUI) for the virtual Linux server, opens with the IP address of the remote machine (172.30.0.21) in the title bar at the top of the window.

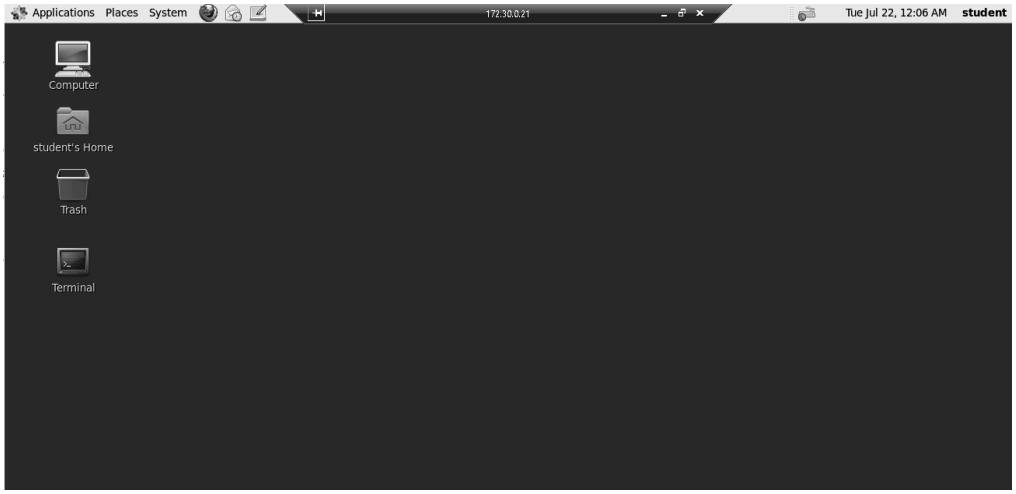


Figure 3 GNOME desktop

3. **Double-click** the **Terminal icon** on the GNOME desktop to open the terminal emulator and access the Linux server command line.

4. At the command prompt, **type su -c 'vi /etc/fstab'** and **press Enter** to open the fstab file in the vi Editor.

5. When prompted, **type P@ssw0rd!**, the root password, and **press Enter**.

▶Note:
You are required to enter a mixed-case password. If you are not using the Citrix Receiver to access this lab, please use the CAPS LOCK button or the On-Screen Keyboard to input the password.

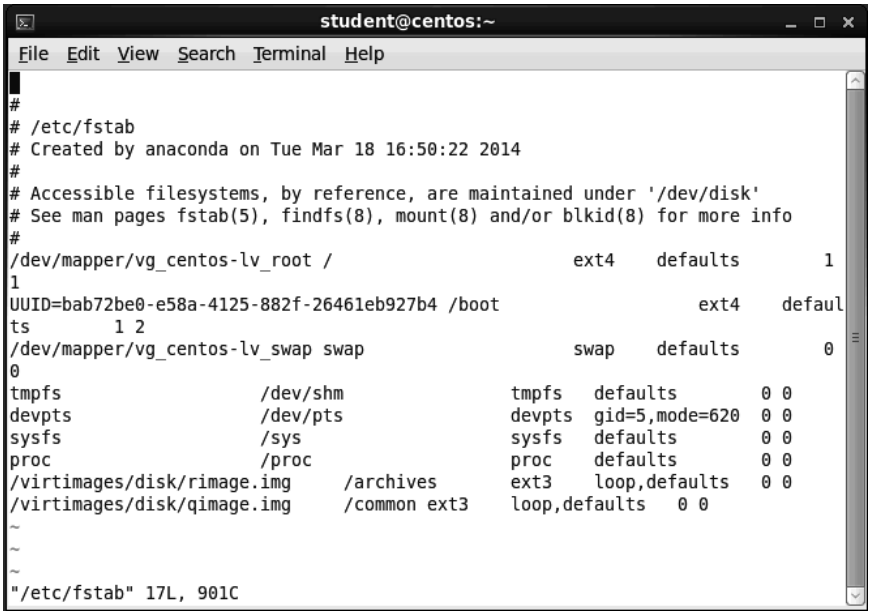


Figure 4 fstab file in the vi Editor

6. **Press** the **i key** to enter the Insert mode.

7. Use the arrow keys to **locate** the following line in the file:

   - **/virtimages/disk/rimage.img /archives ext3 loop,defaults 0 0**

8. Move the cursor immediately behind the word *defaults* and **type ,ro** to apply read-only permissions to the archives directory.

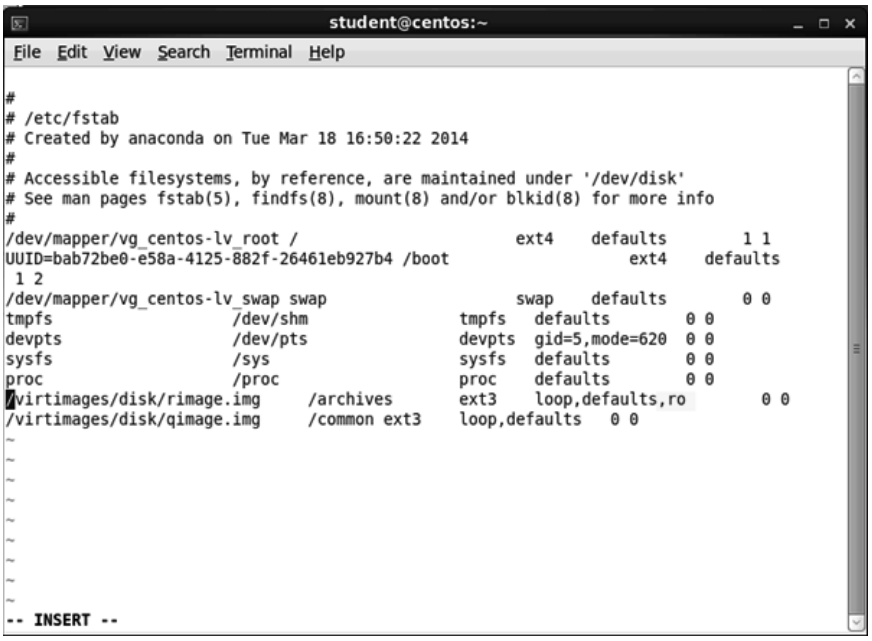


Figure 5 Modify the fstab file

9. **Press** the **Esc key** to exit the Insert mode.

10. **Type :wq!** and **press Enter** to save your changes and exit the vi Editor.

11. At the command prompt, **type cat /etc/fstab** and **press Enter** to display the contents of the file.

12. **Make a screen capture** showing **edited content of the fstab file** and **paste** it into the Lab Report file.

13. At the command prompt, **type su -c 'mount -o remount /archives'** and **press Enter** to remount the archives partition after having made the changes to the fstab file.

14. When prompted, **type P@ssw0rd!**, the root password, and **press Enter**.

▶Note:
You are required to enter a mixed-case password. If you are not using the Citrix Receiver to access this lab, please use the CAPS LOCK button or the On-Screen Keyboard to input the password.

15. At the command prompt, **type cd /archives/2011** and **press Enter** to change the directory.

    Notice that the command prompt indicates that the directory has changed.

16. At the command prompt, **type ls -ls** and **press Enter** to list the files in this directory and review the permissions that are currently applied to each file.

    According to the list command, the revenue.doc file currently has read-write permissions.

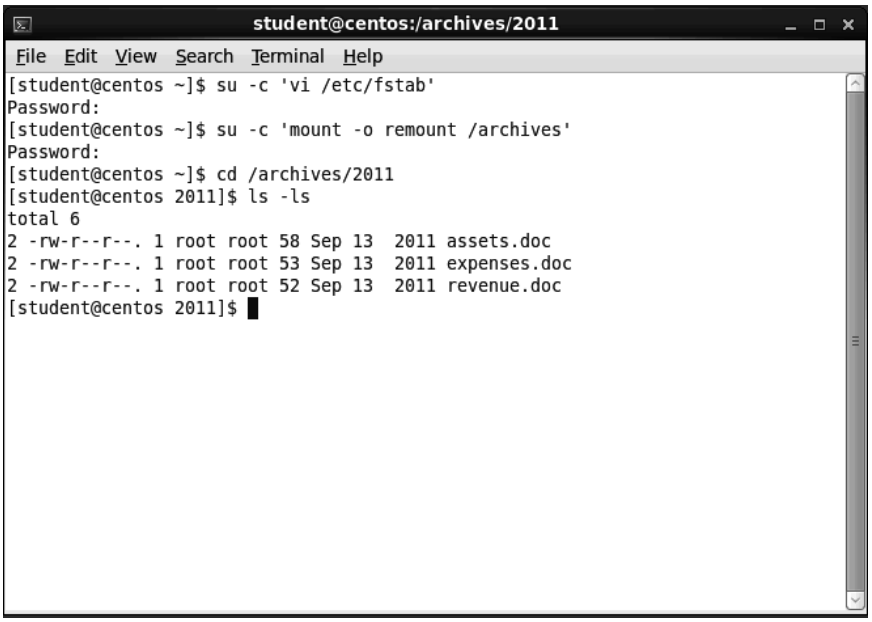


Figure 6 List the archives/2011 directory

17. At the command prompt, **type su -c 'vi revenue.doc'** and **press Enter** to open the revenue.doc file in the vi Editor.

18. When prompted, **type P@ssw0rd!**, the root password, and **press Enter**.

▶Note:
You are required to enter a mixed-case password. If you are not using the Citrix Receiver to access this lab, please use the CAPS LOCK button or the On-Screen Keyboard to input the password.

19. **Press** the **i key** to enter the Insert mode.

    The status line at the bottom of the editor indicates that the file is read-only. So, even though the list command indicated this file was read-write, by changing the permissions on the archives directory, you also changed the permissions for this file.

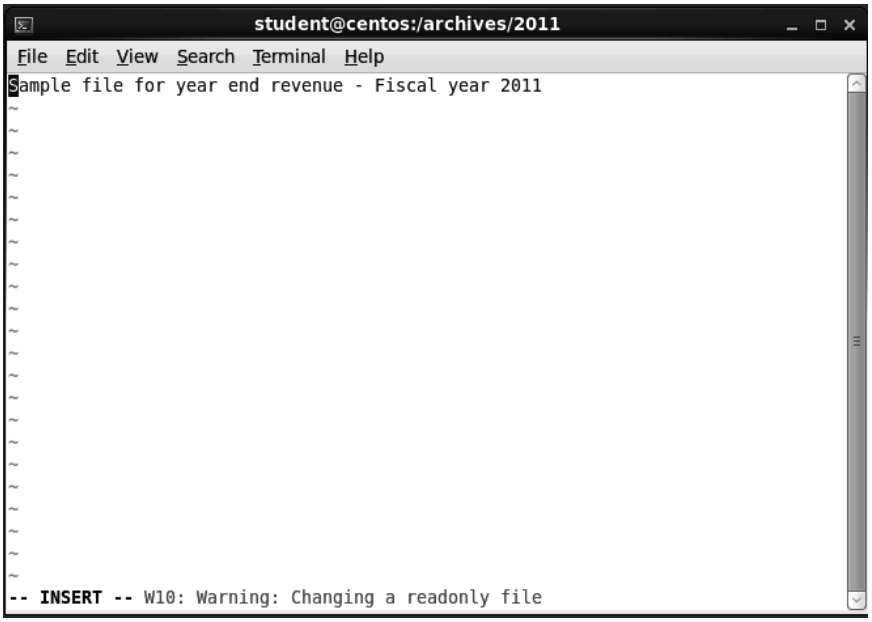


Figure 7 Edit a read-only file

20. **Make a screen capture** showing **the read-only indicator** and **paste** it into the Lab Report file.

21. **Press** the **Esc key** to exit the Insert mode.

22. **Type :q** and **press Enter** to exit the vi Editor without saving any edits.

23. At the command prompt, **type su -c 'touch *yourname*_test.txt'**, replacing *yourname* with your own name, and **press Enter** to create a new file in this directory.

    You should see a "*cannot touch 'yourname_test.txt'*" error message indicating that the file cannot be created in a read-only filesystem.

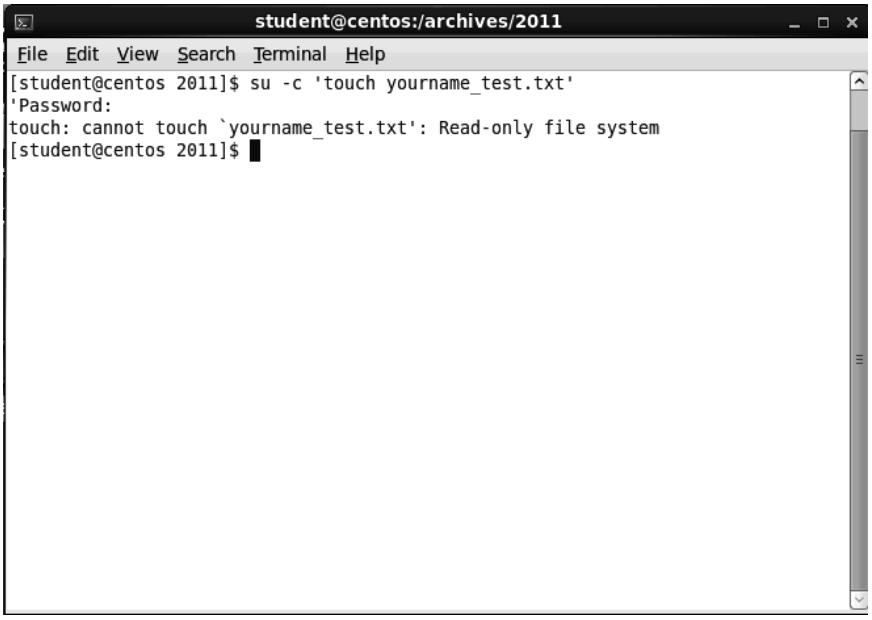


Figure 8 Create a new file in a read-only directory

24. **Make a screen capture** showing **the error message** and **paste** it into the Lab Report file.

Part 2: Setting Quotas

▶Note:
In the next steps, you will apply hardened security measures on this server by setting user account quotas on filesystem partitions. Quotas can be used as a disk management tool to restrict the amount of disk space to which specific users can write.
The following steps are required to establish a quota.

1. Add usrquota to the mounting options and mount or remount.
2. Initialize the quota database.
3. Turn quotas on.
4. Edit the user's quota table to specify a hard limit.

1. At the command prompt, **type su -c 'vi /etc/fstab'** and **press Enter** to reopen the fstab file.
2. When prompted, **type P@ssw0rd!**, the root password, and **press Enter**.

▶Note:
You are required to enter a mixed-case password. If you are not using the Citrix Receiver to access this lab, please use the CAPS LOCK button or the On-Screen Keyboard to input the password.

3. **Press** the **i key** to enter the Insert mode.
4. Use the arrow keys to **locate** the following line in the file:
   - **/virtimages/disk/qimage.img /common ext3 loop,defaults 0 0**

5. Move the cursor immediately behind the word *defaults* and **type ,usrquota** to apply the user quotas.

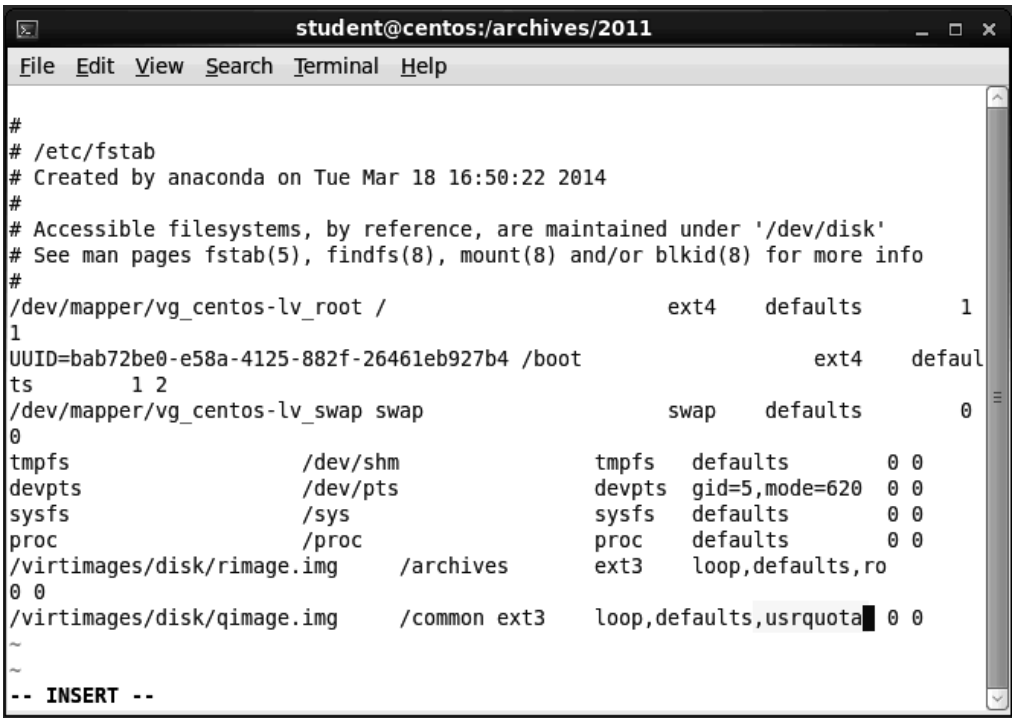


Figure 9 Modify the fstab file

6. **Press** the **Esc key** to exit the Insert mode.

7. **Type :wq!** and **press Enter** to save your changes and exit the vi Editor.

8. At the command prompt, **type cat /etc/fstab** and **press Enter** to display the contents of the file.

9. **Make a screen capture** showing the **edited contents of the fstab file** and **paste** it into the Lab Report file.

10. At the command prompt, **type su -c 'mount -o remount /common'** and **press Enter** to remount the common partition after having made the changes to the fstab file.

11. When prompted, **type P@ssw0rd!**, the root password, and **press Enter**.

▶Note:
You are required to enter a mixed-case password. If you are not using the Citrix Receiver to access this lab, please use the CAPS LOCK button or the On-Screen Keyboard to input the password.

12. At the command prompt, **type su -c ' /sbin/quotacheck -cug /common'** and **press Enter** to initialize the quota database on this folder filesystem.

▶Note:
Editing the /etc/fstab file and remounting the filesystem only alerted Linux to the fact that the filesystem has quota capabilities. You initialize the quota table with the quotacheck command.

13. When prompted, **type P@ssw0rd!**, the root password, and **press Enter**.

▶Note:
You are required to enter a mixed-case password. If you are not using the Citrix Receiver to access this lab, please use the CAPS LOCK button or the On-Screen Keyboard to input the password.

14. At the command prompt, **type su -c '/sbin/quotaon /common'** and **press Enter** to turn quotas on.

15. When prompted, **type P@ssw0rd!**, the root password, and **press Enter**.

▶Note:
You are required to enter a mixed-case password. If you are not using the Citrix Receiver to access this lab, please use the CAPS LOCK button or the On-Screen Keyboard to input the password.

16. At the command prompt, **type su -c '/usr/sbin/edquota -f /common student'** and **press Enter** to open the user quota settings.

17. When prompted, **type P@ssw0rd!**, the root password, and **press Enter**.

▶Note:
You are required to enter a mixed-case password. If you are not using the Citrix Receiver to access this lab, please use the CAPS LOCK button or the On-Screen Keyboard to input the password.

18. **Press** the **i key** to enter the Insert mode.

19. Use the arrow keys to **locate** the **/dev/loop1 line** in the Disk quotas for user student (uid 500) section of the file.

20. **Type** the new limits indicated below to change the existing limits.

    - *First* soft column: **30**
    - *First* hard column: **100**

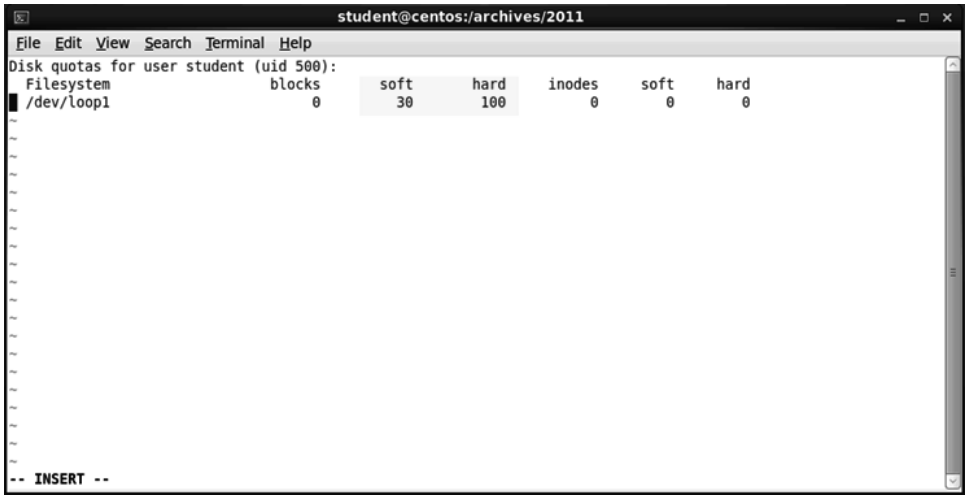


Figure 10 Set the quotas for the student user account

21. **Press** the **Esc key** to exit the Insert mode.

22. **Type :wq!** and **press Enter** to save your changes and exit the vi Editor.

Part 3: Quota Testing and Verification

▶Note:
In the next steps, you will follow several test scenarios to make sure that your filesystem changes in the previous lab parts were effective.

1. At the command prompt, **type su –c 'mkdir /common/student && chown student.student /common/student'** and **press Enter** to create a new directory called student and change ownership of that directory to the student user account.

2. When prompted, **type P@ssw0rd!**, the root password, and **press Enter**.

▶Note:
You are required to enter a mixed-case password. If you are not using the Citrix Receiver to access this lab, please use the CAPS LOCK button or the On-Screen Keyboard to input the password.

3. At the command prompt, **type cd /common/student** and **press Enter** to change the directory.

   Notice that the command prompt indicates that the directory has changed.

4. At the command prompt, **type dd if=/dev/urandom of=*yourname*.file bs=9548576 count=1**, replacing *yourname* with your own name, and **press Enter** to create a file with approximately 100MB of random data.

```
[student@centos ~]$ su -c 'mkdir /common/student && chown student.student /commo
n/student'
Password:
[student@centos ~]$ cd /common/student
[student@centos student]$ dd if=/dev/urandom of=yourname.file bs=9548576 count=1
loop1: warning, user block quota exceeded.
loop1: write failed, user block limit reached.
dd: writing `yourname.file': Disk quota exceeded
1+0 records in
0+0 records out
98304 bytes (98 kB) copied, 1.54778 s, 63.5 kB/s
[student@centos student]$
```

Figure 11 Attempt to create a file that exceeds user quotas

5. **Make a screen capture** showing the **output from your test** and **paste** it into the Lab Report file.

6. At the command line prompt, **type su –c '/usr/sbin/repquota /common'** and **press Enter** to run a report of the amount of the quota limit already used.

   The repquota report displays a summary of the disk usage and quotas for the specified filesystems. The current number of files and amount of space (in kilobytes) is printed for each user, along with any quotas created with edquota.

7. When prompted, **type P@ssw0rd!**, the root password, and **press Enter**.

▶Note:
You are required to enter a mixed-case password. If you are not using the Citrix Receiver to access this lab, please use the CAPS LOCK button or the On-Screen Keyboard to input the password.

```
student@centos:/common/student
File  Edit  View  Search  Terminal  Help
[student@centos student]$
[student@centos student]$ su -c '/usr/sbin/repquota /common'
Password:
*** Report for user quotas on device /dev/loop1
Block grace time: 7days; Inode grace time: 7days
                        Block limits                File limits
User            used    soft    hard  grace    used  soft  hard  grace
----------------------------------------------------------------------
root      --    6178       0       0              4     0     0
student   +-     100      30     100  6days       2     0     0


[student@centos student]$
```

Figure 12 Repquota report

8. At the command line prompt, **type quota** and **press Enter** to run a quota report of the student directory.

9. **Make a screen capture** showing **the quota report** and **paste** it into the Lab Report file.

10. In the Lab Report file, **compare** the output of the repquota and quota commands.

11. **Close** the **remote Linux connection**.

▶Note:
This completes the lab. **Close** the **virtual lab**, if you have not already done so.

Evaluation Criteria and Rubrics

The following are the evaluation criteria and rubrics that the students must perform:

1. Mount a filesystem without execute permissions, so you can safely read the data contained in the disk without executing any unexpected programs – [**20%**]
2. Mount a remote filesystem and configure the system to be mounted at boot time for an automatic network share on a Linux system – [**20%**]
3. Set user quotas on disk to protect the availability and security on the Linux system and to prevent users from taking up all the disk drive space on the system – [**20%**]
4. Edit and modify the /etc/fstab file to manage local and remote network file shares as well as the necessary disk mounting configurations required [**20%**]
5. Configure and use the repquota command to verify usage of disk space by users and manage quotas – [**20%**]

Lab #4 – Assessment Worksheet

Applying Hardened Linux Filesystem Security Controls

Course Name and Number: _____

Student Name: _____

Instructor Name: _____

Lab Due Date: _____

Overview

This lab, an extension of the previous labs, incorporated security hardening for filesystems and user access to mounted filesystems. In this lab, you mounted a filesystem that does not have execute permissions on the CentOS Linux Server. You also mounted a remote filesystem and set quotas for users of mounted filesystems.

Lab Assessment Questions & Answers

1. Which fstab option would allow customers to view PDF files without being able to modify the files?

   Note introducing Part 1. Read-Only or ro

2. Describe the process to create a quota hard limit of 2G for a user.

   Note introducing Part 2. The following steps are required to establish a quota.
   - Add usrquota to the mounting options and mount or remount.
   - Initialize the quota database.
   - Turn quotas on.
   - Edit the user's quota table to specify a hard limit.

3. What command enables you to initialize quotas on a filesystem?

   Part 2, Step 12. Use the command **su -c ' /sbin/quotacheck -cug /<filesystem>'**

4. What command enables you to change disk quotas on the /common filesystem for the student user account?

   Part 2, Step 16. Use the command **su -c '/usr/sbin/edquota -f /common student'**

5. What is the /etc/fstab file for?

   Note introducing Part 1. The /etc/fstab file (or filesystems table) is a system configuration file commonly found on UNIX systems. This file usually lists all available disks and disk partitions, and indicates how they are to be initialized or otherwise integrated into the overall system's filesystem.

6. What is the mount command? Explain.

   Note introducing Part 1. The mount command instructs the operating system that a filesystem is ready to use, and it becomes associated with a particular point in the filesystem's hierarchy.

7. What is the repquota command in Linux used for? Explain. How is this different from the quota command?

   Note following Part 3, Step 6. The repquota report displays a summary of the disk usage and quotas for the specified filesystems. The current number of files and amount of space (in kilobytes) is printed for each user, along with any quotas created with edquota. (Answers to the second question will be unique to each student.)

Lab #5 Hardening Security for Linux Services and Applications

Introduction

This lab is an extension of previous labs, and it incorporates security hardening for Linux services and applications loaded in the physical server. Every service and application in a Linux system has a separate configuration file. These configuration files consist of a collection of execution commands that control various aspects of the program, such as passwords, disk quotas, access, user accounts, and even system messages. In most cases, the configuration files are found in the Linux /etc directory.

In this lab, you will configure security and hardened services and applications to ensure the confidentiality, integrity, and availability of those services. You will configure and secure an Apache Web server and MySQL database and the components necessary to harden the security implementation of both. You also will configure the Sendmail application for secure local messaging and will enable secure, encrypted remote access using Secure Shell (SSH).

This lab has four parts, which should be completed in the order specified. There is no challenge question for this lab.

1. In the first part of the lab, you will apply harden security measures for a MySQL database application.
2. In the second part of the lab, you will apply harden security measures on this server by modifying the Apache Web services configuration file (httpd.conf).
3. In the third part of the lab, you will apply harden security measures on this server by modifying the Sendmail configuration file (sendmail.mc).
4. In the fourth part of the lab, you will edit the SSH configuration file (sshd_config) to disallow direct root login, require all connecting systems be whitelisted (added to a internal registry of recognized systems), and display a warning message to everyone who attempts to log in remotely.

Learning Objectives

Upon completing this lab, you will be able to do the following:

- Harden Linux server services when enabling and installing them, and keep a security perspective during configuration

- Perform basic security configurations to ensure that the system has been hardened before hosting a Web site
- Configure and perform basic security for a MySQL database, understanding the ramifications of a default installation and recommending hardening steps for the database instance
- Set up and perform basic security configuration for Sendmail to be able to leverage the built-in messaging capabilities of the Linux system
- Enable and implement secure SSH for encrypted remote access over the network or across the Internet of a Linux server system

Tools and Software

The following software and/or utilities are required to complete this lab. Students are encouraged to explore the Internet to learn more about the products and tools used in this lab.

- Apache Web Server
- MySQL
- Sendmail
- vi Editor

Deliverables

Upon completion of this lab, you are required to provide the following deliverables to your instructor:

1. Lab Report file including screen captures of the following steps: Part 1, Step 14; Part 2, Steps 11 and 15; Part 3, Step 10; Part 4, Steps 22 and 26;
2. Lab Assessments file.

Hands-On Steps

▶Note:
This lab contains detailed lab procedures, which you should follow as written. Frequently performed tasks are explained in the Common Lab Tasks document on the vWorkstation desktop. You should review these tasks *before* starting the lab.

1. From the vWorkstation desktop, **open** the **Common Lab Tasks file**.

   If you desire, use the File Transfer button to transfer the file to your local computer and print a copy for your reference.

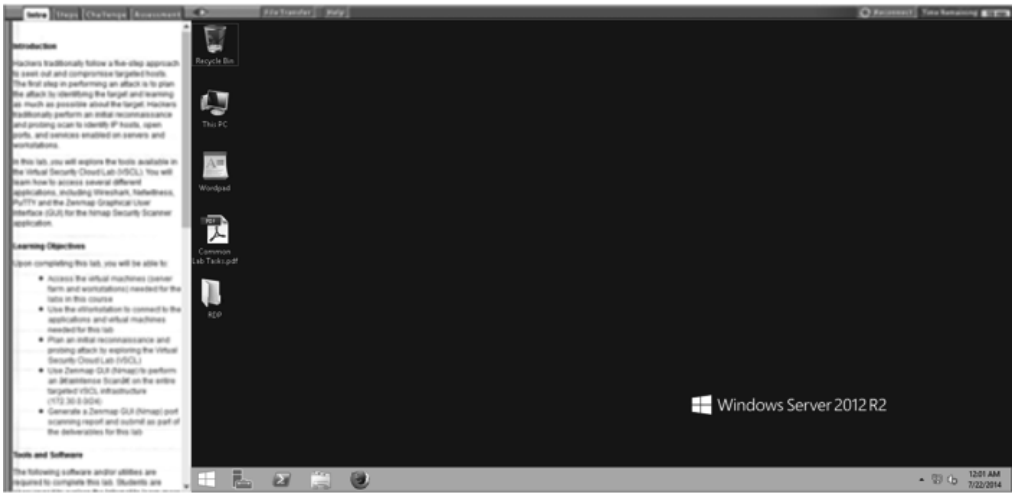


Figure 1 "Student Landing" vWorkstation

2. On your local computer, **create** the **lab deliverable files**.
3. **Review** the **Lab Assessment Worksheet** at the end of this lab. You will find answers to these questions as you proceed through the lab steps.

Part 1: Secure MySQL database

▶Note:
In the next steps, you will harden a MySQL database application by modifying the my.cnf configuration file. You will add skip-networking to prevent remote access to the database and disallow the ability to load a local data file. You also will configure the database to start automatically on runlevel 3, and set the MySQL root password.

Runlevels define the state of the Linux server upon boot-up. Defining runlevels helps define access control parameters for users or system administrators to access the service or application uniquely. Runlevel three, Multi-user Mode with Networking, is the most common mode. It enables multiple user accounts, networking, command line configurations, and remote access to the server.

1. **Double-click** the **RDP folder** icon on the desktop.

2. **Double-click** the **TargetCentOS01.rdp file** to open the Linux server.

   The remote GNOME desktop, the graphical user interface (GUI) for the virtual Linux server, opens with the IP address of the remote machine (172.30.0.21) in the title bar at the top of the window.

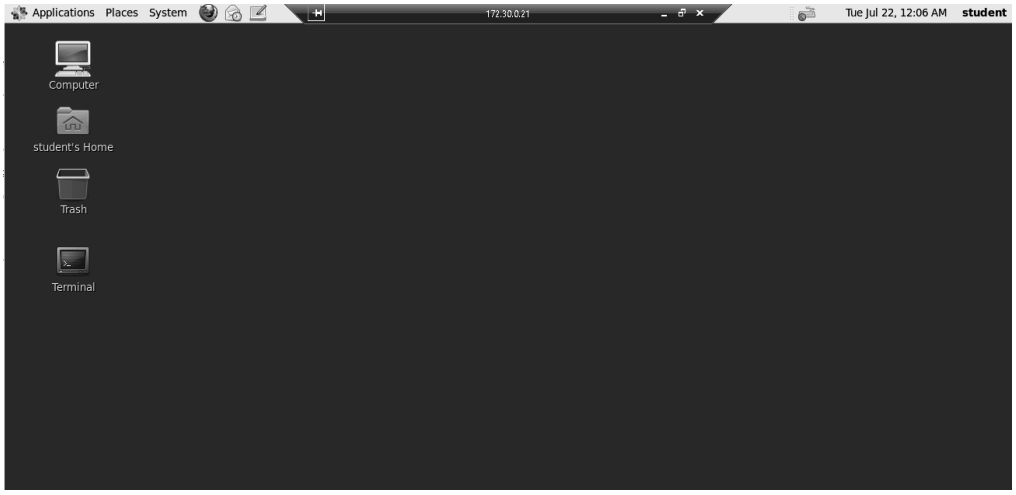


Figure 2 GNOME desktop

3. **Double-click** the **Terminal icon** on the GNOME desktop to open the terminal emulator and access the Linux server command line.

4. At the command prompt, **type sudo /sbin/service mysqld status** and **press Enter** to check the status of the MySQL service.

5. When prompted for a password, **type pass=7890** and **press Enter**.

   The system returns a status indicating that the MySQL daemon service is not running.

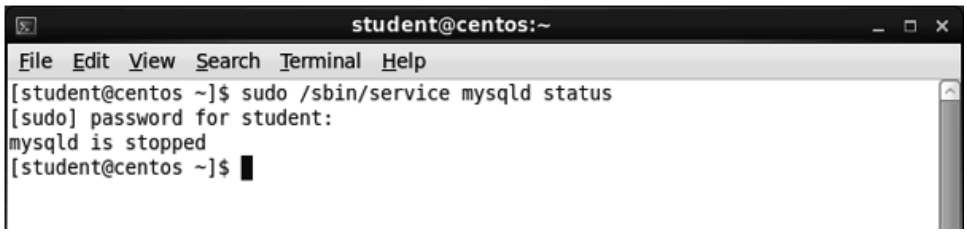


Figure 3 Check the status of a service

6. At the command prompt, **type su -c 'vi /etc/my.cnf' and press Enter** to open the MySQL configuration file in the vi Editor.

7. When prompted, **type P@ssw0rd!**, the root password, and **press Enter**.

▶Note:
You are required to enter a mixed-case password. If you are not using the Citrix Receiver to access this lab, please use the CAPS LOCK button or the On-Screen Keyboard to input the password.

8. **Press** the **i key** to enter the Insert mode.

9. Use the arrow keys to **locate** the **#symbolic-links=0 line** and **delete** the **# symbol** from the beginning of the line to enable this command.

10. Use the arrow keys to **locate** the **#skip-networking line** and **delete** the **# symbol** from the beginning of the line to enable this command.

▶Note:
symbolic-links: Symbolic links are a special type of file that contains a reference to another file or directory in the form of an absolute or relative path and that affects pathname resolution. Because some MySQL statements work by creating a temporary file in the database directory and replacing the original file with the temporary file when the statement operation is complete; this could create several security risks.

skip-networking: This prevents remote connections (including attacks) to the MySQL DB but will still allow localhost connections via the mysql.sock socket.

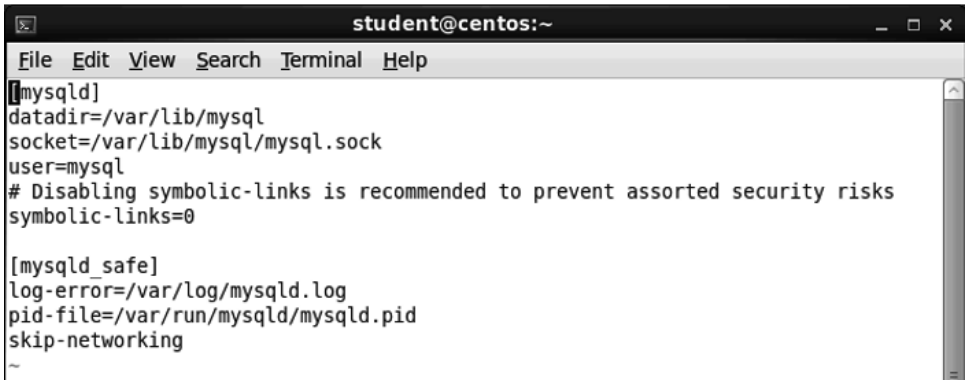


Figure 4 Modify the my.cnf file

11. **Press** the **Esc key** to exit the Insert mode.

12. **Type :wq!** and **press Enter** to save your changes and exit the vi Editor.

13. At the command prompt, **type cat /etc/my.cnf** and **press Enter** to display the contents of the edited file.

14. **Make a screen capture** showing the **contents of the edited file** and **paste** it into the Lab Report file.

15. At the command prompt, **type sudo /sbin/chkconfig --level 3 mysqld on** and **press Enter** to start the database server automatically only in runlevel 3.

16. At the command prompt, **type sudo /sbin/chkconfig mysqld --list** and **press Enter** to view the MySQL runlevel settings and verify that the service is turned on in runlevel 3.

Though the sudo command usually requires a password, repeated sudo commands in the same session (as in this instance) do not required repeated re-entry of the password.

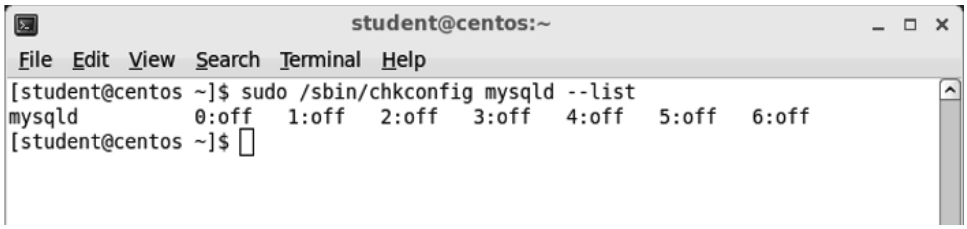


Figure 5 MySQL runlevel settings

17. At the command prompt, **type sudo /sbin/service mysqld start** and **press Enter** to start the database server.

    The system returns an OK flag indicating that the MySQL daemon service is starting. Notice that the service started without a database password.

18. At the command prompt, **type mysql -u root -p** and **press Enter** to enter the MySQL environment.

19. At the password prompt, **press Enter** without entering a password.

    Notice that the command prompt has changed to mysql>. By default, no password is required for the database root user, which can be a significant security risk. You can harden the security by setting a root password for the MySQL server.

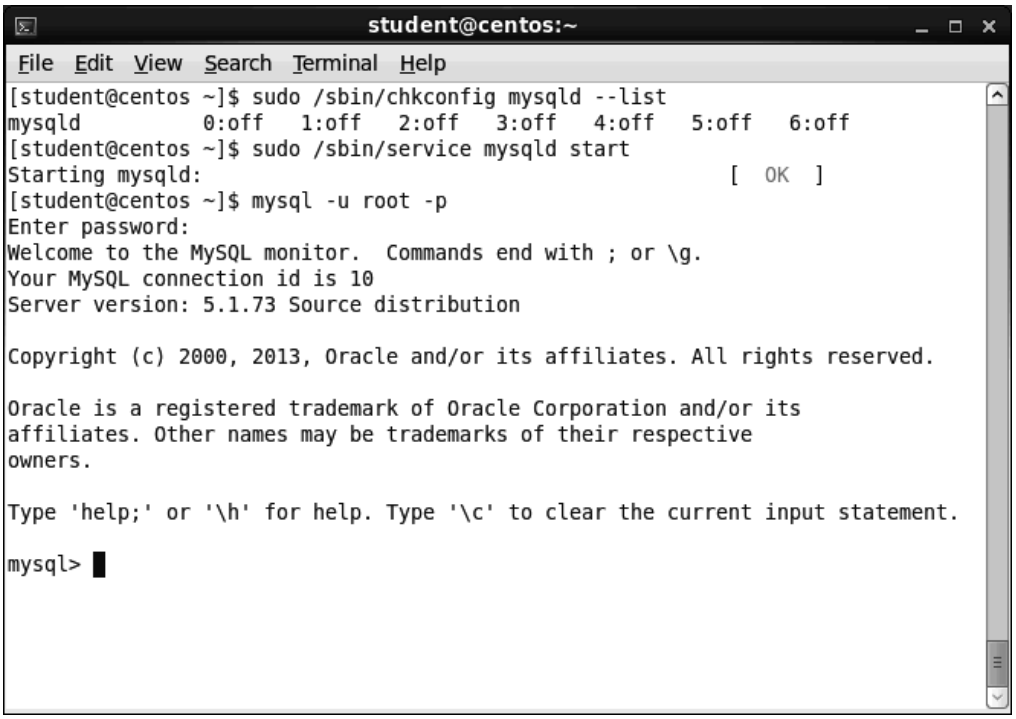


Figure 6 MySQL console

20. At the command prompt, **type SET PASSWORD FOR root@localhost = PASSWORD('pass=7890');** and **press Enter** to set the MySQL root password.

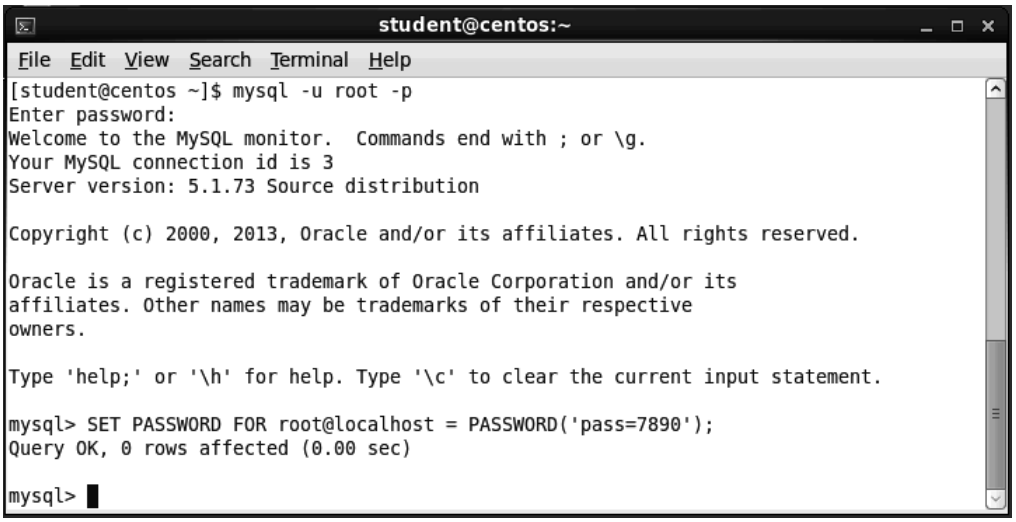


Figure 7 Set the MySQL root password

21. At the command prompt, **type quit** and **press Enter** to exit the MySQL environment and return to the TargetCentOS01 command prompt.

22. Now, repeat step 18 to attempt to log into mysql without entering a password: At the command prompt, **type mysql -u root -p** and **press Enter** to enter the MySQL environment.

23. At the password prompt, **press Enter** without entering a password.

    This time, the access is denied because a password is required.

Part 2: Harden the Apache Web server

▶Note:
The Apache Web server is an open source HTTP server that can run on *nix-based and Windows operating systems. In the next steps, you will harden security measures on this server by modifying the Apache Web services configuration file (httpd.conf). You will first set the service to start automatically in runlevel 3, disable the default HTTP Trace connection method, and then verify your changes.

1. At the command prompt, **type sudo /sbin/chkconfig --level 3 httpd on** and **press Enter** to set the Web service to start automatically on runlevel 3.
2. If prompted for a password, **type pass=7890** and **press Enter**.
3. At the command prompt, **type sudo /sbin/service httpd start** and **press Enter** to start the httpd service.

   The system returns an OK flag indicating that the httpd service is starting.

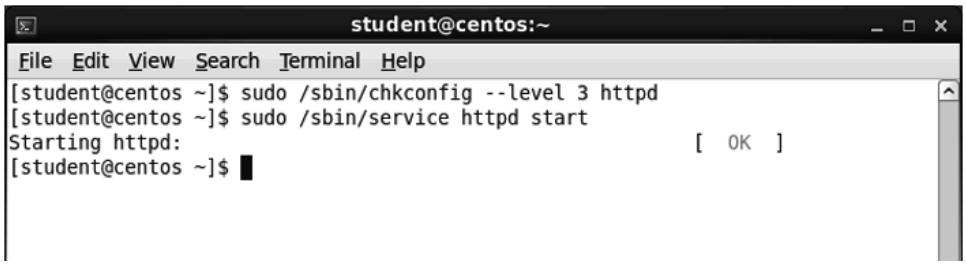


Figure 8 httpd runlevel settings

4. At the command prompt, **type su -c ' vi +86 /etc/httpd/conf/httpd.conf '** and **press Enter** to open the httpd.conf file in the vi Editor and move directly to line 86.
5. When prompted, **type P@ssw0rd!**, the root password, and **press Enter**.

▶Note:
You are required to enter a mixed-case password. If you are not using the Citrix Receiver to access this lab, please use the CAPS LOCK button or the On-Screen Keyboard to input the password.

6. **Press** the **i key** to enter the INSERT mode.

7. Use the arrow keys to **locate** the **#TraceEnable off line** and **delete** the **# symbol** at the beginning of the line to disable the Trace connection method.

   This method has the potential to leak more information about the server than necessary and poses a security risk.

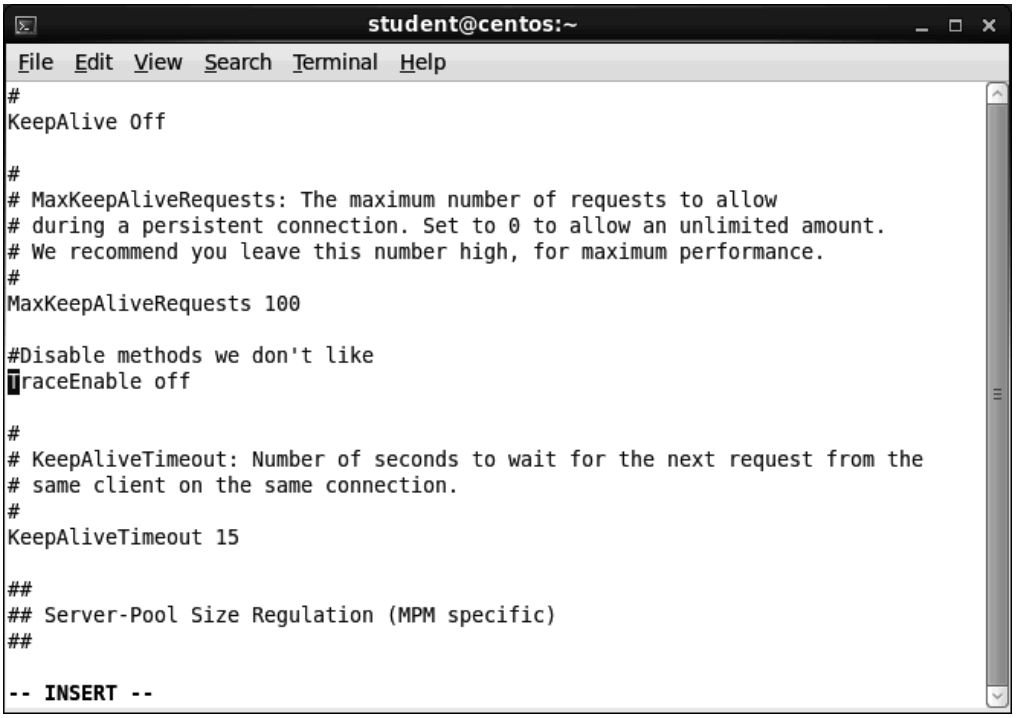


Figure 9 Disable the Trace method

8. **Press** the **Esc key** to exit the Insert mode.

9. **Type :wq!** and **press Enter** to save your changes and exit the vi Editor.

10. At the command prompt, **type sudo /sbin/service httpd configtest** and **press Enter** to test for any syntax errors in the configuration file caused by your edits.

    The system will return a Syntax OK message indicating that the file is error-free.

11. **Make a screen capture** showing the **syntax message** and **paste** it into the Lab Report file.

12. At the command prompt, **type sudo /sbin/service httpd reload** and **press Enter** to reload the configuration file and put your changes into effect.

    The system returns no error indicating that the Web service is reloading.

13. At the command prompt, **type telnet localhost 80** and **press Enter** to open a connection to port 80 to test your configuration changes.

    Once connected to the localhost, the solid cursor becomes the command prompt.

```
[student@centos ~]$ telnet localhost 80
Trying ::1...
Connected to localhost.
Escape character is '^]'.
```

Figure 10 Telnet prompt

14. At the solid cursor command prompt, **type TRACE** and **press Enter** to open the raw code of an HTML file.

    In this case, the system generates an HTML file that indicates the method is not allowed, which verifies that your changes were successful.

```
student@centos:~
File  Edit  View  Search  Terminal  Help
[student@centos ~]$ sudo /sbin/service httpd configtest
Syntax OK
[student@centos ~]$ sudo /sbin/service httpd reload
Reloading httpd:
[student@centos ~]$ telnet localhost 80
Trying ::1...
Connected to localhost.
Escape character is '^]'.
TRACE
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>405 Method Not Allowed</title>
</head><body>
<h1>Method Not Allowed</h1>
<p>The requested method TRACE is not allowed for the URL /.</p>
<hr>
<address>Apache/2.2.15 (CentOS) Server at centos.localdomain Port 80</address>
</body></html>
Connection closed by foreign host.
[student@centos ~]$
```

Figure 11 Output from Telnet connection

15. **Make a screen capture** showing the output of the TRACE command and **paste** it into the Lab Report file.

Part 3: Secure Sendmail

▶Note:
In the next steps, you will harden security measures on this server by modifying the Sendmail configuration file (sendmail.mc). Sendmail is the default Linux mail server and can be the source of many security threats if not hardened properly. You will first set the service to start automatically in runlevel 3, and then configure the sendmail.mc configuration file to restrict relaying mail. An open SMTP relay allows anyone on the Internet to relay e-mail through it.

1. At the command prompt, **type sudo /sbin/chkconfig --level 3 sendmail on** and **press Enter** to set the Sendmail service to start automatically on runlevel 3.
2. If prompted for a password, **type pass=7890** and **press Enter**.
3. At the command prompt, **type su -c 'vi +116 /etc/mail/sendmail.mc'** and **press Enter** to open the mail configuration file in the vi Editor at line 116.
4. When prompted, **type P@ssw0rd!**, the root password, and **press Enter**.

▶Note:
You are required to enter a mixed-case password. If you are not using the Citrix Receiver to access this lab, please use the CAPS LOCK button or the On-Screen Keyboard to input the password.

5. **Press** the **i key** to enter the INSERT mode.
6. Use the arrow keys to **locate** the **DAEMON_OPTIONS('Port=smtp, Name=MTA')dnl line** in the file, move the cursor directly after the word *smtp*, and **type Addr=127.0.0.1,** so that the entire line reads: *DAEMON_OPTIONS(`Port=smtp, Addr=127.0.0.1, Name=MTA')dnl*.

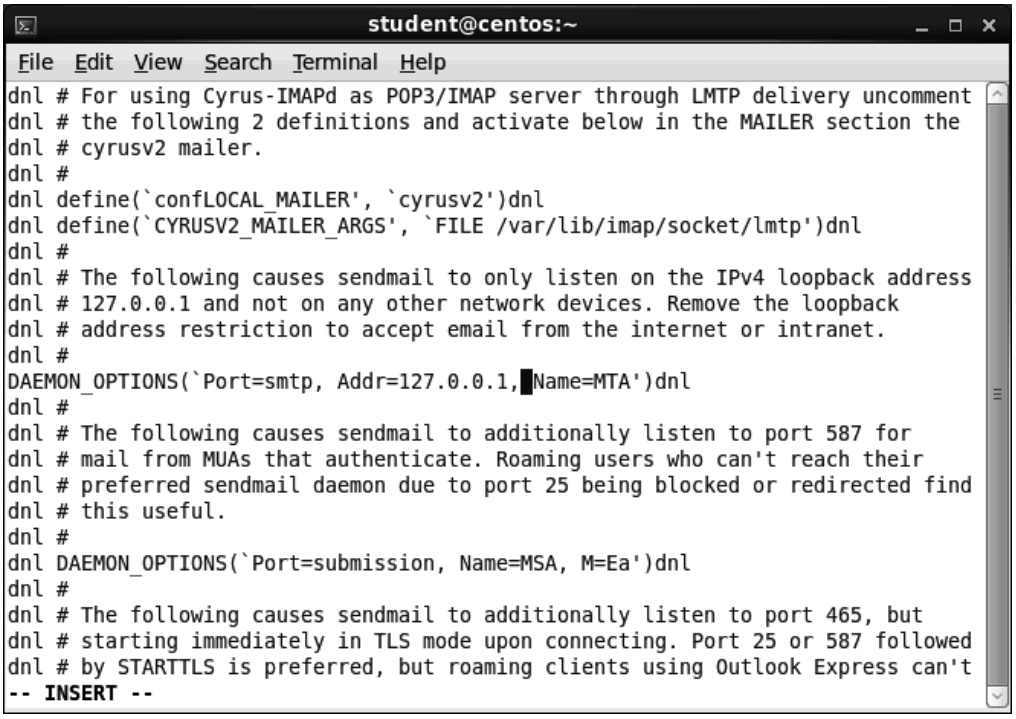


Figure 12 Modify the sendmail.mc file

7. **Press** the **Esc key** to exit the Insert mode.
8. **Type :wq!** and **press Enter** to save your changes and exit the vi Editor.

9. At the command prompt, **type sudo /sbin/service sendmail start** and **press Enter** to start the Sendmail server.

   The system returns OK flags to indicate that both the Sendmail server and client service are running.

10. **Make a screen capture** showing the **OK flags** and **paste** it into the Lab Report file.

Part 4: Secure SSH

▶Note:
Secure Shell (SSH) is an encrypted remote command-line login, and ensures confidentiality in remote access and login by system administrators. Telnet was the predecessor to SSH. It sends remote access and login unencrypted in cleartext and therefore can be compromised easily by a hacker if the IP packets are sniffed and captured. In the next steps, you will first set the service to start automatically in runlevel 3 and then configure the secure shell (SSH service) so that it disallows login by the root account, accepts only recognized hosts, requires *all* hosts be added to the hosts file, and displays a message to *every* user who attempts to log into the server.

1. At the command prompt, **type su -c 'vi /etc/ssh/sshd_config'** and **press Enter** to open the SSH configuration file in the vi Editor.

2. When prompted, **type P@ssw0rd!**, the root password, and **press Enter**.

▶Note:
You are required to enter a mixed-case password. If you are not using the Citrix Receiver to access this lab, please use the CAPS LOCK button or the On-Screen Keyboard to input the password.

3. **Press** the **i key** to enter the INSERT mode.

4. Use the arrow keys to **locate** the **#PermitRootLogin yes line** in the file and **delete** the **# symbol** from the beginning of the line to enable the command.

5. In the PermitRootLogin line, **type no** to *replace the yes* and remove the root account's ability to login.

6. Use the arrow keys to **locate** the **PasswordAuthentication yes line** in the file and **type no** to *replace the yes* and disable logins with passwords.

   Notice that there are 2 PasswordAuthentication lines. The first has a # symbol in front disabling it by default. The second does not have a # symbol, so that is the command the system is currently reading and that is the command line you will need to edit.

7. Use the arrow keys to **locate** the **#UsePAM no line** in the file and **delete** the **# symbol** from the beginning of the line to enable the command.

8. Use the arrow keys to **locate** the **UsePAM yes line** in the file and **type** the **# symbol** at the beginning of the line to disable the command.

9. Use the arrow keys to **locate** the **#Banner none line** in the file and **delete** the **# symbol** from the beginning of the line to enable the command.

10. In the Banner line, **type /etc/motd** *to replace the none* and specify the name of the file that will display an error message to *every* user who attempts to log in.

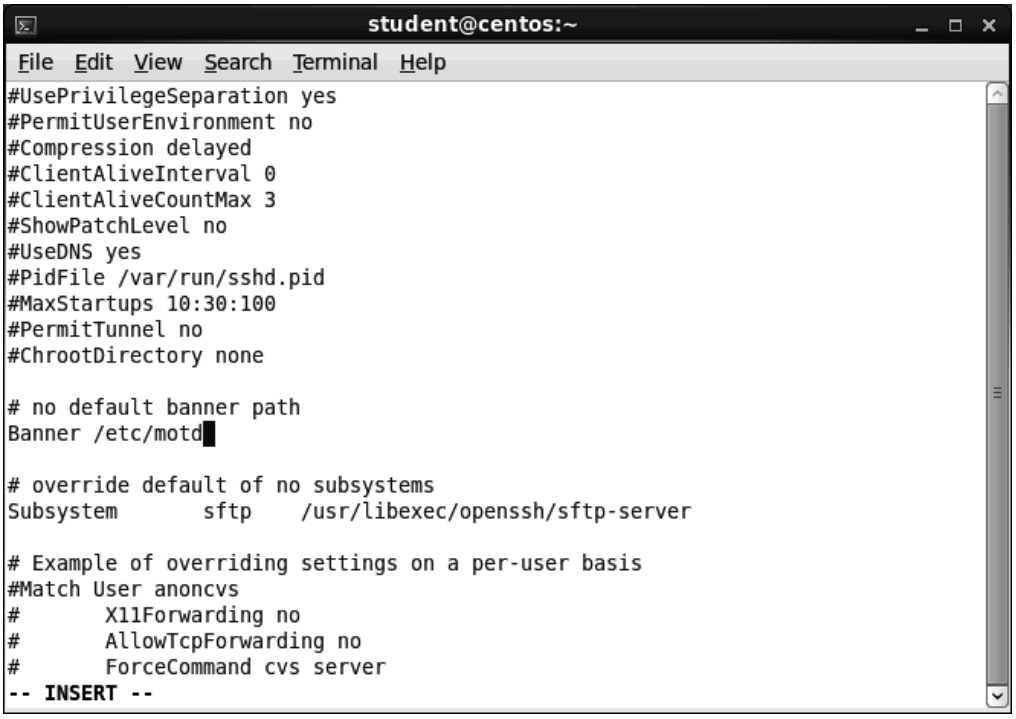


Figure 13 Modify the sshd_config file

11. **Press** the **Esc key** to exit the Insert mode.

12. **Type :wq!** and **press Enter** to save your changes and exit the vi Editor.

13. At the command prompt, **type su -c 'vi /etc/motd'** and **press Enter** to open the MOTD (message of the day) banner file in the vi Editor.

14. When prompted, **type P@ssw0rd!**, the root password, and **press Enter**.

▶Note:
You are required to enter a mixed-case password. If you are not using the Citrix Receiver to access this lab, please use the CAPS LOCK button or the On-Screen Keyboard to input the password.

15. **Press** the **i key** to enter the INSERT mode.

16. At the beginning of the first blank line, **type PROPERTY OF FIRST WORLD BANK SAVINGS AND LOAN. AUTHORIZED USERS ONLY!**

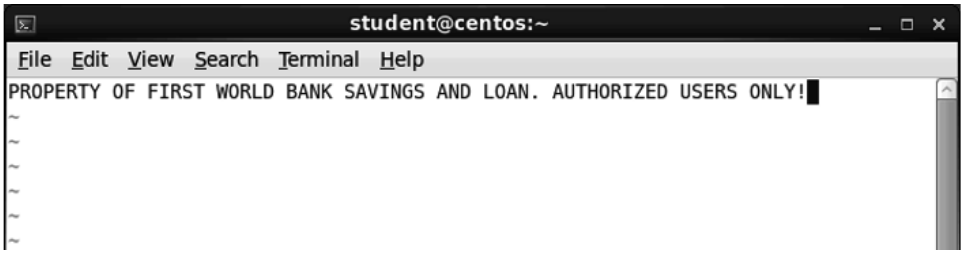


Figure 14 Modify the motd file

17. **Press** the **Esc key** to exit the Insert mode.

18. **Type :wq!** and **press Enter** to save your changes and exit the vi Editor.

19. At the command prompt, **type sudo /sbin/service sshd status** and **press Enter** to check the status of the open SSH server.

20. When prompted for a password, **type pass=7890** and **press Enter**.

    The system will return an indicator that the openssh-daemon is running.

21. **Make a screen capture** showing the **status of the openssh-daemon** and **paste** it into the Lab Report file.

22. At the command prompt, **type sudo /sbin/service sshd reload** and **press Enter** to reload the open SSH configuration file and put your changes into effect.

    The system returns an OK flag indicating that the SSH service is reloading.

23. At the command prompt, **type ssh localhost** and **press Enter** to open an SSH connection to the localhost.

    The system returns an error indicating that *localhost* is not a recognized host. Unless the host is specifically added to the hosts file, which was not done in this lab, this error will occur. The system will also prompt you to continue the attempted connection.

24. When prompted to continue connecting, **type yes** and **press Enter.**

    Because the sshd_config file was configured to deny SSH access to the root user and anyone trying to use a password, the SSH server will prevent the remote access and display the message of the day.

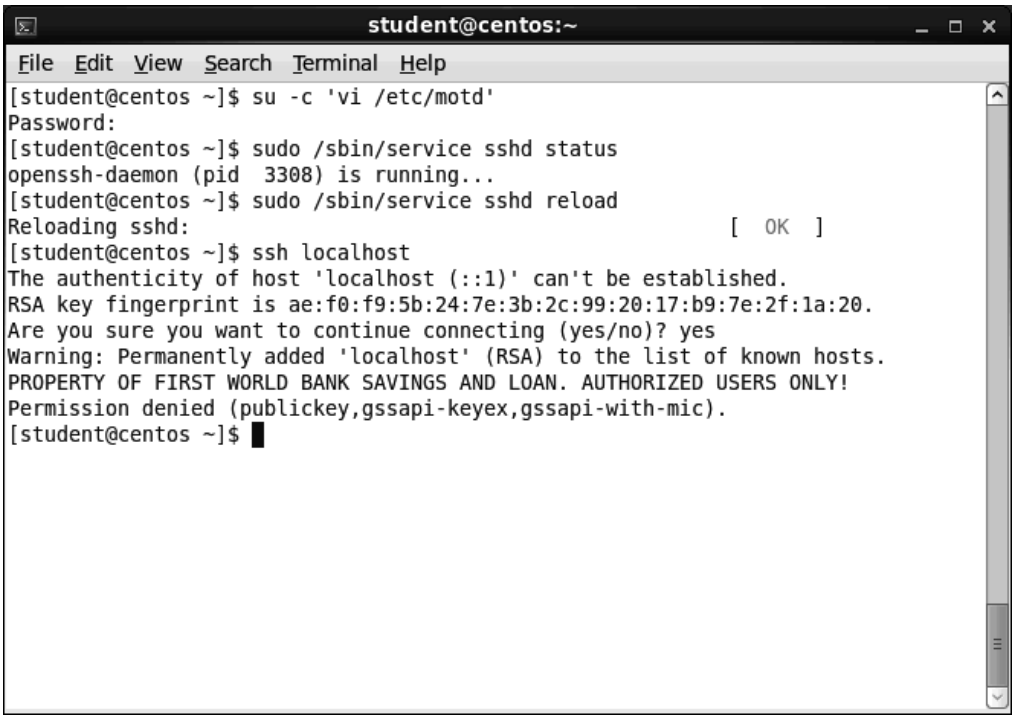


Figure 15 Verify MOTD banner message for SSH login

25. **Make a screen capture** showing **the message of the day banner** and **paste** it into the Lab Report file.

26. **Close** the **remote Linux connection window**.

▶Note:
This completes the lab. **Close** the **virtual lab**, if you have not already done so.

Evaluation Criteria and Rubrics

The following are the evaluation criteria for this lab that students must perform:

1. Harden Linux server services when enabling and installing them, and keep a security perspective during configuration – [**20%**]
2. Perform basic security configurations to ensure that the system has been hardened before hosting a Web site – [**20%**]
3. Configure and perform basic security for a MySQL database, understanding the ramifications of a default installation and recommending hardening steps for the database instance – [**20%**]
4. Set up and perform basic security configuration for Sendmail to be able to leverage the built-in messaging capabilities of the Linux system – [**20%**]
5. Enable and implement secure SSH for encrypted remote access over the network or across the Internet of a Linux server system – [**20%**]

Lab #5 – Assessment Worksheet

Hardening Security for Linux Services and Applications

Course Name and Number: _____

Student Name: _____

Instructor Name: _____

Lab Due Date: _____

Overview

This lab was an extension of previous labs. It incorporated security hardening for Linux services and applications loaded in the physical server. In this lab, you configured security and hardened services and applications to ensure the confidentiality, integrity, and availability of those services. You configured and secured an Apache Web server and MySQL database and the components necessary to harden the security implementation of both. You also configured the Sendmail application for secure local messaging and enabled secure, encrypted remote access using Secure Shell (SSH).

Lab Assessment Questions & Answers

1. When configuring services, what Linux directory typically contains server configuration files?

   Introduction. The /etc directory

2. What is a Linux runlevel for a specific service or application? Which command allows you to define the runlevel uniquely for a service or application?

   Note introducing Part 1. Runlevels define the state of the Linux server upon bootup. Defining runlevels helps define access control parameters for users or system administrators to access the service or application uniquely.

   "chkconfig"
   Part 1, Step 15. chkconfig --level 3 mysqld
   Part 2, Step 1. chkconfig --level 3 httpd
   Part 3, Step 1. chkconfig --level 3 sendmail

3. What is the Apache Web server? Review the /etc/httpd/conf/httpd.conf configuration file, and point out a setting that could enhance security.

   Note introducing Part 2. The Apache Web server is an open source HTTP server that can run on *nix based and Windows operating systems.

   (Answers to the second question will be unique to each student; however, one option is decreasing timeout settings to help prevent against denial of service.)

4. OpenSSH is the de facto method used to remotely access Linux systems. Explain why the use of telnet is discouraged.

   Note introducing Part 4. Secure Shell (SSH) is an encrypted remote command-line login, and ensures confidentiality in remote access and login by system administrators. Telnet was the predecessor to SSH. It sends remote access and login unencrypted in cleartext and therefore can be compromised easily by a hacker if the IP packets are sniffed and captured.

5. What are symbolic links?

   Note following Part 1, Step 10. Symbolic links are a special type of file that contains a reference to another file or directory in the form of an absolute or relative path and that affects pathname resolution.

6. Why is it recommended to disable symbolic links in MySQL?

   Note following Part 1, Step 10. Because some MySQL statements work by creating a temporary file in the database directory and replacing the original file with the temporary file when the statement operation is complete, this could create several security risks.

7. Why would you add the skip-networking command in MySQL?

   Note following Part 1, Step 10. This prevents remote connections (including attacks) to the MySQL DB but will still allow localhost connections via the mysql.sock socket.

Lab #6 Hardening Security by Controlling Access

Introduction

This lab is an extension of the previous labs, and it incorporates access control for the CentOS Linux Server. CentOS has a powerful built-in firewall commonly referred to as IPtables or Netfilter. The most common way to configure IPtables is through the command line. There are some GUI front-ends for IPtables, though they often lack flexibility. You will use the command line configuration in this lab.

IPtables can be thought of as predefined chains or rules that are read from top to bottom which allow access or deny access to specific protocols (TCP, UDP, ICMP) and ports. The first match found in the chain will be processed, so it is important where you place rules. Best practice recommends a default policy to first refuse (DROP) all packets and add specific rules to allow (ACCEPT) acceptable packets.

An additional layer of security can be implemented on a Linux server in the form of TCP Wrappers. Installed by default on CentOS servers, TCP Wrappers provides controlled access using the hosts.allow and hosts.deny files that allow connection to "wrapped" network services after the packet has passed the IPtables firewall. TCP Wrappers reads the hosts.allow (/etc/hosts) file before reading the hosts.deny file. Therefore, if a match is found in the hosts.allow before it reads the hosts.deny rule, the allow rule will be processed.

For example, when a connection attempt is made to a TCP wrapped service, such as SSH, the hosts.allow file is accessed to determine whether the client has an allowed rule. Should the rule not exist in either file or the file is not present, the request is automatically permitted. Rules permitting or denying are read in chronological order beginning with the hosts.allow file therefore placement of rules are of extreme importance.

In this lab, you will first review current host-based IP firewall services, flush the current firewall configuration, and then reconfigure it with stringent permit/deny rule sets. You also will configure TCP Wrappers for unauthorized access controls and logging. Finally, you will configure SELinux for an additional layer of security. This lab has four parts, which should be completed in the order specified.

1. In the first part of the lab, you will enable iptables to help lock down services on a Linux system to permit HTTP, ICMP Ping, and SSH access and deny all other unnecessary access.

2. In the second part of the lab, you will add an additional layer of security of the system by configuring TCP Wrappers to deny and log unauthorized attempts to access services on the system.

3. In the third part of the lab, you will confirm SELinux is enabled and modify some of the default settings.

4. Finally, if assigned by your instructor, you will explore the virtual environment on your own to answer a set of challenge questions that allow you to use the skills you learned in the lab to conduct independent, unguided work, similar to what you will encounter in a real-world situation.

Learning Objectives

Upon completing this lab, you will be able to perform the following:

- Review current internal host-based firewall parameters and configuration settings to verify allowed and denied IP communications
- Configure an internal host-based firewall using iptables and create stringent allow/deny rules for services that may require access to the system over the network
- Harden the system by enabling TCP Wrappers to deny and log unauthorized attempts against services and ports running on the system
- Secure processes running on the system by using and configuring SELinux to help perform more in-depth layered security
- Verify configurations of the settings applied by connecting to the Linux server using SSH and connect to other services running on a Linux server

Tools and Software

The following software and/or utilities are required to complete this lab. Students are encouraged to explore the Internet to learn more about the products and tools used in this lab.

- None

Deliverables

Upon completion of this lab, you are required to provide the following deliverables to your instructor:

1. Lab Report file including screen captures of the following steps: Part 1, Steps 14 and 16; Part 2, Step 18; Part 3, Steps 3, 5, and 16;
2. Lab Assessments file;
3. Optional: Challenge Questions file, if assigned by your instructor.

Hands-On Steps

▶Note:
This lab contains detailed lab procedures, which you should follow as written. Frequently performed tasks are explained in the Common Lab Tasks document on the vWorkstation desktop. You should review these tasks *before* starting the lab.

1. From the vWorkstation desktop, **open** the **Common Lab Tasks file**.

   If you desire, use the File Transfer button to transfer the file to your local computer and print a copy for your reference.

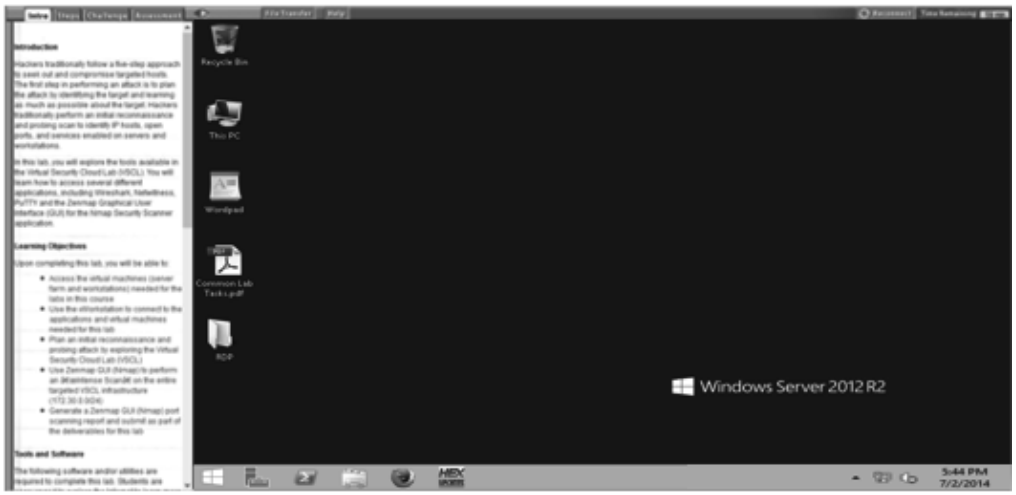


Figure 1 "Student Landing" vWorkstation

2. On your local computer, **create** the **lab deliverable** files.

3. **Review** the **Lab Assessment Worksheet** at the end of this lab. You will find answers to these questions as you proceed through the lab steps.

Part 1: Harden the Linux-based IP Firewall

▶Note:
In the next steps, you will harden security measures for the Linux host-based IP firewall by configuring stringent permit and deny rule sets. You will append the INPUT, OUTPUT, and FORWARD chains to permit HTTP, ICMP Ping, and SSH access and deny all other access. You can view the network port information of your IPtables by using the –v (verbose) switch. For example, iptables –L –v will list the rules and port information.

1. **Double-click** the **RDP folder** on the vWorkstation desktop to open the folder.

2. **Double-click** the **TargetCentOS01.rdp file** to start a remote desktop connection to that machine.

   The remote GNOME desktop, the graphical user interface (GUI) for the virtual Linux server, opens with the IP address of the remote machine (172.30.0.21) in the title bar at the top of the window.

3. **Double-click** the **Terminal icon** on the GNOME desktop to open the terminal emulator and access the Linux server command line.

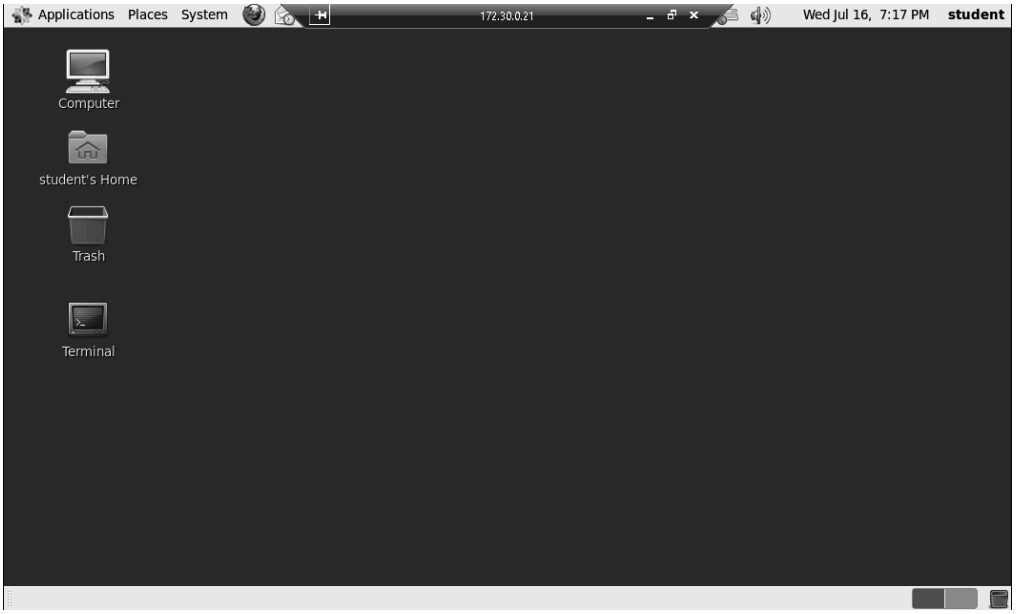


Figure 2 GNOME desktop

4. At the command prompt, **type sudo /sbin/iptables -L** and **press Enter** to list the current host-based firewall rules.

5. When prompted for a password, **type pass=7890** and **press Enter**.

   The system returns a list of the existing INPUT, OUTPUT, and FORWARD chains indicating that there are no firewall rules set for any of them.

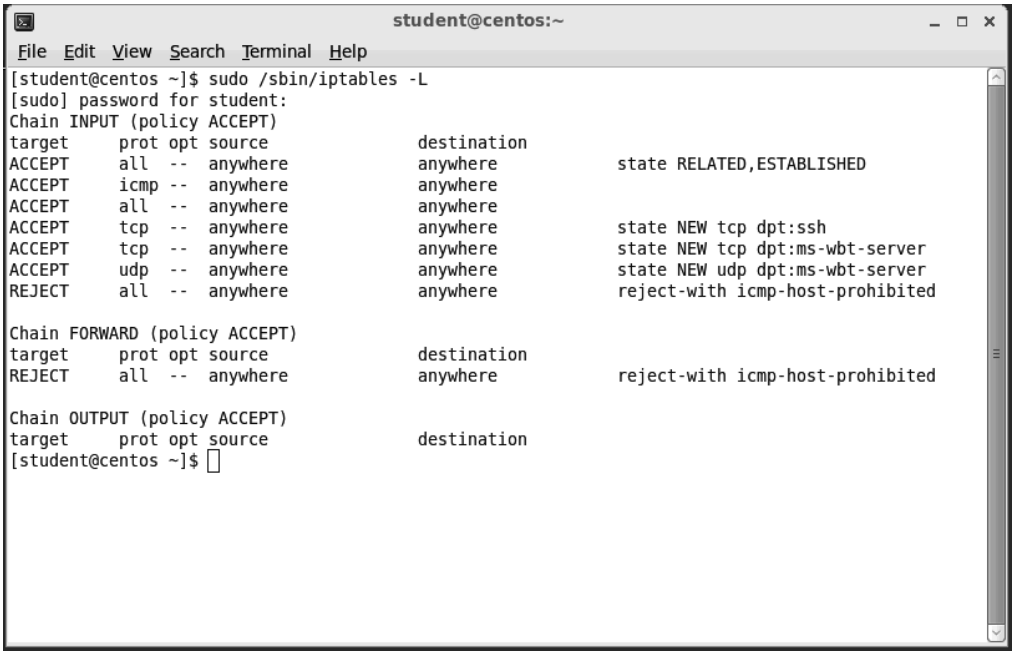


Figure 3 Existing INPUT, OUTPUT and FORWARD chains

6. At the command prompt, **type sudo /sbin/iptables -I** (capital i) **INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT** and **press Enter** to add a new firewall rule that allows INPUT chains to the firewall rules and allow established connections.

7. At the command prompt, **type sudo /sbin/iptables -A INPUT -p tcp --dport 80 -j ACCEPT** and **press Enter** to add a new firewall rule that allows INPUT chains to the firewall rules and allow http (Web) access.

8. At the command prompt, **type sudo /sbin/iptables -A INPUT -p tcp --dport 443 -j ACCEPT** and **press Enter** to add a new firewall rule that allows INPUT chains to the firewall rules and allow https (SSL) access.

9. At the command prompt, **type sudo /sbin/iptables -A INPUT -p tcp --dport 22 -j ACCEPT** and **press Enter** to add a new firewall rule that allows INPUT chains to the firewall rules and allow secure shell (SSH) connections.

10. At the command prompt, **type sudo /sbin/iptables -A INPUT -p icmp -j ACCEPT** and **press Enter** to add a new firewall rule that allows INPUT chains to the firewall rules and allow ICMP pings.

11. At the command prompt, **type sudo /sbin/iptables -A INPUT -p all -j DROP** and **press Enter** to add a new firewall rule that denies all other traffic from the INPUT chains.

12. At the command prompt, **type sudo /sbin/service iptables save** and **press Enter** to save the rule set you just created.

    The system returns OK flag indicating that the rules have been saved.

13. **Make a screen capture** of the terminal window showing the results of the iptables save command and **paste** it into a new text document.

14. At the command prompt, **type sudo /sbin/iptables -L** and **press Enter** to list the newly saved firewall rules. The system returns a list of the existing INPUT, OUTPUT, and FORWARD chains including the new firewall rules you created in this lab.

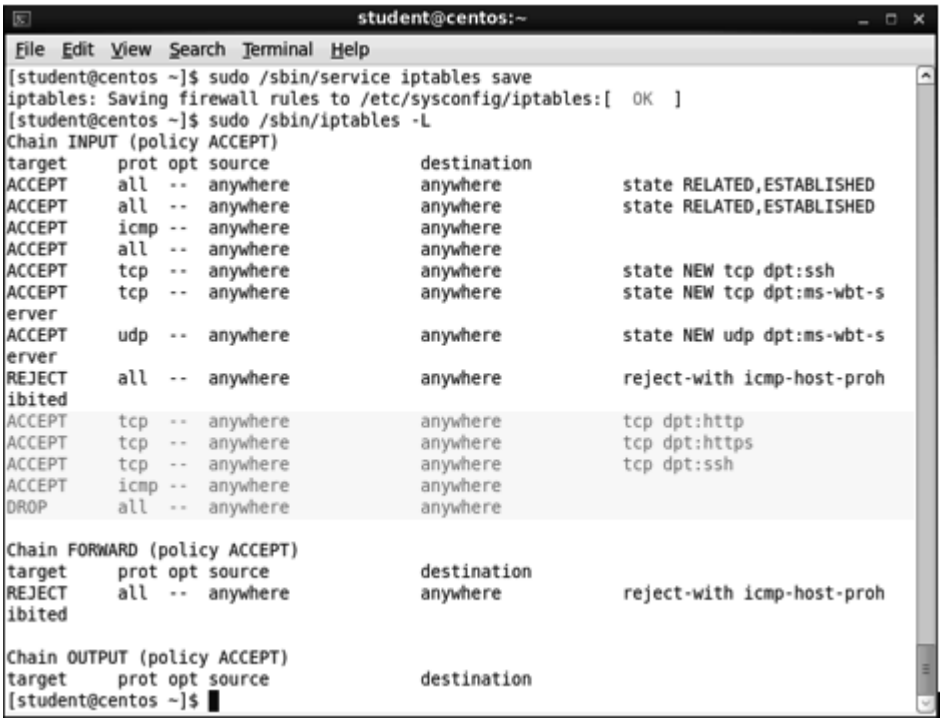


Figure 4 New firewall rules for the INPUT chain

15. **Make a screen capture** showing the **output of the iptables -L command** and **paste** it into the Lab Report file.

Part 2: Configure TCP Wrappers

▶Note:
In the next steps, you will harden security measures on this server by configuring the TCP Wrappers to deny and log all connection attempts from a particular domain (.hackers.com). You will modify the hosts.deny configuration file to deny access to the .hackers.com domain and then you will modify the hosts file to enable to the TargetCent0S server to appear to other servers as if it is coming from the .hackers.com domain. Finally, you will attempt to establish an SSH connection to verify your changes to the hosts.deny file.

1. At the command prompt, **type su -c 'vi /etc/hosts.deny'** and **press Enter** to open the hosts.deny configuration file in the vi Editor.

2. When prompted, **type P@ssw0rd!**, the root password, and **press Enter** to create the new account.

▶Note:
You are required to enter a mixed-case password. If you are not using the Citrix Receiver to access this lab, please use the CAPS LOCK button or the On-Screen Keyboard to input the password.

3. **Press** the **i key** to enter the Insert mode.

4. Use the arrow keys to **locate** the last # line in the file, **delete** the **# symbol** from the beginning of the line and **type ALL : .hackers.com:severity emerg** to create a new line.

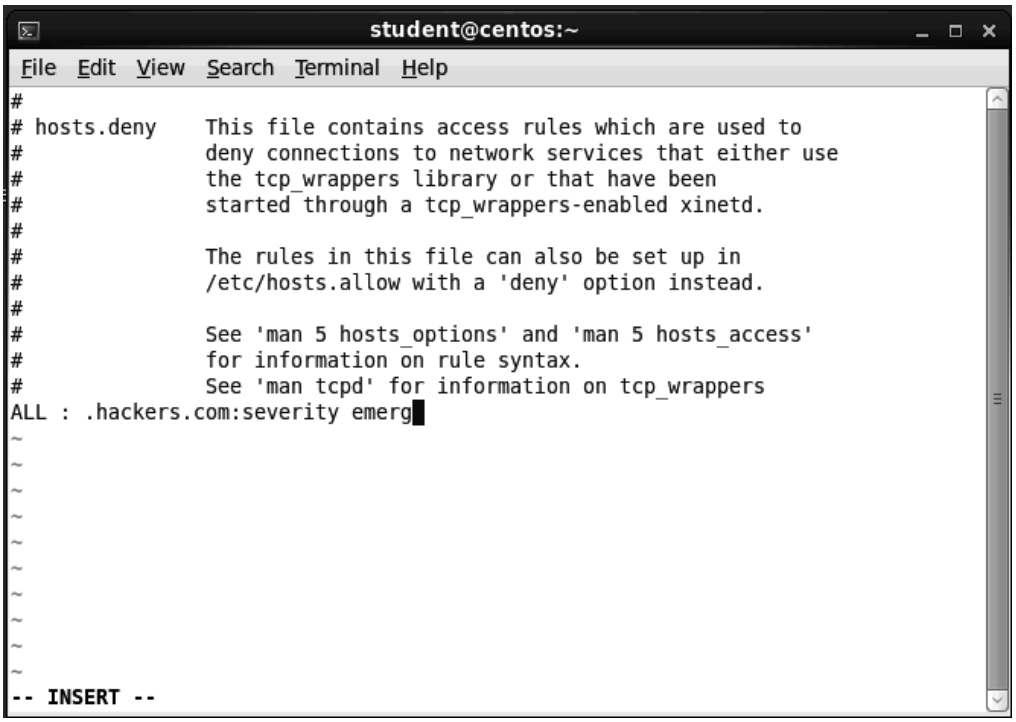


Figure 5 Modify the hosts.deny file

5. **Press** the **Esc key** to exit the Insert mode.

6. **Type :wq!** and **press Enter** to save your changes and exit the vi Editor.

▶Note:
The /etc/hosts file keeps a map of IP addresses and aliases of any computers with which it communicates. In the next steps, you will first identify the IP address for the TargetCentOS machine and then you will modify the /etc/hosts file to map that IP address with the .hackers.com domain that you denied in the previous steps.

7. At the command prompt, **type /sbin/ifconfig eth0** and **press Enter** to find the IP address (*inet addr*) for the eth0 server.

8. In the Lab Report file, **document** the IP address (*inet addr)* you find in the eth0 section. You will need it in a later step.

9. At the command prompt, **type su -c 'vi /etc/hosts'** and **press Enter** to open the hosts file in the vi Editor.

10. When prompted, **type P@ssw0rd!**, the root password, and **press Enter**.

▶Note:
You are required to enter a mixed-case password. If you are not using the Citrix Receiver to access this lab, please use the CAPS LOCK button or the On-Screen Keyboard to input the password.

11. **Press** the **i key** to enter the Insert mode.

12. Use the arrow keys to **locate** the **IP address** you documented in step 8, **move** the **cursor** immediately after that IP address, and **type *yourname*.hackers.com**, replacing *yourname* with your own name, to specify the first hostname for this IP address.

    This change will allow the TargetCentOS01 machine to emulate a computer (with your own name) from the restricted hackers.com domain.

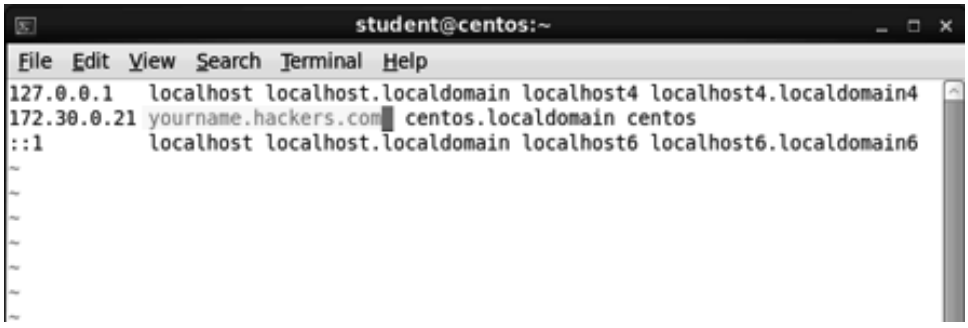


Figure 6 Modify the hosts file

13. **Press** the **Esc key** to exit the Insert mode.

14. **Type :wq!** and **press Enter** to save your changes and exit the vi Editor.

15. At the command prompt, **type sudo /sbin/service sshd status** and **press Enter** to verify that the SSH service is running.

16. When prompted for a password, **type pass=7890** and **press Enter**.

    The system will return a message indicating that the service is running.

    - If the service is running, **skip** to the next step.
    - If the system returns a Failed flag indicating that the service is not running, **repeat steps 15 and 16** until you receive an OK flag indicating that the service is running.

17. At the command prompt, **type ssh centos** and **press Enter** to attempt an SSH connection from the host address that you just entered in the hosts file.

    The system will return a *refused connect* message indicating that *yourname*.hackers.com is being denied access.

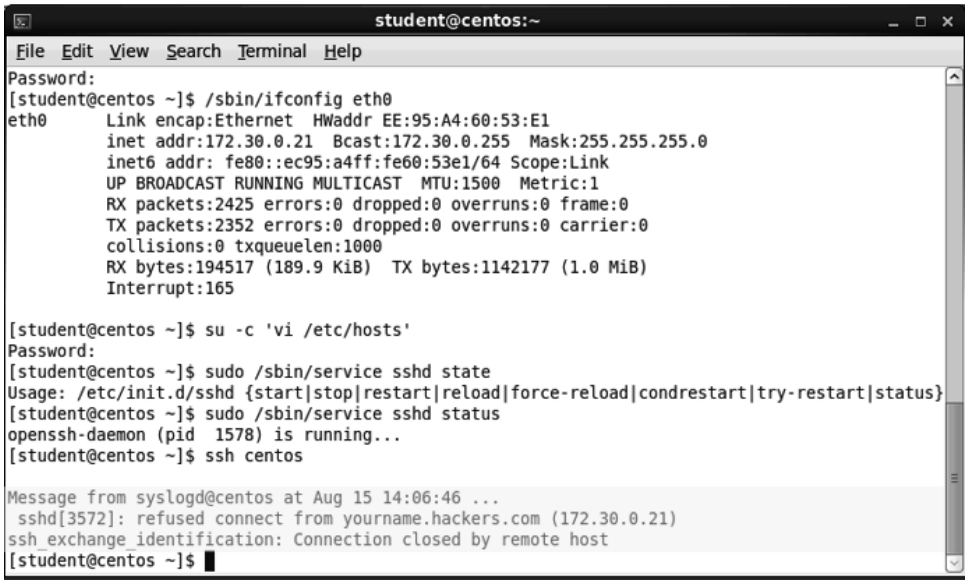


Figure 7 Attempt to connect as yourname.hackers.com

18. **Make a screen capture** showing the **hosts.deny file's output in response to your attempt to connect** and **paste** it into the Lab Report file.

Part 3: Modifiy the SELinux Configuration File

▶Note:
In the next steps, you will harden security measures on this server by verifying that the SELinux configuration file (selinux/config) is set to enforcing mode upon boot or reboot to ensure layered security solutions.

When first installed, SELinux has three possible modes.

- **Permissive mode** will log system access or alert, but not enforce any policies.
- **Disable mode** indicates that SELinux isn't running or logging.
- **Enforcing mode** will block access as defined in the policy.

You also will modify the Boolean settings for the Web server to allow the http server to send email and make use of an NFS share.

1. At the command prompt, **type cat /etc/selinux/config** and **press Enter** to display the SELinux configuration file.

2. Use the arrow keys to **locate** the **SELINUX= command** to verify that it is set to enforcing mode.

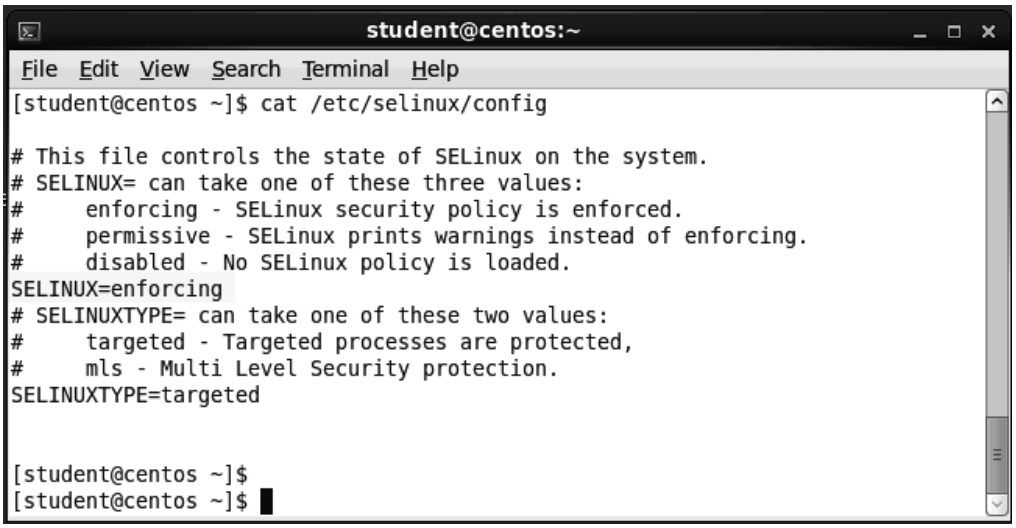


Figure 8 Review the selinux/config file

3. **Make a screen capture** showing the **SELinux mode from the config file** and **paste** it into the Lab Report file.

4. At the command prompt, **type /usr/sbin/sestatus** and **press Enter** to check the current mode for the SELinux status.

   In the output results, the *current mode* and *mode from the config file* both should be set to *enforcing*.

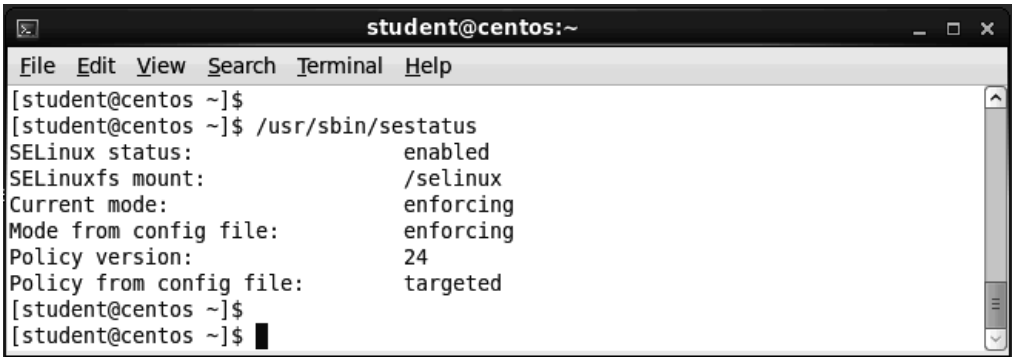


Figure 9 SELinux status

5. **Make a screen capture** showing the **SELinux status output** and **paste** it into the Lab Report file.

6. At the command prompt, **type sudo /sbin/service httpd status** and **press Enter** to check the status of httpd service.

7. When prompted for a password, **type pass=7890** and **press Enter**.

   The system returns a message indicating that the httpd service is stopped.

8. At the command prompt, **type sudo /sbin/service httpd start** and **press Enter** to start the httpd (Web) service.

   The system will return an OK flag indicating that the service is running.

9. At the command prompt, **type ps -ZC httpd** and **press Enter** to view the SELinux setting to see which Web processes are currently protected.

   The system returns a list of processes under the label *unconfined_u:system_r:httpd_t*.

10. At the command prompt, **type /usr/sbin/getsebool -a | grep http** and **press Enter** to view the Boolean settings for the Web server type.

    The system returns a list of settings for this type, including the following settings that you will modify during the next steps of this lab.

    - **httpd_can_sendmail - -> off** (prohibits the Web server from sending email)
    - **httpd_use_nfs - -> off** (prohibits the Web server from connecting to a remote NFS share)

11. At the command prompt, **type su -c '/usr/sbin/setsebool -P httpd_can_sendmail 1'** and **press Enter** to change the settings to allow the Web server to send mail.

12. When prompted, **type P@ssw0rd!**, the root password, and **press Enter**.

    This command may take a few moments to re-label. Do not press any keys until the command prompt returns.

▶Note:
You are required to enter a mixed-case password. If you are not using the Citrix Receiver to access this lab, please use the CAPS LOCK button or the On-Screen Keyboard to input the password.

13. At the command prompt, **type su -c '/usr/sbin/setsebool -P httpd_use_nfs 1'** and **press Enter** to change the settings to allow the Web server to connect to a remote NFS share.

14. When prompted, **type P@ssw0rd!**, the root password, and **press Enter**.

    This command may take a few moments to relabel. Do not press any keys until the command prompt returns.

▶Note:
You are required to enter a mixed-case password. If you are not using the Citrix Receiver to access this lab, please use the CAPS LOCK button or the On-Screen Keyboard to input the password.

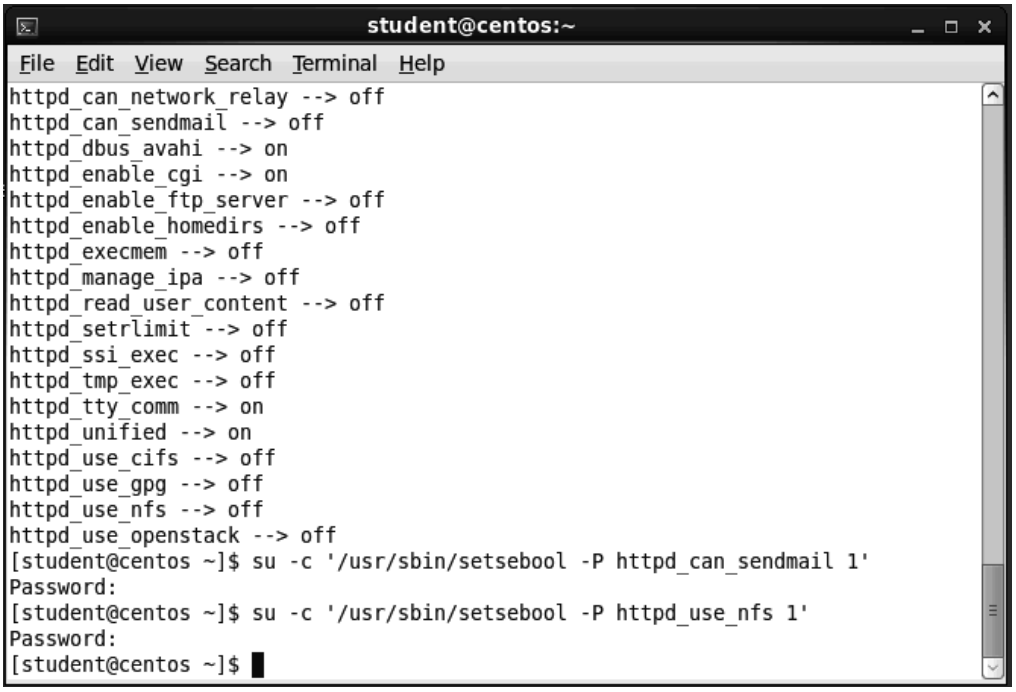


Figure 10 Modify the Web server settings

15. At the command prompt, **type /usr/sbin/getsebool -a | grep http** and **press Enter** to view the Boolean settings for the Web server type *after* having made the edits in the previous steps.

    The system returns a list of settings for this type, including the following settings that you have already modified during this lab.

    - **httpd_can_sendmail - -> on** (allows the Web server from sending email)
    - **httpd_use_nfs - -> on** (allows the Web server from connecting to a remote NFS share)

    If your results do not match this list, **repeat steps 11-15** until they do.

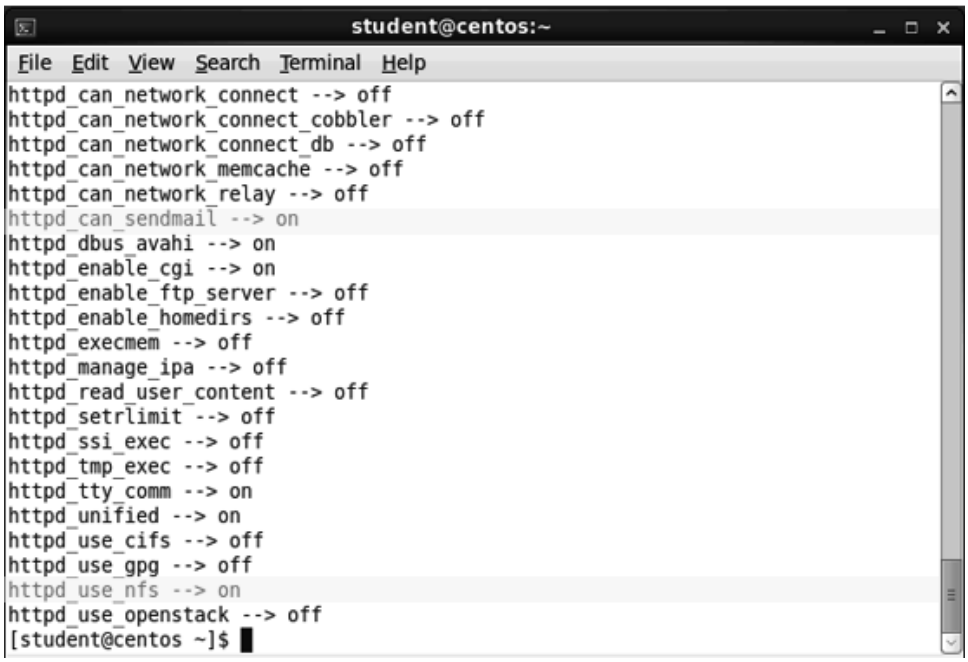


Figure 11 Modified Web server settings

16. **Make a screen capture** showing **your changes to the Boolean settings for the Web server type** and **paste** it into the Lab Report file.

17. **Close** the **remote Linux connection**.

18. **Close** the **virtual lab**, or proceed with Part 4 to answer the challenge question for this lab.

Part 4: Challenge Question

▶Note:
The following challenge question is provided to allow independent, unguided work, similar to what you will encounter in a real situation. You should aim to improve your skills by getting the correct answer in as few steps as possible. Use screen captures in your lab document where possible to illustrate your answers.

1. From your local computer with Internet access, research *SELinux Access control* to find the three forms of access control and their definitions. Record your findings in the Challenge Questions file. Don't forget to cite your references.

   (Answers will be unique to each student, but should include the following three forms of SELinux access control.)

   - **Type Enforcement (TE):** Type Enforcement is the primary mechanism of access control used in the targeted policy
   - **Role-Based Access Control (RBAC):** Based around SELinux users (not necessarily the same as the Linux user), but not used in the default targeted policy
   - **Multi-Level Security (MLS):** Not commonly used and often hidden in the default targeted policy.

▶Note:
This completes the lab. **Close** the **virtual lab**, if you have not already done so.

Evaluation Criteria and Rubrics

The following are the evaluation criteria for this lab that students must perform:

1. Review current internal host-based firewall parameters and configuration settings to verify allowed and denied IP communications – [**20%**]
2. Configure an internal host-based firewall using IPtables and create stringent allow/deny rules for services that may require access to the system over the network – [**20%**]
3. Harden the system by enabling TCP Wrappers to deny and log unauthorized attempts against services and ports running on the system – [**20%**]
4. Secure processes running on the system by using and configuring SELinux to help perform more in-depth layered security – [**20%**]
5. Verify configurations of the settings applied by connecting to the Linux server using SSH and connect to other services running on a Linux server – [**20%]**

Lab #6 – Assessment Worksheet

Hardening Security by Controlling Access

Course Name and Number: _____

Student Name: _____

Instructor Name: _____

Lab Due Date: _____

Overview

In this lab, you first reviewed current host-based IP firewall services, flushed the current firewall configuration, and then reconfigured it with stringent permit/deny rule sets. You also configured TCP Wrappers for unauthorized access controls and logging. Finally, you configured SELinux for an additional layer of security.

Lab Assessment Questions & Answers

1. Suppose the domain hackers.com is denied for all services in the hosts.deny, but the hosts.allow file has the rule ALL:ALL. Will TCP Wrappers allow hackers.com access?

   Introduction. Yes. TCP Wrappers reads the hosts.allow (/etc/hosts) file before reading the hosts.deny file. Therefore, if a match is found in the hosts.allow before it reads the hosts.deny rule, the allow rule will be processed.

2. What is the command to check the SELinux status? How can you be sure that SELinux is in enforcing mode?

   Part 3, Step 4. **/usr/sbin/sestatus**. In the output results, the *current mode* and *mode from the config file* both should be set to *enforcing*.

3. What are three modes of SELinux? Explain their basic functionality.

   Note introducing Part 3.
   - **Permissive mode** will log system access or alert, but not enforce any policies.
   - **Disable mode** indicates that SELinux isn't running or logging.
   - **Enforcing mode** will block access as defined in the policy.

4. Based on your understanding of the IPtables rules you established in Part 1 of this lab, what command would you type to drop any Telnet (port 23) connection attempts?
   Part 1. **sudo /sbin/iptables – A INPUT – dport 23 –j DROP**

5. Based on your understanding of the IPtables rules you established in Part 1 of this lab, what command would you type to allow traffic on the lookback (lo)?

   Part 1. **sudo /sbin/iptables –I INPUT 1 –I lo –j ACCEPT**

6. What switch would you use to view the network port configuration for the IPtables?

   Note introducing Part 1. You can view the network port information of your IPtables by using the –v (verbose) switch. For example, iptables –L –v will list the rules and port information.

7. What is the purpose of the /etc/hosts file?

   Note following Part 2, Step 6. The /etc/hosts file keeps a map of IP addresses and aliases of any computers with which it communicates.

8. Is the order of the rules in the IPtables important?

   Introduction. Yes. The first match found in the chain will be processed, so it is important where you place rules. Best practice recommends a default policy to first refuse (DROP) all packets and add specific rules to allow (ACCEPT) acceptable packets.

9. If either the hosts.deny or the hosts.allow file does not exist, what happens?

   Introduction. Should the rule not exist in either file or the file is not present, the request is automatically permitted.

Lab #7 Hardening Security for the Linux Kernel

Introduction

This lab is an extension of the previous labs and it incorporates security hardening for the Linux kernel with security parameters. The kernel is the core, or base component, of the operating system (OS) and consists of program code that runs and manages all other code and resources. It is important to protect the system kernel from vulnerabilities and potential attacks by applying hardened security measures at a kernel level.

The sysctl.conf file is a simple, human-readable file that contains values used by the system upon bootup. A security administrator should understand that modifying the values defined in this file can help tune the kernel against many forms of attacks. Further, system hardening can also be performed by going through the system and removing any system modules that are unnecessary for the performance expected of the server.

Often, changes at the kernel level require a system reboot to take effect, which means that security demands may conflict with a service level agreement. In these cases, it is necessary to tune the kernel while it is already up and running. The sysctl command enables a security administrator to configure a setting or parameter dynamically on the system.

In this lab, you will view and tune all kernel parameters and discover information regarding the current Loadable Kernel Modules (LKMs) and about the kernel itself. You will explore the sysctl.conf file and make modifications to system settings. Finally, you also will enable and interpret the results of the lsmod command.

This lab has four parts, which should be completed in the order specified. There is no challenge question for this lab.

1. In the first part of the lab, you will look at the current kernel setting and persistent setting for syncookies. You will also modify and then restore the current running setting.
2. In the second part of the lab, you will use to the sysctl command to set the maximum simultaneous files a user can open.
3. In the third part of the lab, you will explore various system kernel settings related to the processes, filesystems, and modules.
4. In the fourth part of the lab, you will add and then remove a kernel module.

Learning Objectives

Upon completing this lab, you will be able to:

- Review and tune the kernel parameters on a CentOS Linux Server for security and monitoring purposes
- Produce kernel versions and loaded options for a better understanding of how the system is configured and to identify potential security vulnerabilities in the CentOS Linux Server
- Examine the /etc/sysctl.conf file and adjust tcp_sysncookies settings to configure secure options for users on a CentOS Linux Server
- Review and assess the Loaded Kernel Modules (LKMs) of the target Linux system and provide recommendations on the output and current running configuration
- Use and interpret the lsmod command output and perform security hardening configurations on the CentOS Linux Server

Tools and Software

The following software and/or utilities are required to complete this lab. Students are encouraged to explore the Internet to learn more about the products and tools used in this lab.

- None

Deliverables

Upon completion of this lab, you are required to provide the following deliverables to your instructor:

1. Lab Report file including screen captures of the following steps: Part 1, Steps 9 and 15; Part 2, Step 3; Part 3, Steps 2, 4, 6, 8, and 10; Part 4, Steps 2 and 6;
2. Lab Assessments file.

Hands-On Steps

▶Note:
This lab contains detailed lab procedures, which you should follow as written. Frequently performed tasks are explained in the Common Lab Tasks document on the vWorkstation desktop. You should review these tasks *before* starting the lab.

1. From the vWorkstation desktop, **open** the **Common Lab Tasks file**.

   If you desire, use the File Transfer button to transfer the file to your local computer and print a copy for your reference.

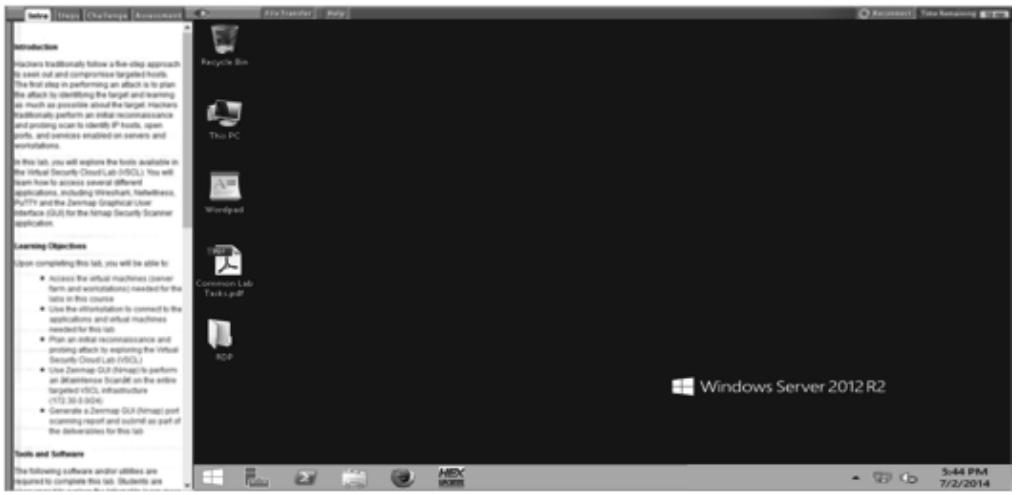


Figure 1 "Student Landing" vWorkstation

2. On your local computer, **create** the **lab deliverable files**.

3. **Review** the **Lab Assessment Worksheet** at the end of this lab. You will find answers to these questions as you proceed through the lab steps.

Part 1: Enable SYN Cookies

▶Note:
To establish a connection, TCP uses a three-way handshake to communicate: SYN (the client requests a connection), SYN-ACK (the server acknowledges the client), and ACK (the client acknowledges the server). In a SYN flood attack, the attacker sends multiple SYN requests, but spoofs the IP address in the SYN packet so that the server cannot send a SYN-ACK reply and the connections cannot be closed. Handling these fake requests can tie up server resources and deny service to legitimate users. SYN cookies are the key element of a technique used to guard against SYN flood denial-of-service attacks.

In the next steps, you will confirm that the net.ipv4.tcp_syncookies are enabled by viewing the system control configuration (sysctl.conf) file. You will also change current running kernel parameters on the system.

1. **Double-click** the **RDP icon** on the desktop. This folder contains links to the virtual servers in this lab environment.

2. **Double-click** the **TargetCentOS01.rdp file** to open the Linux server.

   The remote GNOME desktop, the graphical user interface (GUI) for the virtual Linux server, opens with the IP address of the remote machine (172.30.0.21) in the title bar at the top of the window.

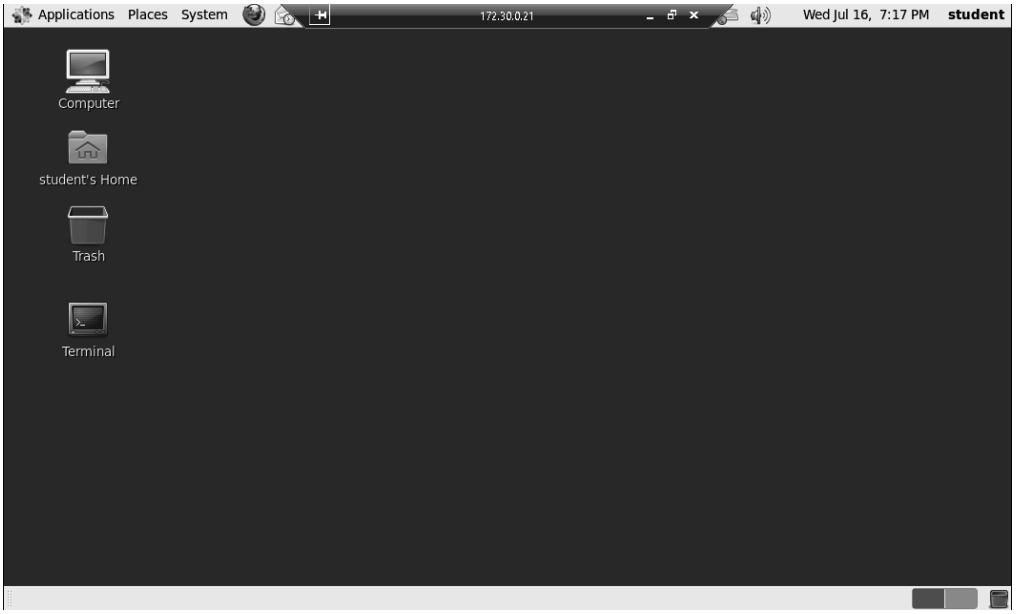


Figure 2 GNOME desktop

3. **Double-click** the **Terminal icon** on the GNOME desktop to open the terminal emulator and access the Linux server command line.

4. At the command prompt, **type cat /etc/sysctl.conf | less** and **press Enter** to view the current settings for the running kernel.

   The system returns a list of the preset configuration. Use the arrow keys to review these settings.

5. Use the arrow keys to **locate** the **net.ipv4.tcp_syncookies = 1 line** in the file.

   A value of 1 indicates that syncookies is enabled. If it was set to 0, *disabled*, the server would be vulnerable to SYN flood attacks. An edit to this file will not cause the setting to take effect until the next time the server is rebooted.

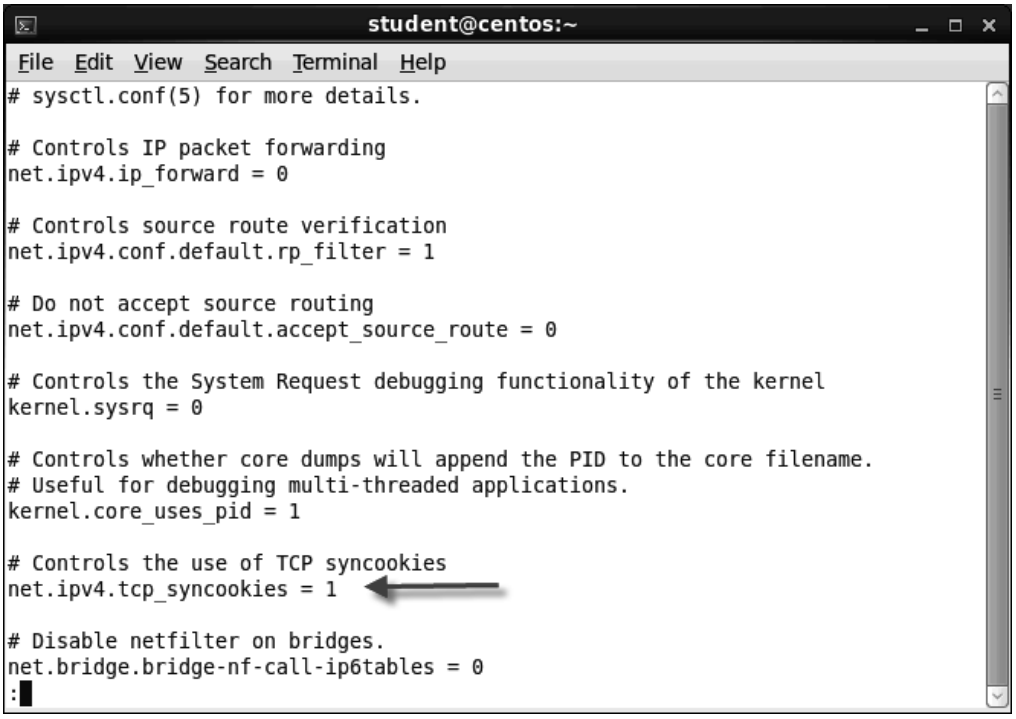


Figure 3 Verify tcp_syncookies is enabled

6. **Make a screen capture** showing the **current syncookies setting in the sysctrl.conf** and **paste** it into the Lab Report file.

7. **Type q** to exit the current view and return to the command prompt.

8. At the command prompt, **type cat /proc/sys/net/ipv4/tcp_syncookies** and **press Enter** to view the current running kernel parameters.

   Again, the system returns a value of 1, indicating that syncookies is enabled.

Figure 4 Verify syncookies is enabled

▶Note:
In the next steps, you will verify that tcp_syncookies is enabled. You will practice making a dynamic change to the kernel without waiting for a system reboot by first disabling, and then re-enabling, this option. Because you are not rebooting the server at this time, the change will be temporary. The file will revert to its original setting (enabled) upon a system reboot. If you wanted to make a permanent setting change, you would open the /etc/sysctl.conf file with a file editor such as vi Editor, edit the setting, and then reboot the server.

9. At the command prompt, **type su -c ' echo "0" > /proc/sys/net/ipv4/tcp_syncookies '** and **press Enter** to change the kernel settings for syncookies without waiting for a reboot.

   The setting will revert to what is in the sysctl.conf file if the system were rebooted.

10. When prompted, **type P@ssw0rd!**, the root password, and **press Enter**.

▶Note:
You are required to enter a mixed-case password. If you are not using the Citrix Receiver to access this lab, please use the CAPS LOCK button or the On-Screen Keyboard to input the password.

11. At the command prompt, type **cat /proc/sys/net/ipv4/tcp_syncookies** and **press Enter** to verify the current kernel parameters are disabled.

12. **Make a screen capture** showing the **current running kernel syncookies setting** and **paste** it into the Lab Report file.

13. At the command prompt, **type su -c ' echo "1" > /proc/sys/net/ipv4/tcp_syncookies '** and **press Enter** to change the kernel settings for syncookies without waiting for a reboot.

    The above command turns syncookies on. The setting will revert to what is in the sysctl.conf file if the system were rebooted.

14. When prompted, **type P@ssw0rd!**, the root password, and **press Enter**.

▶Note:
You are required to enter a mixed-case password. If you are not using the Citrix Receiver to access this lab, please use the CAPS LOCK button or the On-Screen Keyboard to input the password.

Part 2: Change System Parameters

▶Note:
Another common type of attack is when a hacker gains user level access to a system and forces that user account to endlessly create or open files until the server runs out of resources. In the next steps, you will use the sysctl command to change the maximum number of files users can open simultaneously. This security measure can limit the amount of the server's resources a user account can consume.

1. At the command prompt, **type /sbin/sysctl -a | less** and **press Enter** to all available parameters for the running kernel.

   The system returns a list of the available kernel parameters. Piping the output into the less program allows you to view the output using the arrow keys to move forward and backward with the file.

2. Use the arrow keys to **locate** the **fs.file-max line** in the resulting list.

3. **Make a screen capture** showing the **current fs.file-max setting** and **paste** it into the Lab Report file.

4. **Type q** to exit this view and return to the command prompt.

5. At the command prompt, **type su -c ' /sbin/sysctl -w fs.file-max=100000 '** and **press Enter** to change the maximum number of files the user can open at one time to 100,000.

6. When prompted, **type P@ssw0rd!**, the root password, and **press Enter**.

▶Note:
You are required to enter a mixed-case password. If you are not using the Citrix Receiver to access this lab, please use the CAPS LOCK button or the On-Screen Keyboard to input the password.

Part 3: Explore Kernel Settings

▶Note:
In the next steps, you will use the cat command to discover information about the processes, filesystems, modules, and other details about the current running kernel to identify security-hardening measures.

1. At the command prompt, **type cat /proc/filesystems** and **press Enter** to find what types of filesystems are supported by the kernel.

   The nodev (no device) indicates the filesystem is not associated with a physical device.

2. **Make a screen capture** showing the **output of this command** and **paste** it into the Lab Report file. You may have to take multiple screen captures or expand the terminal window to display the entire output.

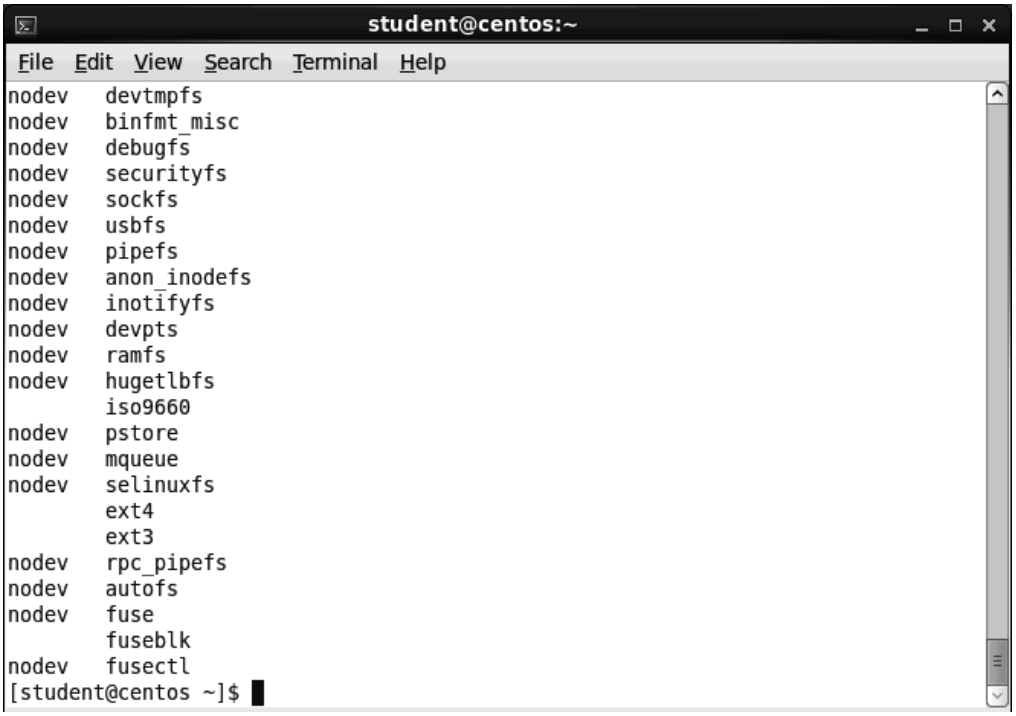


Figure 5 Output from the cat /proc/filesystems command

3. At the command prompt, **type cat /proc/modules** and **press Enter** to find what modules the kernel is loading.

4. **Make a screen capture** of this output and **paste** it into the Lab Report file. You may have to take multiple screen captures to display the entire output.

5. At the command prompt, **type cat /proc/version** and **press Enter** to find what version of the kernel is currently running.

6. **Make a screen capture** showing the **output of this command** and **paste** it into the Lab Report file.

7. At the command prompt, **type cat /proc/cpuinfo** and **press Enter** to find information about the CPU.

8. **Make a screen capture** of this output and **paste** it into the Lab Report file. You may have to take multiple screen captures to display the entire output.

9. At the command prompt, **type cat /proc/meminfo** and **press Enter** to find out what processes are running in memory.

10. **Make a screen capture** showing the **output of this command** and **paste** it into the Lab Report file. You may have to take multiple screen captures to display the entire output.

Part 4: Secure Kernel Modules

▶Note:
In the next steps, you will harden security measures on this server by removing unused modules. First, you will use the lsmod command to list the modules currently loaded in the kernel. You will then add a module and then remove it.

1. At the command prompt, **type /sbin/lsmod** and **press Enter** to list the loaded modules.

   The system returns a list of all the modules currently loaded in the kernel. A 0 in the *Used by* column indicates that the loaded module is not in use.

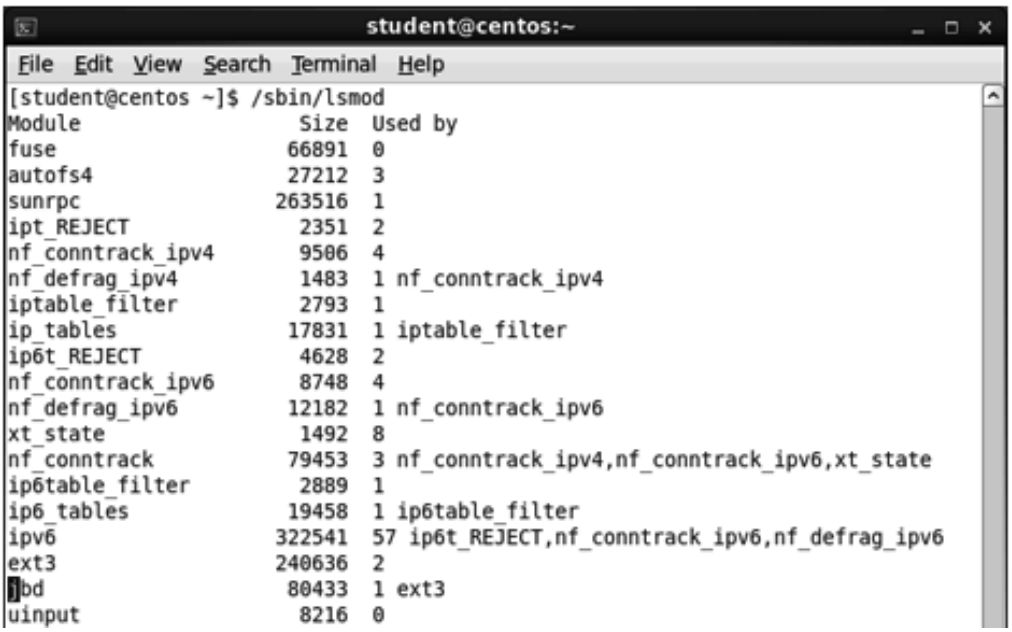


Figure 6 Output from the lsmod command

2. **Make a screen capture** showing the **output of this command** and **paste** it into the Lab Report file. You may have to take multiple screen captures to display the entire output.

3. At the command prompt, **type su -c ' /sbin/modprobe rfcomm '** and **press Enter** to load the rfcomm module.

   The rfcomm module supports Bluetooth devices and is not needed on this server.

4. When prompted, **type P@ssw0rd!**, the root password, and **press Enter**.

▶Note:
You are required to enter a mixed-case password. If you are not using the Citrix Receiver to access this lab, please use the CAPS LOCK button or the On-Screen Keyboard to input the password.

5. At the command prompt, **type /sbin/lsmod | grep rfcomm** and **press Enter** to list the loaded modules that include the word *rfcomm*.

   Notice that the rfcomm module and associated modules are loaded in the running kernel.

6. **Make a screen capture** showing the **output of this command** and **paste** it into the Lab Report file.

7. At the command prompt, **type su -c ' /sbin/modprobe -r rfcomm '** and **press Enter** to remove the rfcomm module.

8. When prompted, **type P@ssw0rd!**, the root password, and **press Enter**.

▶Note:
You are required to enter a mixed-case password. If you are not using the Citrix Receiver to access this lab, please use the CAPS LOCK button or the On-Screen Keyboard to input the password.

9. At the command prompt, **type /sbin/lsmod | grep rfcomm** and **press Enter** to list the loaded modules that include the word "rfcomm".

   Notice that the rfcomm module and associated modules are no longer in this list.

10. **Close** the **remote Linux connection**.

▶Note:
This completes the lab. **Close** the **virtual lab**, if you have not already done so.

Evaluation Criteria and Rubrics

The following are the evaluation criteria for this lab that students must perform:

1. Review and tune the kernel parameters on a CentOS Linux Server for security and monitoring purposes – [**20%**]
2. Produce kernel versions and loaded options for a better understanding of how the system is configured and to identify potential security vulnerabilities in the CentOS Linux Server – [**20%**]
3. Examine the /etc/sysctl.conf file and adjust tcp_sysncookies settings to configure secure options for users on a CentOS Linux Server – [**20%**]
4. Review and assess the Loaded Kernel Modules (LKMs) of the target Linux system and provide recommendations on the output and current running configuration – [**20%**]
5. Use and interpret the lsmod command output and perform security hardening configurations on the CentOS Linux Server – [**20%**]

Lab #7 – Assessment Worksheet

Hardening Security for the Linux Kernel

Course Name and Number: _____

Student Name: _____

Instructor Name: _____

Lab Due Date: _____

Overview

In this lab, you viewed and tuned all kernel parameters and discovered information regarding the current Loadable Kernel Modules (LKMs) and about the kernel itself. You explored the sysctl.conf file and made modifications to system settings. Finally, you enabled and interpreted the results of the lsmod command.

Lab Assessment Questions & Answers

1. What is the command to view the current Linux kernel parameters?

   Part 1, Step 4. **cat /etc/sysctl.conf | less**

2. Which command can you run to list all the kernel's available parameters one screen at a time with the ability to move forward and backward on the output?

   Part 2, Step 1. **/sbin/sysctl -a | less**
   Less is a program that allows both backward and forward movement of a given file or command. Piping the output of the **sysctl -a** command will allow the user to view *all* the parameters available to that command.

3. What is the purpose of enabling SYN cookies in the Linux kernel?

   Note introducing Part 1. SYN cookies are the key element of a technique used to guard against SYN flood denial-of-service attacks.

4. If you wanted to limit the number of files that a user can open simultaneously on the CentOS Linux Server to a maximum of one, what is the command syntax you need to enable in the Linux kernel?

   Part 2, Step 5. **su -c ' /sbin/sysctl -w fs.file-max=1 '**

5. What is the best way to make a systemwide permanent change to the kernel to enable SYN cookies?

   Note following Figure 4. If you wanted to a permanent setting change, you would open the /etc/sysctl.conf file with a file editor such as vi Editor, edit the setting, and then reboot the server.

6. Your boss wants you to make sure a freshly installed system is up to date and locked down at the kernel level. Which command would you use to load a new module? Which command would you use to remove an unwanted module?

   Part 4, Step 3**. su -c ' /sbin/modprobe <modulename> '**
   Part 3, Step 7. **su -c ' /sbin/modprobe -r <modulename> '**

7. What is the relation between sysctl.conf and the sysctl command?
   Introduction. The sysctl.conf file is a simple, human-readable file that contains values used by the system upon bootup. The sysctl command enables a security administrator to configure a setting or parameter dynamically on the system.

8. What command allows you to dynamically modify a kernel parameter without opening the sysctl.conf file in the vi Editor?
   Part 2, Step 5. **su -c ' /sbin/sysctl -w <*kernelparameter*>'** would change any parameter in the conf file.

Lab #8 Applying Best Practices for Secure Software Management

Introduction

Linux applications are usually delivered as a single archived (.tar) and zipped (.gz) file called a tarball or a package. These packages make installations and upgrades easy because all of the required files, documentation, and configuration information is all in one place. Unfortunately, hackers can easily tamper with packages by inserting malicious files or programs into the tarball. These malicious file can be damaging on a standalone system, but disastrous for a network environment. For this reason, best practice for security administrators is to validate the software packages prior to installing them on the network.

Organizations rely on security administrators to use package management tools, such as RPM Package Manager (RPM) and Yellowdog Updater Modified for RPM (YUM), to verify and install packages within the Linux environment. Additional security can be assured by verifying the integrity of tarballs by comparing the hash codes of the original file with the downloaded file. Another tool available to the security administrator is GnuPG (GPG) which can used to verify encryption keys used to encrypt the original package.

This lab is an extension of the previous labs and incorporates best practices for secure software management. In this lab, you will work with a CentOS machine and use RPM to query and verify package files, verify a source tarball used for application integrity verification when downloading and installing new applications, and learn how to create a repository to properly secure the RPN databases. You will also use the md5sum for hashing and integrity verification against downloaded program files. Finally, you will learn to use GPG (GnuPG) tool to view a GPG license key to ensure downloaded software is valid.

This lab has four parts, which should be completed in the order specified.

1. In the first part of the lab, you will explore the RPM Package Manager tool to query and verify packages within a Centos virtual lab environment.
2. In the second part of the lab, you will use md5sum to check the integrity of a tarball file.
3. In the third part of the lab, you will use the GPG (GnuPG) tool to verify a license key and ensure the integrity of the downloaded program.
4. Finally, if assigned by your instructor, you will explore the virtual environment on your own to answer a challenge question that allows you to use the skills you learned in the lab to conduct independent, unguided work, similar to what you will encounter in a real-world situation.

Learning Objectives

Upon completing this lab, you will be able to:

- Query and verify all installed packages in the kernel to help evaluate what security measures are necessary
- Verify a source tarball to determine whether the integrity and contents of the package are what you expect before executing or installing it
- Use and leverage md5sum to verify the integrity of a downloaded software tarball
- Use GPG to view the signature of a downloaded public key
- Configure the rpm database to add repositories securely for the distribution of software to persons who do not need access to the system directly, only to download any updates or rpms

Tools and Software

The following software and/or utilities are required to complete this lab. Students are encouraged to explore the Internet to learn more about the products and tools used in this lab.

- md5sum
- Python
- RPM Package Manager (RPM)

Deliverables

Upon completion of this lab, you are required to provide the following deliverables to your instructor:

1. Lab Report file including screen captures of the following steps: Part 1, Steps 5, 8, and 11; Part 2, Steps 5 and 7; Part 3, Steps 2 and 13;
2. Lab Assessments file;
3. Optional: Challenge Questions file, if assigned by your instructor.

Hands-On Steps

▶Note:
This lab contains detailed lab procedures, which you should follow as written. Frequently performed tasks are explained in the Common Lab Tasks document on the vWorkstation desktop. You should review these tasks *before* starting the lab.

1. From the vWorkstation desktop, **open** the **Common Lab Tasks file**.

   If you desire, use the File Transfer button to transfer the file to your local computer and print a copy for your reference.

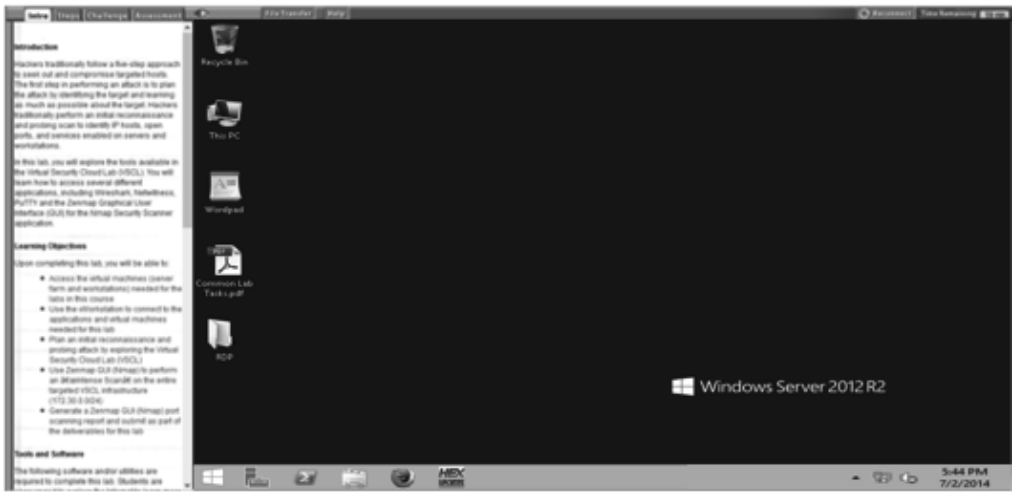


Figure 1 "Student Landing" vWorkstation

2. On your local computer, **create** the **lab deliverable files**.

3. **Review** the **Lab Assessment Worksheet** at the end of this lab. You will find answers to these questions as you proceed through the lab steps.

Part 1: Explore a Tarball with RPM Package Manager

▶Note:
In the next steps, you will explore the built-in RPM Package Manager tool found in the virtual Centos server. This tool has five basic operation modes: installing, uninstalling, upgrading, querying and verifying. It is also a database that holds all RPM package information stored in the Linux system and manages package installations, re-installations, and updates. From the RPM database, users issue command line statements to query and verify installed packages and files to help identify issues, changes, or missing files. As a result, RPM upgrades individual components rather than the entire package, and keeps customized settings already in place on the Linux machine. Developers who use RPM to build their software can ensure the original integrity of the source along with the patches used, including the build instructions. This, in turn, makes for better software for end users. RPM is not foolproof, however. RPM does not automatically install all program dependencies before installing a software package.

1. **Double-click** the **RDP folder** on the vWorkstation desktop. This folder contains RDP connection link to CentOS virtual server in this lab environment.

2. **Double-click** the **TargetCentOS01.rdp** to connect to the remote Linux server.

   The remote GNOME desktop, the graphical user interface (GUI) for the virtual Linux server, opens with the IP address of the remote machine (172.30.0.21) in the title bar at the top of the window.

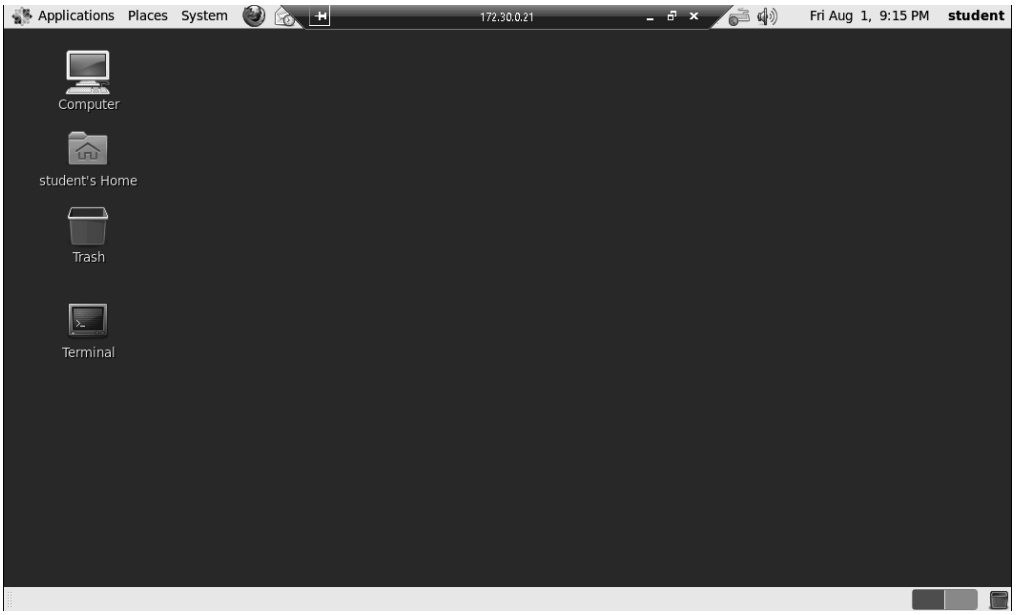


Figure 2 GNOME desktop

3. **Double-click** the **Terminal icon** on the GNOME desktop to open the terminal emulator and access the Linux server command line.

4. At the command prompt, **type rpm -ql sendmail | less** and **press Enter** to view all files associated with the sendmail package.

   The -ql option queries the sendmail package and displays the included files in a list. The less command enables you to use the up and down arrows to scroll through the results.

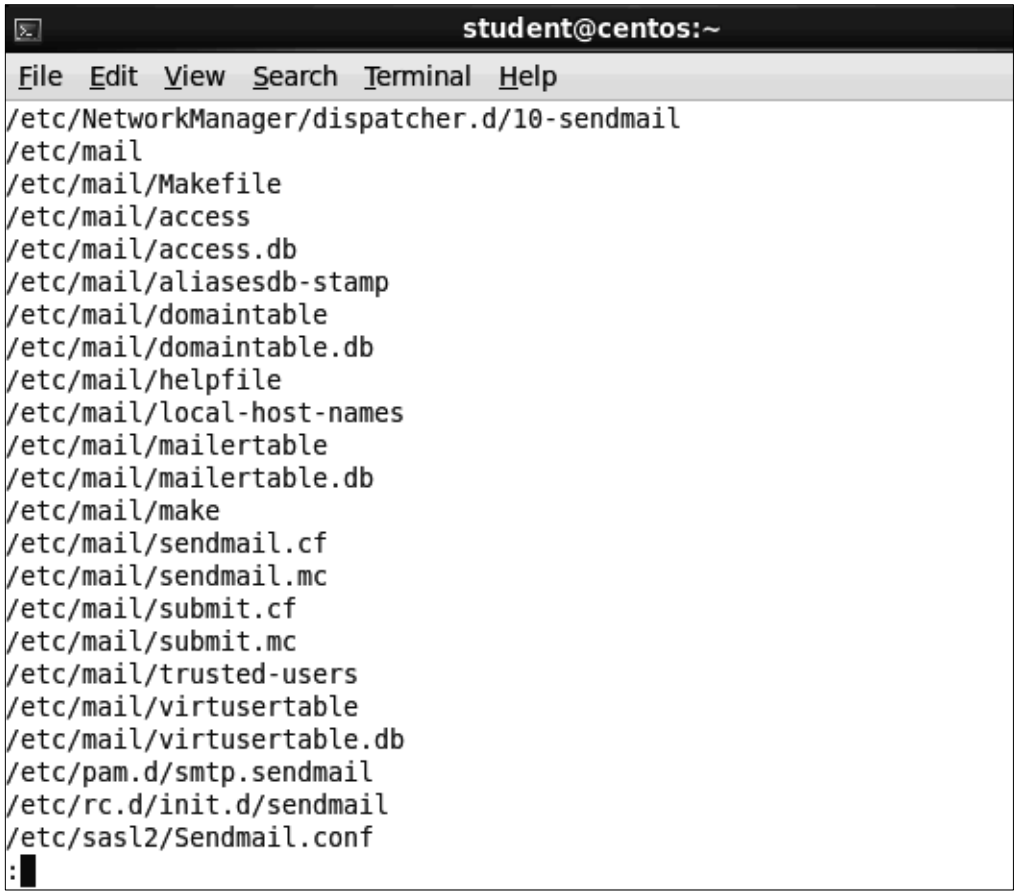


Figure 3 Output of the rpm -ql command

5. **Make a screen capture** showing the **list of sendmail files** and **paste** it into the Lab Report file. You may have to take multiple screen captures to display the entire output.

6. **Type q** to return to the command prompt.

7. At the command prompt, **type rpm -qf /bin/ls** and **press Enter** to discover which package installed the /bin/ls executable.

   The -qf switch option queries the specified path for the name of the package file.

8. **Make a screen capture** showing the **package name** and **paste** it into your Lab Report file.

▶Note:
In the next steps, you will identify any changes to the contents of the file that have taken place. The output of the rpm -V appears in three columns as shown in the following figure.

```
S.5....T.  c /etc/my.cnf
S.5....T.  c /etc/sysconfig/vncservers
....L....  c /etc/pam.d/fingerprint-auth
....L....  c /etc/pam.d/password-auth
....L....  c /etc/pam.d/smartcard-auth
....L....  c /etc/pam.d/system-auth
..5....T.  c /etc/inittab
.......T.  c /etc/ssh/sshd_config
S.5....T.  c /etc/sudoers
..5....T.    /usr/share/ibus-table/tables/compose.db
..5....T.    /usr/share/ibus-table/tables/latex.db
.M....G..    /var/log/gdm
.M.......    /var/run/gdm
.M.......    /var/run/gdm/greeter
S.5....T.  c /etc/mail/sendmail.mc
S.5....T.  c /etc/httpd/conf/httpd.conf
```

Figure 4 Output from rpm -V command

The first column is formatted as a string of nine characters each of which denotes the result of a comparison of one attribute of the file to the value of that attribute recorded in the RPM database. The following table describes each flag. If a package or file can't be found, the output will show "missing" because the file or package was either deleted or moved, or is unreadable.

RPM Flag Description

Flags	Description
.	Passed the test (matches the original)
?	Test could not be performed
S	File size changed
M	Mode / Permissions/ File type changed
5	MD5 checksum changed
D	Device changed
L	Symbolic link changed
U	User ownership changed
G	Group ownership changed
T	File modification time changed
P	Capabilities changed

The second column will contain one of these attribute markers identifying the type of file in the package:

- c – configuration file
- d – documentation file
- g – ghost file, where, for example, the file contents are not included in the package payload
- l – license file
- r – readme file

The third column contains the file name and path for the files included in the package.

9. At the command prompt, **type sudo rpm -V httpd** and **press Enter** to verify the integrity of files in the installed httpd package.

10. This command requires a password, so **type pass=7890** and **press Enter** at the command prompt.

    This command returns any instances where the content of the referenced file, in this case the httpd file, has changed. If no changes have occurred in the file specified, there will be no output. If the file has been changed, the output will indicate what type of change has been made.

11. **Make a screen capture** showing the **results of the rpm –V command** and **paste** it into the Lab Report file.

12. **Use** the **RPM Flag Description table** from the previous note to determine which type of change has been made to the httpd.conf file and **describe your findings** in the Lab Report file.

13. At the command prompt, **type rpm -qa | less** and **press Enter** to view a list of all currently installed packages on the Linux computer. Use the up and down arrow keys to view the entire list.

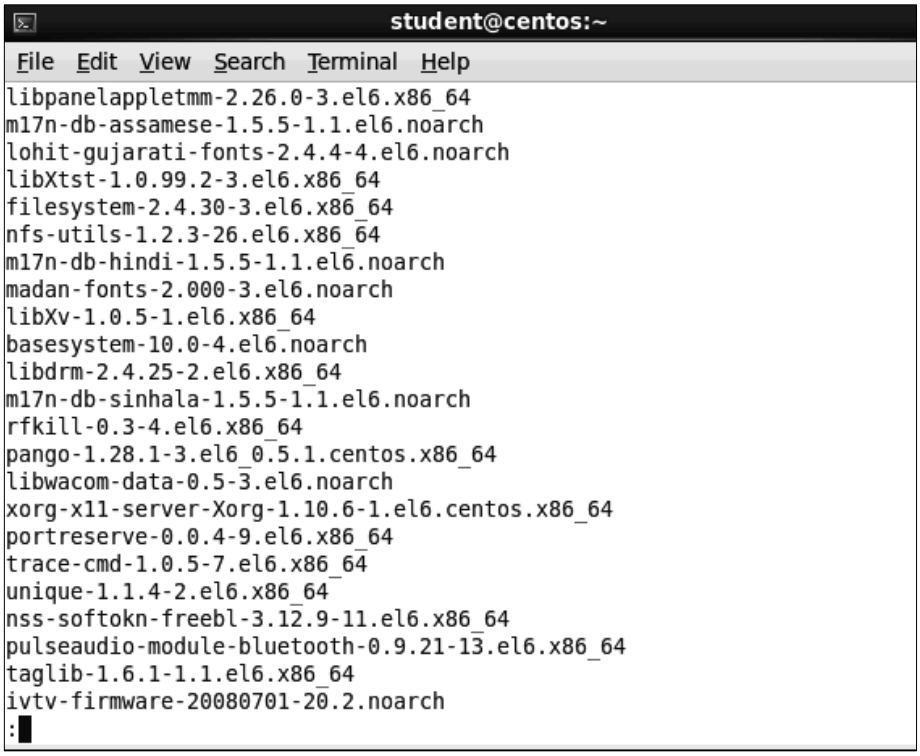


Figure 5 Output of the rpm -qa command

14. In the Lab Report file, **describe** the list. Did the number of file meet your expections?

15. **Type q** to return to the command prompt.

Part 2: Use md5sum Hashing to Verify an Installation File

▶Note:
The md5sum is an algorithm that is used to verify data integrity and authenticity using the MD5 (Message-Digest algorithm 5) 128-bit cryptographic hash. A hash is a unique, constant-length checksum or signature for the data or program. The md5sum runs a comparison check to detect file changes and provides a checksum that users use to see whether it matches the MD5 value signed by the trusted organization or developer of the file/program.

This hash technique is different than encryption because it is a one-way method that doesn't require known keys to encrypt and decrypt information. Any changes to a program and its files will produce a different md5sum value. If there are no changes, then the Md5Sum value will match the md5sum value provided by the trusted source of the program files. Encryption, on the other hand, is a two-way function that requires a known key or keys to encrypt and decrypt the original data. Basically, a hash verifies a file and its integrity, and encryption contains the file and secures it with a key control that both parties must know.

In the next steps, you will use md5sum hashing to verify the integrity of the source code for the downloaded Python software on the Centos machine. Downloaded software is a significant security threat that should be checked and verified to make sure that it hasn't been tampered with before it is installed. This portion of the lab requires access to a workstation with Internet access.

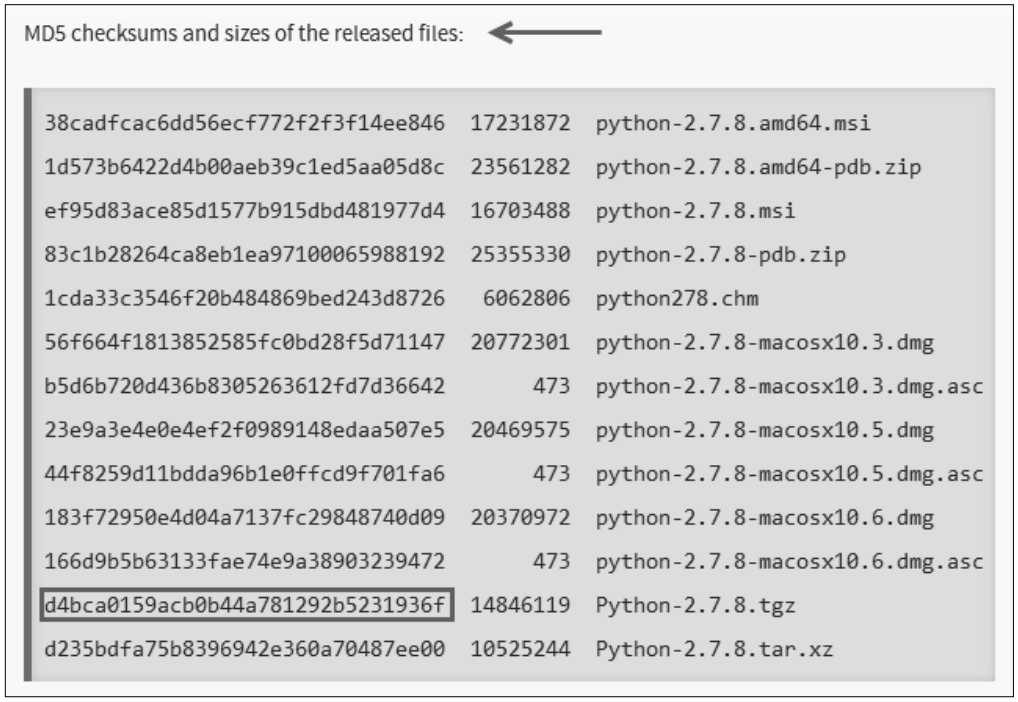
1. At the command prompt, **type ls /opt/software** and **press Enter** to view a list of all of the downloaded software on this computer.

   The system returns a list of downloaded software. In this case, the Python-2.7.8.tgz software.

2. From a workstation with Internet access, **open a Web browser**, such as Mozilla Firefox or Microsoft Internet Explorer.

3. In the browser's address box, **type http://www.python.org/download/releases/2.7.8/**, the URL (uniform resource location) for the Python software, and **press Enter** to open the Web site.

4. On the Python Web site, **locate** the **MD5 checksum** for the Python 2.7.8.tgz release. You may need to scroll down the page to find the section labeled MD5 checksums and sizes of the released files.


MD5 checksums and sizes of the released files:

```
38cadfcac6dd56ecf772f2f3f14ee846  17231872  python-2.7.8.amd64.msi
1d573b6422d4b00aeb39c1ed5aa05d8c  23561282  python-2.7.8.amd64-pdb.zip
ef95d83ace85d1577b915dbd481977d4  16703488  python-2.7.8.msi
83c1b28264ca8eb1ea97100065988192  25355330  python-2.7.8-pdb.zip
1cda33c3546f20b484869bed243d8726   6062806  python278.chm
56f664f1813852585fc0bd28f5d71147  20772301  python-2.7.8-macosx10.3.dmg
b5d6b720d436b8305263612fd7d36642       473  python-2.7.8-macosx10.3.dmg.asc
23e9a3e4e0e4ef2f0989148edaa507e5  20469575  python-2.7.8-macosx10.5.dmg
44f8259d11bdda96b1e0ffcd9f701fa6       473  python-2.7.8-macosx10.5.dmg.asc
183f72950e4d04a7137fc29848740d09  20370972  python-2.7.8-macosx10.6.dmg
166d9b5b63133fae74e9a38903239472       473  python-2.7.8-macosx10.6.dmg.asc
d4bca0159acb0b44a781292b5231936f  14846119  Python-2.7.8.tgz
d235bdfa75b8396942e360a70487ee00  10525244  Python-2.7.8.tar.xz
```

Figure 6 MD5 checksum from the Python Web site

5. **Make a screen capture** showing the **MD5 checksum for the Python release** and **paste** it into the Lab Report file.

6. In the TargetCentOS01 window, **type md5sum /opt/software/Python-2.7.8.tgz** and **press Enter** at the command prompt to view the MD5 checksum for the Python release installed on this computer.

7. **Make a screen capture** showing the **MD5 checksum for the Python tarball** and **paste** it into the Lab Report file.

8. In the Lab Report file, **compare** the **two MD5 checksums** to verify that the version of Python installed on this computer matches the version released on Python's Web site.

Part 3: Use GPG and Create a New Repository File

▶Note:
Software download packages usually include a GPG key, which acts as a digital signature to prove the validity of the source. GPG is an Open Source encryption and signing tool that helps ensure data integrity and confidentiality. Software management tools like RPM and YUM utilities store the public keys for approved package sources to help with software installations.

In the next steps, you will use the gpg command to view and verify GPG license key signature. When managing downloaded software on a Linux platform, you will often need to download GPG keys from the internet and verify their signatures to ensure that the downloaded program is valid and trusted. You will then import that GPG key to the RPM database before creating a new repository file under the YUM repository directory to hold any software published by Google.

1. At the command prompt, **type gpg /opt/software/linux_signing_key.pub** and **press Enter** to view the signature of a downloaded GPG key.

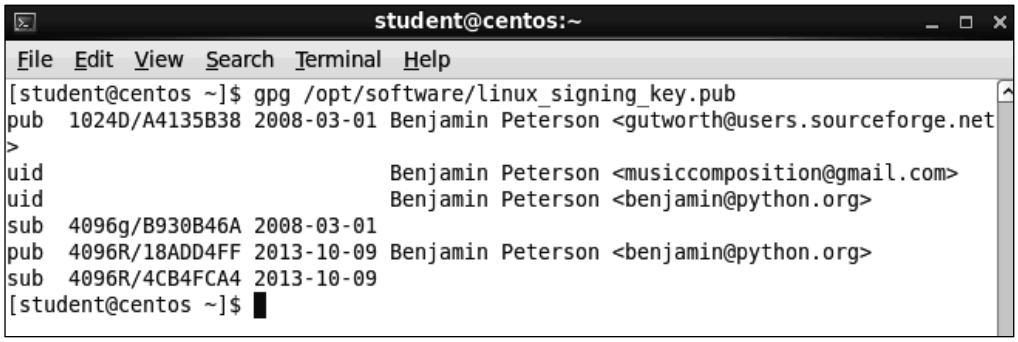


Figure 7 Verify the signature of a downloaded GPG key

2. **Make a screen capture** showing the **GPG signature** and **paste** it into the Lab Report file.
3. At the command prompt, **type sudo rpm --import /opt/software/linux_signing_key.pub** and **press Enter** to import the key into the RPM database.
4. When prompted for a password, **type pass=7890**.
5. At the command prompt, **type cd /etc/yum.repos.d/** and **press Enter** to change the to the yum.repos.d directory.
6. At the command prompt, **type su -c ' vi google.repo '** and **press Enter** to open a new file called google.repo in the vi Editor.
7. When prompted, **type P@ssw0rd!**, the root password, and **press Enter** to create the new account.

▶Note:
You are required to enter a mixed-case password. If you are not using the Citrix Receiver to access this lab, please use the CAPS LOCK button or the On-Screen Keyboard to input the password.

8. **Press** the **i key** to enter the Insert mode.

9. **Use** the **arrow keys** to locate the first blank line in the file and **type** the following new lines noted below.

   - **[Google]**
   - **name=Google Lab**
   - **baseurl=http://dl.google.com/linux/rpm/stable/i386**
   - **enabled=1**
   - **gpgcheck=1**
   - **gpgkey=https://dl-ssl.google.com/linux/linux_signing_key.pub**

Figure 8 Create a new google.repo file

10. **Press** the **Esc key** to exit the Insert mode.

11. **Type :wq!** and **press Enter** to save your changes and exit the vi Editor.

    The new google.repo file will be saved in the yum.repos.d directory. The YUM installer will now check any newly installed software published by Google against the information in this file.

▶Note:
Unlike RPM Package Manager, the YUM installer automatically tracks and installs all dependent applications first before installing the software package you may actually want. YUM looks in the /etc/yum.repos.d/ directory for configured repositories. CentOS has several repositories by default, but third-party repositories can be added to gain access to other software.

12. At the command prompt, **type ls** and **press Enter** to list the files in the yum.repos.d directory.

    The resulting list of files should include the google.repo file you just created.

13. **Make a screen capture** showing the **results of the ls command** and **paste** it into the Lab Report file.

14. **Close** the **remote Linux connection**.

15. **Close** the **virtual lab**, or proceed with Part 4 to answer the challenge question for this lab.

Part 4: Challenge Question

▶Note:
The following challenge question is provided to allow independent, unguided work, similar to what you will encounter in a real situation. You should aim to improve your skills by getting the correct answer in as few steps as possible. Use screen captures in your lab document where possible to illustrate your answers.

1. Explain the differences between RPM and YUM. What is the preferred software installation utility? Why? Use the Internet to research your answer and cite your references.

   (Answers will be unique to each student.) Both are command-line-based tools. The YUM utility is a more intelligent tool that automatically finds required dependencies and installs them prior to installing any software package. The RPM Package Manager tool, on the other hand, doesn't know how to find, and isn't aware of, dependencies during a software package installation. As a result, the installed software may not work correctly. A user must detail the exact location of each dependency when using the rpm command and install them prior to installing the specific software application needed. YUM only requires the program name to find all the dependencies and install them prior to installing the respective software needed.

   As a result, YUM is the preferred method for software installations if user is very comfortable with using command line syntax. Otherwise, many Linux operating systems offer a GUI (graphic user interface) for easy software installations.

▶Note:
This completes the lab. **Close** the **virtual lab**, if you have not already done so.

Evaluation Criteria and Rubrics

The following are the evaluation criteria for this lab that students must perform:

1. Query and verify all installed packages in the kernel to help evaluate what security measures are necessary – [**20%**]
2. Verify a source tarball to determine whether the integrity and contents of the package are what you expect before executing or installing it – [**20%**]
3. Use and leverage md5sum to verify the integrity of a downloaded software tarball – [**20%**]
4. Use GPG to view the signature of a downloaded public key – [**20%**]
5. Configure the rpm database to add repositories securely for the distribution of software to persons who do not need access to the system directly, only to download any updates or rpms – [**20%**]

Lab #8 – Assessment Worksheet

Applying Best Practices for Secure Software Management

Course Name and Number: _____

Student Name: _____

Instructor Name: _____

Lab Due Date: _____

Overview

This lab was an extension of the previous labs. It incorporated best practices for secure software management. In this lab, you worked with a CentOS machine and used RPM to query and verify package files, verified a source tarball used for application integrity verification when downloading and installing new applications, and learned how to create a repository to properly secure the RPN databases. You also used the md5sum for hashing and integrity verification against downloaded program files. Finally, you learned to use GPG (GnuPG) tool to view a GPG license key to ensure downloaded software is valid.

Lab Assessment Questions & Answers

1. Explain the purpose of the **rpm -qf /bin/ls** command.

   Part 1, Step 7. This command will return the name of the package file in the specified location. In this case, it is coreutils-8.4-19.el6.x86_64.

2. Discuss the purpose of a software repository as it relates to YUM.

   Note following Part 3, Step 11. Unlike RPM Package Manager, the YUM installer automatically tracks and installs all dependent applications first before installing the software package you may actually want. YUM looks in the /etc/yum.repos.d/ directory for configured repositories. CentOS has several repositories by default, but third-party repositories can be added to gain access to other software.

3. How can you ensure that a downloaded software package (tarball) is legitimate and hasn't been tampered with?

   Part 2. Download a tarball from a trusted source, and obtain that source's MD5 checksum. Once the tarball is downloaded, run md5sum on the tar download. Then, compare MD5 checksum result against the trusted source's checksum.

4. Explain all of the switches associated with the rpm command that were used in this lab.

    - Part 1 Step 4. -ql (lists all files in the package)
    - Part 1 Step 7. -qf (queries a specified path for the name of the package file)
    - Part 1 Step 9. -V (verifies the integrity of the files in the package)
    - Part 1 Step 13. –qa (lists all currently installed packages)

5. Explain what hashing is and how it differs from encryption.

    Note introducing Part 2. A hash is a unique constant-length checksum or signature for the data or program. This hash technique is different from encryption because it is a one-way method that doesn't require known keys to encrypt and decrypt information. Any changes to a program and its files will produce a different md5sum value. If there are no changes, then the Md5Sum value will match the md5sum value provided by the trusted source of the program files. Encryption, on the other hand, is a two-way function that requires a known key or keys to encrypt and decrypt the original data. Basically, a hash verifies a file and its integrity, and encryption contains the file and secures it with a key control that both parties must know.

6. If you wanted to know which package a certain program belonged to, what command would you run?

    Part 1, Step 7. **rpm -qf <*installed program directory*>**.

7. During this lab, you reviewed the httpd file for changes. What changes did you record in your WordPad document?

    Part 1, Step 12.

    - 5 – MD5 checksum has changed
    - T – The time of the file has change
    - S – The size of the repository has changed

Lab #9 Applying Best Practices for Security Logging and Monitoring

Introduction

Security administration is not simply a matter of locking down a system and then not having to worry about it again. New exploits in existing software and network protocols are constantly being discovered, not to mention the possibility of social engineering attack attempts. To identify anything amiss on a server, it is best practice for security administrators to regularly to check in on the machine.

Checking in on a machine would be meaningless if nothing is being recorded for you to check. By default, Linux servers run a system logging feature. Typically, the system log would reside on the same server it is logging, but best practice is to locate the system log on a remote server instead, particularly if the logged server is open the Internet. Locating the system logs for all servers on a single server provides a more secure location for all logging. Suppose an intruder breaks into a Linux system and deletes all of the local log files. Unless the intruder also compromises the remote logging server, the log files will still be available to access and analyze. System logs open the Internet are also vulnerable to denial service attacks which may fill up the system log to the point where it cannot log any other messages.

Another method of logging events on a server is available by using the Tripwire application. Tripwire is a file integrity tool that keeps a database hash of all files specified in its policy file. Anytime a file is altered, Tripwire will detect the changes.

Rootkit Hunter (rkhunter) is another file integrity checker available to the security administrator. Rkhunter is a script that checks for various rootkits, a type of malicious software that enables unauthorized users access to the server without being detected. It also performs checks on common commands and startup files to determine if they have been modified, among other things.

In this lab, you will configure remote logging in the CentOS Linux Server and send syslogs to a remote host for secure secondary logging. You will use Tripwire, a third-party file integrity tool, to identify modifications to important system files. You will configure Rootkit Hunter, (rkhunter), to search for rootkits and other anomalies on a set schedule. You also will search the log files for specific criteria.

This lab has four parts, which should be completed in the order specified.

1. In the first part of this lab, you will configure remote logging for an external logging and monitoring server by creating a new rsyslog.conf remote log configuration file; you will then search through the log files to search for evidence of an intrusion.

2. In the second part of this lab, you will configure a default policy file for Tripwire and create a site and local passphrase; you will then initialize the Tripwire database and index all of the files on the system.

3. In the third part of this lab, you will edit the rkhunter configuration file, schedule the rkhunter report to run at a specific time, and run the rkhunter check summary report.

4. Finally, if assigned by your instructor, you will explore the virtual environment or a related topic on your own to answer a set of challenge questions that allow you to use the skills you learned in the lab to conduct independent, unguided work, similar to what you will encounter in a real-world situation.

Learning Objectives

Upon completing this lab, you will be able to perform the following:

- Configure remote logging on the CentOS Linux Server and send syslogs and other events to a remote host for secure secondary logging
- Search through different log files on the CentOS Linux Server to identify where certain types of logs are stored and how often they get recycled
- Configure the Tripwire file integrity tool so that modifications to important system files are quickly identified and properly logged both locally and remotely
- Configure and schedule rkhunter to run at said interval using the cron subsystem so that a rootkit can be properly and quickly identified if possible
- Configure both automatic searches on log files as well as automatic running of important security applications to properly monitor a CentOS Linux Server for malicious activity

Tools and Software

The following software and/or utilities are required to complete this lab. Students are encouraged to explore the Internet to learn more about the products and tools used in this lab.

- Rootkit Hunter
- Tripwire

Deliverables

Upon completion of this lab, you are required to provide the following deliverables to your instructor:

1. Lab Report file including screen captures of the following steps: Part 1, Steps 13, 26, and 29; Part 2, Step 23; Part 3, Steps 6, 18, and 23;
2. Lab Assessments file;
3. Optional: Challenge Questions file, if assigned by your instructor.

Hands-On Steps

▶Note:
This lab contains detailed lab procedures, which you should follow as written. Frequently performed tasks are explained in the Common Lab Tasks document on the vWorkstation desktop. You should review these tasks *before* starting the lab.

1. From the vWorkstation desktop, **open** the **Common Lab Tasks file**.

   If you desire, use the File Transfer button to transfer the file to your local computer and print a copy for your reference.

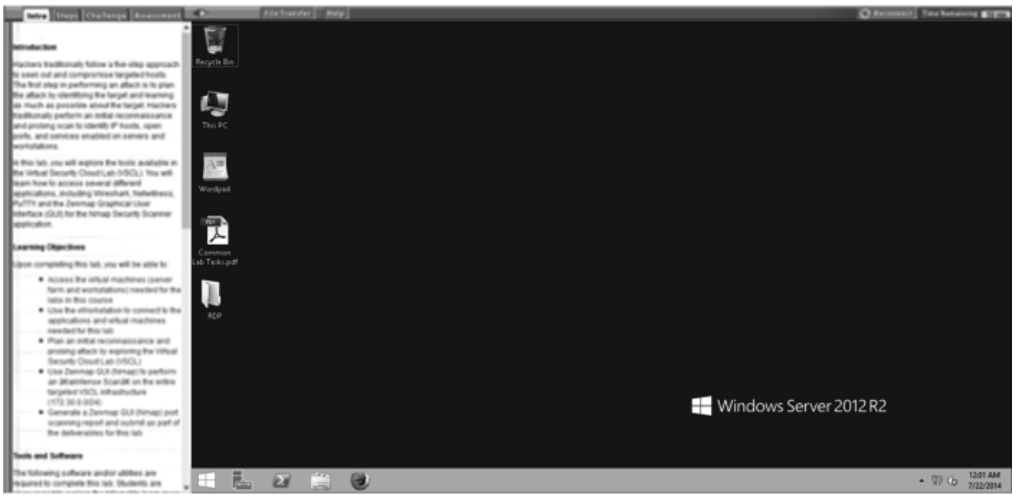


Figure 1 "Student Landing" vWorkstation

2. On your local computer, **create** the **lab deliverable files**.

3. **Review** the **Lab Assessment Worksheet** at the end of this lab. You will find answers to these questions as you proceed through the lab steps.

Part 1: Configuring and Investigating the Linux Log File

▶Note:
In the next steps, you will explore the robust nature of Linux's log files. First, you will configure remote logging for an external logging and monitoring server by creating a new remote log configuration file, the rsyslog.conf file. Next, you will search through the log files for evidence of an intrusion.

1. **Double-click** the **RDP folder** on the vWorkstation desktop to open the folder.

2. **Double-click** the **TargetCentOS01.rdp** file in the RDP folder to open a remote connection to the Linux machine.

   The remote GNOME desktop, the graphical user interface (GUI) for the virtual Linux server, opens with the IP address of the remote machine (172.30.0.21) in the title bar at the top of the window.

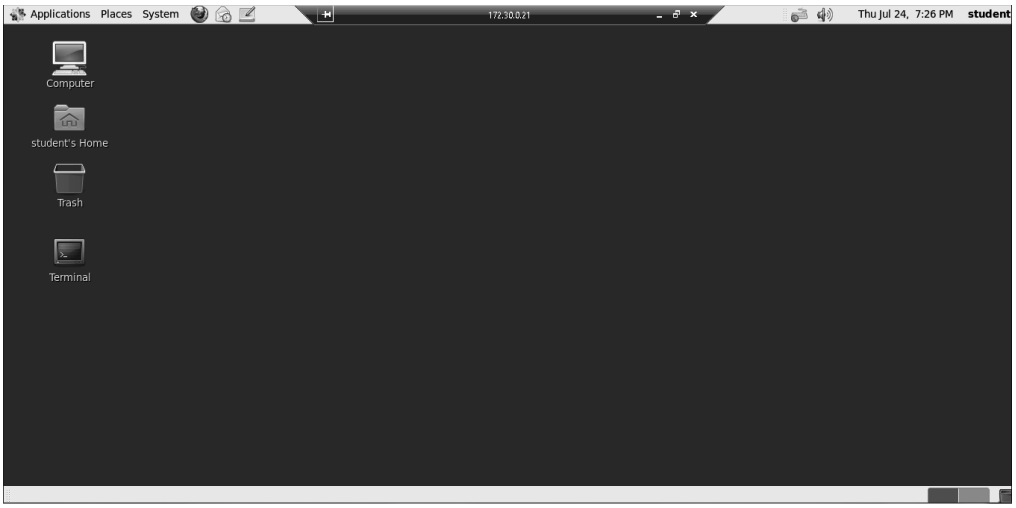


Figure 2 GNOME desktop

3. **Double-click** the **Terminal icon** on the GNOME desktop to open the terminal emulator and access the Linux server command line.

4. At the command prompt, **type su -c ' vi /etc/rsyslog.conf '** and **press Enter** to create a new remote system log configuration file in the vi Editor.

5. When prompted, **type P@ssw0rd!**, the root password, and **press Enter**.

▶Note:
You are required to enter a mixed-case password. If you are not using the Citrix Receiver to access this lab, please use the CAPS LOCK button or the On-Screen Keyboard to input the password.

6. **Press** the **i key** to enter the Insert mode.

7. **Use the arrows keys** to move to the last line in the file and **press Enter** to create a new line above the last line in the file.

8. **Press** the **up-arrow key** so that the cursor is now at the beginning of the new line you just created.

9. **Type *.* @@logs.firstworldbank-example.com** to direct the TargetCentOS01 server to send all (*.*) logging information to a remote server named logs.firstworldbank-example.com.

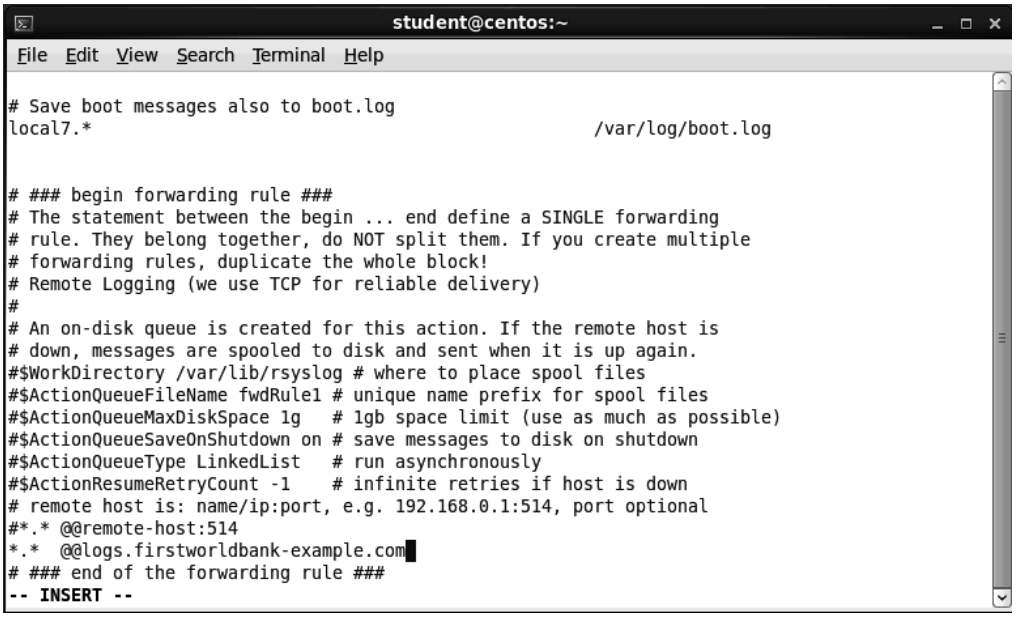


Figure 3 Edit the rsyslog.conf file

10. **Press** the **Esc key** to exit the Insert mode.

11. **Type :wq!** and **press Enter** to save your changes and exit the vi Editor.

12. At the command prompt, **type cat /etc/rsyslog.conf** to display the contents of the file.

13. **Make a screen capture** showing **the edited file** and **paste** it into the Lab Report file.

14. At the command prompt, **type sudo /sbin/service rsyslog restart** and **press Enter** to restart the syslog logging mechanism with your changes without rebooting the server.

15. When prompted, **type pass=7890**, the student password, and **press Enter** to create the new account.

    The system will return OK flags indicating that the process has restarted.

16. At the command prompt, **type sudo /sbin/service sshd status** and **press Enter** to check the running status of the openSSH server.

17. If prompted, **type pass=7890**, the student password, and **press Enter**.

    - If the system indicates that the service is running, skip to step 18.
    - If the service is not running, **type sudo /sbin/service sshd start** and **press Enter** at the command prompt to start the SSH service. Repeat until you receive the indicator that the service is running.

18. At the command prompt, **type ssh nonexist@localhost** and **press Enter** to attempt to establish an SSH connection to an account that does not exist on this server.

19. If prompted to answer the question: *Are you sure you want to continue connecting (yes/*no*)?*, **type yes** and **press Enter**.

20. When prompted for a password for the nonexist@localhost account, **type test** and **press Enter** to attempt to login to the server.

    Because this user account does not exist on the server, the login attempt will fail and the failed attempt will be logged into the system's log file.

21. **Repeat step 20** each time the system prompts you for a password for this account.

    After three failed attempts, the system will display a Permission denied message indicating that the login attempt has been aborted and will return to the command prompt.

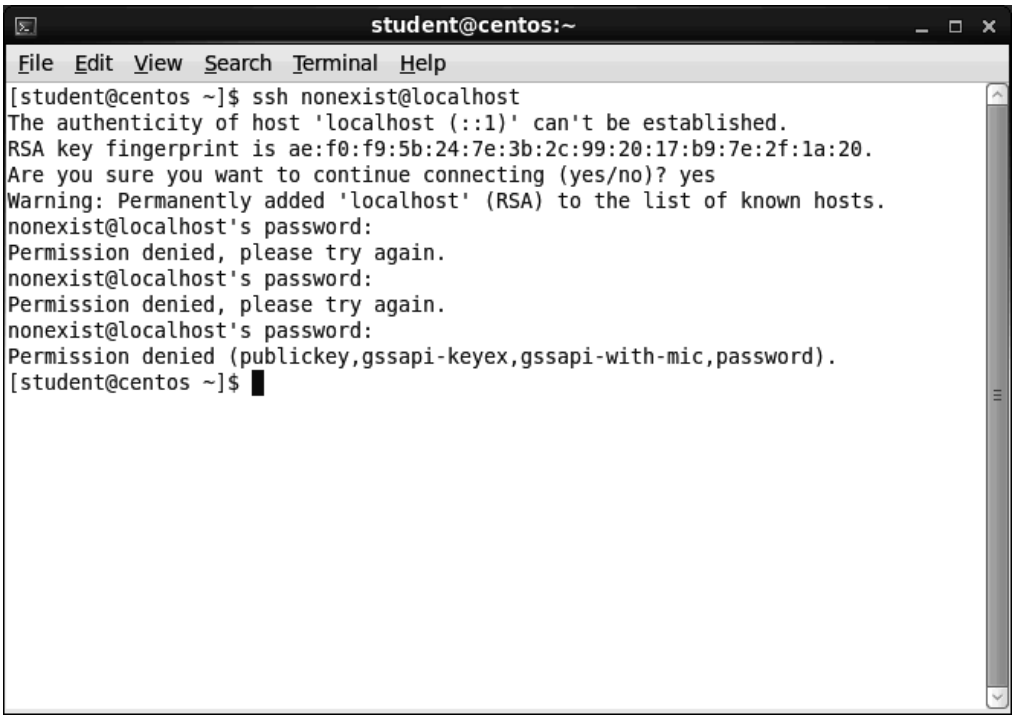


Figure 4 Generate failed login data

22. At the command prompt, **type su -c ' cat /var/log/secure | grep nonexist '** and **press Enter** to search the log file for all of the login attempts for the user account named nonexist.

▶Note:
The /var directory is where all the system logs go by default on the local system. It is best practice to create a /var partition so that attacks or over-subscription of the disk due to logging activity does not hamper the rest of the system from performing its business function.

23. When prompted, **type P@ssw0rd!**, the root password, and **press Enter**.

▶Note:
You are required to enter a mixed-case password. If you are not using the Citrix Receiver to access this lab, please use the CAPS LOCK button or the On-Screen Keyboard to input the password.

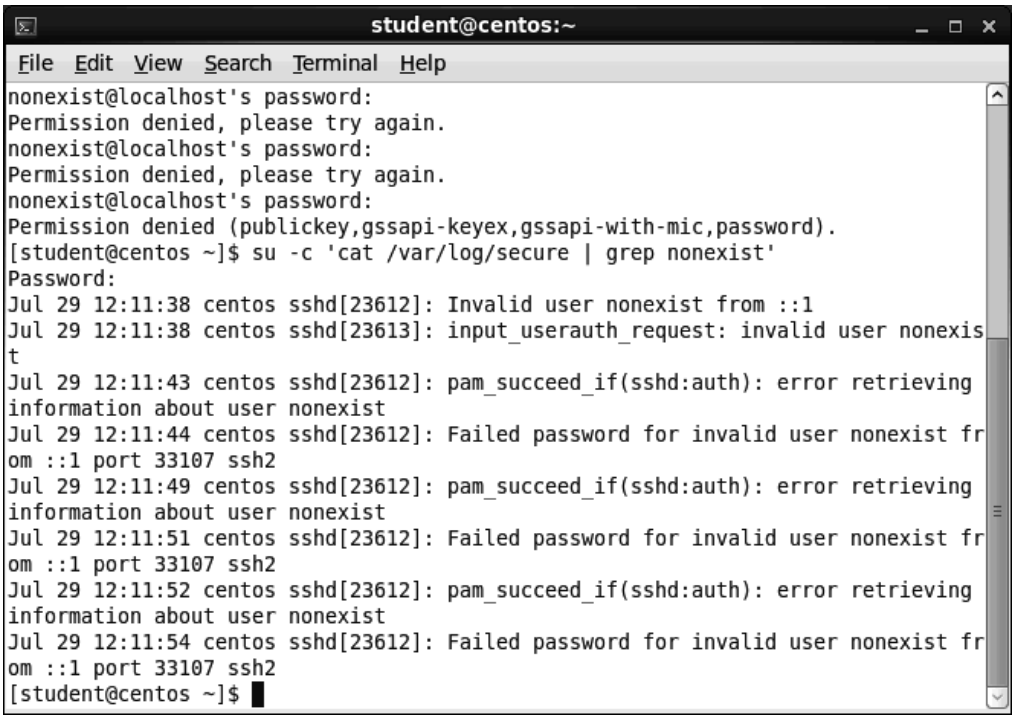


Figure 5 Failed login attempts by nonexist@localhost

24. At the command prompt, **type su -c ' lastb '** and **press Enter** to read only the failed login attempts on the TargetCentOS server.

25. When prompted, **type P@ssw0rd!**, the root password, and **press Enter**.

▶Note:
You are required to enter a mixed-case password. If you are not using the Citrix Receiver to access this lab, please use the CAPS LOCK button or the On-Screen Keyboard to input the password.

26. **Make a screen capture** showing the **results of this command** and **paste** it into the Lab Report file.

27. At the command prompt, **type su -c ' tail /var/log/messages '** and **press Enter** to read the messages from the last 10 lines recorded in the log file.

28. When prompted, **type P@ssw0rd!**, the root password, and **press Enter**.

▶Note:
You are required to enter a mixed-case password. If you are not using the Citrix Receiver to access this lab, please use the CAPS LOCK button or the On-Screen Keyboard to input the password.

29. **Make a screen capture** showing the **results of this command** and **paste** it into the Lab Report file.

Part 2: Configuring Tripwire

▶Note:
In the next steps, you will use Tripwire, a third-party tool loaded as a module on this server, to perform an integrity check. First, you will configure a default policy file for Tripwire and create a site and local passphrase. With the passphrase in place, you will initialize the Tripwire database and index all of the files on the system.

The site passphrase encrypts the Tripwire configuration and policy files, so that it wouldn't be possible to view or change either file without the passphrase. The local passphrase would be used to protect the Tripwire database files. It is important to point out that the passphrases used in this lab (*thelocalpass* and *thesitepass*) as oversimplified. In a real-life situation you would choose a more complex passphrase: at least 8 characters in length with a mix of letter cases and numbers.

1. At the command prompt, **type su -c ' /usr/sbin/tripwire-setup-keyfiles '** and **press Enter** to load the configuration files, the first step in creating a default encrypted policy for Tripwire.

2. When prompted, **type P@ssw0rd!**, the root password, and **press Enter**.

▶Note:
You are required to enter a mixed-case password. If you are not using the Citrix Receiver to access this lab, please use the CAPS LOCK button or the On-Screen Keyboard to input the password.

3. When prompted by the Tripwire process to enter a site keyfile passphrase, **type thesitepass** and **press Enter**.

4. **Type thesitepass** again to verify the site keyfile passphrase.

5. When prompted to create a local keyfile passphrase, **type thelocalpass** and **press Enter**.

6. **Type thelocalpass** again to verify the local keyfile passphrase.

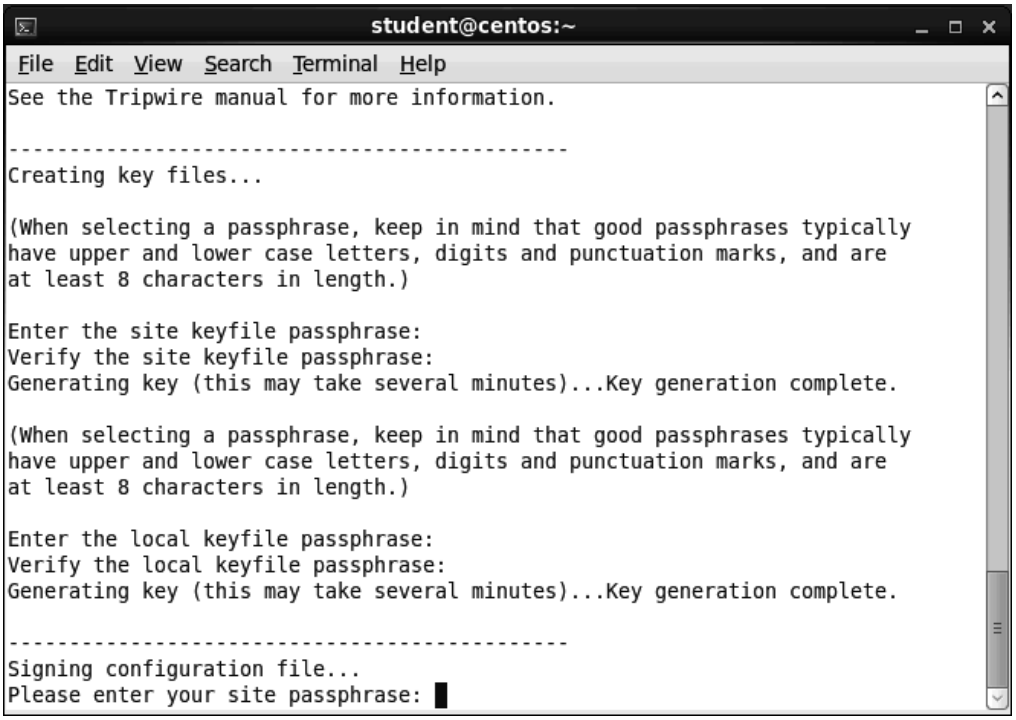


Figure 6 Configure the default policy file for Tripwire

7. When prompted for the site passphrase to sign the configuration file (tw.cfg), **type thesitepass** and **press Enter**.

▶Note:
A cleartext version of the configuration file, /etc/tripwire/twcfg.txt, is created at this time. In a real-life situation, you would move this cleartext file to a more secure location and/or encrypt it once you've examined the contents.

8. When prompted for the site passphrase to sign the policy file (tw.pol), **type thesitepass** and **press Enter**.

▶Note:
A cleartext version of the policy file, /etc/tripwire/twpol.txt, is created during this step. Again, in a real-life situation, you would move this file to a secure location and/or encrypt it after you've examined it.

9. To confirm that the Tripwire configuration file is now encrypted, **type su -c ' cat /etc/tripwire/tw.cfg '** and **press Enter**.

10. When prompted, **type P@ssw0rd!**, the root password, and **press Enter**.

▶Note:
You are required to enter a mixed-case password. If you are not using the Citrix Receiver to access this lab, please use the CAPS LOCK button or the On-Screen Keyboard to input the password.

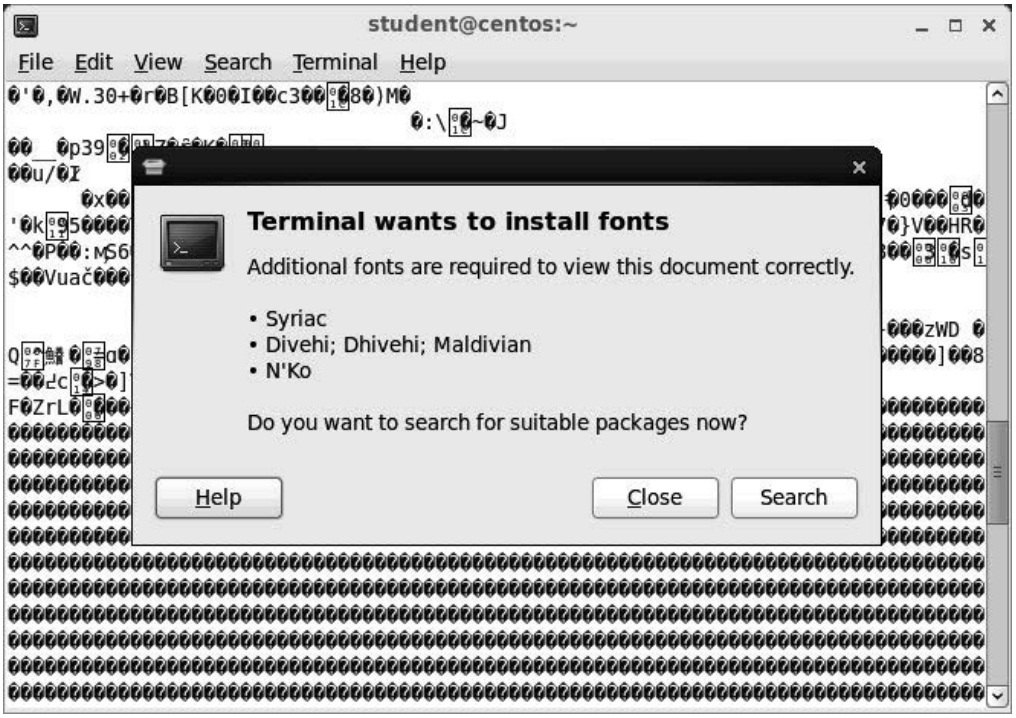


Figure 7 Encrypted configuration file

11. If prompted, **click Close** to dismiss the pop-up window.

12. To confirm that the Tripwire policy file is also encrypted, **type su -c ' cat /etc/tripwire/tw.pol '** and **press Enter**.

▶Note:
After the policy file is created, Tripwire will provide instructions to run the init command to initialize the database. This process reads the policy file and generates a database from its contents.

13. When prompted, **type P@ssw0rd!**, the root password, and **press Enter**.

▶Note:
You are required to enter a mixed-case password. If you are not using the Citrix Receiver to access this lab, please use the CAPS LOCK button or the On-Screen Keyboard to input the password.

14. If prompted, **click Close** to dismiss the pop-up window.

15. At the command prompt, **type su -c ' /usr/sbin/tripwire --init '** and **press Enter** to begin the initialization process.

16. When prompted, **type P@ssw0rd!**, the root password, and **press Enter**.

▶Note:
You are required to enter a mixed-case password. If you are not using the Citrix Receiver to access this lab, please use the CAPS LOCK button or the On-Screen Keyboard to input the password.

17. When prompted for a local passphrase, **type thelocalpass**.

▶Note:
Tripwire will index all of the files on the computer as specified in the policy file. The local passphrase was requested because indexing results in writing to the Tripwire database. This may take several minutes, so do not touch any keys until the terminal prompt appears. You will see several No such file or directory messages because the policy file used in this lab references several file locations that are not found on this server.

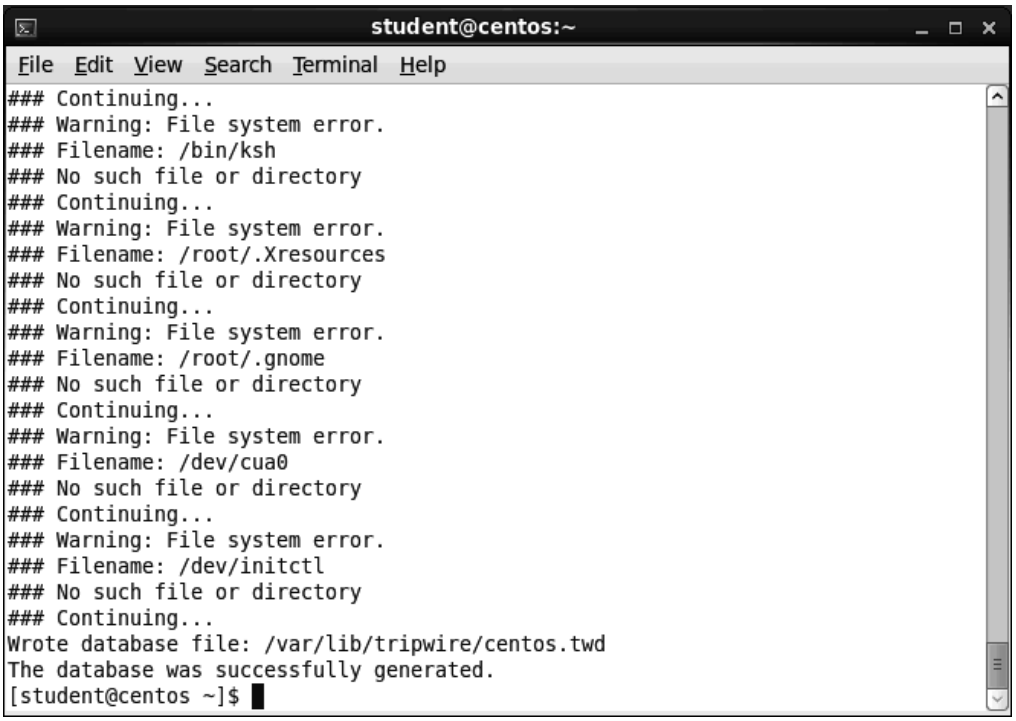


Figure 8 Initialize the Tripwire database

18. At the command prompt, **type su -c ' touch /bin/ls '** and **press Enter** to force a timestamp change on the bin/ls file.

19. When prompted, **type P@ssw0rd!**, the root password, and **press Enter**.

▶Note:
You are required to enter a mixed-case password. If you are not using the Citrix Receiver to access this lab, please use the CAPS LOCK button or the On-Screen Keyboard to input the password.

20. At the command prompt, **type su -c ' /usr/sbin/tripwire --check '** and **press Enter** to run a file integrity check with Tripwire.

21. When prompted, **type P@ssw0rd!**, the root password, and **press Enter**.

> **▶Note:**
> You are required to enter a mixed-case password. If you are not using the Citrix Receiver to access this lab, please use the CAPS LOCK button or the On-Screen Keyboard to input the password.

Tripwire will check the indexed files as specified in the policy file. This may take several minutes, so do not touch any keys until the terminal prompt appears. You will see several No such file or directory messages because the policy file used in this lab references several file locations that are not found on this server.

22. Use the scrollbar to **move** to the **top of the report** and **review** the **reported violations** in the integrity check.

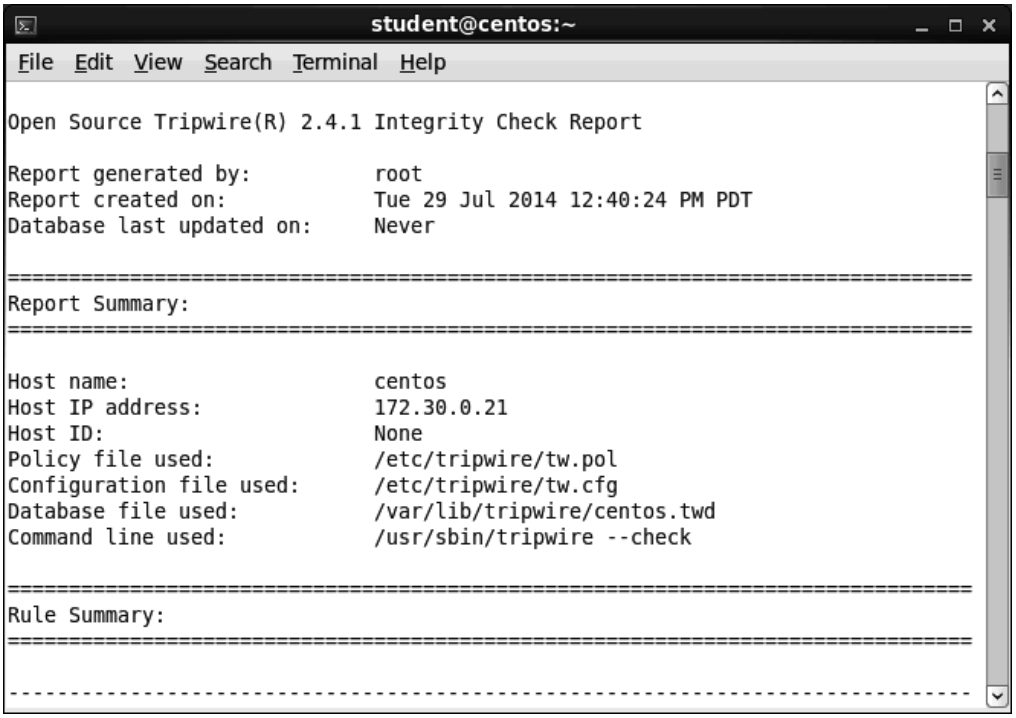


Figure 9 Tripwire Integrity Check Report

23. **Make a screen capture** showing **the report** and **paste** it into the Lab Report file. You may have to take multiple screen captures to display the entire output.

Part 3: Configuring Rootkit Hunter

▶Note:
In the next steps, you will use rkhunter (Rootkit Hunter), a tool that scans the server for rootkits, backdoors, and other anomalies. You will edit the rkhunter configuration file, schedule the rkhunter report to run at a specific time, and run the rkhunter check summary report.

1. At the command prompt, **type su -c ' vi /etc/rkhunter.conf '** and **press Enter** to open the system log configuration file in the vi Editor.

2. When prompted, **type P@ssw0rd!**, the root password, and **press Enter**.

▶Note:
You are required to enter a mixed-case password. If you are not using the Citrix Receiver to access this lab, please use the CAPS LOCK button or the On-Screen Keyboard to input the password.

3. **Press** the **i key** to enter the Insert mode.

4. Use the arrow keys to **locate** the **#MAIL-ON-WARNING=me@mydomain root@mydomain line** and **move** to the **end of the line** and **press Enter** to create a new line.

5. **Type MAIL-ON-WARNING=student** to add the student account to the rkhunter tool.

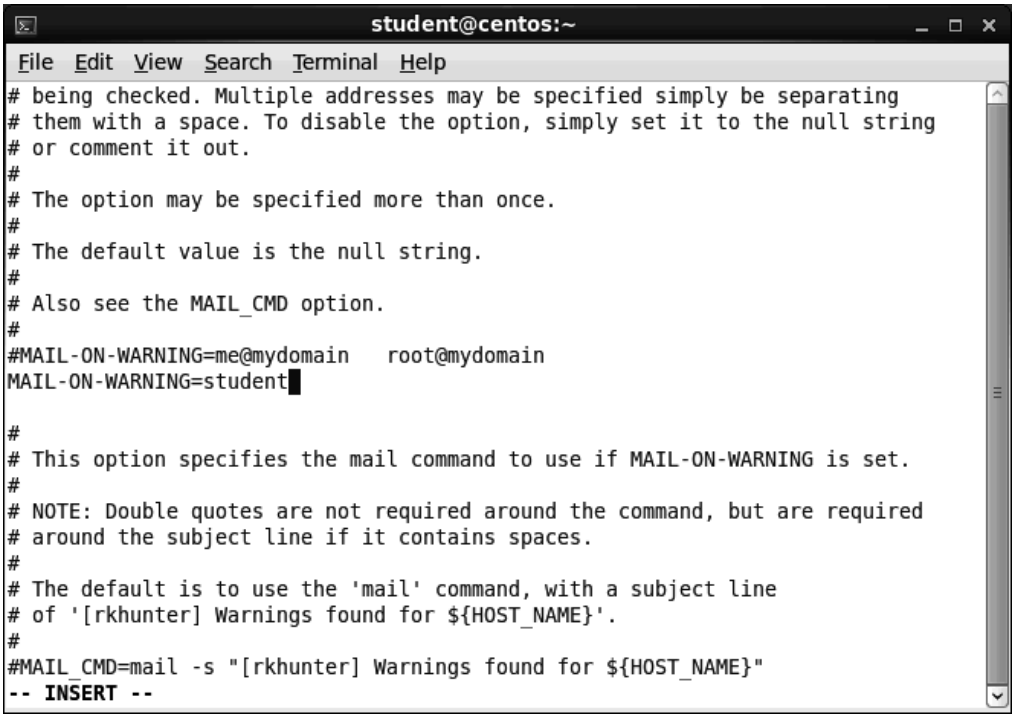


Figure 10 Modify the rkhunter.conf file

6. **Make a screen capture** showing **the edited file** and **paste** it into the Lab Report file.

7. **Press** the **Esc key** to exit the Insert mode.

8. **Type :wq!** and **press Enter** to save your changes and exit the vi Editor.
9. At the command prompt, **type vi rkhunter.txt** and **press Enter** to create a new text file in the vi Editor.
10. **Press** the **i key** to enter the Insert mode.
11. **Type** the following new line of text to use the cron scheduler to run an rkhunter report every morning at 2:30a.m.
    - **30 2 * * * /usr/bin/rkhunter -c -q >/dev/null 2>&1**

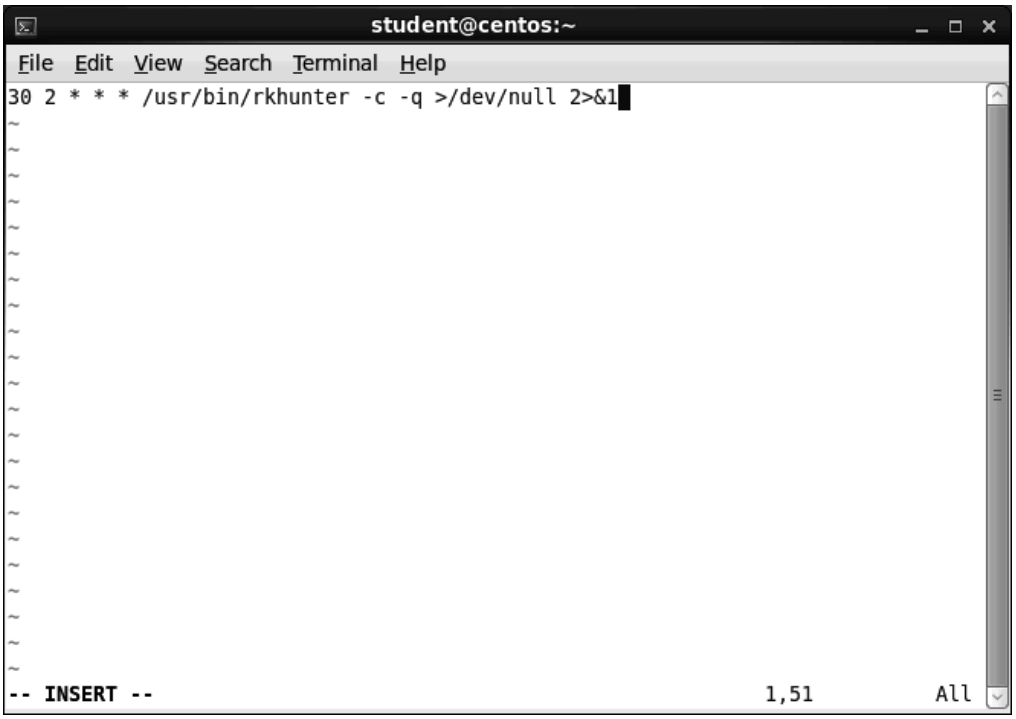


Figure 11 Create the rkhunter.txt file

12. **Press** the **Esc key** to exit the Insert mode.
13. **Type :wq!** and **press Enter** to save your changes and exit the vi Editor.
14. At the command prompt, **type su -c ' crontab rkhunter.txt '** and **press Enter** to schedule the cron job for the root user.
15. When prompted, **type P@ssw0rd!**, the root password, and **press Enter**.

▶Note:
You are required to enter a mixed-case password. If you are not using the Citrix Receiver to access this lab, please use the CAPS LOCK button or the On-Screen Keyboard to input the password.

16. At the command prompt, **type su -c ' crontab -l '** and **press Enter** to list the scheduled cron jobs.

17. When prompted, **type P@ssw0rd!**, the root password, and **press Enter**.

▶Note:
You are required to enter a mixed-case password. If you are not using the Citrix Receiver to access this lab, please use the CAPS LOCK button or the On-Screen Keyboard to input the password.

18. **Make a screen capture** showing the **output of this command** and **paste** it into the Lab Report file.

▶Note:
If the output of the crontab –l command is empty, you will need to check that the crond daemon is running in the background. At the command prompt, **type service crond status** and **press Enter**. If the crond daemon is running, **repeat steps 16-18**. If the crond daemon is stopped, **type service crond start**, **press Enter**, and **repeat steps 16-18**.

19. At the command prompt, **type su -c ' /usr/bin/rkhunter -c '** and **press Enter** to run the rkhunter check summary report.

20. When prompted, **type P@ssw0rd!**, the root password, and **press Enter**.

▶Note:
You are required to enter a mixed-case password. If you are not using the Citrix Receiver to access this lab, please use the CAPS LOCK button or the On-Screen Keyboard to input the password.

Rkhunter will check the system for any anomalies that could indicate a breach. This check may take several minutes. Throughout this process, rkhunter will prompt you to [Press <ENTER> to continue].

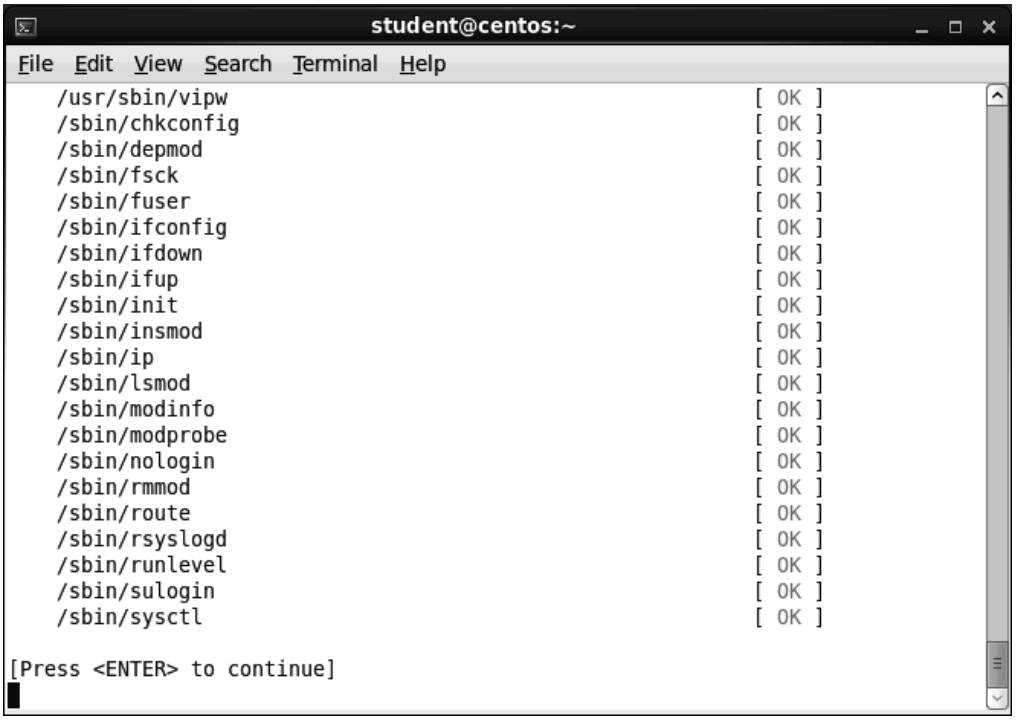


Figure 12 Run the rkhunter report

21. Follow the onscreen instructions and **press Enter** as required until the command prompt returns.

22. Use the scrollbar to **review** the **reported warnings** in the summary.

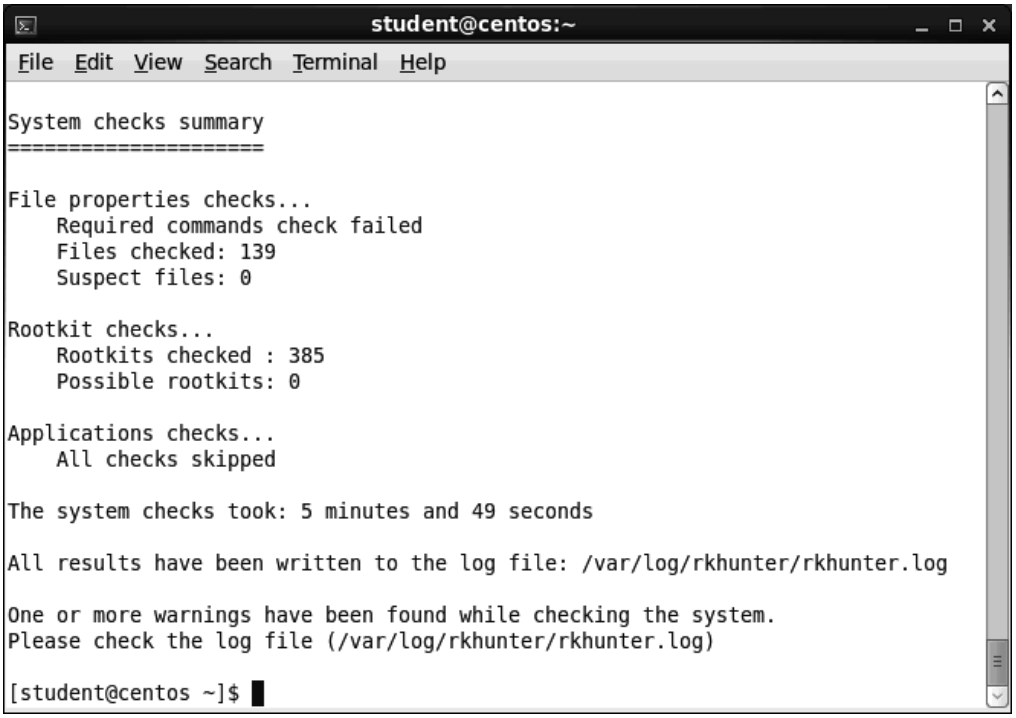


Figure 13 rkhunter check summary report

23. **Make a screen capture** showing the **summary and any warnings** and **paste** it into the Lab Report file. You may have to take multiple screen captures to display the entire summary.

24. **Close** the **remote Linux connection**.

25. **Close** the **virtual lab**, or proceed with Part 4 to answer the challenge question for this lab.

Part 4: Challenge Questions

▶Note:
The following challenge questions are provided to allow independent, unguided work, similar to what you will encounter in a real situation. You should aim to improve your skills by getting the correct answer in as few steps as possible. Use screen captures in your lab document where possible to illustrate your answers.

1. How would you edit the rsyslog.conf file to send all cron jobs to a remote server identified as 172.130.1.254 using the UDP protocol? How would you make sure that the changes take place immediately?

   In the # *Log cron stuff* section of the file, comment out line that says *cron.* /var/log/cron* and add a new line to the same section: cron.* @172.130.1.254. Save the changes to the file and restart the rsyslog service.

2. What edits would you make to send only error conditions or higher to that remote server using the UDP protocol?

   In this case, the new line would read: cron.err @172.130.1.254.

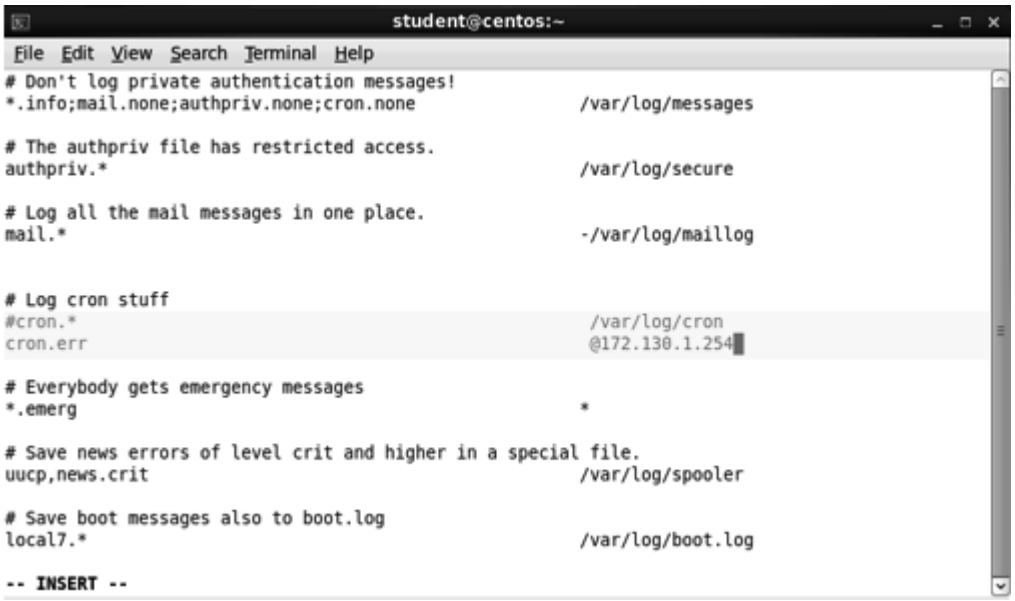


Figure 14 Edited rsyslog.conf file

▶Note:
This completes the lab. **Close** the **virtual lab**, if you have not already done so.

Evaluation Criteria and Rubrics

The following are the evaluation criteria and rubrics that students must perform:

1. Configure remote logging on the CentOS Linux Server and send syslogs and other events to a remote host for secure secondary logging – [**20%**]
2. Search through different log files on CentOS Linux Server to identify where certain types of logs are stored and how often they get recycled – [**20%**]
3. Configure the Tripwire file integrity tool so that modifications to important system files are quickly identified and properly logged both locally and remotely – [**20%**]
4. Configure and schedule rkhunter to run at said interval using the cron subsystem so that a rootkit can be properly and quickly identified if possible – [**20%**]
5. Configure both automatic searches on log files as well as automatic running of important security applications to properly monitor a CentOS Linux Server for malicious activity – [**20%**]

Lab #9 – Assessment Worksheet

Applying Best Practices for Security Logging and Monitoring

Course Name and Number: _____

Student Name: _____

Instructor Name: _____

Lab Due Date: _____

Overview

In this lab, you configured remote logging on the CentOS Linux Server and sent syslogs to a remote host for secure secondary logging. You used Tripwire, a third-party file integrity tool, to identify modifications to important system files. You configured Rootkit Hunter, (rkhunter), to search for rootkits and other anomalies on a set schedule. You also searched the log files for specific criteria.

Lab Assessment Questions & Answers

1. What is the primary place to store log files on a local Linux system, and what are recommended procedures for that location?

   Note following Part 1, Step 22. The /var directory is where all the system logs go by default on the local system. It is best practice to create a /var partition so that attacks or over-subscription of the disk due to logging activity does not hamper the rest of the system from performing its business function.

2. Why is remote logging to a central server considered a best practice?

   Introduction Locating the system logs for all servers on a single server provides a more secure location for all logging. Suppose an intruder breaks into a Linux system and deletes all of the local log files. Unless the intruder also compromises the remote logging server, the log files will still be available to access and analyze.

3. Why is the Tripwire application considered a file integrity checker?

   Introduction. Tripwire keeps a database hash of all files specified in its policy file. Any time a file is altered, Tripwire will detect the changes.

4. Could rkhunter be considered a file integrity checker? Why or why not?

   Introduction. Yes. Rkhunter is a script that checks for various rootkits, a type of malicious software that enables unauthorized users access to the server without being detected. It also performs checks on common commands and startup files to determine if they have been modified, among other things.

5. How would you check to see that a recurring cron job was scheduled to run?

   Note following Part 3, Step 16. Use crontab -l to list.

6. What is the difference between the site and local passphrases used by Tripwire?

   Note introducing Part 2. The site passphrase encrypts the Tripwire configuration and policy files, so that it wouldn't be possible to view or change either file without the passphrase. The local passphrase would be used to protect the Tripwire database files.

7. What is a security implication of locating the syslog service on a system with Internet access?

   Introduction. System logs open the Internet are also vulnerable to denial of service attacks, which may fill up the system log to the point where it cannot log any other messages.

Lab #10 Defining Linux OS and Application Backup and Recovery Procedures

Introduction

A well-documented and tested disaster recovery process should be a part of any organization's defense-in-depth security strategy. As part of the disaster recovery process, the security team should make regular backups of the systems. One such method, in the Linux server environment, is to use the tar command to create an archive which contains the files and folder structure of the targeted directory. This archive can then be compressed so as to take up less space. Compression is the process of encoding data to use fewer bits, thus making it smaller. Compressed data by itself, however, is not considered secure.

Encrypting backups should be as expected as encrypting communications on the network. Encryption helps to secure data so unauthorized entities can't read or access it. Encryption converts the data into ciphertext, making it unreadable without a key or passphrase.

Compromised backups are one of the primary ways of stealing corporate data. Backups may contain all of the information, including private customer and company confidential data in an organization. Emails, like backups, if not encrypted could contain huge amounts of potentially sensitive information and thus should be secured both in transit and at rest on the server. If emails aren't encrypted, it becomes much easier for intruders to sniff traffic for emails and reconstruct all of the captured plaintext information.

Sometimes a file may have been inadvertently deleted while a program is in the middle of accessing it. In such cases, instead of locating an appropriate archive from which to restore a copy of the file, it may be possible to recover the file without resorting to a backup as the file may still reside under the /proc directory.

In this lab, you will maximize availability and define a recovery time objective (RTO) for data file backups and recovery on a production CentOS Linux server. You will secure a data file backup using OpenSSL encryption and restore the data file from the encrypted backup. You also will recover a deleted file using the /proc recovery function.

This lab has four parts, which should be completed in the order specified.

1. In the first part of the lab, you will back up a file on the Linux OS and then secure it with encryption.
2. In the second part of the lab, you will delete a file and then use decryption to restore the file on the Linux OS. You also will document the RTO for this process.
3. In the third part of the lab, you will identify the process ID (PID) from a deleted file and restore the file using the built-in Linux OS virtual filesystem called /proc.

4. Finally, if assigned by your instructor, you will explore the virtual environment on your own to answer a set of challenge questions that allow you to use the skills you learned in the lab to conduct independent, unguided work, similar to what you will encounter in a real-world situation.

Learning Objectives

Upon completing this lab, you will be able to perform the following:

- Ensure Linux OS, application, and data availability with documented backup and recovery procedures
- Configure and perform backups within the Linux operating system as an automated and stable way of enhancing backup and recovery procedures and maximizing system availability
- Encrypt backups in the Linux operating system as they are being performed and for securing data backups and storage
- Restore encrypted backups for full recovery of the Linux OS as per defined recovery time objectives (RTO)
- Backup and restore deleted files using /proc in Linux so that an entire system does not have to be restored in the instance of a deleted or corrupted file

Tools and Software

The following software and/or utilities are required to complete this lab. Students are encouraged to explore the Internet to learn more about the products and tools used in this lab.

- None

Deliverables

Upon completion of this lab, you are required to provide the following deliverables to your instructor:

1. Lab Report file including screen captures of the following steps: Part 1, Step 13; Part 2, Step 10; Part 3, Steps 7, 11, and 17;
2. Lab Assessments file;
3. Optional: Challenge Questions file, if assigned by your instructor.

Hands-On Steps

▶Note:
This lab contains detailed lab procedures, which you should follow as written. Frequently performed tasks are explained in the Common Lab Tasks document on the vWorkstation desktop. You should review these tasks *before* starting the lab.

1. From the vWorkstation desktop, **open** the **Common Lab Tasks file**.

   If you desire, use the File Transfer button to transfer the file to your local computer and print a copy for your reference.

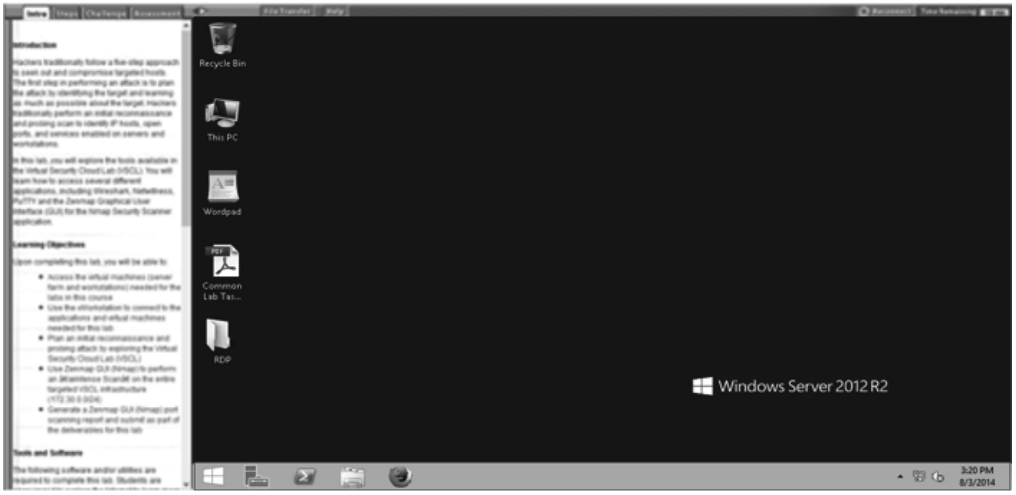


Figure 1 "Student Landing" vWorkstation

2. On your local computer, **create** the **lab deliverable files**.
3. **Review** the **Lab Assessment Worksheet** at the end of this lab. You will find answers to these questions as you proceed through the lab steps.

Part 1: Back Up a Data File on the Linux OS

▶Note:
In the next steps, you will back up a data file on the Linux OS. You will secure the backup file, encrypt it using the openssl command, and then remove the unencrypted data file.

1. **Double-click** the **RDP folder** on the vWorkstation desktop.
2. **Double-click** the **TargetCentOS01.rdp file** to open the Linux server.

   The remote GNOME desktop, the graphical user interface (GUI) for the virtual Linux server, opens with the IP address of the remote machine (172.30.0.21) in the title bar at the top of the window.

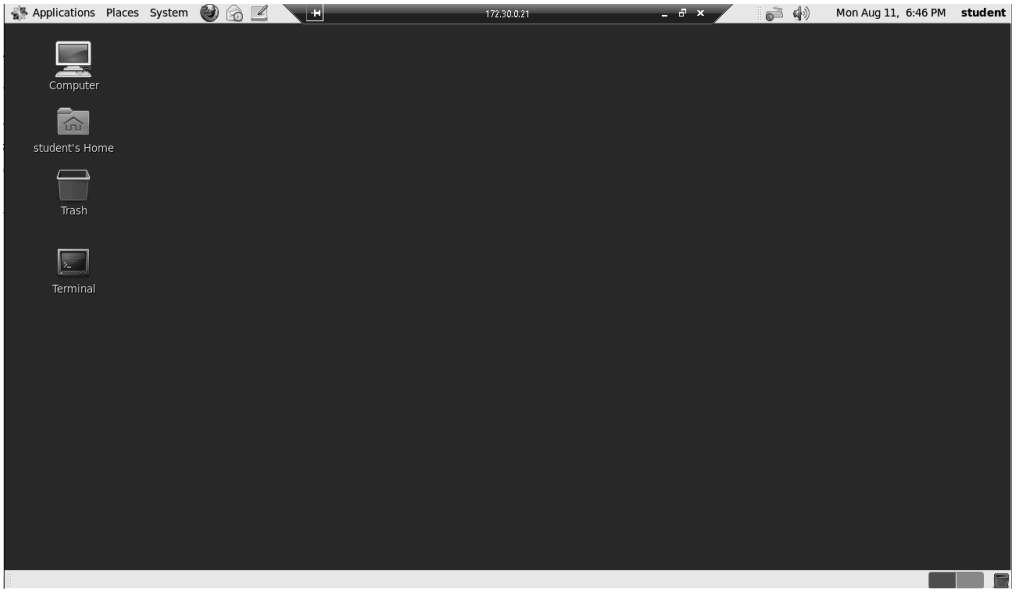


Figure 2 The GNOME desktop

3. **Double-click** the **Terminal icon** on the GNOME desktop to open the terminal emulator and access the Linux server command line.

4. At the command prompt, **type pwd** and **press Enter** to verify that you are in the home directory.

   The system will return the current directory as /home/student.

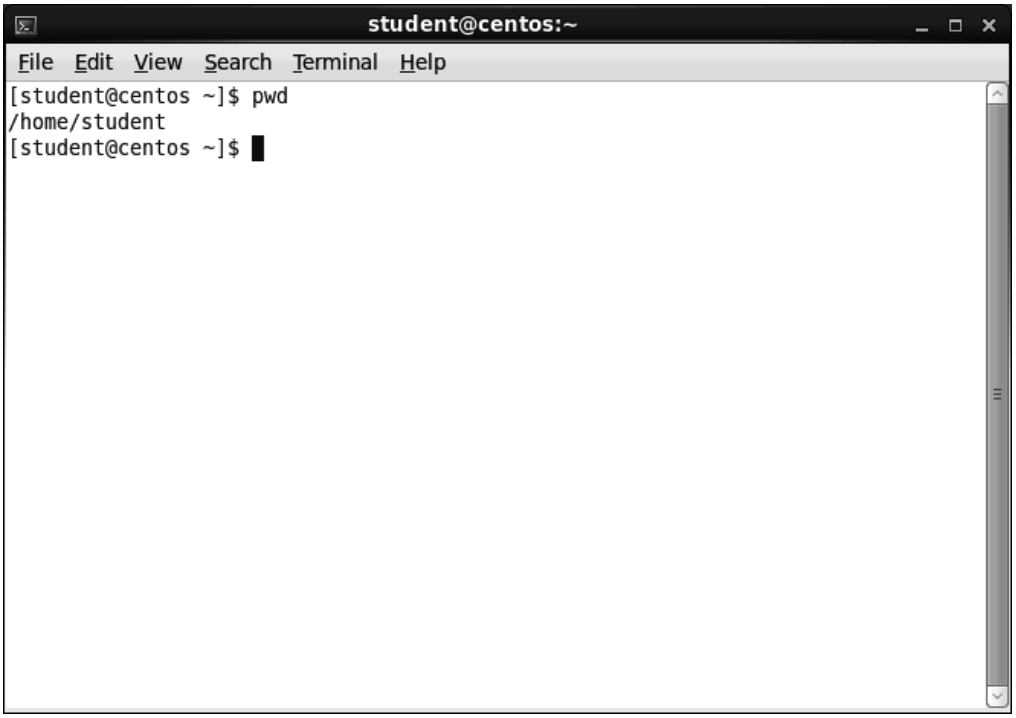


Figure 3 Verify the working directory

5. At the command prompt, **type su -c ' tar zcvf *yourname*.tar.gz /etc /var '**, replacing *yourname* with your own name, and **press Enter** to archive and compress the /etc and /var directories for backup.

▶Note:
The tar command is used to combine multiple files into a single file, while still preserving the complete pathname information. It can be used with several switch options, such as the zcvf switch used in this example.

- -z: unzip a compressed tar ball
- -c: create an archive
- -v: provide verbose output (display progress) for executed command
- -f: force the command even if there are errors
- -C: provide directory as root directory when extracting

Another switch that can be used with the tar command is the –x switch, which extracts the contents of the tar ball. You will use this switch later in the lab.

6. When prompted, **type P@ssw0rd!**, the root password, and **press Enter**.

▶Note:
You are required to enter a mixed-case password. If you are not using the Citrix Receiver to access this lab, please use the CAPS LOCK button or the On-Screen Keyboard to input the password.

The system will return all directories and files as they are backed up. This may take several minutes. Once the backup process is complete, the system will create a new

compressed file named *yourname*.tar.gz containing the contents of the /etc and the /var directories.

7. At the command prompt, **type su -c ' openssl des3 -salt -in *yourname*.tar.gz -out *yourname*.tar.gz.des3 '** and **press Enter** to encrypt the file.

8. When prompted, **type P@ssw0rd!**, the root password, and **press Enter**.

▶Note:
You are required to enter a mixed-case password. If you are not using the Citrix Receiver to access this lab, please use the CAPS LOCK button or the On-Screen Keyboard to input the password.
To finalize the encryption process, the system will prompt you for an encryption password that will be required to decrypt the file later. In the virtual lab, you use simple, easy to remember, passwords, but in a real-world situation you would want to choose a more complex password to encrypt your backup files.

9. When prompted to enter a des-ede3-cbc encryption password, **type mypassword** and **press Enter**.

10. When prompted to verify the des-ede3-cbc encryption password, **type mypassword** and **press Enter**.

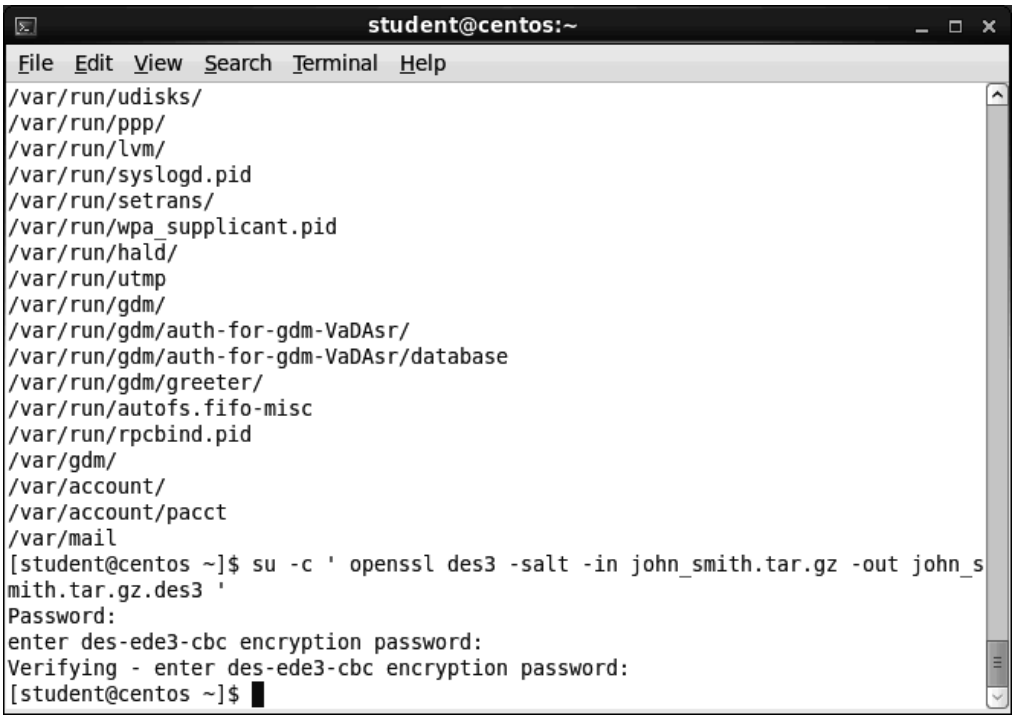


Figure 4 Create a password for the des3 encrypted file

11. At the command prompt, **type ls *yourname*.tar.gz.des3** and **press Enter** to verify that the new encrypted file has been created.

▶Note:
The system will return the *yourname*.tar.gz.des3 filename. If the system returns a *No such file or directory* message, confirm your spelling in step 11, or repeat steps 7-11 to ensure that the file is created correctly.

12. At the prompt, **type rm -f *yourname*.tar.gz** and **press Enter** to delete (remove) the original unencrypted compressed backup file.

13. **Make a screen capture** of the terminal window showing the **string of commands for the encryption process** and **paste** it into the Lab Report file.

Part 2: Restore a Deleted File using an Encrypted Backup

▶Note:
In the next steps, you will simulate a scenario in which a required file is deleted. First, you will "delete" the file, then you will decrypt the backup copy of that file using the provided password and use that copy to restore the "deleted" file. Throughout this process, you will be track the time it takes to restore the file. In other words, you will be recording the recovery time. The recovery time objective (RTO), the timeframe within which an essential business process or file must be restored after a disaster, is an important measurement for IT support professionals.

1. At the command prompt, **type su -c ' mv /etc/mail/sendmail.mc /tmp '** and **press Enter** to move the sendmail.mc file into the /tmp directory simulating a deleted sendmail configuration file.

2. When prompted, **type P@ssw0rd!**, the root password, and **press Enter**.

▶Note:
You are required to enter a mixed-case password. If you are not using the Citrix Receiver to access this lab, please use the CAPS LOCK button or the On-Screen Keyboard to input the password.

3. In the Lab Report file, **record** the **time** you started this set of steps.

   Record the time using the Linux machine's system clock which is displayed in the upper-right corner of the remote Linux desktop.

4. At the command prompt, **type su -c ' openssl des3 -d -salt -in *yourname*.tar.gz.des3 -out *yourname*.tar.gz '**, replacing *yourname* with your own name in both instances, and **press Enter** to decrypt the backup file.

5. When prompted, **type P@ssw0rd!**, the root password, and **press Enter**.

▶Note:
You are required to enter a mixed-case password. If you are not using the Citrix Receiver to access this lab, please use the CAPS LOCK button or the On-Screen Keyboard to input the password.

6. When prompted for the des-ede3-cbc decryption password, **type mypassword**, the encryption password for this file, and **press Enter**.

   The decryption process will take several minutes. Do not touch any keys until the command prompt returns.

7. At the command prompt, **type su -c ' tar zxvf *yourname*.tar.gz -C / etc/mail/sendmail.mc '** and **press Enter** to restore the sendmail configuration file from the backup file to its appropriate location.

8. When prompted, **type P@ssw0rd!**, the root password, and **press Enter**.

▶Note:
You are required to enter a mixed-case password. If you are not using the Citrix Receiver to access this lab, please use the CAPS LOCK button or the On-Screen Keyboard to input the password.

9. At the command prompt, **type ls /etc/mail/sendmail.mc** and **press Enter** to verify that the sendmail.mc file has been restored.

▶Note:
The system will return the sendmail.mc filename. If the system returns a No such file or directory message, confirm your spelling in step 9 or repeat steps 4-9 to ensure that the file is created.

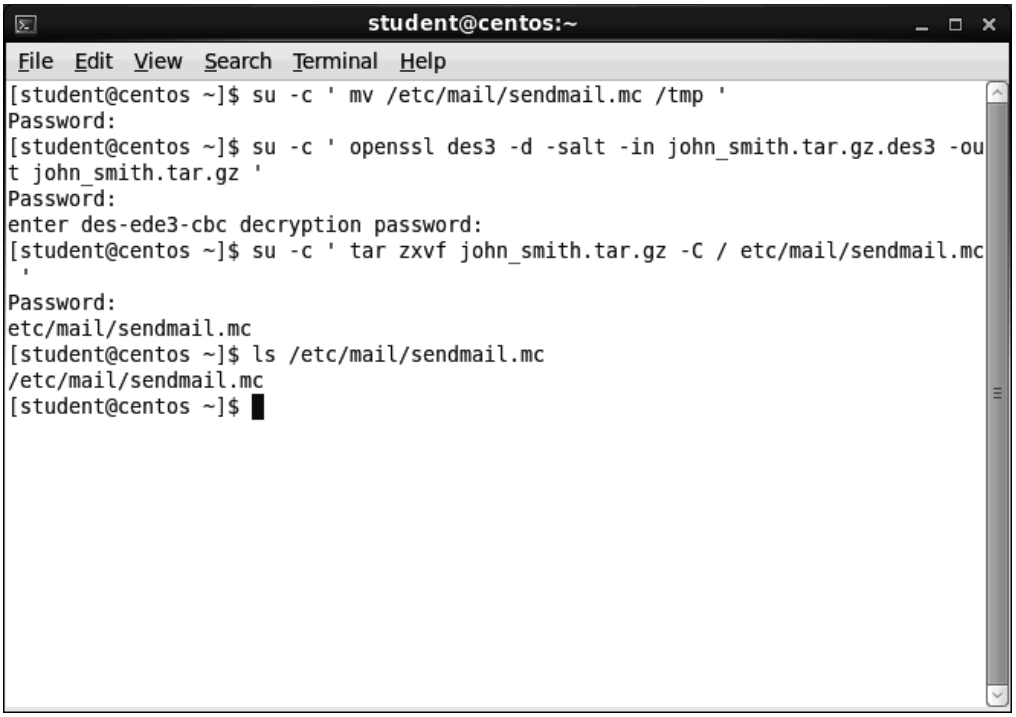


Figure 5 Restore the sendmail.mc data file

10. **Make a screen capture** of the terminal window showing the **results of the ls /etc/mail/sendmail.mc command** and **paste** it into the Lab Report file.

11. In the Lab Report file, **record** the **time** you completed this set of steps.

    Record the time using the Linux machine's system clock which is displayed in the upper-right corner of the remote Linux desktop.

12. In the Lab Report file, **record** the **RTO** (*RTO=stop time* minus *start time*) for the recovery of the sendmail.mc file.

▶Note:
The recovery time objective (RTO) for an organization can be adjusted for mission critical applications by giving priority to stored backups of systems, applications, and data files in order to meet company-specific goals for the RTO. The automation of recovery steps from backup data files can also help achieve a desired RTO.

Part 3: Restore a Deleted File using the Process ID (PID)

▶Note:
In the next steps, you will restore a deleted file that was not captured in a backup data file. The system will hold deleted files in memory for a period of time with a process ID number (PID). As long as the file is still being referenced by the less command, you can restore it.

First, you will create a new file (hacked.sh) that is not a part of the *yourname*.tar.gz backup and then you will delete it. Finally, you will restore the deleted file using the /proc command.

1. At the command prompt, **type vi hacked.sh** and **press Enter** to open a new file called hacked.sh in the VI Editor.

2. **Press** the **i key** to enter the Insert mode.

3. Use the arrow keys to **locate** the **first blank line** in the file and **type You have been hacked!**.

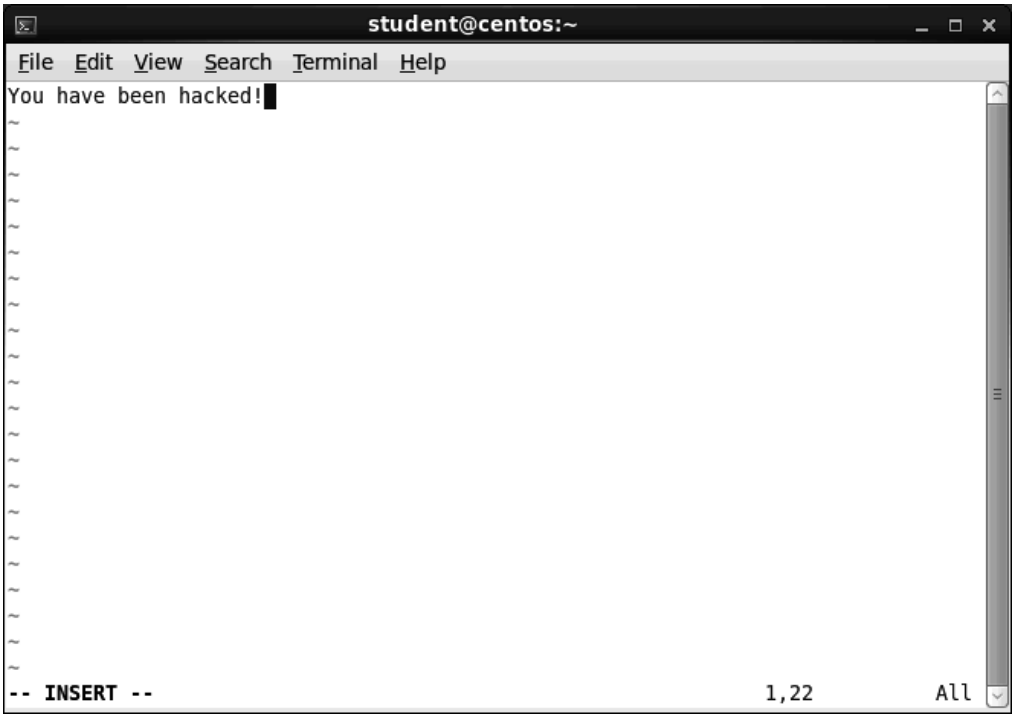


Figure 6 Create a new hacked.sh file

4. **Press** the **Esc key** to exit the Insert mode.
5. **Type :wq!** and **press Enter** to save your changes and exit the vi Editor.
6. At the command prompt, **type less hacked.sh** and **press Enter** to view the contents of the hacked.sh file you just created.
7. **Make a screen capture** showing **your contents of the hacked.sh file** and **paste** it into the Lab Report File.
8. **Press** the **CTRL+Z keys** to exit the less screen.

▶Note:
The CTRL+Z key pair puts the *less hacked.sh* session in a suspended state, which means that the process still exists, as opposed to existing the session outright.

9. At the command prompt, **type rm -f hacked.sh** and **press Enter** to delete the hacked.sh file.
10. At the command prompt, **type /usr/sbin/lsof | grep hacked** and **press Enter** to verify that the file is still being referenced by the less command, and obtain the process ID (PID).

▶Note:
The *lsof* command is used to *list* (ls) *open files* (of) on the system, along with the processes that are opening the files. The result of this step shows that the hacked.sh file is still opened by the less process despite the file having been deleted from the filesystem. Until the less process releases its hold on the hacked.sh file, the file still exists, even though it is no longer on the filesystem itself. The PID is a numeric reference number for the file. In this figure, the PID is 2642. Your number may be different.

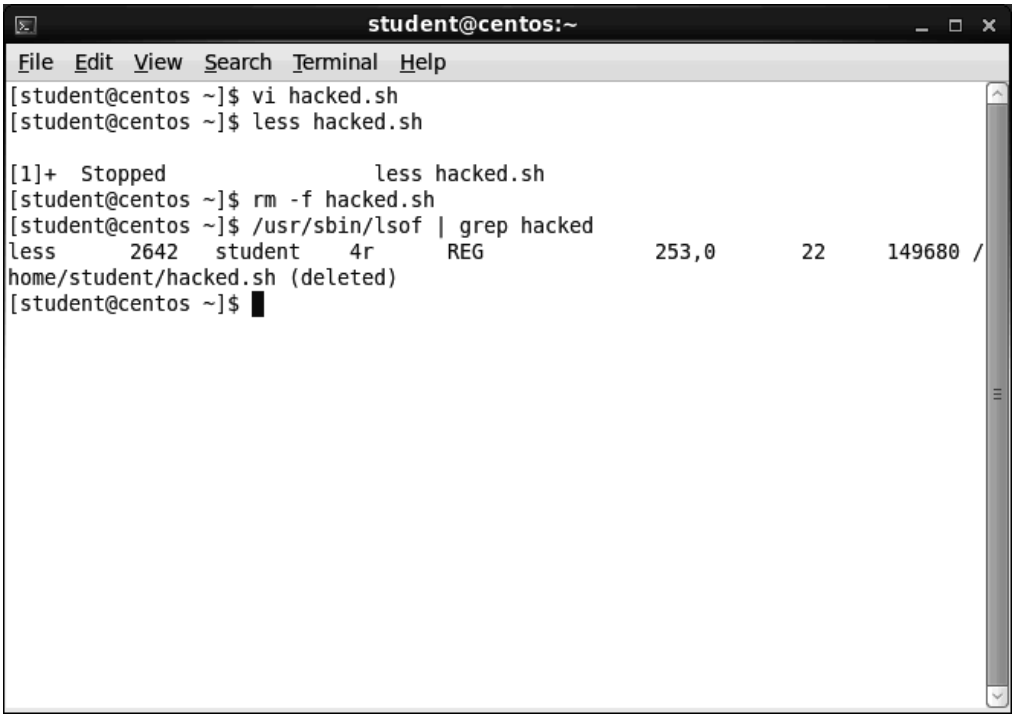


Figure 7 Find the PID for the hacked.sh file

11. **Make a screen capture** showing **the process ID** and **paste** it into the Lab Report File.

12. At the command prompt, **type cd /proc/*PID*/fd/**, replacing *PID* with the process ID you documented in step 11, and **press Enter** to find the file in the system memory.

▶Note:
A virtual filesystem, /proc doesn't contain actual files, but instead contains runtime system information such as system memory, devices mounted, and hardware configuration. Thus, this pseudo-filesystem can be regarded as a control and information center for the Linux kernel. Therefore, even though the file has been deleted the file remains in the /proc directory as long as the file is still being used. When a file in Linux is deleted, it is "unlinked." The inode contains the files data, and the inode is still there as long as the file is still being used.

13. At the command prompt, **type ls -ls** and **press Enter** to locate the file descriptor associated with the deleted file.

    Though several file descriptors may be returned, the correct descriptor will reference the previous location of the deleted file (/home/student/hacked.sh). In the following figure, the file descriptor for the deleted file is 4.

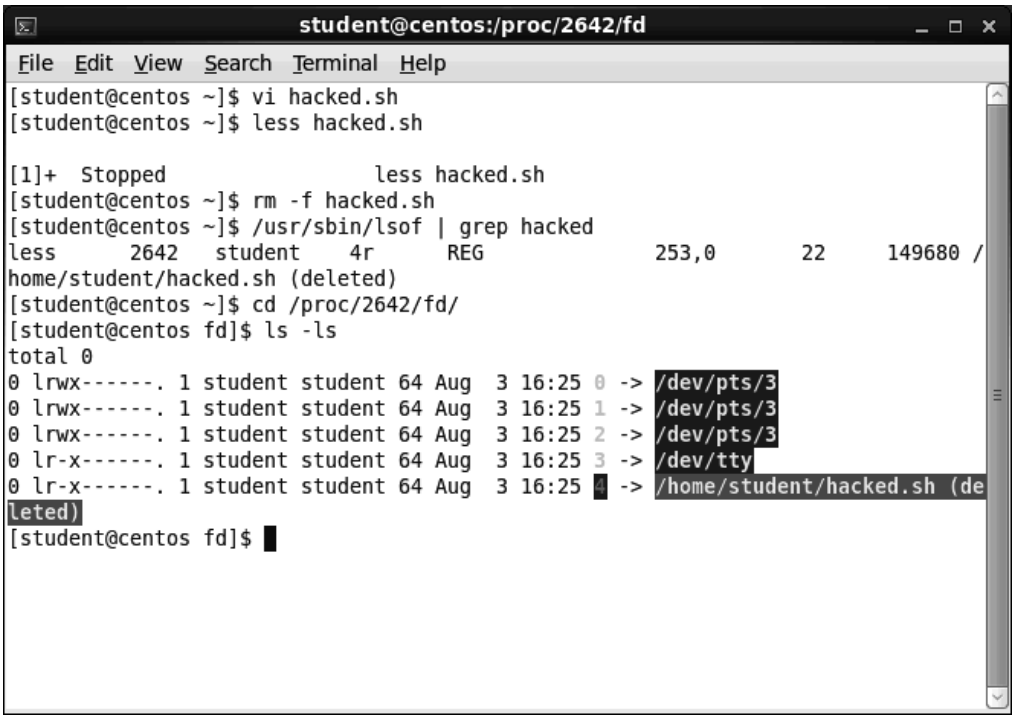


Figure 8 Find the file descriptor for the hacked.sh file

14. In the Lab Report file, **record** the **file descriptor** for the hacked.sh file.

15. At the command prompt, **type cp *descriptor* /home/student/hacked.recovered**, replacing *descriptor* with the file descriptor you recorded in step 14, and **press Enter** to recover the file by copying the file descriptor to the hard drive.

16. At the command prompt, **type cat /home/student/hacked.recovered** and **press Enter** to view the contents of the recovered file.

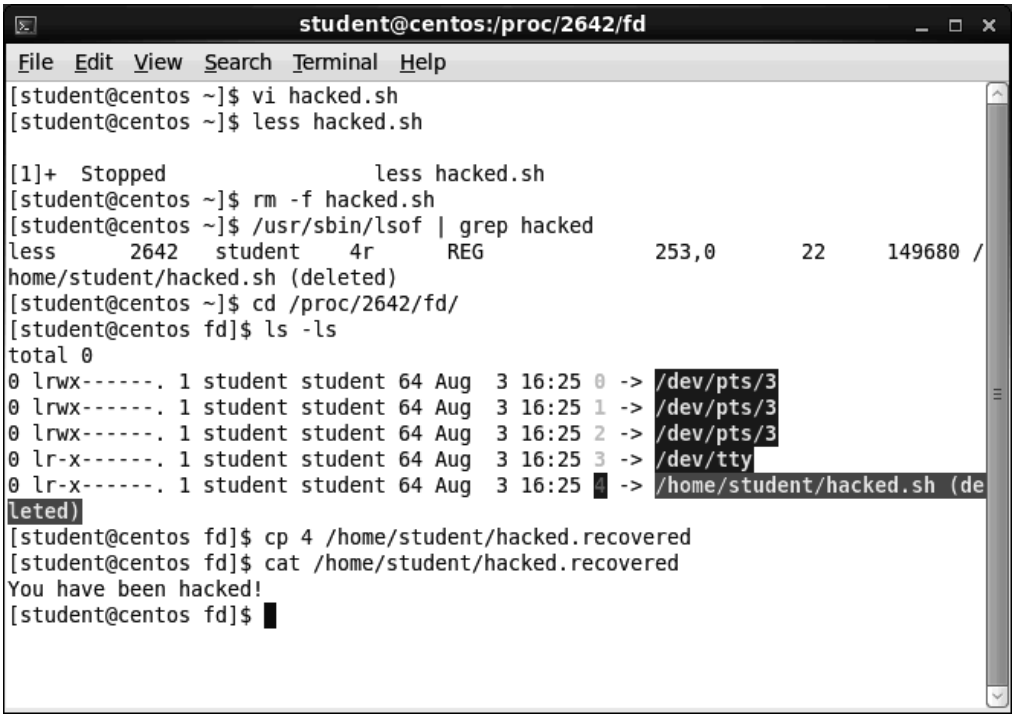


Figure 9 Recover the hacked.sh file

17. **Make a screen capture** showing the **results of the file recovery** and **paste** it into the Lab Report file.

18. **Close** the **remote Linux connection**.

19. **Close** the **virtual lab**, or proceed with Part 4 to answer the challenge question for this lab.

Part 4: Challenge Question

▶Note:
The following challenge question is provided to allow independent, unguided work, similar to what you will encounter in a real situation. You should aim to improve your skills by getting the correct answer in as few steps as possible. Use screen captures in your lab document where possible to illustrate your answers.

1. In Part 2, Step 4 of this lab you used the openssl command with the -salt option while encrypting the backup file. Why is the -salt option used?

   The -salt option should always be used if the encryption key is being derived from a password. Without the -salt option, it is possible to perform efficient dictionary attacks on the password and to attack stream cipher encrypted data. Without the -salt option, the same password always generates the same encryption key; with the option, a random key is generated when encrypting the file.

   If the same password generates the same encryption key, then it is possible for an attacker to use a rainbow table. A rainbow table is a pre-compiled list of hashes derived from a set of dictionary-based inputs. By comparing the encryption key against the rainbow table, the attacker may be more likely to determine what the original password is.

▶Note:
This completes the lab. **Close** the **virtual lab**, if you have not already done so.

Evaluation Criteria and Rubrics

The following are the evaluation criteria for this lab that students must perform:

1. Ensure Linux OS, application, and data availability with documented backup and recovery procedures – [**20%**]
2. Configure and perform backups within the Linux operating system as an automated and stable way of enhancing backup and recovery procedures and maximizing system availability – [**20 %**]
3. Encrypt backups in the Linux operating system as they are being performed and for securing data backups and storage – [**20%**]
4. Restore encrypted backups for full recovery of the Linux OS as per defined recovery time objectives (RTO) – [**20%**]
5. Backup and restore deleted files using /proc in Linux so that an entire system does not have to be restored in the instance of a deleted or corrupted file – [**20%**]

Lab #10 – Assessment Worksheet

Defining Linux OS and Application Backup and Recovery Procedures

Course Name and Number: _____

Student Name: _____

Instructor Name: _____

Lab Due Date: _____

Overview

In this lab, you maximized availability and defined a recovery time objective (RTO) for data file backups and recovery on a production CentOS Linux server. You secured a data file backup using OpenSSL encryption and restored the data file from the encrypted backup. You also recovered a deleted file using the /proc recovery function.

Lab Assessment Questions & Answers

1. Why is encrypting an already compressed file necessary?

   Introduction. Encryption and compression are two different things. Compression is the process of encoding data to use fewer bits, thus making it smaller. Compressed data by itself, however, is not considered secure. Encryption converts the data into ciphertext, making it unreadable without a key or passphrase.

2. Why is it best practice to encrypt backups?

   Introduction. Compromised backups are one of the primary ways of stealing corporate data. Backups may contain all of the information, including private customer and company confidential data in an organization. Regular backups should be part of the disaster recovery process and a defense-in-depth strategy. Encrypting backups should be as expected as encrypting communications on the network. Encryption helps to secure data so unauthorized entities can't read or access it.

3. Why is performing messaging, such as e-mails, in an encrypted fashion recommended as part of a secure communications strategy? Explain.

   Introduction. E-mails, like backups, if not encrypted, could contain huge amounts of potentially sensitive information and thus should be secured both in transit and at rest on the server. If e-mails aren't encrypted, it becomes much easier for intruders to sniff traffic for e-mails and reconstruct all of the captured plaintext information.

4. Explain each of the switches used in the following command: **tar zxvf fwbsl.tar.gz etc/mail/sendmail.mc -C / etc/mail**

   Note following Part 1, Step 5.
   - -z: Unzips a compressed tarball
   - -x: Extracts the contents of a tarball
   - -v: Provides verbose output to a tarball command that is being executed
   - -f: Force the command even if there are errors
   - -C: Use provided directory as root directory when extracting

5. How is it possible to recover a deleted file from the pseudo filesystem /proc?

   Note following Part 3, Step 12. A virtual filesystem, /proc doesn't contain actual files, but instead contains runtime system information such as system memory, devices mounted, and hardware configuration. Thus, this pseudo-filesystem can be regarded as a control and information center for the Linux kernel. Therefore, even though the file has been deleted the file remains in the /proc directory as long as the file is still being used. When a file in Linux is deleted, it is "unlinked." The inode contains the files data, and the inode is still there as long as the file is still being used.

6. If the recovery time objective (RTO) was unacceptable to your organization's business continuity plan, what could you do to ensure that you achieve the desired RTO for data files, applications, or systems?

   Note following Part 2, Step 12. The recovery time objective (RTO) for an organization can be adjusted for mission-critical applications by giving priority to stored backups of systems, applications, and data files in order to meet company-specific goals for the RTO. The automation of recovery steps from backup data files can also help achieve a desired RTO.

7. What descriptor did you record in Part 3, Step 14 of this lab?

   Part 3, Step 14 (Number actually used in step 15). (Answers will be unique to each student.)