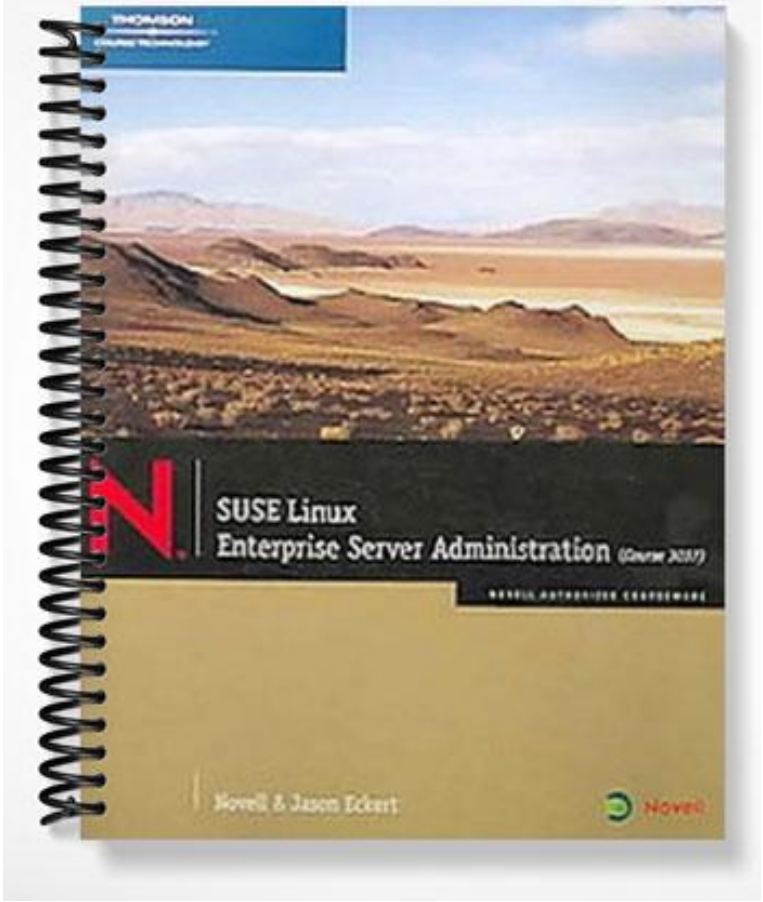
SOLUTIONS MANUAL



Chapter 2

Manage User Access and Security

At a Glance

Instructor's Manual Table of Contents

Lecture Notes

Overview

Chapter 2 describes basic Linux user security features. Students will learn to manage Linux users and groups. Next, students will learn to manage and secure the Linux user environment. Chapter 2 also shows how to secure files and directories with permissions and how to configure user authentication with PAM. Finally, students will implement and monitor enterprise security policies.

Objectives

- Describe Basic Linux User Security Features
- Manage Linux Users and Groups
- Manage and Secure the Linux User Environment
- Secure Files and Directories with Permissions
- Configure User Authentication with PAM
- Implement and Monitor Enterprise Security Policies

Teaching Tips

Describe Basic Linux User Security Features

1. This section describes the main points to maintain a secure environment, including:
    a. File System Security Components
    b. Users and Groups
    c. Ownership and Access Permissions

File System Security Components

1. Describe the Linux file system types of components, including:
    a. Users
    b. Groups
    c. Ownerships
    d. Permission

Users and Groups

1. Define the user ID (UID) as the user number assigned to each user, and the group ID (GID) as the number that represents the group to which the user is a member.

2. Explain that the command *id* displays the user's UID and the groups she is assigned. The command *groups* displays the groups in which a user is a member. Finally, the command *finger* displays additional information about local users.

3. Explain that regular user accounts allow employees and others to log in to the Linux environment. System user accounts are used by services, utilities, and other applications to run effectively on the server.

4. Mention that in a private scheme, a user is assigned his own group that he can manage. In a public scheme, a user is assigned to a general, public group.

5. Explain that each user has a user account identified by a login name and a personal password. Additionally, each user has a directory in the directory /home/.

6. Describe the information stored in the /etc/passwd file. Use Figure 2-3 to illustrate your explanation.

Teaching Tip	For more information about the /etc/passwd file visit: www.cyberciti.biz/faqs/2006/02/understanding-etcpasswd-file-format.php.

7. Explain the information stored in the /etc/shadow file. Use Figure 2-5 to illustrate your explanation.

Teaching Tip	Read more about the /etc/shadow file at: www.cyberciti.biz/faqs/2006/02/understanding-etcshadow-file.php.

8. Describe the information stored in the /etc/group file. Use Figure 2-6 to illustrate your explanation.

9. Explain how to check /etc/passwd and /etc/shadow using commands such as:
    a. tail
    b. pwconv
    c. pwck

Exercise 2-1 Check User and Group Information on Your Server

1. In this exercise you will check the user and group information on your SLES 9 server.

Ownership and Access Permissions

1. Explain that each file and directory in the file system is assigned access permissions. Permissions determine the level of access a given user has.

2. Describe the permission levels, including
    a. Owner
    b. Group
    c. Other

Manage Linux Users and Groups

1. This section describes the tasks involved in managing Linux users and groups:
    a. Create and Edit User Accounts with YaST
    b. Create and Edit Groups with YaST
    c. Edit User Account Properties
    d. Configure Account Password Settings
    e. Manage User Accounts from the Command Line
    f. Manage Groups from the Command Line
    g. Create Text Login Messages

Create and Edit User Accounts with YaST

1. Explain that you can use the Edit and Create Users module in YaST to create, edit, and delete Linux user accounts.

2. Describe how to create and edit user account with YaST as explained in this chapter. Use Figure 2-7 and Figure 2-8 to illustrate your explanation.

Create and Edit Groups with YaST

1. Explain that you can use the Edit and Create Groups module in YaST to create, edit, and delete Linux groups.

2. Describe how to create and edit groups with YaST as explained in this chapter. Use Figure 2-9 and Figure 2-10 to illustrate your explanation.

Edit User Account Properties

1. Explain that you can use YaST to edit user account properties.

2. Describe how to edit user account properties with YaST as explained in this chapter. Use Figure 2-11 to illustrate your explanation.

Configure User Account Password Settings

1. Explain that you can use YaST to configure user account password settings.

2. Describe how to configure user account passwords with YaST as explained in this chapter. Use Figure 2-12 to illustrate your explanation.

Manage User Accounts from the Command Line

1. Describe the commands that a root user can user to manage user accounts, including:
    a. useradd
    b. userdel
    c. usermod
    d. passwd

Manage Groups from the Command Line

1. Describe the commands that a root user can user to manage groups, including:
    a. groupadd
    b. groupdel
    c. groupmod

Teaching Tip	Read more about user accounts and group management at: www.cae.wisc.edu/site/public/?title=linaccounts.

Create Text Login Messages

1. Explain that text login messages are useful for displaying information when a user logs in from a terminal window, a virtual terminal, or remotely (such as an ssh login).

2. Describe the files that you can modify to create text login messages, including:
    a. /etc/issue
    b. /etc/motd

Exercise 2-2 Create and Manage Users and Groups from the Command Line

1. In this exercise you will set up your SLES 9 server with user accounts and groups to help train the database administrators in your Digital Airlines office.

Quick Quiz 1

1. The file _____ stores group information.
   Answer: /etc/group

2. User configuration is handled with two files (/etc/passwd and _____).
   Answer: /etc/shadow

3. The _____ command lets you change a user's password.
   Answer: passwd

4. Edit the _____ file to configure an initial message of the day.
   Answer: /etc/motd

Manage and Secure the Linux User Environment

1. This section explains how to perform the following tasks:
    a. Perform Administrative Tasks as root
    b. Delegate Administrative Tasks with sudo
    c. Set Defaults for New User Accounts
    d. Configure Security Settings

Perform Administrative Tasks as root

1. Explain how to use the su command to switch to another user as described in this chapter.

2. Describe how to use the newgrp or sg commands to switch to another group as explained in the book.

3. Explain how to start programs as another user from KDE as described in this chapter. Use Figure 2-13 to illustrate your explanation.

Delegate Administrative Tasks with sudo

1. Explain that sudo enables a command to be run by a normal user. The administrator needs to modify the configuration file /etc/sudoers to specify which commands a user can or cannot enter. You can modify this file using the command visudo.

2. Describe the structure of the /etc/sudoers configuration file. Use Figure 2-14 to illustrate your explanation.

Teaching Tip	Read more about the sudo command at: http://aplawrence.com/Basics/sudo.html.

Set Defaults for New User Accounts

1. Explain that you can use YaST to set defaults for new user accounts.

2. Describe how to set defaults for new user accounts with YaST as explained in this chapter. Use Figure 2-15 to illustrate your explanation.

Configure Security Settings

1. Describe the preset security settings, including:
    a. Level 1 (Home Workstation)
    b. Level 2 (Networked Workstation)
    c. Level 3 (Network Server)

2. Mention that you can create your own configuration. Use Figure 2-16 to illustrate your explanation.

3. Describe how to modify the password setting using YaST. Use Figure 2-17 to illustrate your explanation.

4. Explain how to modify the boot settings using YaST. Use Figure 2-18 to illustrate your explanation.

5. Describe how to modify the login setting using YaST. Use Figure 2-19 to illustrate your explanation.

6. Explain how to modify the adding user settings using YaST. Use Figure 2-20 to illustrate your explanation.

7. Describe how to modify the miscellaneous global setting using YaST. Use Figure 2-21 to illustrate your explanation.

Exercise 2-3 Configure the Password Security Settings

1. In this exercise you will configure the password security settings.

Secure Files and Directories with Permissions

1. This section explains what you need to know to set permissions for files and directories, including:
    a. Permissions and Permission Values
    b. How to Set Permissions from the Command Line
    c. How to Set Permissions from a GUI Interface
    d. How to Modify Default Access Permissions
    e. How to Configure Special File Permissions
    f. How to Configure Additional File Attributes for ext2

Permissions and Permission Values

1. Describe the permissions to a file or directory, such as:
    a. Read (r)
    b. Write (w)
    c. Execute (x)

2. Describe how to view permissions, owner, and group for each directory or file using the ls command or Konqueror. Use Figure 2-22 and Figure 2-23 to illustrate your explanation.

How to Set Permissions from the Command Line

1. Explain how to use the chmod command to add, remove, or assign permissions assigned to a file or directory. Use Figure 2-24 and Table 2-4 and Table 2-5 to illustrate your explanation.

Teaching Tip	Learn more about the chmod command at: http://en.wikipedia.org/wiki/Chmod.

2. Describe how to change the owner or group assigned to a file or directory using the chown and chgrp commands.

How to Set Permissions from a GUI Interface

1. Explain how to use the Konqueror in KDE to change permissions as described in this chapter. Use Figure 2-25 and Figure 2-26 to illustrate your explanation.

How to Modify Default Access Permissions

1. Explain that files are created with access mode 666 and directories with mode 777 by default.

2. Describe how to use the umask command to change the access mode permissions. Use Table 2-6 and Table 2-7 to illustrate your explanation.

How to Configure Special File Permissions

1. Use Table 2-8 to describe the special attributes, including:
    a. Sticky bit
    b. SGID
    c. SUID

How to Configure Additional File Attributes for ext2

1. Use Table 2-9 to describe the additional file attributes included in ext2 (and also available in ext3).

2. Explain how to use the chattr and lsattr commands to set and display these ext2 attributes. Use Table 2-10 and Table 2-11 to illustrate your explanation.

Exercise 2-4 Set Permissions for Files and Directories from the Command Line

1. In this exercise you will set permissions for files and directories from the command line.

Configure User Authentication with PAM

1. Define PAM as Pluggable Authentication Modules used by Linux in the authentication process as a layer that communicates between users and applications. PAM lets you configure and change authentication methods between users and individual applications.

Teaching Tip	For more information about PAM visit: www.kernel.org/pub/linux/libs/pam/.

Location and Purpose of PAM Configuration Files

1. Mention that PAM provides a variety of modules. The configuration files for these modules are located at /etc/pam.d/program_name. Use Figure 2-27 to illustrate your explanation.

2. Explain that in addition to these configuration files, global configuration files for most PAM modules are stored in /etc/security.

PAM Configuration File Structure

1. Use Figure 2-28 to describe the PAM configuration file structure.

PAM Configuration File Examples

1. Describe various PAM configuration file examples, including:
    a. pam_securetty.so
    b. pam_nologin.so

PAM Documentation Resources

1. Describe the PAM documentation available in directory /usr/share/doc, including:
    a. READMEs
    b. The Linux-PAM System Administrators' Guide
    c. The Linux-PAM Module Writers' Manual
    d. The Linux-PAM Application Developers' Guide

Exercise 2-5 Configure PAM Authentication for Digital Airlines Employees

1. In this exercise, you perform tests that prevent all normal users from logging in to see how PAM is used by the system.

Implement and Monitor Enterprise Security Policies

1. This section describes the following points:
    a. Guidelines for Implementing Security Policies
    b. Security Rules and Tips
    c. SuSE Security Information Resources
    d. How to Monitor Login Activity

Guidelines for Implementing Security Policies

1. Explain that the main goal of local security is to keep users separate from each other.

2. Mention that a Linux password is stored encrypted. Each time a password is entered, it is encrypted again and the encrypted strings are compared. If they match, access is granted to the user.

3. Explain that Boot procedure protection prevents your Linux system from booting using a floppy disk or CD.

4. Describe why you should always work with the most restrictive privileges possible for a given task. In addition, describe the special permission files in directory /etc/, such as:
    a. permissions
    b. permissions.easy
    c. permissions.secure
    d. permissions.paranoid

5. Describe the relationship between network security and local security.

Security Rules and Tips

1. Describe various security rules and tips, including:
    a. Use most restrictive set of permissions possible
    b. Use encrypted connections for a remote machine
    c. Avoid authentication based on IP addresses alone
    d. Keep network-related packages up-to-date
    e. Disable any network services you do not require
    f. Verify the integrity of any SUSE RPM package
    g. Check backups of user and system files regularly
    h. Check your log files
    i. Use SUSEfirewall
    j. Design your security measures to be redundant

SUSE Security Information Resources

1. Mention that you should install updated packages recommended by security announcements as soon as possible.

2. Describe how to subscribe to the SUSE security announcement list.

3. Describe other information resources, including:
    a. suse-securityannounce@suse.de list
    b. suse-security@suse.de mailing list
    c. bugtraq@securityfocus.com

How to Monitor Login Activity

1. Describe and explain various commands that you can use to monitor login activity, including:
    a. who
    b. w
    c. finger
    d. last
    e. lastlog
    f. faillog

Exercise 2-6 Change the Security Settings

1. SUSE provides configuration files for locking down your system. From a files perspective, there are three settings: easy, secure, and paranoid.

2. In this exercise, you change to the paranoid setting and observe the impact on the system.

Quick Quiz 2

1. You can use the _____ command to add, remove, or assign permissions assigned to a file or directory.
   Answer: chmod

2. To modify (restrict) the default access mode settings, you can use the command _____.
   Answer: umask

3. You can use the _____ PAM module to prevent users from logging into the system.
   Answer: pam_nologin.so

4. The _____ command formats and displays the contents of the failure log (/var/log/faillog) and maintains failure counts and limits.
   Answer: faillog

Class Discussion Topics

1. Why should you shadow your password file?

2. What are the main advantages and disadvantages of using PAM to authenticate users?

Additional Projects

1. Ask your students to explain the shadowing password process used by Linux.

2. Ask your students to use the Internet to research about the syslog command and find out how to use the syslog to track all sudo commands.

Additional Resources

1. Linux Password & Shadow File Formats
   www.tldp.org/LDP/lame/LAME/linux-admin-made-easy/shadow-file-formats.html

2. /etc/passwd File
   www.unet.univie.ac.at/aix/files/aixfiles/passwd_etc.htm

3. Configuring the shadow password file
   http://docsrv.sco.com:507/en/OSAdminG/uaD.shadow.html

4. Linux User Management
   www.comptechdoc.org/os/linux/commands/linux_cruserman.html

5. Linux Users and Sudo
   www.linuxhomenetworking.com/linux-hn/addusers.htm

6. Using sudo
   www.chinalinuxpub.com/doc/www.siliconvalleyccie.com/linux-hn/sudo.htm

7. Information about the Linux / UNIX chmod command
   www.computerhope.com/unix/uchmod.htm

Key Terms

- **/boot/grub/menu.lst** - The configuration file for the GRUB boot loader in SLES.
- **/etc/default/passwd** - A file that contains default values used when changing passwords such as encryption algorithm.
- **/etc/default/useradd** - A file that contains default values used when creating user accounts.
- **/etc/group** - The file that contains system groups and their members.
- **/etc/issue** - A text file that contains a message for users that log into a command-line terminal.
- **/etc/login.defs** - A file that contains default values used when creating user accounts.
- **/etc/motd** - A text file that contains a message (or “message of the day”) for users that log into a command-line terminal.
- **/etc/pam.d** - The directory that stores PAM configuration information for PAM programs.

- **/etc/passwd** - The file that contains user account information such as name, UID, primary group, home directory, and shell.
- **/etc/permissions.easy** - A file that lists the least secure file permission restrictions for system files.
- **/etc/permissions.local** - A file that lists user-defined file permission restrictions for system files.
- **/etc/permissions.paranoid** - A file that lists the most secure file permission restrictions for system files.
- **/etc/permissions.secure** - A file that lists secure file permission restrictions for system files.
- **/etc/security** - The directory that stores PAM configuration information for PAM modules.
- **/etc/shadow** - The file that typically contains encrypted passwords and password expiry information for user accounts on the system.
- **/etc/shells** - A file that lists valid system shells such as /bin/bash.
- **/etc/skel** - A directory that contains files and directories that are copied to all new users' home directories after they are created.
- **/etc/sudoers** - A file that lists the users who are allowed to run certain commands as other users.
- **/home** - The default directory used to store user home directories.
- **/root** - The root user's home directory.
- **/var/log/faillog** - A text file that lists failed login attempts.
- **/var/log/wtmp** - A text file that lists successful login attempts.
- **attributes** - Special flags on a file or directory that modify its usage. The read-only attribute prevents contents from being changed.
- **Blowfish** - An encryption method used to encrypt Linux passwords.
- **chattr** - Used to change the attributes on a file or directory.
- **chgrp (change group) command** - Used to change the group owner of a file or directory.
- **chmod (change mode) command** - Used to change the mode (permissions) of a file or directory.
- **chown (change owner) command** - Used to change the owner and group owner of a file or directory.
- **cuckoo egg** - A file that, when executed, creates a security problem.
- **Data Encryption Standard (DES)** - The default encryption method used in SLES for passwords.
- **effective group** - See **primary group**.
- **execute permission** - Allows you to execute files as well as access directory contents.
- **Ext2** - The traditional file system used on older Linux systems.
- **Ext3** - A journaling version of the Ext2 file system.
- **faillog command** - Displays the contents of /var/log/faillog.
- **finger command** - Displays information about local user accounts.
- **General Electric Comprehensive Operating System (GECOS)** - Represents a description of a user account stored in the comments field of /etc/passwd.
- **group** - When referring to a long file or directory listing, it represents the group ownership of a file or directory.
- **Group ID (GID)** - A number that uniquely identifies system groups.
- **groupadd command** - Used to add a group to the system.
- **groupdel command** - Used to delete a group from the system.

- **groupmod command** - Used to modify the name, membership, or GID of a group on the system.
- **groups command** - Displays the groups that a user is a member of.
- **id command** - Displays the UID and GIDs associated with a user account.
- **last command** - Displays the most recent users who have logged into the system from entries in /var/log/wtmp.
- **lastlog command** - Displays the most recent users who have logged into the system from entries in /var/log/lastlog.
- **locate command** - Used to search for files on the system via a pre-indexed database.
- **lsattr** - Used to list the attributes on a file or directory.
- **Message Digest 5 (MD5)** - An encryption method used to encrypt Linux passwords.
- **mkpasswd command** - Used to create an encrypted password for use with user or group accounts.
- **newgrp command** - Used to change the current primary group for a user account.
- **others** - When referring to a long file or directory listing, it represents all users on the Linux system that are not the owner or a member of the group on the file or directory.
- **owner** - The user whose name appears in a long listing of a file or directory and who typically has the most permissions to that file or directory.
- **passwd command** - Used to modify user passwords and expiry information as well as lock and unlock user accounts.
- **Pluggable Authentication Modules (PAM)** - A set of components that allow programs to access user account information.
- **primary group** - The group specified for a user in the /etc/passwd file that becomes the group owner on newly created files and directories.
- **private scheme** - A method that, during user creation, creates a new group for each user that can be managed by the user.
- **public scheme** - A method that places new users in a common group that is managed by the root user.
- **pwck command** - Used to check the validity of the /etc/passwd and /etc/shadow files.
- **pwconv command** - Used to convert entries from the /etc/passwd file to the /etc/shadow file.
- **Read permission** - Allows you to open and read files as well as list directory contents.
- **Red Hat Package Manager (RPM)** - A format used to distribute software packages on most Linux systems.
- **regular users** - User accounts that may be used to log in to the system interactively.
- **rpm command** - Used to install, remove, and find information on RPM software packages.
- **Set Group ID (SGID)** - A special permission set on executable files and directories. When you run an executable program that has the SGID permission set, you become the group owner of the executable file for the duration of the program. On a directory, the SGID sets the group that gets attached to newly created files.
- **Set User ID (SUID)** - A special permission set on executable files. When you run an executable program that has the SUID permission set, you become the owner of the executable file for the duration of the program.
- **shadow passwords** - Passwords that are stored in the /etc/shadow file instead of the /etc/passwd file.
- **sticky bit** - A special permission that is set on directories that prevents users from removing files that they do not own.
- **su (switch user) command** - Used to change the current user account.

- **sudo command** - Used to run commands as another user via entries in /etc/sudoers.
- **system users** - User accounts that may be used by system services and cannot be used by users to log in to the system interactively.
- **trapdoor algorithm** - An algorithm that encrypts data but cannot be used to decrypt it.
- **umask** - A system variable that removes permissions on all new files and directories.
- **umask command** - Used to view and change the system umask.
- **updatedb command** - Used to update the database used by the **locate** command.
- **user ID (UID)** - A number that uniquely identifies each system user account.
- **useradd command** - Used to add a user account to the system.
- **userdel command** - Used to remove a user account from the system.
- **usermod command** - Used to modify the properties of a user account on the system.
- **visudo command** - Used to edit the /etc/sudoers file with the vi text editor.
- **w command** - Displays the users currently logged in to the system and their processes.
- **who command** - Displays the users currently logged in to the system. It also can be used to display the contents of the /var/log/wtmp file.
- **write permission** - Allows you to open and edit files as well as add or remove directory contents.

Technical Notes for Discovery Exercises

Using the Skeleton Directory:

- This project requires root access to your SLES system.

Deleting Users:

- This project requires root access to your SLES system.

Setting File Ownership and Permissions:

- This project requires root access to your SLES system.

Researching PAM Modules:

- This project requires an Internet connection.