Fundamental of Linux Administration

By Jamilur Rahman

Topics

Basic Commands

Users and Groups Management

File Systems

Package Management

Storage System (Logical Volume Manager (LVM)> PV, VG, LV)

Linux Firewall

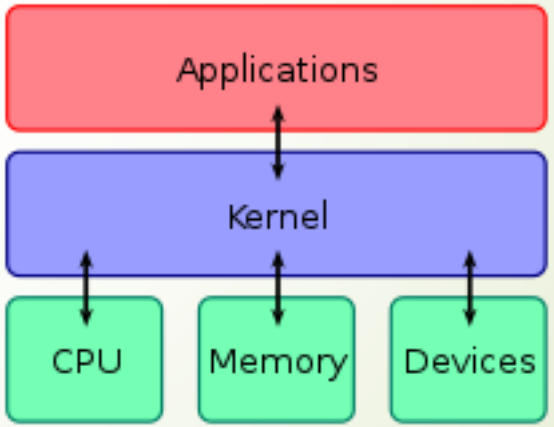
Logging

Scheduling a Job (cronjob)

Installation of different Services (mail server, DNS, web server etc.)

Introduction to Linux: What is Linux?

- Generally it is an Operating System
- But, by nature, it is not only an Operating System, it is the Kernel also.
- kernel is a computer program at the core of an operating system and has complete control over everything in the system. It directly communicates with underlying hardware.
- Linux is open source



Linux Distributions (Distros)

- As Linux is Open source, many people and organizations have modified the Linux Kernel along with other components.
- Thus different customized operating systems with different flavor of Linux is developed.
- Some Linux distros are designed with a specific purpose in mind.
- For example: Scientific Linux: A popular Linux distro, preinstalled with lots of scientific applications makes it number one choice in many scientists and respective community.
- For example: Kali Linux: used and designed for digital forensics and penetration testing.
- Popular Linux distros: Ubuntu, CentOS, RedHat, Debian, AlmaLinux, Fedora etc.

Users and Groups Management

- Linux is a multiuser and multigroup Operating System
- Many users and groups are allowed to access the system at the same time
- User information is stored in ***/etc/passwd*** file
- A group is a collection of users who share the same role or purpose
- All groups have their information stored in the ***/etc/group*** file

/etc/passwd file formation

```
  1    2  3    4          5                    6              7
elliot:x:1000:1000:Elliot Alderson:/home/elliot:/bin/bash
```

Field	What does it store?
1	This field stores the username.
2	This field usually has an `x` in it, which means the user's password is encrypted and stored in the file `/etc/shadow`.
3	This field stores the **UID (User ID)** number.
4	This field stores the primary **GID (Group ID)** of the user.
5	This field stores a comment on the user, which is usually the user's first and last name.
6	This field stores the path of the user's home directory.
7	This field stores the user's default shell.

/etc/group file formation

- Each line consists of 4 fields

```
1   2   3    4
sudo:x:27:elliot
```

Field	What does it store?
1	This field stores the group name.
2	This field usually has an `x` in it, which means the group password is encrypted and stored in the file `/etc/gshadow`.
3	This field stores the **GID (Group ID)** number.
4	This field stores the usernames of the group members.

User and Group Commands

- **useradd** command is used to add or remove a user on a Linux server.

Syntax: useradd username

- **passwd** command is used to create and change the password for a user.

Syntax: passwd **username**

- **userdel** command is used to delete any user

Syntax: userdel user_name

- **su** command provides administrative access to another user.

Syntax: su user_name

- **groupadd** command is used to create a user group.

Syntax: groupadd group_name

- **groupdel** command is used to delete any groups

Syntax: groupdel group_name

- **Usermod** is used to Add an Existing User to a Group

Syntax: usermod -a -G groupname username

- **gpasswd** command is used to Remove a User From a Group

Syntax: gpasswd -d username groupname

File and Directory creation and operation

- Linux file system is a structured collection of files on a disk drive or a partition.
- **Types of File System:**

When we install the Linux operating system, it offers many file systems such as **Ext, Ext2, Ext3, Ext4, JFS, ReiserFS, XFS, btrfs,** and **swap**.

- **pwd** (present working directory)
- To change directory, **cd**
- To open/edit any file, **vi** or **nano** or **cat**(only view/display) or **tail** (for logging mainly)

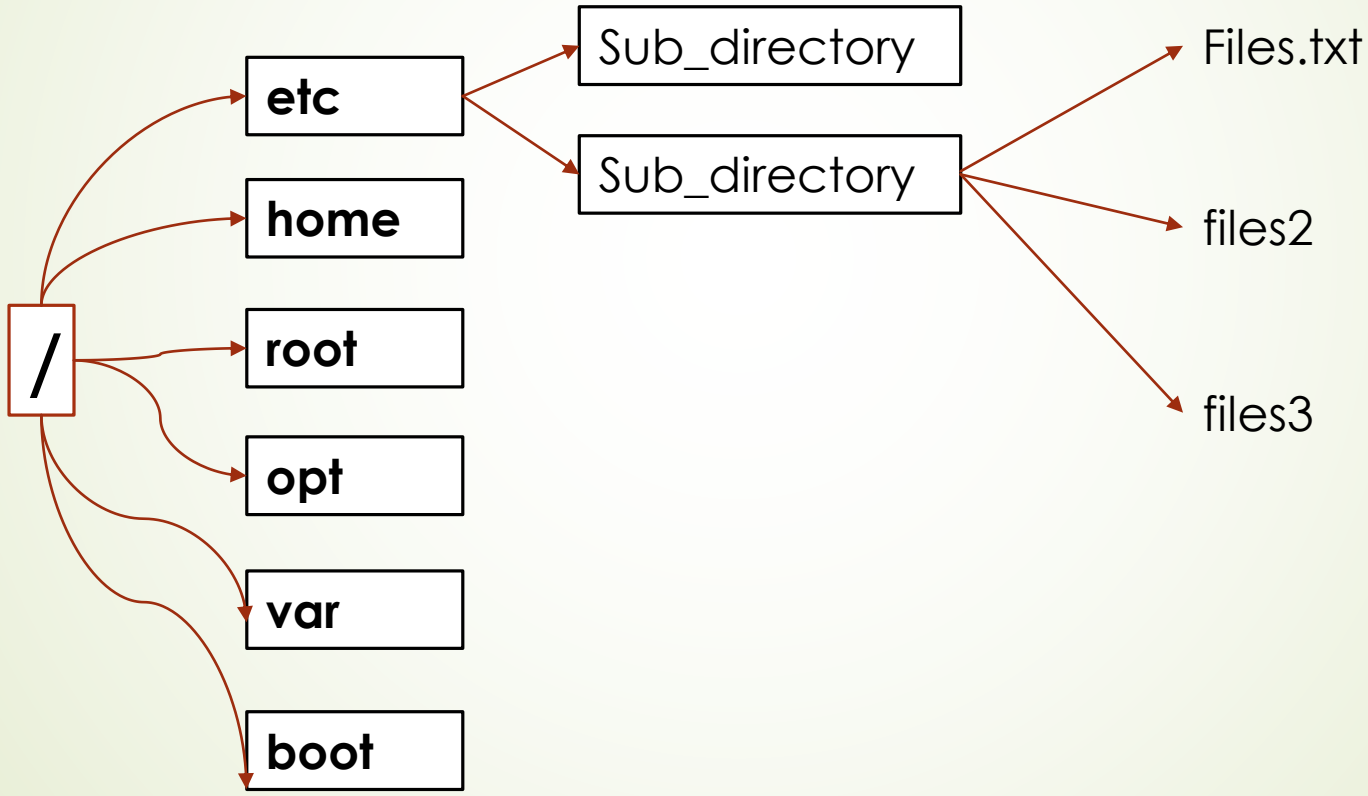
File and Directory Commands

Command	Description	Syntax
file	Determines file types	file file_name
touch	To create a file	touch file_name
cat	Shows contents of file	cat file_name
	Combines multiple files	cat file1 file2 > file
rm	To remove a file	rm file_name
cp	To copy a file	cp copied_file/directoy target_file/directory
mv	Moving/renaming files/directories	mv moved_file/directoy target_file/directory
ls	Listing files	ls
ls -al	Listing files with all info	ls -al
mkdir	to create a new directory under any directory	mkdir directory_name
rmdir	To remove directories	rmdir directory_name
rm -rf	To remove non-empty directories and all the files within them recursively	rm –rf directory_name

Directory Types

Directory Types	Types of stored Files
Root Directory	Root of the filesystem where everything begins
Binary Directories	Contains binary or compiled source code files, eg, /bin, /sbin etc.
Configuration Directories	Contain configuration files of the system, eg, /etc, /boot
Data Directories	Stores data files, eg, /home, /root etc.
Memory Directories	Stores device files which doesn't take up actual hard disk space, eg, /dev, /proc, /sys.
Usr (Unix System Resources)	Contains sharable, read only data, eg, /usr/bin, /usr/lib etc.
Var (Variable Directories)	Contains larger size data, eg, /var/log, /var/cache etc.
Non-Standard Directories	Directories which do not come under standard FHS, eg, lost+found, /run etc

Navigating through the Directory Tree



File & Directory Ownership & Permissions

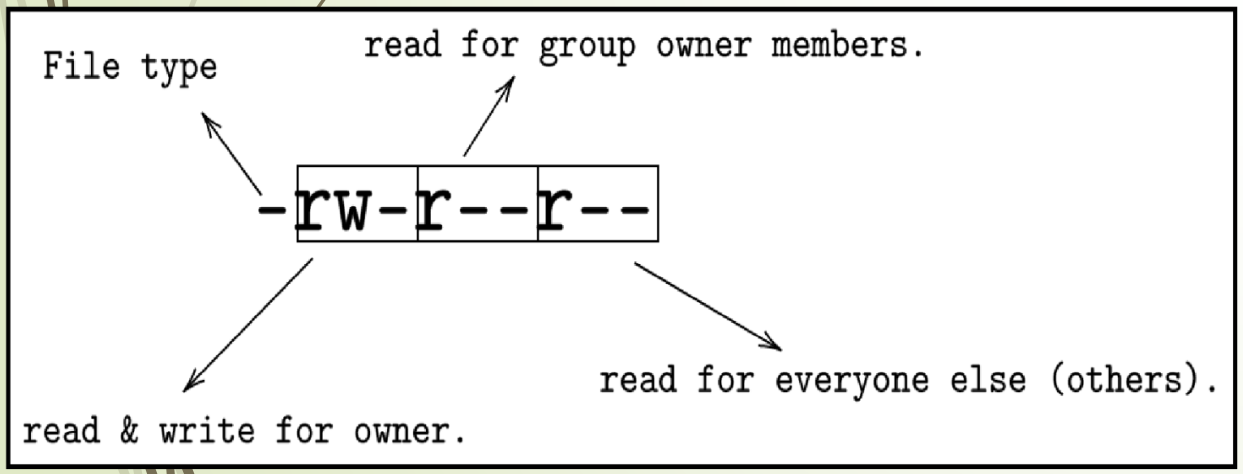
- Every file in Linux is owned by a specific user and a specific group
- By default, the owner is who created the file
- By default, the primary group of the user owner owns the file

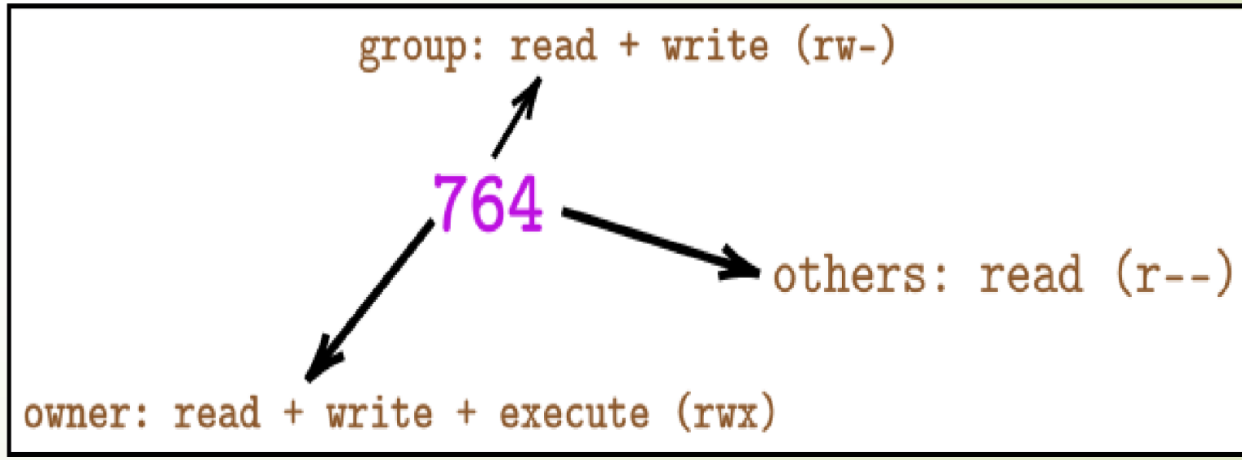
- Every file/directory is assigned access permission for 3 entities:
  - User owner of the file
  - Group owner of the file
  - Everyone else (also referred to as others/world)
- Each file/directory has 3 types of access permissions:
  - Read
  - Write
  - Execute

Syntax for ownership change of a file: chown user:group /directory/file
Syntax for ownership change of a directory: chown –R user:group /directory/sub-dir

File Permission

Permission	File	Directory
Read	Able to view the file content	Able to list the directory content
Write	Able to edit the file content	Able to create and remove file in the directory
Execute	Able to run the file (if executabile)	Able to change to the directory





Permission Combination

Number	Meaning	Literal Equivalence
0	Zero/No Permissions	`---`
1	Execute	`--x`
2	Write	`-w-`
3	Write + Execute	`-wx`
4	Read	`r--`
5	Read + Execute	`r-x`
6	Read + Write	`rw-`
7	Read + Write + Execute	`rwx`

Syntax for permission change: chmod 764 /directory/file
To recursively operate on all files and directories under a given directory,
chmod -R 755 directory_name

Text Editor

- **nano** (easy to use, and instructions are given within file opened by nano)
- **vi** > works on 2 modes: command mode and insert mode
- Insert mode is used to edit contents of a file. To go this mode, press small **i** and to exit the mode, press **esc** button
- Command mode is used for other operations
- When entering a file, vi is in command mode.

Command mode	Description
:w	Save the file without quit
:wq	Save the file and quit vi
/	search for any keyword
:q	Quit without saving
:q!	Quit forcefully without saving

Searching

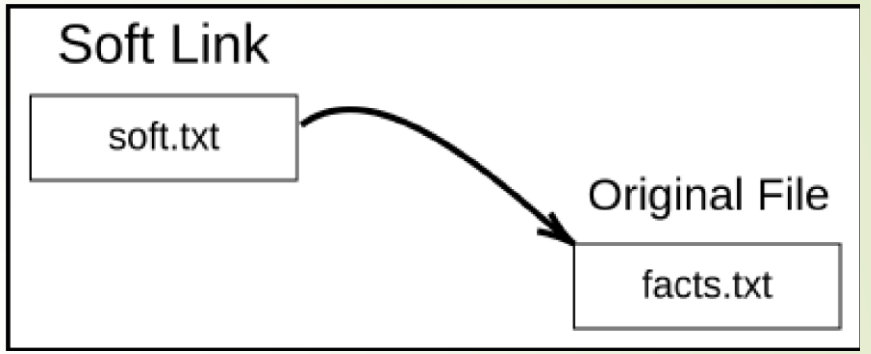
- **locate** command (need to install mlocate package)

Syntax: locate something

- **find**
- To filter any keyword from a file,

Syntax: cat file_name | grep “anythings”

Soft Link



- Simply a file that points to another file

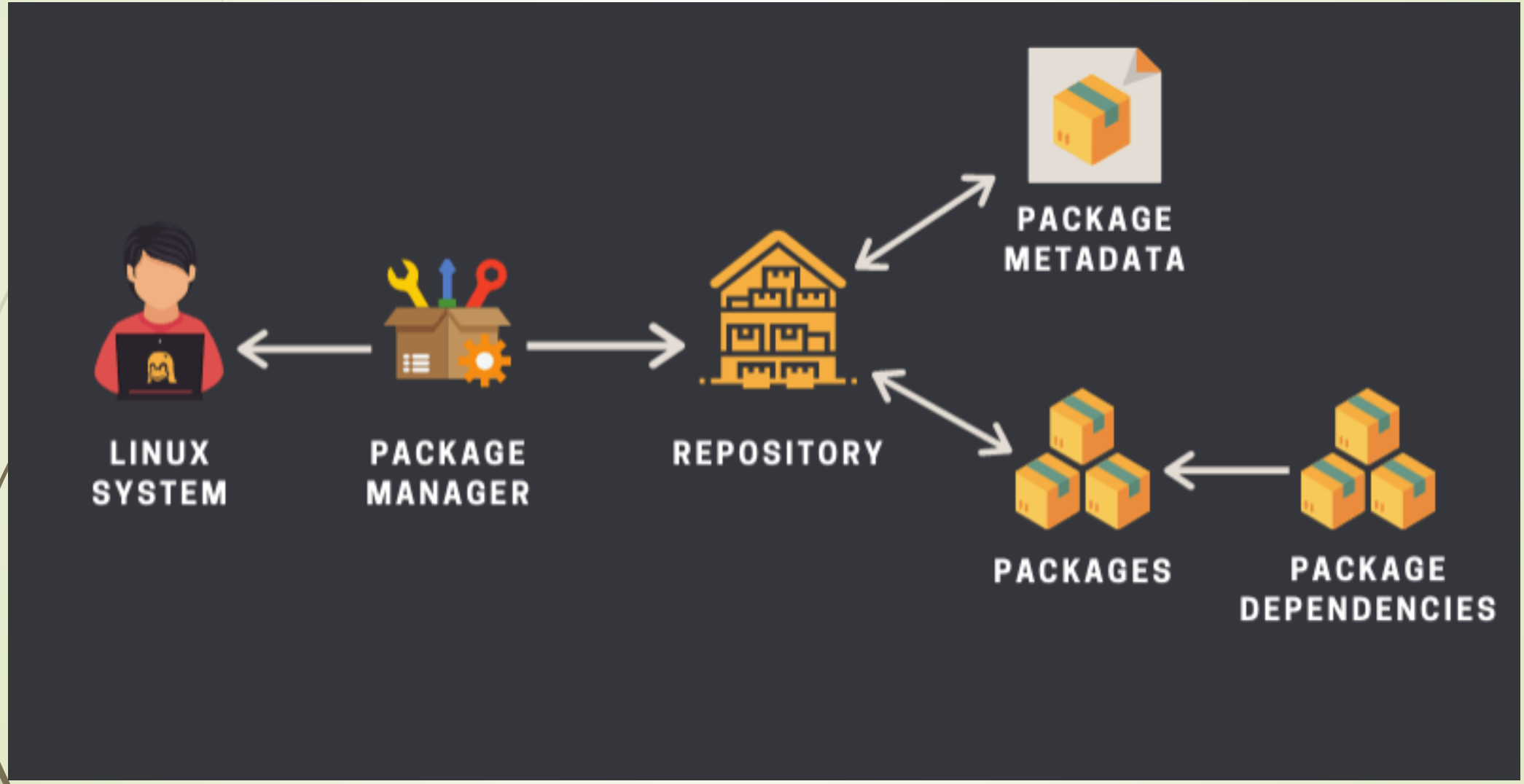
Syntax: ln –s original_file soft_link

- To see the soft link,

Syntax: ls –l soft_link

- If you delete soft link, nothing will happen
- If you delete the original file, the soft link will become useless
- Any change to the soft link is actually a change in the original file
- You can create soft links to the directories

Linux Package Management



Package Management

Execution	Command
Updating the repository	apt update
Upgrading the installed packages	apt upgrade
Installation of a package	apt install package_name
Searching for a package	apt search package_name
Removing a package	apt remove package_name

Useful Commands

- **date**
- **time**
- **dpkg-reconfigure tzdata**

- **clear** command: used to clear the terminal screen.

- **df** command: used to display the disk space used in the whole file system.
- **du** command: to check how much space a file or a directory takes

- **top command:** display a list of running processes and how much CPU each process uses. Similar to task manager in windows

Useful Commands

- **Ip link show**: shows information for all network interfaces
- **Ifconfig:** shows network interface configuration

- **uname –a:** will print detailed information about your Linux system like the machine name, operating system, kernel, and so on.

- **man:** stands for manual which is a reference book of a Linux OS.
- **history**
- **exit** command: to exit from the current shell

Accessing a server

- **SSH (Secure Shell)**

The Secure Shell Protocol is a cryptographic network protocol for operating network services securely over an unsecured network.

Default SSH port is **22.** In production, this default port must has to be changed.

Syntax: **ssh user@IP_address –p port_number**

- **hostname**
- **hostname -d**

- **ping** command is used to check the connectivity between two nodes
- Example: ping google.com

- **wget** command: download files from the internet

Continuing topics for upcoming sessions….

- **Storage System (Logical Volume Manager (LVM)> PV, VG, LV)**
- **Linux Firewall**
- **Logging**
- **Scheduling a Job (cronjob)**
- **Installation of different Services (mail server, DNS, web server etc.)**