Linux 101: Comprehensive Beginner's Guide ~ OBEDPoP
please refer for tutorial: https://academy.tcm-sec.com/p/linux-101

Table of Contents

Introduction to Linux

What is Linux?
- Open-source Unix-like operating system kernel
- Created by Linus Torvalds in 1991
- Typically packaged as a Linux distribution (Ubuntu, Fedora, Debian, etc.)

Linux vs Windows
- Free and open-source vs proprietary
- Command-line focused vs GUI focused
- Better stability and security
- More customizable

Linux Distributions
- **Debian-based**: Ubuntu, Mint, Kali Linux
- **Red Hat-based**: Fedora, CentOS, RHEL
- **Arch-based**: Manjaro, EndeavourOS
- **Others**: Slackware, openSUSE

Getting Started
- Terminal/Shell: Interface to interact with Linux
- Bash (Bourne Again Shell): Default shell in most distributions

---

Linux Filesystem Hierarchy

Directory	Purpose
`/`	Root directory
`/bin`	Essential user binaries
`/etc`	System configuration files
`/home`	User home directories
`/var`	Variable data (logs, databases)
`/tmp`	Temporary files
`/usr`	User programs and utilities
`/lib`	System libraries

`/boot`	Boot loader files
`/dev`	Device files
`/proc`	Process information
`/opt`	Optional/third-party software
`/root`	Root user's home directory
`/sbin`	System administration binaries

Basic Commands

Navigation
- `pwd` - Print working directory
- `cd` - Change directory
- `ls` - List directory contents
  - `ls -l` - Long listing format
  - `ls -a` - Show hidden files
- `tree` - Display directory structure as tree

File Operations
- `touch` - Create empty file
- `cat` - Display file content
- `less`/`more` - View file page by page
- `cp` - Copy files/directories
- `mv` - Move/rename files
- `rm` - Remove files
  - `rm -r` - Remove directories recursively
- `mkdir` - Create directory
- `rmdir` - Remove empty directory
- `find` - Search for files
  - `find / -name "filename"`

System Information
- `uname -a` - System information
- `df -h` - Disk space usage
- `free -h` - Memory usage
- `uptime` - System uptime and load average
- `top`/`htop` - Process viewer

File Permissions

Understanding Permissions
- Three permission types:
  - `r` (read)
  - `w` (write)
  - `x` (execute)
- Three permission groups:
  - `user` (owner)
  - `group`
  - `others`

Viewing Permissions
```bash
ls -l
# Output: -rwxr-xr-- 1 user group 2048 Jan 1 10:00 file.txt
```
- First character: file type (- for regular file, d for directory)

- Next 9 characters: permissions (rwxr-xr--)

Changing Permissions
- `chmod` - Change file permissions
  - Symbolic: `chmod u+x file` (add execute for user)
  - Numeric: `chmod 755 file` (rwxr-xr-x)
- `chown` - Change file owner
  - `chown user:group file`
- `chgrp` - Change file group
  - `chgrp group file`

Special Permissions
- SUID (Set User ID): `chmod u+s file`
- SGID (Set Group ID): `chmod g+s file`
- Sticky Bit: `chmod +t directory`

User Management

User Accounts
- `/etc/passwd` - User account information
- `/etc/shadow` - Encrypted passwords
- `/etc/group` - Group information

Commands
- `useradd` - Add new user
- `usermod` - Modify user
- `userdel` - Delete user
- `passwd` - Change password
- `groupadd` - Add new group
- `groups` - Show user's groups
- `id` - Show user and group information

Sudo
- `sudo` - Execute command as superuser
- `/etc/sudoers` - Sudo configuration file
- `visudo` - Edit sudoers file safely

Process Management

Viewing Processes
- `ps` - Display current processes
  - `ps aux` - Show all processes
- `top` - Interactive process viewer
- `htop` - Enhanced process viewer (needs installation)

Managing Processes
- `kill` - Terminate process by PID
  - `kill -9 PID` - Force kill
- `killall` - Kill processes by name
- `pkill` - Kill processes by pattern
- `nice` - Run process with modified priority
- `renice` - Change priority of running process

Background/Foreground
- `&` - Run command in background

- `jobs` - List background jobs
- `fg` - Bring job to foreground
- `bg` - Continue stopped job in background
- `Ctrl+Z` - Suspend current job
- `Ctrl+C` - Terminate current job

Package Management

Debian/Ubuntu (APT)
- `apt update` - Update package list
- `apt upgrade` - Upgrade installed packages
- `apt install package` - Install package
- `apt remove package` - Remove package
- `apt search term` - Search for package
- `apt list --installed` - List installed packages

Red Hat/CentOS (YUM/DNF)
- `yum update` or `dnf update`
- `yum install package` or `dnf install package`
- `yum remove package` or `dnf remove package`
- `yum search term` or `dnf search term`

Arch Linux (Pacman)
- `pacman -Syu` - Update system
- `pacman -S package` - Install package
- `pacman -R package` - Remove package
- `pacman -Ss term` - Search for package

Snap/Flatpak (Universal)
- `snap install package`
- `flatpak install package`

Text Processing

Viewing Files
- `cat` - Display entire file
- `less`/`more` - View file page by page
- `head` - Show first lines
- `tail` - Show last lines
  - `tail -f` - Follow file changes

Searching
- `grep` - Search text patterns
  - `grep "pattern" file`
  - `grep -r "pattern" /dir` - Recursive search
- `find` - Search for files

Editing
- `nano` - Simple text editor
- `vim`/`vi` - Powerful text editor
- `sed` - Stream editor
- `awk` - Text processing language

File Comparison
- `diff` - Compare files line by line

- `cmp` - Compare files byte by byte
- `comm` - Compare sorted files

Networking

Basic Commands
- `ping` - Test network connectivity
- `ifconfig`/`ip` - Network interface configuration
- `netstat` - Network statistics
- `ss` - Socket statistics
- `traceroute`/`tracepath` - Trace network path
- `dig`/`nslookup` - DNS lookup
- `hostname` - Show system hostname
- `wget`/`curl` - Download files

SSH
- `ssh user@host` - Connect to remote host
- `scp` - Secure copy
  - `scp file user@host:/path`
- `ssh-keygen` - Generate SSH keys
- `ssh-copy-id` - Copy SSH key to remote host

Firewall
- `ufw` (Uncomplicated Firewall)
  - `ufw enable`
  - `ufw allow port`
- `iptables` - Advanced firewall configuration

Shell Scripting Basics

Script Structure
```bash
#!/bin/bash
# This is a comment
echo "Hello, World!"
```

Variables
```bash
name="Linux"
echo "Hello, $name"
```

Input
```bash
read -p "Enter your name: " username
echo "Hello, $username"
```

Conditionals
```bash
if [ $age -gt 18 ]; then
  echo "Adult"
else
  echo "Minor"
```

```
fi
```

Loops
```bash
# For loop
for i in {1..5}; do
  echo "Number: $i"
done

# While loop
count=1
while [ $count -le 5 ]; do
  echo "Count: $count"
  ((count++))
done
```

Functions
```bash
greet() {
  echo "Hello, $1"
}
greet "Alice"
```

System Monitoring

Performance
- `top`/`htop` - Process monitoring
- `vmstat` - Virtual memory statistics
- `iostat` - CPU and I/O statistics
- `sar` - System activity reporter
- `dmesg` - Kernel messages

Disk Usage
- `df -h` - Filesystem disk usage
- `du -h` - Directory space usage
- `ncdu` - Interactive disk usage viewer

Logs
- `/var/log/` - System log directory
- `journalctl` - Systemd journal logs
- `tail -f /var/log/syslog` - Follow system log

Services and Daemons

Systemd (Modern Systems)
- `systemctl start service`
- `systemctl stop service`
- `systemctl restart service`
- `systemctl status service`
- `systemctl enable service`
- `systemctl disable service`
- `systemctl list-units --type=service`

SysV Init (Older Systems)
- `service service start`
- `service service stop`
- `service service status`

Cron Jobs

Scheduling Tasks
- `crontab -e` - Edit user's cron jobs
- `crontab -l` - List cron jobs
- `crontab -r` - Remove all cron jobs

Cron Syntax
```
* * * * * command
- - - - -
| | | | |
| | | | +----- Day of week (0 - 6) (Sunday=0)
| | | +------- Month (1 - 12)
| | +--------- Day of month (1 - 31)
| +----------- Hour (0 - 23)
+------------- Minute (0 - 59)
```

Examples
```
0 * * * * /path/to/script.sh  # Every hour
30 3 * * * /backup.sh         # 3:30 AM daily
0 0 * * 0 /weekly-report.sh   # Midnight every Sunday
```

SSH and Remote Access

Basic SSH
```bash
ssh username@remote_host
ssh -p port_number username@remote_host
```

Key Authentication
1. Generate key pair: `ssh-keygen -t rsa`
2. Copy public key: `ssh-copy-id username@remote_host`
3. Disable password login (in `/etc/ssh/sshd_config`):
   ```
   PasswordAuthentication no
   ```

SCP (Secure Copy)
```bash
scp file.txt user@remote:/path/to/destination
scp user@remote:/path/to/file.txt /local/destination
```

SSH Config

Edit `~/.ssh/config` for easy connections:
```
Host myserver
    HostName server.example.com
    User username
    Port 2222
    IdentityFile ~/.ssh/id_rsa
```

Basic Troubleshooting

Common Issues
1. **Permission denied**: Check file permissions and ownership
2. **Command not found**: Check PATH or install package
3. **No space left on device**: Check with `df -h`
4. **Process not responding**: Kill with `kill` or `kill -9`

Diagnostic Commands
- `dmesg` - Kernel messages
- `journalctl` - System logs
- `strace` - Trace system calls
- `lsof` - List open files

Recovery
- **Single user mode**: Boot with `init=/bin/bash`
- **Live CD**: Use for system recovery
- **fsck**: Filesystem check and repair

Conclusion

This guide covers fundamental Linux concepts and commands. To become proficient:
1. Practice regularly in a Linux environment
2. Read man pages (`man command`)
3. Explore advanced topics as you become comfortable
4. Join Linux communities for support

Remember: **Google is your friend** when you encounter problems! Most issues have been solved before and documented online.