Session 14-18 Linux Mastery Notes

1. Shell Basics

Definition: A shell is a command-line interface to interact with the OS.
Command Structure: command [options] [arguments]

Example: cp -i file1.txt file2.txt
Files & Directories:
File: file.txt
Directory path: dir/file.txt

2. File Viewing & Editing

nano filename → simple editor. Exit with Ctrl+X, save with Y.
less filename → view file, quit with q, search with /.
cat filename → print whole file.
head filename → first 10 lines.
tail filename → last 10 lines.
tail -f file.log → monitor in real-time.

3. File Management

ls → list files.
ls -l detailed view.
ls -a hidden files.
Combine: ls -la.
cp src dest → copy.
mv src dest → move/rename.
rm file → delete file.
rm -r dir → recursive delete.
rm -i file → confirm before delete.
mkdir dir → make directory.
stat file → show file properties.
find dir → recursive file listing.
find dir | grep name → search by name.

4. Navigation

pwd → print working directory.
cd dir → change directory.
cd .. → go up one level.
cd ~ → go to home.
cd - → return to previous dir.

5. Manual & Help

man command → manual.
command --help or command -h → short help.

6. Variables

Access: $VAR or ${VAR}.
Set: VAR=value.
Export: export VAR=value.

7. Redirection & Pipes

> → overwrite output file.
>> → append output.
< → take input from file.
<< → here document, multi-line input.
| → pipe output of one command into another.
Error redirection: 2>.
Output + error redirection: &>.

8. Inspecting Commands

type command → shows what command runs.
which command → path of command.

9. Administrative Access

sudo command → run as superuser.
Use with caution.

10. Package Management

Debian/Ubuntu/Kali:

- sudo apt update → refresh packages.
- sudo apt upgrade → upgrade.
- sudo apt install pkg → install.
- sudo apt remove pkg → remove.

RedHat/CentOS/Fedora:

- yum or dnf for package mgmt.
- rpm -i file.rpm → install package.

11. Networking Basics

ip a or ifconfig → view interfaces/IPs.
ping host → test connectivity.
traceroute host → trace network path.
hostname → display system name.
netstat -tulnp or ss -tulnp → view open ports.
scp user@host:file . → secure copy.

12. Process Management

ps aux → list processes.
top → live monitor (CPU/mem usage).
htop → advanced monitor.
kill PID → terminate.
kill -9 PID → force terminate.
pidof name / pgrep name → find PID.

13. Password Management

passwd → change own password.
sudo passwd user → change other user’s password.

14. Editors

vim/vi:vi filename.
Modes: i insert, Esc command.
:w save, :q quit, :wq save + quit.

15. Permissions & Ownership

View: ls -l → -rwxr-xr--
- file, d directory.
Owner perms, group perms, others.

Change perms:
chmod 755 file.
chmod u+x file.sh.
Change ownership:
sudo chown user:group file.

16. Logs & Forensics

Common Logs:

- System: /var/log/syslog
- Authentication: /var/log/auth.log
- Events: /var/log/daemon.log
- Boot: /var/log/boot.log

17.Practical Exercises

journalctl -n 100 → last 100 logs.

journalctl --since "1 hour ago" → last hour.

journalctl -u ssh → SSH service logs.

journalctl | grep "error" → search errors.

Save logs: journalctl -b > logs_boot.txt.

awk for log parsing:

- awk '{print $1, $2, $3}' file → date/time.
- awk '/root/ {print $0}' file → filter by keyword.
- awk '/login/ {count++} END {print count}' auth.log → count logins.
- awk '/session opened/ {user[$11]++} END {for(u in user) print u,user[u]}' auth.log

→ summarize sessions.

tail for monitoring:

- tail file → last lines.
- tail -f file → follow logs live.
- tail -f file | grep --color=auto "error" → highlight errors.

logwatch:

```
sudo apt install logwatch
sudo logwatch --detail low --range today
```

auditd:

```
sudo service auditd start
sudo auditctl -w /bin/chmod -p x -k chmod_changes
chmod 755 file
sudo ausearch -k chmod_changes
```