

The Ethical Hacker's Command Handbook

Chapter 1 – Linux Fundamentals for Ethical Hackers

"The terminal is the first tool every ethical hacker learns to master."

Learning Objectives

Navigate the Linux filesystem, manage files and directories, search for files and text, understand file permissions, and build confidence using the Linux terminal in authorized security labs.

Why Linux?

Most penetration-testing distributions such as Kali Linux are Linux-based. Understanding the terminal is essential because security tools are commonly executed from the command line.

Understanding the Prompt

Example prompt: `kali@kali:~$`

kali = username, **@** = separator, second **kali** = hostname, **~** = home directory, **\$** = standard user.

pwd

Purpose: Display the current working directory.

Syntax: `pwd`

Description: Shows the absolute path of your current location.

Tip: Check your location before creating or deleting files.

ls

Purpose: List files and directories.

Syntax: `ls`

Description: Displays directory contents.

Tip: Useful options: `ls -l`, `ls -a`, `ls -lh`, `ls -lah`.

cd

Purpose: Change directories.

Syntax: `cd Desktop`

Description: Move between folders.

Tip: Special forms: `cd ..`, `cd ~`, `cd -`, `cd /`.

mkdir

Purpose: Create directories.

Syntax: `mkdir CyberLab`

Description: Creates a new folder.

Tip: Use -p to create nested folders.

touch

Purpose: Create empty files.

Syntax: touch notes.txt

Description: Creates a file if it doesn't exist.

Tip: Can create multiple files at once.

cp

Purpose: Copy files.

Syntax: cp report.txt backup.txt

Description: Copies files.

Tip: Use -r for directories.

mv

Purpose: Move or rename files.

Syntax: mv old.txt new.txt

Description: Moves or renames.

Tip: Useful for organizing notes.

rm

Purpose: Delete files.

Syntax: rm file.txt

Description: Deletes files.

Tip: Use -r for folders. Be careful with rm -rf.

cat

Purpose: Display file contents.

Syntax: cat notes.txt

Description: Prints file contents.

Tip: Can concatenate multiple files.

less

Purpose: Read large files.

Syntax: less access.log

Description: Scrollable viewer.

Tip: Press q to quit, / to search.

find

Purpose: Locate files.

Syntax: `find . -name "*.txt"`

Description: Searches by name.

Tip: Supports many filters.

grep

Purpose: Search text.

Syntax: `grep password notes.txt`

Description: Searches inside files.

Tip: Use `-i` for case-insensitive, `-r` for recursive.

chmod

Purpose: Change permissions.

Syntax: `chmod +x script.sh`

Description: Modifies file permissions.

Tip: 755 is a common executable permission set.

Quick Command Cheat Sheet

Command	Purpose
<code>pwd</code>	Current directory
<code>ls -lah</code>	Detailed listing
<code>cd</code>	Change directory
<code>mkdir</code>	Create folder
<code>touch</code>	Create file
<code>cp</code>	Copy
<code>mv</code>	Move/Rename
<code>rm</code>	Delete
<code>cat</code>	Display file
<code>less</code>	View large file
<code>find</code>	Locate files
<code>grep</code>	Search text
<code>chmod</code>	Change permissions

Practice Lab

1. Create a directory named CyberLab.
2. Create notes.txt inside it.
3. Copy it to backup.txt.

4. Rename backup.txt to lab_notes.txt.
5. Search for all .txt files with find.
6. Search for the word 'password' using grep.
7. Make a script executable with chmod +x.
8. Verify your location with pwd.
9. List all files using ls -lah.

Chapter Summary

This chapter introduced the Linux commands used most frequently in ethical hacking labs. Mastering these commands provides the foundation for tools such as Nmap, Metasploit, and Wireshark.