Day 135

Topic: Linux Commands Practical

Objective: To become proficient in the Linux Command Line Interface (CLI), essential for using hacking tools.

Theoretical Concepts:
Unlike Windows, most security tools run natively on Linux CLI. We covered the Linux file system hierarchy (/bin, /etc, /home, /var). We discussed file permissions (Read, Write, Execute) and user privilege management (sudo/root).

Practical Work:
We spent the day executing essential commands: File Management: *ls, cd, pwd, mkdir, rm, cp, mv*. File Viewing: *cat, less, head, tail, grep* (for searching text). Permissions: *chmod* (changing permissions, e.g., chmod +x script.sh) and *chown*. Process Management: *ps, top, kill*. We practiced piping commands (e.g., *cat file | grep "password"*) to manipulate data streams.

Tools Used: Kali Linux Terminal.

Outcome: Comfortably navigating the Linux file system and managing files via terminal.