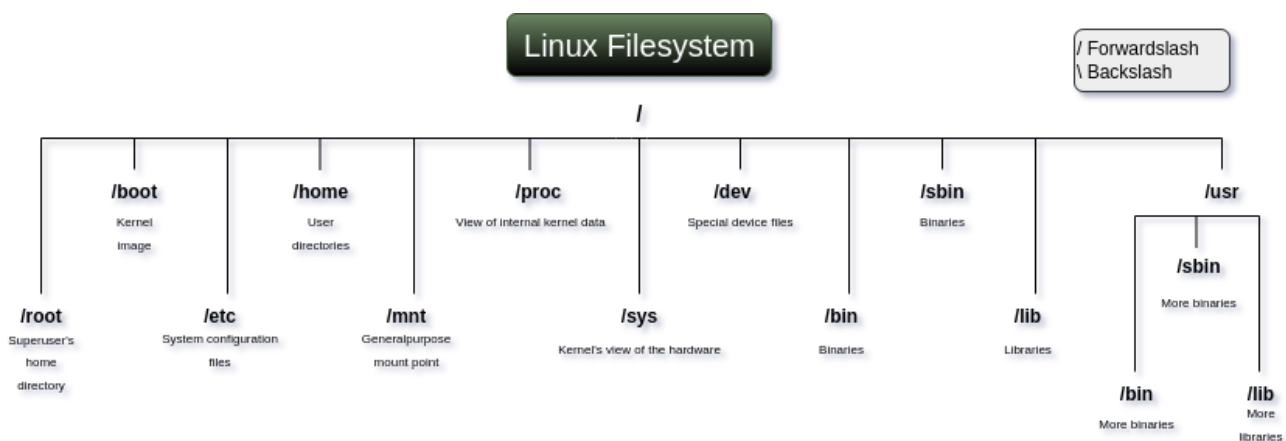




**The Linux Filesystems
and
63 Common Terminal Commands**



/boot: Contains boot-related files like the kernel. Modifying this can make the system unbootable.

/home: Stores user directories and personal data.

/proc: Provides information about the kernel and running processes. Useful for malware analysis and security monitoring.

/etc: Contains system configuration files. Hackers target this to alter system behavior.

/mnt: Used for mounting external drives and partitions.

/sys: Represents the kernel's view of hardware.

/dev: Contains special files for system devices. Can be used for direct disk access.

/bin & /sbin: Stores essential system binaries like ls, bash, and iptables.

/lib & /usr/lib: Holds shared libraries needed by executables.

/usr/bin & /usr/sbin: Additional binaries for regular users and system administration.

Most Important Directories in Hacking and Cybersecurity:

/etc/passwd & /etc/shadow: Contain user account info and hashed passwords.

/var/log: Stores system logs, crucial for forensic analysis.

/proc: Can be used to inspect hidden processes or rootkits.

/home: Contains user data, which is often a target.

63 Common Terminal Commands

- 1) pwd – Find yourself
- 2) whoami – Checking your login
- 3) cd – Navigate through directories
- 4) ls – List directories
- 5)