Day 9 -LINUX LOGS

What Are Logs?

Logs are text files that record system events, processes, errors, and activities. They're essential for:

- Troubleshooting issues
- Monitoring security
- Performing audits and forensic analysis

Where Are Logs Stored?

All logs are typically stored in the directory:
/var/log/

📄 Common Linux Log Files:

Log File	Description
`auth.log`	Authentication logs (login attempts, sudo usage)
`syslog`	General system events and messages
`dmesg`	Kernel ring buffer logs (hardware info, drivers at boot)
`boot.log`	Logs related to system boot processes
`secure`	Similar to `auth.log`, often used on RedHat-based systems
`messages`	General log file including errors, info, debug messages (on some distros)
`apt/history.log`	Package installation history (on Debian-based systems)
`faillog`	Failed login attempts
`lastlog`	Last login times of all users

🛠️ Useful Commands:

Command	Description
`cat /var/log/syslog`	Displays the entire syslog file

`tail /var/log/auth.log`	Shows the last 10 lines of auth.log
`tail -f /var/log/syslog`	Live-updates the syslog file in real-time
`grep "Failed password" /var/log/auth.log`	Searches for failed password attempts
`grep -c "Failed password" /var/log/auth.log`	Counts number of failed password attempts

Why Logs Matter in Cybersecurity:

- Detect unauthorized access attempts
- Monitor sudo and root actions
- Identify brute-force or password guessing attacks
- Track when and where users log in from