**Objective**

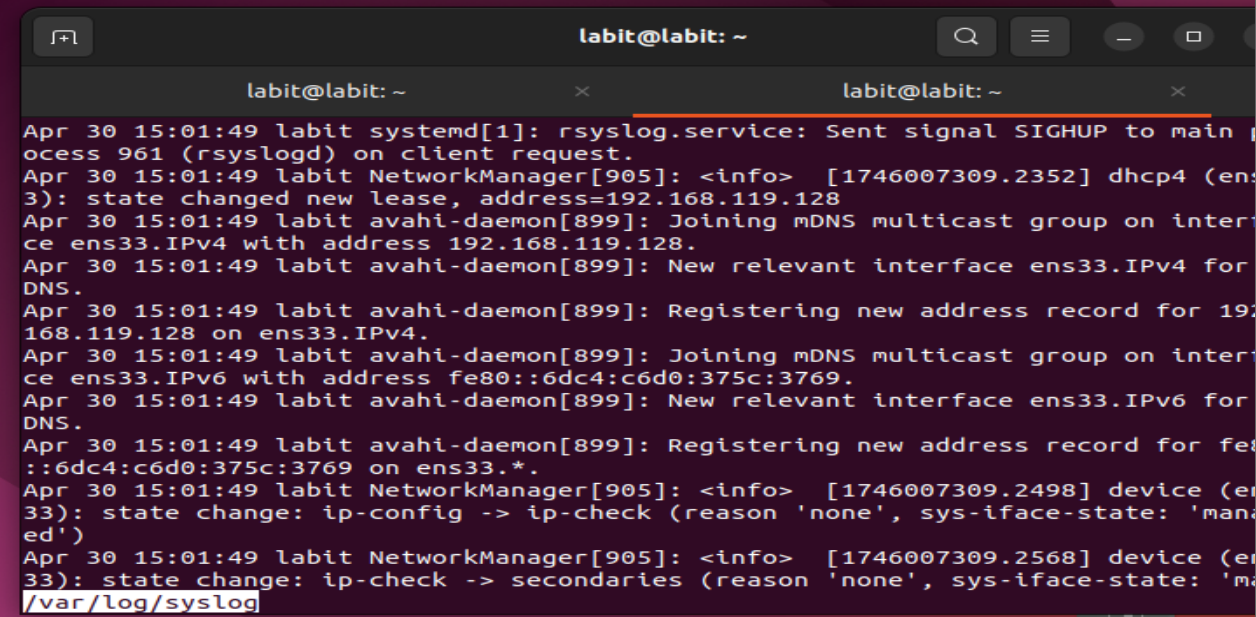
To understand system log files in Linux and practice identifying, analyzing, and debugging system and application issues using logs.

**Software/Tools Required:**

* Linux OS (Ubuntu/CentOS)
* Terminal
* Log file viewer tools (cat, less, grep, tail, journalctl)

**Key Log Files to Study:**

1. /var/log/syslog or /var/log/messages
2. /var/log/auth.log
3. /var/log/dmesg
4. /var/log/apache2/access.log (if web server is installed)
5. /var/log/fail2ban.log (if applicable)

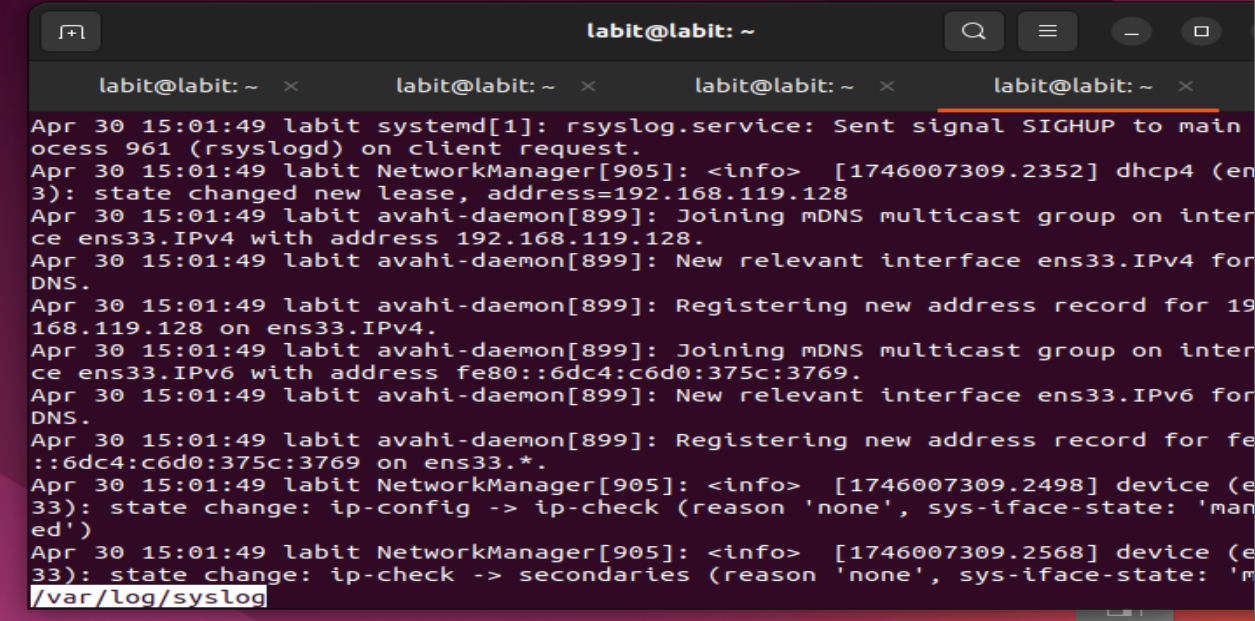


**Experiment Steps:**

**1. Viewing General System Logs**

* Use cat, less, or tail to read logs:
* sudo less /var/log/syslog

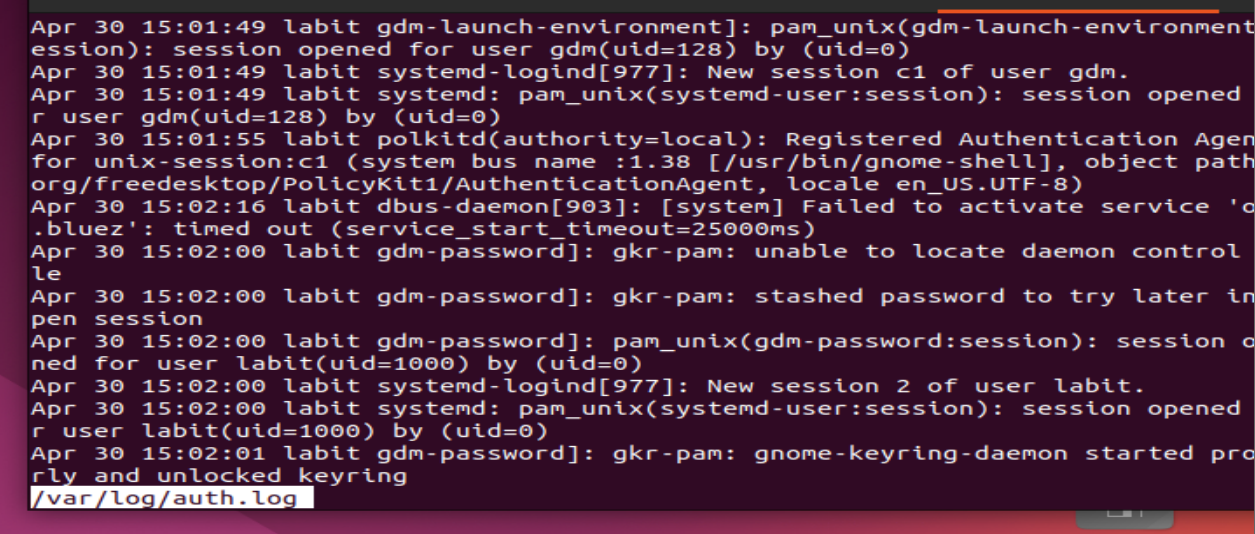
sudo tail -f /var/log/syslog



**2. Analyzing Authentication Logs**

* Examine login attempts:
* sudo less /var/log/auth.log

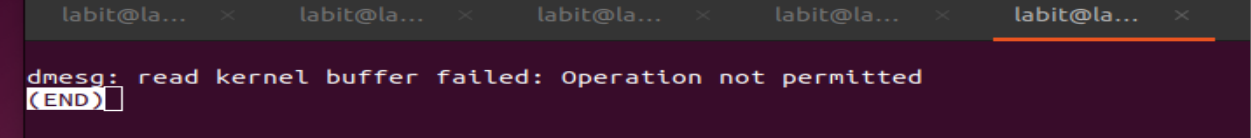
grep 'Failed' /var/log/auth.log



**3. Examining Boot and Kernel Logs**

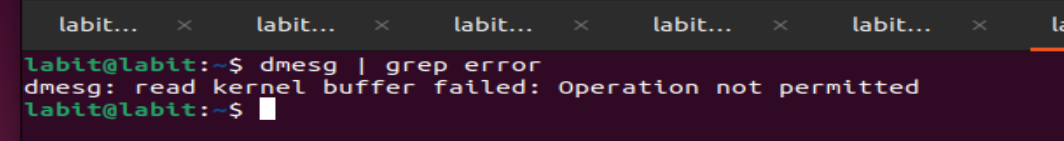
* View messages generated during boot:

dmesg | less



* Search for hardware issues:

dmesg | grep error



**4. Using journalctl (Systemd-based Systems)**

* View complete journal:

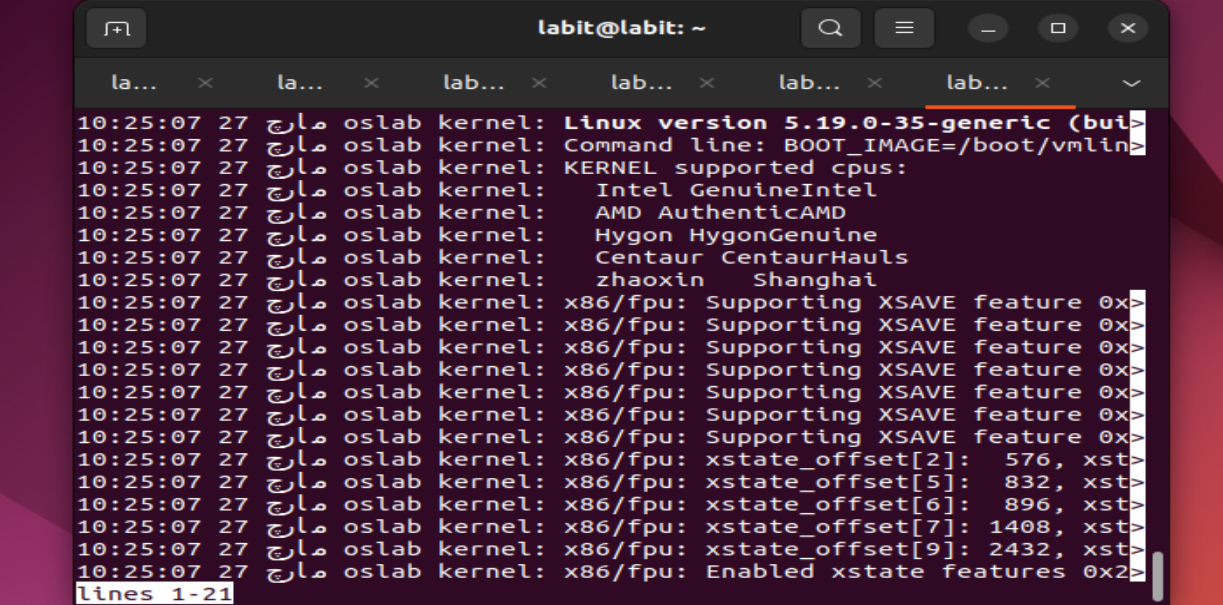
journalctl

* Show only current boot logs:

journalctl -b

* Search for specific service:

journalctl -u ssh



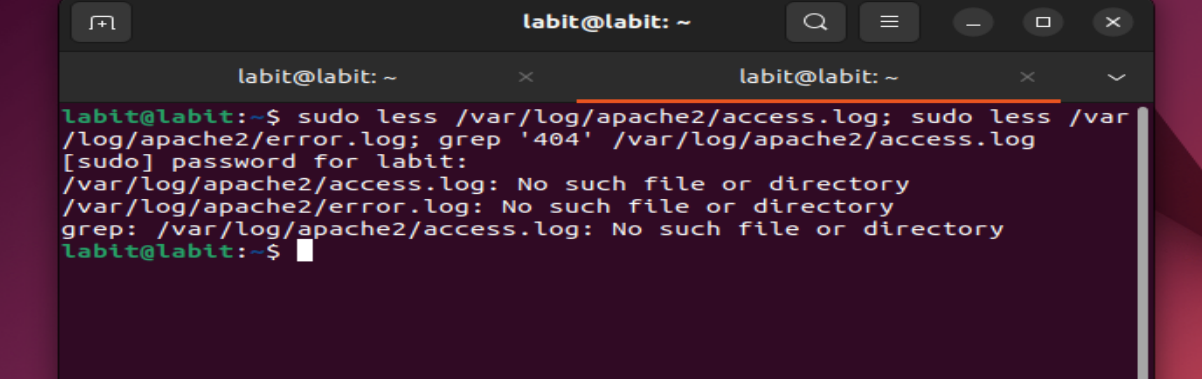
**5. Analyzing Web Server Logs**

* If Apache is installed:
* sudo less /var/log/apache2/access.log

sudo less /var/log/apache2/error.log

* Look for 404 errors:

grep '404' /var/log/apache2/access.log



**Final Observations**

* **Most log files were clean with expected behavior.**
* **Authentication logs showed potential attack signs.**
* **Web logs identified misconfigured links and unauthorized access attempts.**

**Result**

**Successfully explored system logs using various command-line tools, identified patterns and issues, and interpreted log data for system debugging and auditing.**

**Viva Questions with Sample Answers**

1. **What is the difference between syslog and journalctl?**  
   ➤ syslog is a traditional logging system; journalctl is used in systemd-based systems and provides structured, queryable logs.
2. **How can you continuously monitor a log file?**  
   ➤ Use tail -f <logfile> to follow a log in real time.
3. **What kind of issues can you identify in the auth.log file?**  
   ➤ Failed login attempts, sudo access, SSH authentication, and potential brute-force attacks.
4. **Why is log analysis important for system administrators?**  
   ➤ Helps detect security breaches, monitor service health, troubleshoot issues, and maintain audit trails.