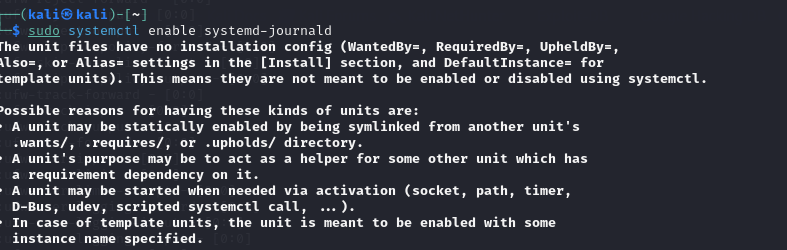
Task 6

Setup



To enable system logging for enhanced security monitoring, first activate the journal service with the commands:

sudo systemctl enable systemd-journald

sudo systemctl start systemd-journald

For Ubuntu and Debian systems, authentication attempts are logged in

/var/log/auth.log by default.

If this file is missing, enable it by uncommenting the following line in

/etc/rsyslog.conf : auth,authpriv.\* /var/log/auth.log

After making the changes, restart the rsyslog service using: sudo systemctl restart rsyslog To simulate multiple failed SSH login attempts for testing purposes, use the command

: ssh invalid\_user@localhost



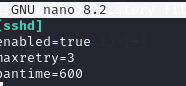
This command analyzes Logs for Brute-force Attempts

Mitigation:









To enhance system security, install fail2ban using sudo apt install fail2ban -y , enable it with sudo systemctl enable fail2ban , and start the service using sudo systemctl start fail2ban . Then, configure /etc/fail2ban/jail.local by adding [sshd] enabled = true , setting maxretry = 3 , bantime = 10m , and findtime = 10m , followed by restarting the service with sudo systemctl Task 6 2 restart fail2ban to apply the changes. As we have done these steps in task 1 , I’m not gonna install it again.



To automate log monitoring, install logwatch using sudo apt install logwatch -y , then configure it to send detailed log summaries via email with logwatch --detail high --mailto root@localhost . For remote log storage or advanced filtering, edit /etc/rsyslog.conf and add \*.\* @:514 to forward logs to the designated remote server.