**Proof of Concept (PoC) Report**

**Task 6: Log Analysis & Intrusion Detection**

# Executive Summary

This PoC demonstrates the importance of log analysis and intrusion detection in identifying and mitigating brute-force attacks and unauthorized access attempts. The task involves enabling system logging, simulating failed SSH login attempts, analyzing logs to detect brute-force attempts, and implementing mitigation measures using fail2ban and log monitoring tools.

# Objectives

* **Setup:** Enable system logging and simulate multiple failed SSH login attempts.
* **Exploit:** Analyze logs to identify brute-force attempts and unauthorized access.
* **Mitigation:** Implement fail2ban to block repeated failed attempts and set up log monitoring automation.

# Setup

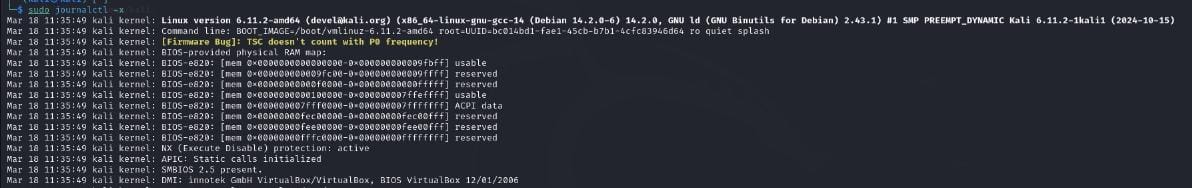
**3.1 Enable System Logging**

System logging was enabled using journalctl and rsyslog to monitor authentication attempts.

**Commands Used:**

sudo systemctl start rsyslog sudo systemctl enable rsyslog



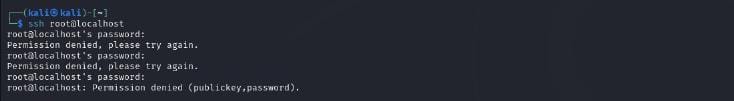


**3.2 Simulate Failed SSH Login Attempts**

Multiple failed SSH login attempts were simulated to generate log entries for analysis.

**Commands Used:**

ssh user@localhost



# Exploitation

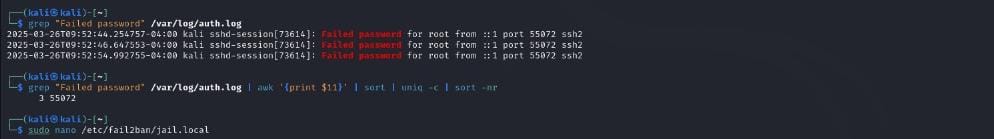
**4.1 Analyze Logs for Failed Attempts**

The logs were analyzed to identify failed SSH login attempts and potential brute-force attacks.

**Commands Used:**

grep "Failed password" /var/log/auth.log grep "Failed password" /var/log/auth.log | awk '{print $11}' | sort |

uniq -c | sort –nr



# Mitigation

**5.1 Implement fail2ban**

fail2ban was configured to block IP addresses with repeated failed login attempts.

**Commands Used:**

sudo nano /etc/fail2ban/jail.local **Configuration:**

[sshd]

enabled = true maxretry = 3 bantime = 3600



**5.2 Restart fail2ban**  fail2ban was restarted to apply the new configuration.

**Commands Used:**

sudo systemctl restart fail2ban

**5.3 Set Up Log Monitoring Automation** logwatch was configured to send detailed log reports via email.

**Commands Used:**

sudo logwatch --detail high --mailto mahaselvan100@gmail.com -- range today



# Conclusion

This PoC successfully demonstrated how log analysis can be used to detect brute-force attacks and unauthorized access attempts. By implementing fail2ban and setting up log monitoring automation, the system was secured against repeated failed login attempts.

# Recommendations

* Regularly review logs for suspicious activity.
* Use tools like fail2ban to automatically block malicious IP addresses.
* Set up automated log monitoring and reporting using logwatch or similar tools.