POC TASK 6

Step 1: Setting Up System Logging

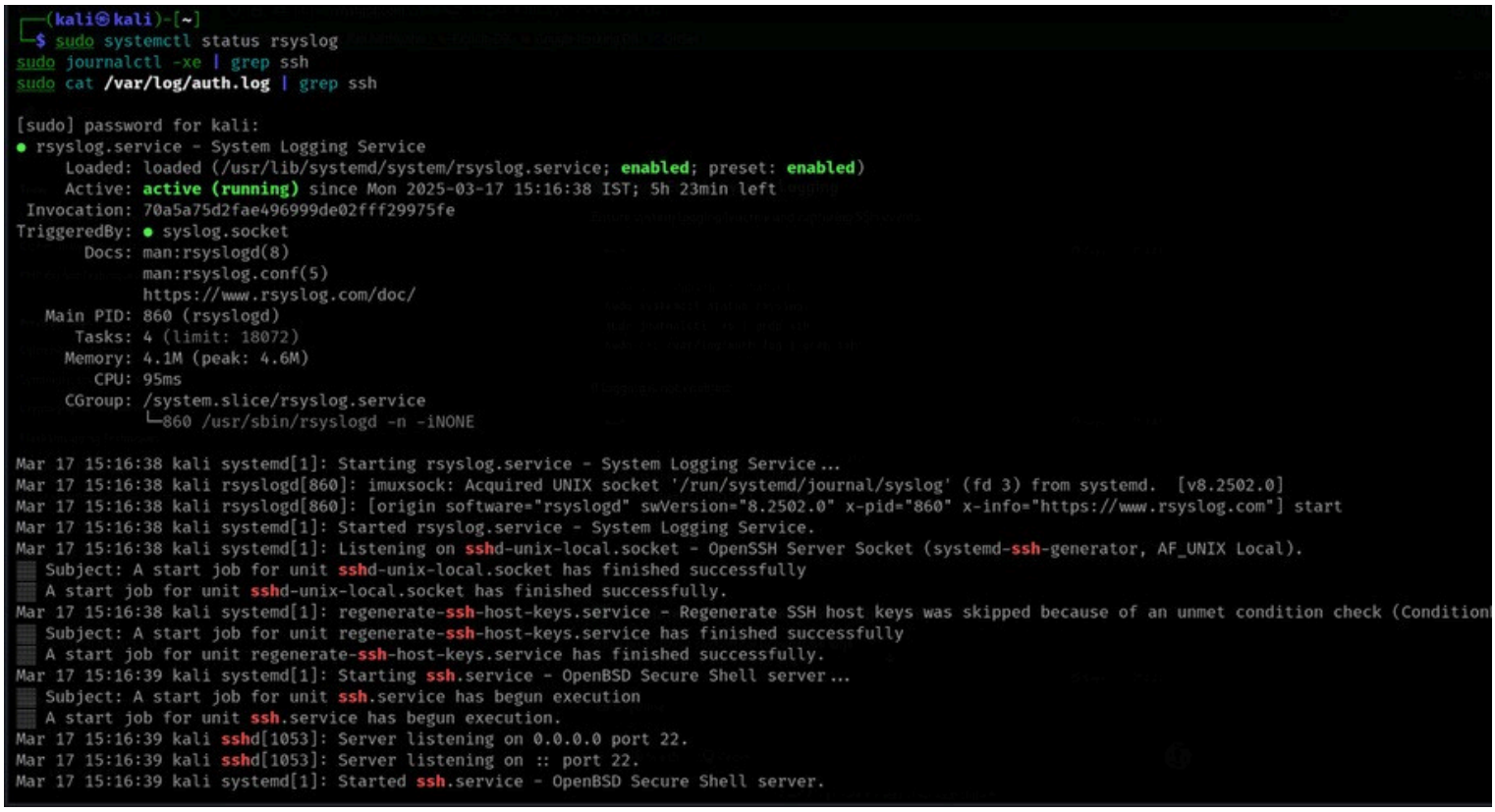
1. Verify System Logging for SSH Events

Ensure logging is active and capturing SSH-related activities:

- sudo systemctl status rsyslog
- sudo journalctl -xe | grep ssh
- sudo cat /var/log/auth.log | grep ssh

If logging is not enabled, activate and restart rsyslog:

- sudo systemctl enable rsyslog
- sudo systemctl restart rsyslog



Step 2: Simulating Multiple Failed SSH Login Attempts

1. Manual Brute-Force Simulation

Try logging in with incorrect credentials multiple times:

- ssh user@localhost

2. Automated Brute-Force Simulation with Hydra

Use Hydra to attempt SSH brute-force attacks:

- hydra -l root -P password_list.txt ssh://<target-ip>

Step 3: Exploiting and Analyzing Logs

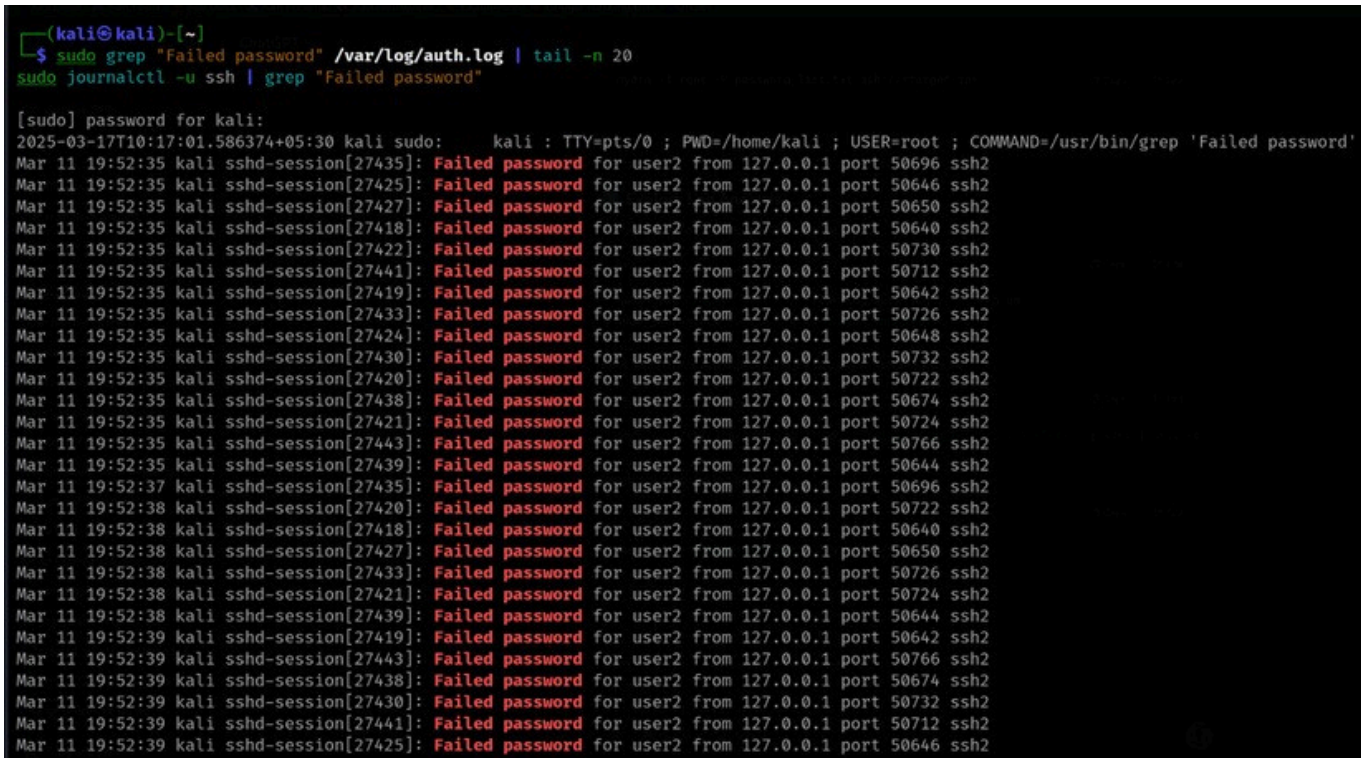
1. Extracting Failed SSH Login Attempts

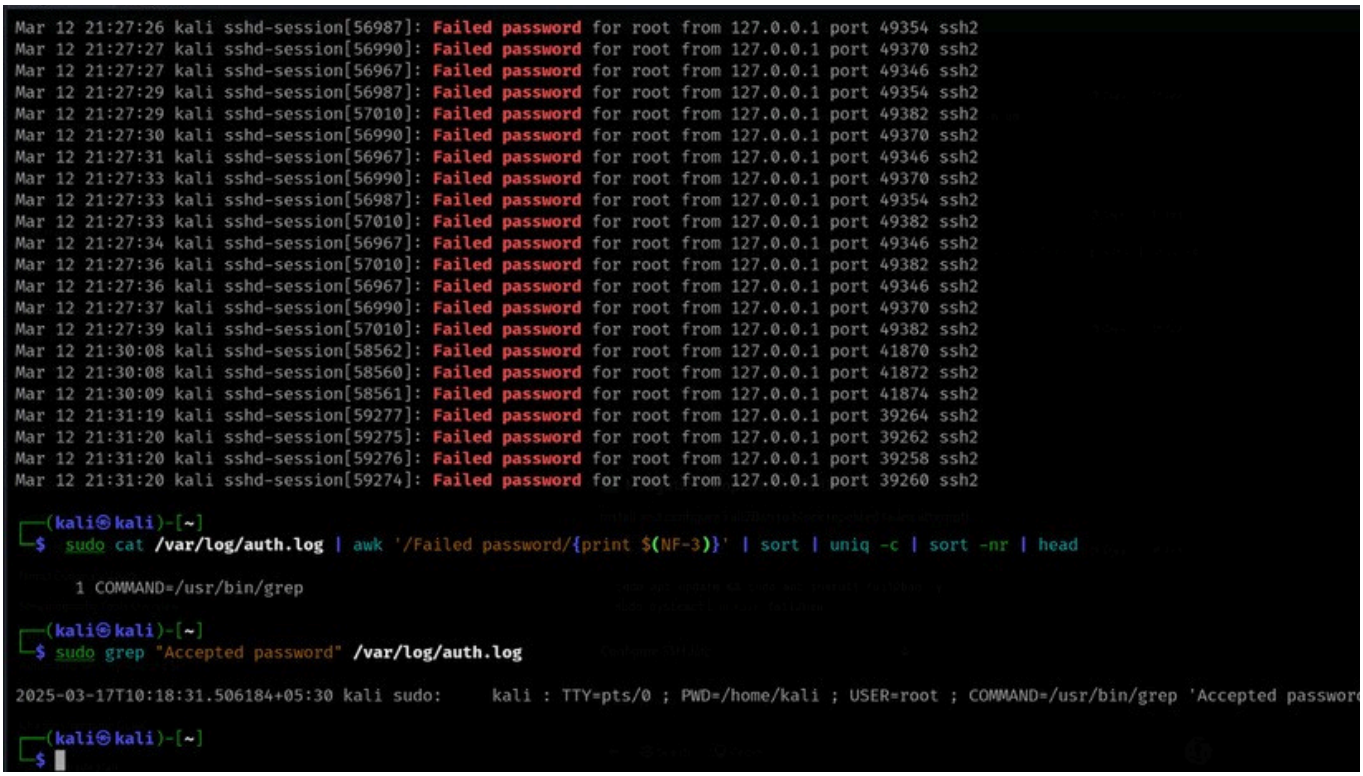
Use grep to find failed login attempts:

- sudo grep "Failed password" /var/log/auth.log | tail -n 20

Or check logs using journalctl:

- sudo journalctl -u ssh | grep "Failed password"





2. Detecting Brute-Force Attacks

Find repeated failed attempts from the same IP

- sudo cat /var/log/auth.log | awk '/Failed password/{print $(NF-3)}' | sort | uniq -c | sort -nr | head

3. Identifying Successful SSH Logins

List all successful authentication attempts:

- sudo grep "Accepted password" /var/log/auth.log

Step 4: Mitigating Attacks with Fail2Ban

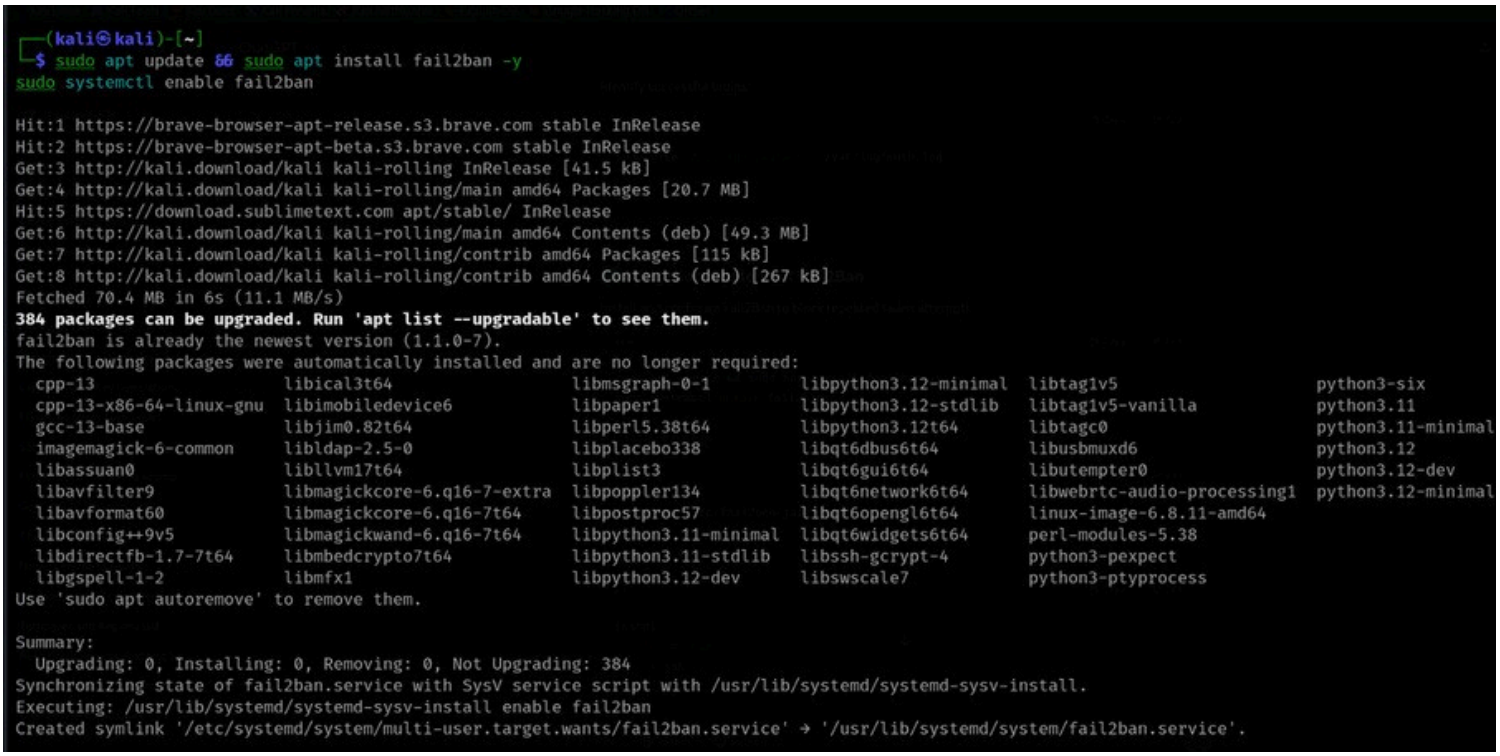
1. Installing and Enabling Fail2Ban

- sudo apt update && sudo apt install fail2ban -y
- sudo systemctl enable fail2ban

2. Configuring Fail2Ban for SSH Protection

Edit the Fail2Ban jail configuration:

- sudo nano /etc/fail2ban/jail.local



Add the following rules:

- [sshd]
- enabled = true
- port = ssh
- filter = sshd
- logpath = /var/log/auth.log
- maxretry = 5
- bantime = 600

3. Restart Fail2Ban and Verify Banned IPs

Apply the new configuration:

- sudo systemctl restart fail2ban

Check which IPs have been banned:

- sudo fail2ban-client status sshd

Step 5: Automating Log Monitoring

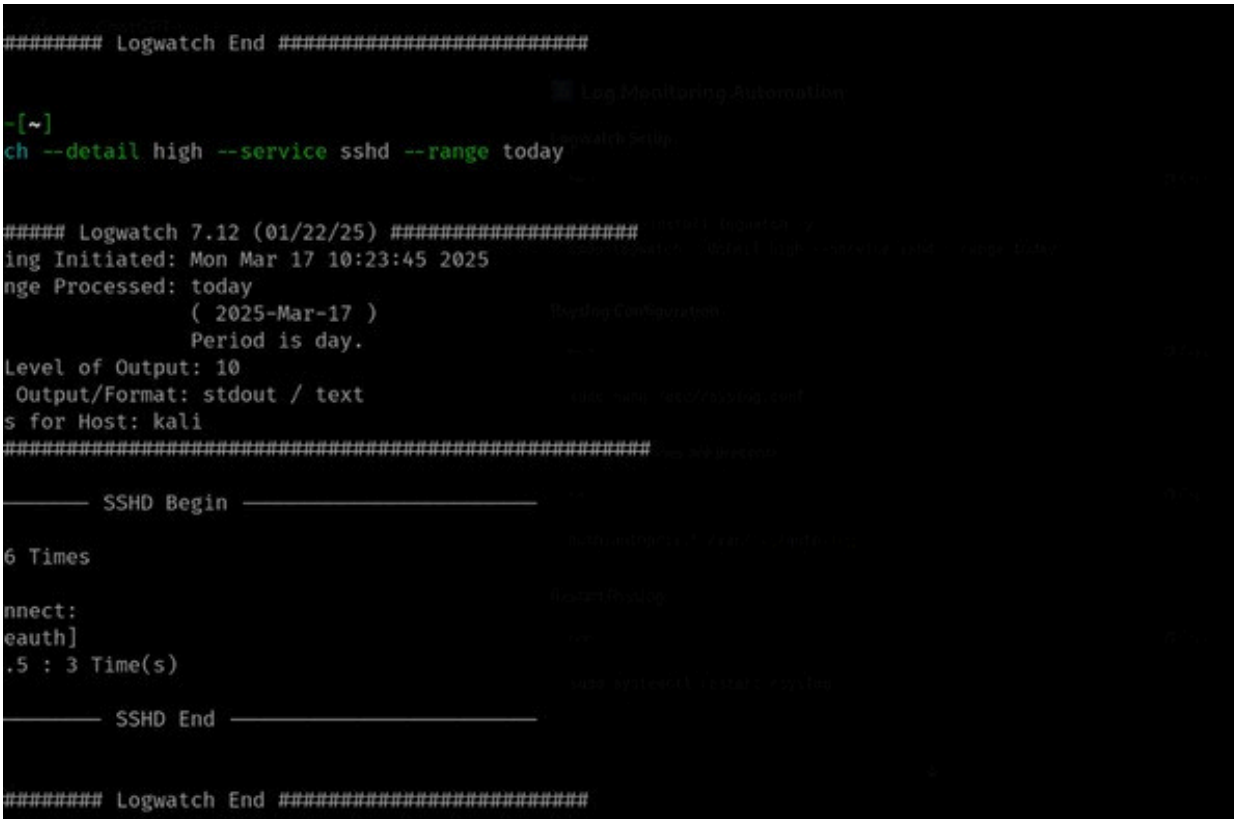
1. Setting Up Logwatch

Install Logwatch to automate log analysis:

- sudo apt install logwatch -y

Run a detailed SSH log report for today's activity:

- sudo logwatch --detail high --service sshd --range today



2. Configuring Rsyslog for Log Storage

Edit the Rsyslog configuration file:

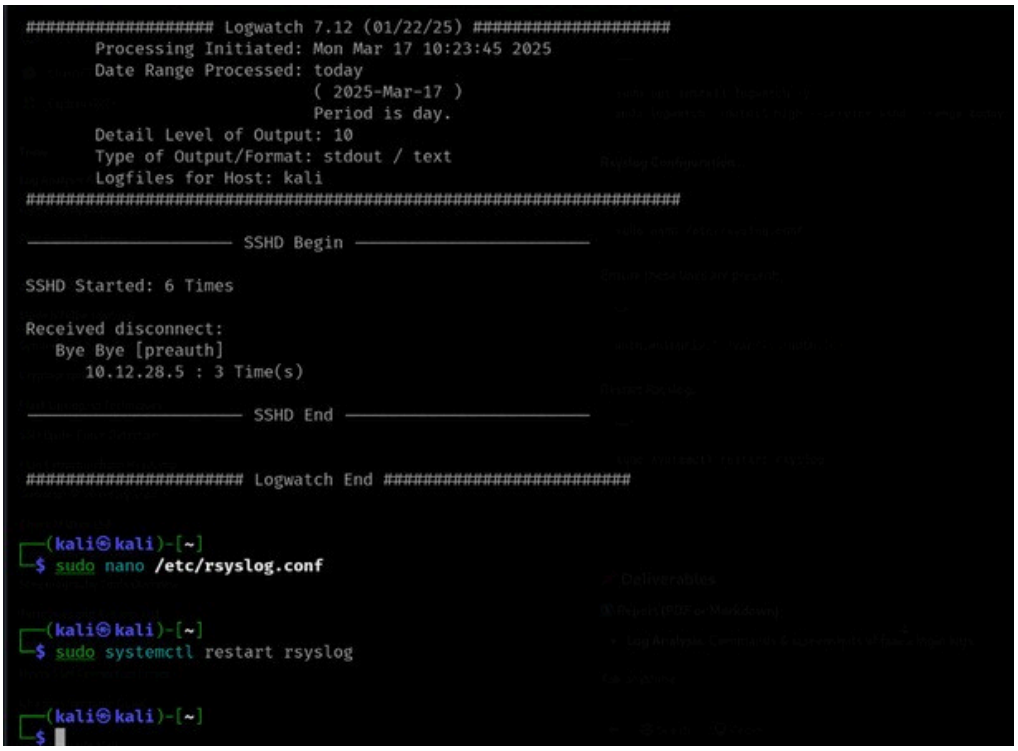
- sudo nano /etc/rsyslog.conf

Ensure the following lines exist to capture authentication logs:

- auth,authpriv.* /var/log/auth.log

Restart Rsyslog to apply changes:

- sudo systemctl restart rsyslog



Conclusion

✅ System logging ensures SSH activities are recorded.

✅ Brute-force simulation tests security vulnerabilities.

✅ Log analysis helps identify suspicious activity.

✅ Fail2Ban protects against repeated SSH attacks.

✅ Logwatch and Rsyslog automate security monitoring.