

# Task 6

## Proof of Concept (PoC) Report

### Task 6: Log Analysis & Intrusion Detection

#### 1. 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.

#### 2. 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.

#### 3. Setup

##### 3.1 Enable System Logging

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

Commands Used:

```
(kali@kali)-[~]  
$ sudo systemctl enable rsyslog && sudo systemctl start rsyslog
```

```
(kali@kali)-[~]  
$ ssh kali@localhost  
The authenticity of host 'localhost (::1)' can't be established.  
ED25519 key fingerprint is SHA256:kjohvE3xDYnnhyETAioZIAHMS+9DIF6zLYLF+YU/wMM.  
This key is not known by any other names.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added 'localhost' (ED25519) to the list of known hosts.  
kali@localhost's password:  
Linux kali 6.11.2-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.11.2-1kali1 (2024-10-15) x86_64  
  
The programs included with the Kali GNU/Linux system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.
```

## 1. 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:

```
(kali@kali)~$ sudo grep "Failed password" /var/log/auth.log
[sudo] password for kali:
2025-03-25T02:58:08-04:00 kali sudo:    kali : TTY=pts/2 ; PWD=/home/kali ; USER=root ; COMMAND=/usr/bin/grep
ep 'Failed password' /var/log/auth.log
```

## 5. Mitigation

### 5.1 Implement fail2ban

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

Commands Used:

```
(kali@kali)~$ sudo systemctl restart fail2ban
```

```
(kali@kali)~$ sudo fail2ban-client status sshd
Status for the jail: sshd
- Filter
|   - Currently failed: 0
|   - Total failed: 0
|   - Journal matches: _SYSTEMD_UNIT=ssh.service + _COMM=sshd
- Actions
|   - Currently banned: 0
|   - Total banned: 0
|   - Banned IP list:
```

```
sudo nano /etc/fail2ban/jail.local
```

```
sudo nano /etc/fail2ban/jail.local
```

Configuration:

```
[sshd]
enabled = true
maxretry = 3
```

### 5.2 Restart fail2ban

fail2ban was restarted to apply the new configuration.

Commands Used:

```
(kali@kali)-[~]  
$ sudo systemctl restart fail2ban
```

`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 Praveenraj2k05@gmail.com --range today`

```
(kali@kali)-[~]  
$ sudo systemctl restart fail2ban  
(kali@kali)-[~]  
$ sudo systemctl status rsyslog  
● rsyslog.service - System Logging Service  
   Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled; preset: enabled)  
   Active: active (running) since Tue 2025-03-25 04:03:17 EDT; 9min ago  
     Invocation: 4f75df6dc1240b39eb5126f8574375a  
   TriggeredBy: ● syslog.socket  
     Docs: man:rsyslogd(8)  
           man:rsyslog.conf(5)  
           https://www.rsyslog.com/doc/  
   Main PID: 517 (rsyslogd)  
     Tasks: 4 (limit: 3425)  
   Memory: 3.2M (peak: 3.4M)  
     CPU: 154ms  
   CGroup: /system.slice/rsyslog.service  
           └─17 /usr/sbin/rsyslogd -n -lNONE  
  
Mar 25 04:03:17 kali systemd[1]: Starting rsyslog.service - System Logging Service...  
Mar 25 04:03:17 kali rsyslogd[517]: imuxsock: Acquired UNIX socket '/run/systemd/journal/syslog' (fd 3) from syste  
Mar 25 04:03:17 kali rsyslogd[517]: [origin software="rsyslogd" swVersion="8.2502.0" x-pid="517" x-info="https://w  
Mar 25 04:03:17 kali systemd[1]: Started rsyslog.service - System Logging Service.
```

## 6. 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.

## 7. 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.