

# Proof Of Concept

## Linux Security- Exploitation & Hardening

### Task 6: Log Analysis & Intrusion Detection

#### 1. Executive Summary

This PoC demonstrates how to analyze system logs to detect and mitigate brute-force SSH login attempts. The task involves enabling system logging, simulating failed login attempts, analyzing logs for intrusion detection, and implementing fail2ban to block repeated failed attempts.

#### 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 rsyslog to capture authentication logs in /var/log/auth.log.

#### Commands Used:

sudo systemctl status rsyslog

```
---(ilansart@jaivanti)-[~/ssh]
$ sudo systemctl status rsyslog
● rsyslog.service - System Logging Service
   Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled; preset: enabled)
   Active: active (running) since Mon 2025-03-17 13:49:12 IST; 47min ago
     Invocation: de64753f0f44f00b6f0dca771f226d5
   TriggeredBy: ● syslog.socket
       Docs: man:rsyslogd(8)
             man:rsyslog.conf(5)
             https://www.rsyslog.com/doc/
    Main PID: 680 (rsyslogd)
      Tasks: 4 (limit: 10230)
    Memory: 4.2M (peak: 4.4M)
       CPU: 304ms
    CGroup: /system.slice/rsyslog.service
            └─680 /usr/sbin/rsyslogd -n -iNONE

Mar 17 13:49:12 jaivanti systemd[1]: Starting rsyslog.service - System Logging Service...
Mar 17 13:49:12 jaivanti rsyslogd[680]: imuxsock: Acquired UNIX socket '/run/systemd/journal/syslog' (fd 3) from systemd. [v8.2502.0]
Mar 17 13:49:12 jaivanti rsyslogd[680]: [origin software="rsyslogd" swVersion="8.2502.0" x-pid="680" x-info="https://www.rsyslog.com"] start
Mar 17 13:49:12 jaivanti systemd[1]: Started rsyslog.service - System Logging Service.
```

## 3.2 Simulate Failed SSH Login Attempts

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

### Commands Used:

```
hydra -l invaliduser -P world1k.txt ssh://localhost
```

```
---(llanofart@jaivanti)-[~]
$ hydra -l wordlist.txt -P wordlist.txt ssh://localhost
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-17 14:34:03
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 9 tasks per 1 server, overall 9 tasks, 9 login tries (l:3/p:3), -1 try per task
[DATA] attacking ssh://localhost:22/
[ERROR] target ssh://127.0.0.1:22/ does not support password authentication (method reply 4).
```

## 4. Exploitation

### 4.1 Analyze Logs for Failed Login Attempts

The /var/log/auth.log file was analyzed to identify failed SSH login attempts.

### Commands Used:

```
grep "Failed password" /var/log/auth.log
```

```
---(llanofart@jaivanti)-[~]
$ grep "Failed password" /var/log/auth.log
2025-03-16T22:34:00.647710+05:30 jaivanti sshd-session[19243]: Failed password for invalid user invaliduser from 192.168.29.149 port 58212 ssh2
```

## 5. 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
```

```
sudo systemctl restart fail2ban
```

```
---(llanofart@jaivanti)-[~/.ssh]
$ sudo nano /etc/fail2ban/jail.local

---(llanofart@jaivanti)-[~/.ssh]
$ cat /etc/fail2ban/jail.local
[sshd]
enabled = true
maxretry = 3
bantime = 3600

---(llanofart@jaivanti)-[~/.ssh]
$ sudo systemctl restart fail2ban
```

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

## 5.2 Set Up Log Monitoring Automation

Log monitoring was automated using logwatch and rsyslog to ensure continuous monitoring and alerting.

### Commands Used:

```
sudo logwatch --detail high --mailto user@example.com --range today
```

```
sudo systemctl status rsyslog
```

```
--(llanofart@jaivanti)-[/].ssh
└─$ sudo logwatch --detail high --mailto jaivantints12@gmail.com --range today

--(llanofart@jaivanti)-[/].ssh
└─$ sudo systemctl status rsyslog
● rsyslog.service - System Logging Service
   Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled; preset: enabled)
   Active: active (running) since Mon 2025-03-17 13:49:12 IST; 47min ago
     Invocation: d6d4752f7d44f0bbe6bca771f226d5
   TriggeredBy: ● syslog.socket
      Docs: man:rsyslogd(8)
            man:rsyslog.conf(5)
            https://www.rsyslog.com/doc/
    Main PID: 680 (rsyslogd)
      Tasks: 4 (limit: 18730)
     Memory: 4.2M (peak: 4.4M)
        CPU: 304ms
    CGroup: /system.slice/rsyslog.service
            └─680 /usr/sbin/rsyslogd -n -lNONE

Mar 17 13:49:12 jaivanti systemd[1]: Starting rsyslog.service - System Logging Service...
Mar 17 13:49:12 jaivanti rsyslogd[680]: Imuxsock: Acquired UNIX socket '/run/systemd/journal/syslog' (fd 3) from systemd. [v0.2502.0]
Mar 17 13:49:12 jaivanti rsyslogd[680]: [origin software="rsyslogd" swversion="0.2502.0" x-pid="680" x-info="https://www.rsyslog.com"] start
Mar 17 13:49:12 jaivanti systemd[1]: Started rsyslog.service - System Logging Service.
```

## 6. Conclusion

This PoC successfully demonstrated how to detect brute-force SSH login attempts through log analysis and mitigate the risk using fail2ban. By automating log monitoring, the system can proactively respond to potential security threats.