SOC LOG ANALYSIS & DETECTION

Project Title

Web Server Security Assessment – SOC Log Analysis & Detection

Environment

- Target System: Ubuntu Server (LAMP Stack)
- Attacker System: Kali Linux
- Environment Type: Controlled Lab
- Services Analyzed: SSH, FTP, MySQL, SMTP

Objective

The objective of this report is to analyze system and application logs generated during simulated attacks, identify Indicators of Compromise (IOCs), detect malicious behavior, and recommend mitigation actions from a SOC analyst perspective.

Overview of SOC Log Analysis

Log analysis is a critical responsibility of a Security Operations Center (SOC). It involves monitoring authentication events, service access logs, and application activity to identify unauthorized access, brute-force attempts, and misuse of services.

In this project, simulated penetration testing activities were performed to understand how real-world attacks appear in logs and how SOC analysts detect and respond to them.

Scope of Log Analysis

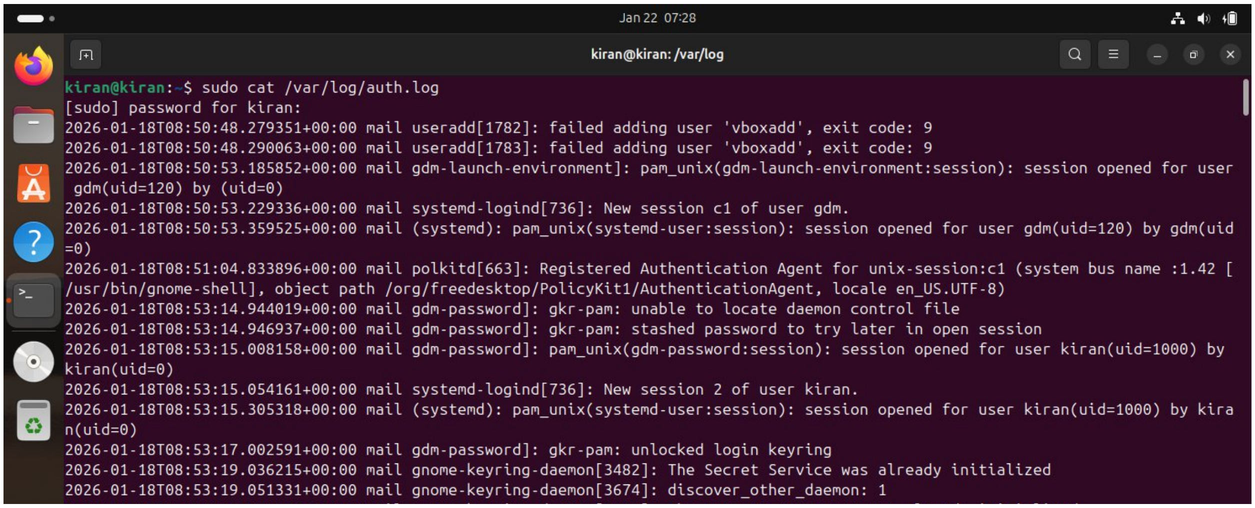
The following logs were analyzed:

- SSH Authentication Logs (`/var/log/auth.log`)
- FTP Service Logs (`/var/log/vsftpd.log`)
- MySQL Database Logs (`/var/log/mysql/mysql.log`)
- SMTP Mail Logs (`/var/log/mail.log`)

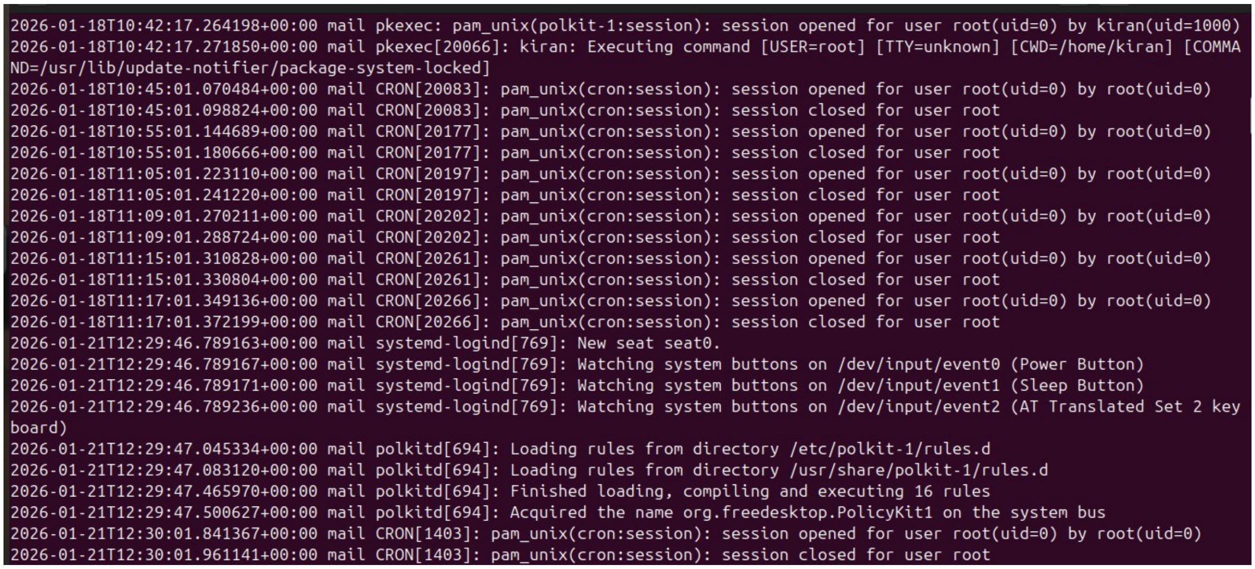
SSH Log Analysis and Detection

Log File

`/var/log/auth.log`



```
kiran@kiran:~$ sudo cat /var/log/auth.log
[sudo] password for kiran:
2026-01-18T08:50:48.279351+00:00 mail useradd[1782]: failed adding user 'vboxadd', exit code: 9
2026-01-18T08:50:48.290063+00:00 mail useradd[1783]: failed adding user 'vboxadd', exit code: 9
2026-01-18T08:50:53.185852+00:00 mail gdm-launch-environment]: pam_unix(gdm-launch-environment:session): session opened for user
 gdm(uid=120) by (uid=0)
2026-01-18T08:50:53.229336+00:00 mail systemd-logind[736]: New session c1 of user gdm.
2026-01-18T08:50:53.359525+00:00 mail (systemd): pam_unix(systemd-user:session): session opened for user gdm(uid=120) by gdm(uid
=0)
2026-01-18T08:51:04.833896+00:00 mail polkitd[663]: Registered Authentication Agent for unix-session:c1 (system bus name :1.42 [
/usr/bin/gnome-shell], object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8)
2026-01-18T08:53:14.944019+00:00 mail gdm-password]: gkr-pam: unable to locate daemon control file
2026-01-18T08:53:14.946937+00:00 mail gdm-password]: gkr-pam: stashed password to try later in open session
2026-01-18T08:53:15.008158+00:00 mail gdm-password]: pam_unix(gdm-password:session): session opened for user kiran(uid=1000) by
kiran(uid=0)
2026-01-18T08:53:15.054161+00:00 mail systemd-logind[736]: New session 2 of user kiran.
2026-01-18T08:53:15.305318+00:00 mail (systemd): pam_unix(systemd-user:session): session opened for user kiran(uid=1000) by kira
n(uid=0)
2026-01-18T08:53:17.002591+00:00 mail gdm-password]: gkr-pam: unlocked login keyring
2026-01-18T08:53:19.036215+00:00 mail gnome-keyring-daemon[3482]: The Secret Service was already initialized
2026-01-18T08:53:19.051331+00:00 mail gnome-keyring-daemon[3674]: discover_other_daemon: 1
```



```
2026-01-18T10:42:17.264198+00:00 mail pkexec: pam_unix(polkit-1:session): session opened for user root(uid=0) by kiran(uid=1000)
2026-01-18T10:42:17.271850+00:00 mail pkexec[20066]: kiran: Executing command [USER=root] [TTY=unknown] [CWD=/home/kiran] [COMMA
ND=/usr/lib/update-notifier/package-system-locked]
2026-01-18T10:45:01.070484+00:00 mail CRON[20083]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2026-01-18T10:45:01.098824+00:00 mail CRON[20083]: pam_unix(cron:session): session closed for user root
2026-01-18T10:55:01.144689+00:00 mail CRON[20177]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2026-01-18T10:55:01.180666+00:00 mail CRON[20177]: pam_unix(cron:session): session closed for user root
2026-01-18T11:05:01.223110+00:00 mail CRON[20197]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2026-01-18T11:05:01.241220+00:00 mail CRON[20197]: pam_unix(cron:session): session closed for user root
2026-01-18T11:09:01.270211+00:00 mail CRON[20202]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2026-01-18T11:09:01.288724+00:00 mail CRON[20202]: pam_unix(cron:session): session closed for user root
2026-01-18T11:15:01.310828+00:00 mail CRON[20261]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2026-01-18T11:15:01.330804+00:00 mail CRON[20261]: pam_unix(cron:session): session closed for user root
2026-01-18T11:17:01.349136+00:00 mail CRON[20266]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2026-01-18T11:17:01.372199+00:00 mail CRON[20266]: pam_unix(cron:session): session closed for user root
2026-01-21T12:29:46.789163+00:00 mail systemd-logind[769]: New seat seat0.
2026-01-21T12:29:46.789167+00:00 mail systemd-logind[769]: Watching system buttons on /dev/input/event0 (Power Button)
2026-01-21T12:29:46.789171+00:00 mail systemd-logind[769]: Watching system buttons on /dev/input/event1 (Sleep Button)
2026-01-21T12:29:46.789236+00:00 mail systemd-logind[769]: Watching system buttons on /dev/input/event2 (AT Translated Set 2 key
board)
2026-01-21T12:29:47.045334+00:00 mail polkitd[694]: Loading rules from directory /etc/polkit-1/rules.d
2026-01-21T12:29:47.083120+00:00 mail polkitd[694]: Loading rules from directory /usr/share/polkit-1/rules.d
2026-01-21T12:29:47.465970+00:00 mail polkitd[694]: Finished loading, compiling and executing 16 rules
2026-01-21T12:29:47.500627+00:00 mail polkitd[694]: Acquired the name org.freedesktop.PolicyKit1 on the system bus
2026-01-21T12:30:01.841367+00:00 mail CRON[1403]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2026-01-21T12:30:01.961141+00:00 mail CRON[1403]: pam_unix(cron:session): session closed for user root
```

Observed Activity

- Multiple failed SSH login attempts from a single source IP
- Repeated authentication failures within a short time interval
- Successful login after multiple failed attempts

Sample Log Indicators

- `Failed password for invalid user`
- `Failed password for root`
- `Accepted password for user`

Indicators of Compromise (IOCs)

- High number of failed login attempts from one IP
- Login attempts for non-existent users
- Brute-force behavior patterns

Detection Rule:

```
Condition: More than 5 failed SSH login attempts from the same IP
within 1 minute
```

```
Action: Generate Brute Force Alert
```

SOC Analysis

This activity indicates an SSH brute-force attack where an attacker attempts multiple username and password combinations to gain unauthorized access.

Severity

High

FTP Log Analysis and Detection

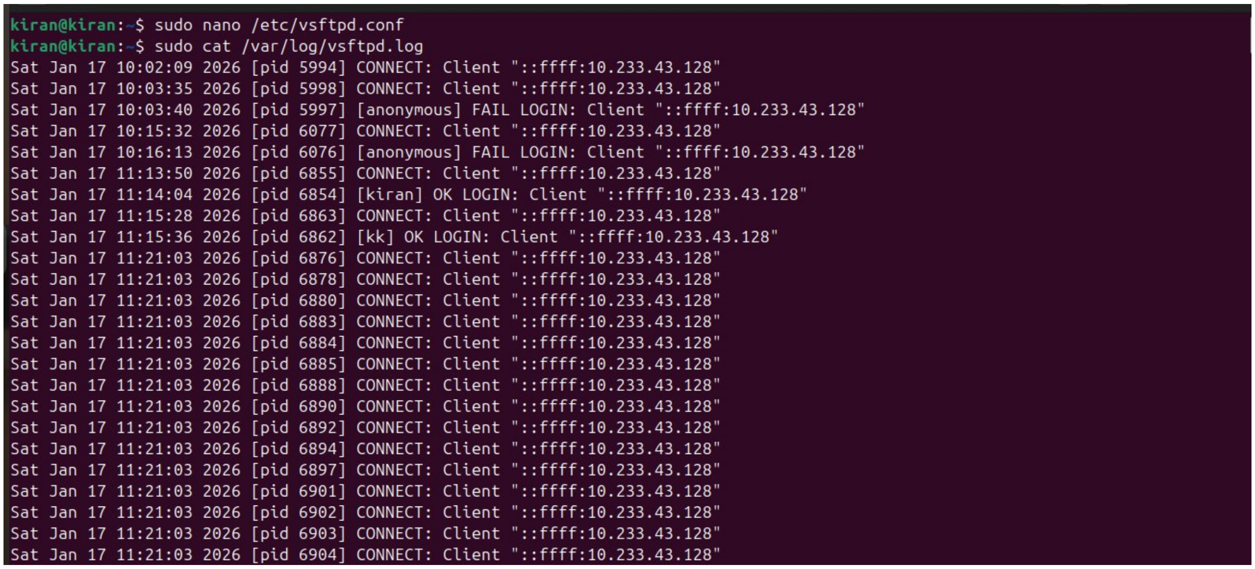
Log File

```
sudo nano /etc/vsftpd.conf
```

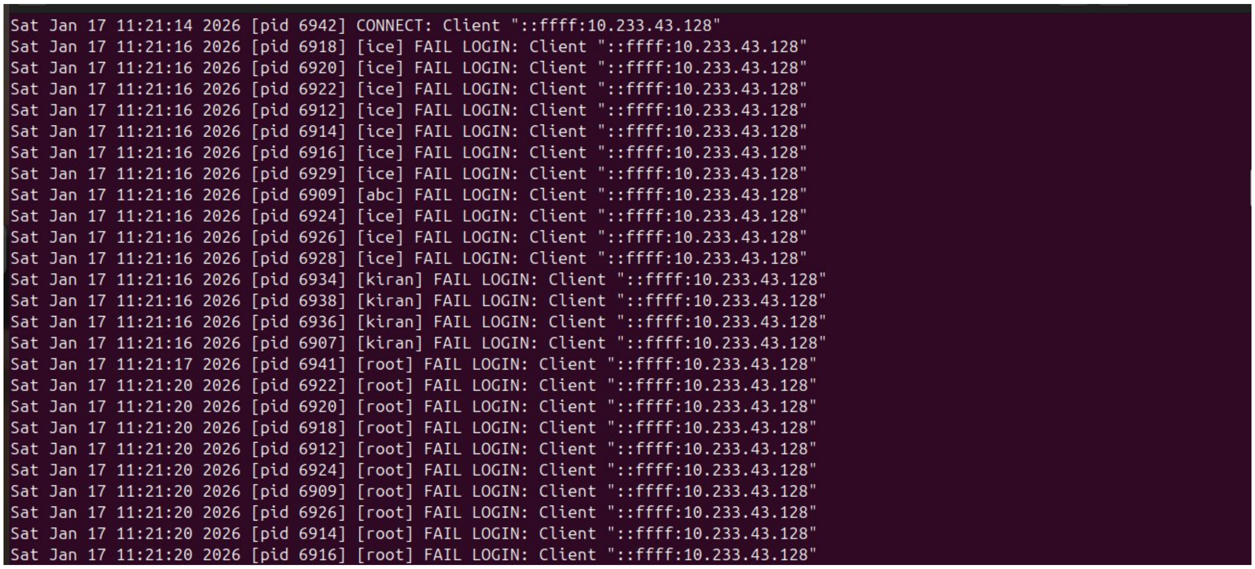
```
log_ftp_protocol=YES
```

```
sudo systemctl restart vsftpd
```

```
/var/log/vsftpd.log
```



```
kiran@kiran:~$ sudo nano /etc/vsftpd.conf
kiran@kiran:~$ sudo cat /var/log/vsftpd.log
Sat Jan 17 10:02:09 2026 [pid 5994] CONNECT: Client "::ffff:10.233.43.128"
Sat Jan 17 10:03:35 2026 [pid 5998] CONNECT: Client "::ffff:10.233.43.128"
Sat Jan 17 10:03:40 2026 [pid 5997] [anonymous] FAIL LOGIN: Client "::ffff:10.233.43.128"
Sat Jan 17 10:15:32 2026 [pid 6077] CONNECT: Client "::ffff:10.233.43.128"
Sat Jan 17 10:16:13 2026 [pid 6076] [anonymous] FAIL LOGIN: Client "::ffff:10.233.43.128"
Sat Jan 17 11:13:50 2026 [pid 6855] CONNECT: Client "::ffff:10.233.43.128"
Sat Jan 17 11:14:04 2026 [pid 6854] [kiran] OK LOGIN: Client "::ffff:10.233.43.128"
Sat Jan 17 11:15:28 2026 [pid 6863] CONNECT: Client "::ffff:10.233.43.128"
Sat Jan 17 11:15:36 2026 [pid 6862] [kk] OK LOGIN: Client "::ffff:10.233.43.128"
Sat Jan 17 11:21:03 2026 [pid 6876] CONNECT: Client "::ffff:10.233.43.128"
Sat Jan 17 11:21:03 2026 [pid 6878] CONNECT: Client "::ffff:10.233.43.128"
Sat Jan 17 11:21:03 2026 [pid 6880] CONNECT: Client "::ffff:10.233.43.128"
Sat Jan 17 11:21:03 2026 [pid 6883] CONNECT: Client "::ffff:10.233.43.128"
Sat Jan 17 11:21:03 2026 [pid 6884] CONNECT: Client "::ffff:10.233.43.128"
Sat Jan 17 11:21:03 2026 [pid 6885] CONNECT: Client "::ffff:10.233.43.128"
Sat Jan 17 11:21:03 2026 [pid 6888] CONNECT: Client "::ffff:10.233.43.128"
Sat Jan 17 11:21:03 2026 [pid 6890] CONNECT: Client "::ffff:10.233.43.128"
Sat Jan 17 11:21:03 2026 [pid 6892] CONNECT: Client "::ffff:10.233.43.128"
Sat Jan 17 11:21:03 2026 [pid 6894] CONNECT: Client "::ffff:10.233.43.128"
Sat Jan 17 11:21:03 2026 [pid 6897] CONNECT: Client "::ffff:10.233.43.128"
Sat Jan 17 11:21:03 2026 [pid 6901] CONNECT: Client "::ffff:10.233.43.128"
Sat Jan 17 11:21:03 2026 [pid 6902] CONNECT: Client "::ffff:10.233.43.128"
Sat Jan 17 11:21:03 2026 [pid 6903] CONNECT: Client "::ffff:10.233.43.128"
Sat Jan 17 11:21:03 2026 [pid 6904] CONNECT: Client "::ffff:10.233.43.128"
```



```
Sat Jan 17 11:21:14 2026 [pid 6942] CONNECT: Client "::ffff:10.233.43.128"
Sat Jan 17 11:21:16 2026 [pid 6918] [ice] FAIL LOGIN: Client "::ffff:10.233.43.128"
Sat Jan 17 11:21:16 2026 [pid 6920] [ice] FAIL LOGIN: Client "::ffff:10.233.43.128"
Sat Jan 17 11:21:16 2026 [pid 6922] [ice] FAIL LOGIN: Client "::ffff:10.233.43.128"
Sat Jan 17 11:21:16 2026 [pid 6912] [ice] FAIL LOGIN: Client "::ffff:10.233.43.128"
Sat Jan 17 11:21:16 2026 [pid 6914] [ice] FAIL LOGIN: Client "::ffff:10.233.43.128"
Sat Jan 17 11:21:16 2026 [pid 6916] [ice] FAIL LOGIN: Client "::ffff:10.233.43.128"
Sat Jan 17 11:21:16 2026 [pid 6929] [ice] FAIL LOGIN: Client "::ffff:10.233.43.128"
Sat Jan 17 11:21:16 2026 [pid 6909] [abc] FAIL LOGIN: Client "::ffff:10.233.43.128"
Sat Jan 17 11:21:16 2026 [pid 6924] [ice] FAIL LOGIN: Client "::ffff:10.233.43.128"
Sat Jan 17 11:21:16 2026 [pid 6926] [ice] FAIL LOGIN: Client "::ffff:10.233.43.128"
Sat Jan 17 11:21:16 2026 [pid 6928] [ice] FAIL LOGIN: Client "::ffff:10.233.43.128"
Sat Jan 17 11:21:16 2026 [pid 6934] [kiran] FAIL LOGIN: Client "::ffff:10.233.43.128"
Sat Jan 17 11:21:16 2026 [pid 6938] [kiran] FAIL LOGIN: Client "::ffff:10.233.43.128"
Sat Jan 17 11:21:16 2026 [pid 6936] [kiran] FAIL LOGIN: Client "::ffff:10.233.43.128"
Sat Jan 17 11:21:16 2026 [pid 6907] [kiran] FAIL LOGIN: Client "::ffff:10.233.43.128"
Sat Jan 17 11:21:17 2026 [pid 6941] [root] FAIL LOGIN: Client "::ffff:10.233.43.128"
Sat Jan 17 11:21:20 2026 [pid 6922] [root] FAIL LOGIN: Client "::ffff:10.233.43.128"
Sat Jan 17 11:21:20 2026 [pid 6920] [root] FAIL LOGIN: Client "::ffff:10.233.43.128"
Sat Jan 17 11:21:20 2026 [pid 6918] [root] FAIL LOGIN: Client "::ffff:10.233.43.128"
Sat Jan 17 11:21:20 2026 [pid 6912] [root] FAIL LOGIN: Client "::ffff:10.233.43.128"
Sat Jan 17 11:21:20 2026 [pid 6924] [root] FAIL LOGIN: Client "::ffff:10.233.43.128"
Sat Jan 17 11:21:20 2026 [pid 6909] [root] FAIL LOGIN: Client "::ffff:10.233.43.128"
Sat Jan 17 11:21:20 2026 [pid 6926] [root] FAIL LOGIN: Client "::ffff:10.233.43.128"
Sat Jan 17 11:21:20 2026 [pid 6914] [root] FAIL LOGIN: Client "::ffff:10.233.43.128"
Sat Jan 17 11:21:20 2026 [pid 6916] [root] FAIL LOGIN: Client "::ffff:10.233.43.128"
```

Observed Activity

- Anonymous FTP login attempts
- Failed authentication attempts for valid users
- Successful login using weak credentials

Sample Log Indicators

- `Anonymous FTP login allowed`
- `530 Login incorrect`
- `230 Login successful`

Indicators of Compromise (IOCs)

- Anonymous access enabled
- Repeated login failures
- Unauthorized file access attempts

Detection Logic

```
If anonymous FTP login detected → Policy Violation Alert
```

```
If repeated FTP login failures from same IP → Brute Force Alert
```

SOC Analysis

FTP services are commonly abused for unauthorized access and data exfiltration. Anonymous login increases attack surface and risk.

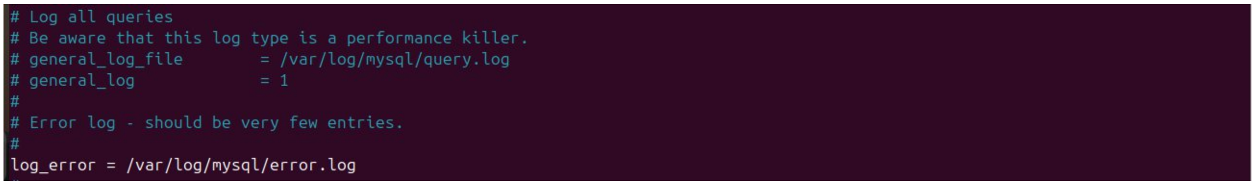
Severity

Medium to High

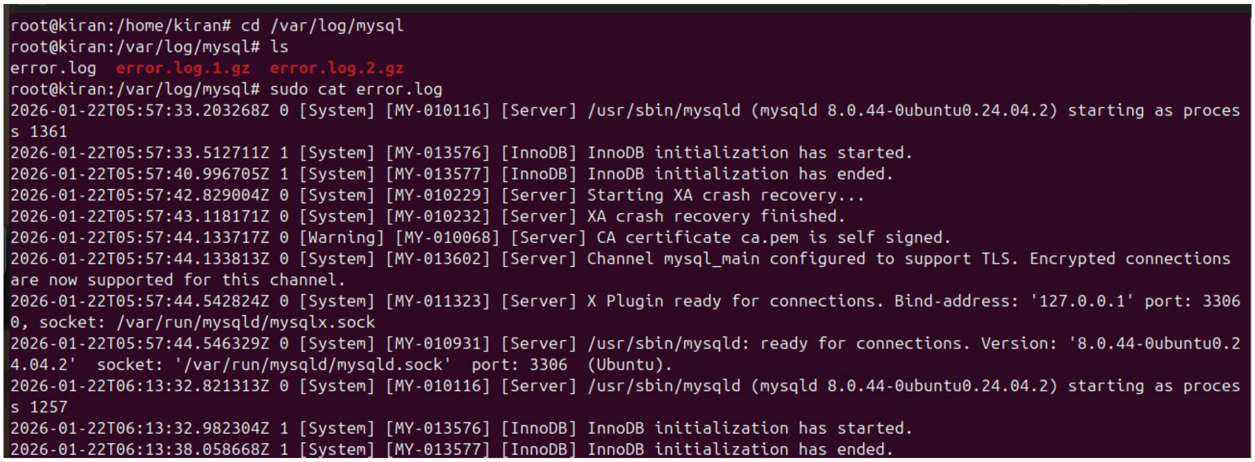
MySQL Log Analysis and Detection

Log File

- ➢ `sudo nano /etc/mysql/mysql.conf.d/mysqld.cnf`
- ➢ `general_log = ON`
- ➢ `general_log_file = /var/log/mysql/mysql.log`
- ➢ `sudo systemctl restart mysql`
- ➢ `/var/log/mysql/error.log`



```
# Log all queries
# Be aware that this log type is a performance killer.
# general_log_file        = /var/log/mysql/query.log
# general_log             = 1
#
# Error log - should be very few entries.
#
log_error = /var/log/mysql/error.log
```



```
root@kiran:/home/kiran# cd /var/log/mysql
root@kiran:/var/log/mysql# ls
error.log  error.log.1.gz  error.log.2.gz
root@kiran:/var/log/mysql# sudo cat error.log
2026-01-22T05:57:33.203268Z 0 [System] [MY-010116] [Server] /usr/sbin/mysqld (mysqld 8.0.44-0ubuntu0.24.04.2) starting as proces
s 1361
2026-01-22T05:57:33.512711Z 1 [System] [MY-013576] [InnoDB] InnoDB initialization has started.
2026-01-22T05:57:40.996705Z 1 [System] [MY-013577] [InnoDB] InnoDB initialization has ended.
2026-01-22T05:57:42.829004Z 0 [System] [MY-010229] [Server] Starting XA crash recovery...
2026-01-22T05:57:43.118171Z 0 [System] [MY-010232] [Server] XA crash recovery finished.
2026-01-22T05:57:44.133717Z 0 [Warning] [MY-010068] [Server] CA certificate ca.pem is self signed.
2026-01-22T05:57:44.133813Z 0 [System] [MY-013602] [Server] Channel mysql_main configured to support TLS. Encrypted connections
are now supported for this channel.
2026-01-22T05:57:44.542824Z 0 [System] [MY-011323] [Server] X Plugin ready for connections. Bind-address: '127.0.0.1' port: 3306
0, socket: /var/run/mysqld/mysqlx.sock
2026-01-22T05:57:44.546329Z 0 [System] [MY-010931] [Server] /usr/sbin/mysqld: ready for connections. Version: '8.0.44-0ubuntu0.2
4.04.2'  socket: '/var/run/mysqld/mysqld.sock'  port: 3306  (Ubuntu).
2026-01-22T06:13:32.821313Z 0 [System] [MY-010116] [Server] /usr/sbin/mysqld (mysqld 8.0.44-0ubuntu0.24.04.2) starting as proces
s 1257
2026-01-22T06:13:32.982304Z 1 [System] [MY-013576] [InnoDB] InnoDB initialization has started.
2026-01-22T06:13:38.058668Z 1 [System] [MY-013577] [InnoDB] InnoDB initialization has ended.
```

Observed Activity

- Remote login attempts using privileged accounts
- Multiple failed authentication attempts
- Database enumeration activity

Sample Log Indicators

- `Access denied for user`
- `Authentication failed`
- `Query execution from remote IP`

Indicators of Compromise (IOCs)

- External IP attempting database access
- Repeated authentication failures
- Use of high-privileged accounts

Detection Logic

```
If MySQL login attempt from external IP → Unauthorized Access Alert
```

```
If multiple failed database logins → Credential Abuse Alert
```

SOC Analysis

Database services should not be exposed publicly. These logs indicate credential abuse and potential data compromise attempts.

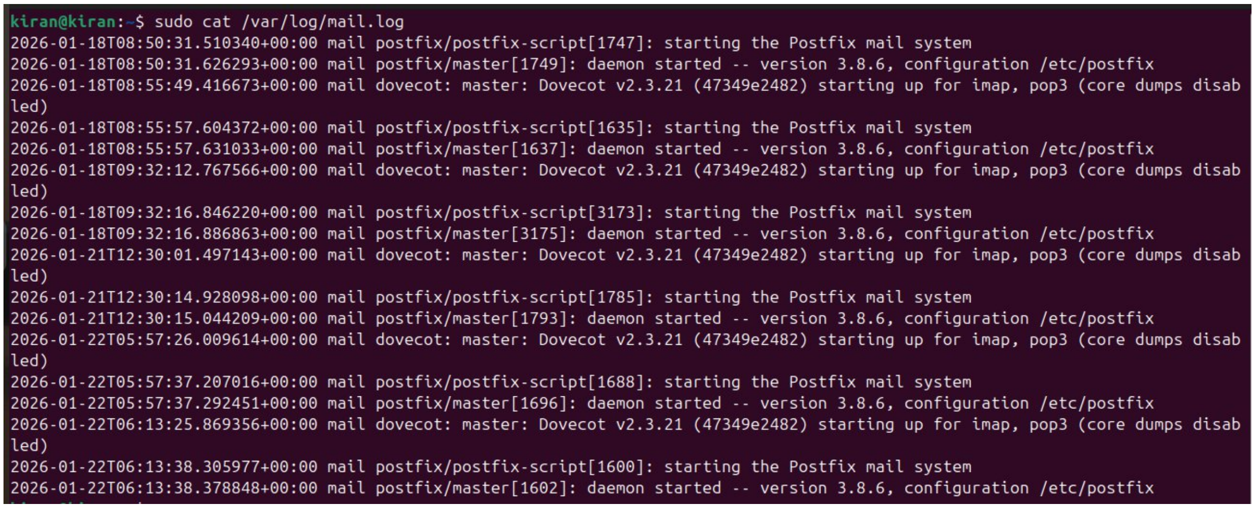
Severity

High

SMTP Log Analysis and Detection

Log File

`/var/log/mail.log`



```
kiran@kiran:~$ sudo cat /var/log/mail.log
2026-01-18T08:50:31.510340+00:00 mail postfix/postfix-script[1747]: starting the Postfix mail system
2026-01-18T08:50:31.626293+00:00 mail postfix/master[1749]: daemon started -- version 3.8.6, configuration /etc/postfix
2026-01-18T08:55:49.416673+00:00 mail dovecot: master: Dovecot v2.3.21 (47349e2482) starting up for imap, pop3 (core dumps disab
led)
2026-01-18T08:55:57.604372+00:00 mail postfix/postfix-script[1635]: starting the Postfix mail system
2026-01-18T08:55:57.631033+00:00 mail postfix/master[1637]: daemon started -- version 3.8.6, configuration /etc/postfix
2026-01-18T09:32:12.767566+00:00 mail dovecot: master: Dovecot v2.3.21 (47349e2482) starting up for imap, pop3 (core dumps disab
led)
2026-01-18T09:32:16.846220+00:00 mail postfix/postfix-script[3173]: starting the Postfix mail system
2026-01-18T09:32:16.886863+00:00 mail postfix/master[3175]: daemon started -- version 3.8.6, configuration /etc/postfix
2026-01-21T12:30:01.497143+00:00 mail dovecot: master: Dovecot v2.3.21 (47349e2482) starting up for imap, pop3 (core dumps disab
led)
2026-01-21T12:30:14.928098+00:00 mail postfix/postfix-script[1785]: starting the Postfix mail system
2026-01-21T12:30:15.044209+00:00 mail postfix/master[1793]: daemon started -- version 3.8.6, configuration /etc/postfix
2026-01-22T05:57:26.009614+00:00 mail dovecot: master: Dovecot v2.3.21 (47349e2482) starting up for imap, pop3 (core dumps disab
led)
2026-01-22T05:57:37.207016+00:00 mail postfix/postfix-script[1688]: starting the Postfix mail system
2026-01-22T05:57:37.292451+00:00 mail postfix/master[1696]: daemon started -- version 3.8.6, configuration /etc/postfix
2026-01-22T06:13:25.869356+00:00 mail dovecot: master: Dovecot v2.3.21 (47349e2482) starting up for imap, pop3 (core dumps disab
led)
2026-01-22T06:13:38.305977+00:00 mail postfix/postfix-script[1600]: starting the Postfix mail system
2026-01-22T06:13:38.378848+00:00 mail postfix/master[1602]: daemon started -- version 3.8.6, configuration /etc/postfix
```

Observed Activity

- Unauthorized SMTP connections
- Open relay testing behavior
- Suspicious email sending attempts

Sample Log Indicators

- `Relay access denied`
- `Connection from unknown host`
- `Authentication failure`

Indicators of Compromise (IOCs)

- Unknown IP sending mail
- Relay misuse attempts
- Excessive SMTP connections

Detection Logic

```
If SMTP relay attempt without authentication → Mail Abuse Alert

If multiple mail attempts from unknown IP → Spam Activity Alert
```

SOC Analysis

SMTP servers are frequently abused for spam and phishing. Improper configuration can lead to blacklisting and reputation damage.

Severity

Medium

Summary of Detected Threats

Service	Attack Type	Detection Source	Severity
SSH	Brute Force	auth.log	High
FTP	Unauthorized Access	vsftpd.log	Medium
MySQL	Credential Abuse	mysql.log	High
SMTP	Mail Relay Abuse	mail.log	Medium

Incident Timeline (Example)

1. Reconnaissance detected via service scans
2. Brute-force attempts observed in authentication logs
3. Successful unauthorized access identified
4. SOC alert triggered based on detection rules
5. Mitigation actions applied

Mitigation and Response Actions

- Enabled Fail2Ban for SSH brute-force protection
- Disabled anonymous FTP access
- Restricted MySQL access to localhost
- Secured SMTP relay configuration
- Recommended centralized logging and SIEM integration

Lessons Learned (SOC Perspective)

- Log visibility is critical for early attack detection
- Brute-force attacks are easily identifiable through log correlation
- Proper service hardening significantly reduces risk
- SOC analysts must understand both attack methods and defensive controls

Conclusion

This SOC log analysis demonstrates how simulated attacks against web server services can be detected using system and application logs. The project reflects real-world SOC analyst responsibilities including monitoring, detection, analysis, and response, making it relevant for blue-team and cybersecurity analyst roles.