Log Monitoring & Analysis Report

Objective

The objective of this task is to understand system log files, monitor authentication activities, detect suspicious or anomalous behavior, and analyze security-related events using Linux logs and Windows Event Viewer. This task helps in developing incident detection and basic SOC (Security Operations Center) skills.

Tools Used

- Linux System Logs
- Windows Event Viewer
- Terminal (Kali Linux / Ubuntu)
- (Optional – Conceptual) SIEM tools such as Splunk

Understanding Logs

Logs are automatically generated records that store information about system activities, user actions, authentication attempts, and errors. Logs play a crucial role in cybersecurity as they help in monitoring, detecting, and investigating security incidents.

Types of Logs Analyzed

- Authentication Logs
- System Logs
- Security Event Logs

Linux Log Analysis

Authentication Logs

In Linux systems, authentication-related activities are recorded in the following file:

/var/log/auth.log

This log contains information about:

- Successful login attempts
- Failed login attempts
- Invalid user access
- Privilege escalation (sudo usage)

Analysis Performed

The authentication log was examined to identify:

- Failed login attempts
- Repeated authentication failures
- Suspicious login behavior

Filtering was done to specifically view failed login attempts, which helps in identifying possible brute-force attacks.

Detection of Failed Login Attempts

Multiple failed login entries were observed in the authentication logs. These entries indicate unauthorized access attempts or incorrect password usage.

Indicators observed:

- Repeated failed login attempts
- Attempts using invalid usernames
- Authentication failures within short time intervals

Such behavior may indicate brute-force attacks or unauthorized access attempts.

Anomaly Detection

Anomalies are activities that deviate from normal system behavior. In this task, anomalies included:

- Multiple failed logins from the same source
- Login attempts during unusual hours
- Repeated authentication failures without successful login

Detecting anomalies helps in identifying potential security threats early.

Event Correlation

Event correlation involves connecting multiple log events to understand a complete incident. For example:

- Several failed login attempts followed by a successful login
- Same IP address attempting access using different usernames

Correlation helps security analysts confirm whether an incident is malicious or accidental.

Windows Event Viewer Analysis

Security Logs

Windows Event Viewer was used to analyze security events.

Path:

Windows Logs → Security

Important Event IDs

- **Event ID 4624** – Successful login
- **Event ID 4625** – Failed login attempt

The security logs showed failed login attempts which can indicate unauthorized access or incorrect credentials.

Introduction to SIEM (Conceptual)

SIEM (Security Information and Event Management) systems collect logs from multiple sources, analyze them in real time, and generate alerts for suspicious activities.

Key functions of SIEM:

- Log collection
- Event correlation
- Threat detection
- Alert generation
- Incident response support

Examples include Splunk, ELK Stack, and Q Radar.

Alert Example (Conceptual)

An alert can be generated when:

- More than 5 failed login attempts occur from the same IP address within 5 minutes.

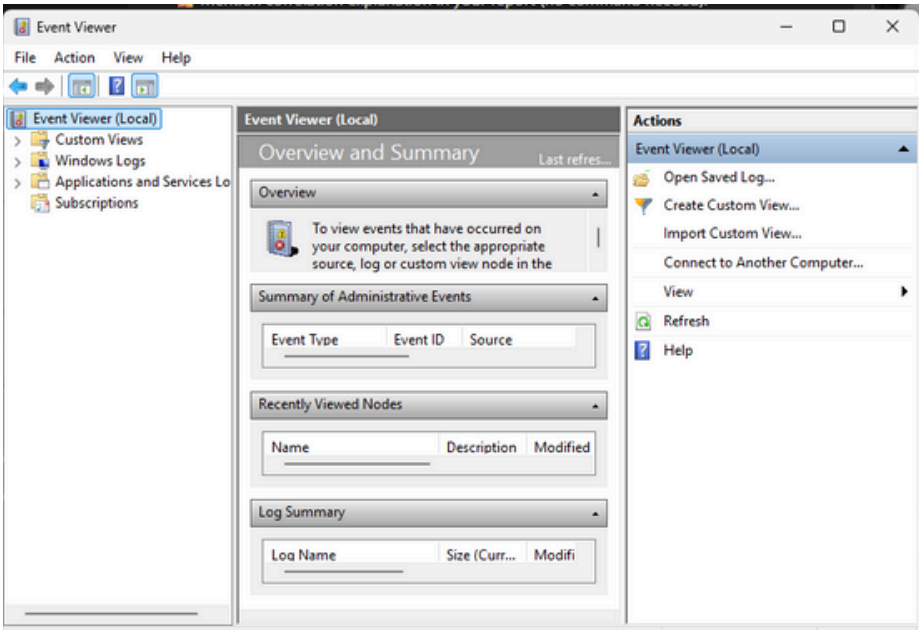
This helps security teams respond quickly to potential attacks.

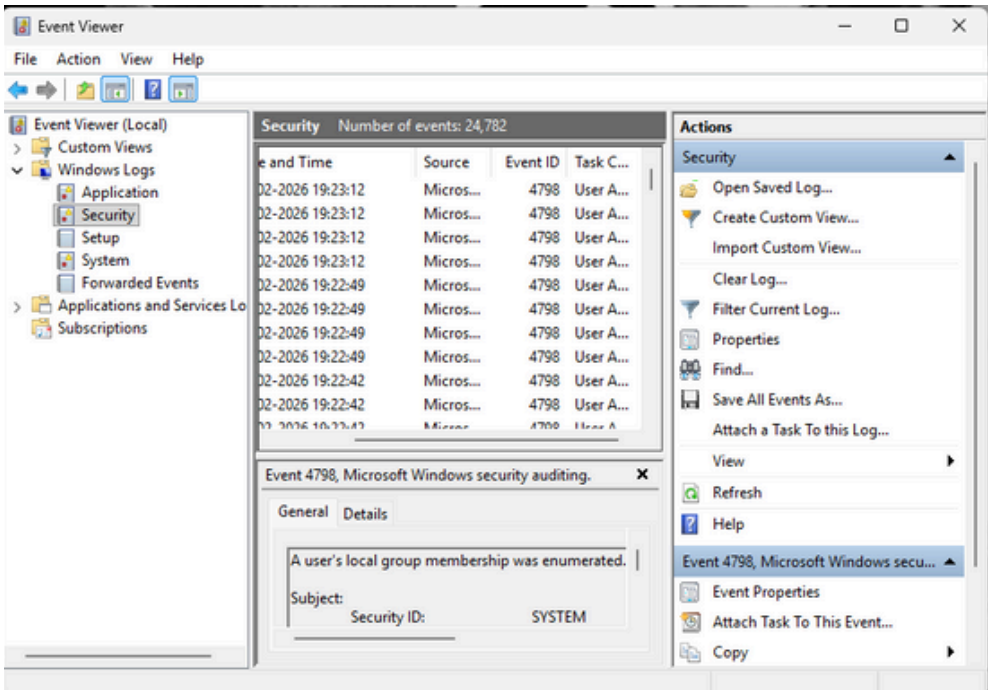
Findings

- Authentication logs recorded multiple failed login attempts.
- Repeated failures indicate possible brute-force activity.
- Log correlation helps identify real security incidents.
- Logs are critical for monitoring and forensic analysis.

```
File  Machine  View  Input  Devices  Help
1  2  3  4                                                    (genmon)XXX  8:52
kali@kali: ~
Session  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ sudo cat /var/log/auth.log

[sudo] password for kali:
2026-02-06T08:25:02.034359-05:00 kali CRON[2495]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2026-02-06T08:25:02.045508-05:00 kali CRON[2495]: pam_unix(cron:session): session closed for user root
2026-02-06T08:35:01.111083-05:00 kali CRON[2702]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2026-02-06T08:35:01.132796-05:00 kali CRON[2702]: pam_unix(cron:session): session closed for user root
2026-02-06T08:39:01.179373-05:00 kali CRON[2777]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2026-02-06T08:39:01.190701-05:00 kali CRON[2777]: pam_unix(cron:session): session closed for user root
2026-02-06T08:45:01.223669-05:00 kali CRON[2875]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2026-02-06T08:45:01.234952-05:00 kali CRON[2875]: pam_unix(cron:session): session closed for user root
2026-02-06T08:55:01.301958-05:00 kali CRON[2941]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2026-02-06T08:55:01.328522-05:00 kali CRON[2941]: pam_unix(cron:session): session closed for user root
2026-02-06T09:03:47.679690-05:00 kali xfce4-screensaver-dialog: gkr-pam: unlocked login keyring
2026-02-06T09:03:47.684953-05:00 kali xfce4-screensaver-dialog: pam_unix(xfce4-screensaver:account): setuid failed: Operation not permitted
2026-02-06T09:04:03.939918-05:00 kali sudo:     kali : TTY=pts/0 ; PWD=/home/kali ; USER=root ; COMMAND=/usr/bin/apt update
2026-02-06T09:04:03.941308-05:00 kali sudo: pam_unix(sudo:session): session opened for user root(uid=0) by kali(uid=1000)
2026-02-06T09:05:01.361178-05:00 kali CRON[3161]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2026-02-06T09:05:01.366343-05:00 kali CRON[3161]: pam_unix(cron:session): session closed for user root
2026-02-06T09:09:01.383930-05:00 kali CRON[3186]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2026-02-06T09:09:01.390501-05:00 kali CRON[3186]: pam_unix(cron:session): session closed for user root
2026-02-06T09:15:01.417328-05:00 kali CRON[3276]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2026-02-06T09:15:01.421072-05:00 kali CRON[3276]: pam_unix(cron:session): session closed for user root
2026-02-06T09:17:01.432199-05:00 kali CRON[3292]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2026-02-06T09:17:01.442024-05:00 kali CRON[3292]: pam_unix(cron:session): session closed for user root
2026-02-06T09:25:01.463731-05:00 kali CRON[3348]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2026-02-06T09:25:01.487875-05:00 kali CRON[3348]: pam_unix(cron:session): session closed for user root
2026-02-06T09:35:01.519569-05:00 kali CRON[3397]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2026-02-06T09:35:01.525504-05:00 kali CRON[3397]: pam_unix(cron:session): session closed for user root
2026-02-06T09:39:01.546367-05:00 kali CRON[3423]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2026-02-06T09:39:01.555821-05:00 kali CRON[3423]: pam_unix(cron:session): session closed for user root
2026-02-06T09:43:35.077035-05:00 kali xfce4-screensaver-dialog: gkr-pam: unlocked login keyring
```

```
1  2  3  4                                                    (genmon)XXX  8:53
kali@kali: ~
Session  Actions  Edit  View  Help
2026-02-09T08:50:56.179683-05:00 kali polkitd[593]: Error opening rules directory: Error opening directory "/usr/local/share/polkit-1/rules.d": No such file or direct
ory (g-file-error-quark, 4)
2026-02-09T08:50:56.179695-05:00 kali polkitd[593]: Loading rules from directory /usr/share/polkit-1/rules.d
2026-02-09T08:50:56.235425-05:00 kali polkitd[593]: Finished loading, compiling and executing 8 rules
2026-02-09T08:50:56.243497-05:00 kali polkitd[593]: Acquired the name org.freedesktop.PolicyKit1 on the system bus
2026-02-09T08:51:02.119210-05:00 kali lightdm: pam_unix(lightdm-greeter:session): session opened for user lightdm(uid=112) by (uid=0)
2026-02-09T08:51:02.160220-05:00 kali systemd-logind[595]: New session 'c1' of user 'lightdm' with class 'greeter' and type 'x11'.
2026-02-09T08:51:02.254839-05:00 kali (systemd): pam_unix(systemd-user:session): session opened for user lightdm(uid=112) by lightdm(uid=0)
2026-02-09T08:51:02.256318-05:00 kali systemd-logind[595]: New session '1' of user 'lightdm' with class 'manager-early' and type 'unspecified'.
2026-02-09T08:51:02.870104-05:00 kali lightdm: pam_unix(lightdm-greeter:session): session opened for user lightdm(uid=112) by (uid=0)
2026-02-09T08:51:20.429430-05:00 kali lightdm: gkr-pam: unable to locate daemon control file
2026-02-09T08:51:20.430611-05:00 kali lightdm: gkr-pam: stashed password to try later in open session
2026-02-09T08:51:20.482873-05:00 kali lightdm: pam_unix(lightdm-greeter:session): session closed for user lightdm
2026-02-09T08:51:20.483444-05:00 kali lightdm: pam_unix(lightdm-greeter:session): session closed for user lightdm
2026-02-09T08:51:20.498857-05:00 kali systemd-logind[595]: Removed session c1.
2026-02-09T08:51:20.502686-05:00 kali lightdm: pam_unix(lightdm:session): session opened for user kali(uid=1000) by kali(uid=0)
2026-02-09T08:51:20.530771-05:00 kali systemd-logind[595]: New session '2' of user 'kali' with class 'user' and type 'x11'.
2026-02-09T08:51:20.813220-05:00 kali (systemd): pam_unix(systemd-user:session): session opened for user kali(uid=1000) by kali(uid=0)
2026-02-09T08:51:20.815063-05:00 kali systemd-logind[595]: New session '3' of user 'kali' with class 'manager' and type 'unspecified'.
2026-02-09T08:51:21.088519-05:00 kali lightdm: gkr-pam: unlocked login keyring
2026-02-09T08:51:23.899296-05:00 kali polkitd[593]: Registered Authentication Agent for unix-session:2 (system bus name :1.47 [/usr/libexec/polkit-mate-authentication
-agent-1], object path /org/mate/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8)
2026-02-09T08:51:30.884571-05:00 kali systemd-logind[595]: Removed session 1.
2026-02-09T08:51:30.885626-05:00 kali (sd-pam): pam_unix(systemd-user:session): session closed for user lightdm
2026-02-09T08:51:52.196736-05:00 kali sudo:     kali : TTY=pts/0 ; PWD=/home/kali ; USER=root ; COMMAND=/usr/bin/cat /var/log/auth.log
2026-02-09T08:51:52.213340-05:00 kali sudo: pam_unix(sudo:session): session opened for user root(uid=0) by kali(uid=1000)

┌──(kali㉿kali)-[~]
└─$ sudo grep "Failed password" /var/log/auth.log

grep: /var/log/auth.log: binary file matches
```





Conclusion

This task provided hands-on experience in analyzing system logs, detecting suspicious activities, and understanding the importance of log monitoring in cybersecurity. It helped develop foundational skills required for SOC operations and incident detection.