NAME: Kadiyala Sri Pavan

UNIVERSITY: Aditya University

EMAIL: pavancc1478@gmail.com

Task-12

Log Monitoring & Analysis

Objective:

Log Monitoring and Analysis is the process of collecting, reviewing, and analyzing log data generated by operating systems, applications, and network devices to identify security incidents, system issues, and suspicious activities. Logs act as digital evidence of everything happening inside a system.

1.Understand log types:

1. Linux Logs

- Authentication Logs – Record login attempts and sudo usage.
- System Logs – Record system messages and services.
- Kernel Logs – Record kernel-level events.

2. Windows Logs

- Application Logs – Application-related events.
- Security Logs – Login, logout, and security events.
- System Logs – Operating system events.

2.Analyze authentication logs.

Authentication logs store information about successful and failed login attempts.

By analyzing these logs, we can detect unauthorized access attempts and account misuse.

Examples:

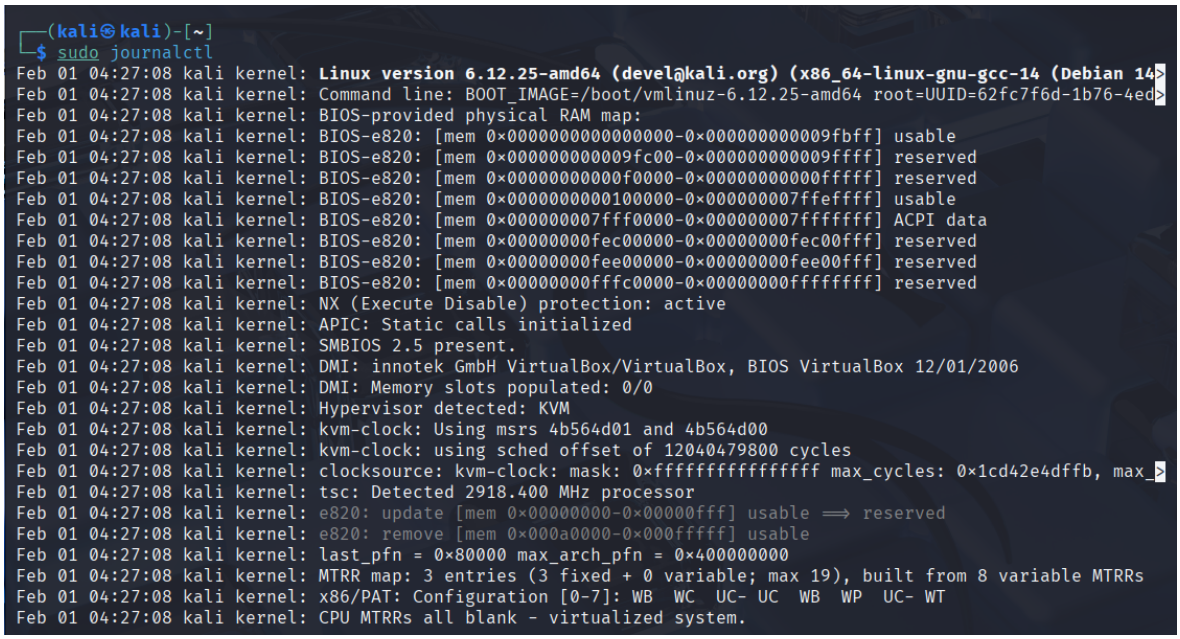
- Successful login
- Failed login
- Privilege escalation (sudo)

2.Analyze authentication logs.

STEP 1: Open Authentication Logs

Since Kali uses journal:

sudo journalctl



Scroll and observe.

Press **Q** to exit.

STEP 2: Search for Authentication Keywords

sudo journalctl | grep "password"

```
┌──(kali㉿kali)-[~]
└─$ sudo journalctl | grep "password"
Feb 01 04:27:08 kali systemd[1]: Started systemd-ask-password-wall.path - Forward Password Requests to Wall Di
rectory Watch.
Feb 01 04:27:08 kali systemd[1]: systemd-ask-password-console.path - Dispatch Password Requests to Console Dir
ectory Watch was skipped because of an unmet condition check (ConditionPathExists=!/run/plymouth/pid).
Feb 01 04:27:08 kali systemd[1]: Started systemd-ask-password-plymouth.path - Forward Password Requests to Ply
mouth Directory Watch.
Feb 01 04:27:59 kali lightdm[1025]: gkr-pam: stashed password to try later in open session
Feb 01 05:12:56 kali gnome-keyring-daemon[1064]: couldn't initialize slot with master password: The password o
r PIN is incorrect
Feb 01 05:12:56 kali gnome-keyring-d[1064]: couldn't initialize slot with master password: The password or PIN
 is incorrect
Feb 01 06:31:24 kali unix_chkpwd[54389]: password check failed for user (kali)
Feb 01 06:31:24 kali xfce4-screensaver-dialog[54313]: pam_winbind(xfce4-screensaver:auth): getting password (0
x00000388)
Feb 01 06:31:24 kali xfce4-screensaver-dialog[54313]: pam_winbind(xfce4-screensaver:auth): pam_get_item return
ed a password
Feb 01 06:31:30 kali gnome-keyring-daemon[1064]: couldn't initialize slot with master password: The password o
r PIN is incorrect
Feb 01 06:31:30 kali gnome-keyring-d[1064]: couldn't initialize slot with master password: The password or PIN
 is incorrect
Feb 01 06:31:40 kali systemd[1]: systemd-ask-password-plymouth.path: Deactivated successfully.
Feb 01 06:31:40 kali systemd[1]: Stopped systemd-ask-password-plymouth.path - Forward Password Requests to Ply
mouth Directory Watch.
Feb 01 06:31:40 kali systemd[1]: systemd-ask-password-wall.path: Deactivated successfully.
Feb 01 06:31:40 kali systemd[1]: Stopped systemd-ask-password-wall.path - Forward Password Requests to Wall Di
rectory Watch.
Feb 03 00:15:17 kali systemd[1]: Started systemd-ask-password-wall.path - Forward Password Requests to Wall Di
```

You may see lines like:

“password check failed for user kali”

This is authentication log.

3.Identify failed logins.

Finding records where login/password was incorrect.

STEP 1: Run This Command

sudo journalctl | grep "password check failed"

```
kali@kali: ~
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ sudo journalctl | grep "failed"

Feb 01 04:28:01 kali colord[1323]: failed to get edid data: EDID length is too small
Feb 01 04:28:01 kali dbus-daemon[790]: [system] Activation via systemd failed for unit 'dbus-org.freedesktop.A
vahi.service': Unit dbus-org.freedesktop.Avahi.service not found.
Feb 01 04:28:01 kali dbus-daemon[790]: [system] Activation via systemd failed for unit 'dbus-org.freedesktop.A
vahi.service': Unit dbus-org.freedesktop.Avahi.service not found.
Feb 01 04:28:02 kali dbus-daemon[790]: [system] Activation via systemd failed for unit 'dbus-org.bluez.service
': Unit dbus-org.bluez.service not found.
Feb 01 04:28:03 kali dbus-daemon[1058]: [session uid=1000 pid=1058 pidfd=5] Activation via systemd failed for
unit 'evolution-source-registry.service': Unit evolution-source-registry.service not found.
Feb 01 04:28:03 kali dbus-daemon[1058]: [session uid=1000 pid=1058 pidfd=5] Activation via systemd failed for
unit 'evolution-source-registry.service': Unit evolution-source-registry.service not found.
Feb 01 05:12:56 kali xfce4-screensaver-dialog[23378]: pam_unix(xfce4-screensaver:account): setuid failed: Oper
ation not permitted
Feb 01 06:31:24 kali unix_chkpwd[54389]: password check failed for user (kali)
Feb 01 06:31:24 kali xfce4-screensaver-dialog[54313]: pam_winbind(xfce4-screensaver:auth): request wbcLogonUse
r failed: WBC_ERR_WINBIND_NOT_AVAILABLE, PAM error: PAM_AUTHINFO_UNAVAIL (9)!
Feb 01 06:31:30 kali xfce4-screensaver-dialog[54449]: pam_unix(xfce4-screensaver:account): setuid failed: Oper
ation not permitted
Feb 01 06:31:39 kali dbus-daemon[790]: [system] Activation via systemd failed for unit 'dbus-org.freedesktop.n
m-dispatcher.service': Refusing activation, D-Bus is shutting down.
Feb 03 00:15:31 kali colord[1288]: failed to get edid data: EDID length is too small
Feb 03 00:15:32 kali dbus-daemon[508]: [system] Activation via systemd failed for unit 'dbus-org.freedesktop.A
vahi.service': Unit dbus-org.freedesktop.Avahi.service not found.
Feb 03 00:15:32 kali dbus-daemon[508]: [system] Activation via systemd failed for unit 'dbus-org.freedesktop.A
vahi.service': Unit dbus-org.freedesktop.Avahi.service not found.
Feb 03 00:15:33 kali dbus-daemon[508]: [system] Activation via systemd failed for unit 'dbus-org.bluez.service
```

If you see:

“password check failed for user kali”

Means wrong password attempt.

STEP 2: Count Failed Logins

sudo journalctl | grep "password check failed" | wc -l

```
┌──(kali㉿kali)-[~]
└─$ sudo journalctl | grep "password check failed" | wc -l
3
```

Meaning: 3 failed login attempts.

4.Detect anomalies.

Finding **unusual or abnormal login behavior** in logs.

STEP 1: Check Login Times

Last

```
┌──(kali㉿kali)-[~]
└─$ last

kali     tty7         :0               Tue Feb  3 09:10 - still logged in
lightdm  tty7         :0               Tue Feb  3 09:09 - 09:10  (00:00)
kali     tty7         :0               Tue Feb  3 00:15 - 01:19  (01:04)
lightdm  tty7         :0               Tue Feb  3 00:15 - 00:15  (00:00)
kali     tty7         :0               Sun Feb  1 04:27 - 06:31  (02:03)
lightdm  tty7         :0               Sun Feb  1 04:27 - 04:27  (00:00)
postgres                               Thu May 29 15:22 - 15:22  (00:00)
```

It’s normal login there is no suspicious logins

STEP 2: Check Repeated Failed Attempts

sudo journalctl | grep "password check failed"

```
┌──(kali㉿kali)-[~]
└─$ sudo journalctl | grep "password check failed"

[sudo] password for kali:
Feb 01 06:31:24 kali unix_chkpwd[54389]: password check failed for user (kali)
Feb 03 09:10:08 kali unix_chkpwd[854]: password check failed for user (kali)
Feb 03 09:10:14 kali unix_chkpwd[857]: password check failed for user (kali)
```

5.Learn SIEM basics.

1. What SIEM Is

SIEM = Security Information and Event Management
It's a system that **collects, analyzes, and stores security logs** from many sources.

2. Why SIEM Is Used

- Detect security threats
- Monitor suspicious activity
- Investigate incidents
- Meet compliance requirements

3. Data Sources

SIEM collects logs from:

- Servers (Windows, Linux)
- Firewalls & routers
- IDS/IPS
- Applications
- Databases
- Cloud services

4. Log Collection

- Logs are sent to SIEM using agents or protocols (Syslog, API)
- SIEM normalizes logs into a common format

5. Correlation

SIEM **connects events together**
Example:

- Multiple failed logins
- Followed by a successful login
  Possible brute-force attack

6. Alerts

- Rules trigger alerts when suspicious patterns appear
- Alerts are sent to SOC analysts

7. Dashboards

- Visual view of security status
- Shows threats, trends, and system health

8. Incident Investigation

- Analysts search logs
- Build timelines
- Identify attacker behavior

9. Compliance

SIEM helps with standards like:

- ISO 27001
- PCI-DSS
- HIPAA
- GDPR

10. Common SIEM Tools

- Splunk
- IBM QRadar
- Microsoft Sentinel
- ArcSight

- Elastic SIEM

6.Write alerts.

Alerts are automatic notifications triggered when specific conditions are met.

Example alerts:

Brute Force Alert

- 5 failed logins
- Same IP
- 5 minutes

Suspicious Admin Access

- User added to admin group
- Outside business hours

Impossible Travel

- Same user
- Two distant locations
- Short time gap

7. Conclusion

The analysis identified suspicious authentication activity that may indicate attempted or successful unauthorized access. Further monitoring and preventive controls are recommended.