Task 12: Log Monitoring & Analysis

1. Understand log types.

Log File	Purpose
/var/log/auth.log	Login attempts (MOST IMPORTANT)
/var/log/syslog	System activity
/var/log/kern.log	Kernel events
/var/log/dpkg.log	Package install history
/var/log/boot.log	Boot events

2. Analyze authentication logs

Authentication logs show **login success & failures**.

```
sudo journalctl -u ssh
```

```
sudo journalctl -u ssh | grep “invalid”
```

Look for keywords:

- Failed password
- Accepted password
- Invalid user

3. Identify failed logins.

What this means

- Multiple failures from same IP = **Brute force attempt**
- Random usernames = **Reconnaissance**

4. Detect anomalies

Anomalies were detected by analyzing SSH logs using journalctl. Invalid banner exchange messages, repeated malformed SSH requests, and authentication timeouts were identified as abnormal behavior. These anomalies indicate potential reconnaissance, scanning activity, or misconfigured clients attempting to access the system.

5. Correlate events.

Event correlation means **connecting multiple related log entries** to understand the **full attack or activity pattern**.

Example:

- Multiple failed attempts
- Followed by timeouts or malformed requests
  ➞ Indicates **probing or attack behavior**

Command: **sudo journalctl -u ssh | grep -E "failed|invalid|timeout"**

What this shows

- failed → authentication failures
- invalid → malformed or invalid SSH attempts
- timeout → incomplete authentication sessions

6. Learn SIEM basics.

SIEM (Security Information and Event Management) is a security solution that:

- Collects logs from multiple systems
- Analyzes and correlates events
- Detects security incidents
- Generates alerts and reports

In this task:

- SSH logs were analyzed manually using journalctl
- A SIEM tool would automate:
  - Failed login detection
  - Anomaly identification
  - Event correlation
  - Alert generation

Examples of SIEM Tools

- Splunk
- ELK Stack (Elasticsearch, Logstash, Kibana)
- Wazuh
- Graylog

SIEM Use Case Example

- Detect multiple failed SSH login attempts
- Identify malformed SSH connections
- Alert on suspicious IP addresses
- Correlate login failures with timeouts

7.Write alerts.

Writing alerts means defining **conditions** that trigger a warning when suspicious activity is detected.

Alerts help:

- Identify attacks early
- Notify security teams
- Reduce response time

From your SSH logs, we observed:

- Invalid SSH banner exchange attempts
- Authentication timeouts
- Repeated abnormal connections

These can be used to define alert rules.

Alert 1: SSH Scanning Detection

IF multiple "invalid banner exchange" events are detected

FROM the same IP within a short time

THEN raise SSH scanning alert

Alert 2: Authentication Timeout Alert

IF SSH connections timeout before authentication

THEN raise suspicious SSH activity alert

Alert 3: Brute Force Attempt Alert

IF failed login attempts > 5

FROM the same IP in 5 minutes

THEN raise brute-force alert

8. Document findings.

Observations

- SSH service was running and listening on port 22.
- Multiple SSH connection attempts with **invalid banner format** were detected.
- Authentication timeout events occurred before login completion.
- Repeated abnormal SSH requests were observed from the same IP addresses.
- One external IP attempted malformed SSH communication.

Security Impact

- Invalid banner exchange attempts indicate possible **SSH scanning or probing**.
- Timeout events may be caused by **automated scripts or misconfigured clients**.
- Repeated abnormal behavior suggests **reconnaissance activity**.
- No successful unauthorized access was detected.

Conclusion

- The system experienced **suspicious SSH activity**.
- Early-stage attack behavior was identified.
- Log monitoring helps detect threats before compromise.