Future Interns – Cybersecurity Internship

Task 2: Security Alert Monitoring and Incident Response

Submitted by: Sandhya B

Date: 25/11/2025

1. Introduction

This report covers the analysis I did for Task 2 of the internship.
Since we were asked to work with *simulated* alerts and *sample log files*, I created a small set of log files that represent common security events.

I reviewed these logs manually and noted down the unusual or suspicious activities. Based on the alerts I found, I prepared this report with incident details and recommendations.

2. Log Files Used

I worked with four types of logs:

1. **Authentication Log (auth_log.txt)** – shows login attempts.
2. **Firewall Log (firewall_log.txt)** – shows blocked IPs and suspicious activity.
3. **Web Access Log (web_access_log.txt)** – shows website access requests.
4. **Network Traffic Log (network_traffic.log)** – shows unusual network activity.

These logs helped me understand what kind of attacks could be happening.

3. How I Analyzed the Logs

I did the analysis manually.
I opened each log file and checked for patterns like:

- repeated failed login attempts
- unknown or foreign IP addresses
- strange URLs
- requests to restricted files
- large outgoing data transfers
- malware-related domains
- port scanning behaviour

I wrote down what looked suspicious and added those points in my alert summary.

4. Alerts Identified from the Logs

From the four logs, I found the following alerts:

1. Several failed SSH login attempts from the same IP.
2. Firewall blocked a connection to a known malware domain.
3. A SQL injection attempt appeared in the web server logs.
4. Someone tried to access `/etc/passwd`, which is a sensitive file.
5. A large amount of data was sent out to an external IP.
6. Port scanning activity was detected.

All these point to possible attack attempts.

5. Incident Classification

Incident	Category	Severity
Repeated SSH login failures	Brute-force attack	High
Connection to malware domain	Malware / C2	Critical
SQL injection attempt	Application attack	High
Access to `/etc/passwd`	Privilege escalation attempt	High
200MB outbound data transfer	Data exfiltration	Critical
Port scanning activity	Reconnaissance	Medium

6. Brief Analysis of Each Incident

Brute-Force Login

There were many failed SSH login attempts from the same IP. This looks like someone trying different passwords.

Malware Domain

The firewall log showed a connection attempt to *malware.bad.com*. This means the system might be infected.

SQL Injection

The web log contained `' OR '1'='1`, which is a common SQL injection pattern.

Unauthorized Access

Someone tried to access `/etc/passwd`. This file should not be touched by normal users.

Data Exfiltration

A large amount of data (200MB) was sent to an external IP, which is not normal.

Port Scanning

Port scan activity usually means an attacker is checking open ports before attacking.

7. Recommended Actions

Here are the steps I would take:

- Block the attacker IPs.
- Change passwords and enable MFA on SSH.
- Fix the web vulnerabilities and validate inputs.
- Run a malware scan on the affected device.
- Check if any sensitive data was taken.
- Monitor outgoing network traffic.
- Enable stricter firewall and IDS/IPS rules.

8. Conclusion

By reviewing the logs, I was able to identify several suspicious events.
This task helped me understand how SOC teams detect attacks by analyzing logs and spotting patterns.
The alerts I found clearly show attempted brute-force, web attacks, malware communication, and data exfiltration.