SOC Analyst Report: Suspicious Login Investigation

Prepared By: Dasi Abhinay

📝 Project Overview

This project focuses on detecting and investigating suspicious login activity within a corporate network using **Windows Event Logs** and **Splunk**. The goal is to identify potential brute-force attacks or compromised accounts by analysing failed and successful login attempts.

1. Data Collection

🔍 Logs Used

- **Source**: Windows Event Logs (Security)
- **Log File Type**: .evtx (Exported from Event Viewer)
- **Event IDs Analyzed**:
    - **4624** → Successful logins
    - **4625** → Failed login attempts

📥 Log Extraction Process

1. **Opened Event Viewer** (eventvwr via Run).
2. **Filtered Security Logs** for Event IDs **4624** and **4625**.
3. **Saved Filtered Logs** as .evtx for analysis in Splunk.

2. Log Analysis with Splunk

🔎 Query 1: Checking for Failed Login Attempts (4625)

Query Used:

```
index=main sourcetype="WinEventLog:Security" EventCode=4625
| stats count by Account_Name, IpAddress
| sort -count
```

Findings:

- Total failed login attempts: 2
- Accounts affected: Only my account
- IP Addresses involved: None detected (local logins only)

📌 **Conclusion:** No brute-force attack detected as there were only **2 failed attempts**, which is within normal limits.

🔎 **Query 2: Checking for Successful Logins (4624)**

Query Used:

```
index=main sourcetype="WinEventLog:Security" EventCode=4624
| stats count by Account_Name, IpAddress
| sort -count
```

Findings:

- Total successful logins: 22
- Accounts involved: Only my username
- IP Addresses involved: None detected (local logins only)
- Logon Type Analysis:
    - No remote logins (Logon Type 10)
    - All logins were from the local machine (Logon Type 2)

📌 **Conclusion:** No unauthorized access detected. All logins were performed by the expected user.

3. Last Conclusion & Recommendations

📊 **Summary of Findings**

- No brute-force attack found (minimal number of unsuccessful login attempts).
- No external login attempts or unknown IP addresses.
- All logins were executed by the same user.
- Logon types show local logins, with no remote desktop access (RDP) involved.

📌 **What If We Catch a Brute-Force Attack?**

If there is a detected brute-force attack (multiple failed attempts from a single IP address), we ought to:

Block the attacking IP through the Windows Firewall:

```
netsh advfirewall firewall add rule name="Block Attacker" dir=in action=block remoteip=ATTACKER_IP
```

Enable account lockout policies:

- Prevents repeated failed attempts by locking the account after a number of failures.
- Track login attempts in real-time through a Splunk alert to alert security teams.

📌 What If We Discover a Suspicious Login?

If we discover logins from an unknown IP or an unexpected location, we should:

- Reset the user's password immediately.
- Enable Multi-Factor Authentication (MFA) to avoid unauthorized access.
- Verify if the account was utilized for privilege escalation or data access.
- Scan the system for malware if the attacker left a backdoor.

🛡️ Preventive Security Measures

Even though no suspicious activity was detected, proactive security measures must be applied:

Enable Account Lockout Policy (Prevents brute-force attempts).

Set Up Multi-Factor Authentication (MFA) (Increases security).

Enable Real-Time Login Alerts in Splunk (Identifies future unauthorized logins).

Daily Scanning of Security Logs to catch suspicious behaviour prior to an attack growing.