TASK 2 REPORT

Task Title: SIEM-Based Incident Monitoring and Analysis
Track Code: FUTURE_CS_02
Intern Name: Yandrapu Mahesh

Aim:

To monitor and analyze simulated security alerts using a SIEM (Splunk) to identify suspicious activities, classify incidents, and recommend mitigation strategies based on log analysis from simulated brute force and account compromise scenarios.

Tools Used:

- **SIEM Tool:** Splunk Free Trial
- **Environment:** Windows Event Logs (custom generated)
- **File:** brute_force_pattern_logs.txt

Procedure & Findings: A custom Windows log file containing simulated security events was uploaded into Splunk. Log analysis was conducted focusing on three main event types:

- **4625:** Failed login attempts
- **4624:** Successful login
- **4634:** Logoff event

Splunk queries were used to identify brute force patterns and track successful compromises following repeated failures. A critical incident was detected: multiple failed logins to the `administrator` account from a single IP, followed by a successful login from the same source — indicating a brute force success.

Incident Classification:

Type	Description	Severity
Brute Force Attack	Multiple failed login attempts from same IP	High
Account Compromise	Successful login after failed attempts (admin)	Critical
Recon Activity	Attempts on non-existent accounts like `guest`	Medium

---

Splunk Queries Used:

1. Search for Failed Logons:

```
index=* source="brute_force_pattern_logs.txt" EventCode=4625
```

>	5	7/2/25 10:58:14.000 AM	Date/Time: 2025-07-02 10:58:14 Event ID: 4625 Log Name: Security Account: administrator Failure Reason: Bad password Show all 6 lines host = Yandrapu_Mahesh source = brute_force_pattern_logs.txt sourcetype = logs
>	6	7/2/25 10:58:09.000 AM	Date/Time: 2025-07-02 10:58:09 Event ID: 4625 Log Name: Security Account: svc_account Failure Reason: Account locked out Show all 6 lines host = Yandrapu_Mahesh source = brute_force_pattern_logs.txt sourcetype = logs
>	7	7/2/25 10:58:05.000 AM	Date/Time: 2025-07-02 10:58:05 Event ID: 4625 Log Name: Security Account: admin Failure Reason: Unknown user name or bad password Show all 6 lines host = Yandrapu_Mahesh source = brute_force_pattern_logs.txt sourcetype = logs
>	8	7/2/25 10:58:03.000 AM	Date/Time: 2025-07-02 10:58:03 Event ID: 4625 Log Name: Security Account: guest Failure Reason: Account does not exist Show all 6 lines host = Yandrapu_Mahesh source = brute_force_pattern_logs.txt sourcetype = logs

2.Search for Successful Logons:

index=* source="brute_force_pattern_logs.txt" EventCode=4624

i		Time	Event
>	1	7/2/25 11:10:07.000 AM	Date/Time: 2025-07-02 11:10:07 Event ID: 4624 Log Name: Security Account: backup_admin Logon Type: 10 (RemoteInteractive) IP Address: 192.168.1.101 Collapse host = Yandrapu_Mahesh | source = brute_force_pattern_logs.txt | sourcetype = logs
>	2	7/2/25 10:58:25.000 AM	Date/Time: 2025-07-02 10:58:25 Event ID: 4624 Log Name: Security Account: administrator Logon Type: 3 (Network) IP Address: 192.168.1.100 Collapse host = Yandrapu_Mahesh | source = brute_force_pattern_logs.txt | sourcetype = logs

3. Failed Logons by Account:

```
index=* source="brute_force_pattern_logs.txt" EventCode=4625
| stats count by Account
| sort -count
```

4. IP Addresses with Multiple Failures:

```
index=* source="brute_force_pattern_logs.txt" EventCode=4625
| stats count by "IP Address", Account
| sort -count
```

5. Accounts with Failures and a Success:

```
(index=* source="brute_force_pattern_logs.txt") (EventCode=4624 OR EventCode=
4625)
| stats values(EventCode) as event_codes by Account, "IP Address"
| where mvcount(event_codes)=2 AND "4625" IN event_codes AND "4624" IN event_
codes
```

6. Events for Specific Account:

```
index=* source="brute_force_pattern_logs.txt" Account="administrator"
```

Security Recommendations:

- **Immediate:**
    - Block or monitor IPs `192.168.1.100`, `192.168.1.101`
    - Reset affected user passwords
    - Enforce MFA for admin-level users
- **Preventive:**
    - Implement account lockout policies
    - Enable CAPTCHA and login rate limiting
    - Use detection rules for excessive 4625 events
- **Review:**
    - Audit `administrator` logon patterns
    - Tweak Splunk alert logic for brute force detection
    - Educate users and SOC staff on recognizing these attacks

---

Learning Outcomes:

- Understood the structure and relevance of Windows Event Logs
- Learned to identify brute force and post-compromise patterns using Splunk
- Gained hands-on experience with SIEM search queries and alerting workflows

Ethical Note:
All activity was conducted in a controlled lab environment using simulated logs and ethical testing tools. No real systems were harmed.

Conclusion: This task successfully demonstrated how Splunk SIEM can be used to detect and classify brute force attacks and possible compromises. The report emphasizes the value of log correlation, pattern detection, and automated querying in real-world incident response.

Prepared by: Yandrapu Mahesh