Lab Report: Brute Force & Privileged Login Detection Using Elastic SIEM (Trial Version)

Internship Phase: SIEM Detection Use Case – Phase 1
Scenario1: Brute Force Login (T1110) followed by Successful Privileged Access (T1078)
Tools Used: **CrackMapExec, Windows 10, Kali Linux, Winlogbeat, Elastic Cloud (Trial)**

Lab Setup

Component	Configuration
Target Machine	Windows 10 (logs monitored via Winlogbeat)
Attacker Machine	Kali Linux
Attack Tool	CrackMapExec (SMB brute force)
SIEM	Elastic Cloud (Trial version)
Log Forwarder	Winlogbeat (installed on Windows 10)
Logs Monitored	Windows Security Logs (Event ID 4625 & 4624)

Attack Simulation

Brute Force via SMB (CrackMapExec)

crackmapexec smb 192.168.1.5 -u Machine1 -p indian-passwords.txt

- This generated multiple failed login attempts (Event ID 4625) from the Kali IP.
- Once the correct password was used, a successful login (Event ID 4624) was logged.

Log Collection (Winlogbeat)

- Winlogbeat configured on Windows 10 to ship logs to Elastic Cloud.
- Security event IDs shipped:
  - 4625 – Failed login attempts
  - 4624 – Successful logins

Detection Rules in Elastic SIEM (Trial Version)

Since Elastic Cloud Trial doesn't support rule correlation, I used two separate threshold rules:

Rule 1: Brute Force Attempt Detection

- Rule Name: Brute Force Detected – Multiple Failed Logins (T1110)
- Type: Custom threshold rule
- event.code: "4625"
- Threshold: ≥10 attempts from same source.ip within 5 minutes

Rule 2: Suspicious Successful Login

- Rule Name: Successful Login After Brute Force (T1078)
- Type: Custom threshold rule
- event.code: "4624"
- Timeframe: Within 5 minutes after the brute force attempts
- Note: This rule detects a login from the same IP, but correlation is done manually via Kibana or alert review.

Manual Correlation Method (Workaround)

Since advanced rule chaining isn't available in the trial:

- I used Kibana Timeline and Dashboards to visually correlate:
  - Alert from Rule 1 (4625 events)
  - Alert from Rule 2 (4624 from same IP shortly after)
- Matched on:
  - source.ip
  - Time proximity (within 5 minutes)
  - user.name and host.name

Email Alerts

- Configured email connector in Elastic.
- Alerts included context like IP, event time, and event code.

Sample Subjects:

- Brute Force Attempt Detected – 10 Failures
- Suspicious Successful Login After Brute

Visualizations

Created Kibana dashboards showing:

- Count of 4625 and 4624 events over time
- Filtered view by host, user, and source IP

Outcome Summary

Detection Component	Result
Brute Force Detection	Alert triggered for ≥10 failed logins
Successful Login Detection	Alert triggered for Event 4624
Correlation	No automatic correlation in trial – done manually
Visibility	Dashboards and timeline used
Alerting	Email alerts sent successfully

Conclusion

The lab successfully demonstrated the detection of a brute force login attempt and a subsequent suspicious successful login using Elastic SIEM (Trial). Despite the lack of rule chaining in the trial version, the use of separate threshold rules and manual timeline correlation provided visibility into this attack pattern.