SIEM Correlation Rules Development & Detection Report (ELK Stack)

Student Name: Suhas
Role: SOC / Blue Team Intern
SIEM Platform: ELK Stack (Elasticsearch, Logstash, Kibana)

1. Objective

The objective of this task is to develop and test custom SIEM correlation rules to detect credential stuffing, DNS tunnelling, and PowerShell exploitation attacks.

2. Tools Used

Elasticsearch, Logstash, Kibana, Winlogbeat, Filebeat, Authentication Logs, DNS Logs, PowerShell Logs.

3. Attack Techniques Covered

Credential Stuffing, DNS Tunnelling, PowerShell Exploitation.

4. Correlation Rule Analysis

Credential Stuffing: Detection of multiple failed login attempts from a single IP within a short time window.

DNS Tunnelling: Identification of abnormal DNS query lengths, frequency, and suspicious domain patterns.

PowerShell Exploitation: Detection of encoded or obfuscated PowerShell commands and suspicious execution behavior.

5. Testing & Validation

Simulated logs were used to test detection rules and alerts were triggered based on predefined thresholds.

6. MITRE ATT&CK; Mapping

T1110 – Credential Stuffing
T1071.004 – DNS Tunnelling
T1059.001 – PowerShell Exploitation

7. Conclusion

This task enhanced hands-on experience in SIEM rule creation and real-world attack detection using the ELK Stack.

Submission Statement

This report is submitted as part of my cybersecurity internship learning activities.