□ **Incident Response Report**

Internship: Cybersecurity Content Specialist – Task 2
Tool Used: Splunk Enterprise (Free Edition)
Analyst: Mohit Ojha
CIN ID: FIT/MAY25/CS1542
Date: 20 Oct 2025

□ 1. Objective

To analyze provided log samples in Splunk, detect potential malicious activity, and generate a summary report with actionable security recommendations.

□ 2. Methodology

1. Installed Splunk Enterprise on Windows.
2. Uploaded the sample log file shared in the internship document.
3. Indexed data under the default main index and verified field extractions (source, host, sourcetype).
4. Executed search queries to detect suspicious events:
5. index=main (error OR fail OR attack OR malware OR suspicious)
6. | stats count by source, host, user, dest_ip, action
7. Built visual dashboards showing event frequency and source IP activity.
8. Reviewed results for repeated authentication failures, anomalous IP access, and malware indicators.

□ 3. Findings / Incident Summary

Incident Type	Description	Evidence (Fields)	Severity	Action Taken
Brute-Force Login Attempt	Multiple failed logins followed by a success within seconds from the same IP	src_ip=192.168.10.45, user=admin	High	Blocked source IP, password reset enforced
Malware Execution	Detected command line process execution with suspicious hash	process=cmd.exe /c powershell …	High	Quarantined host and flagged for forensic analysis

Incident Type	Description	Evidence (Fields)	Severity	Action Taken
Network Scanning Activity	Sequential port probes from external IP on multiple hosts	src_ip=203.0.113.77	Medium	Added to firewall deny list
Failed Authentication Attempts	Several unauthorized logins from foreign locations	action=failed_login	Medium	Triggered account lockout policy

---

□ 4. Impact Assessment

- **Affected Hosts:** 2 workstations within test network
- **Compromised Accounts:** None confirmed (but brute-force attempt detected)
- **Data Exfiltration:** No evidence found
- **Overall Risk Level:** ⚠ Medium to High

□ 5. Recommendations

1. Enable Multi-Factor Authentication (MFA) for all accounts.
2. Implement account lockout after 3–5 failed login attempts.
3. Update antivirus definitions and OS patches.
4. Block identified malicious IP addresses at firewall level.
5. Schedule continuous Splunk alerts for keywords: attack, malware, unauthorized.
6. Educate users on phishing and credential safety.

□ 6. Conclusion

Splunk successfully identified multiple malicious patterns within the provided log dataset.
The detected activities highlight the importance of log analysis in early threat detection and response.
By applying the recommended security controls, future attacks can be prevented and system resilience improved.

□ 7. Appendix (Optional)

- **Screenshots:** Splunk Dashboard, Search Queries, Visualization Graphs