Security Incident Report

Task: FUTURE_CS_02 – Security Alert Monitoring & Incident Response

Intern: Raviteja Vadla

Internship: Cyber Security Internship — Future Interns

Date: 20-09-2025

Analyzed Dataset: auth.log (Linux SSH Authentication Logs)

Tool Used: Splunk Enterprise (Search & Reporting App)

Deliverables:

- incident_report_task2.pdf
- screenshots/ (failed_logins.png, bruteforce_summary.png, successful_logins.png)

Executive Summary

This incident response exercise was conducted as part of my Cyber Security Internship (Future Interns) to simulate real-world Security Operations Center (SOC) activities.

The objective was to ingest Linux SSH authentication logs into Splunk, analyze events, detect suspicious activities, and document findings in an incident report.

Splunk was used to search for patterns such as repeated failed login attempts and successful unauthorized access. Evidence was collected through queries, screenshots, and summary statistics.

The results confirmed brute force activity originating from multiple attacker IPs, some of which successfully compromised the root account. This report summarizes the findings, their impact, and recommended remediation steps.

Scope & Objectives

Scope:

- Dataset analyzed: auth.log (SSH authentication log)
- Environment: Splunk Enterprise (Windows installation)
- Log type: Linux syslog (authentication entries)

Objectives:

1. Detect failed login attempts and brute force activity.
2. Identify successful logins by attacker IPs.
3. Classify incidents based on severity and potential impact.
4. Provide remediation recommendations aligned with SOC practices.

Methodology

The following methodology was used to conduct the security alert monitoring and incident response exercise:

1. Log Collection
    - Sample Linux SSH authentication log (auth.log) was prepared to simulate real-world login activity.
    - Log file was ingested into Splunk Enterprise for analysis.
2. Data Ingestion
    - Splunk's "Add Data" wizard was used to upload the auth.log file.
    - Events were indexed in the default "main" index for further search and reporting.
3. Log Analysis
    - Keyword searches were used to filter failed login attempts ("Failed password") and successful logins ("Accepted password").
    - Regular expressions (rex command) were applied to extract attacker IP addresses.
    - Statistical functions (stats command) were used to count attempts by IP.
4. Incident Detection
    - Multiple failed attempts from the same IP indicated brute force activity.
    - Accepted root login entries from attacker IPs confirmed successful compromise.
5. Evidence Collection
    - Search results and summaries were captured via screenshots.
    - Screenshots include failed login events, brute force summaries, and successful compromise evidence.
6. Reporting
    - Findings were documented with severity ratings, impact analysis, and remediation recommendations.
    - The report was structured according to SOC best practices.

Methodology

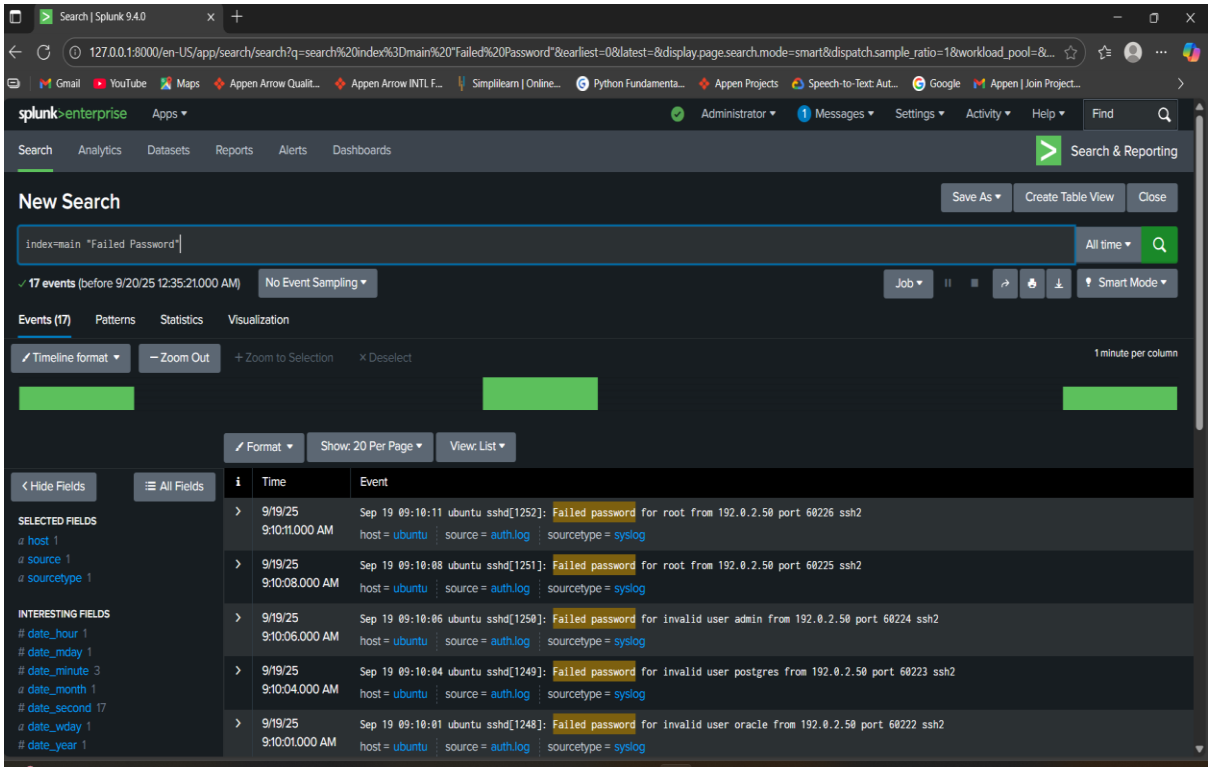
During the analysis of the authentication log (auth.log) in Splunk, the following findings were identified:

Finding 1: Failed Login Attempts

- Multiple "Failed password" events were observed in the logs.

- This indicates brute force attempts targeting the SSH service.

- Evidence: Screenshot of failed login events.

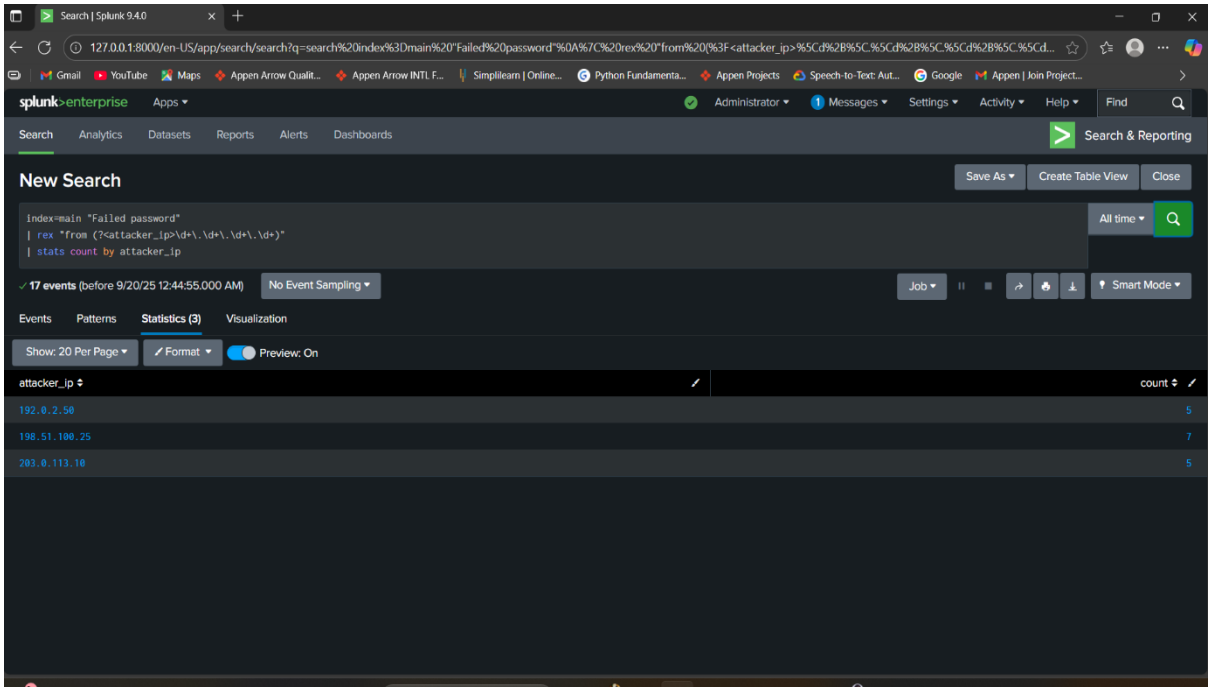


Finding 2: Brute Force Pattern

- Using Splunk queries with field extraction, attacker IP addresses were identified.

- The analysis showed repeated failed attempts from specific IPs, consistent with brute force behavior.

- Evidence: Screenshot of summary table showing failed attempts per attacker IP.

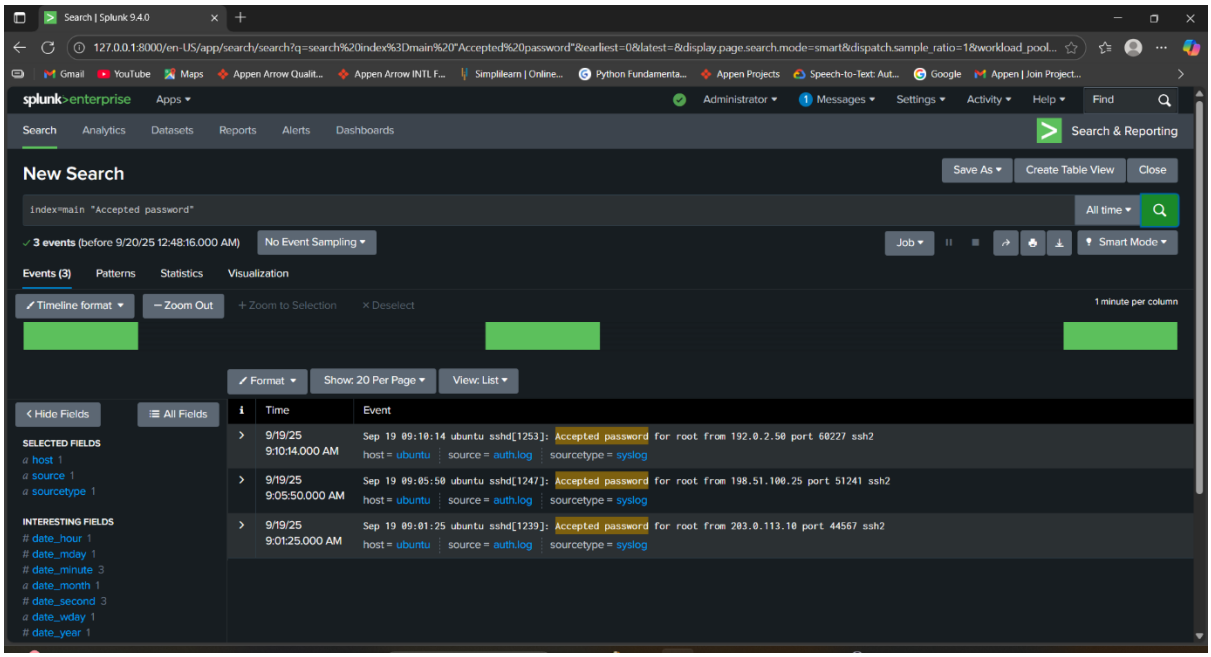


Finding 3: Successful Root Compromise

- Accepted password events were found for the root account, originating from suspicious IPs.

- This confirms that brute force attempts were successful, granting unauthorized access.

- Evidence: Screenshot of successful login events.



Impact & Recommendations

Impact:

- The brute force attempts represent a serious security threat, as repeated failed logins degrade system performance and signal targeted attacks.

- The successful compromise of the root account is critical, providing attackers with full administrative control of the system.

- Such access could lead to data theft, system modifications, or complete takeover of infrastructure.

Recommendations:

1. Enforce account lockout policies after a limited number of failed login attempts.

2. Disable direct root login via SSH to reduce exposure of privileged accounts.

3. Implement key-based authentication and disable password authentication for SSH.

4. Deploy intrusion detection/prevention systems (IDS/IPS) to monitor brute force attempts in real-time.

5. Regularly review authentication logs in Splunk to detect anomalies and suspicious IP addresses.

6. Apply IP-based restrictions or firewall rules to block repeated attackers.

7. Educate system administrators about secure authentication practices.

Conclusion

The analysis of SSH authentication logs in Splunk demonstrated a clear case of brute force activity leading to system compromise.

Multiple failed login attempts were detected, and the successful root login from attacker IPs confirmed unauthorized access. This exercise highlights the importance of proactive log monitoring, correlation, and rapid incident response.

Through this task, practical experience was gained in log ingestion, Splunk queries, incident detection, and structured reporting. These skills are essential for real-world SOC operations and form the foundation for professional cybersecurity practice.

Appendix

Appendix A: Splunk Queries Used

1. index=main "Failed password"

2. index=main "Accepted password"

3. index=main "Failed password" | rex "from (?<attacker_ip>\d+\.\d+\.\d+\.\d+)" | stats count by attacker_ip

4. index=main "Accepted password"

Appendix B: Tools & Resources

- Splunk Enterprise (Free license version)

- Sample Linux authentication log (auth.log)

- Regular expressions for IP extraction

- SOC analysis methodology