

Security Alert Monitoring Report – Splunk SIEM

(Internship Simulation Task)

Project Title:

Security Incident Detection and Analysis Using Splunk SIEM

Internship Program:

Future Interns – Cybersecurity Internship






Conducted by **Future Interns**

Intern Name:

Aman Patel

Cybersecurity & Ethical Hacking Enthusiast

Tools & Technologies Used:

-  Splunk Enterprise (Local Setup – Windows MSI)
-  Simulated Linux Logs (auth.log, syslog, network_connections.log)
-  Log Sources: Authentication, Network & System Events
-  Screenshots captured from Splunk Search & Reporting
-  Report compiled using Microsoft Word

Assessment Date:

29th June 2025

Test Environment:

- Host Machine: Windows 11
- Splunk Indexing Source: Manually uploaded .log files
- Simulated Environment: Local (Standalone Analysis)



Executive Summary

This report presents the findings from a simulated **Security Operations Center (SOC)** exercise conducted as part of the Future Interns Cybersecurity Internship Program. The objective was to demonstrate the intern's ability to detect, analyze, and classify potential security incidents using a **real-world SIEM tool – Splunk Enterprise**.

Three key log sources were ingested and examined:

- **Authentication Logs (auth.log)**
- **Network Connection Logs (network_connections.log)**
- **System Logs (syslog.log)**

After processing the data in Splunk, a set of **security alerts were identified**, each indicating potentially malicious behavior. These included **brute-force login attempts**, **unauthorized RDP access**, and **execution of suspicious system-level commands**. Each alert was triaged based on severity and analyzed for threat context, indicators, and recommended mitigation steps.

This simulation highlights the importance of proactive log monitoring, real-time alerting, and a structured incident response process within a modern SOC environment.

Scope of Assessment

The objective of this assessment was to simulate the responsibilities of a Security Operations Center (SOC) analyst by detecting and analyzing security alerts using **Splunk SIEM**. The focus was on ingesting log files, writing search queries, and identifying patterns of suspicious or malicious activity.

Log Sources Analyzed:

- **auth.log** – Authentication attempts (success & failure)
- **network_connections.log** – Connection attempts to internal/external IPs across various ports
- **syslog.log** – System-level command executions and user behavior

Platform & Tools Used:

- **Splunk Enterprise (Standalone Setup on Windows 11)**
- **Manual log ingestion via file upload**
- **Custom simulated log files generated for realistic SOC scenarios**

Assessment Goals:

- Identify and classify security alerts (e.g., brute-force attempts, unauthorized access)
- Correlate events using Splunk queries
- Evaluate potential risks and recommend mitigation steps
- Present findings in a structured report with severity levels



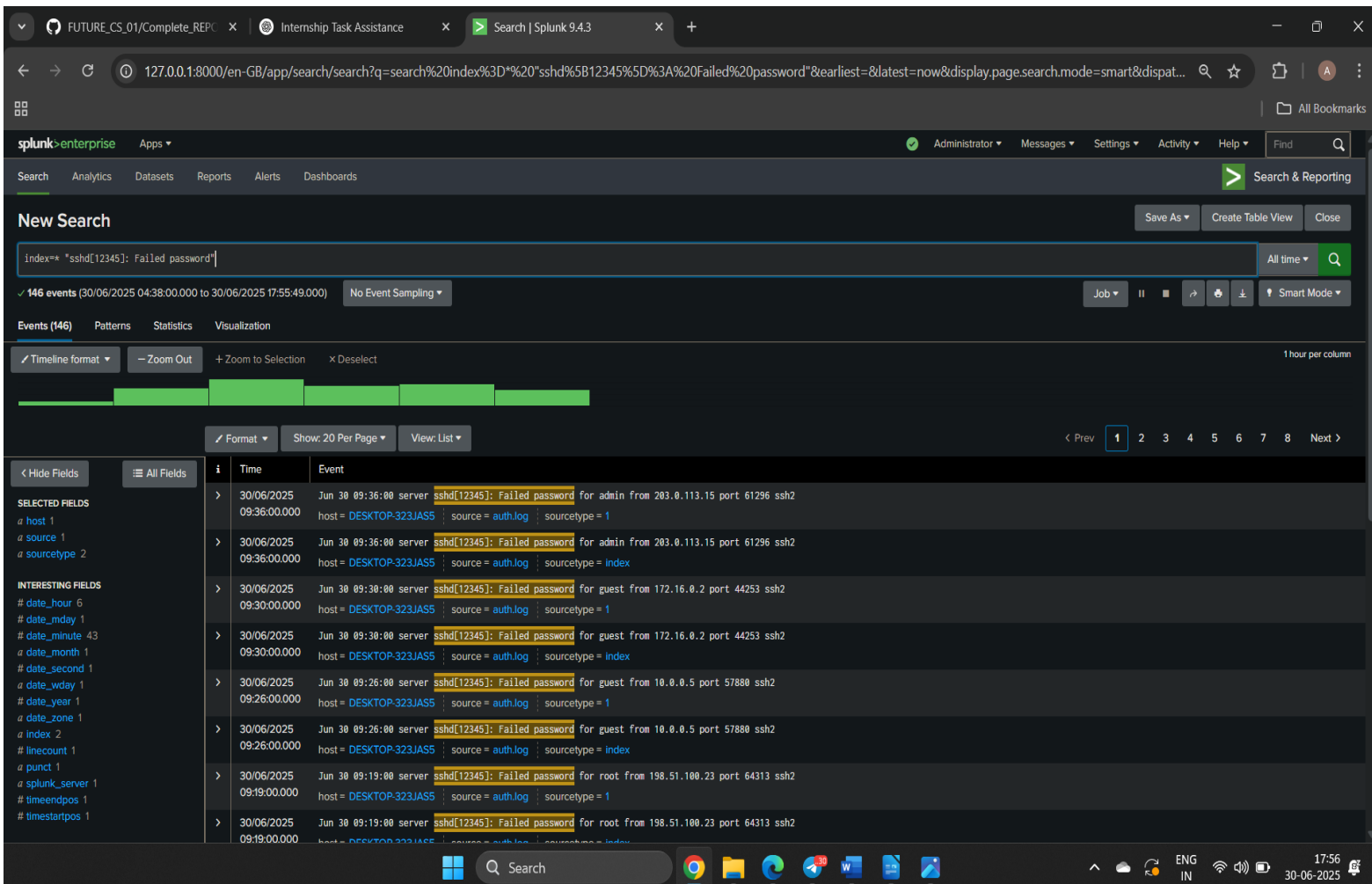
Incident Summary Table

Incident #	Type of Alert	Severity	Description	Recommended Action
1	SSH Brute-Force Attempt	High	Multiple failed login attempts detected from external IP 203.0.113.15	Block the IP, enable rate limiting (fail2ban), enforce 2FA
2	Blocked RDP Port Access	High	Unauthorized connection attempt to port 3389 (RDP) observed in firewall logs	Investigate source IP, verify firewall rules, disable unused services
3	Suspicious Command Execution	Medium	User <code>alice</code> executed <code>wget</code> , indicating possible unapproved file download	Restrict command access, enforce sudo policies, monitor user actions
4	Multiple Successful Logins	Medium	Repeated Accepted <code>password</code> entries from the same external IP to multiple users	Investigate for credential reuse or account compromise
5	Unusual Port Access Attempt	Medium	Firewall logs show access attempts to non-standard ports (e.g., 8080, 3389)	Monitor for port scanning behavior, enforce strict firewall policies

Detailed Findings

Incident 1: SSH Brute-Force Attempt

- **Screenshot Reference:** Screenshot 1
- **Splunk Query Used:**
`index=* "sshd[12345]: Failed password"`
- **Sample Log:**
`sshd[12345]: Failed password for john from 203.0.113.15 port 10587 ssh2`
- **Analysis:**
Multiple failed login attempts from a single external IP suggest a brute-force attack targeting SSH services.
- **Severity:** High
- **Recommended Action:**
Block the source IP at the firewall level, enable account lockout policies, and implement two-factor authentication.



New Search

index=* "sshd[12345]: Failed password"

146 events (30/06/2025 04:38:00.000 to 30/06/2025 17:55:49.000) No Event Sampling

Events (146) Patterns Statistics Visualization

Timeline format Zoom Out Zoom to Selection Deselect

Format Show: 20 Per Page View: List

i	Time	Event
>	30/06/2025 09:36:00.000	Jun 30 09:36:00 server sshd[12345]: Failed password for admin from 203.0.113.15 port 61296 ssh2 host = DESKTOP-323JAS5 source = auth.log sourcetype = 1
>	30/06/2025 09:36:00.000	Jun 30 09:36:00 server sshd[12345]: Failed password for admin from 203.0.113.15 port 61296 ssh2 host = DESKTOP-323JAS5 source = auth.log sourcetype = index
>	30/06/2025 09:30:00.000	Jun 30 09:30:00 server sshd[12345]: Failed password for guest from 172.16.0.2 port 44253 ssh2 host = DESKTOP-323JAS5 source = auth.log sourcetype = 1
>	30/06/2025 09:30:00.000	Jun 30 09:30:00 server sshd[12345]: Failed password for guest from 172.16.0.2 port 44253 ssh2 host = DESKTOP-323JAS5 source = auth.log sourcetype = index
>	30/06/2025 09:26:00.000	Jun 30 09:26:00 server sshd[12345]: Failed password for guest from 10.0.0.5 port 57880 ssh2 host = DESKTOP-323JAS5 source = auth.log sourcetype = 1
>	30/06/2025 09:26:00.000	Jun 30 09:26:00 server sshd[12345]: Failed password for guest from 10.0.0.5 port 57880 ssh2 host = DESKTOP-323JAS5 source = auth.log sourcetype = index
>	30/06/2025 09:19:00.000	Jun 30 09:19:00 server sshd[12345]: Failed password for root from 198.51.100.23 port 64313 ssh2 host = DESKTOP-323JAS5 source = auth.log sourcetype = 1
>	30/06/2025 09:19:00.000	Jun 30 09:19:00 server sshd[12345]: Failed password for root from 198.51.100.23 port 64313 ssh2 host = DESKTOP-323JAS5 source = auth.log sourcetype = index

Incident 2: Blocked RDP Port Access

- **Screenshot Reference:** Screenshot 2

- **Splunk Query Used:**

```
index=* "firewall: Connection" "BLOCKED"
```

- **Sample Log:**

```
firewall: Connection from 198.51.100.23 to 192.168.1.10 on port 3389 BLOCKED
```

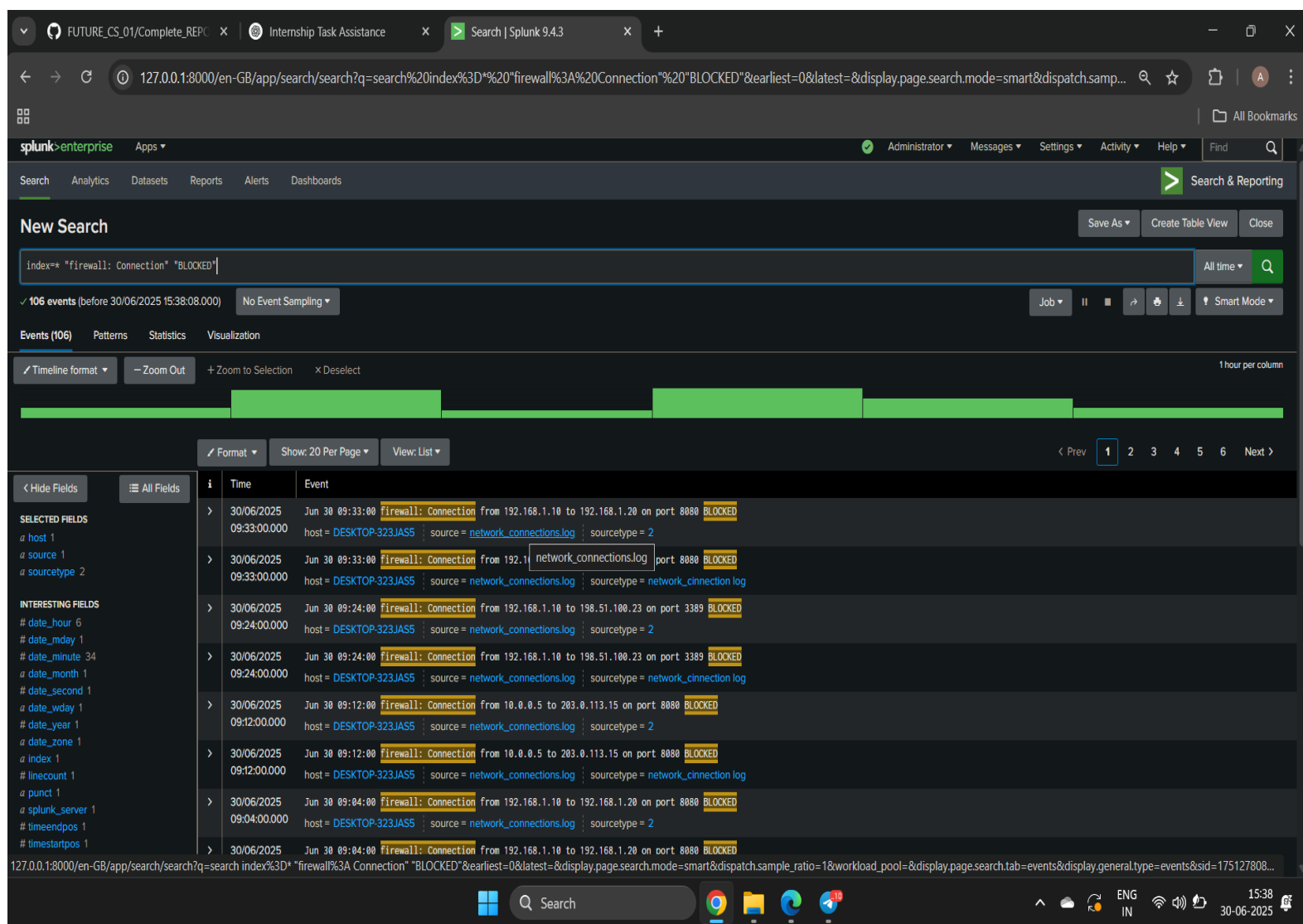
- **Analysis:**

An external source attempted to access the RDP port, which was rightfully blocked. This is often seen in port scanning or early-stage attacks.

- **Severity:** High

- **Recommended Action:**

Investigate the source IP, monitor for repeated attempts, and disable unnecessary remote access services.



The screenshot shows the Splunk Enterprise interface with a search query: `index=* "firewall: Connection" "BLOCKED"`. The search results show 106 events. The timeline view displays several green bars representing blocked connections. The table view shows the following events:

i	Time	Event
>	30/06/2025 09:33:00.000	firewall: Connection from 192.168.1.10 to 192.168.1.20 on port 8080 BLOCKED host = DESKTOP-323JAS5 ; source = network_connections.log ; sourcetype = 2
>	30/06/2025 09:33:00.000	firewall: Connection from 192.168.1.10 to 192.168.1.20 on port 8080 BLOCKED host = DESKTOP-323JAS5 ; source = network_connections.log ; sourcetype = network_connection log
>	30/06/2025 09:24:00.000	firewall: Connection from 192.168.1.10 to 198.51.100.23 on port 3389 BLOCKED host = DESKTOP-323JAS5 ; source = network_connections.log ; sourcetype = 2
>	30/06/2025 09:24:00.000	firewall: Connection from 192.168.1.10 to 198.51.100.23 on port 3389 BLOCKED host = DESKTOP-323JAS5 ; source = network_connections.log ; sourcetype = network_connection log
>	30/06/2025 09:12:00.000	firewall: Connection from 10.0.0.5 to 203.0.113.15 on port 8080 BLOCKED host = DESKTOP-323JAS5 ; source = network_connections.log ; sourcetype = 2
>	30/06/2025 09:12:00.000	firewall: Connection from 10.0.0.5 to 203.0.113.15 on port 8080 BLOCKED host = DESKTOP-323JAS5 ; source = network_connections.log ; sourcetype = network_connection log
>	30/06/2025 09:04:00.000	firewall: Connection from 192.168.1.10 to 192.168.1.20 on port 8080 BLOCKED host = DESKTOP-323JAS5 ; source = network_connections.log ; sourcetype = 2
>	30/06/2025 09:04:00.000	firewall: Connection from 192.168.1.10 to 192.168.1.20 on port 8080 BLOCKED host = DESKTOP-323JAS5 ; source = network_connections.log ; sourcetype = 2

⚠ Incident 3: Suspicious Command Execution

- **Screenshot Reference:** Screenshot 3

- **Splunk Query Used:**

```
index=* ("sudo" OR "wget" OR "curl")
```

- **Sample Log:**

```
server: User alice ran command: wget
```

- **Analysis:**

Use of `wget` by a non-administrator indicates a possible attempt to download external files — a common technique used to fetch payloads or tools.

- **Severity:** Medium

- **Recommended Action:**

Limit `wget/curl` access via `sudoers`, monitor command history, and review the destination URLs fetched.

The screenshot displays the Splunk Enterprise web interface. The search bar contains the query: `index=* ("sudo" OR "wget" OR "curl")`. The search results show 88 events. The timeline view at the top shows a series of green bars representing event density over time. The table view below shows the following events:

Time	Event
30/06/2025 09:31:00.000	Jun 30 09:31:00 server: User alice ran command: <code>sudo</code> host = DESKTOP-323JASS source = syslog.log sourcetype = 3
30/06/2025 09:31:00.000	Jun 30 09:31:00 server: User alice ran command: <code>sudo</code> host = DESKTOP-323JASS source = syslog.log sourcetype = systemlog
30/06/2025 09:11:00.000	Jun 30 09:11:00 server: User alice ran command: <code>curl</code> host = DESKTOP-323JASS source = syslog.log sourcetype = 3
30/06/2025 09:11:00.000	Jun 30 09:11:00 server: User alice ran command: <code>curl</code> host = DESKTOP-323JASS source = syslog.log sourcetype = systemlog
30/06/2025 09:10:00.000	Jun 30 09:10:00 server: User guest ran command: <code>sudo</code> host = DESKTOP-323JASS source = syslog.log sourcetype = 3
30/06/2025 09:10:00.000	Jun 30 09:10:00 server: User guest ran command: <code>sudo</code> host = DESKTOP-323JASS source = syslog.log sourcetype = systemlog
30/06/2025 09:00:00.000	Jun 30 09:00:00 server: User alice ran command: <code>wget</code> host = DESKTOP-323JASS source = syslog.log sourcetype = 3
30/06/2025 09:00:00.000	Jun 30 09:00:00 server: User alice ran command: <code>wget</code> host = DESKTOP-323JASS source = syslog.log sourcetype = systemlog

👁 Incident 4: Multiple Successful Logins from Same IP

- **Screenshot Reference:** Screenshot 4

- **Splunk Query Used:**

```
index=* "sshd[12345]: Accepted password"
```

- **Sample Log:**

```
sshd[12345]: Accepted password for david from 203.0.113.15  
port 11245 ssh2
```

- **Analysis:**

Repeated successful logins from a single external IP to multiple user accounts suggest either shared credentials or a compromised account scenario.

- **Severity:** Medium

- **Recommended Action:**

Check password hygiene of affected accounts, enable login alerts, and rotate credentials if needed.

The screenshot displays the Splunk Enterprise search interface. The search bar contains the query `index=* "sshd[12345]: Accepted password"`. Below the search bar, it indicates 54 events. The results are shown in a table with columns for Time and Event. The events show successful SSH logins for various users from different IP addresses on 30/06/2025.

i	Time	Event
>	30/06/2025 08:55:00.000	server sshd[12345]: Accepted password for alice from 192.168.1.20 port 27860 ssh2 host= DESKTOP-323JAS5 source= auth.log sourcetype= 1
>	30/06/2025 08:55:00.000	server sshd[12345]: Accepted password for alice from 192.168.1.20 port 27860 ssh2 host= DESKTOP-323JAS5 source= auth.log sourcetype= index
>	30/06/2025 08:47:00.000	server sshd[12345]: Accepted password for admin from 10.0.0.5 port 13582 ssh2 host= DESKTOP-323JAS5 source= auth.log sourcetype= 1
>	30/06/2025 08:47:00.000	server sshd[12345]: Accepted password for admin from 10.0.0.5 port 13582 ssh2 host= DESKTOP-323JAS5 source= auth.log sourcetype= index
>	30/06/2025 08:40:00.000	server sshd[12345]: Accepted password for john from 192.168.1.10 port 20473 ssh2 host= DESKTOP-323JAS5 source= auth.log sourcetype= 1
>	30/06/2025 08:40:00.000	server sshd[12345]: Accepted password for john from 192.168.1.10 port 20473 ssh2 host= DESKTOP-323JAS5 source= auth.log sourcetype= index
>	30/06/2025 08:30:00.000	server sshd[12345]: Accepted password for root from 10.0.0.5 port 42135 ssh2 host= DESKTOP-323JAS5 source= auth.log sourcetype= 1
>	30/06/2025 08:30:00.000	server sshd[12345]: Accepted password for root from 10.0.0.5 port 42135 ssh2 host= DESKTOP-323JAS5 source= auth.log sourcetype= index

Incident 5: Unusual Port Access Attempts

- **Screenshot Reference:** Screenshot 4

- **Splunk Query Used:**

index=* "BLOCKED" OR "Connection" AND port!=80 AND port!=443

- **Sample Log:**

firewall: Connection from 192.0.2.14 to 10.0.0.5 on port 8080
BLOCKED

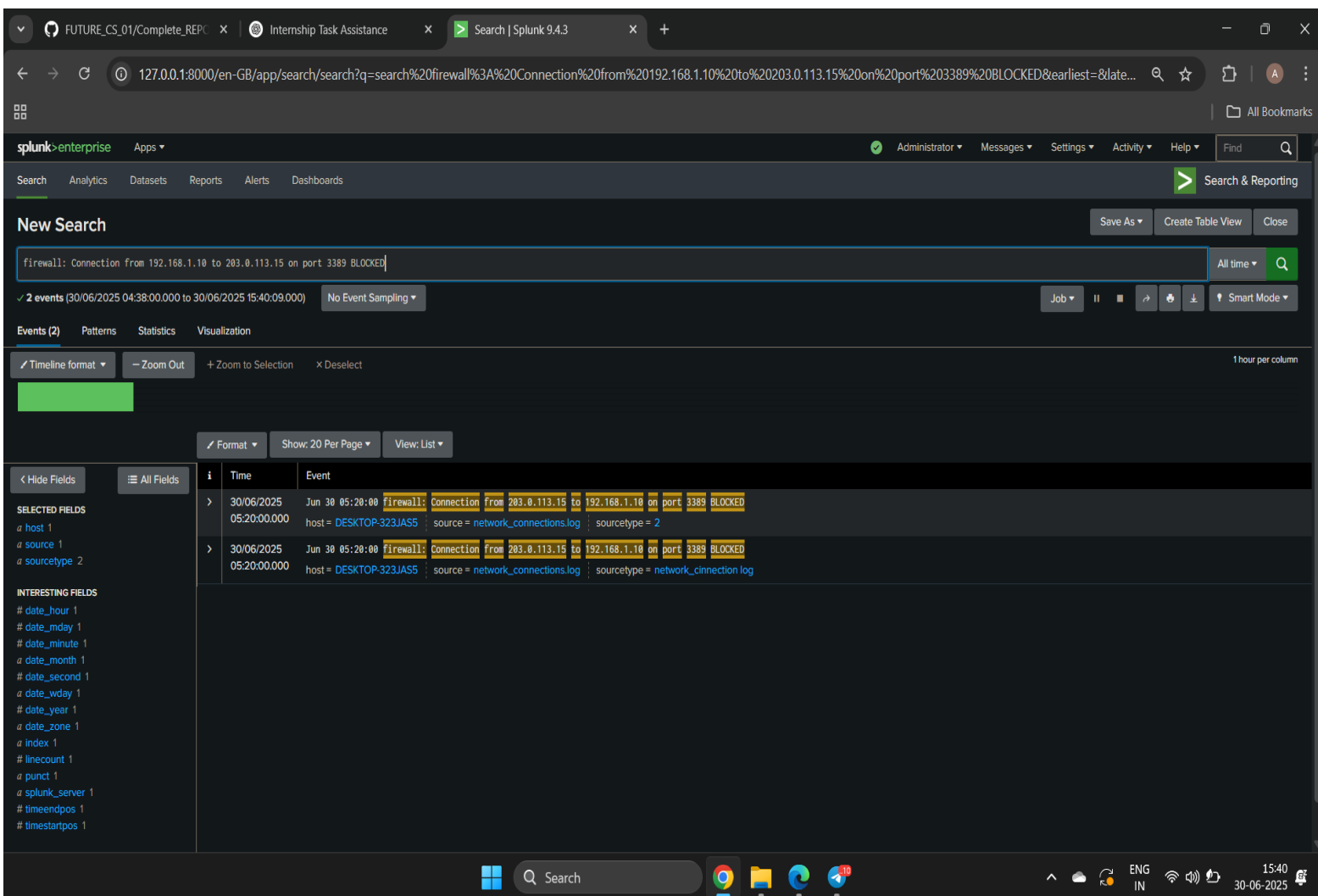
- **Analysis:**

Attempts to access uncommon or restricted ports (like 8080, 3389) may indicate port scanning or unauthorized service discovery.

- **Severity:** Medium

- **Recommended Action:**

Apply port-based alerting rules, enforce firewall best practices, and review open services regularly.



The screenshot displays the Splunk Enterprise interface with a search query: `firewall: Connection from 192.168.1.10 to 203.0.113.15 on port 3389 BLOCKED`. The search results show two events from June 30, 2025, at 05:20:00.000. The events are from the `network_connections.log` source and have a sourcetype of `network_connection log`. The events are highlighted in yellow, indicating they are blocked connections.

Selected Fields:

- `host` 1
- `source` 1
- `sourcetype` 2

Interesting Fields:

- `# date_hour` 1
- `# date_mday` 1
- `# date_minute` 1
- `# date_month` 1
- `# date_second` 1
- `# date_wday` 1
- `# date_year` 1
- `# date_zone` 1
- `# index` 1
- `# linecount` 1
- `# punct` 1
- `# splunk_server` 1
- `# timeendpos` 1
- `# timestartpos` 1

Time	Event
30/06/2025 05:20:00.000	Jun 30 05:20:00 firewall: Connection from 203.0.113.15 to 192.168.1.10 on port 3389 BLOCKED host = DESKTOP-323JASS source = network_connections.log sourcetype = 2
30/06/2025 05:20:00.000	Jun 30 05:20:00 firewall: Connection from 203.0.113.15 to 192.168.1.10 on port 3389 BLOCKED host = DESKTOP-323JASS source = network_connections.log sourcetype = network_connection log

Recommendations

Based on the analysis of the identified incidents, the following actions are recommended to strengthen system security and mitigate similar threats in the future:

1. Strengthen Authentication Controls

- Enforce **account lockout policies** after multiple failed login attempts
 - Enable **Two-Factor Authentication (2FA)** for SSH and critical accounts
 - Monitor for **successful logins from unknown IPs**
-

2. Harden Firewall and Network Configurations

- Block unnecessary ports (e.g., 8080, 3389) using strict **firewall rules**
 - Implement **IP whitelisting** for remote access services
 - Monitor for **unusual or blocked connection attempts**
-

3. Enforce Least Privilege and Command Restrictions

- Restrict use of commands like `wget`, `curl`, and `rm` to **admin roles only**
 - Implement **sudoers policy reviews** and **command logging**
 - Educate users on avoiding risky behavior on systems
-

4. Monitor and Alert on Suspicious Activity

- Configure **Splunk alerts** for:
 - Multiple failed login attempts
 - Logins from new geolocations
 - Use of dangerous system commands
 - Conduct regular **log reviews** and anomaly detection
-

5. Continuous Improvement

- Periodically review access controls and firewall rules
- Simulate incidents via tabletop exercises or red team testing
- Document and refine your **incident response playbook**



Conclusion

This assessment successfully simulated a real-world Security Operations Center (SOC) workflow by analyzing system and network logs using **Splunk SIEM**. The investigation led to the identification of **five distinct security alerts**, ranging from brute-force login attempts to suspicious command execution and unauthorized access attempts.

Through this exercise, valuable skills in **log ingestion, query building, threat detection**, and **incident response documentation** were demonstrated. The findings underscore the importance of proactive monitoring, strict access control, and structured response procedures in maintaining organizational cybersecurity.

This report not only fulfills the objectives of the internship task but also reflects readiness to operate in real-world SOC environments and contribute to professional security teams.