**Splunk SSH Log Analysis Report**

**Project Objective:**

This report documents the process and results of analyzing SSH log events using Splunk. The objective was to identify failed login attempts, successful SSH sessions, and detect suspicious activities based on given criteria.

**Task 1: Identify All Failed Access Attempts**

**Query:**

index="main" "Failed password"

| rex field=\_raw "Failed password for( invalid user)? (?<user>\w+) from (?<src\_ip>\d+\.\d+\.\d+\.\d+) port (?<port>\d+) ssh2"

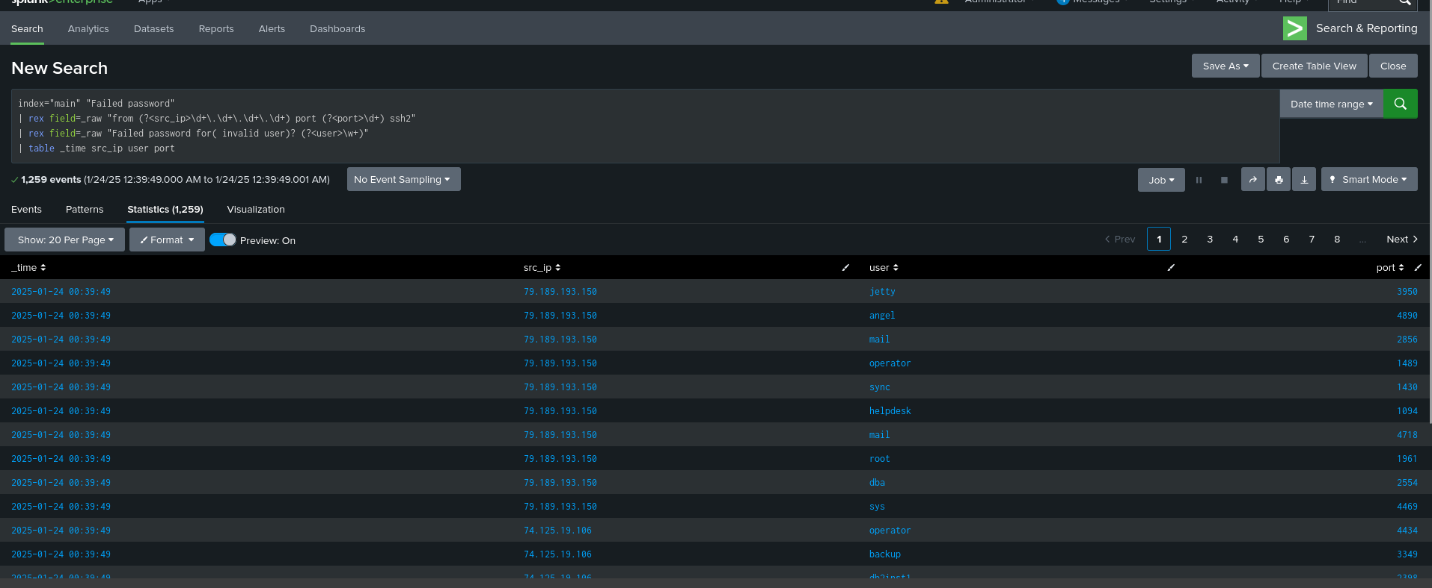
| table \_time src\_ip user port

**Explanation:**

* This query searches for all SSH failed login events using the keyword "Failed password."
* A regex (rex) extraction captures the username, source IP address, and port.
* The results are presented in a table format showing the timestamp, source IP, username, and port.

**Result:**

A total of **1259 failed login attempts** were detected. The output table lists details of each event, with a summary available in the attached screenshot.



**Task 2: Identify Successful SSH Sessions by User djohnson**

**Query:**

index="main" "session opened for user djohnson"

| rex field=\_raw "session opened for user (?<user>\w+).\*by \(uid=(?<uid>\d+)\)"

| table \_time user uid

**Explanation:**

* This query looks for successful SSH session openings by filtering for the string "session opened for user djohnson."
* Regex is used to extract the user and UID.
* The output table presents the timestamps and associated UIDs for each successful session.

**Result:**

**36 successful SSH sessions** for user djohnson were identified, with detailed logs shown in the result table.

A screenshot of a computer

Description automatically generated

**Task 3: Identify Failed Access Attempts from IP 86.212.199.60**

**Query:**

index="main" "Failed password" src\_ip="86.212.199.60"

| rex field=\_raw "Failed password for( invalid user)? (?<user>\w+) from (?<src\_ip>\d+\.\d+\.\d+\.\d+) port (?<port>\d+)"

| table \_time user port

**Explanation:**

* The query searches for failed login attempts specifically from the IP 86.212.199.60.
* Regex is used to extract the username and port associated with each failed attempt.

**Result:**

The IP 86.212.199.60 was responsible for **1259 failed login attempts**, indicating a brute-force attack.

A black and white text on a black background

Description automatically generated

**Task 4: Identify IP Addresses with More Than 5 Failed Attempts**

**Query:**

index="main" "Failed password"

| rex field=\_raw "from (?<src\_ip>\d+\.\d+\.\d+\.\d+)"

| stats count by src\_ip

| where count > 5

| table src\_ip count

**Explanation:**

* The query extracts the source IPs from failed login attempts using regex.
* Events are grouped by IP, and only IPs with more than 5 failed attempts are displayed.

**Result:**

A total of **71 IP addresses** were identified with more than 5 failed attempts. Among these, several IPs had high activity, such as **109.169.32.135 (29 attempts)** and **194.146.236.22 (30 attempts)**, indicating possible brute-force attack sources.

A screenshot of a computer

Description automatically generated

**Task 5: Search for "Internal Server Error" Events**

**Query:**

index="main" "Internal Server Error"

| rex field=\_raw "from (?<src\_ip>\d+\.\d+\.\d+\.\d+)"

| table \_time src\_ip \_raw

**Explanation:**

* This query attempts to locate events containing "Internal Server Error" and extracts the source IP.
* The \_raw log data is included for further inspection.

**Result:**

No events related to "Internal Server Error" were found. A broad search using terms such as "500" and "error" was also conducted, but no significant findings were detected.

**Conclusion:** The system showed no signs of internal server errors during the investigation. It is possible that such errors are logged using a different structure or in logs not indexed by Splunk.

A screenshot of a computer

Description automatically generated

**Conclusion and Recommendations**

**Summary of Findings:**

* **1259 failed login attempts** were detected, with a significant portion coming from IP 86.212.199.60, indicating a potential brute-force attack.
* **36 successful SSH sessions** were opened by user djohnson.
* **71 IP addresses** had more than 5 failed attempts, with some showing high activity.
* No internal server errors were detected.

**Recommendations:**

* **Mitigate brute-force attacks:** Consider blocking IPs with high failed attempts using firewall rules or intrusion prevention systems.
* **Set up alerts:** Configure Splunk alerts to monitor failed login attempts and detect brute-force behavior in real-time.
* **Audit log sources:** Ensure that all critical system and application logs are properly indexed, especially for monitoring internal server errors.
* **Review security measures:** Conduct a comprehensive security audit to identify and address vulnerabilities.

By following these steps, the system’s security posture can be significantly improved, preventing unauthorized access and ensuring early detection of suspicious activity.

**Appendices**

* Screenshots of query outputs are included as supporting evidence for each task.
* Additional investigation queries can be conducted as needed based on future requirements.

**Prepared By:** **Fikrat Chalabiyev**  (Cybersecurity Analyst )