SOC Log Monitoring & Incident Response Project

Using Linux Authentication Logs and Splunk

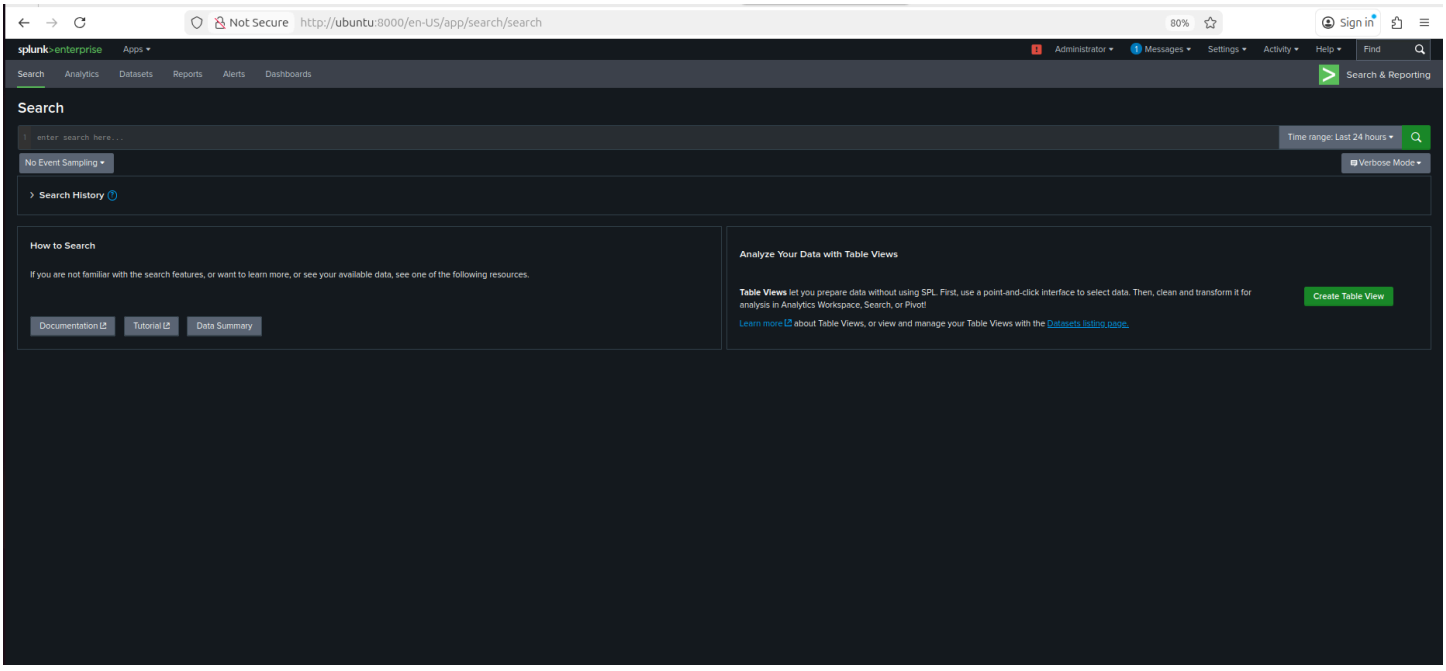
1. Overview of SOC Log Monitoring & Incident Response

A Security Operations Center (SOC) is responsible for continuously monitoring systems and networks to detect, analyze, and respond to security incidents. One of the most critical SOC functions is log monitoring, which provides visibility into system activity and potential security threats.

In this project, SOC log monitoring is demonstrated by analyzing Linux authentication logs to detect suspicious login activity, specifically SSH brute-force attacks. Incident response techniques are applied to investigate the detected activity, assess its impact, and recommend mitigation actions.

This project simulates a real-world SOC workflow, including log ingestion, threat detection, investigation, and documentation.

Splunk HomePage:



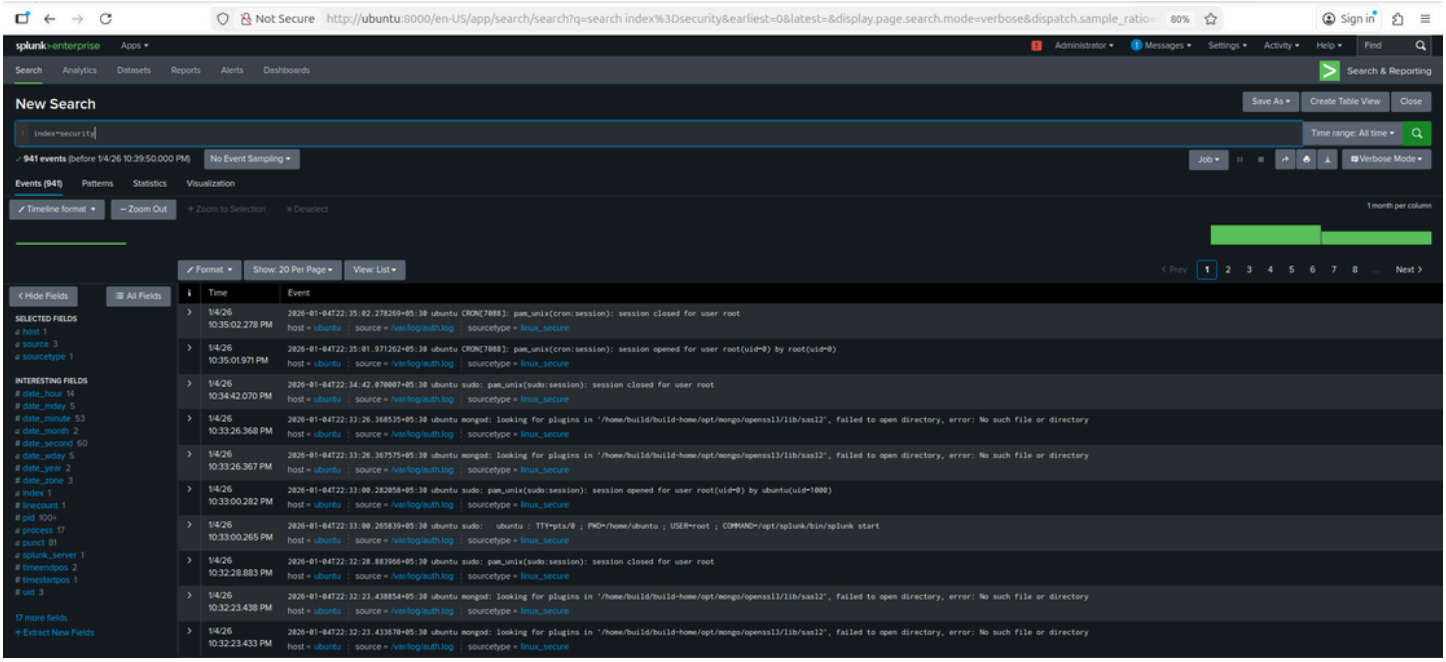
2. Understanding How Splunk Monitoring Works

Splunk is a Security Information and Event Management (SIEM) platform used by SOC teams to collect, index, search, and analyze log data from multiple sources.

Splunk monitoring works through the following core components:

- **Log Ingestion: Security-relevant logs are collected from systems and applications.**
- **Indexing: Logs are stored in indexes that allow fast searching.**
- **Search and Correlation: Analysts use queries to identify suspicious patterns across logs.**
- **Visualization and Alerting: Dashboards and alerts convert raw logs into actionable security insights.**

In SOC operations, Splunk enables analysts to move from raw event data to incident detection and response by correlating authentication events over time.



3. Splunk Installation on Linux and Log Configuration Steps

Step 1: Download Splunk - take the link from the offlicial website of the splunk and paste it in the terminal

wget -O splunk.tgz https://download.splunk.com/products/splunk/releases/9.2.0/linux/splunk-9.2.0-linux-x86_64.tgz

Step 2: Extract

dpkg -i -xvzf splunk-9.2.0-linux-x86_64.tgz

Step 3: Start Splunk

/opt/splunk/bin/splunk start --accept-license

Step 4: Access Web UI

http://<SERVER_IP>:8000

Step 5: Enable Auto-Start

/opt/splunk/bin/splunk enable boot-start

Now we have installed the splunk lets set up Log Configuration

Step 6: To add the system logs

/opt/splunk/bin/splunk add monitor /var/log/syslog

or to add multiple logs

/opt/splunk/bin/splunk add monitor /var/log/auth.log

/opt/splunk/bin/splunk add monitor /var/log/secure

Deploying a SIEM in a Linux environment involves installing the Splunk Enterprise service and configuring it to ingest relevant security logs.

Linux systems generate authentication logs that record:

- **Failed login attempts**
- **Successful logins**
- **Privilege escalation activity (sudo)**

These logs are critical for SOC monitoring because authentication attacks are often the first stage of a security breach.

In this project:

- **Splunk is installed on a Linux host**
- **Linux authentication logs are identified as a high-value data source**
- **Logs are configured to be ingested into a dedicated security index**

This mirrors real-world SOC environments, where log selection and source prioritization are key responsibilities.

Best for:

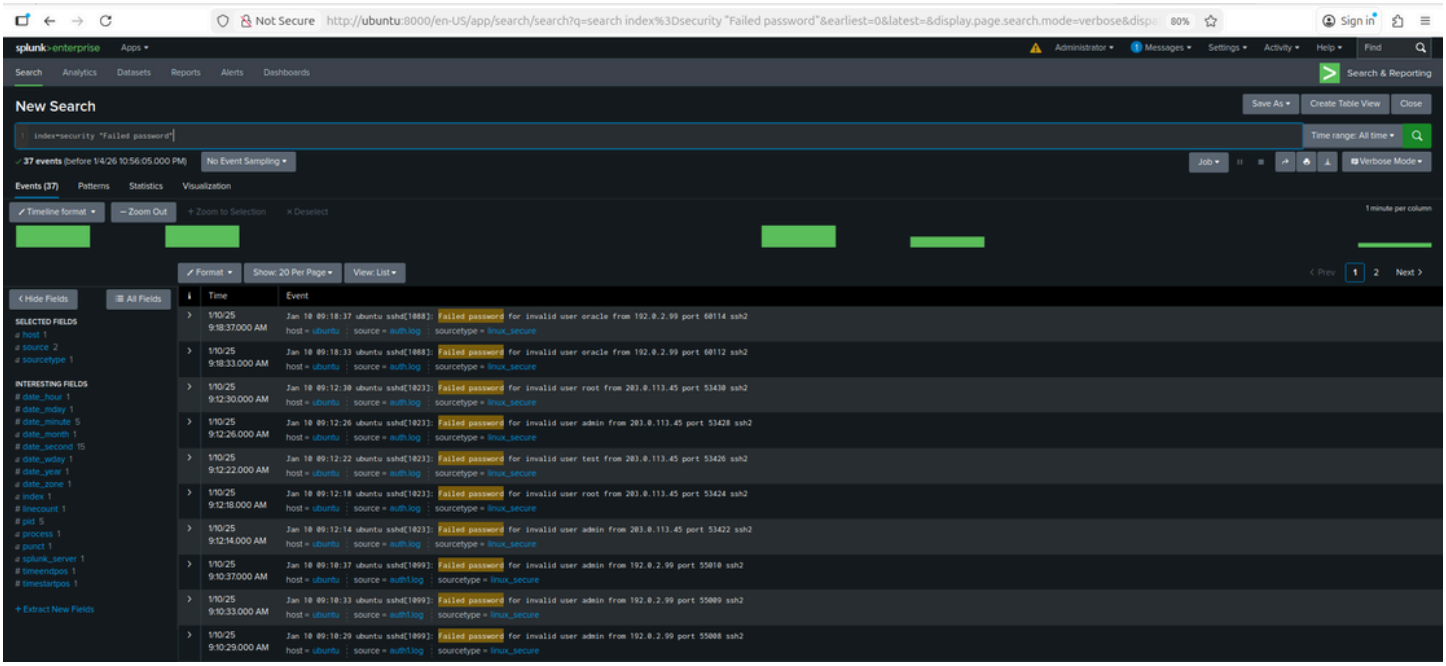
- **SSH brute-force detection**
- **Privilege escalation monitoring**
- **Linux forensic timelines**

4. Practical Execution: Detecting Suspicious Authentication Activity

Once logs were ingested, practical SOC analysis was performed to identify suspicious behavior.

The focus of this step was detecting repeated failed SSH login attempts, which are a strong indicator of brute-force or credential-guessing attacks.

By filtering authentication logs for failed login events and analyzing their frequency, it was possible to identify abnormal login patterns that exceed normal user behavior



5. Correlation and Investigation of Authentication Events

After identifying failed login activity, correlation analysis was performed to understand the scope and severity of the incident.

This included:

- **Identifying source IP addresses generating repeated failures**
- **Determining which user accounts were targeted**
- **Analyzing whether failed attempts were followed by successful authentication**

Correlating failed and successful login events is critical in SOC investigations, as it helps determine whether an attack resulted in unauthorized access.

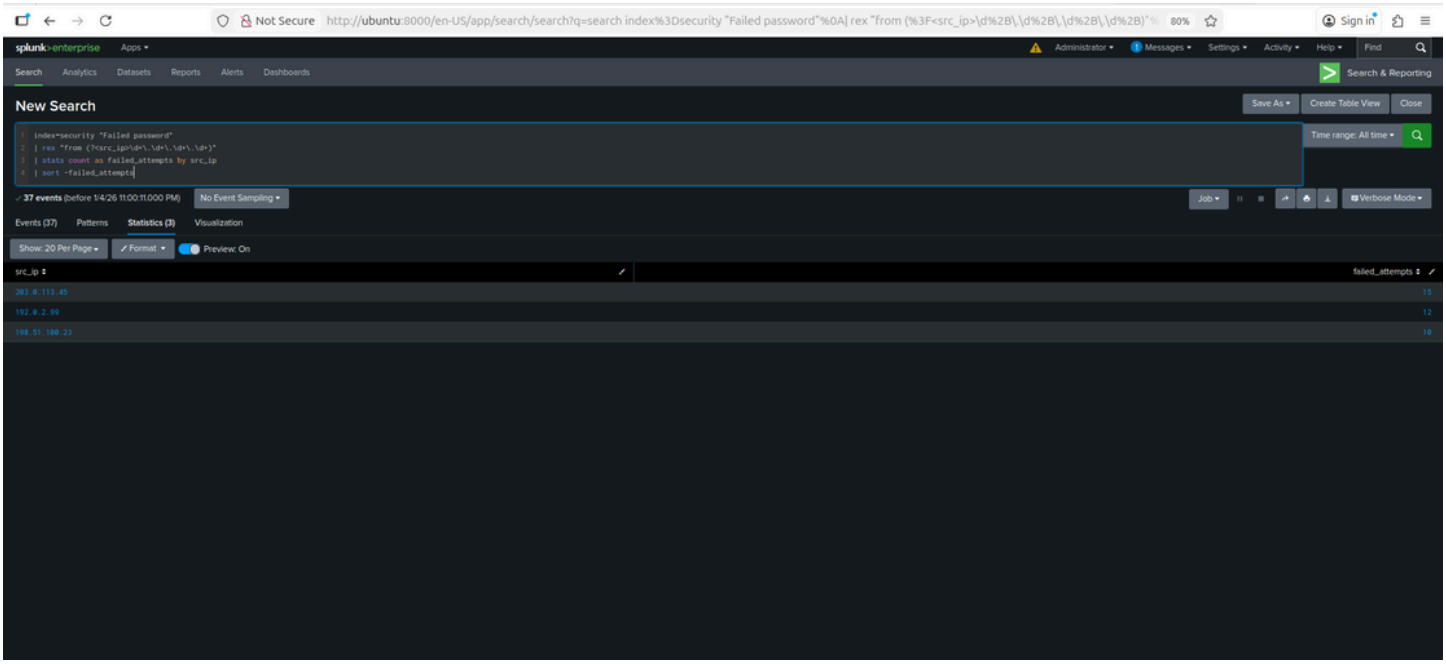
Query:- Identify Source IP Addresses Generating Repeated Failures

index=security "Failed password"

| rex "from (?<src_ip>\d+\.\d+\.\d+\.\d+)"

| stats count as failed_attempts by src_ip

| sort -failed_attempts



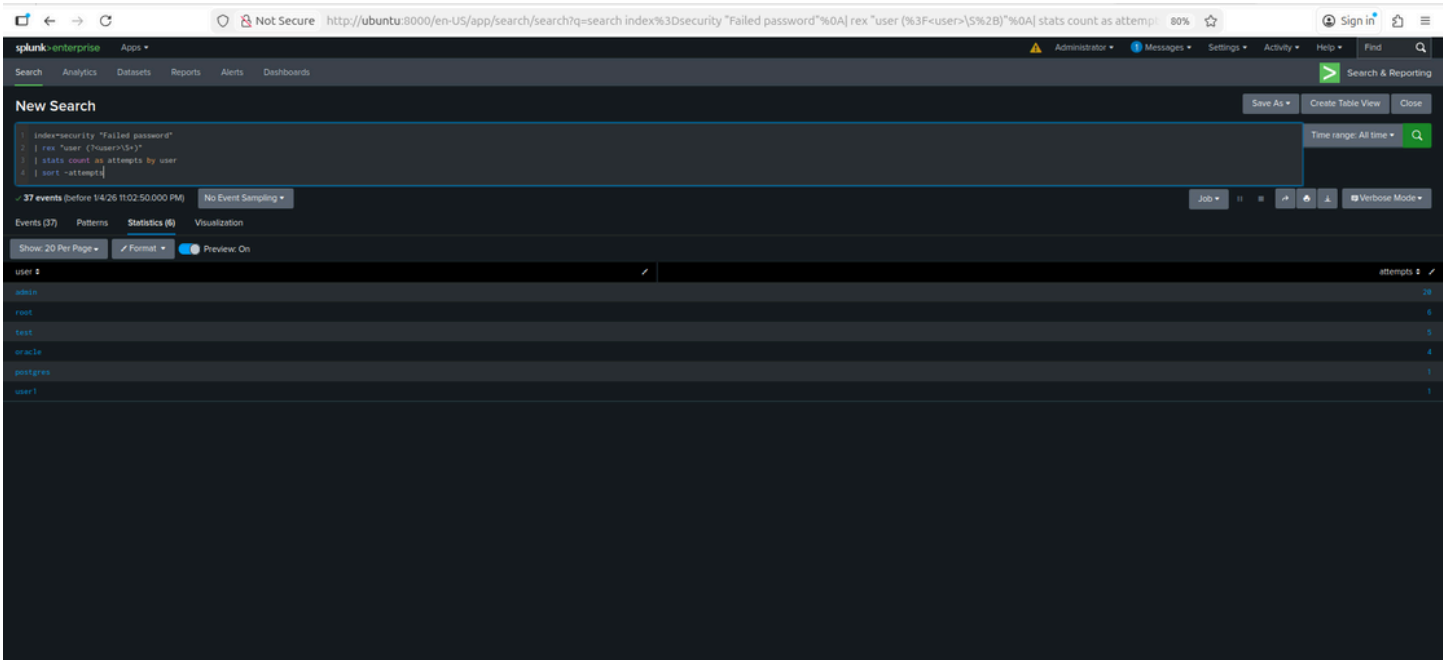
Query :- Determine Which User Accounts Were Targeted

index=security "Failed password"

| rex "user (?<user>\S+)"

| stats count as attempts by user

| sort -attempts



Query:-Analyze Whether Failed Attempts Were Followed by Successful Authentication

index=security ("Failed password" OR "Accepted password")

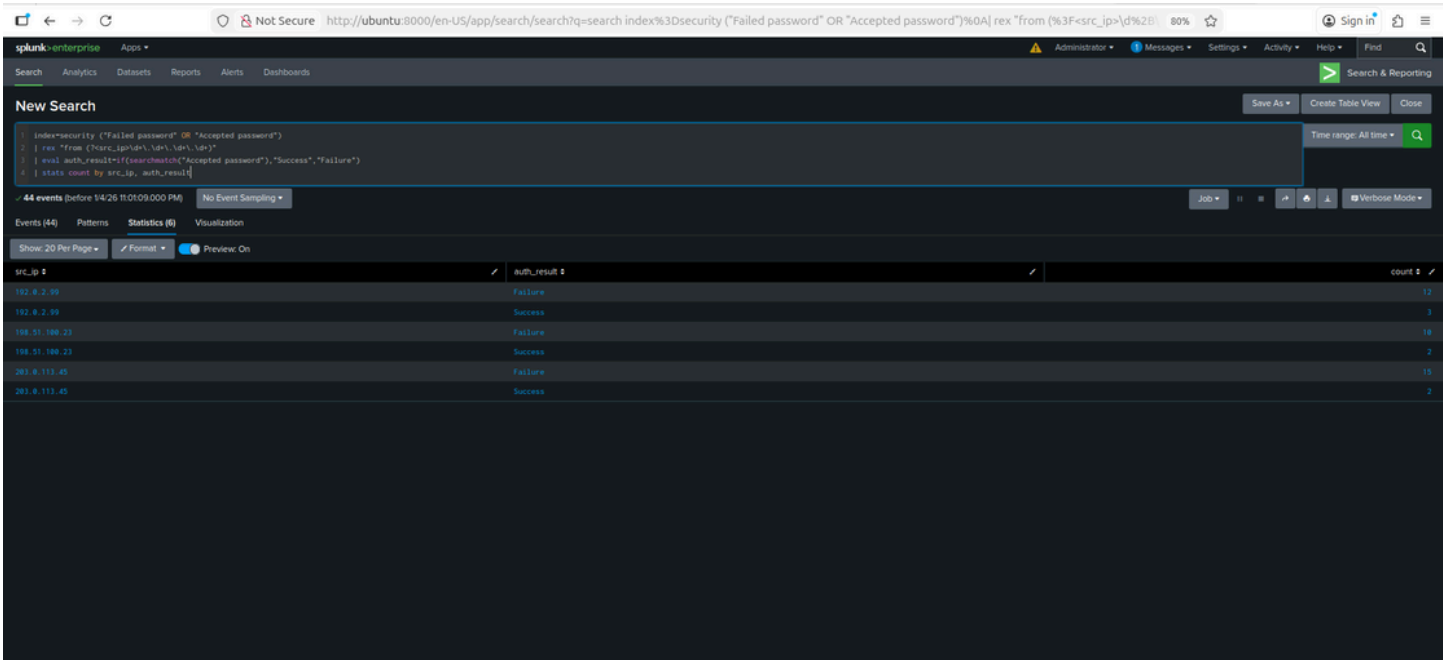
| rex "from (?<src_ip>\d+\.\d+\.\d+\.\d+)"

| eval auth_result=if(searchmatch("Accepted password"),"Success","Failure")

| stats count by src_ip, auth_result

Query:- High-Risk Correlation: Failed → Successful

```
index=security
| rex "from (?<src_ip>\d+\.\d+\.\d+\.\d+)"
| stats
    count(eval(searchmatch("Failed password"))) as failures
    count(eval(searchmatch("Accepted password"))) as successes
    by src_ip
| where failures > 5 AND successes > 0
```



6. Security Analysis and Threat Interpretation

The observed authentication activity was analyzed to determine whether it represented malicious behavior.

Repeated failed login attempts targeting common administrative accounts strongly indicate brute-force attack activity. When such attempts are followed by successful authentication, the risk level increases significantly and may indicate credential compromise.

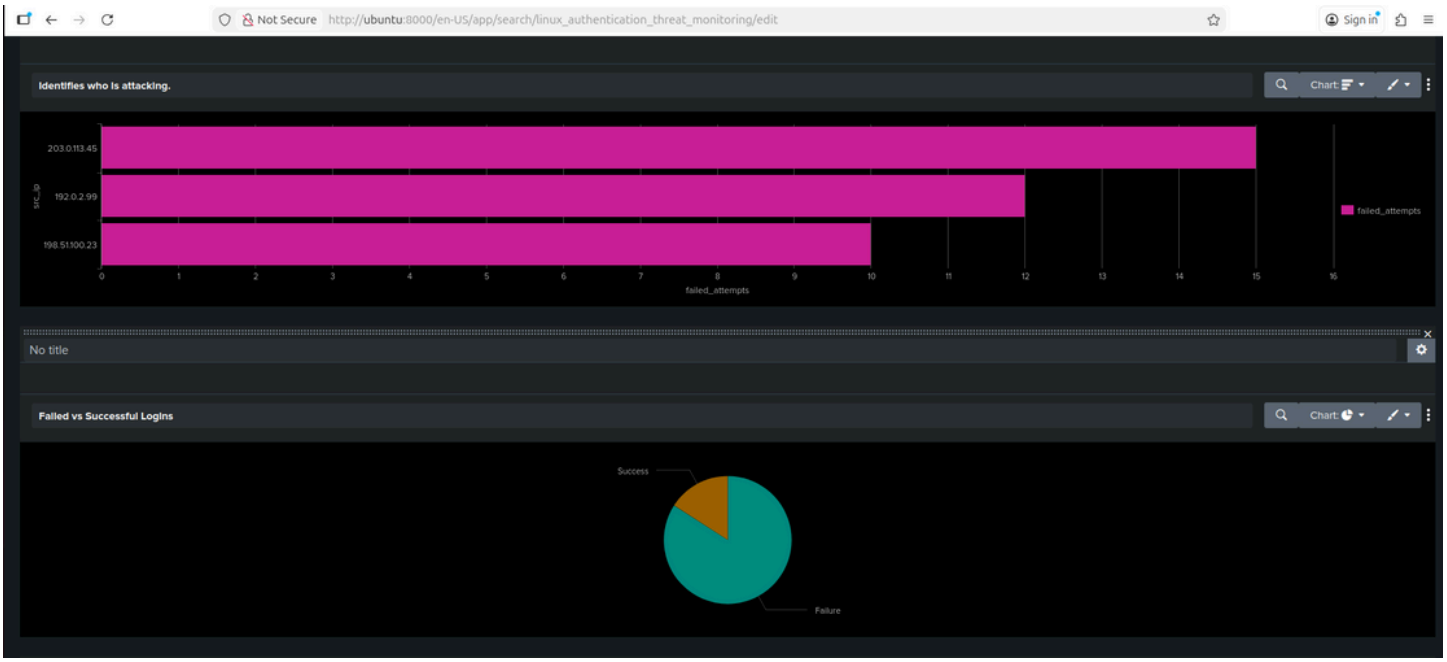
Although this project focuses on authentication attacks rather than traditional malware, the same SOC analytical principles apply:

- **Behavior-based detection**
- **Event correlation**
- **Evidence-driven conclusions**

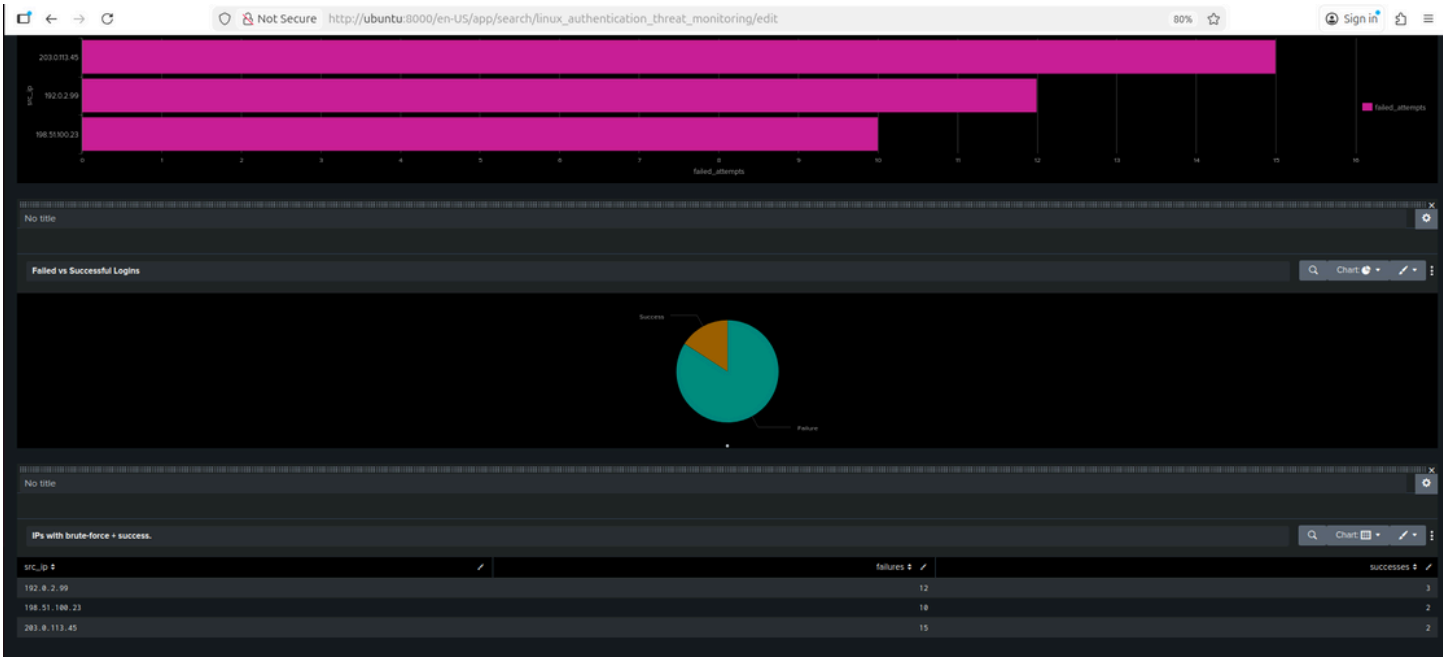
Dashboards

Pannel-1: authentication failures

Pannel 2&3-Identifies who is attacking&Failed vs Successful Logins



Pannel 4-IPs with brute-force + success



7. Use Cases and Applications in SOC Operations

The techniques demonstrated in this project apply directly to real-world SOC operations, including:

- **SSH brute-force attack detection**
- **Account compromise investigation**
- **Credential abuse monitoring**
- **Early-stage intrusion detection**

8. Conclusion

This project demonstrates a complete SOC-style log monitoring and incident response workflow using Linux authentication logs and Splunk.

By centralizing logs, detecting suspicious authentication activity, correlating security events, and documenting findings, the project highlights the importance of SIEM platforms in modern SOC operations.

The outcome reinforces how proactive monitoring and structured analysis enable SOC teams to identify and respond to security threats before they escalate into full compromises.

Thankyou!

Done by

S.JITHENDRA REDDY