TITTLE: SSH Brute Force Analysis Report

Date: November 12, 2025

Analyst: OLATUNJI OLANIKE

Monitored Systems: Linux servers hosting patient-record microservices.

Sourcetype=csv.

1. Executive Summary

This report details the investigation on a surge in SSH brute-force attempts, credential-stuffing, and unauthorized login activities on the Linux servers hosting patient-record microservices of X Health Systems.

The primary objective of automated defense was not met, as the existing logging tools lacked correlation, generating excessive false alerts and failed to detect low-velocity distributed attacks. This increased analyst workload, created alert fatigue, and left potential openings for compromise of Protected Health Information (PHI).

Over the n period, **2000** brute-force incidents were identified. 135 Enumeration attempts, 385 targeting valid user attempts, 468 received disconnect attempts and 520 failed password attempts. Top 10 offending IPs were also identified with 183.62.140.253 attempting a brute force attack 286 times from Beijing city of China

Continuous monitoring, refinement of geolocation baselines and strong password policy are recommended to improve detection accuracy and prevent future occurrence.

2. Methodology and Objectives Fulfillment

The analysis was executed against four key objectives:

Log ingestion: Data to be analysed was transferred to Splunk

Anomaly detection: Unusual activities on the network detection.

SOC automation: Trigger logic was created to counter the findings

Visualization, Visual dashboard for easier analysis was created

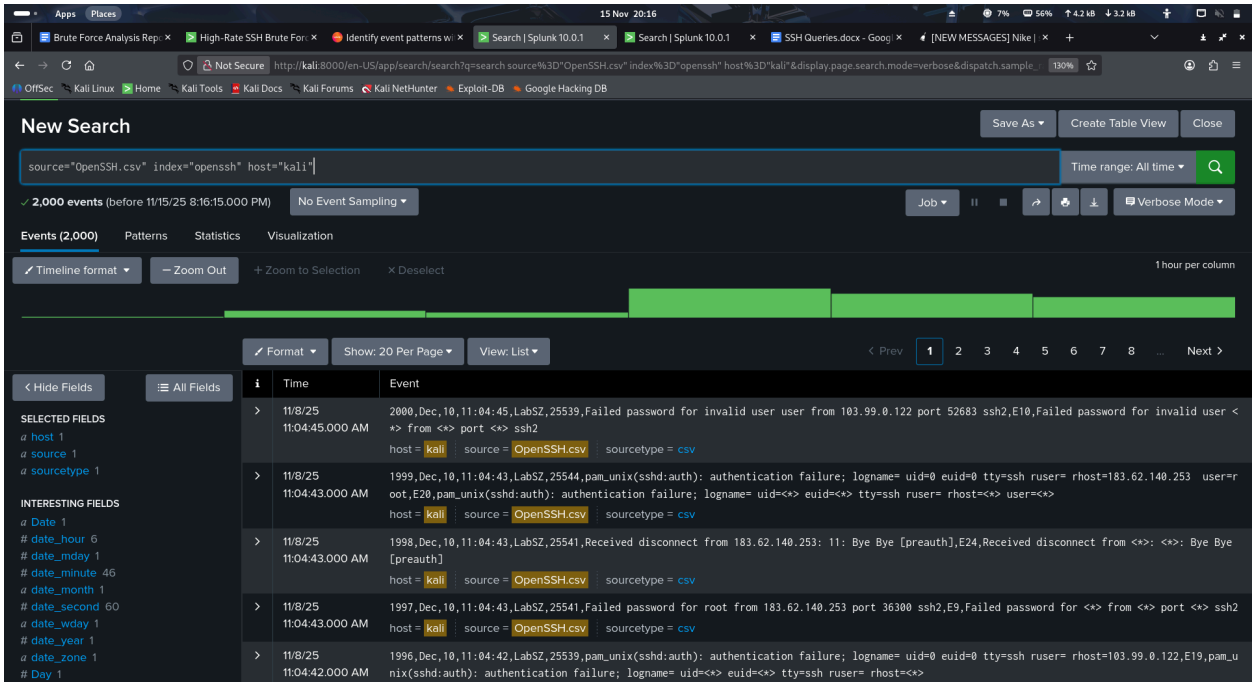
2.1. Objective 1: Ingest and Parse SSH Logs in Splunk Enterprise

Status	Details
Complete	SSH logs from the monitored Linux/Unix servers hosting patient's microservice were successfully ingested. Logs are indexed under Openssh. index underwith a source type OpenSSH.csv Critical fields (src_ip, user, action, _time) are correctly parsed

SPL for Log Parsing:

```
source="OpenSSH.csv" index="openssh" host+"kali"
```

Screenshot of the 2000 brute force attempt events



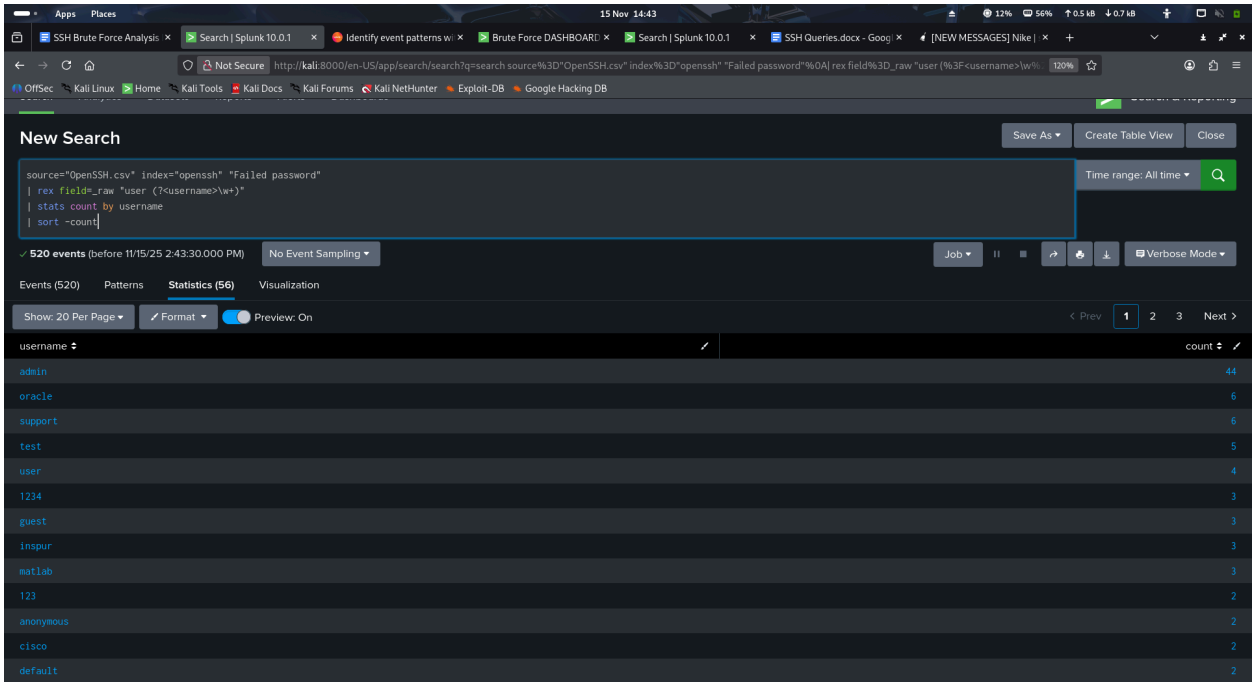
2.2. Objective 2: Detect Abnormal SSH Behavior

Anomaly detection focused on six primary types of suspicious activity:

A. Repeated Failed Password Attempt by User (Brute Force)

- **Metric:** Count of Failed password events per unique username
- **Findings:** 56 unusual usernames were flagged for suspicious login attempts. The highest observed rate was **from an invalid username "admin"** with 44 count

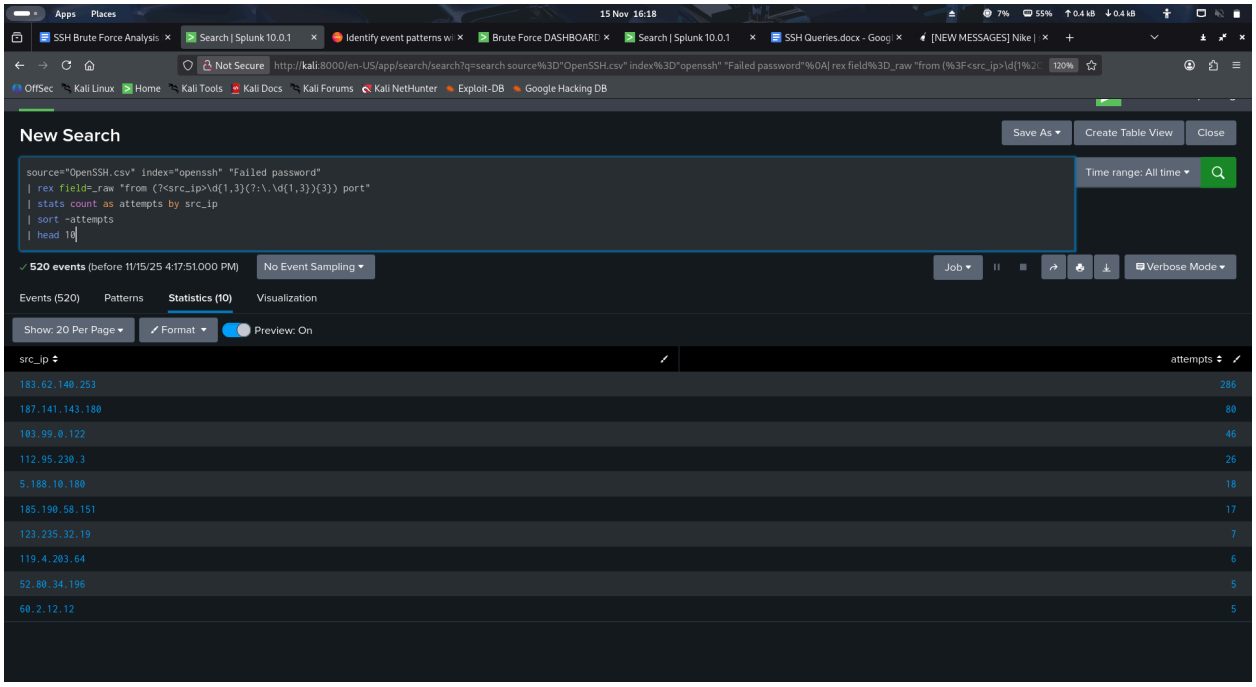
Screenshot of failed password attempt by user



B. Top 10 Offending IPs With Failed Password

- **Metric:** Login attempts from suspicious IPs.
- **Tool:** The | head 10 command was used to map the top ten offending IP addresses.
- **Findings:** most unusual activities was recorded from 183.62.140.253 with 286 attempts

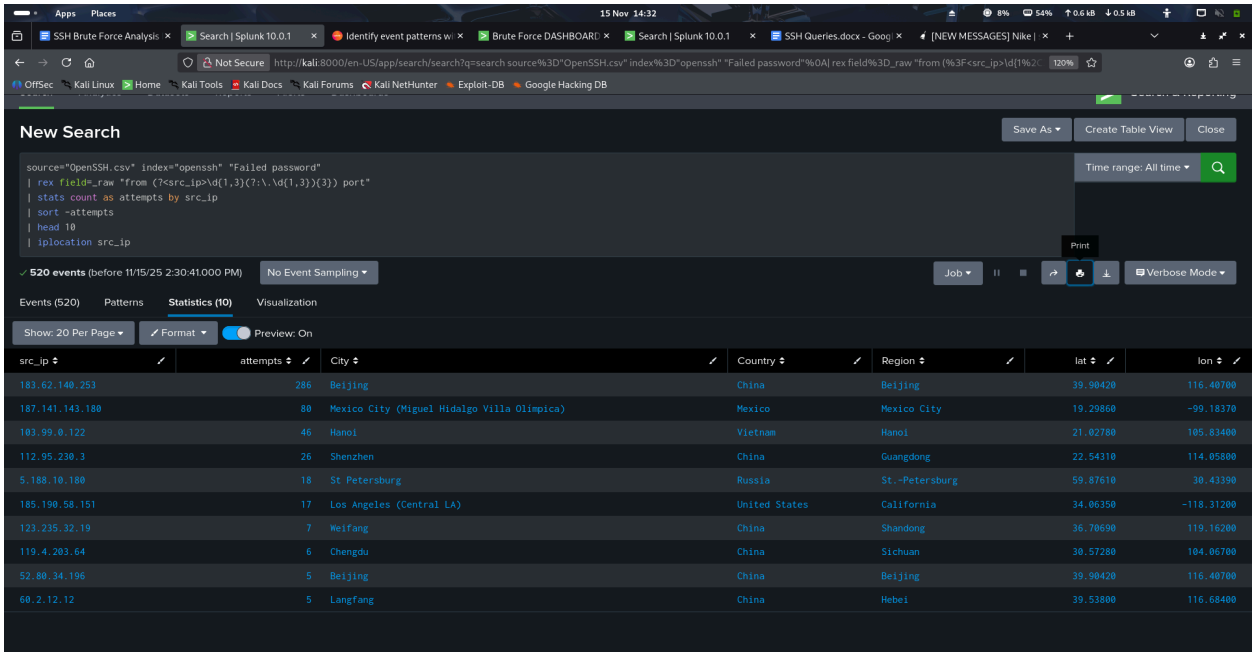
Screenshot of 10 top offending IPs



C. Login from Unusual Geolocation

- **Metric:** Login attempts where src_ip geolocation is outside of established organizational regions or **"high-risk"** countries.
- **Tool:** The | iplocation src_ip command was used to map all traffic origins of the top ten offending IP addresses.
- **Findings:** Three of the most suspicious were the **286** of failed password attempts originated from the high-risk region of **Beijing in China,** 80 failed password attempts originated from **Mexico City (Miguel Hidalgo Villa Olímpica** and 40 failed passwords originated from **Hanoi Vietnam** .

Screenshot of the geolocation of the top10 offending IPs

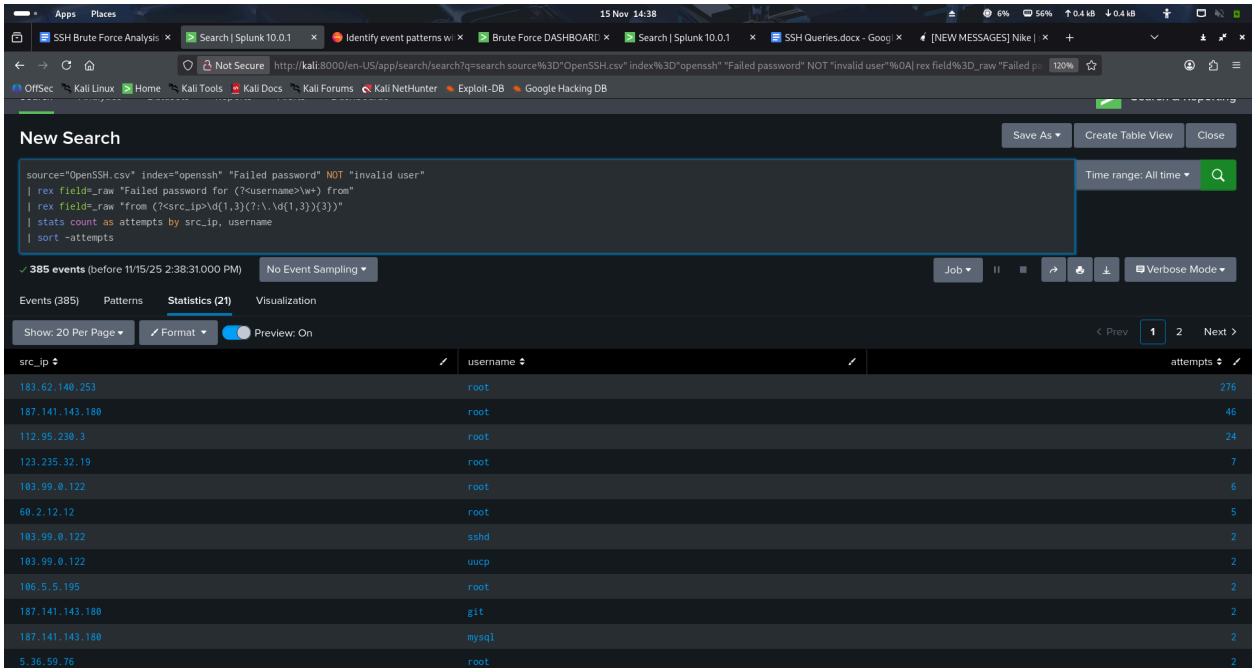


src_ip	attempts	City	Country	Region	lat	lon
183.62.140.253	286	Beijing	China	Beijing	39.90420	116.40700
187.141.143.180	80	Mexico City (Miguel Hidalgo Villa Olímpica)	Mexico	Mexico City	19.29860	-99.18370
103.99.0.122	46	Hanoi	Vietnam	Hanoi	21.02780	105.83400
112.95.230.3	26	Shenzhen	China	Guangdong	22.54310	114.05800
5.188.10.180	18	St Petersburg	Russia	St.-Petersburg	59.87610	30.43390
185.190.58.151	17	Los Angeles (Central LA)	United States	California	34.06350	-118.31200
123.235.32.19	7	Weifang	China	Shandong	36.70690	119.16200
119.4.203.64	6	Chengdu	China	Sichuan	30.57280	104.06700
52.80.34.196	5	Beijing	China	Beijing	39.90420	116.40700
60.2.12.12	5	Langfang	China	Hebei	39.53800	116.68400

D. Username Spraying (Targeting Valid User)

- **Metric:** src_ip attempting to log in as users
- **Findings:** 21 IPs targeted valid user on the system, with the most attempt coming from 183.62.140.253. This IP is located in Beijing China

Screenshot of the targeted valid user accounts

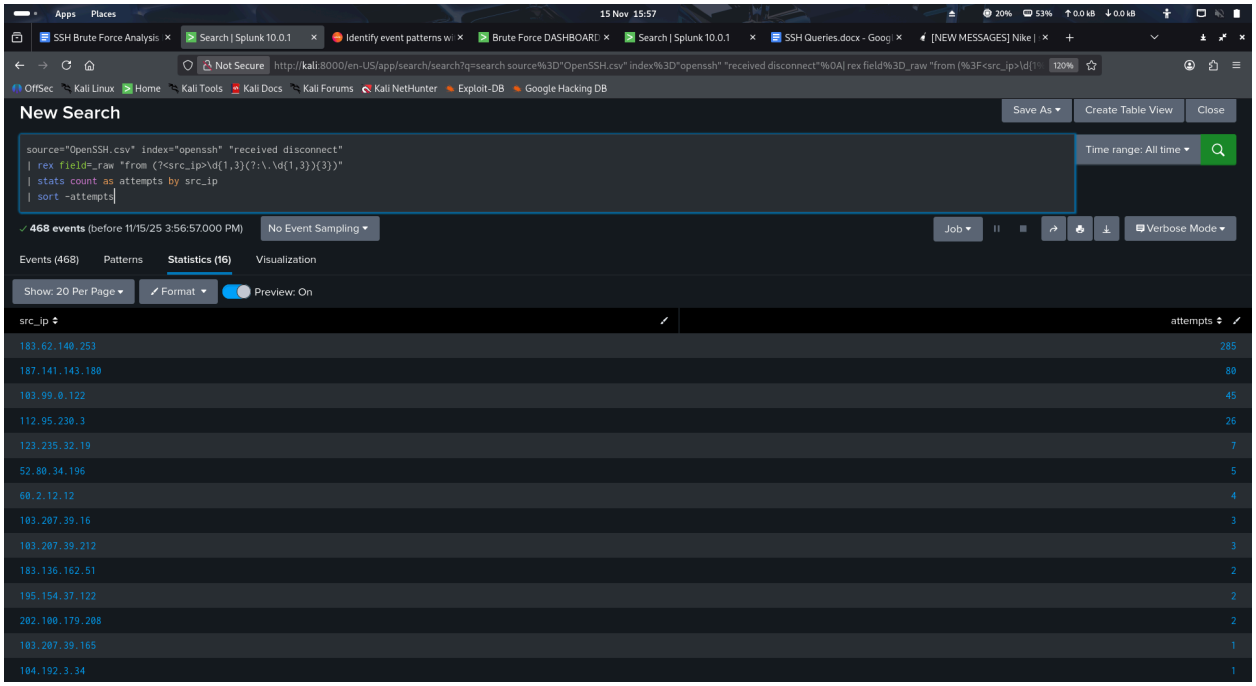


src_ip	username	attempts
183.62.140.253	root	276
187.141.143.180	root	46
112.95.230.3	root	24
123.235.32.19	root	7
103.99.0.122	root	6
60.2.12.12	root	5
103.99.0.122	sshd	2
103.99.0.122	uucp	2
106.5.5.195	root	2
187.141.143.180	git	2
187.141.143.180	mysql	2
5.36.59.76	root	2

E. Received disconnect

- **Metric:** The session ended before authentication completed
- **Findings:** There were 486 received disconnect with 16 suspicious IPs receiving a disconnect message before they could authenticate, with the most suspicious originating from 183.62.140.253, 187.141.143.180 , 103.99.0.122, 103.99.0.122 and 112.95.230.3

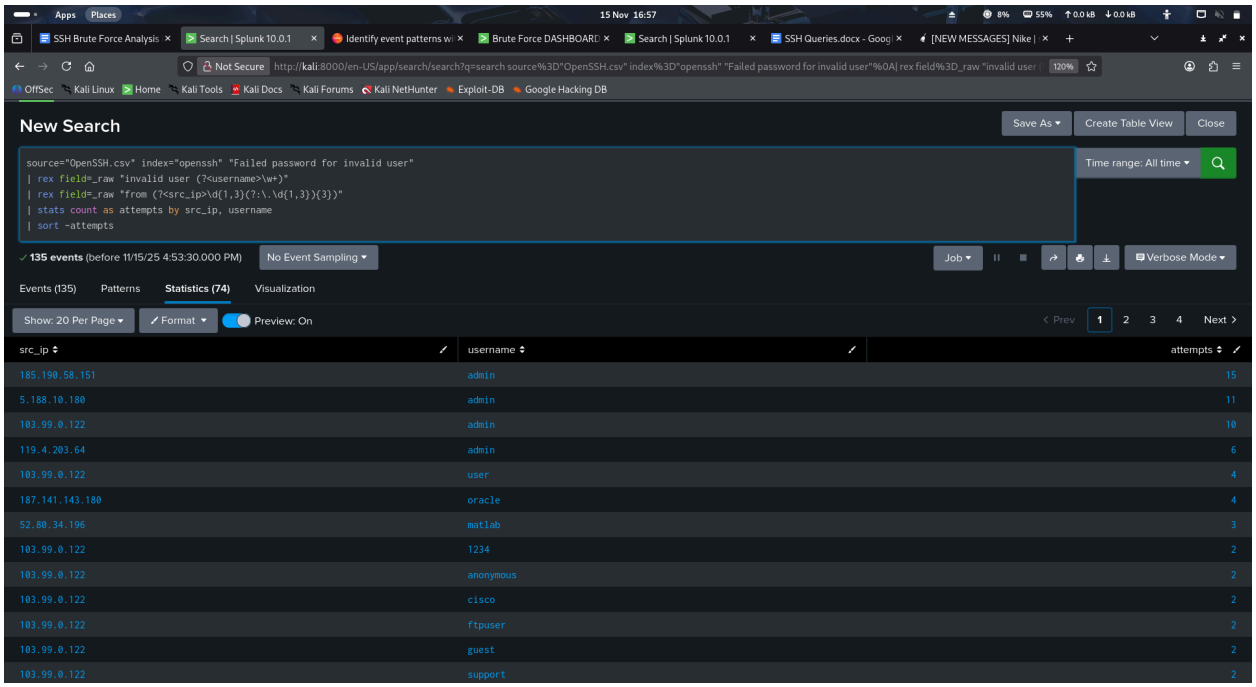
Screenshot of the received disconnect querries



F. Enumeration Attempts

- **Metric:** Attempt to discover valid username or other information on a system
- **Findings:** There were 135 attempts to discover valid user accounts from 74 suspicious IPs

Screenshot of the Enumeration Attempts

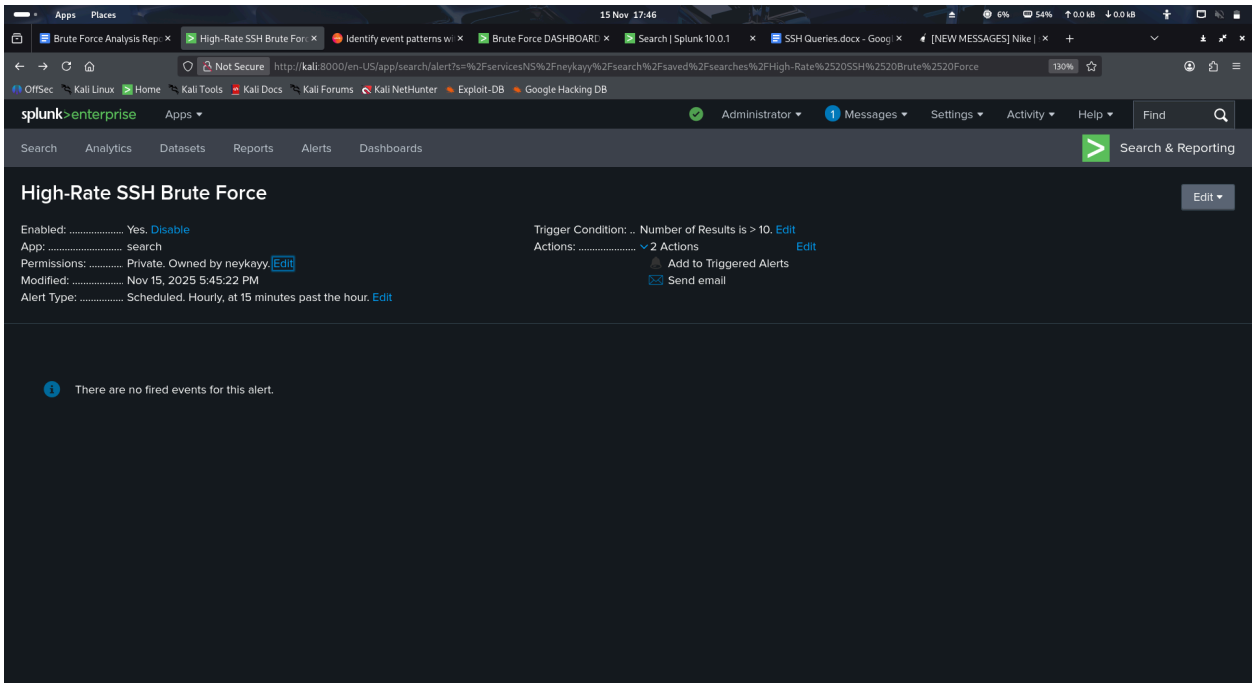


2.3. Objective 3: Automate SOC Response using Splunk Alerting:

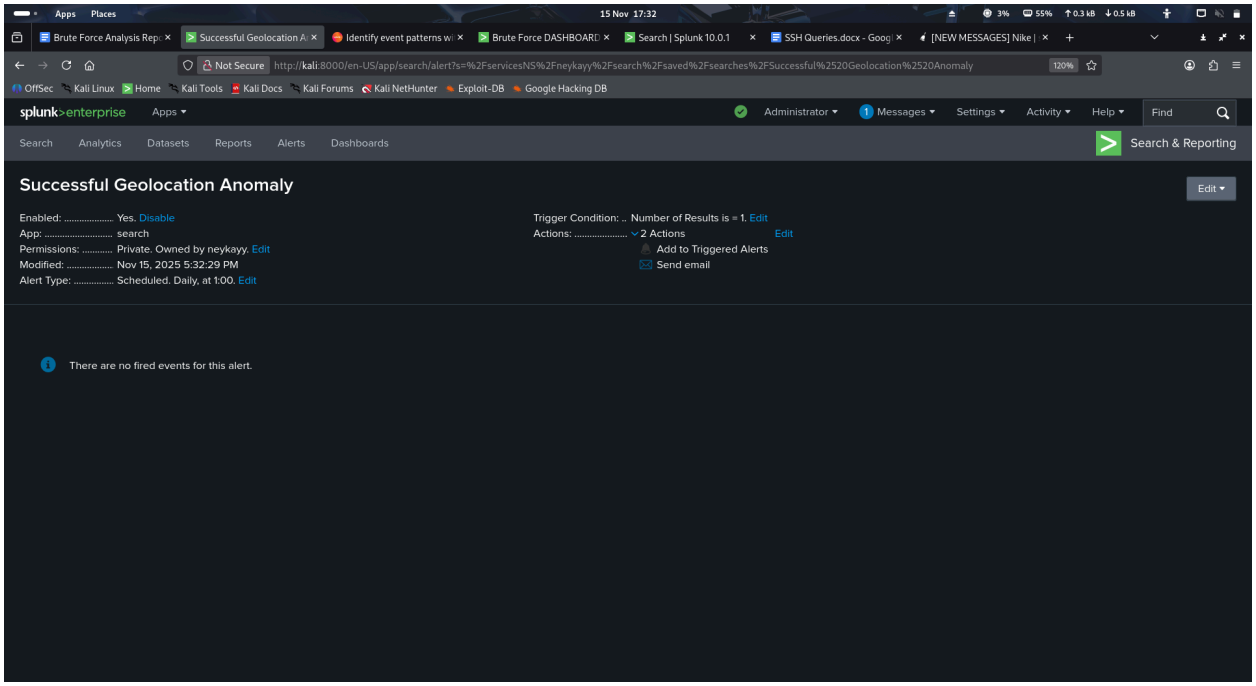
Splunk Alerts was configured to automatically execute a response when a defined detection threshold is met, enabling a faster response that manual intervention

Alert Name	Trigger Logic	Automated Action
High-Rate SSH Brute Force	src_ip > 10 in 5 minutes.	1. Email notification to SOC. 2. Adaptive Response: **Send Malicious IP to Firewall Block List.**
Successful Geolocation Anomaly	Successful login (action=success) from a previously unseen country.	Email Alert with HIGH severity.

Screenshot of alert created for suspicious ip addresses



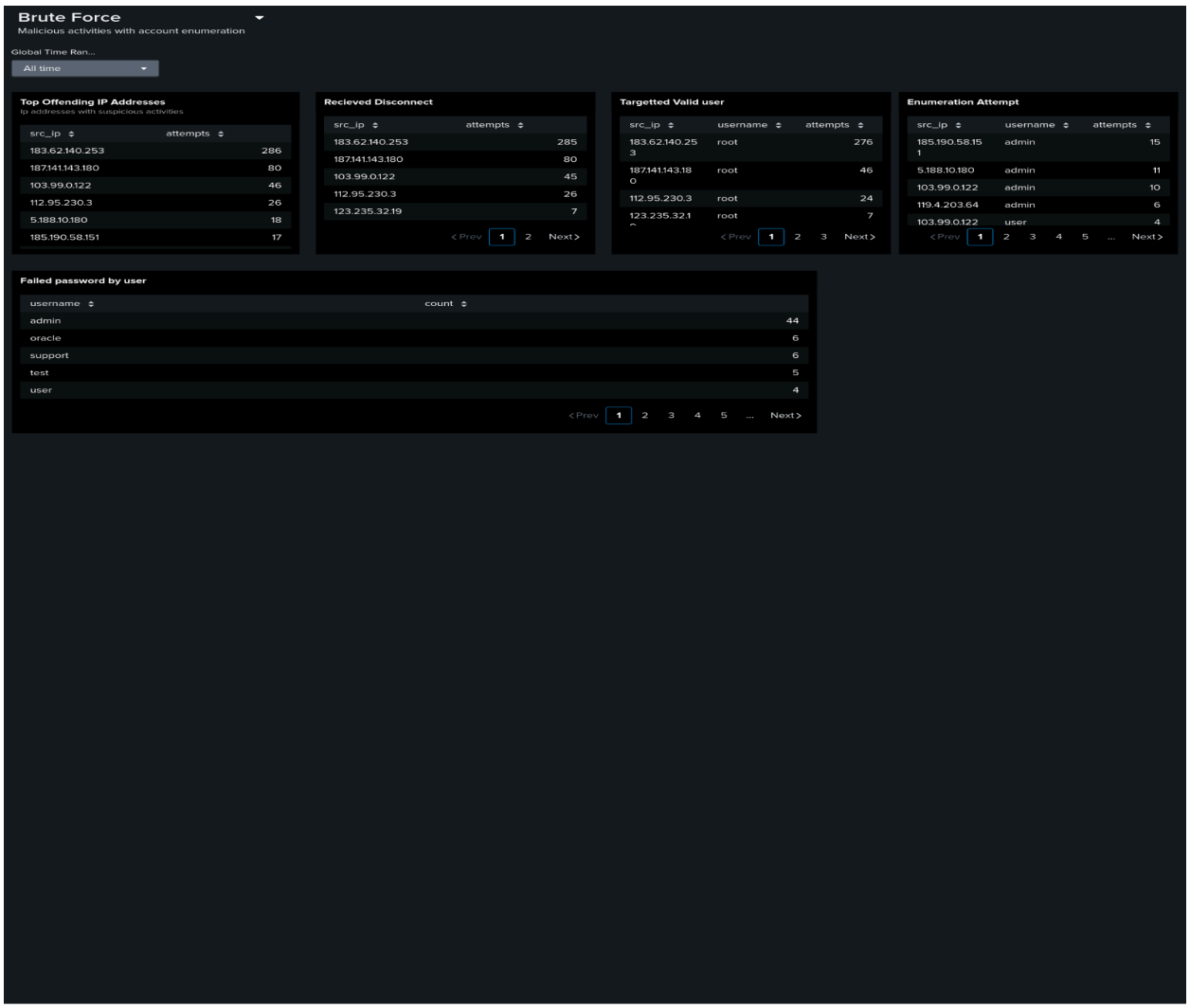
Screenshot of alert created for anomaly geolocation



2.4. Objective 4: Visual Dashboards For Visual Analysis

A dedicated SSH Security Dashboard was developed, providing immediate visual correlation for faster incident triage.

Screenshot of the dashboard



3. Conclusion and Recommendations.

The analysis of the brute force attempt reveals a high-volume, automated attack originating from a distributed network of compromised IP addresses from suspicious geolocation, primarily targeting SSH and root account. Over 2000 login attempts were recorded within a 6-hour window. Fine tuning the Splunk configuration will be highly effective in detecting and automatically responding to common SSH brute-force patterns..

Recommendations for Improvement

1. **Geolocation Baselines:** Refine the "unusual geolocation" detection by building a specific user-to-country successful login lookup. This will better identify compromised accounts logging in from unexpected locations .
2. **Increased Alert Context:** Enhance the alert payload sent to the SOC with a list of the **top 5 usernames** targeted by the malicious aiding the SOC in prioritizing which user accounts to review.
3. **Adaptive Thresholds:** Explore using **Splunk Machine Learning Toolkit (MLTK)** to establish dynamic thresholds for failed attempts, moving beyond static counts of 10 or 20. This will reduce false positives during legitimate spikes in activity (e.g., automated systems rebooting) while catching slower, more persistent attacks.
4. **Stronger password policy:** Using password that are long, complex, paraphrases avoiding personal information and predictable words
5. **Lock out policy**: using a security setting that temporarily blocks a user account after a set number of failed passwords attack, using the three main settings.
6. **Implementing Multifactor Authentication**: using more than one authentication method