Detection of Brute Force and Port Scanning Attacks Using Splunk SIEM

Prepared By: Rabbi Wasti

Table of Contents

Abstract

This project illustrates how the Security Operations Center (SOC) simulation could be implemented with the help of Splunk SIEM. The actual cyberattacks like SSH brute-force and network port scanning were simulated with the help of Kali Linux. The detection and analysis of these attacks were performed on centralized log monitoring in Splunk, with alerts being set up to mimic enterprise SOC detection workflows.

1. Problem

Unauthorized access and reconnaissance attacks are constant threats to organizations. These threats are not detected without a SIEM system. This project will attempt to model these attacks and illustrate the detection and notification of security teams by SIEM tools.

2. Objectives

- Simulate brute-force and port scan attacks
- Centralize logs using Splunk Forwarder
- Analyze authentication and system logs
- Identify attacker IP addresses
- Create automated SOC alerts

3. Architecture &Environment

Component	Role
Kali Linux	Attacker
Fedora Linux	Victim
Splunk Enterprise	SIEM
Splunk Forwarder	Log Collector

4. Tools & Technologies

- Splunk Enterprise
- Splunk Universal Forwarder
- Hydra
- Nmap
- Kali Linux
- Fedora Linux

5.Attack Simulation

6.1 SSH Brute Force Attack

A password-guessing attack attempting unauthorized system access.

Tool Used: Hydra

Command executed on Kali:

hydra -l root -P /usr/share/wordlists/rockyou.txt ssh://192.168.1.48

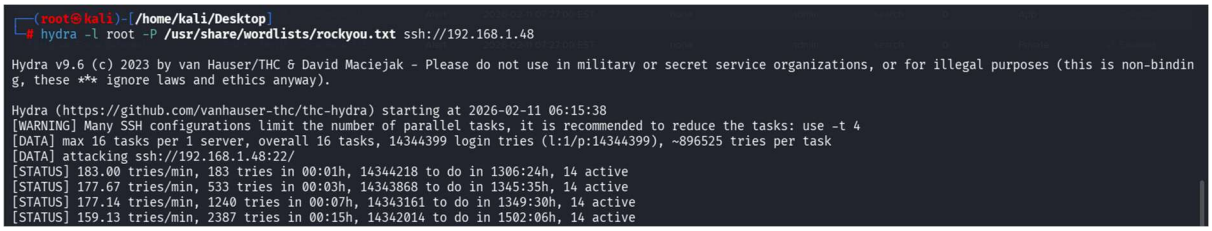

Figure 1:Kali terminal showing Hydra brute force attack.

(Source:-Self-creation)

6.2 Port Scanning Attack

Reconnaissance activity to identify open services.

Tool Used: Nmap

Command:

nmap -sS -p- 192.168.1.48

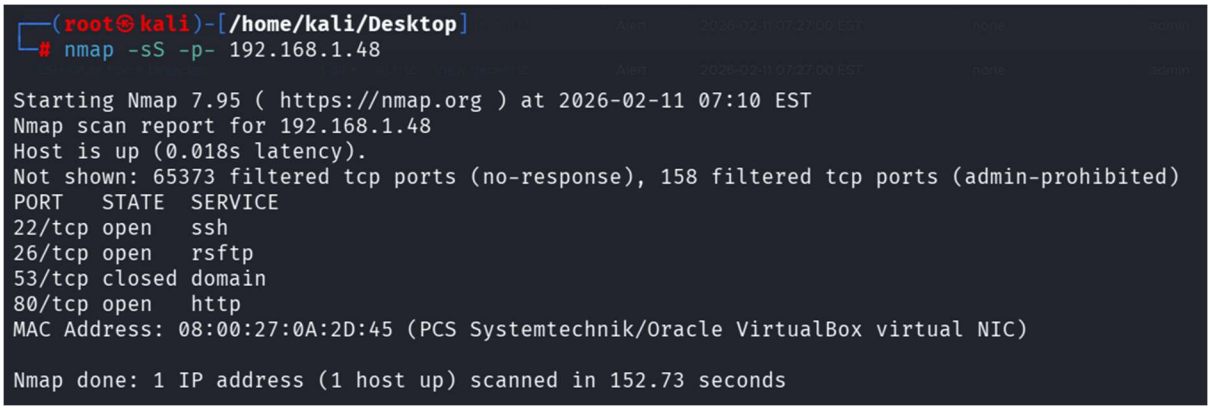

Figure 2:Kali terminal showing Nmap open ports

(Source:-Self-creation)

6.3 Log Collection & SIEM Integration

Fedora system logs (/var/log/secure, /var/log/messages) were forwarded to Splunk using Universal Forwarder**.**

Search:

index=* host=fedora

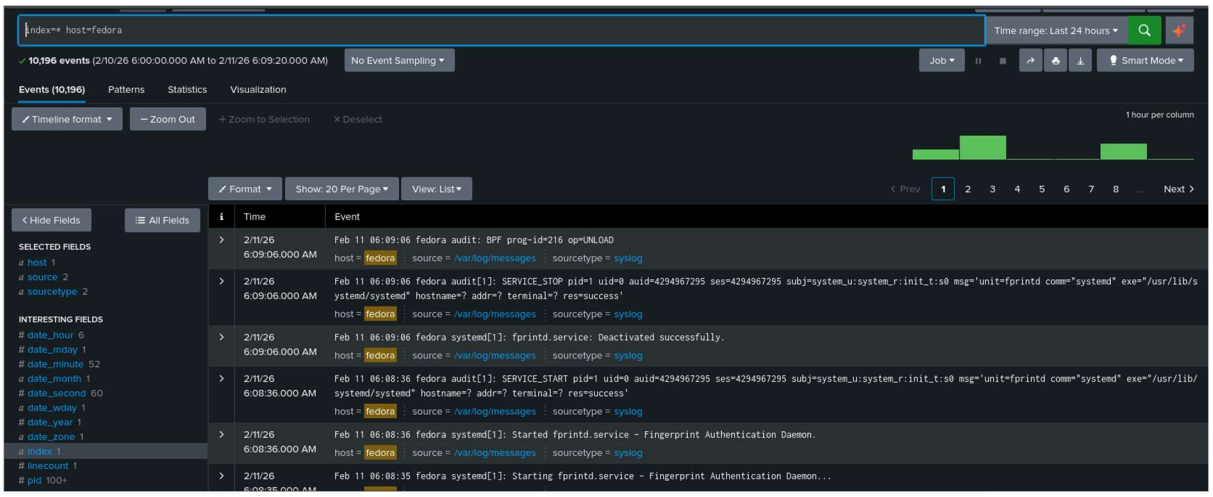

Figure 3:Splunk showing Fedora system logs.

(Source:-Self-creation)

This confirmed successful log ingestion.

6.Brute Force Detection

6.1 Raw Log Identification

"Failed password"

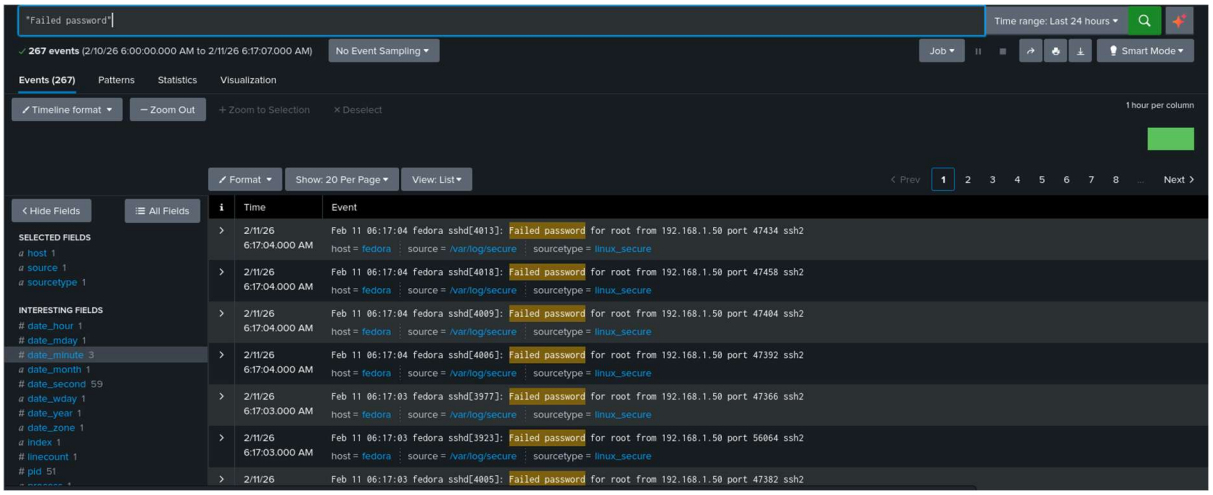

Figure 4:Multiple failed SSH login events.

(Source:-Self-creation)

This filters SSH authentication failures.

6.2 Attacker IP Extraction

"Failed password"

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

| stats count by attacker_ip

| sort -count

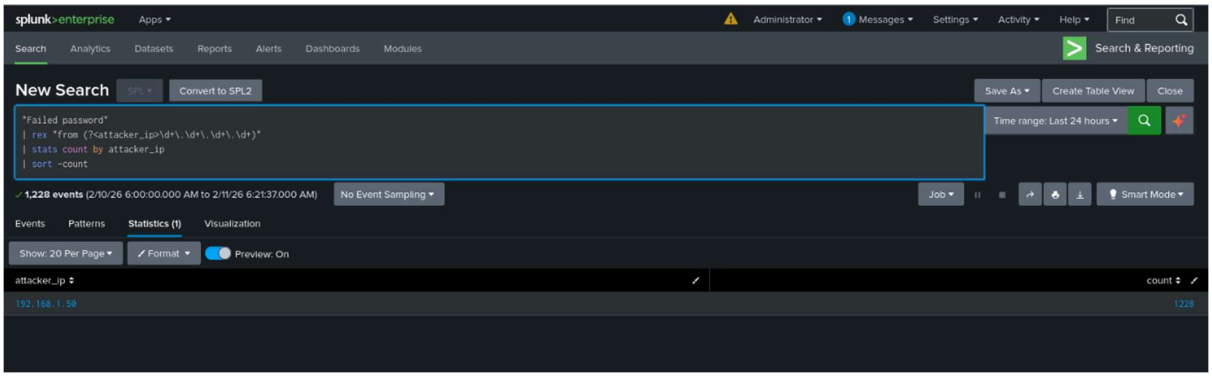

Figure 5:Table showing attacker IP and count

(Source:-Self-created)

This query:

- Filters failed login attempts
- Extracts the attacker IP
- Counts login attempts
- Flags excessive activity

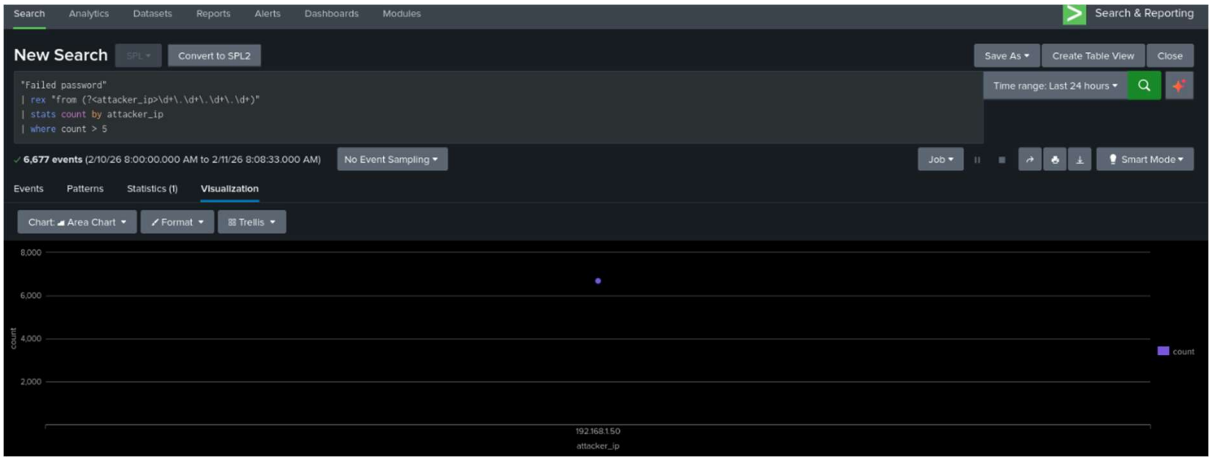

Figure 6:Visualization showing attacker_ip vs count

(Source:Self-created)

The visualization clearly shows a spike in login attempts from IP 192.168.1.50, indicating brute-force behavior.

6.3. Brute Force Alert

Alert Name: **SSH Brute Force Detected**

Trigger: Per result

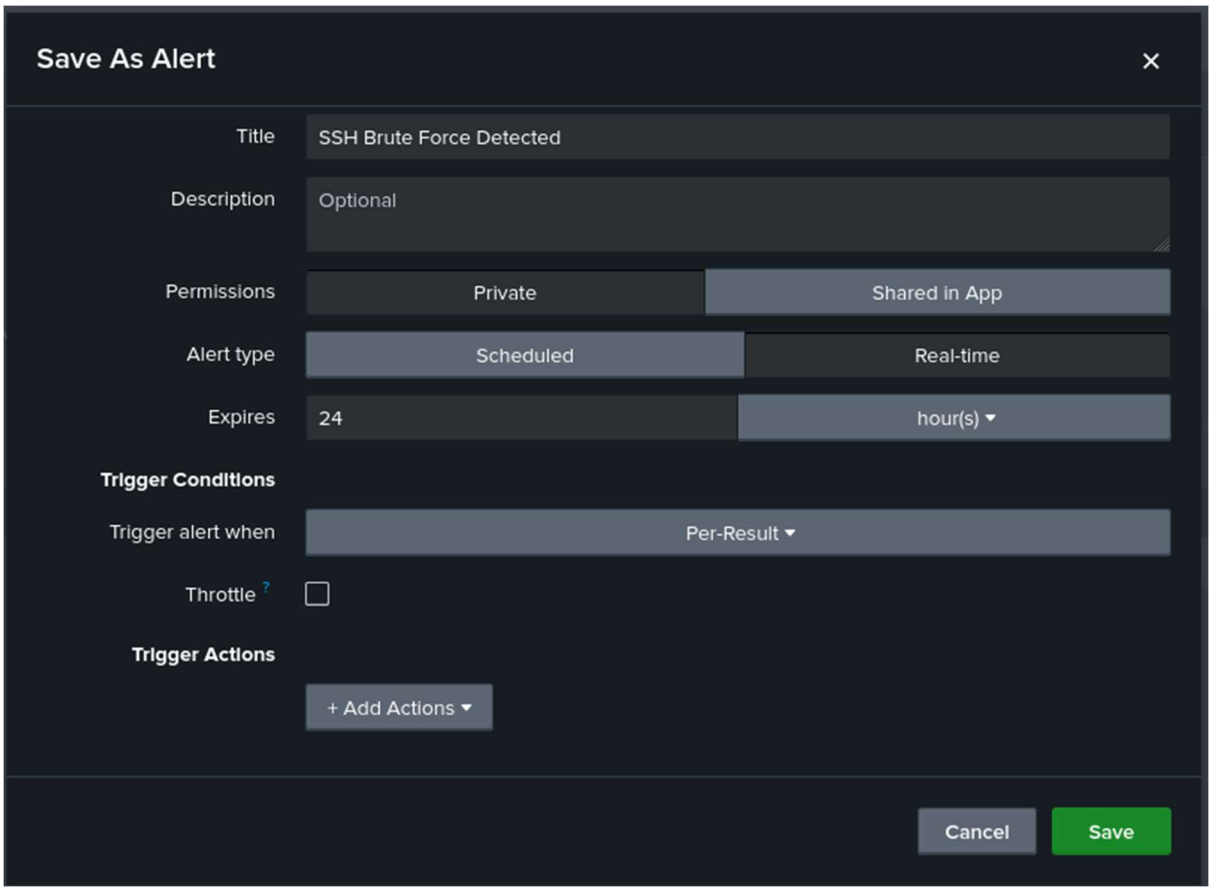

Figure 7:Alert creation page

(Source:Self-created)

7.Port Scan Detection

Search:

index=* host=fedora (ssh OR failed OR refused OR nmap OR scan OR denied OR rejected)

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

| stats count by attacker_ip

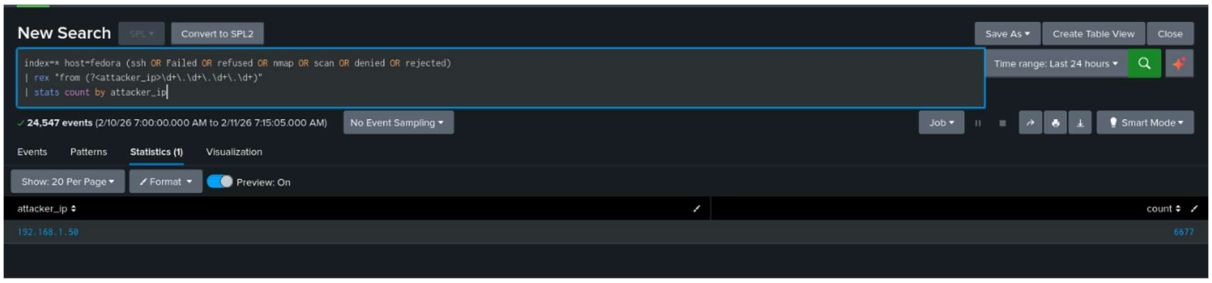

Figure 8:Attacker IP detected with high event count.

(Source:Self-created)

This query:

- Correlates suspicious connection attempts
- Extracts attacker IP
- Aggregates event counts

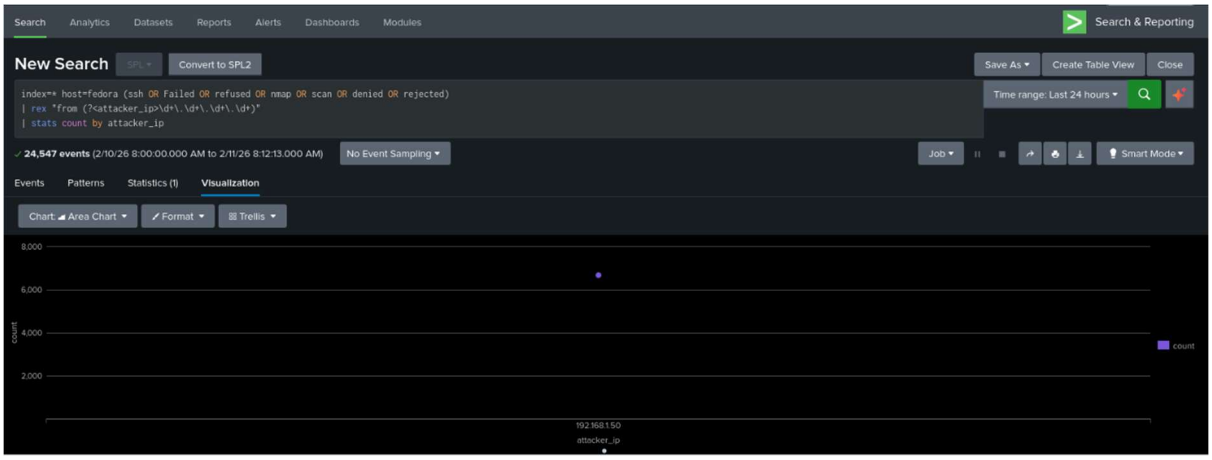

Figure 9:Visualization graph of port scan activity

(Source:Self-created)

The graph highlights a significant volume of suspicious activity originating from the attacker IP, confirming reconnaissance behavior.

7.1 Port Scan Alert

Alert Name: **Port Scan Detected**

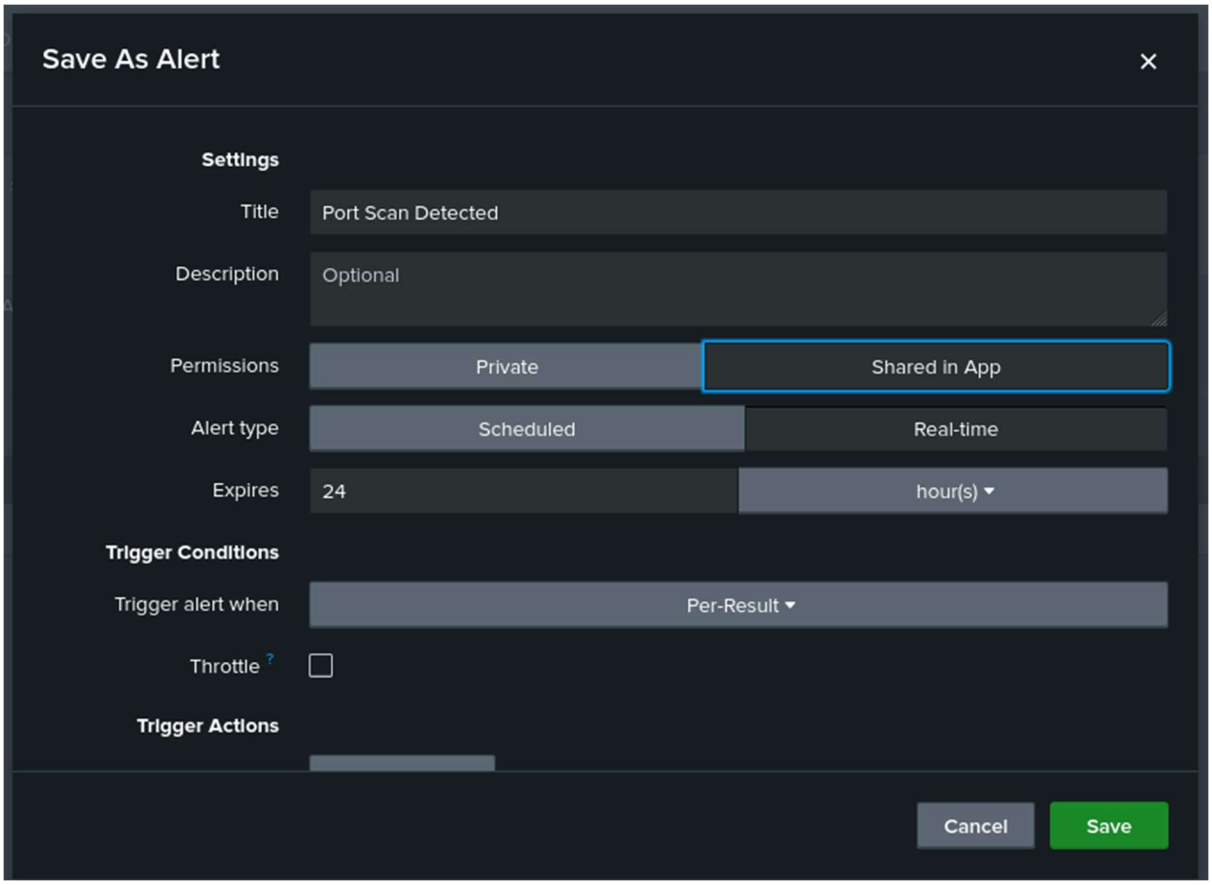

Figure 10:Port Scan alert creation screen

(Source:Self-created)

8.Result

Attack	Attacker IP	Events
Brute Force	192.168.1.50	1228+
Port Scan	192.168.1.50	6677+

9.Security Analysis

The following threat patterns were successfully detected:

Attack	MITRE Technique	Result
SSH Brute Force	T1110	Identified attacker IP
Port Scan	T1046	Detected reconnaissance

10.Security Impact

- Early detection of unauthorized access
- Identification of threat actor IP
- Automated alerting for SOC teams

11.Future Enhacenents

- Geo-IP correlation
- Threat intelligence integration
- SOAR automation
- Dashboards

Conclusion

This SOC simulation successfully demonstrated how SIEM tools like Splunk can detect and alert on real-world cyber threats.
The system effectively identified attacker behavior and generated security alerts, simulating an enterprise SOC workflow.