SIEM PROJECT

SOC ANALYSIS

Author - ANSHUL

Project Overview

This project demonstrates the core functionality of a Security Information and Event Management (SIEM) system by monitoring a Windows server for a brute-force attack initiated from Kali Linux using the tool Hydra. This setup allows you to observe how a SIEM detects, analyzes, and alerts on malicious activity by collecting and correlating logs.

Objectives

The core goal of this project is to set up a SIEM solution to detect and alert on a brute-force attack launched from Kali Linux using the Hydra tool against a Windows server service RDP.

Project architecture

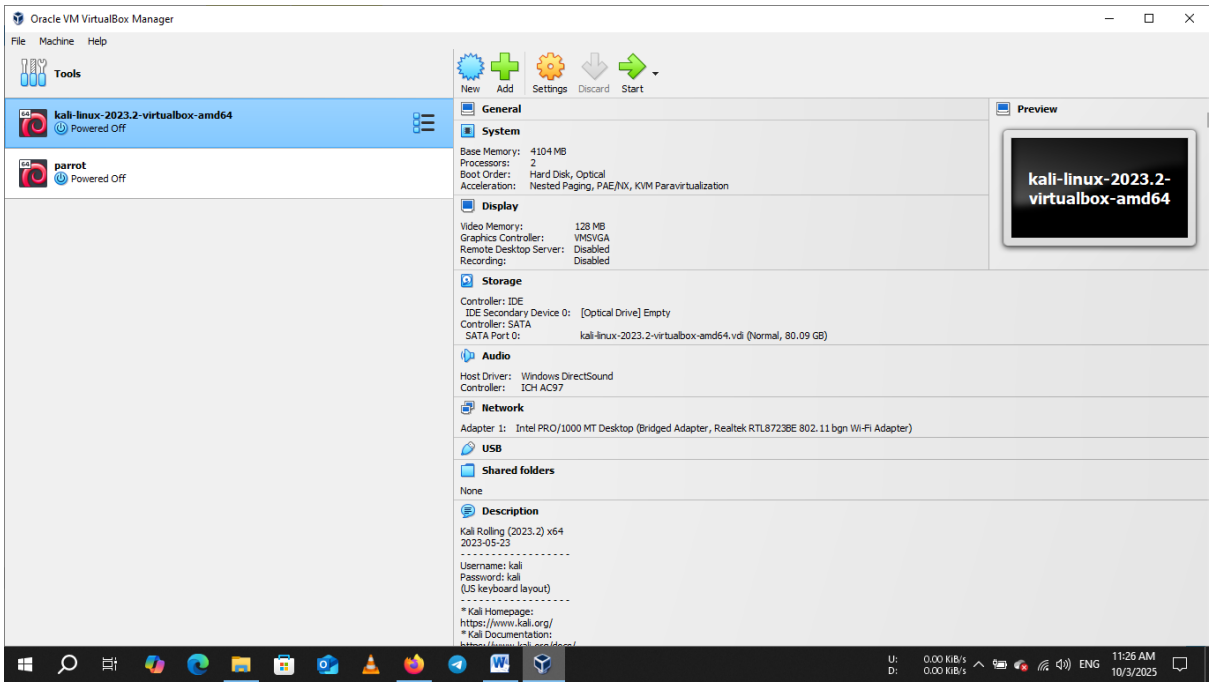
Windows Server: The target of the attack. You will install a log forwarding agent on this machine to send security events to the SIEM.

Kali Linux (Attacker): The source of the brute-force attack. You will use Hydra to attempt multiple login attempts against a service on the Windows Server.

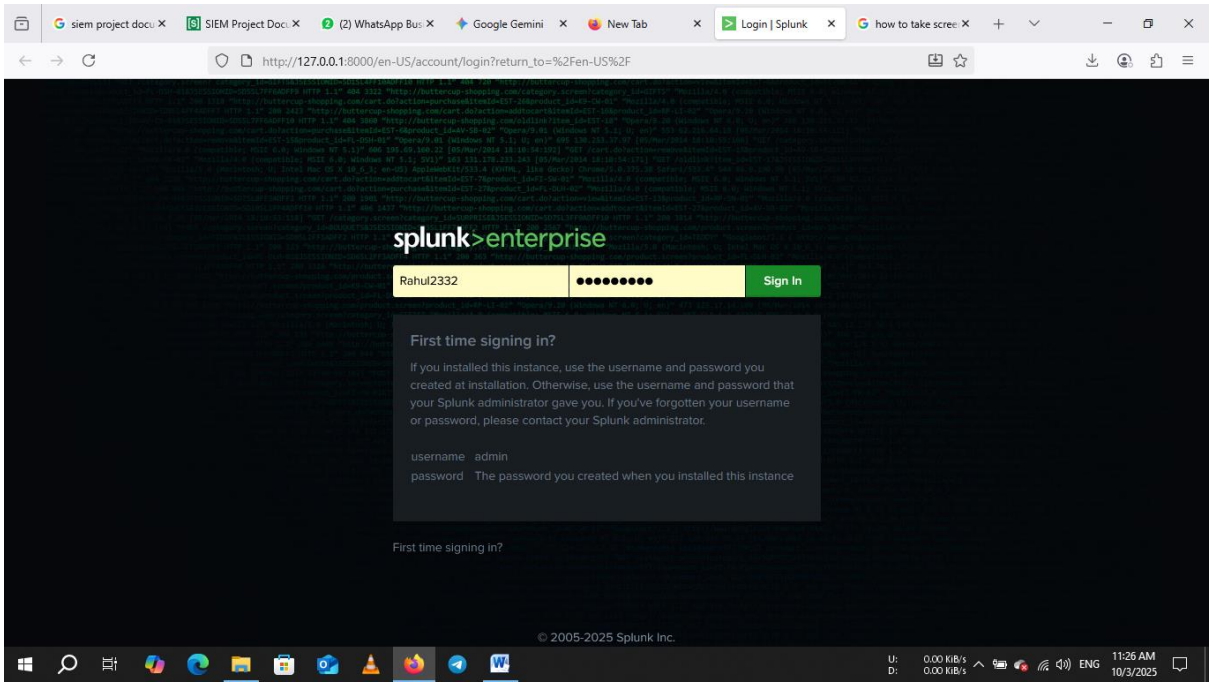
SIEM Platform: The central analysis engine .Collects, analyzes, and visualizes logs from the server.

Lab Setup

- **Virtual Machine Setup:** Create two virtual machines (VMs): one for the Windows Server and one for Kali Linux. Ensure they are on the same virtual network so they can communicate.



- **SIEM Deployment:** Install and configure the SIEM enterprise.



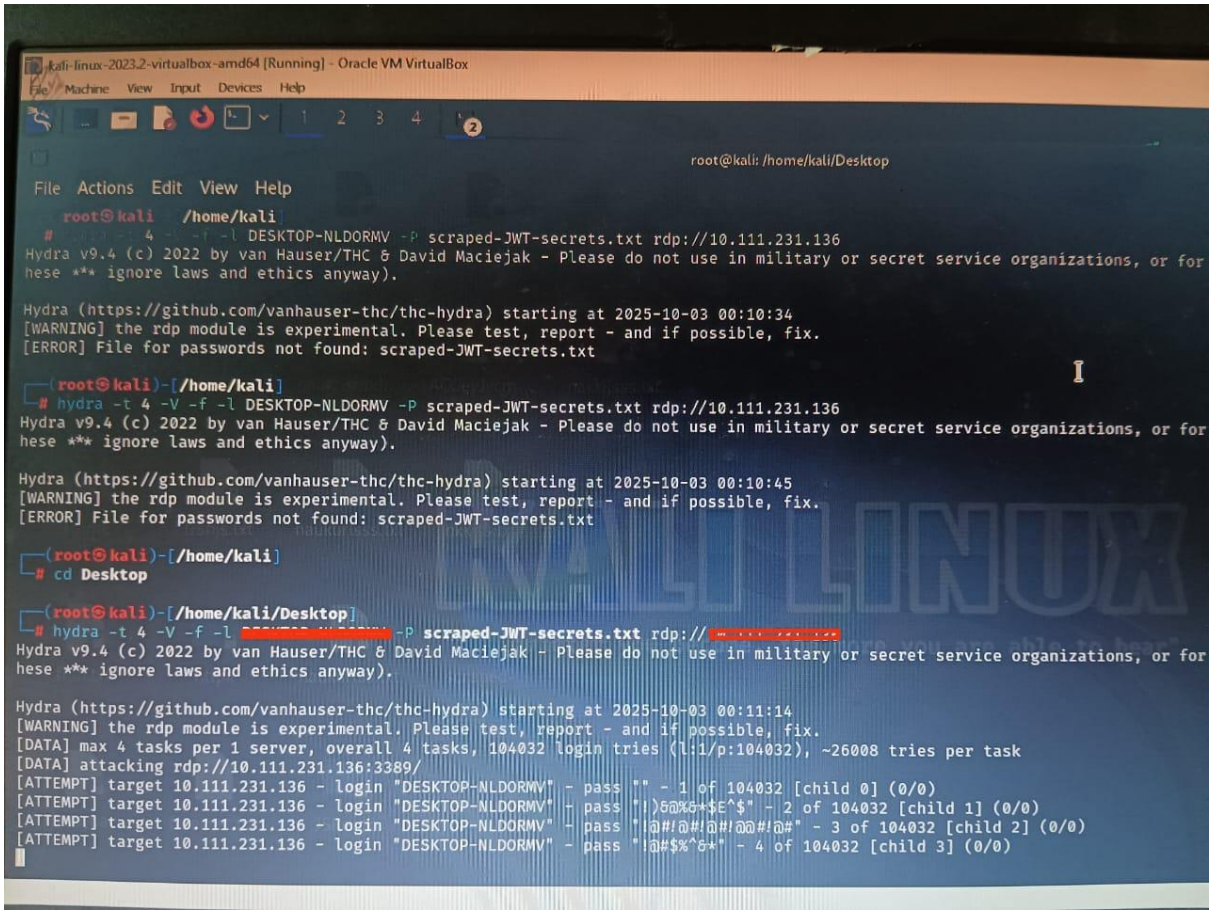
- **Log Forwarding:** Install the Universal forwarder on the Windows Server and configure it to send **Security Event Logs** (specifically failed login attempts) to your SIEM.

Attack Simulation

1. **Identify Target Service:** Choose the RDP service on the Windows server to attack. Common choices include:
    - **RDP (Port 3389):** For remote desktop access credentials.

Launch Hydra Attack: From the Kali Linux VM, use **Hydra** to execute a brute-force attack against the chosen service on the Windows Server's IP address.

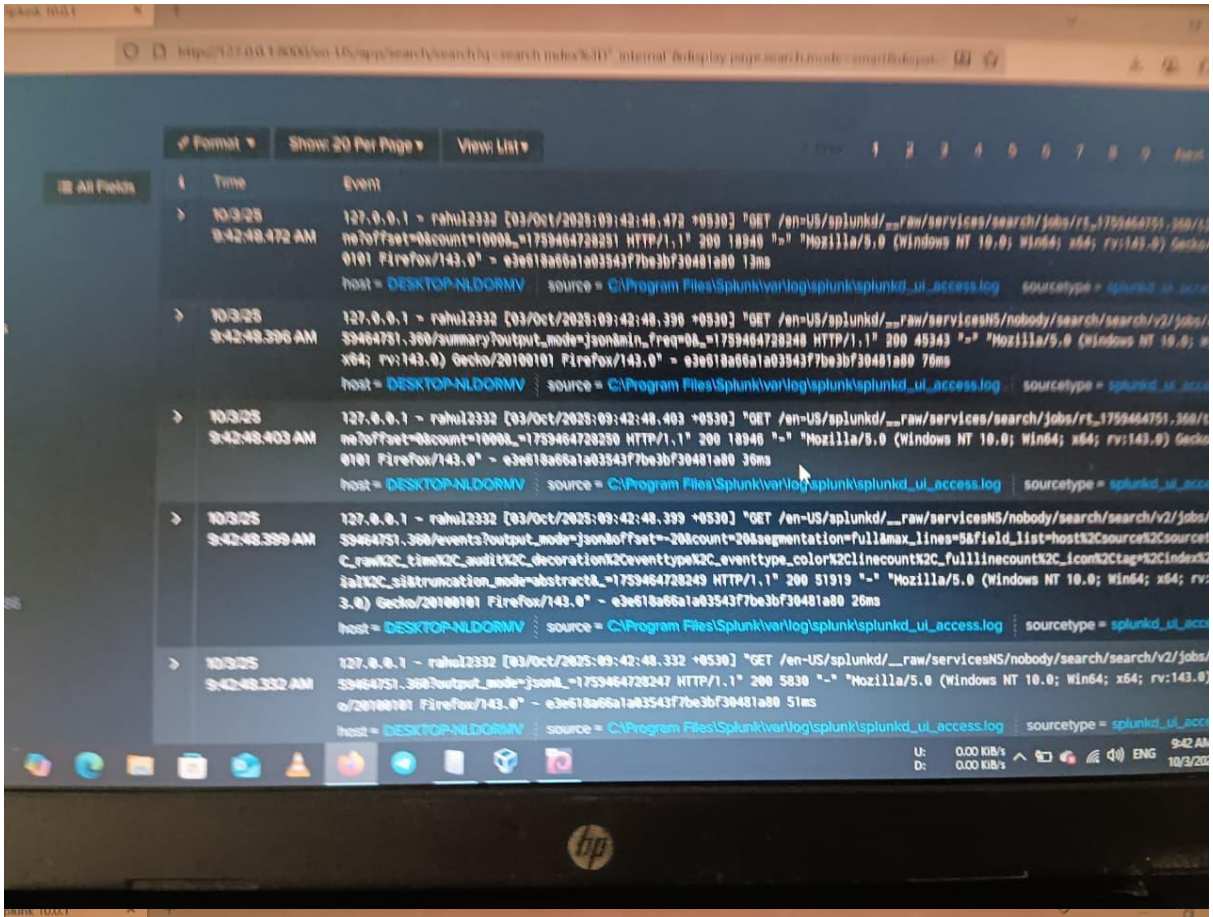
- *Example command (for RDP):* `hydra -L <userlist> -P <passlist> <windows_ip> rdp`

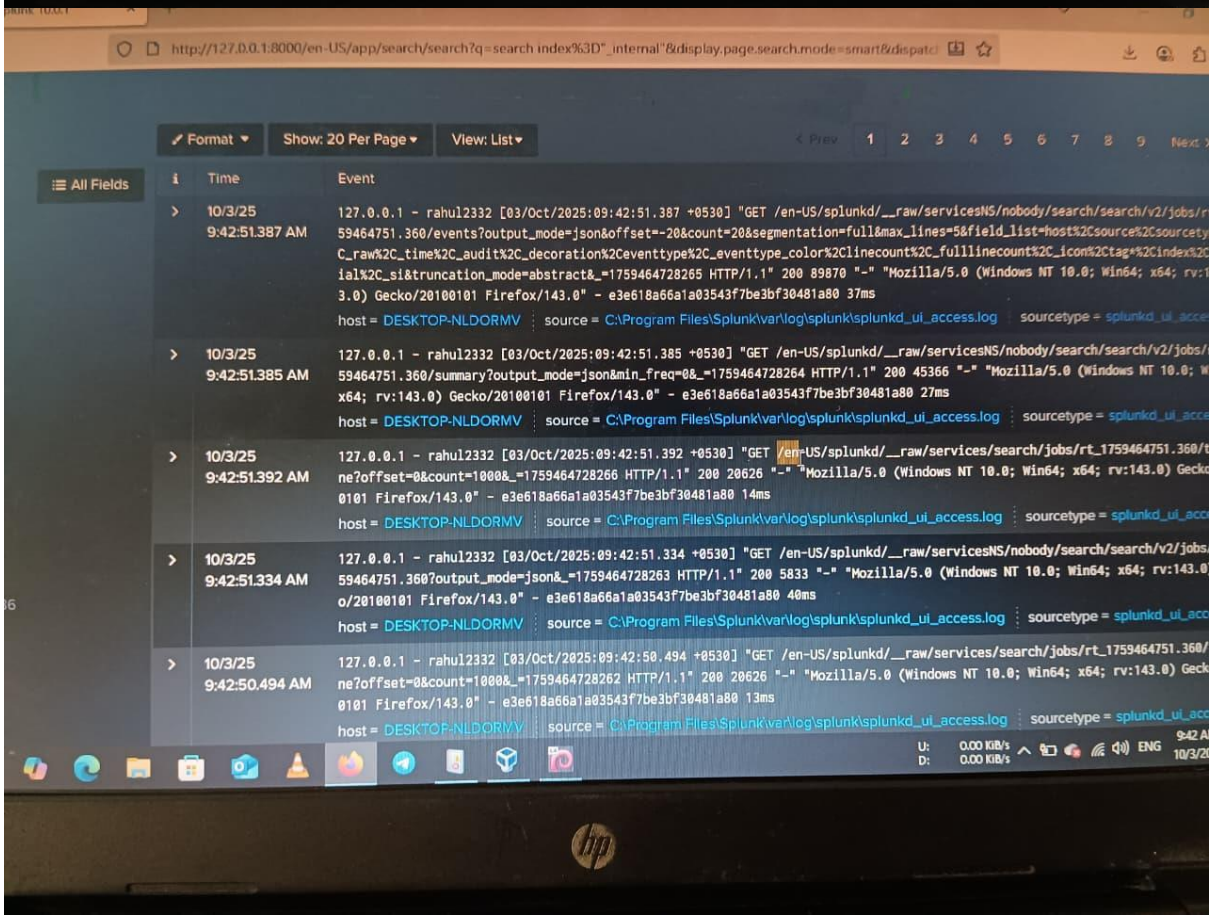


Generate Logs: The Hydra attack will generate a large volume of failed login attempts on the Windows Server, which the log forwarder should capture and send to the SIEM.

Detection and Analysis

Verify Log Ingestion: Check the SIEM to ensure the Windows Security Event Logs are being ingested and indexed. The event IDs for failed logins are crucial (e.g., **Event ID 4625** for failed logon attempts).


Format
Show: 20 Per Page
View: List
All Fields
Time
Event
10/3/25 9:42:48.472 AM
10/3/25 9:42:48.396 AM
10/3/25 9:42:48.403 AM
10/3/25 9:42:48.399 AM
10/3/25 9:42:48.332 AM
host = DESKTOP-NLDORMV
source = C:\Program Files\Splunk\var\log\splunk\splunkd_ui_access.log


http://127.0.0.1:8000/en-US/app/search/search?q=search index%3D"_internal"&display.page.search.mode=smart&dispatch
Format
Show: 20 Per Page
View: List
All Fields
Time
Event
10/3/25 9:42:51.387 AM
10/3/25 9:42:51.385 AM
10/3/25 9:42:51.392 AM
10/3/25 9:42:51.334 AM
10/3/25 9:42:50.494 AM
host = DESKTOP-NLDORMV
source = C:\Program Files\Splunk\var\log\splunk\splunkd_ui_access.log

Analyzing Logs

Analyzing logs of brute force

Using SPL(Search processing language) for indexing

- **Top 10 Events ----**

  index="_internal"| top limit=10 EventCode

- **From which sources it will come -------**

  stats count by SourceName

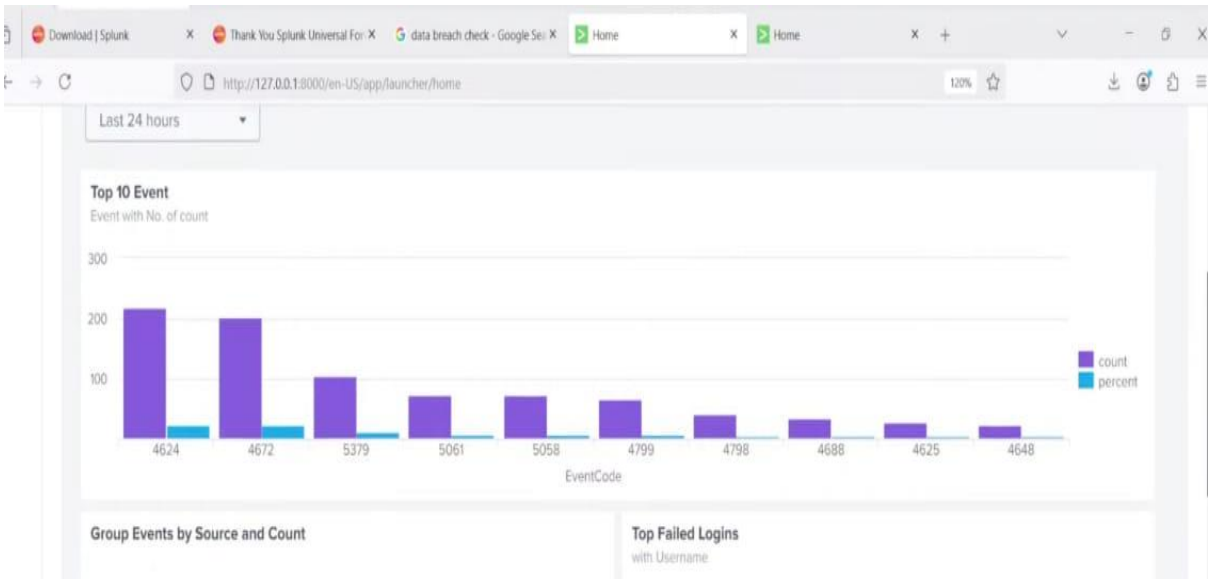
- **how much events will come in which hour ------**

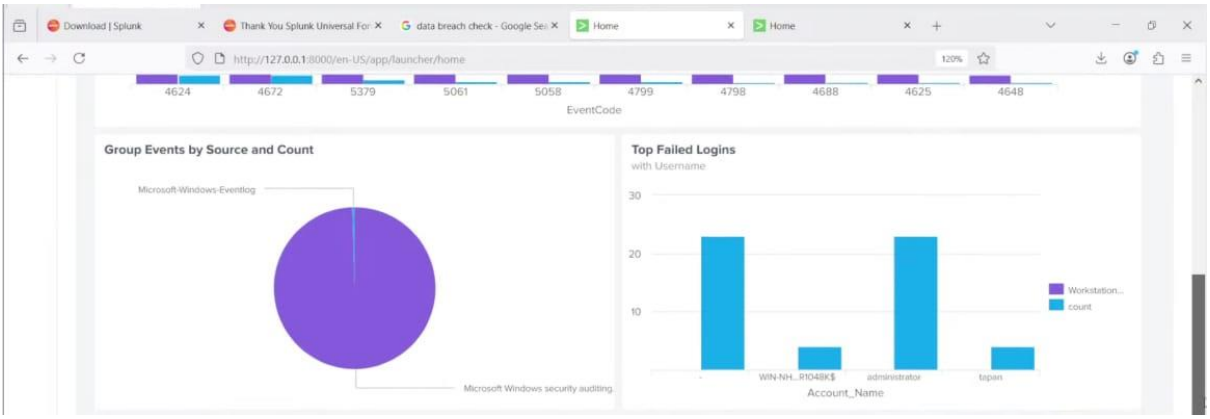
  index="_internal"| timechart span=1h count

- **Filter failed(brute force logs) ----------**

  index="_internal" EventCode=4625

Here the Dashboard/ o/p ----------





Adding Alert's

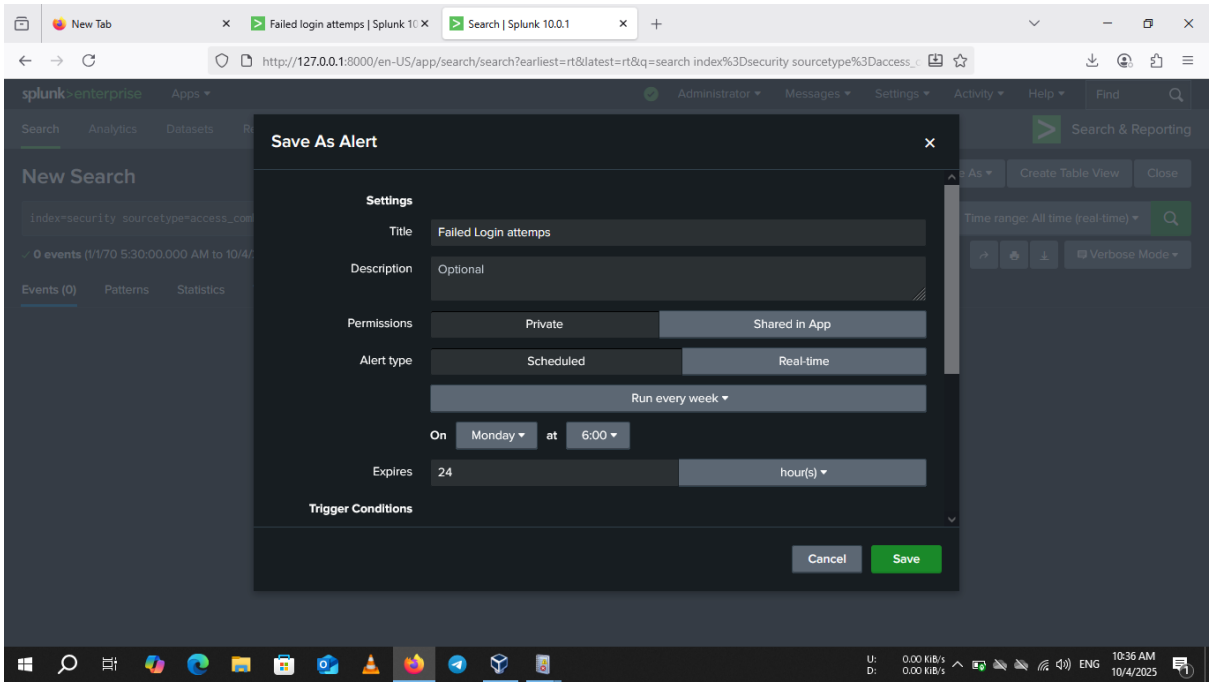
I create a alert to get notify that my server is under attack of a Brute force.

I add a new index script

index=security sourcetype=access_combined status 404

This script describe that if there are more than 5 failed login occur in 1 minute , it will send a alert on my email address.

Configuring panel



Adding email address to get alert