



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

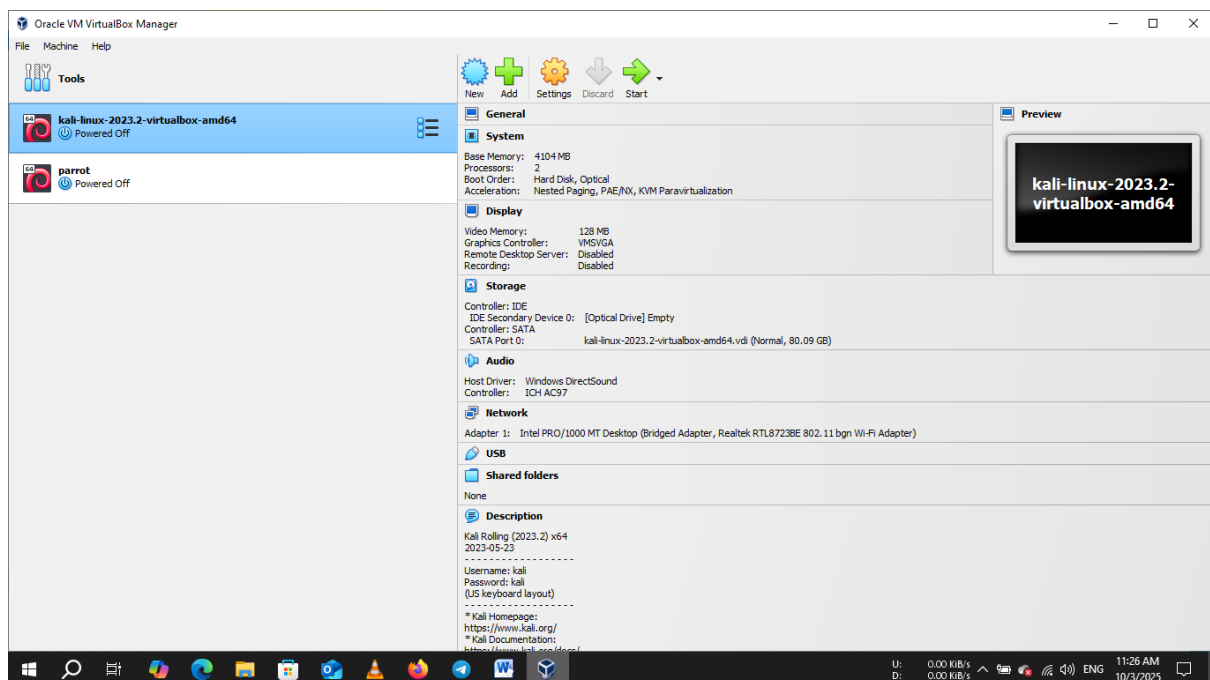
Windows Server: The target of the attack. You will install a log forwarding agent on this machine to send security events to the SIEM.

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.

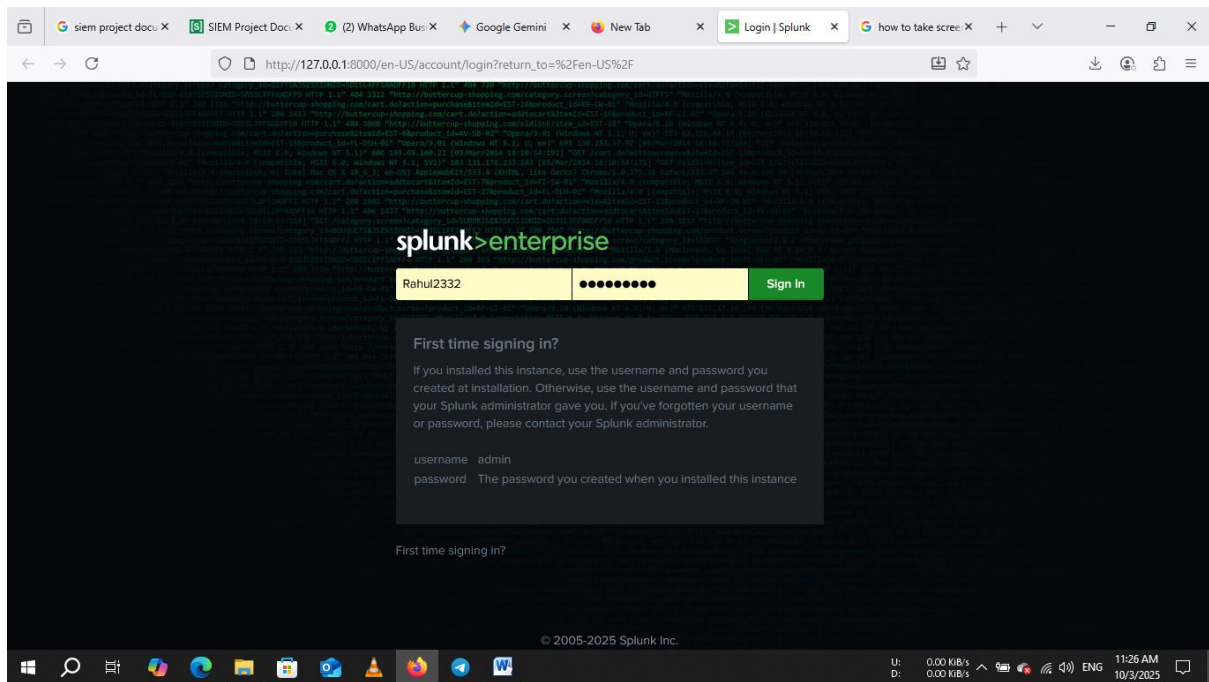
SIEM Platform: The central analysis engine .Collects, analyzes, and visualizes logs from the server.

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`

```
kali-linux-2023.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: /home/kali/Desktop

root@kali ~# hydra -t 4 -f -l DESKTOP-NLDORMV -P scraped-JWT-secrets.txt rdp://10.111.231.136
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for
these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-03 00:10:34
[WARNING] the rdp module is experimental. Please test, report - and if possible, fix.
[ERROR] File for passwords not found: scraped-JWT-secrets.txt

root@kali ~# hydra -t 4 -V -f -l DESKTOP-NLDORMV -P scraped-JWT-secrets.txt rdp://10.111.231.136
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for
these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-03 00:10:45
[WARNING] the rdp module is experimental. Please test, report - and if possible, fix.
[ERROR] File for passwords not found: scraped-JWT-secrets.txt

root@kali ~# cd Desktop
root@kali ~/Desktop# hydra -t 4 -V -f -l DESKTOP-NLDORMV -P scraped-JWT-secrets.txt rdp://10.111.231.136
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for
these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-03 00:11:14
[WARNING] the rdp module is experimental. Please test, report - and if possible, fix.
[DATA] max 4 tasks per 1 server, overall 4 tasks, 104032 login tries (l:1/p:104032), ~26008 tries per task
[DATA] attacking rdp://10.111.231.136:3389/
[ATTEMPT] target 10.111.231.136 - login "DESKTOP-NLDORMV" - pass "" - 1 of 104032 [child 0] (0/0)
[ATTEMPT] target 10.111.231.136 - login "DESKTOP-NLDORMV" - pass "!)50%$+tE^$" - 2 of 104032 [child 1] (0/0)
[ATTEMPT] target 10.111.231.136 - login "DESKTOP-NLDORMV" - pass "i0#i0#i0#i0#i0#" - 3 of 104032 [child 2] (0/0)
[ATTEMPT] target 10.111.231.136 - login "DESKTOP-NLDORMV" - pass "i0#$%0+" - 4 of 104032 [child 3] (0/0)
```

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).

http://127.0.0.1:8000/en-US/app/search/search?q=search%3D%22internal%22&display.page.search.mode=smart&dispatch=

Format Show: 20 Per Page View: List

All Fields	Time	Event
>	10/3/25 9:42:48.472 AM	127.0.0.1 - rahu12332 [03/Oct/2025:09:42:48.472 +0530] "GET /en-US/splunkd/_raw/services/search/jobs/rt_1759464751.360/offset=0&count=1000&_1759464728231 HTTP/1.1" 200 18940 "-" Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:143.0) Gecko/20100101 Firefox/143.0 - e3e618a66a1a03543f7be3bf30481a80 13ms host = DESKTOP-NLDORMV source = C:\Program Files\Splunk\var\log\splunk\splunkd_ui_access.log sourcetype = splunkd_ui_access
>	10/3/25 9:42:48.396 AM	127.0.0.1 - rahu12332 [03/Oct/2025:09:42:48.396 +0530] "GET /en-US/splunkd/_raw/servicesNS/nobody/search/search/v2/jobs/59464751.360/summary?output_mode=json&min_freq=0&_1759464728240 HTTP/1.1" 200 45343 "-" Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:143.0) Gecko/20100101 Firefox/143.0 - e3e618a66a1a03543f7be3bf30481a80 76ms host = DESKTOP-NLDORMV source = C:\Program Files\Splunk\var\log\splunk\splunkd_ui_access.log sourcetype = splunkd_ui_access
>	10/3/25 9:42:48.403 AM	127.0.0.1 - rahu12332 [03/Oct/2025:09:42:48.403 +0530] "GET /en-US/splunkd/_raw/servicesNS/nobody/search/search/v2/jobs/59464751.360/events?output_mode=json&offset=-20&count=20&segmentation=full&max_lines=50&field_list=host%2Csource%2Csourcetype%2Craw%2C_time%2C_audit%2C_decoration%2Ceventtype%2C_eventtype_color%2Clinecount%2C_fulllinecount%2C_icon%2Ctag%2Cindex%2C_ial%2C_sl&truncation_mode=abstract&_1759464728243 HTTP/1.1" 200 51919 "-" Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:143.0) Gecko/20100101 Firefox/143.0 - e3e618a66a1a03543f7be3bf30481a80 26ms host = DESKTOP-NLDORMV source = C:\Program Files\Splunk\var\log\splunk\splunkd_ui_access.log sourcetype = splunkd_ui_access
>	10/3/25 9:42:48.332 AM	127.0.0.1 - rahu12332 [03/Oct/2025:09:42:48.332 +0530] "GET /en-US/splunkd/_raw/servicesNS/nobody/search/search/v2/jobs/59464751.360/output_mode=json&_1759464728247 HTTP/1.1" 200 5830 "-" Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:143.0) Gecko/20100101 Firefox/143.0 - e3e618a66a1a03543f7be3bf30481a80 51ms host = DESKTOP-NLDORMV source = C:\Program Files\Splunk\var\log\splunk\splunkd_ui_access.log sourcetype = splunkd_ui_access

U: 0.00 KiB/s D: 0.00 KiB/s 9:42 AM 10/3/25

http://127.0.0.1:8000/en-US/app/search/search?q=search%3D%22internal%22&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	127.0.0.1 - rahu12332 [03/Oct/2025:09:42:51.387 +0530] "GET /en-US/splunkd/_raw/servicesNS/nobody/search/search/v2/jobs/rt_1759464751.360/events?output_mode=json&offset=-20&count=20&segmentation=full&max_lines=50&field_list=host%2Csource%2Csourcetype%2Craw%2C_time%2C_audit%2C_decoration%2Ceventtype%2C_eventtype_color%2Clinecount%2C_fulllinecount%2C_icon%2Ctag%2Cindex%2C_ial%2C_sl&truncation_mode=abstract&_1759464728265 HTTP/1.1" 200 89870 "-" Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:143.0) Gecko/20100101 Firefox/143.0 - e3e618a66a1a03543f7be3bf30481a80 37ms host = DESKTOP-NLDORMV source = C:\Program Files\Splunk\var\log\splunk\splunkd_ui_access.log sourcetype = splunkd_ui_access
>	10/3/25 9:42:51.385 AM	127.0.0.1 - rahu12332 [03/Oct/2025:09:42:51.385 +0530] "GET /en-US/splunkd/_raw/servicesNS/nobody/search/search/v2/jobs/59464751.360/summary?output_mode=json&min_freq=0&_1759464728264 HTTP/1.1" 200 45366 "-" Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:143.0) Gecko/20100101 Firefox/143.0 - e3e618a66a1a03543f7be3bf30481a80 27ms host = DESKTOP-NLDORMV source = C:\Program Files\Splunk\var\log\splunk\splunkd_ui_access.log sourcetype = splunkd_ui_access
>	10/3/25 9:42:51.392 AM	127.0.0.1 - rahu12332 [03/Oct/2025:09:42:51.392 +0530] "GET /en-US/splunkd/_raw/servicesNS/nobody/search/search/v2/jobs/59464751.360/output_mode=json&_1759464728266 HTTP/1.1" 200 20626 "-" Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:143.0) Gecko/20100101 Firefox/143.0 - e3e618a66a1a03543f7be3bf30481a80 14ms host = DESKTOP-NLDORMV source = C:\Program Files\Splunk\var\log\splunk\splunkd_ui_access.log sourcetype = splunkd_ui_access
>	10/3/25 9:42:51.334 AM	127.0.0.1 - rahu12332 [03/Oct/2025:09:42:51.334 +0530] "GET /en-US/splunkd/_raw/servicesNS/nobody/search/search/v2/jobs/59464751.360/output_mode=json&_1759464728263 HTTP/1.1" 200 5833 "-" Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:143.0) Gecko/20100101 Firefox/143.0 - e3e618a66a1a03543f7be3bf30481a80 40ms host = DESKTOP-NLDORMV source = C:\Program Files\Splunk\var\log\splunk\splunkd_ui_access.log sourcetype = splunkd_ui_access
>	10/3/25 9:42:50.494 AM	127.0.0.1 - rahu12332 [03/Oct/2025:09:42:50.494 +0530] "GET /en-US/splunkd/_raw/services/search/jobs/rt_1759464751.360/offset=0&count=1000&_1759464728262 HTTP/1.1" 200 20626 "-" Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:143.0) Gecko/20100101 Firefox/143.0 - e3e618a66a1a03543f7be3bf30481a80 13ms host = DESKTOP-NLDORMV source = C:\Program Files\Splunk\var\log\splunk\splunkd_ui_access.log sourcetype = splunkd_ui_access

U: 0.00 KiB/s D: 0.00 KiB/s 9:42 AM 10/3/25

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

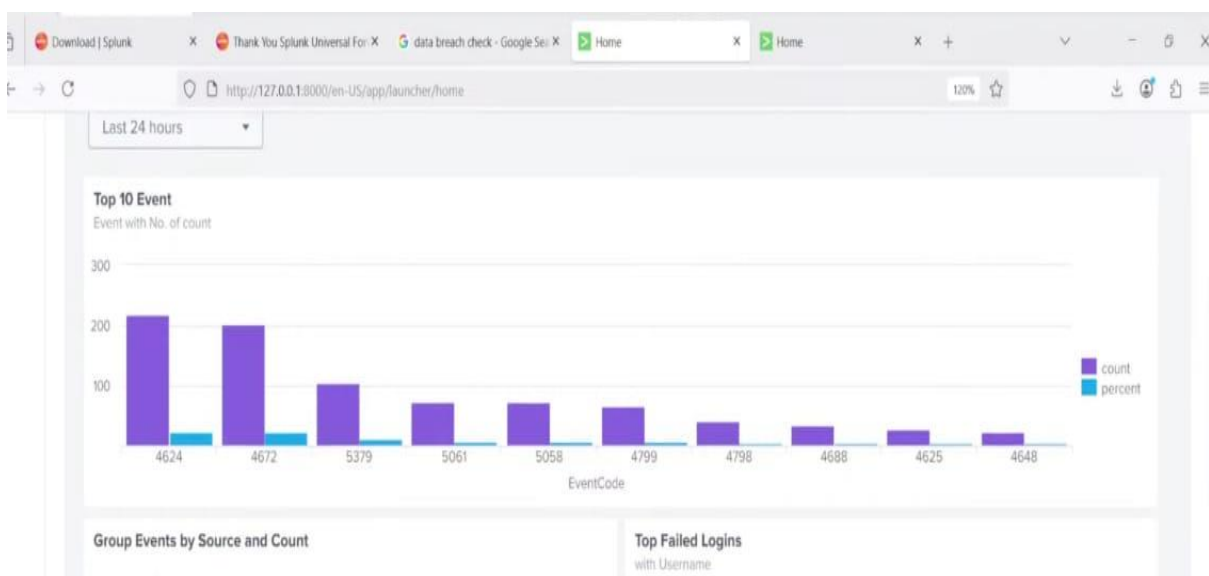
- **how much events will come in which hour -----**

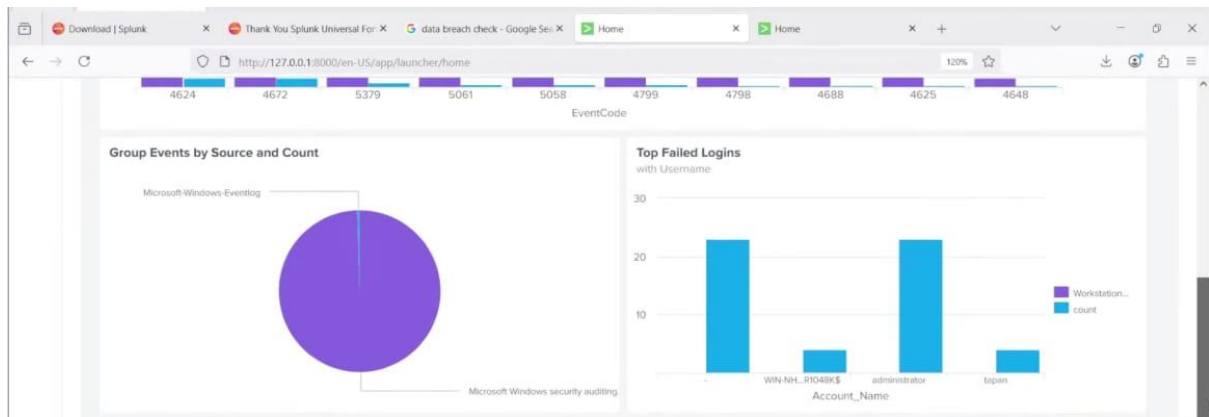
index="_internal"| timechart span=1h count

- **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

The screenshot shows the 'Save As Alert' configuration window in Splunk. The window is titled 'Failed Login attempts' and is configured with the following settings:

- Title:** Failed Login attempts
- Description:** Optional
- Permissions:** Private
- Alert type:** Scheduled
- Run every week**
- On:** Monday at 6:00
- Expires:** 24 hour(s)
- Trigger Conditions:** (Empty)

The window includes 'Cancel' and 'Save' buttons at the bottom right.

Adding email address to get alert

