Name: Aditee Srivastava

Roll Number: 23BCE11417

Course / Department: Cyber Security analyst / VIT btech

Project Title: Active Cyber Defense: Real-Time Threat Detection and Response with a Splunk-Based SIEM

Executive Summary

This project demonstrates a complete, end-to-end cybersecurity incident response cycle within a controlled virtual lab. The primary goal was to address the challenge of delayed threat detection by building a mini-Security Operations Center (SOC) using professional tools. A lab environment was created with an attacker (Kali Linux), a victim server (Ubuntu Server), and a central monitoring station (Splunk Enterprise). A simulated brute-force attack was launched, successfully detected in real-time by Splunk through log analysis, and then actively blocked at the victim's firewall. The key result was the successful validation of an integrated detect-and-respond workflow, proving that with proper monitoring, threats can be identified and neutralized swiftly.

Project Overview

- **Problem Statement:** In many network environments, malicious activities like brute-force login attempts go unnoticed until it's too late. This lack of real-time visibility provides attackers with a large window of opportunity to compromise systems. This project addresses the need for active monitoring and immediate response capabilities.

- **Objectives:**

1. To build a functional virtual lab simulating an attacker and a target server.
2. To configure Splunk to ingest and analyze security logs from the target in real-time.
3. To simulate a common SSH brute-force attack.
4. To detect the attack using Splunk queries and then contain the threat using host-based firewall rules.

- **Scope of Work:**
  - Included: The simulation of one specific attack type (SSH brute-force), real-time log forwarding and analysis, and a manual, host-level response to the threat, Ubuntu server as target server.
  - Excluded: Automated alerting, statistical analysis with Splunk's stats command, network-level firewalls, and in-depth forensic analysis, Metasploitable2 as target server.

Tools & Lab Setup

- **Primary Tools Used:** VirtualBox, Kali Linux, Ubuntu Server, Splunk Enterprise, Splunk Universal Forwarder, Hydra, iptables.

- **Environment Details:**
    1. Virtual Machine Setup: Oracle VM VirtualBox
    2. Target VM: Ubuntu Server (version 18.04 LTS)
    3. Network Mode: NAT Network

- **Tool Configuration & Commands (if any):**
    - Splunk Forwarder Configuration (on Ubuntu-victim): After downloading the Splunk forwarder on ubuntu:
        - Unpack the file: tar -xvzf splunk.tgz
        - Go into the bin directory: cd splunkforwarder/bin
        - Start Splunk: ./splunk start --accept-license
        - Tell it where my Windows PC's Splunk server is: ./splunk add forward-server 10.0.2.2:9997
        - Tell it to watch the login log file: ./splunk add monitor /var/log/auth.log
        - Restart the forwarder: ./splunk restart

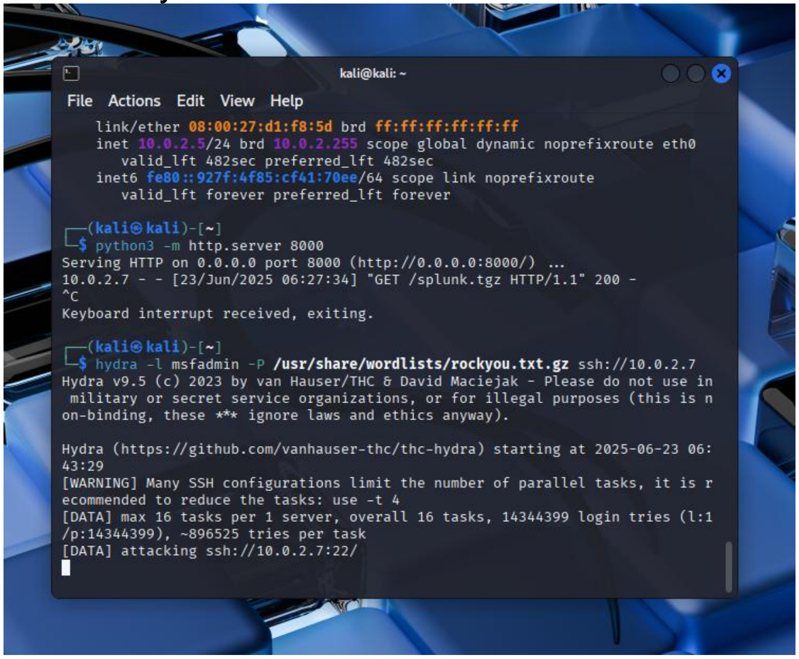
    - Hydra attack Command: hydra -l msfadmin -P /usr/share/wordlists/rockyou.txt.gz ssh://10.0.2.7
    - Firewall Response Command: sudo iptables -A INPUT -s <Attacker_IP> -j DROP

Implementation & Execution Summary

The project was executed by first setting up two virtual machines, Kali Linux and Ubuntu Server, on a NAT Network to ensure connectivity. The Splunk Universal Forwarder was installed and configured on the Ubuntu server to send its authentication logs (auth.log) to a custom index on the main Splunk Enterprise instance. An SSH brute-force attack was then launched from the Kali VM using Hydra. This activity was monitored in Splunk, where a query was used to isolate the "Failed password" events and identify the attacker's source IP. Finally, a response was executed by logging into the Ubuntu server and using an iptables rule to block all incoming traffic from the identified malicious IP, successfully neutralizing the threat.

Screenshots :

➔ **The Attack**: The Kali Linux terminal showing the hydra command running successfully for the first time.



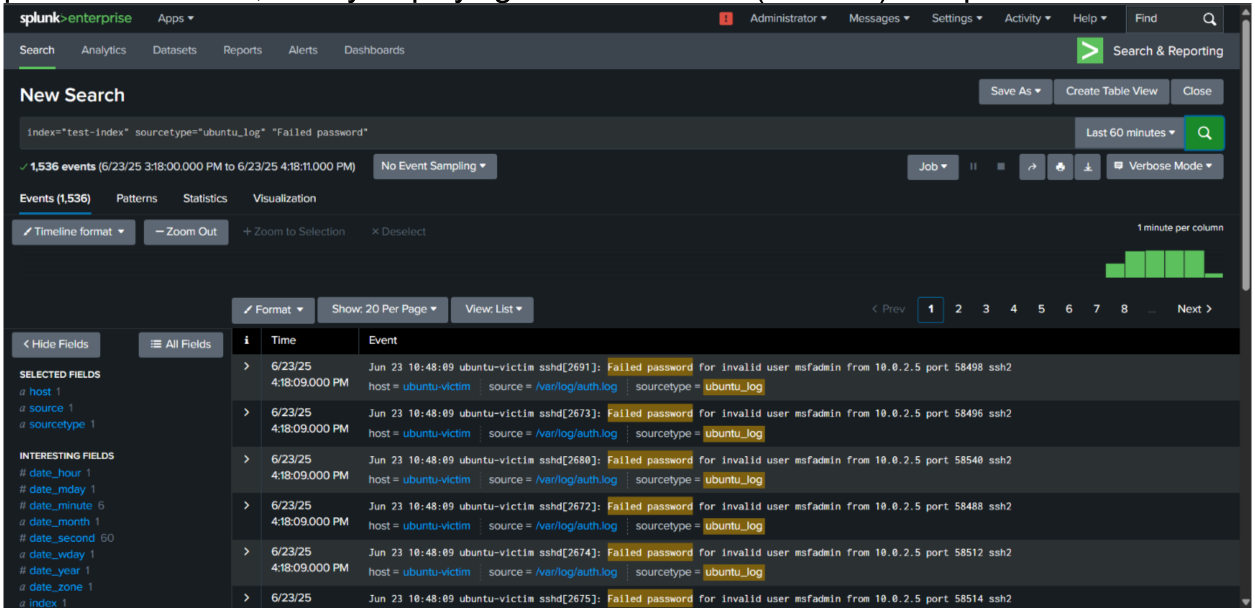
```
    link/ether 08:00:27:d1:f8:5d brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.5/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
       valid_lft 482sec preferred_lft 482sec
    inet6 fe80::927f:4f85:cf41:70ee/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(kali㉿kali)-[~]
└─$ python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.0.2.7 - - [23/Jun/2025 06:27:34] "GET /splunk.tgz HTTP/1.1" 200 -
^C
Keyboard interrupt received, exiting.

┌──(kali㉿kali)-[~]
└─$ hydra -l msfadmin -P /usr/share/wordlists/rockyou.txt.gz ssh://10.0.2.7
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in
 military or secret service organizations, or for illegal purposes (this is n
on-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-06-23 06:
43:29
[WARNING] Many SSH configurations limit the number of parallel tasks, it is r
ecommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1
/p:14344399), ~896525 tries per task
[DATA] attacking ssh://10.0.2.7:22/
```

➔ **The Detection**: The Splunk search results showing the list of raw "Failed password" events, clearly displaying the attacker's IP (10.0.2.5) multiple times.



New Search

```
index="test-index" sourcetype="ubuntu_log" "Failed password"
```

✓ 1,536 events (6/23/25 3:18:00.000 PM to 6/23/25 4:18:11.000 PM)

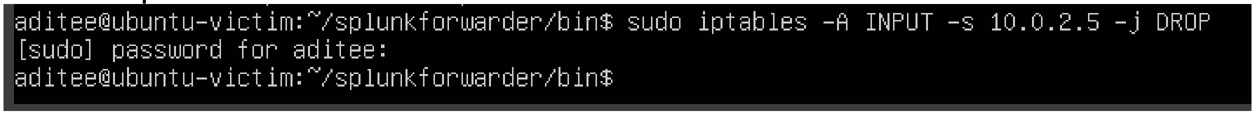
Events (1,536)

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
# date_hour 1
# date_mday 1
# date_minute 6
a date_month 1
# date_second 60
a date_wday 1
# date_year 1
a date_zone 1
a index 1

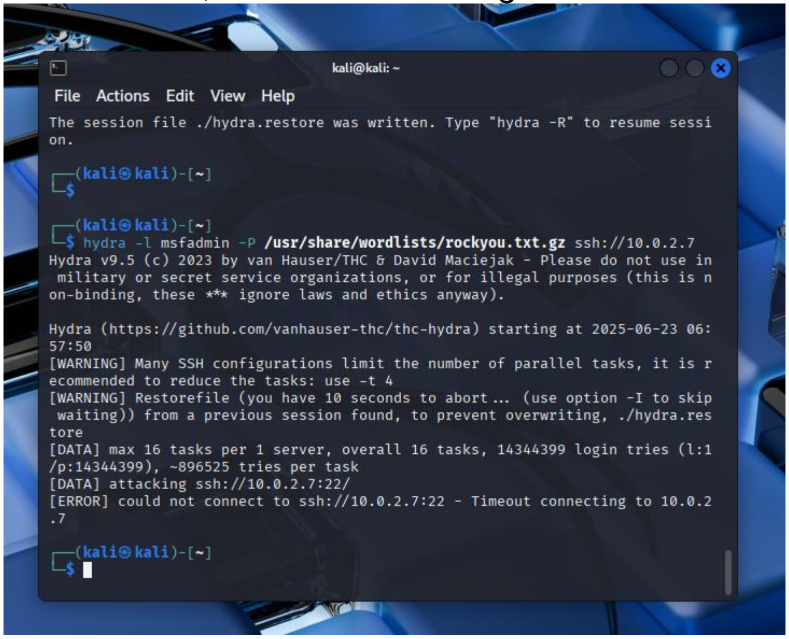
i	Time	Event
›	6/23/25 4:18:09.000 PM	Jun 23 10:48:09 ubuntu-victim sshd[2691]: Failed password for invalid user msfadmin from 10.0.2.5 port 58498 ssh2 host = ubuntu-victim source = /var/log/auth.log sourcetype = ubuntu_log
›	6/23/25 4:18:09.000 PM	Jun 23 10:48:09 ubuntu-victim sshd[2673]: Failed password for invalid user msfadmin from 10.0.2.5 port 58496 ssh2 host = ubuntu-victim source = /var/log/auth.log sourcetype = ubuntu_log
›	6/23/25 4:18:09.000 PM	Jun 23 10:48:09 ubuntu-victim sshd[2680]: Failed password for invalid user msfadmin from 10.0.2.5 port 58540 ssh2 host = ubuntu-victim source = /var/log/auth.log sourcetype = ubuntu_log
›	6/23/25 4:18:09.000 PM	Jun 23 10:48:09 ubuntu-victim sshd[2672]: Failed password for invalid user msfadmin from 10.0.2.5 port 58488 ssh2 host = ubuntu-victim source = /var/log/auth.log sourcetype = ubuntu_log
›	6/23/25 4:18:09.000 PM	Jun 23 10:48:09 ubuntu-victim sshd[2674]: Failed password for invalid user msfadmin from 10.0.2.5 port 58512 ssh2 host = ubuntu-victim source = /var/log/auth.log sourcetype = ubuntu_log
›	6/23/25	Jun 23 10:48:09 ubuntu-victim sshd[2675]: Failed password for invalid user msfadmin from 10.0.2.5 port 58514 ssh2

➔ **The Response**: The Ubuntu-Victim terminal showing the successful execution of the sudo iptables ... command to block the attacker's IP.



```
aditee@ubuntu-victim:~/splunkforwarder/bin$ sudo iptables -A INPUT -s 10.0.2.5 -j DROP
[sudo] password for aditee:
aditee@ubuntu-victim:~/splunkforwarder/bin$
```

➔ **The Verification**: The Kali Linux terminal showing the hydra command being run a second time, but this time resulting in a "Timeout" or connection error.



```
The session file ./hydra.restore was written. Type "hydra -R" to resume sessi
on.

┌──(kali㉿kali)-[~]
└─$

┌──(kali㉿kali)-[~]
└─$ hydra -l msfadmin -P /usr/share/wordlists/rockyou.txt.gz ssh://10.0.2.7
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in
 military or secret service organizations, or for illegal purposes (this is n
on-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-06-23 06:
57:50
[WARNING] Many SSH configurations limit the number of parallel tasks, it is r
ecommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip
 waiting)) from a previous session found, to prevent overwriting, ./hydra.res
tore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1
/p:14344399), ~896525 tries per task
[DATA] attacking ssh://10.0.2.7:22/
[ERROR] could not connect to ssh://10.0.2.7:22 - Timeout connecting to 10.0.2
.7

┌──(kali㉿kali)-[~]
└─$
```

Challenges Faced

The project encountered significant initial setup challenges. The original target VM, Metasploitable2, proved incompatible with modern 64-bit tools, causing kernel panics and preventing the installation of the Splunk Forwarder. This required a strategic pivot to a modern Ubuntu Server VM. Additionally, network configuration was a major hurdle, with Bridged mode failing on the college Wi-Fi due to client isolation, forcing a reconfiguration to a more robust NAT Network setup. These challenges highlighted the importance of adaptability and thorough troubleshooting in a real-world IT environment.

Findings & Analysis

The technical findings were clear and successful. The Hydra attack generated over a thousand "Failed password" log entries in the auth.log file, which were successfully ingested by Splunk in real-time. Analysis of the raw log events in Splunk **(as shown in Screenshot #2)** provided direct evidence of the attack, clearly showing the repetitive nature of the failed attempts and consistently identifying the attacker's IP address (10.0.2.x) as the source. The subsequent iptables firewall rule was 100% effective, as verified by the immediate connection timeout on the second attack attempt **(Screenshot #4)**. This demonstrates a direct cause-and-effect relationship between the attack, its detection via raw log analysis, and its successful mitigation.

Learning Outcomes

Technically, this project provided hands-on experience with SIEM implementation, log forwarding, virtual networking (NAT vs. Bridged), Linux server administration, and the use of both offensive (Hydra) and defensive (iptables) command-line tools. Professionally, the project was a powerful lesson in perseverance and systematic troubleshooting. Overcoming the initial VM and network failures taught the critical skill of adapting a project plan when tools or environments are incompatible—a common occurrence in the cybersecurity field.

Future Scope

This project could be enhanced in several ways. An immediate next step would be to build upon the raw log search by creating a Splunk Alert that automatically sends an email when more than 10 "Failed password" events from the same IP occur in one minute. For a more advanced setup, the manual iptables response could be automated using a SOAR (Security Orchestration, Automation, and Response) tool. Finally, the scope could be broadened to monitor other data sources, like web server logs, to detect a wider variety of threats.