SOC ANALYST REPORT
(Practical)

MAHENDRANATHREDDY NARPALA

LinkedIn Profile

Phone: +91 7995886401

Operating System: Kali Linux

Tools used: Splunk

February 1, 2025

Contents

Practical Challenges

Task 1: Log Analysis and Anomaly Detection

- **Question:** How can you identify abnormal login attempts on a network using log data?
- **Task:** Collect logs from a Windows/Linux server using free tools like OSQuery or Sysmon. Import the logs into a SIEM tool like Splunk (Free version) or ELK Stack. Write a query to detect abnormal login attempts (e.g., multiple failed login attempts in a short period).
- **Tools:** OSQuery, Sysmon, Splunk Free, ELK Stack.

Answer:

To identify abnormal login attempts on a network using log data, follow these key steps:

- **Collect Logs:** Gather login logs from relevant systems like servers, firewalls, and applications. Ensure logs capture details such as user IDs, timestamps, IP addresses, login results (success or failure), and device information.
- **Detect Failed Login Patterns:** Look for multiple failed login attempts in a short span, as this could indicate a brute-force attack. Unusual patterns, like 10 failed attempts in 5 minutes, stand out because normal users rarely fail so often consecutively.
- **Monitor Logins from Unusual Locations:** Identify logins from IP addresses or locations that deviate from a user's normal activity, such as foreign countries, especially if the user consistently logs in from a specific region.
- **Check for Logins at Odd Hours:** Spot logins that occur at times outside the user's regular work hours, such as late at night, which could signal unauthorized access.
- **Analyze IP Addresses:** Investigate logins from known suspicious or blacklisted IP addresses. Cross-reference these IPs with threat intelligence databases to identify potential risks.
- **Track Multiple Logins from Different Locations:** If a user account logs in simultaneously from geographically distant locations, it may indicate the account has been compromised.
- **Examine Unusual Devices or Browsers:** Keep an eye on logins from unfamiliar devices or browsers that a user doesn't typically use. A sudden change could be a sign of unauthorized access.

By following these steps and analyzing login patterns, you can spot abnormal login behaviors and protect the network from potential threats.

Step 1: Install Splunk on Kali Linux

To install Splunk on Kali Linux, follow these steps:

0.0.1 Download Splunk

Use the following command to download Splunk:

```
sudo wget -O splunk-9.3.0-51ccf43db5bd-Linux-x86_64.tgz \
https://download.splunk.com/products/splunk/releases/9.3.0/linux/splunk-9.3.0-51ccf43db5bd-Linux
```

0.0.2 Extract Splunk

Extract the downloaded file with this command:

```
sudo tar -xvzf splunk-9.3.0-51ccf43db5bd-Linux-x86_64.tgz -C /opt
```

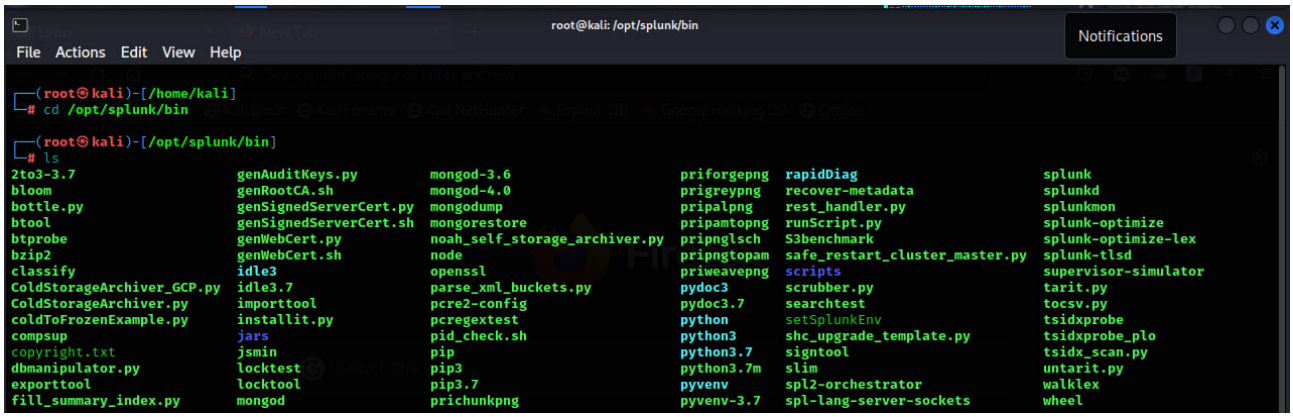

Figure 1: splunk extraction

0.0.3 Start Splunk

Start Splunk and accept the license:

```
sudo /opt/splunk/bin/splunk start --accept-license
```

0.0.4 Enable Splunk on Boot

Enable Splunk to start on boot with:

```
sudo /opt/splunk/bin/splunk enable boot-start
```

0.0.5 Start, Stop, and Restart Splunk

To start Splunk:

`sudo /opt/splunk/bin/splunk start`

To stop Splunk:

`sudo /opt/splunk/bin/splunk stop`

To restart Splunk:

`sudo /opt/splunk/bin/splunk restart`

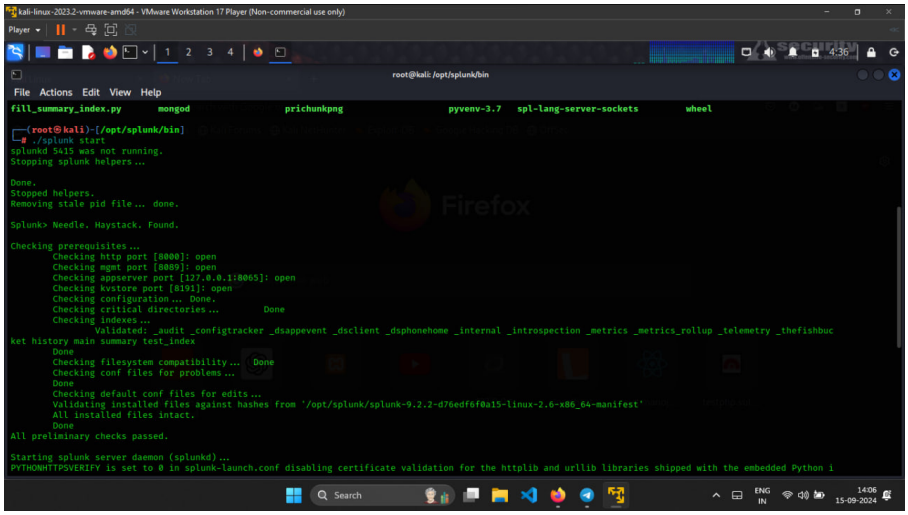

Figure 2: splunk start

0.0.6 Access Splunk Web Interface

After starting Splunk, access the web interface at: `http://localhost:8000`

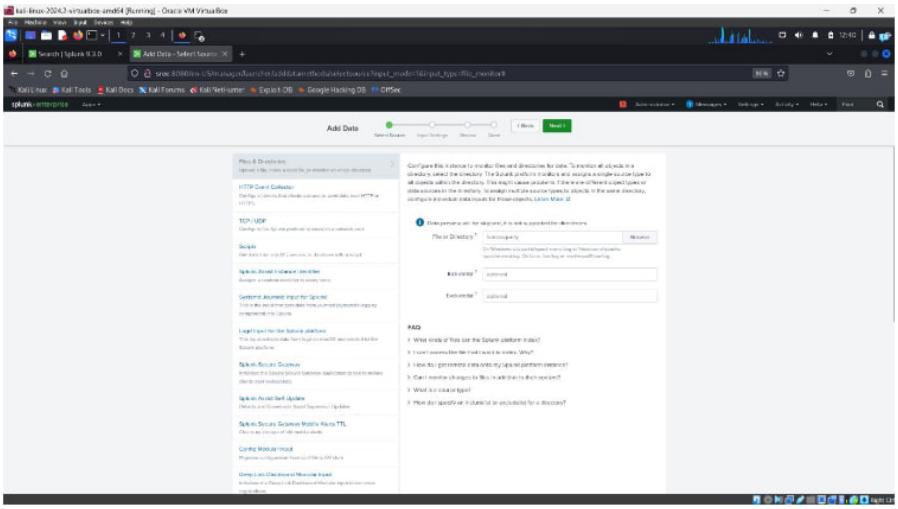

Figure 3: splunk website

Step 2: Install and Configure OSQuery

To install and configure OSQuery on Kali Linux:

0.0.7 Install OSQuery

Update the package list and install OSQuery with:

```
sudo apt-get update
sudo apt-get install osquery
```

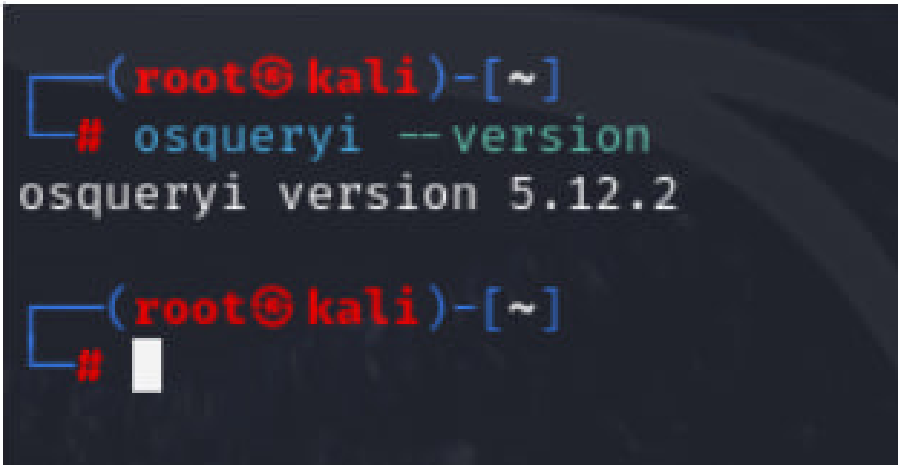

Figure 4: osquery version

0.0.8 Configure OSQuery

Create or modify the OSQuery configuration file:

```
sudo nano /etc/osquery/osquery.conf
```

Add the following configuration:

```
{
  "schedule": {
    "failed_logins": {
      "query": "SELECT * FROM last WHERE event = 'login';",
      "interval": 3600
    }
  }
}
```

0.0.9 Restart OSQuery

Restart the OSQuery service with:

```
sudo systemctl restart osqueryd
```

Figure 5: osquery data

Step 3: Import OSQuery Logs into Splunk

To import OSQuery logs into Splunk:

0.0.10 Configure Splunk to Receive OSQuery Logs

1. Open the Splunk web interface.
2. Navigate to `Settings > Data inputs > Files and Directories`.
3. Click `Add New` and specify the OSQuery logs directory, e.g., `/var/log/osquery/`.

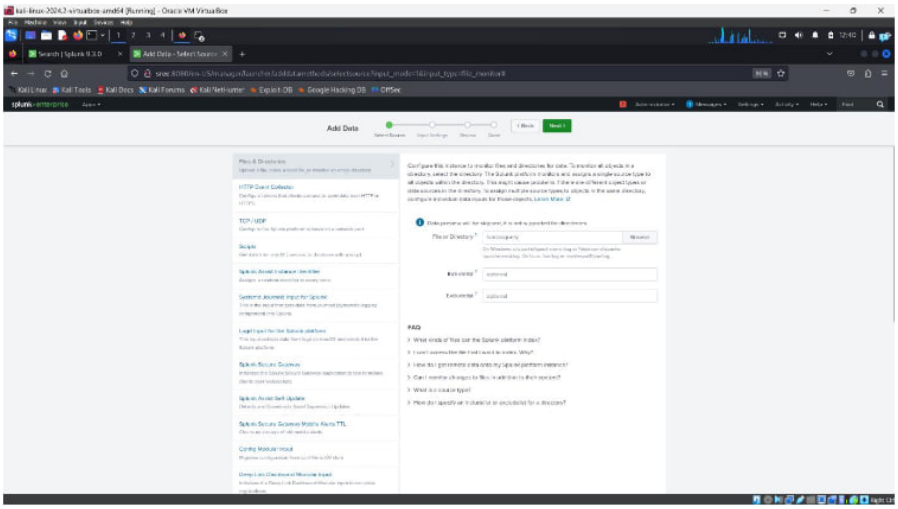

Figure 6: osquery data

Step 4: Analyze OSQuery Logs in Splunk

0.0.11 View OSQuery Logs

Use the following query in Splunk to view all OSQuery logs:

```
source="/var/log/osquery/*" host="<your-hostname>"
```

0.0.12 Detect Abnormal Login Attempts

To find failed login attempts, use the following query:

```
source="/var/log/osquery/*" host="<your-hostname>" Fail*
```

Notes:

- The query ‘Fail*‘ searches for logs containing the word ‘Fail‘, representing failed login attempts.
- Adjust the ‘host‘ parameter to match your specific hostname.

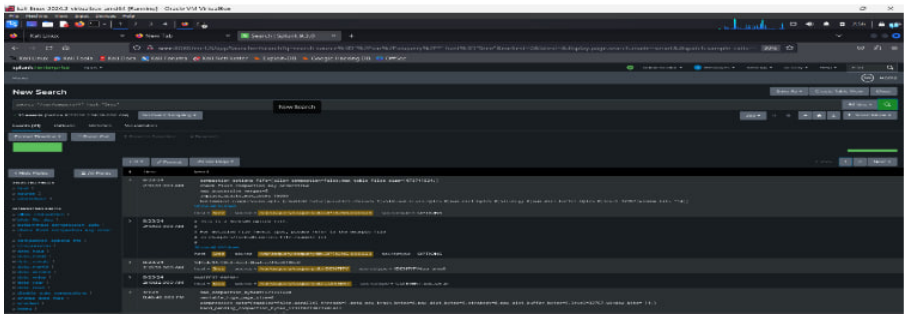

Figure 7: osquery data

Step 5: Analyze Results

After running the query, examine the log events detailing failed login attempts. Investigate repeated failed attempts or other unusual behaviors to identify potential unauthorized access.

Task 2: Threat Hunting with Open-Source Tools:

- **Question:** How can you proactively detect malware using threat hunting techniques?
- **Task:** Use OSQuery or Sysmon to monitor system behavior and network traffic. Look for signs of malware, such as unusual process execution or outbound traffic to suspicious IP addresses. Create custom queries to detect potential indicators of compromise (IOCs).
- **Tools:** OSQuery, Sysmon, Wireshark.

Answer:

Detecting malware proactively through threat hunting is like being a vigilant security guard who inspects a building for hidden threats before they cause damage. Here's how it works in simple terms:

- Understand Normal Activity: First, you need to get familiar with what normal looks like on your network. This means knowing how your computers, servers, and applications usually perform.
- Spot the Unusual: With a clear picture of what's normal, you start looking for anything that stands out—like unexpected files, apps that are using too much memory, or strange connections to unfamiliar websites. These are your warning signs.
- Use Smart Tools: Threat hunters rely on advanced tools like antivirus software, firewalls, and machine learning to scan for these anomalies. It's like using a high-tech flashlight to explore hidden areas.
- Investigate Further: If you come across something suspicious, you dig deeper. You check if it's a known malware or if it's trying to conceal its presence.
- Take Action: Once you verify that it's malware, you act quickly to remove it and strengthen your defenses to stop it from coming back.

By actively hunting for threats, you're not waiting for malware to strike—you're actively searching for potential dangers before they can cause harm. This proactive approach helps keep your system safer and ensures a faster response to any threats.

0.0.13 Installation:

- osquery: You've installed osquery on your virtual machine.
- Wireshark: Since Wireshark comes pre-installed with Kali Linux, you should have it ready to go.

0.0.14 Starting osquery:

The command sudo osqueryi is typically used to start the interactive shell for osquery. You can use this command to run osquery queries interactively.

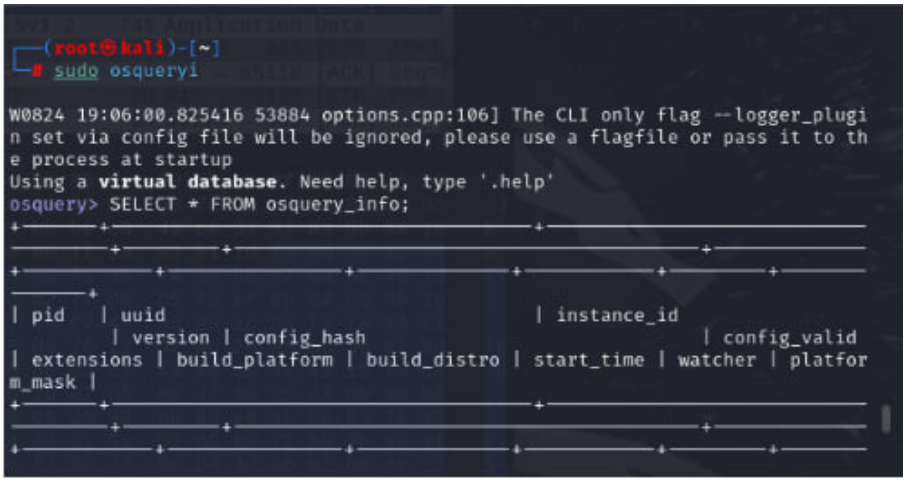

Figure 8: osquery data

- created a file by using command: sudo nano /etc/osquery/osquery.conf

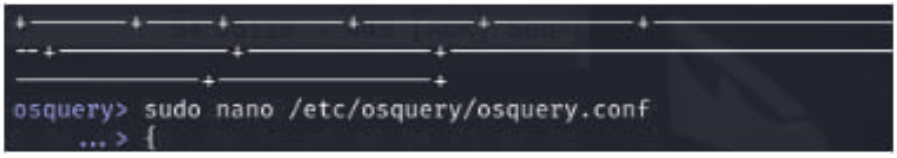

Figure 9: osquery

- Configuration Example: Here's a basic example of what might be included in your osquery.conf file:

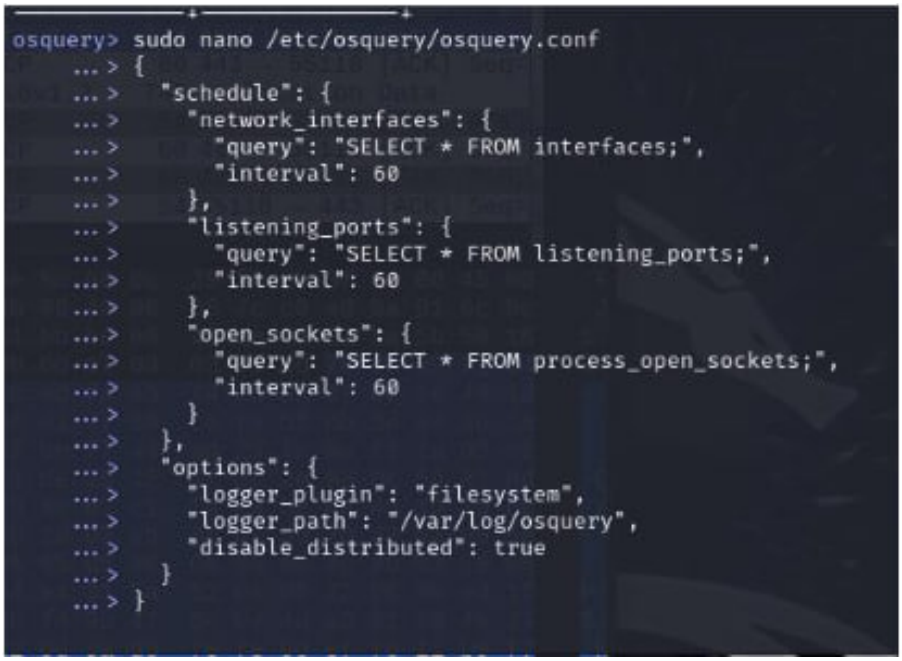

Figure 10: osquery

- restart my osquery using the command:sudo systemctl restart osqueryd

Figure 11: osquery

0.0.15 Wireshark

As soon as I entered this command, a task manager menu appeared, allowing me to view and control the processes and applications currently running on my computer.

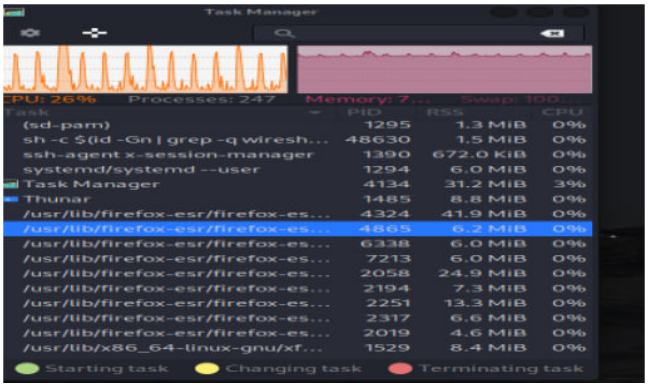

Figure 12: panel

- used my wireshark to capture traffic on eth0

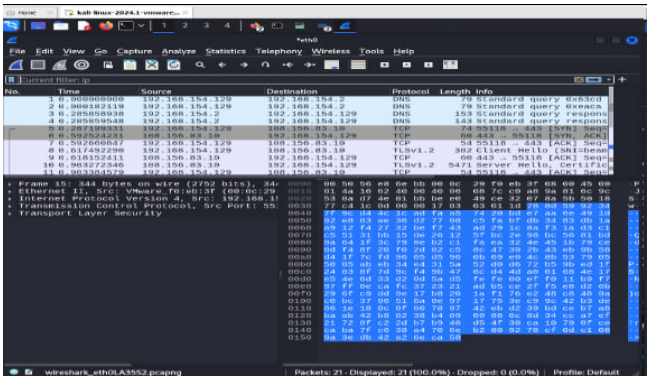

Figure 13: panel

After that I went back to my terminal and used the command promt to check for the logs being captured

- sudo tail -f /var/log/osquery/osqueryd.results.log

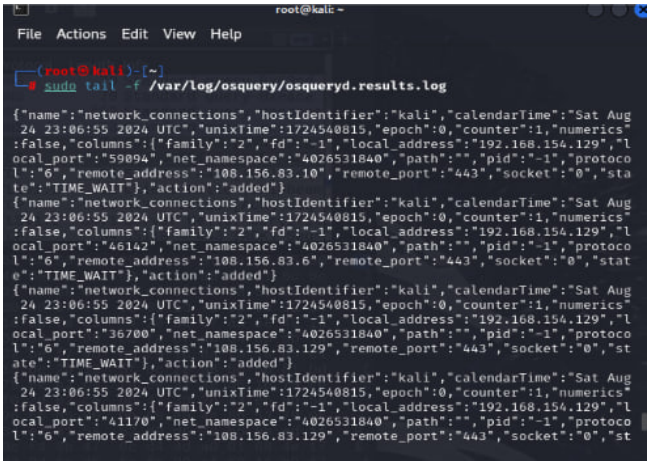

Figure 14: osquery

- To create a custom query for detecting potential IoCs, specifically suspicious processes:
- Create a file to save your custom query.In this file, input a query to list processes with their PID, name, and path. For example:

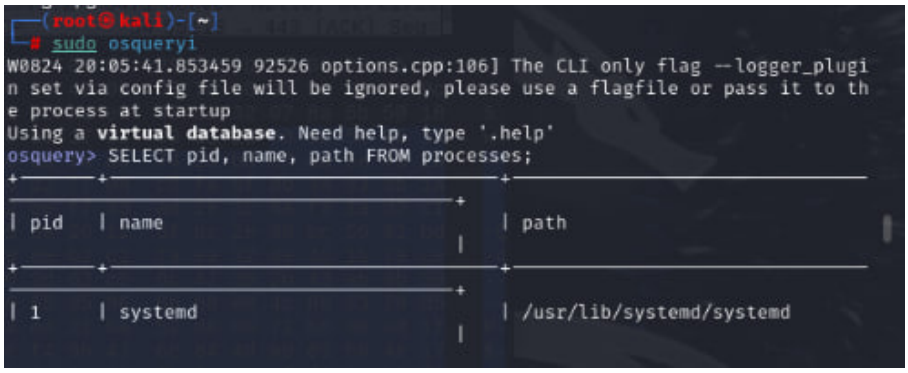

Figure 15: osquery

- Detecting Unusual Network Connections
- To find unusual network connections, which could also indicate an IoC:
- Run Query in osquery:
- The query in the file is shown below

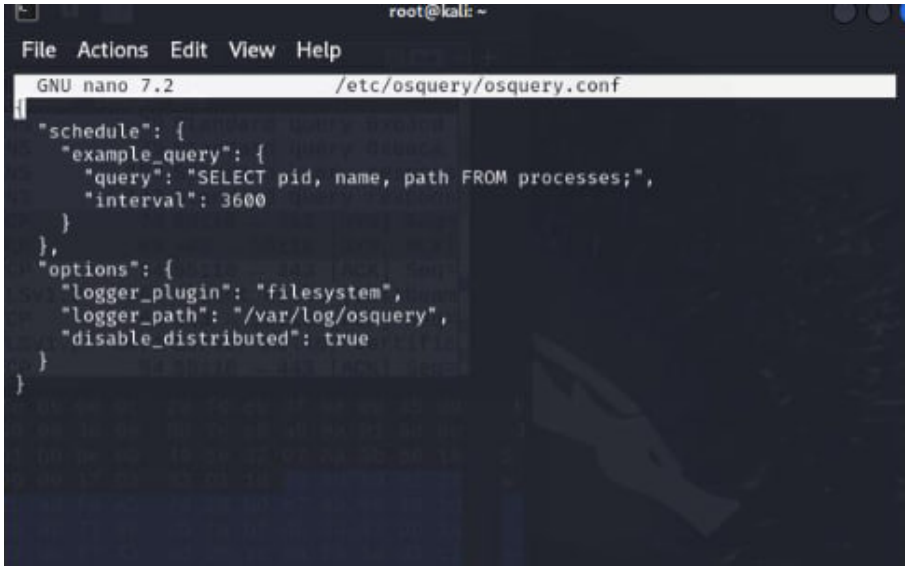

Figure 16: osquery

- To detect unusual network connections, which could be an indicator of compromise (IoC), you can use the following osquery command:
- SELECT * FROM listeningports WHERE port > 25;

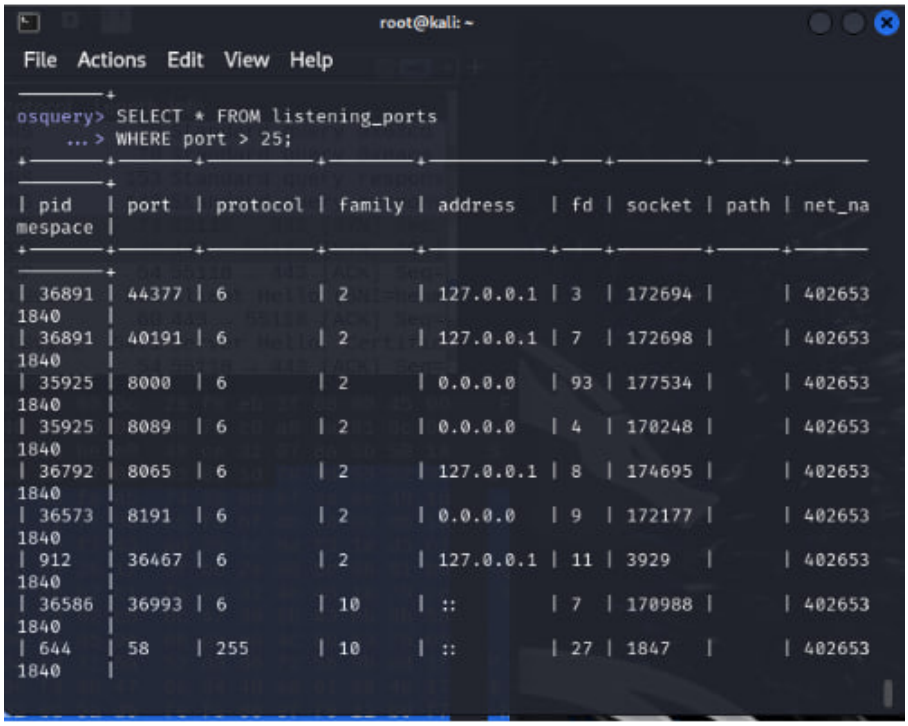

Figure 17: osquery

Task 3: Network Traffic Analysis:

- **Question:** How can you detect suspicious network traffic that might indicate a cyber attack?
- **Task:** Capture network traffic using Wireshark. Analyze the traffic to identify signs of a potential attack, such as port scanning, abnormal DNS queries, or unexpected outbound traffic. Document your findings and propose mitigation steps.
- **Tools:** Wireshark, Nmap.

Answer:

Effective Methods for Detecting Suspicious Network Traffic:

- Signature-Based Detection This method identifies attacks by recognizing predefined patterns in network traffic, such as malicious instructions or known byte sequences. These patterns, or signatures, are stored in a database, and when traffic matches a signature, it's flagged as suspicious. Limitations: It struggles to detect new or unknown attacks since they don't have existing signatures.
- Behavior-Based Detection (Anomaly-Based or Heuristic Detection)

  This approach focuses on identifying unknown attacks by detecting abnormal behavior or deviations from normal network activity. Machine learning algorithms are often used to spot unusual patterns in traffic that could signal a cyber attack.

  Advantage: It excels in detecting new and evolving threats that do not yet have signatures.
- Unusual Traffic Patterns Sudden increases in traffic volume or traffic coming from unknown or untrusted sources may indicate an attack. For instance, if a company with remote employees in Lagos suddenly experiences network requests from Ghana or sees a system jump from consuming 2 MB per second to 25 MB per second, this could signal a DDoS attack or other suspicious activity.
- Too Many Failed Login Attempts There are two common types of attacks involving failed logins: Brute Force Attack: Multiple failed attempts from the same IP or user account could signal a brute force attempt to crack passwords. Password Spraying: Attackers attempt a common password across multiple accounts to gain access without triggering too many failed attempts on a single account.
- Port Scanning Attackers often scan open ports to find vulnerabilities. Monitoring for unauthorized or excessive port scanning activity can reveal potential threats. Commonly scanned ports include: HTTP (80) HTTPS (443) Telnet (23) SSH (22)
- Log Analysis Regularly reviewing logs for unusual patterns, errors, or anomalies is essential for detecting suspicious traffic. SIEM (Security Information and Event Management) systems, firewall logs, and syslogs should be continuously monitored for irregularities.
- Traffic Analysis Establishing a baseline for normal network traffic is crucial. Any deviations, such as unusual protocol usage or unexpected traffic types, can indicate suspicious activity. Consistently monitoring traffic helps detect deviations that could signal a cyber attack.

- Network Security Devices Devices such as firewalls, Web Application Firewalls (WAF), Next-Generation Firewalls (NGFW), and Network Access Control (NAC) should be used to filter and block malicious traffic. WAFs specifically help defend against attacks like SQL injection and cross-site scripting (XSS). Tools like Wireshark for deep packet inspection and monitoring outbound traffic for data exfiltration can provide valuable insights into potentially malicious activities.

Task:

- Using Wireshark on Kali Linux to analyze network traffic is a great way to monitor and detect potential security threats

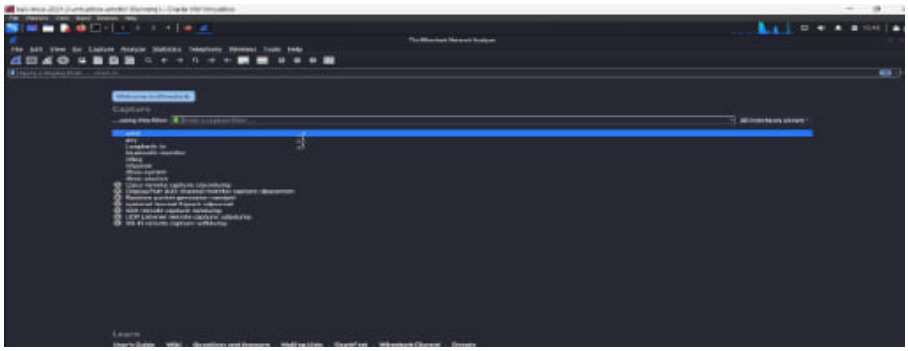

Figure 18: Wireshark

- By visiting websites like Google, Facebook, and Twitter while running a Wireshark capture, you'll generate a lot of network traffic. Here's what would typically happen during your capture:

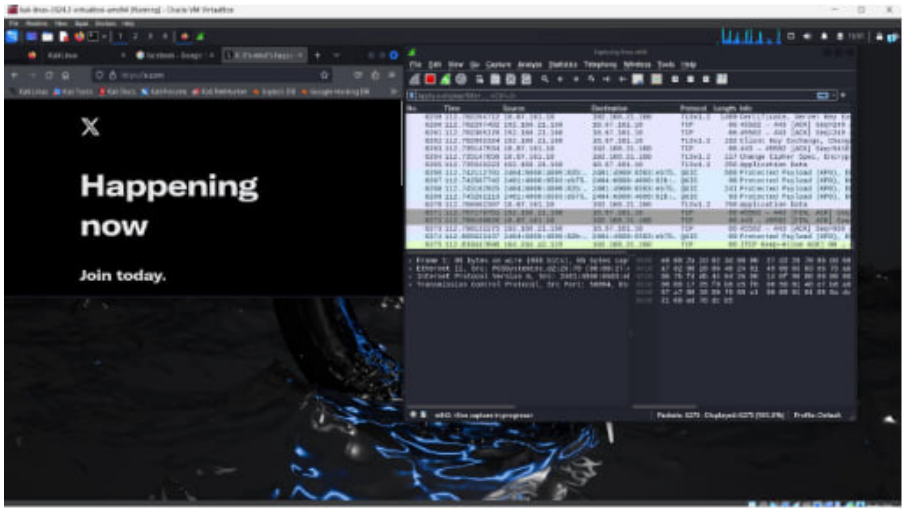

Figure 19: Wireshark

- By applying the tcp filter in Wireshark, you're narrowing down the captured traffic to only show packets using the Transmission Control Protocol (TCP). Here's what you'll likely observe and what it means:

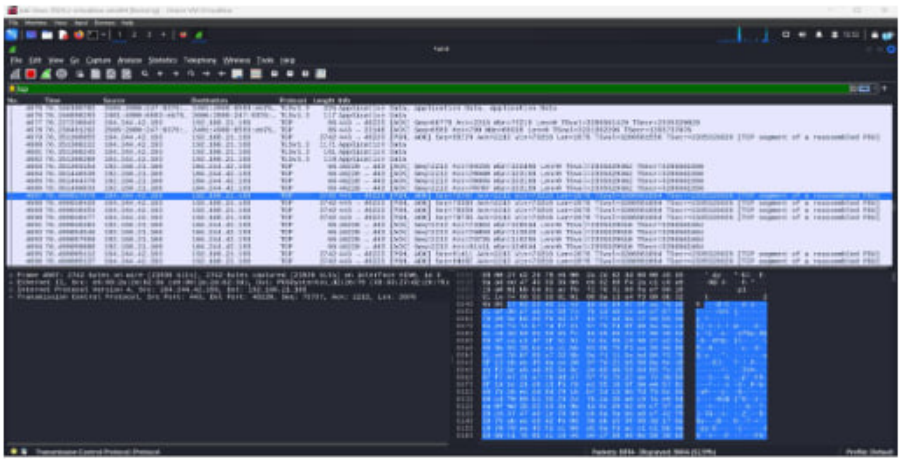

Figure 20: Wireshark

- When you filtered for DNS traffic in Wireshark, you focused on the Domain Name System, which is responsible for translating human-readable domain names (like google.com) into IP addresses. Here's what to expect and how to interpret the DNS traffic you see:

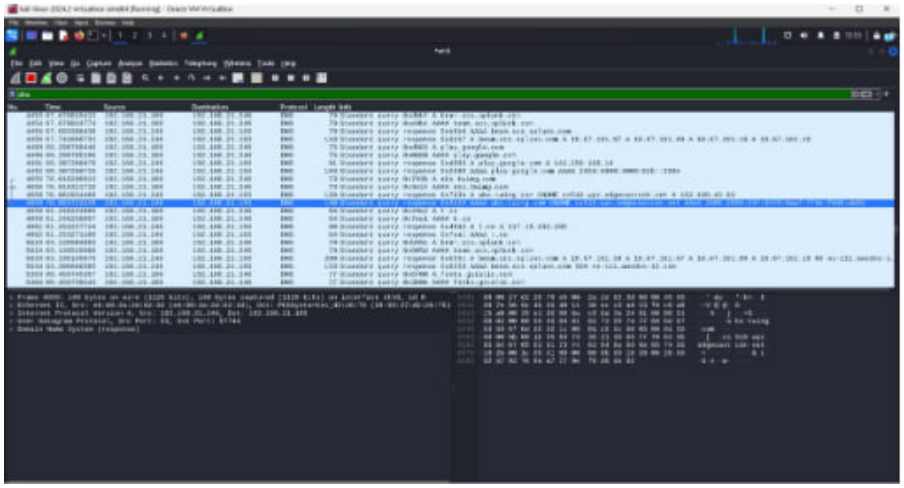

Figure 21: Wireshark

- Filtering HTTP traffic in Wireshark is especially useful for analyzing unencrypted web traffic
- Findings: **–**i noticed multiple packets being detected from IP address (192.168.154.2 192.168.154.129) respectively targeting ports 22,80 which shows a port scan attempt.

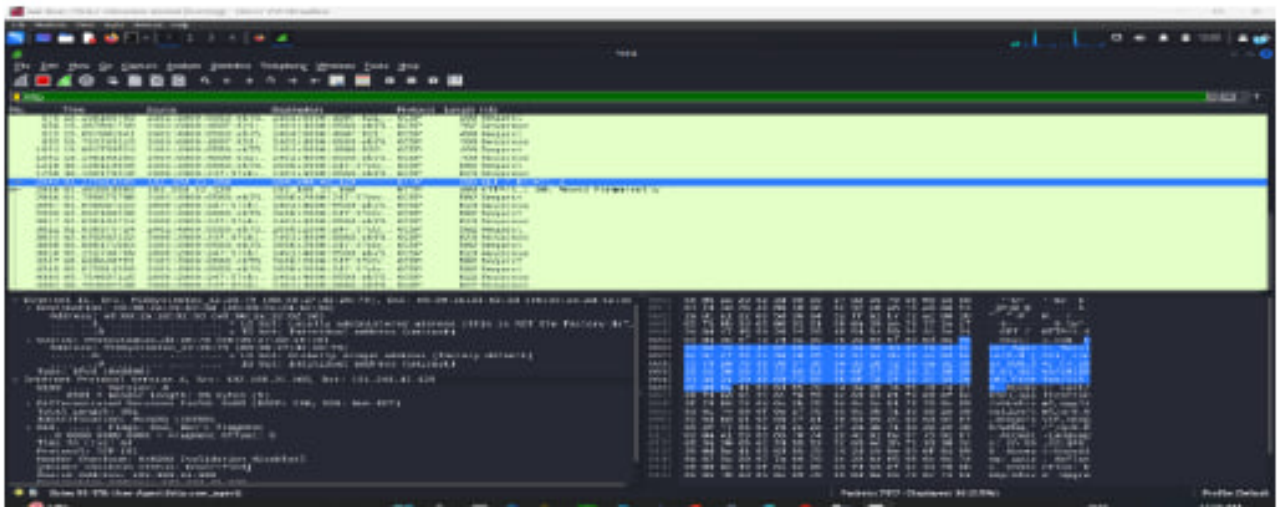

Figure 22: Wireshark

Nmap

- Using Nmap The results are shown below

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -A 192.168.71.129
Starting Nmap 7.93 ( https://nmap.org ) at 2024-07-27 12:06 EDT
Nmap scan report for 192.168.71.129
Host is up (0.00048s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE VERSION
22/tcp  open  ssh     OpenSSH 6.0p1 Debian 4+deb7u7 (protocol 2.0)
| ssh-hostkey:
|   1024 c4d659e6774c227a961660678b42488f (DSA)
|   2048 1182fe534edc5b327f446482757dd0a0 (RSA)
|_  256 3daa985c87afea84b823688db9055fd8 (ECDSA)
80/tcp  open  http    Apache httpd 2.2.22 ((Debian))
|_http-server-header: Apache/2.2.22 (Debian)
| http-robots.txt: 36 disallowed entries (15 shown)
| /includes/ /misc/ /modules/ /profiles/ /scripts/
| /themes/ /CHANGELOG.txt /cron.php /INSTALL.mysql.txt
| /INSTALL.pgsql.txt /INSTALL.sqlite.txt /install.php /INSTALL.txt
|_/LICENSE.txt /MAINTAINERS.txt
|_http-generator: Drupal 7 (http://drupal.org)
|_http-title: Welcome to Drupal Site | Drupal Site
111/tcp open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100024  1          46542/tcp   status
|   100024  1          48548/udp6  status
|   100024  1          49379/udp   status
|_  100024  1          52749/tcp6  status
MAC Address: 00:0C:29:C4:6F:EF (VMware)
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3
OS details: Linux 3.2 - 3.16
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Figure 23: NMAP

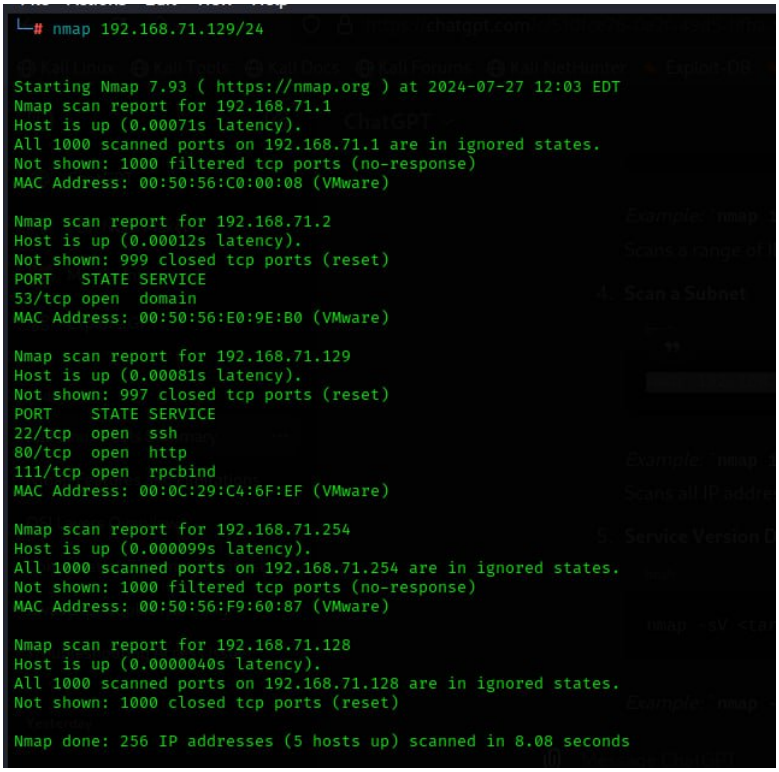

Figure 24: NMAP

Task 4: SIEM Configuration and Monitoring:

- **Question:** How would you configure a SIEM system to monitor and alert on security incidents in a network?
- **Task:** Set up a SIEM tool like Splunk Free or ELK Stack. Configure it to collect logs from various sources (firewalls, servers, endpoints). Create and customize alerts to trigger when certain suspicious activities are detected (e.g., a high number of failed login attempts or unusual outbound traffic).
- **Tools:** Splunk Free, ELK Stack.

Answer:

To configure a SIEM system to monitor and alert on security incidents in a network, follow these essential steps:

- Collect Data from All Devices Connect key devices such as servers, firewalls, routers, and applications to the SIEM. These devices will send logs containing information about network activity, login attempts, system events, and potential threats. This data is critical to detecting unusual behavior.
- Set Up Detection Rules Define rules for detecting security threats. Examples of detection rules might include: Multiple failed login attempts, which could indicate a brute-force attack. Unusual data transfers or access to sensitive information. Network traffic from suspicious IP addresses or known malicious

domains.

- Understand Normal Behavior Baseline normal network behavior by observing regular patterns, like typical login times, common user activity, or standard traffic volumes. This allows the SIEM to identify deviations from the norm, flagging unusual login times or data usage as potential threats.

- Create Alerts for Suspicious Activity Configure real-time alerts to notify you of suspicious activities, such as: Logins from unrecognized or geographically distant locations. High data transfers or unusual traffic during off-hours. Unauthorized access attempts to restricted files or systems.

- Integrate Threat Intelligence Add external threat intelligence feeds to your SIEM. These feeds provide real-time data on known malicious IP addresses, domains, and malware signatures, allowing the SIEM to detect and respond to known threats.

- Prioritize Alerts Not all alerts need immediate attention, so assign priority levels: High priority for critical events, such as logins from suspicious locations or large-scale data exfiltration. Low priority for minor issues, like a single failed login or non-critical system events.

- Automate Responses Implement automatic responses to high-priority alerts. For example: Automatically blocking a source IP after detecting a severe threat. Sending urgent notifications or emails to the security team for immediate action.

- Review and Improve Continuously monitor and adjust the SIEM's performance. Regularly refine detection rules, update baseline behaviors, and integrate new threat intelligence as your network changes or new threats arise.

By following these steps, your SIEM system will be well-equipped to monitor network activity, detect early signs of security incidents, and issue timely alerts to help mitigate cyber threats.

TASK:

- Configure Splunk to Collect Logs from Various Sources

- Local Event Log Collection (Windows Event Logs)

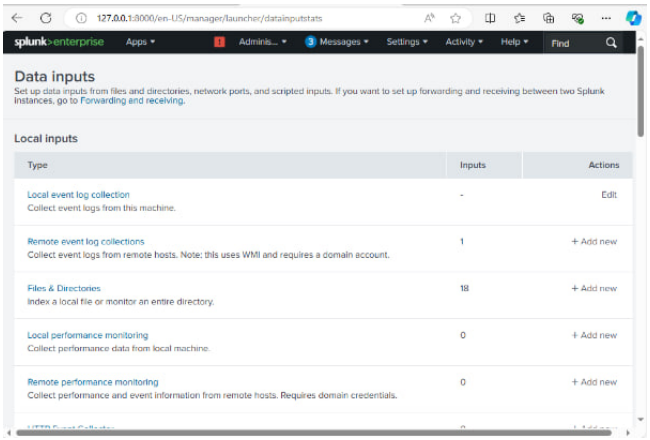

Figure 25: Splunk

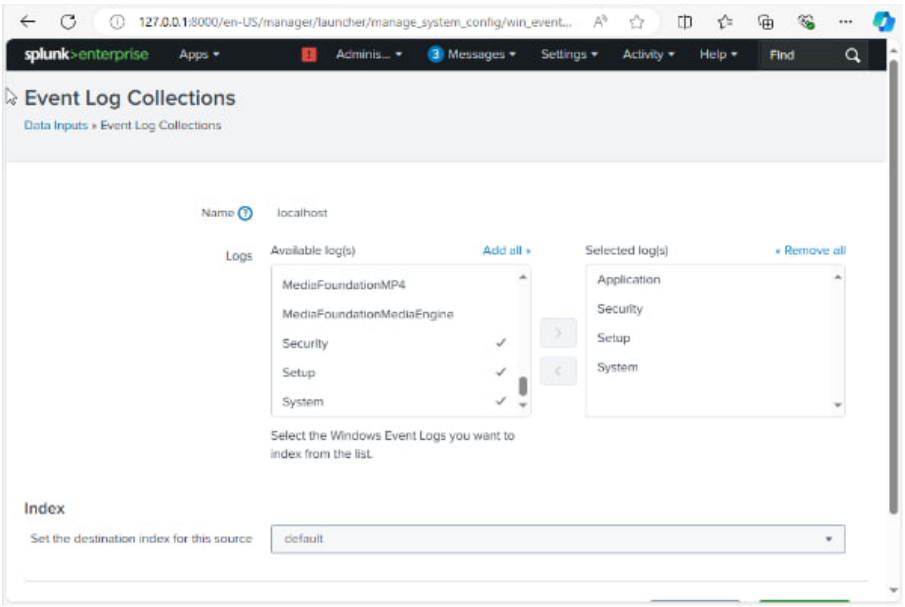

Figure 26: Splunk

- Creating and customizing alerts in Splunk for detecting suspicious activities, such as failed login attempts, involves setting up saved searches and alert actions

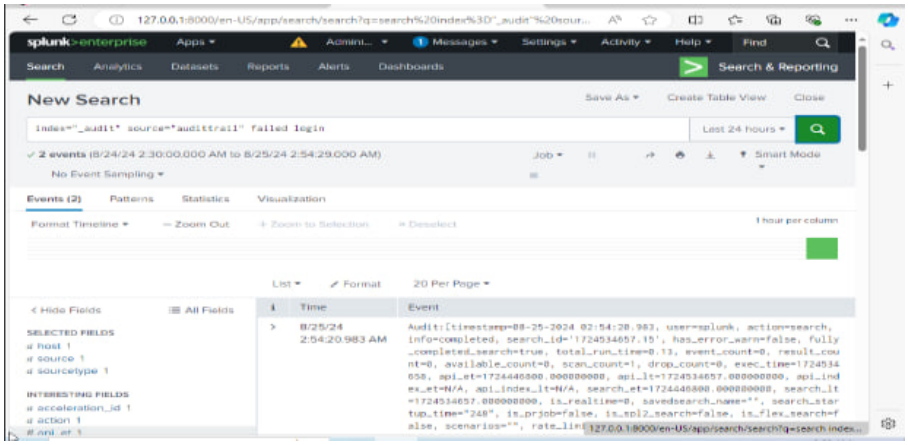

Figure 27: Splunk

- Configure Alert Settings

```
index=your_index sourcetype="WinEventLog:Security" EventCode=4625
| stats count by src_ip | where count > 5
```

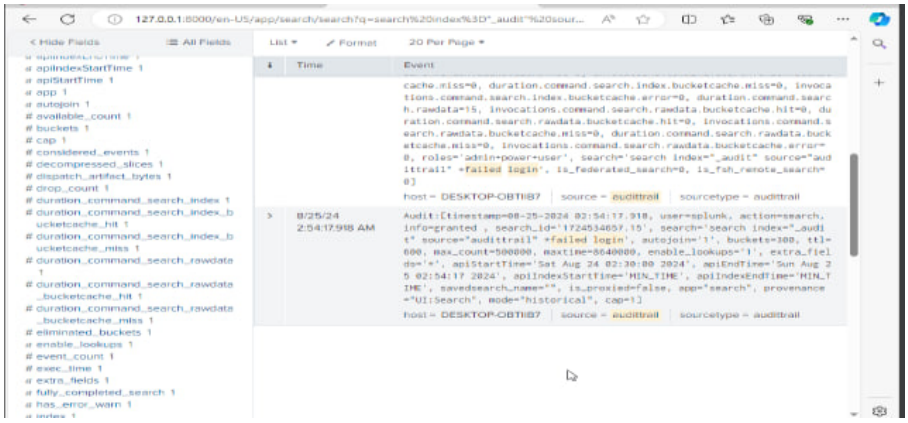

Figure 28: Splunk

- To create and customize an alert in Splunk for detecting a high number of failed logins, follow these steps:

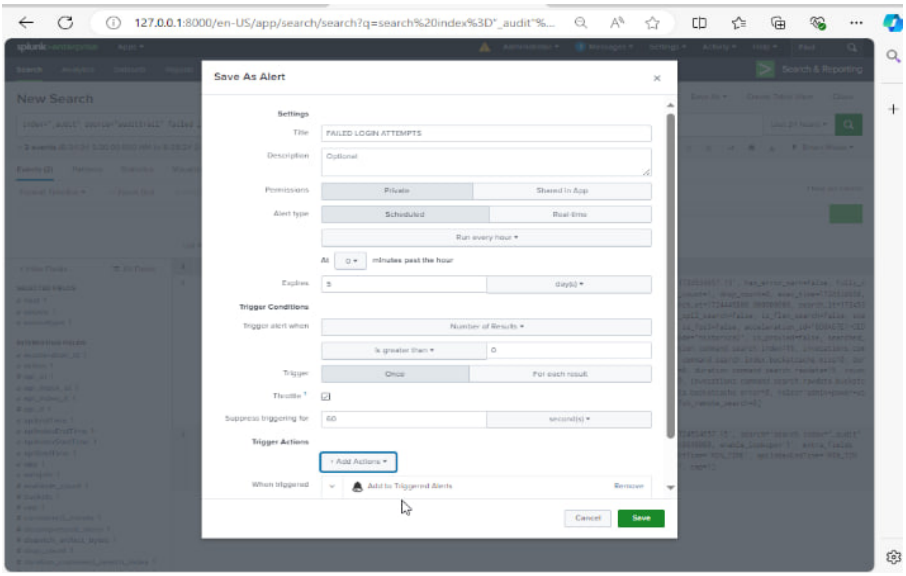

Figure 29: Splunk

- adjusted the permissions for your Splunk alert. This typically involves setting who can view, edit, or manage the alert. Here's a quick overview of what you might have done:

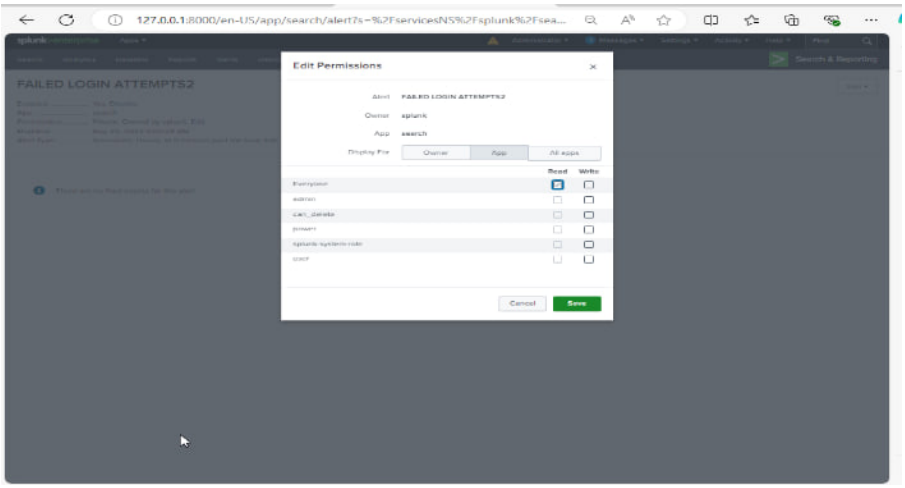

Figure 30: Splunk

Alert setup sounds well-configured for monitoring high volumes of failed login attempts. Here's a summary of your configuration:

- Alert Name: failed login attempts2
- Trigger Condition: More than 20 failed login attempts
- Run Schedule: Every hour
- Expiration: Alert will expire after 5 days
- Trigger Frequency: Triggers only once when the condition is met

With this setup, you'll be alerted if there's a significant number of failed login attempts, allowing you to investigate potential security issues promptly. If you need any further tweaks or have other questions By managing permissions effectively, you can ensure that the right people have access to the alerts while maintaining security and control over sensitive information.If you have any specific questions about permissions or need further assistance.

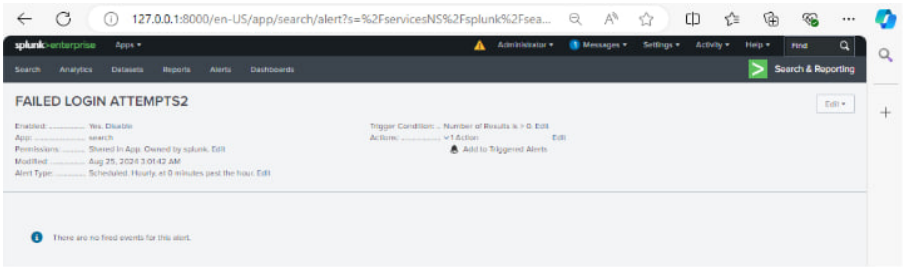

Figure 31: Splunk

Task5: Endpoint Security and Malware Detection:

- **Question:** How would you detect and respond to a malware infection on an endpoint?
- **Task:** Set up a test environment with Sysmon installed on a Windows machine. Simulate a malware infection by executing a test malware file. Monitor the endpoint for unusual behavior (e.g., new processes, registry changes) and document your incidentresponse steps to contain and remove the malware.
- **Tools:** Sysmon, Process Explorer (from Sysinternals Suite).

Detect and Respond to a Malware Infection

1. Detect the Malware Infection

- **Monitor Unusual Behavior:** Watch for slow system performance, unexpected pop-ups, unknown programs, or strange files.
- **Run Scans:** Use trusted antivirus or antimalware software to detect known malware signatures or suspicious files.
- **Check Network Activity:** Look for unusual outgoing traffic or connections to unknown IPs.
- **Review Logs:** Analyze system and security logs for anomalies or errors.

2. Isolate the Infected System

- **Disconnect from the Network:** Immediately unplug the infected device to prevent the malware from spreading or exfiltrating data.

3. Remove the Malware

- **Quarantine:** Use antivirus tools to quarantine the malware and prevent it from running.
- **Remove Malicious Files:** Follow antivirus instructions to delete infected files or restore the system to a previous safe state.
- **Manual Check:** If necessary, manually search for and remove any remaining malicious files or processes.

4. Investigate and Contain the Threat

- **Identify the Source:** Determine how the malware entered the system (e.g., phishing emails, malicious websites).
- **Update Security Measures:** Ensure antivirus, firewalls, and system software are up-to-date to close vulnerabilities.

5. Restore and Monitor

- **Restore the System:** If needed, restore from a clean backup to eliminate any traces of malware.
- **Monitor for Recurrence:** Keep an eye on the system for signs of reinfection or abnormal behavior.

6. Educate Users

- **User Awareness:** Teach users about the infection, safe browsing practices, email security, and avoiding suspicious links or downloads.

TASK

- Installing and Configuring Sysmon

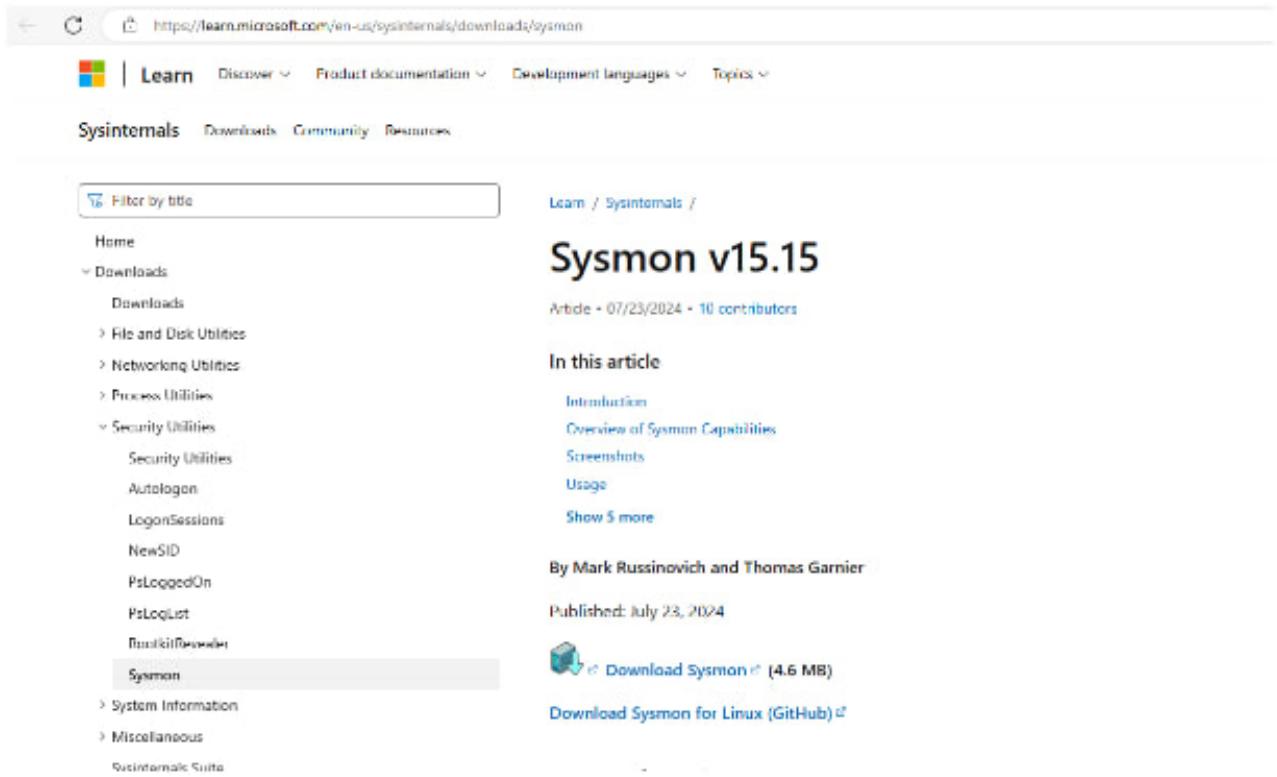

Figure 32: Sysmon

Here's a step-by-step guide for configuring and installing Sysmon using PowerShell:

- Open PowerShell as Administrator

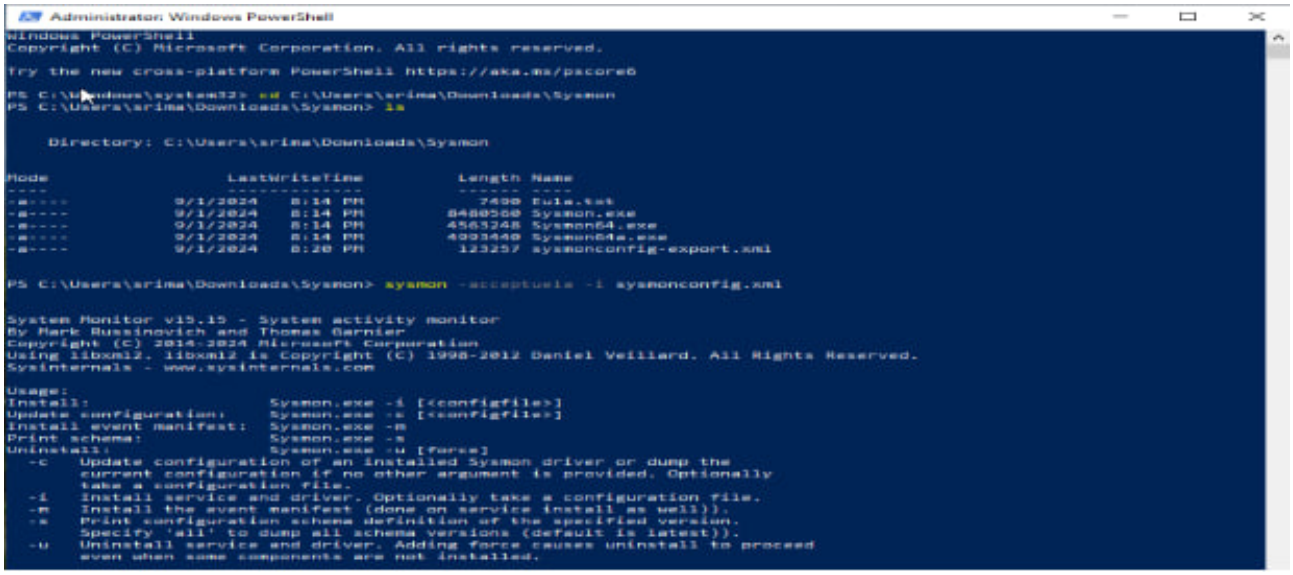

Figure 33: Sysmon

- installed Sysmon.exe with powershell

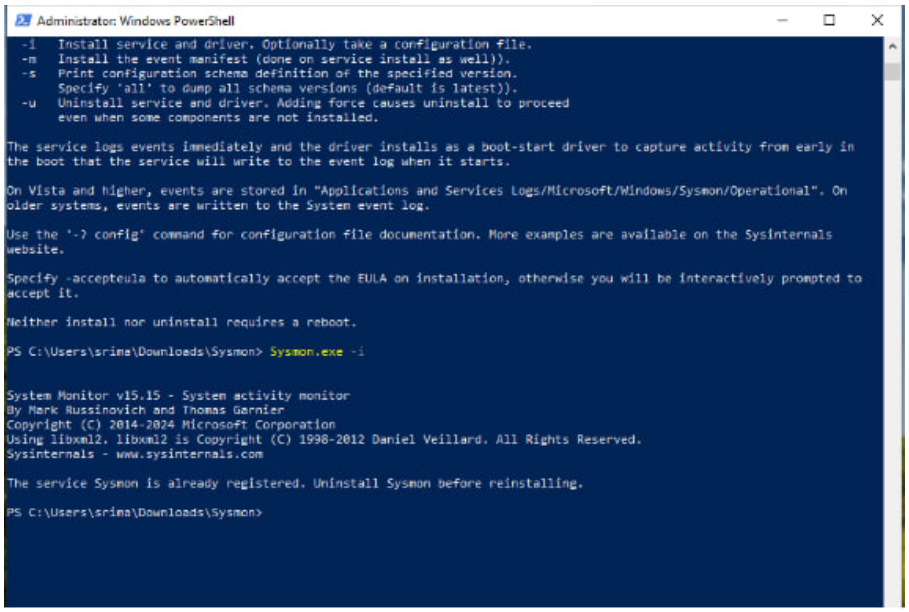

Figure 34: Sysmon

- created malicious file and executed on the windows system VM.

Figure 35: Sysmon

- Monitored the Windows endpoint for abnormal behavior by using Event Viewer to review Sysmon logs.

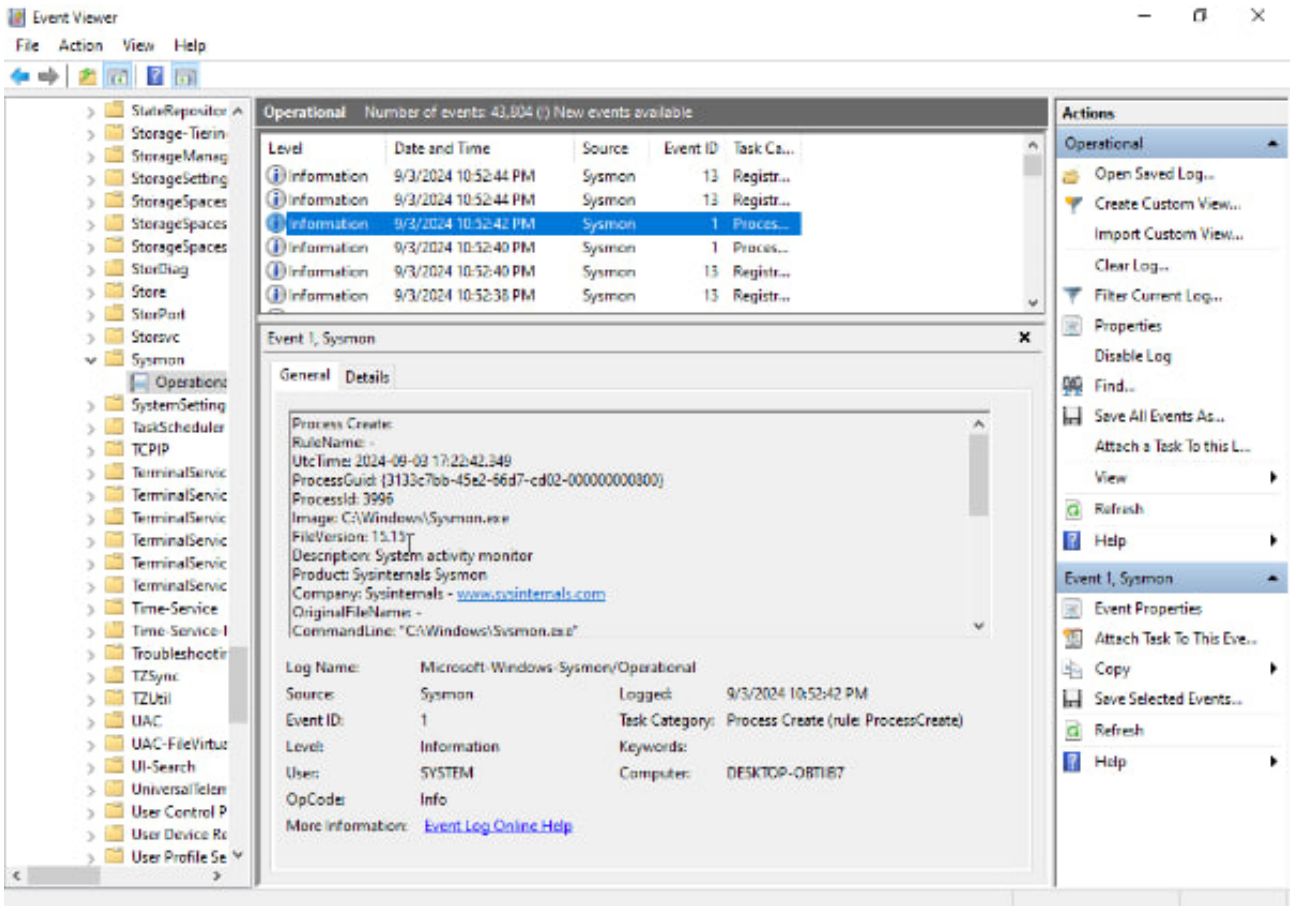

Figure 36: Sysmon

- Utilized Process Explorer to detect processes running from atypical directories. The image path feature in Process Explorer helped pinpoint the location of the executable files, while the command line information was used to understand how these files were executed.

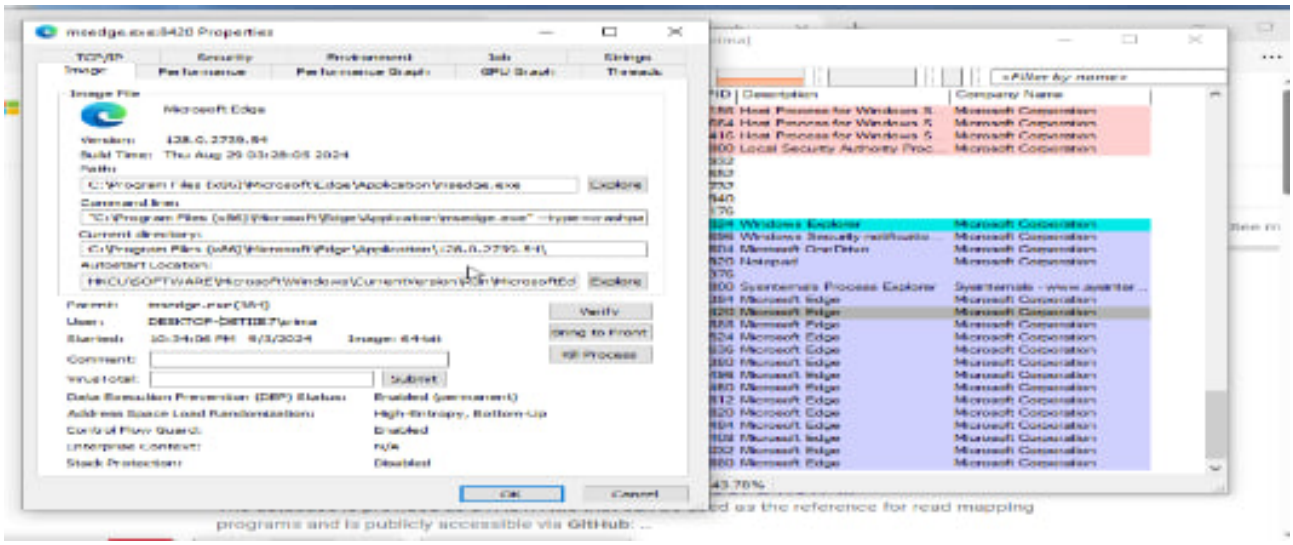

Figure 37: Sysmon

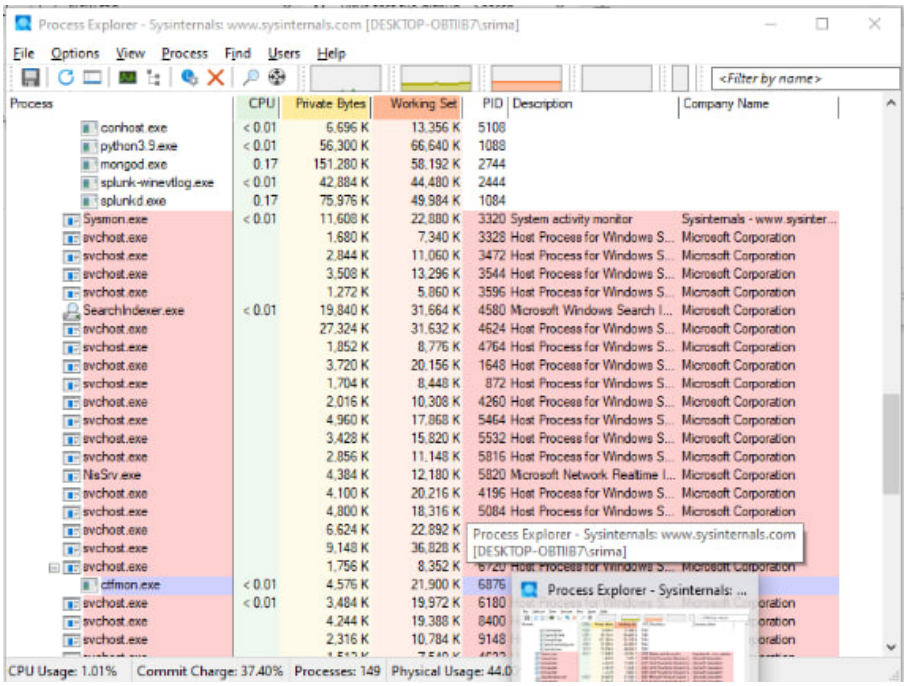

Figure 38: Sysmon

- Observed the VirusTotal integration in Process Explorer and used it to check the VirusTotal score for the processes.

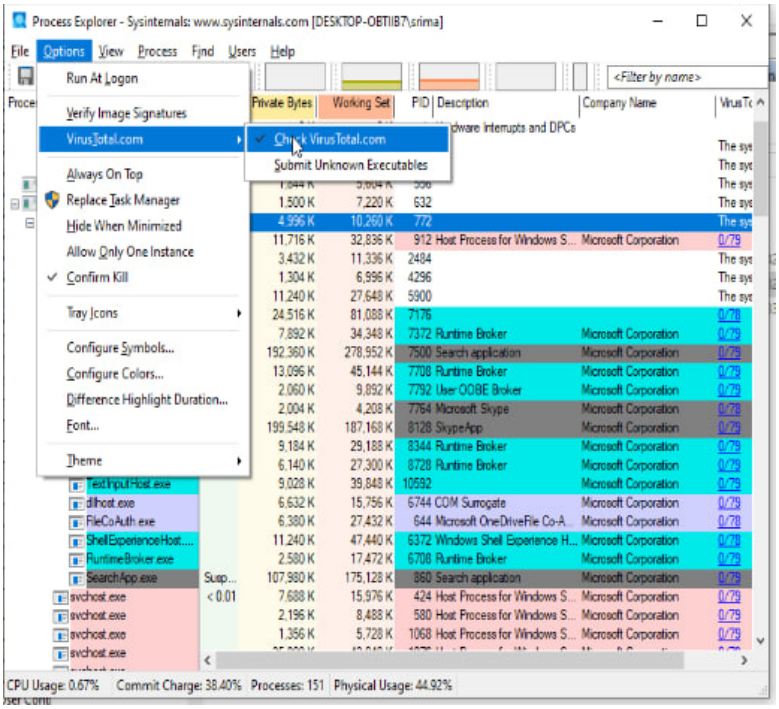

Figure 39: Sysmon

For containment and removal of the malware:

- Terminated Suspicious Processes: I used the 'Kill Process' feature to stop any suspicious processes.
- Disconnected the Machine: I disconnected the machine from the network to prevent the malware from spreading further.

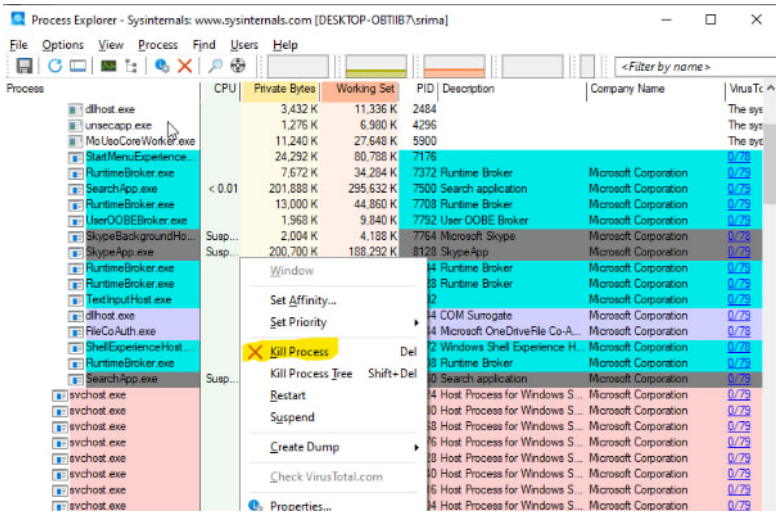

Figure 40: Sysmon

- Deleted the malware file and reversed the registry changes made by the malware.