**CYBERSECURITY AND ETHICAL HACKING PROJECT**

**TITLE: ENTERPRISE-LEVEL THREAT DETECTION & INCIDENT RESPONSE SYSTEM**

**-By KARTHIKEYA VALISETTY**

**Submission date – 02/04/2025**

**Security Monitoring and Incident Response Report**

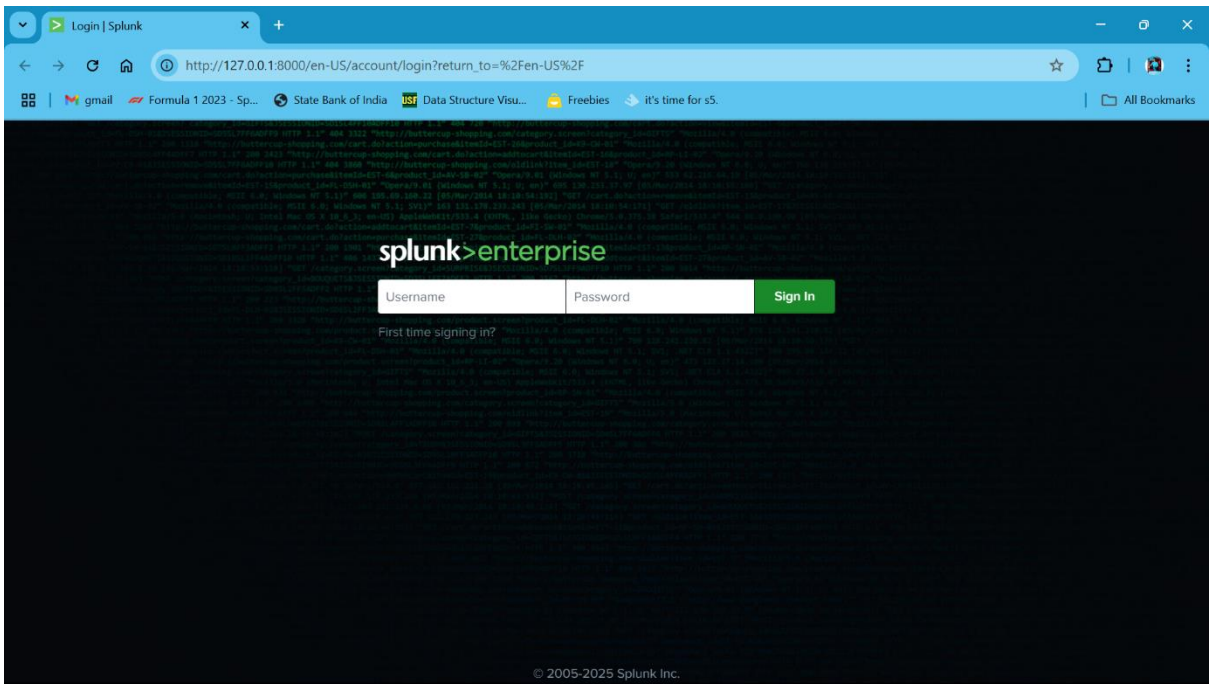
# 1. Introduction

This report provides a detailed analysis of the security monitoring architecture, log forwarding setup, automation scripts, intrusion detection system (IDS) configurations, and penetration testing activities. The goal is to document the setup, analyze logs, and provide security recommendations.

# 2. Splunk Setup Architecture

## 2.1 Overview

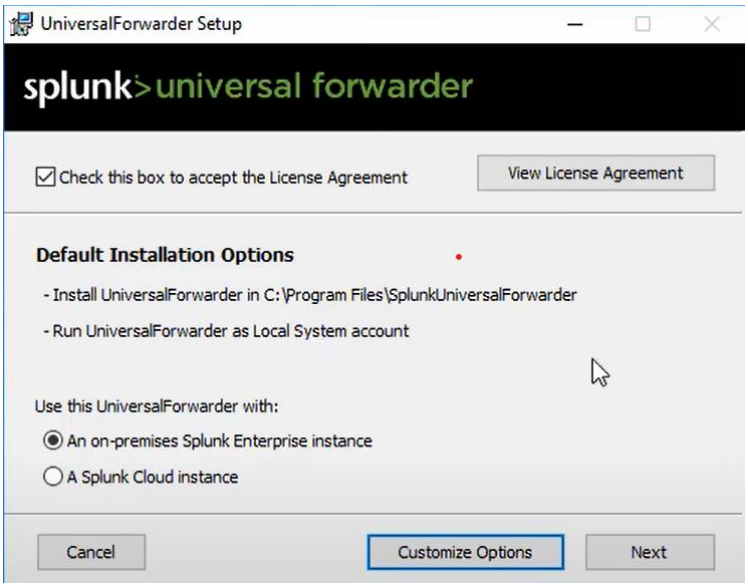
Splunk has been configured to collect and analyze logs from multiple devices using the Universal Forwarder. The logs are then indexed and monitored through Splunk's web interface.



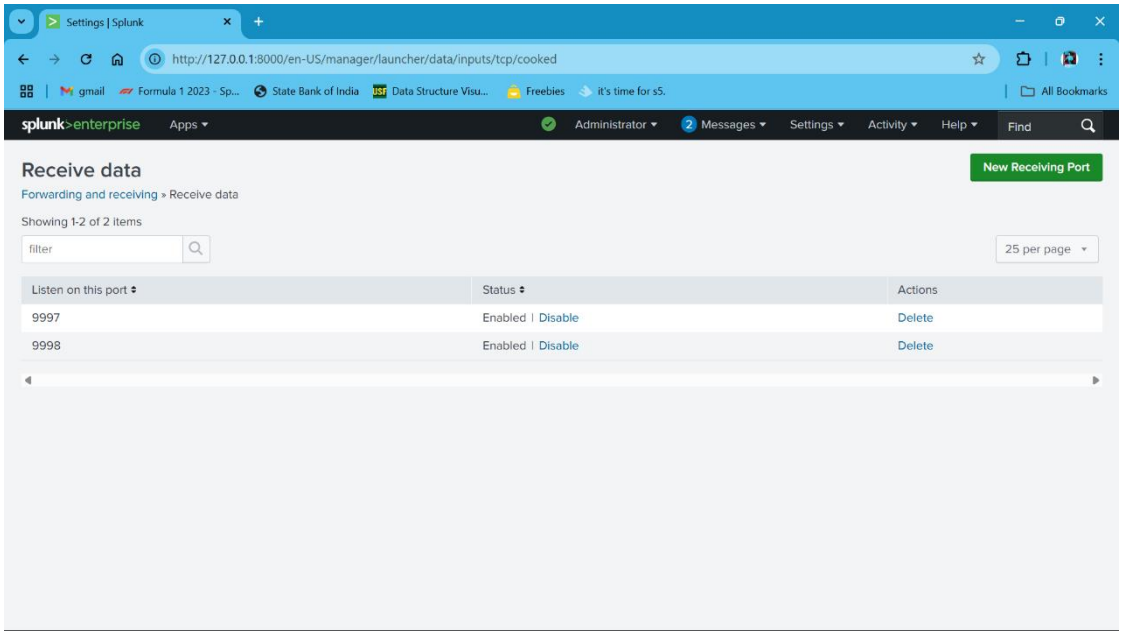

Continued….

## 2.2 Configuration Details

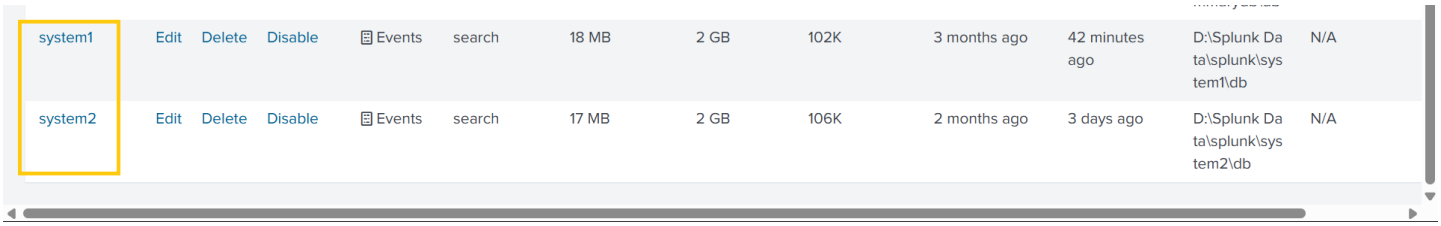
- **Universal Forwarder Setup:** Installed and configured on multiple devices.




- **Receiving Ports:** Configured on Splunk to accept logs from Universal Forwarders.

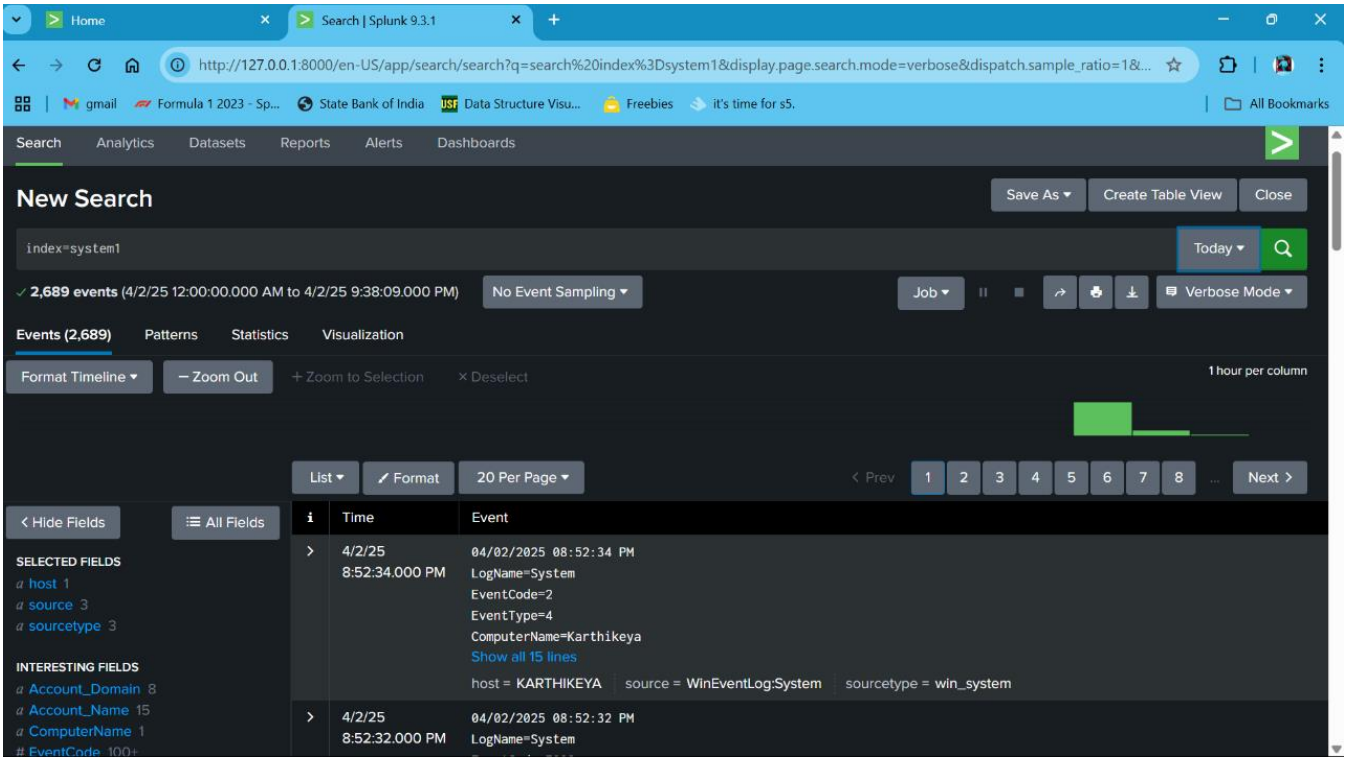


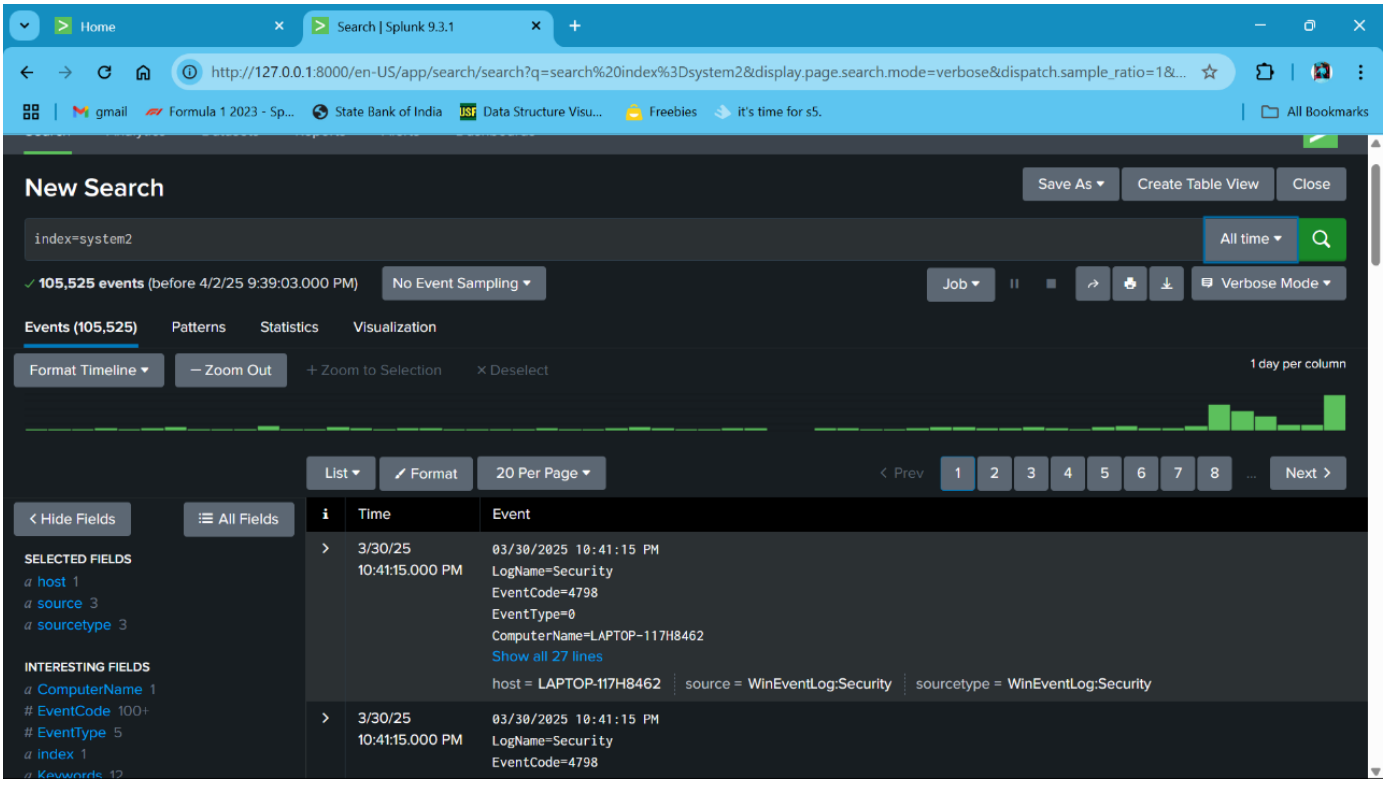

- **Indexing:** Separate indexes created for each system.




Continued….

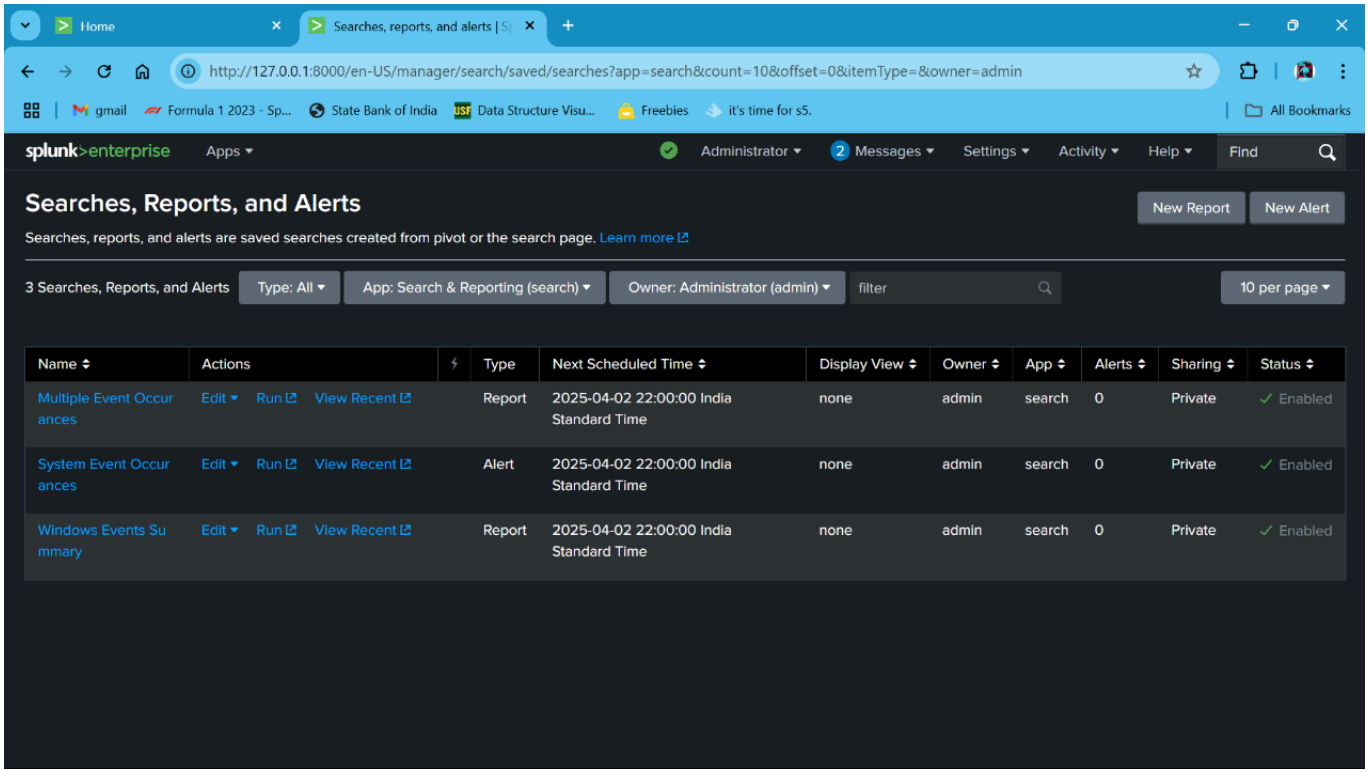
- **Log Forwarding:** Successfully verified for each system.



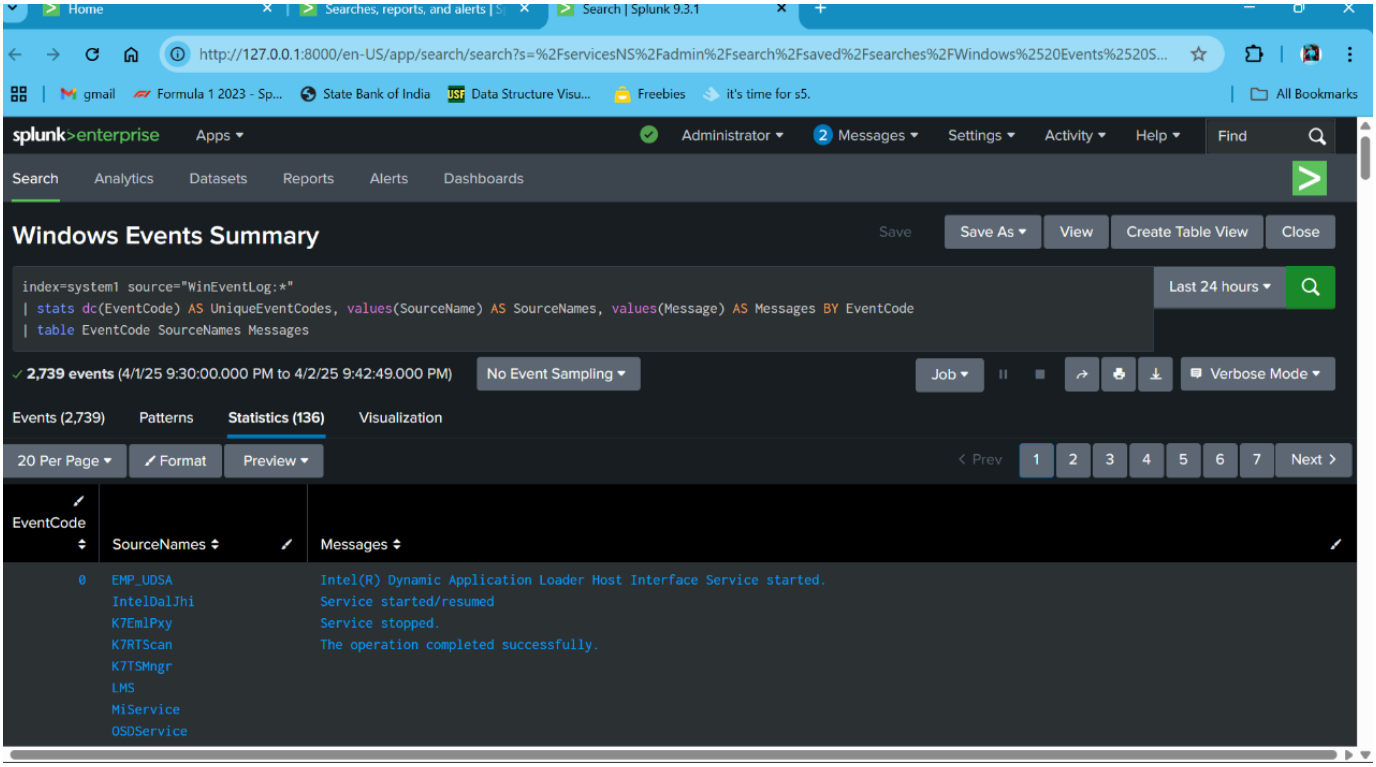




Continued….

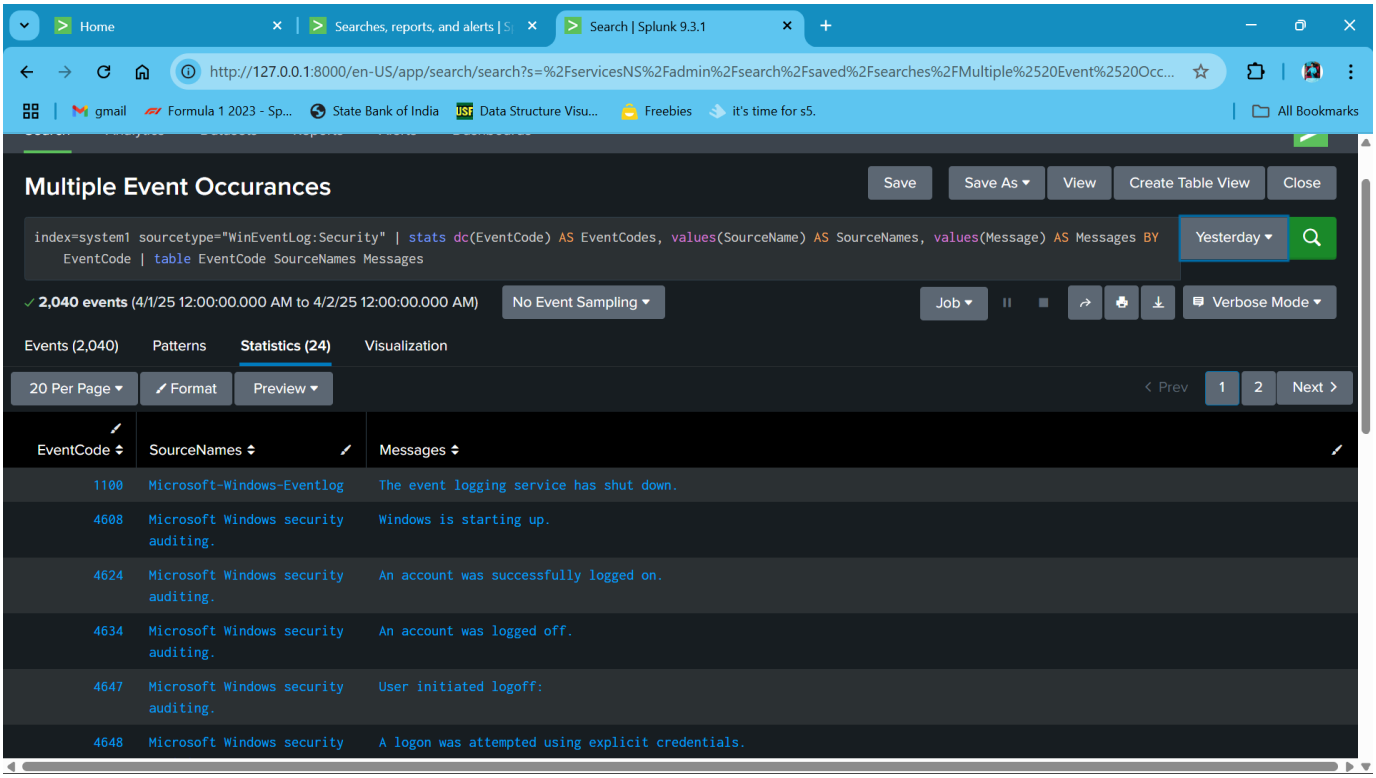
- **Alerts and Reports:** Configured periodic alerts and automated reports.

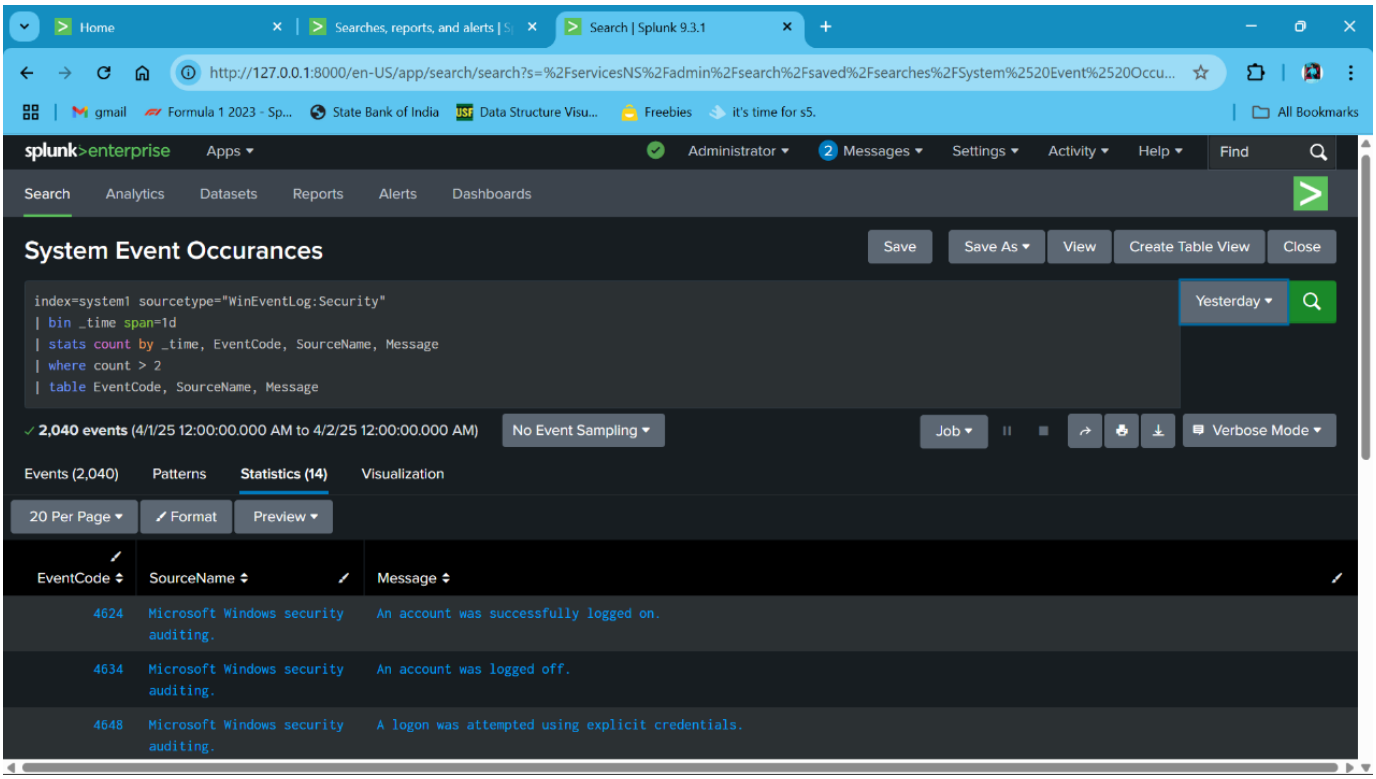



- **Search Queries:** Queries for monitoring logs and triggering alerts.




Continued….


Home
Searches, reports, and alerts | S
Search | Splunk 9.3.1
http://127.0.0.1:8000/en-US/app/search/search?s=%2FservicesNS%2Fadmin%2Fsearch%2Fsaved%2Fsearches%2FMultiple%2520Event%2520Occ...
gmail
Formula 1 2023 - Sp...
State Bank of India
Data Structure Visu...
Freebies
it's time for s5.
All Bookmarks
Multiple Event Occurances
Save
Save As
View
Create Table View
Close
index=system1 sourcetype="WinEventLog:Security" | stats dc(EventCode) AS EventCodes, values(SourceName) AS SourceNames, values(Message) AS Messages BY EventCode | table EventCode SourceNames Messages
Yesterday
2,040 events (4/1/25 12:00:00.000 AM to 4/2/25 12:00:00.000 AM)
No Event Sampling
Job
Verbose Mode
Events (2,040)
Patterns
Statistics (24)
Visualization
20 Per Page
Format
Preview
Prev
1
2
Next
EventCode
SourceNames
Messages
1100 Microsoft-Windows-Eventlog The event logging service has shut down.
4608 Microsoft Windows security auditing. Windows is starting up.
4624 Microsoft Windows security auditing. An account was successfully logged on.
4634 Microsoft Windows security auditing. An account was logged off.
4647 Microsoft Windows security auditing. User initiated logoff:
4648 Microsoft Windows security A logon was attempted using explicit credentials.


Home
Searches, reports, and alerts | S
Search | Splunk 9.3.1
http://127.0.0.1:8000/en-US/app/search/search?s=%2FservicesNS%2Fadmin%2Fsearch%2Fsaved%2Fsearches%2FSystem%2520Event%2520Occu...
gmail
Formula 1 2023 - Sp...
State Bank of India
Data Structure Visu...
Freebies
it's time for s5.
All Bookmarks
splunk>enterprise
Apps
Administrator
2 Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
System Event Occurances
Save
Save As
View
Create Table View
Close
index=system1 sourcetype="WinEventLog:Security"
| bin _time span=1d
| stats count by _time, EventCode, SourceName, Message
| where count > 2
| table EventCode, SourceName, Message
Yesterday
2,040 events (4/1/25 12:00:00.000 AM to 4/2/25 12:00:00.000 AM)
No Event Sampling
Job
Verbose Mode
Events (2,040)
Patterns
Statistics (14)
Visualization
20 Per Page
Format
Preview
EventCode
SourceName
Message
4624 Microsoft Windows security auditing. An account was successfully logged on.
4634 Microsoft Windows security auditing. An account was logged off.
4648 Microsoft Windows security auditing. A logon was attempted using explicit credentials.

Continued….

# 3. Python Log Analysis Automation

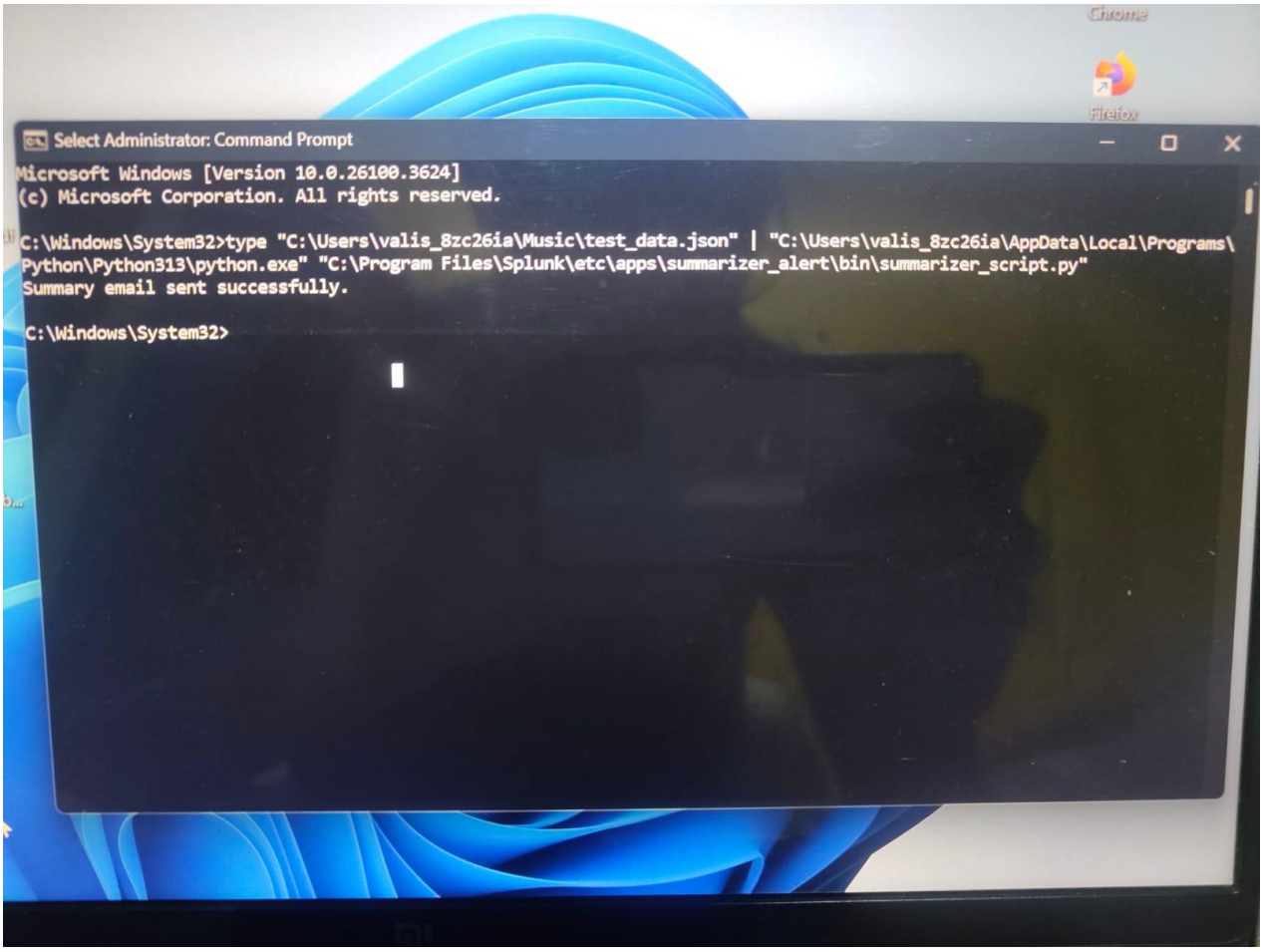
## 3.1 Overview

A Python script was developed for log analysis automation, executing predefined search queries and sending summarized reports via email.

## 3.2 Configuration Details

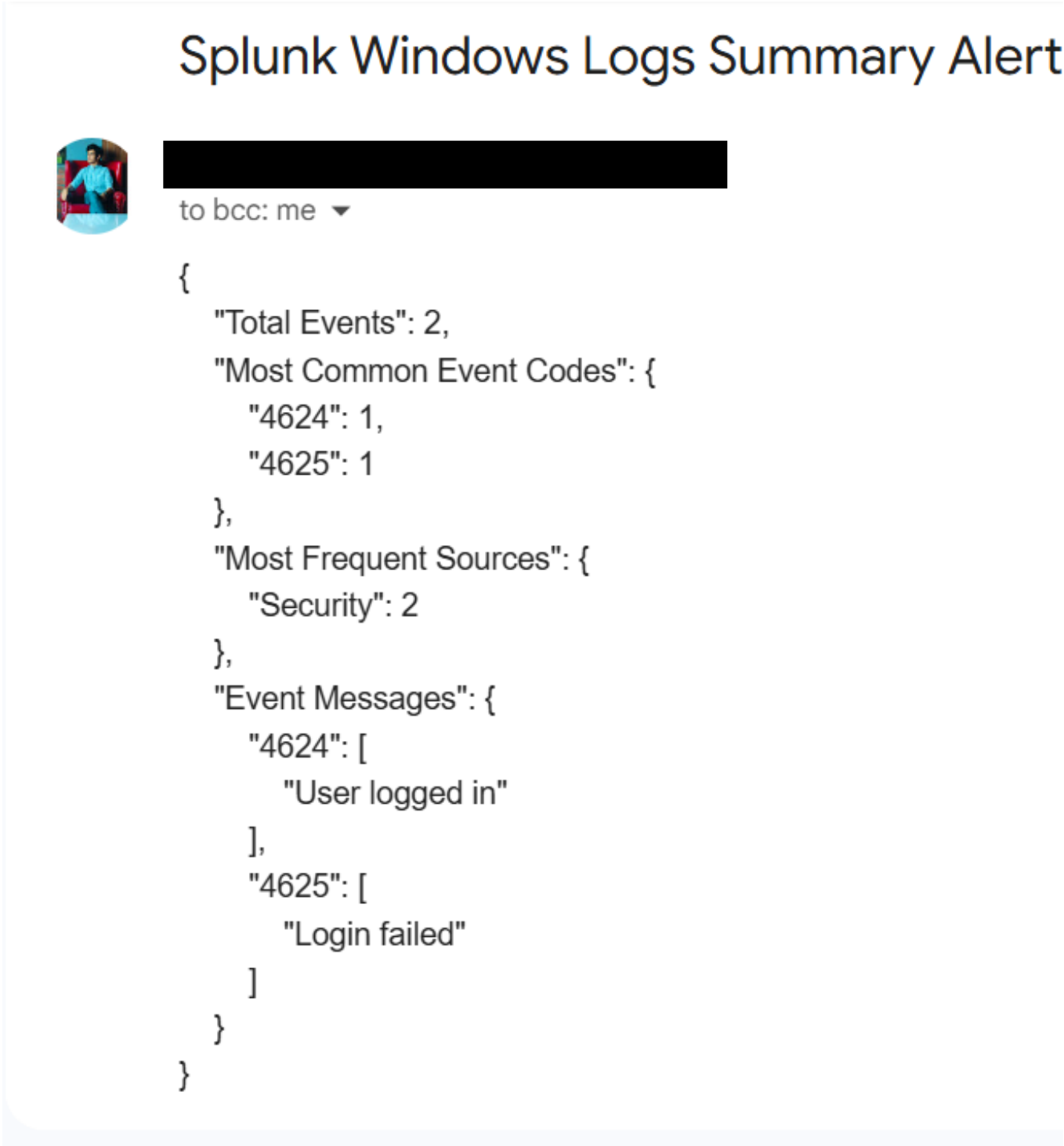
- **Checkout the script here:**
  https://github.com/Karthikeya1125/Automation_Scripts/tree/main/Python_Scripts
- **Execution Commands:** Commands required to run the script documented.

  "C:\Users\valis_8zc26ia\Music\test_data.json" |
  "C:\Users\valis_8zc26ia\AppData\Local\Programs\Python\Python313\python.exe" "C:\Program Files\Splunk\etc\apps\summarizer_alert\bin\summarizer_script.py"
- **Output Verification:** Screenshot of script execution results.




Continued….

- **Email Notifications:** Verified successful email alerts upon execution.




Continued….

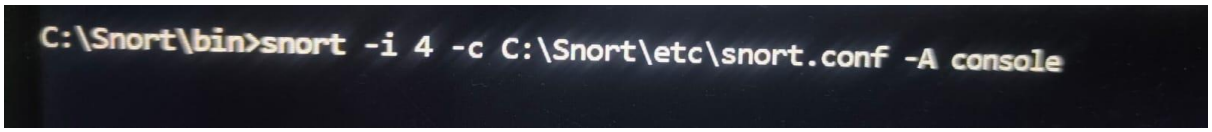
# 4. Snort Intrusion Detection System Setup

## 4.1 Overview

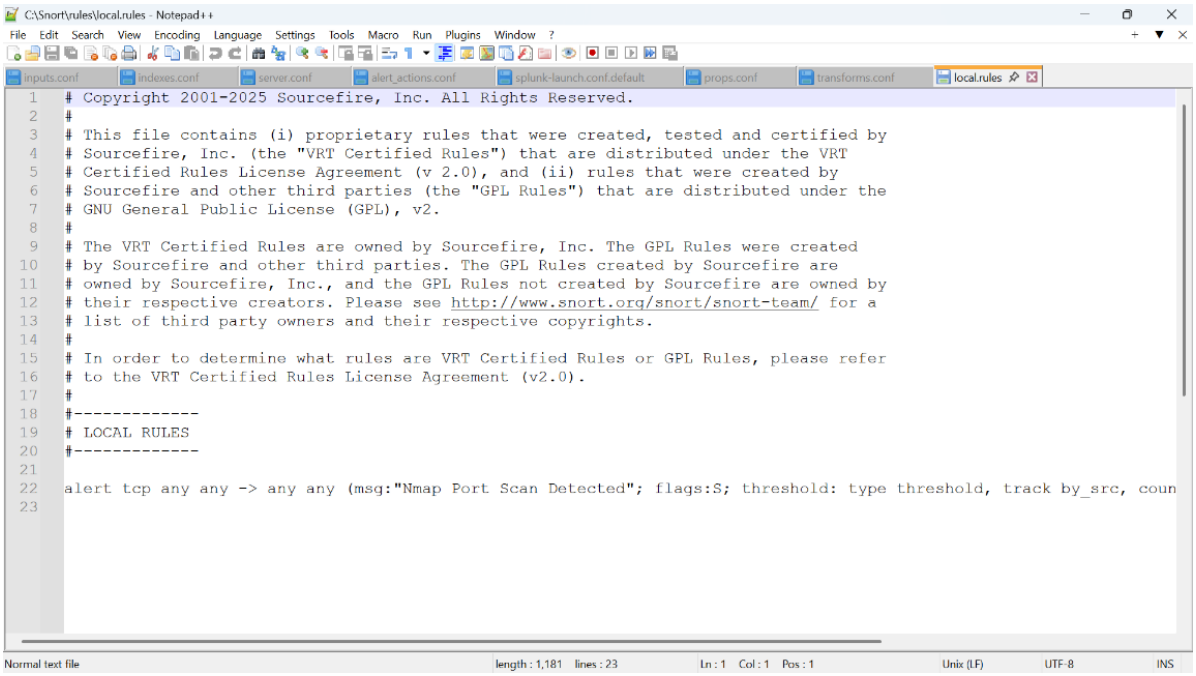
Snort has been installed and configured to detect network intrusions and generate logs for security analysis.

## 4.2 Configuration Details

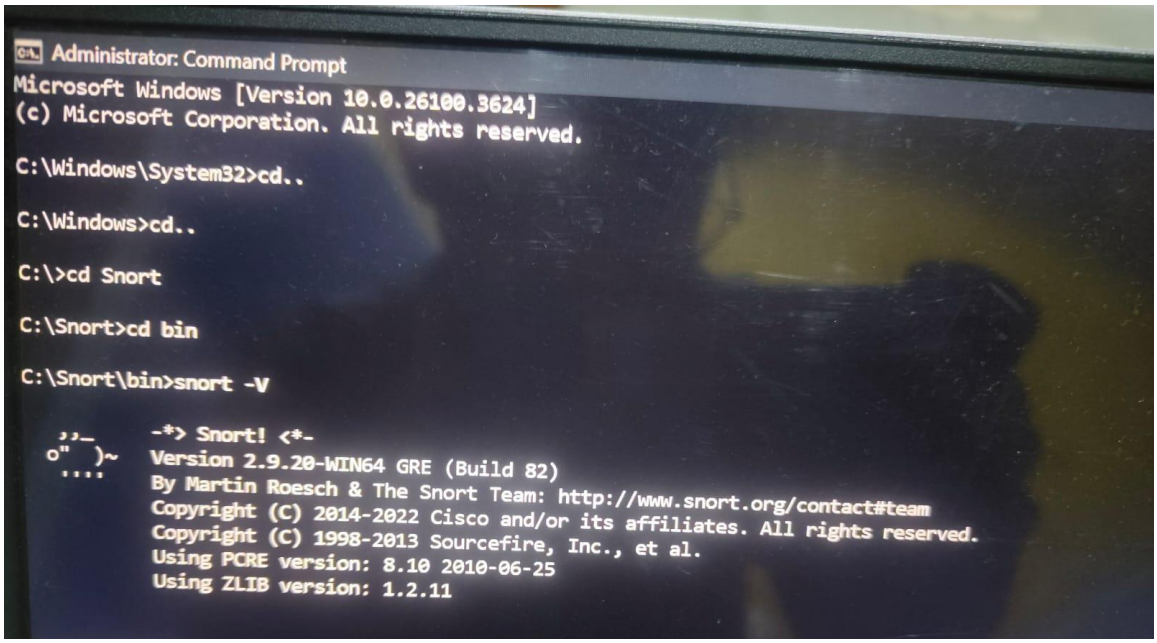
- **Snort Configuration:** Configured snort.conf for IDS mode.



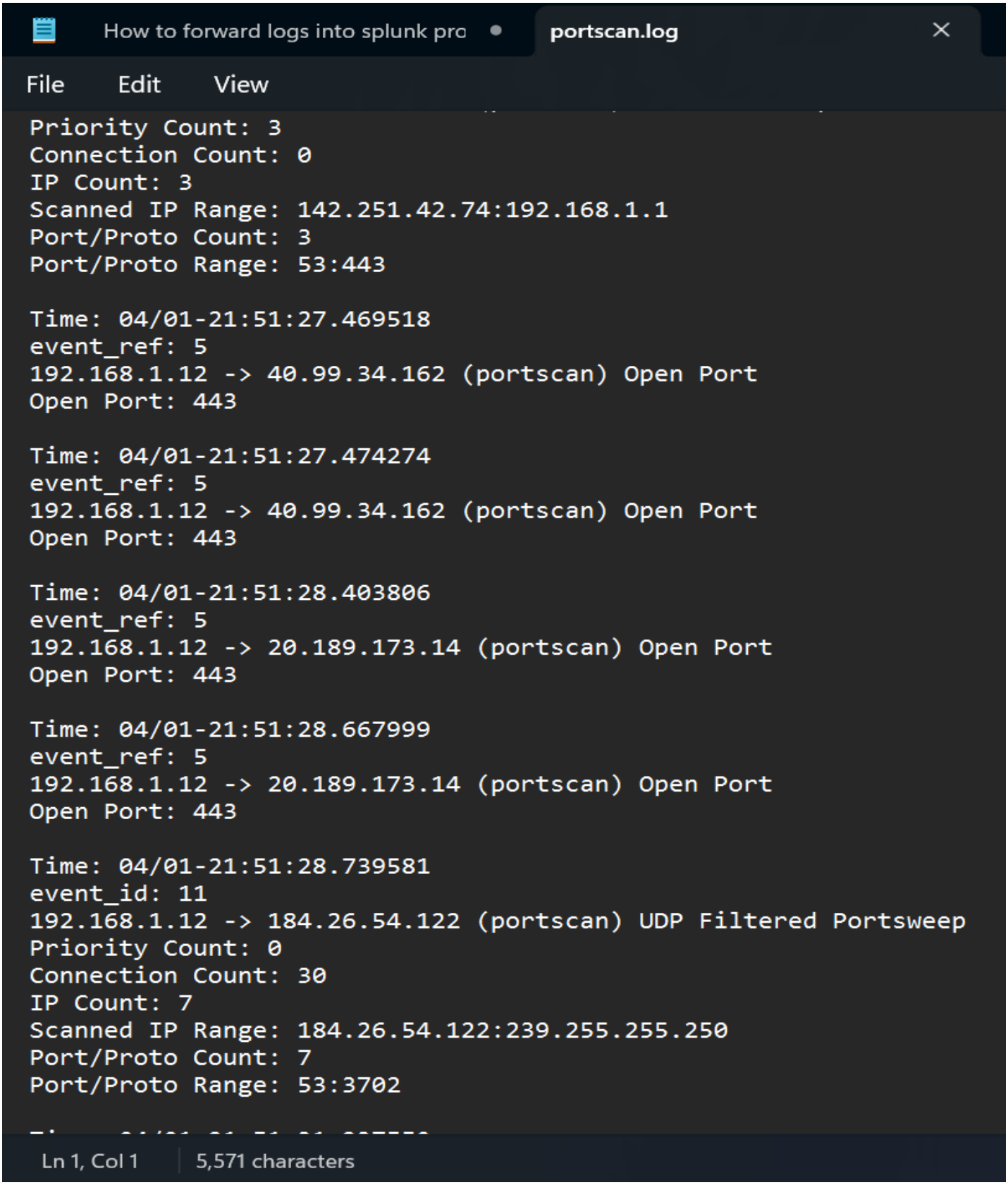

- **Custom Rules:** Added local rules in local.rules file to detect suspicious activities.




- **Version Check:** Verified Snort version using terminal commands.



- **Running Snort in IDS Mode:** Documented commands and execution results.
- **Log Analysis:** Verified logs generated in portscan.log, including detection of an Nmap scan.



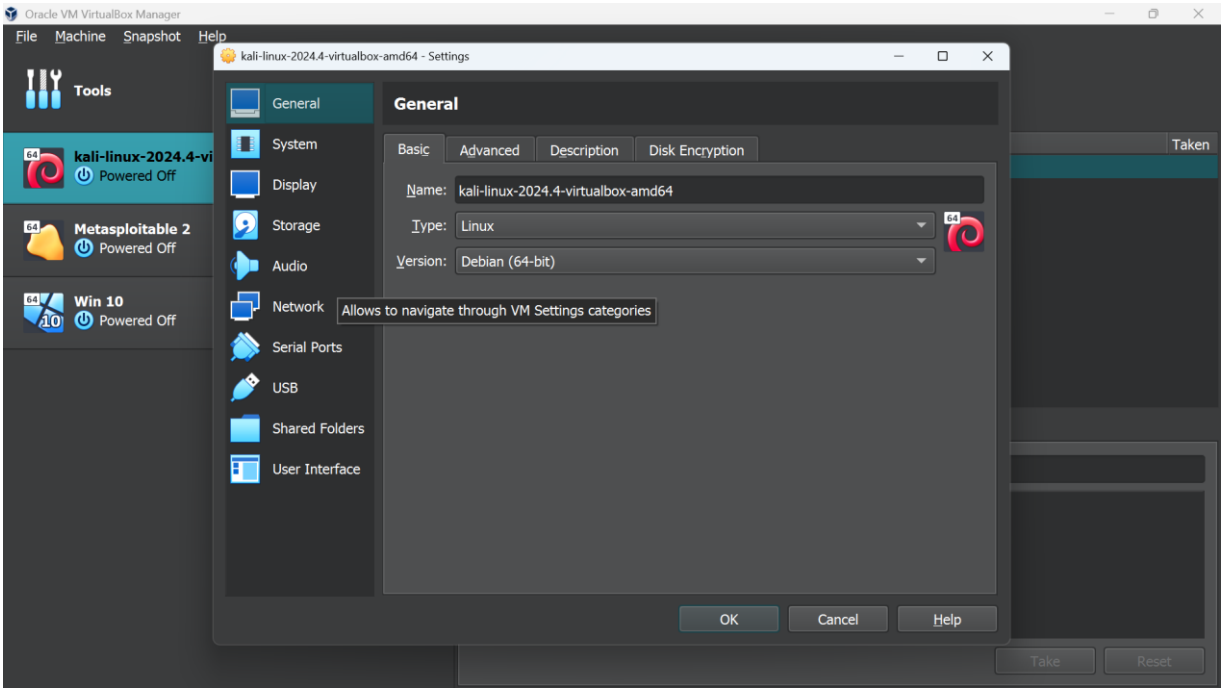
# 5. Kali Linux Setup and Penetration Testing

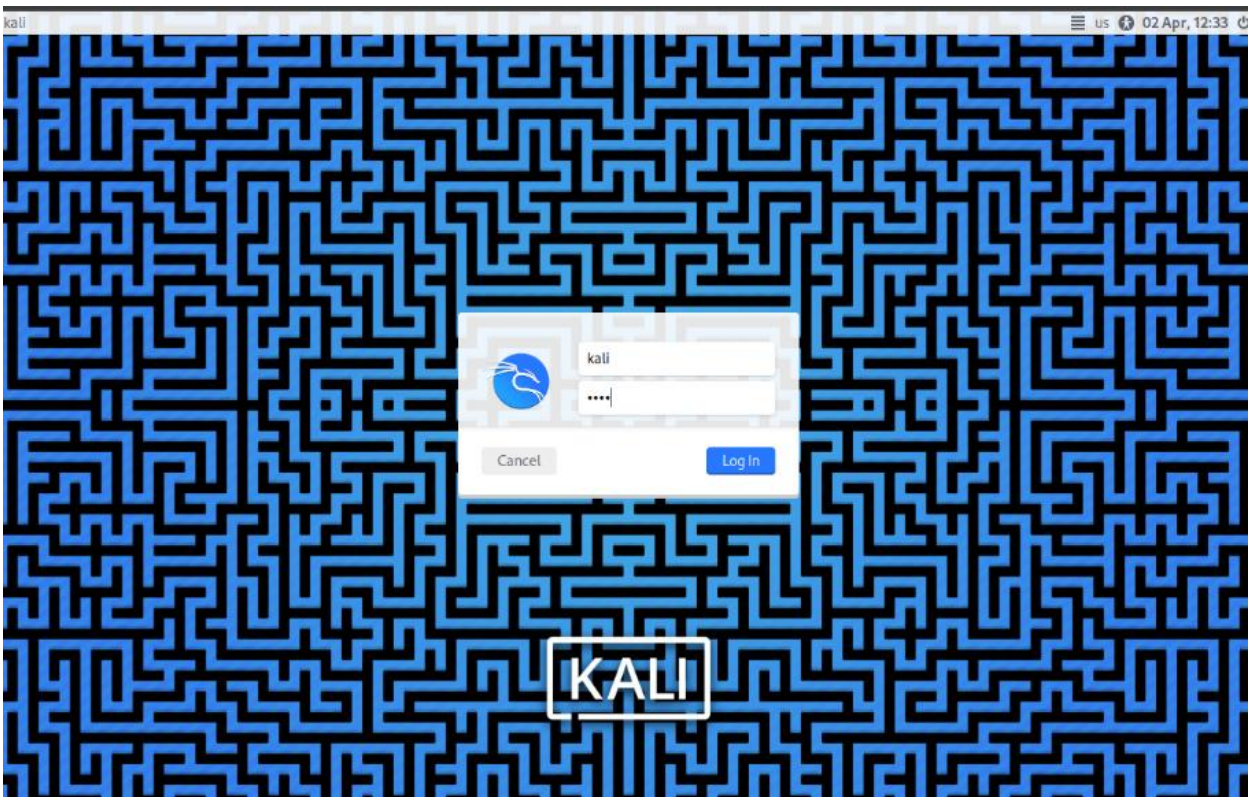
## 5.1 Overview

Kali Linux was used for penetration testing to assess network security.

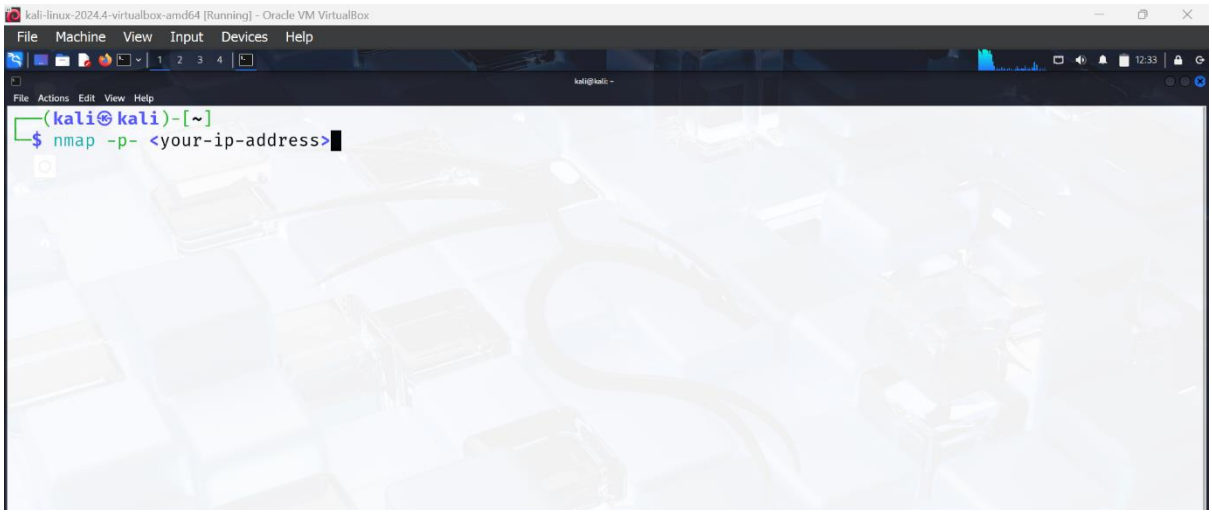
## 5.2 Configuration Details

- **Kali Linux Installation:** Successfully set up and configured.

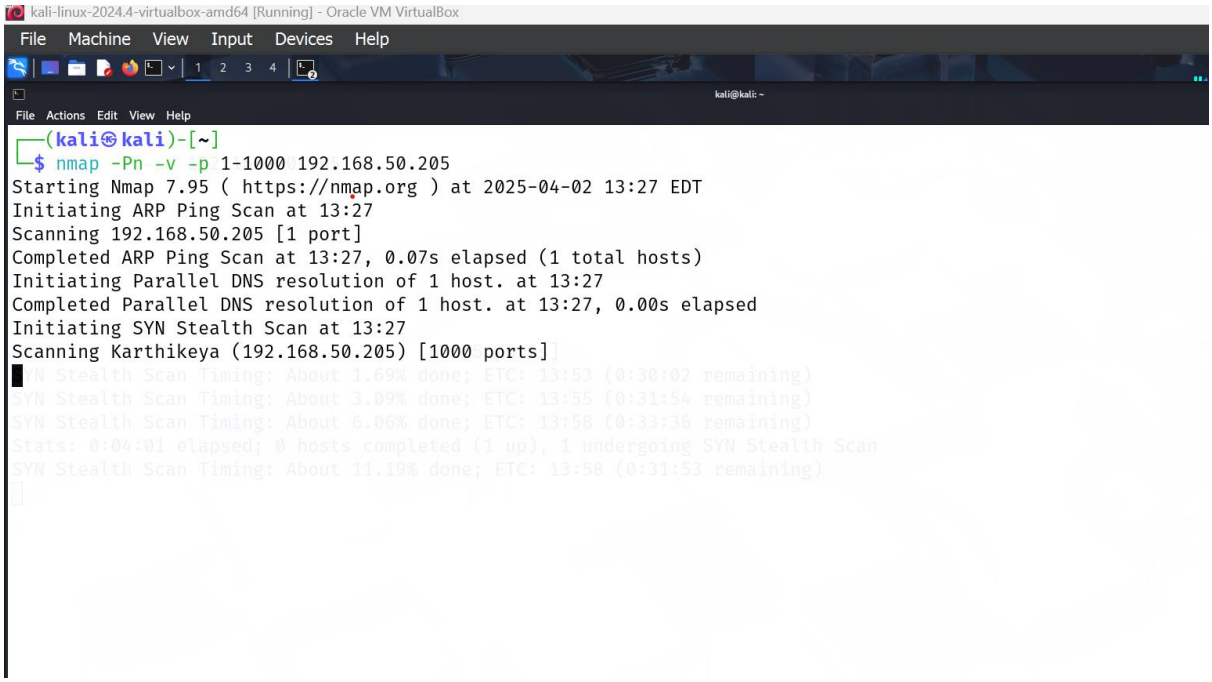


- **Nmap Scan Execution:** Conducted an Nmap scan on a target system.




- **Command Documentation:** Screenshots of commands used.




- **Scan Results:** Analyzed scan output to identify open ports and vulnerabilities.

# 6. Incident Response and Findings

## 6.1 Security Event Detection

- Splunk alerts successfully triggered based on predefined queries.
- Snort detected unauthorized network scanning activity (Nmap scan).
- Python automation script provided timely log summaries via email.

## 6.2 Security Recommendations

- **Splunk Optimization:** Implement advanced correlation rules and dashboards.
- **Snort Enhancement:** Expand rule set to detect a wider range of attacks.
- **Network Hardening:** Limit open ports and monitor suspicious activities.
- **Incident Response Plan:** Establish a standardized incident response framework.

# 7. Conclusion

This report documents the security setup and its effectiveness in detecting security events. Based on the findings, recommendations have been provided to improve overall cybersecurity resilience. Continuous monitoring, log analysis, and proactive security measures are essential for maintaining a robust security infrastructure.