

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

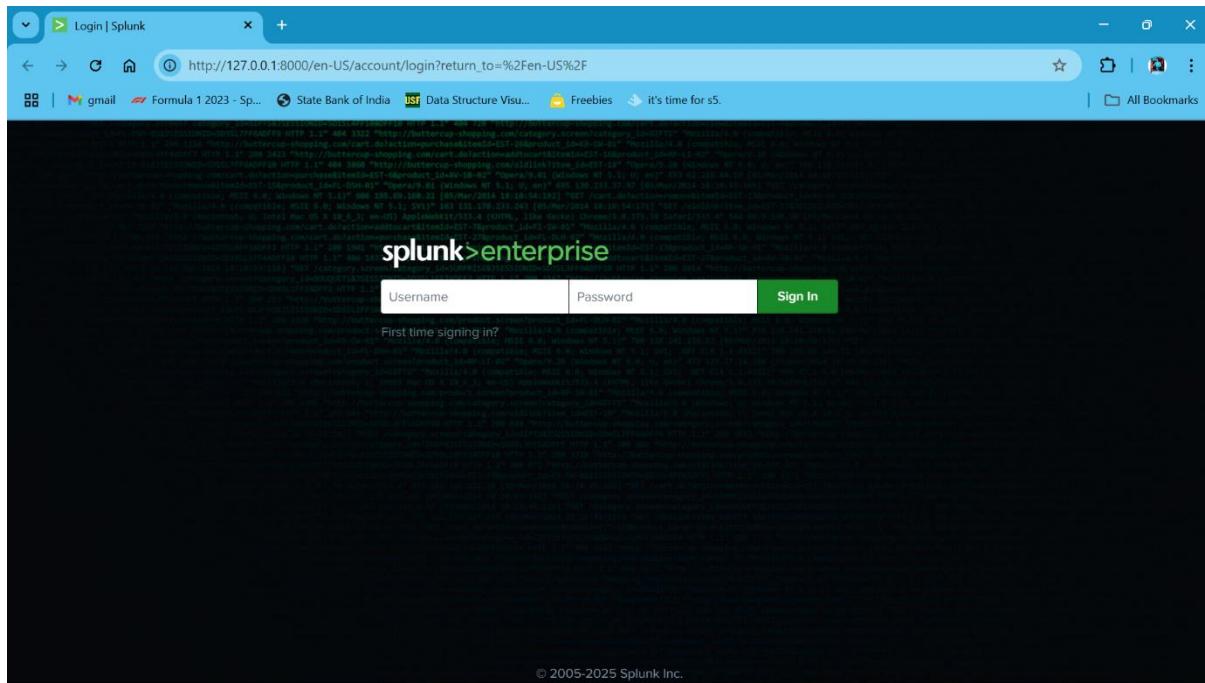
1. Introduction

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

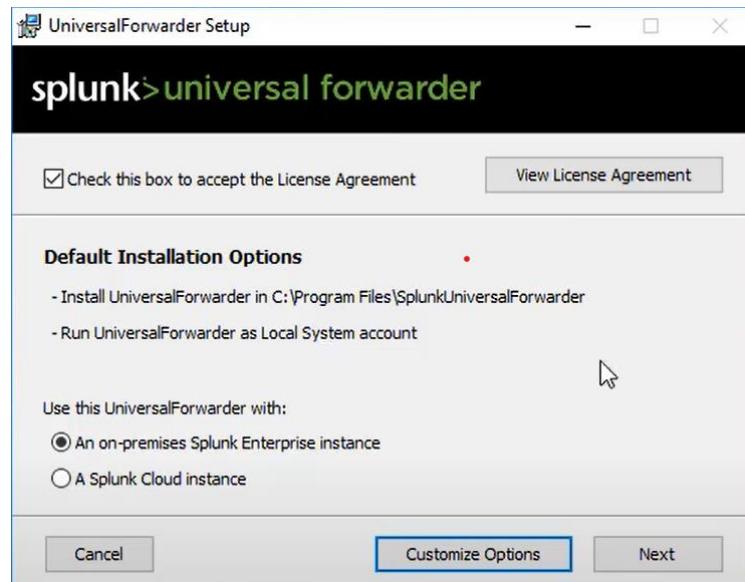
Splunk has been configured to collect and analyze logs from multiple devices using the Universal Forwarder. The logs are then indexed and monitored through Splunk's web interface.



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.

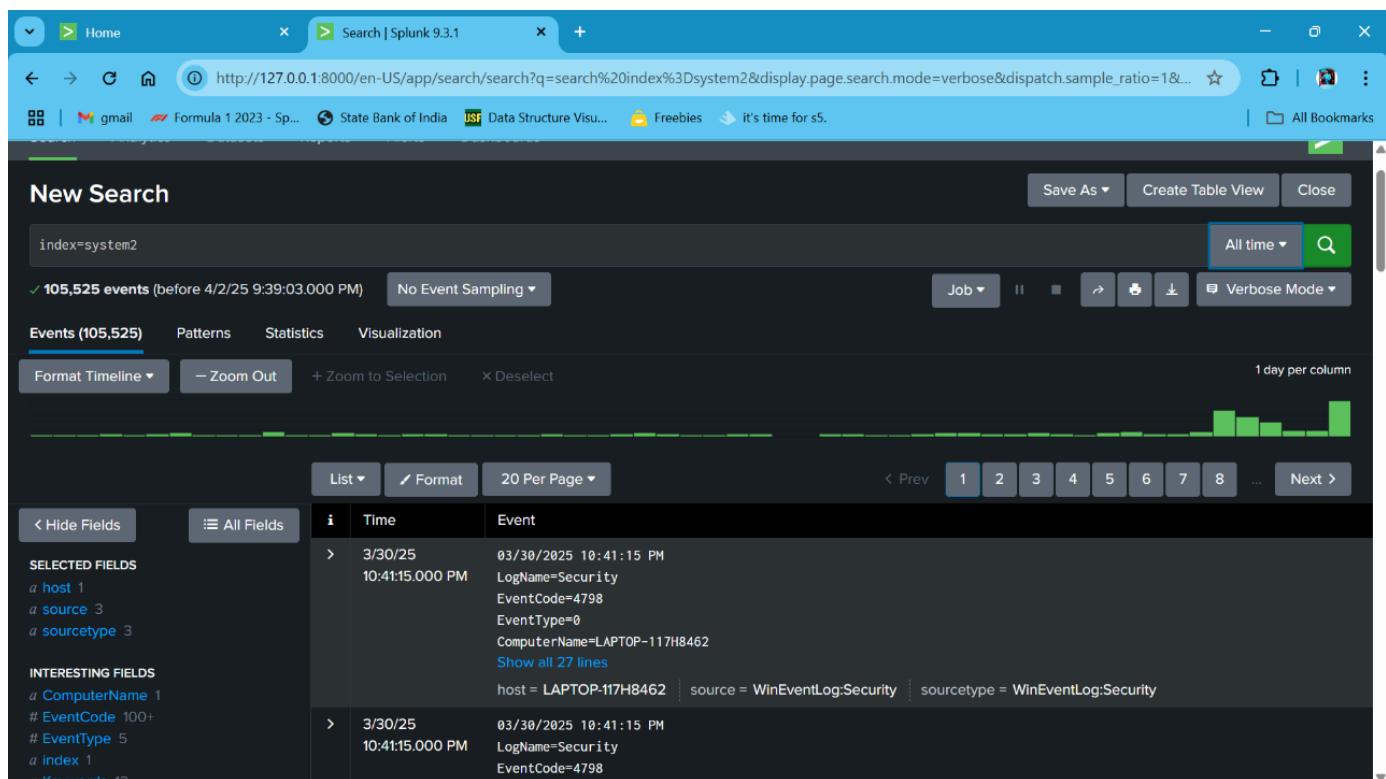
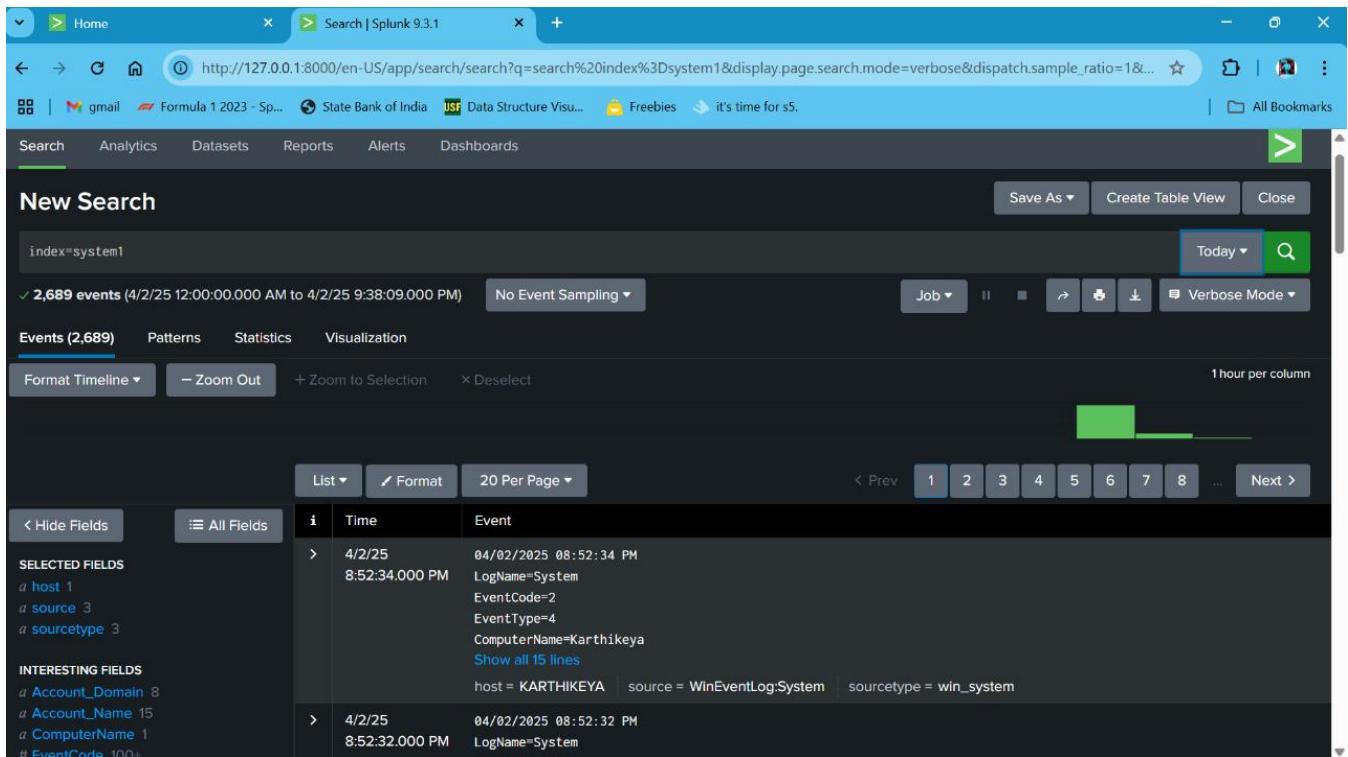
The screenshot shows the 'splunk>enterprise' Settings interface. The URL in the address bar is 'http://127.0.0.1:8000/en-US/manager/launcher/data/inputs/tcp/cooked'. The page title is 'Receive data'. It shows a table of receiving ports with two items listed: port 9997 (Enabled) and port 9998 (Enabled). A green 'New Receiving Port' button is visible at the top right. The table has columns for 'Listen on this port', 'Status', and 'Actions'.

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

system1	Edit	Delete	Disable	Events	search	18 MB	2 GB	102K	3 months ago	42 minutes ago	D:\Splunk Data\splunk\sys tem1\db	N/A
system2	Edit	Delete	Disable	Events	search	17 MB	2 GB	106K	2 months ago	3 days ago	D:\Splunk Data\splunk\sys tem2\db	N/A

Continued....

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



Continued....

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

Screenshots of Splunk Enterprise interface:

Searches, Reports, and Alerts

3 Searches, Reports, and Alerts Type: All ▾ App: Search & Reporting (search) ▾ Owner: Administrator (admin) ▾ filter 10 per page ▾

Name	Actions	Type	Next Scheduled Time	Display View	Owner	App	Alerts	Sharing	Status
Multiple Event Occurrences	Edit ▾ Run ▾ View Recent ▾	Report	2025-04-02 22:00:00 India Standard Time	none	admin	search	0	Private	Enabled
System Event Occurrences	Edit ▾ Run ▾ View Recent ▾	Alert	2025-04-02 22:00:00 India Standard Time	none	admin	search	0	Private	Enabled
Windows Events Summary	Edit ▾ Run ▾ View Recent ▾	Report	2025-04-02 22:00:00 India Standard Time	none	admin	search	0	Private	Enabled

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

Screenshots of Splunk Enterprise interface:

Windows Events Summary

index=_system1 source="WinEventLog:*" | stats dc(EventCode) AS UniqueEventCodes, values(SourceName) AS SourceNames, values(Message) AS Messages BY EventCode | table EventCode SourceNames Messages

2,739 events (4/1/25 9:30:00.000 PM to 4/2/25 9:42:49.000 PM) No Event Sampling ▾ Job ▾ Last 24 hours ▾ Verbose Mode ▾

Events (2,739) Patterns Statistics (136) Visualization

20 Per Page ▾ Format Preview ▾ 1 2 3 4 5 6 7 Next ▾

EventCode	SourceNames	Messages
0 EMP_UDSA		Intel(R) Dynamic Application Loader Host Interface Service started.
IntelDalJhi		Service started/resumed
K7EmIPxy		Service stopped.
K7RTScan		The operation completed successfully.
K7TSMngr		
LMS		
MiService		
OSDService		

Continued....

Home | Searches, reports, and alerts | Search | Splunk 9.3.1

http://127.0.0.1:8000/en-US/app/search/search?s=%2FservicesNS%2Fadmin%2Fsearch%2Fsaved%2Fsearches%2Fmultiple%2520Event%2520Occu... ☆

All Bookmarks

Multiple Event Occurrences

index=system1 sourcetype="WinEventLog:Security" | stats dc(EventCode) AS EventCodes, values(SourceName) AS SourceNames, values(Message) AS Messages BY EventCode | table EventCode SourceNames Messages

✓ 2,040 events (4/1/25 12:00:00.000 AM to 4/2/25 12:00:00.000 AM) No Event Sampling ▾ Job ▾ II ■ ⌂ ⌂ ⌂ Verbose Mode ▾

Events (2,040) Patterns Statistics (24) Visualization

20 Per Page ▾ Format Preview ▾

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.

< Prev 1 2 Next >

Home | Searches, reports, and alerts | 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... ☆

All Bookmarks

splunk>enterprise Apps ▾

Administrator 2 Messages Settings Activity Help Find Q

Search Analytics Datasets Reports Alerts Dashboards

System Event Occurrences

index=system1 sourcetype="WinEventLog:Security"
| bin _time span=1d
| stats count by _time, EventCode, SourceName, Message
| where count > 2
| table EventCode, SourceName, Message

✓ 2,040 events (4/1/25 12:00:00.000 AM to 4/2/25 12:00:00.000 AM) No Event Sampling ▾ Job ▾ II ■ ⌂ ⌂ ⌂ 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

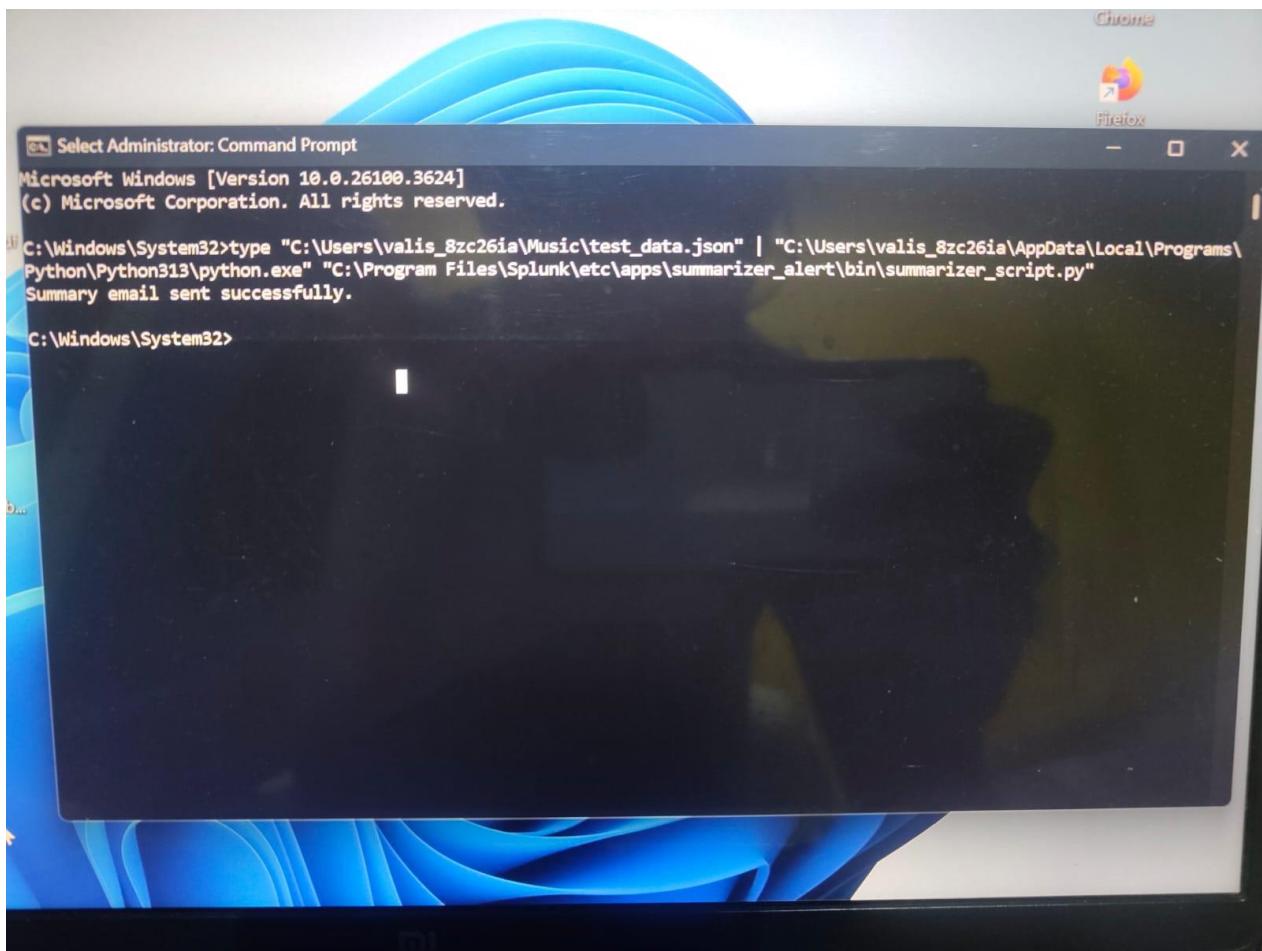
- **Checkout the script here:**

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.

Splunk Windows Logs Summary Alert



[REDACTED]
to bcc: me ▾

```
{  
    "Total Events": 2,  
    "Most Common Event Codes": {  
        "4624": 1,  
        "4625": 1  
    },  
    "Most Frequent Sources": {  
        "Security": 2  
    },  
    "Event Messages": {  
        "4624": [  
            "User logged in"  
        ],  
        "4625": [  
            "Login failed"  
        ]  
    }  
}
```

Continued....

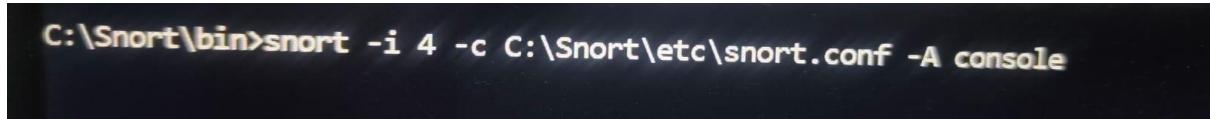
4. Snort Intrusion Detection System Setup

4.1 Overview

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

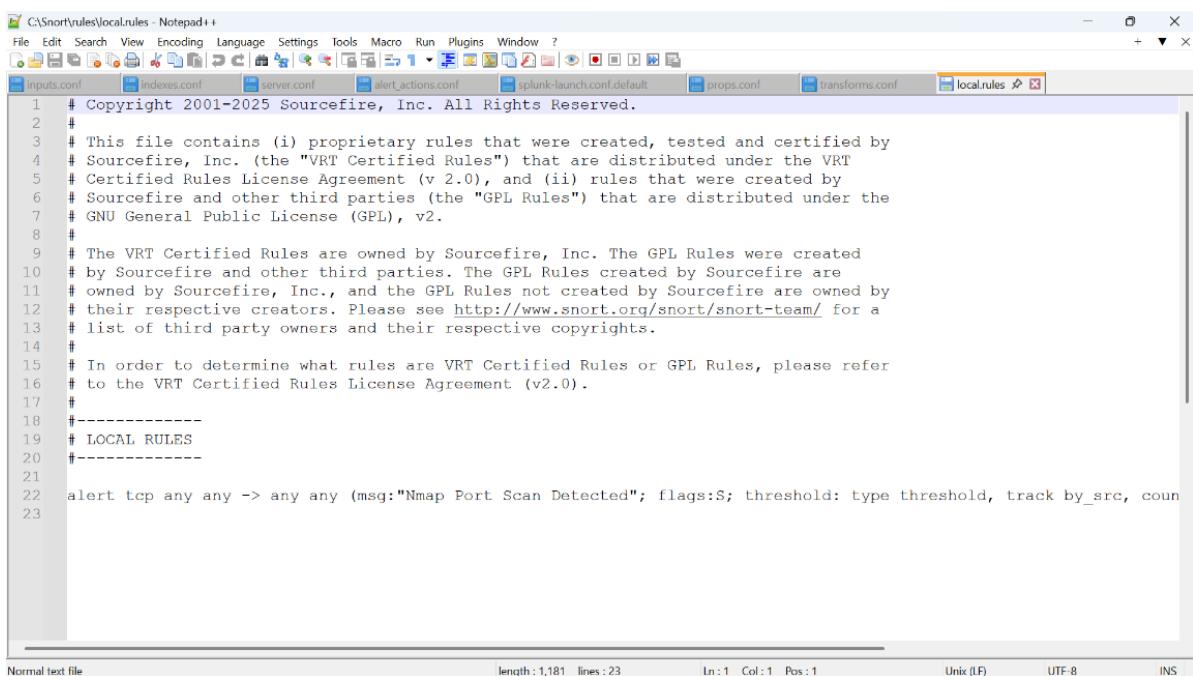
4.2 Configuration Details

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



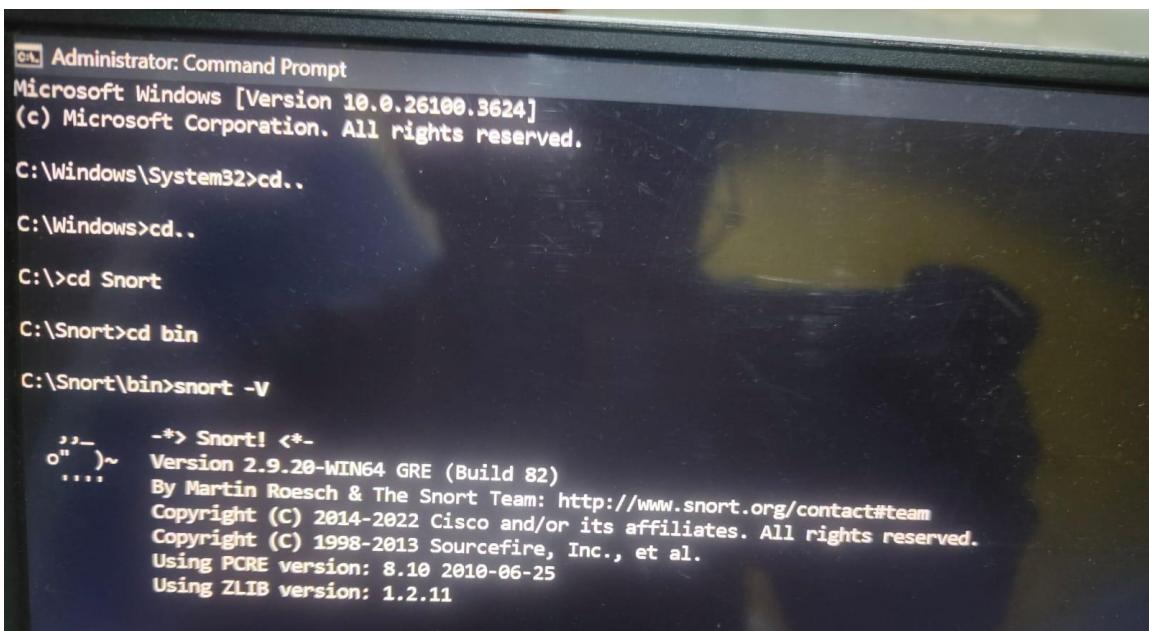
```
C:\Snort\bin>snort -i 4 -c C:\Snort\etc\snort.conf -A console
```

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



```
C:\Snort\rules\local.rules - Notepad++  
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?  
inputs.conf indexes.conf server.conf alert_actions.conf splunk-launch.conf.default props.conf transforms.conf local.rules  
1 # Copyright 2001-2025 Sourcefire, Inc. All Rights Reserved.  
2 #  
3 # This file contains (i) proprietary rules that were created, tested and certified by  
4 # Sourcefire, Inc. (the "VRT Certified Rules") that are distributed under the VRT  
5 # Certified Rules License Agreement (v 2.0), and (ii) rules that were created by  
6 # Sourcefire and other third parties (the "GPL Rules") that are distributed under the  
7 # GNU General Public License (GPL), v2.  
8 #  
9 # The VRT Certified Rules are owned by Sourcefire, Inc. The GPL Rules were created  
10 # by Sourcefire and other third parties. The GPL Rules created by Sourcefire are  
11 # owned by Sourcefire, Inc., and the GPL Rules not created by Sourcefire are owned by  
12 # their respective creators. Please see http://www.snort.org/snort-snort-team/ for a  
13 # list of third party owners and their respective copyrights.  
14 #  
15 # In order to determine what rules are VRT Certified Rules or GPL Rules, please refer  
16 # to the VRT Certified Rules License Agreement (v2.0).  
17 #  
18 #-----  
19 # LOCAL RULES  
20 #-----  
21  
22 alert tcp any any -> any any (msg:"Nmap Port Scan Detected"; flags:S; threshold: type threshold, track by_src, count  
23
```

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



```
Administrator: Command Prompt  
Microsoft Windows [Version 10.0.26100.3624]  
(c) Microsoft Corporation. All rights reserved.  
C:\Windows\System32>cd..  
C:\Windows>cd..  
C:\>cd Snort  
C:\Snort>cd bin  
C:\Snort\bin>snort -V  
--> Snort! <--  
o" )~ Version 2.9.20-WIN64 GRE (Build 82)  
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team  
Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.  
Copyright (C) 1998-2013 Sourcefire, Inc., et al.  
Using PCRE version: 8.10 2010-06-25  
Using ZLIB version: 1.2.11
```

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

The screenshot shows a terminal window with the title bar "How to forward logs into splunk pro" and the tab "portscan.log". The window contains the following text:

```
Priority Count: 3
Connection Count: 0
IP Count: 3
Scanned IP Range: 142.251.42.74:192.168.1.1
Port/Proto Count: 3
Port/Proto Range: 53:443

Time: 04/01-21:51:27.469518
event_ref: 5
192.168.1.12 -> 40.99.34.162 (portscan) Open Port
Open Port: 443

Time: 04/01-21:51:27.474274
event_ref: 5
192.168.1.12 -> 40.99.34.162 (portscan) Open Port
Open Port: 443

Time: 04/01-21:51:28.403806
event_ref: 5
192.168.1.12 -> 20.189.173.14 (portscan) Open Port
Open Port: 443

Time: 04/01-21:51:28.667999
event_ref: 5
192.168.1.12 -> 20.189.173.14 (portscan) Open Port
Open Port: 443

Time: 04/01-21:51:28.739581
event_id: 11
192.168.1.12 -> 184.26.54.122 (portscan) UDP Filtered Portsweep
Priority Count: 0
Connection Count: 30
IP Count: 7
Scanned IP Range: 184.26.54.122:239.255.255.250
Port/Proto Count: 7
Port/Proto Range: 53:3702

--
```

Ln 1, Col 1 | 5,571 characters

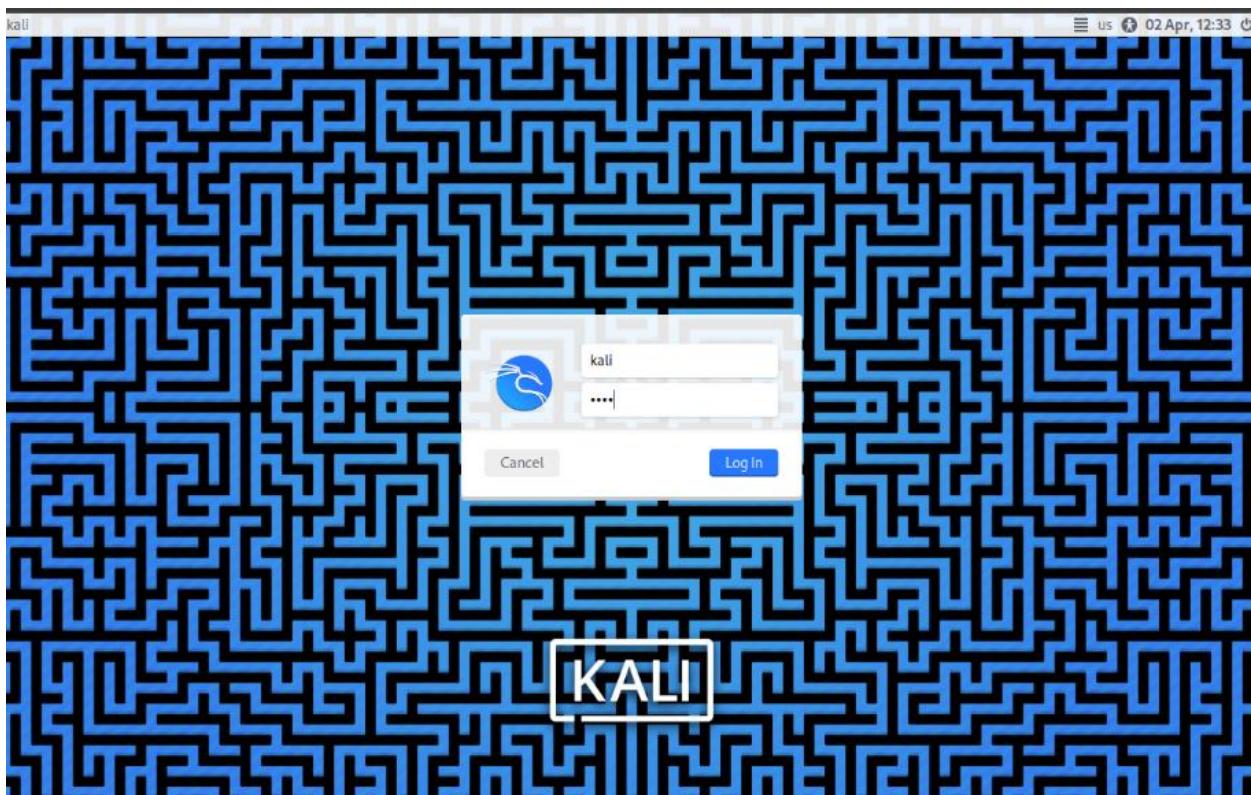
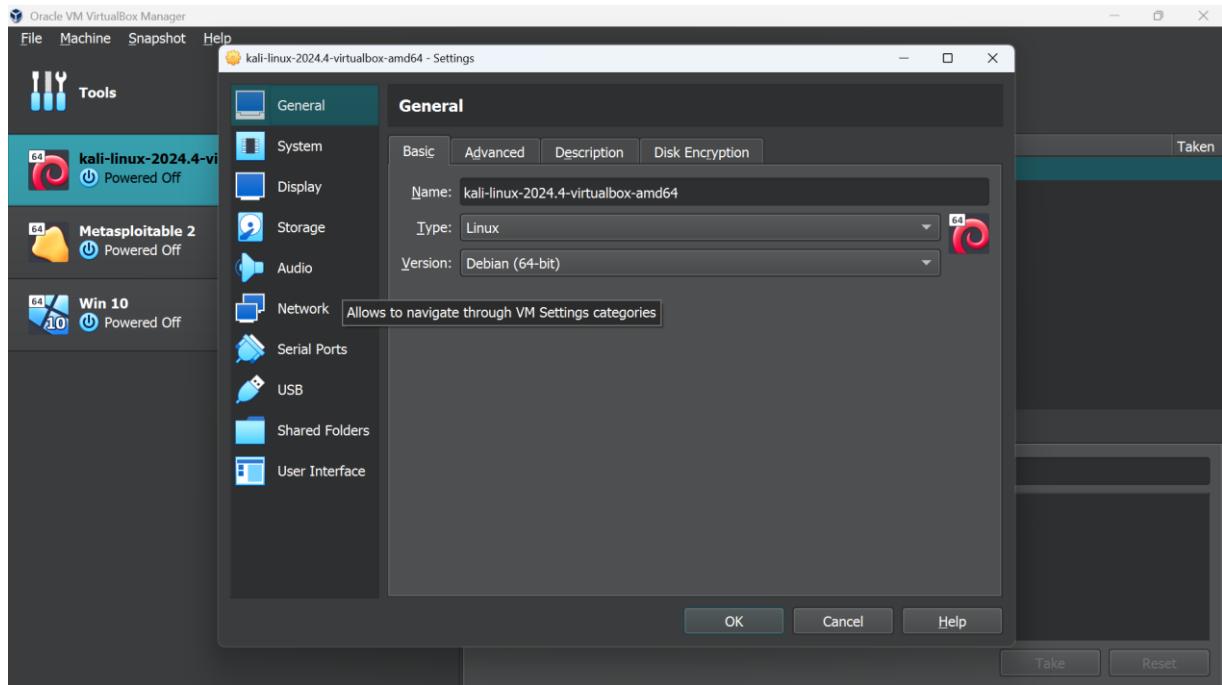
5. Kali Linux Setup and Penetration Testing

5.1 Overview

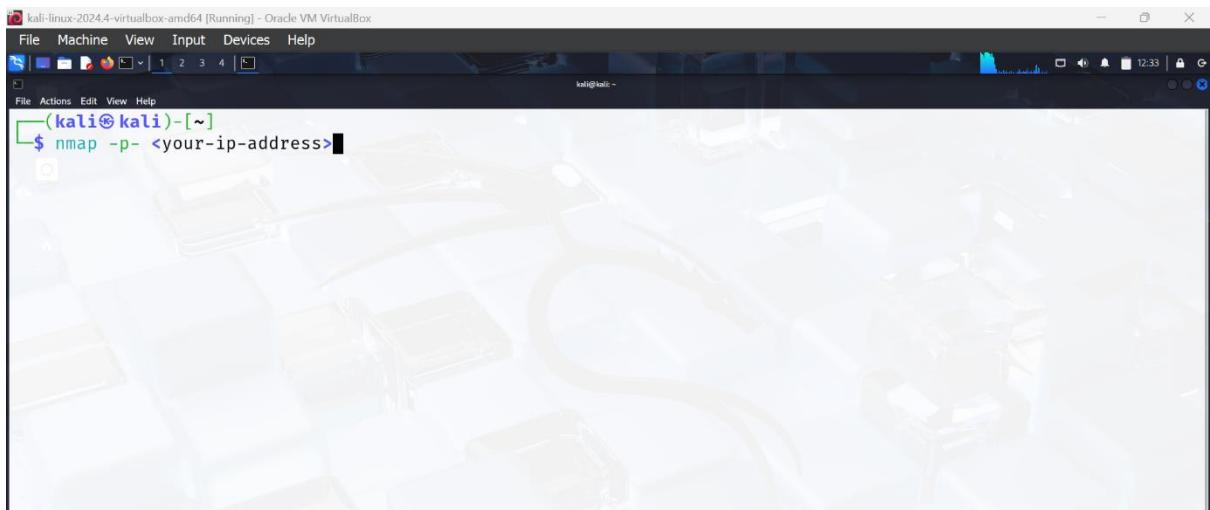
Kali Linux was used for penetration testing to assess network security.

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.

```
$ nmap -Pn -v -p 1-1000 192.168.50.205
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-02 13:27 EDT
Initiating ARP Ping Scan at 13:27
Scanning 192.168.50.205 [1 port]
Completed ARP Ping Scan at 13:27, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:27
Completed Parallel DNS resolution of 1 host. at 13:27, 0.00s elapsed
Initiating SYN Stealth Scan at 13:27
Scanning Karthikeya (192.168.50.205) [1000 ports]
Nmap Stealth Scan Timing: About 1.69% done; ETC: 13:53 (0:30:02 remaining)
SYN Stealth Scan Timing: About 3.09% done; ETC: 13:55 (0:31:54 remaining)
SYN Stealth Scan Timing: About 6.06% done; ETC: 13:58 (0:33:36 remaining)
Stats: 0/104:01 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 11.19% done; ETC: 13:58 (0:31:53 remaining)
```

- **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.