DETECTING AND VISUALIZING NMAP SCANS USING SURICATA AND SPLUNK

INTRODUCTION

This project simulates a real-world network intrusion detection and monitoring scenario. The goal was to detect Nmap SYN scan activity (reconnaissance) from an attacker in real time using Suricata and to visualize the resulting alert patterns through Splunk.

While SYN scan is not a direct attack, it's a reconnaissance technique. It is usually used during the information-gathering phase of an attack to identify open ports on a system.

PROJECT OBJECTIVES:

- Install and Configure Suricata to monitor network traffic in real-time.
- Create a custom rule to detect Nmap SYN scans.
- Run an Nmap scan from Kali Linux to trigger alerts.
- Forward Suricata logs to Splunk using Splunk Universal Forwarder.

LAB SETUP

VIRTUAL MACHINE	ROLE	IP ADDRESS
UBUNTU VM	Victim Machine running Suricata	192.168.1.30
Kali Linux VM	Attacker Machine simulating Nmap scans	192.168.1.59
Splunk Server	Receives logs and visualizes Alerts	192.168.1.200

PHASE 1: Installing and Configuring Suricata on Ubuntu (Victim Machine)

Suricata Repository and Packages were installed using:

Bash

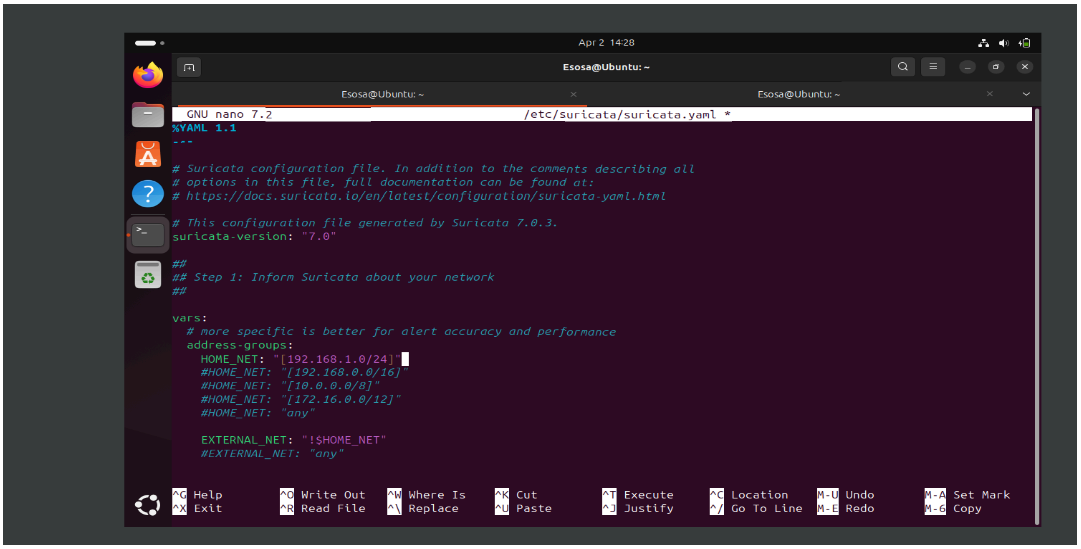
```
sudo add-get-repository ppa:suricata-stable
sudo apt update
sudo apt install suricata -y
suricata --build-info
sudo systemctl enable Suricata
sudo systemctl start Suricata
```

Configured Suricata:

The HOME_NET variable was set to the home network.

```
sudo nano /etc/suricata/suricata.yaml
```

```
Home-net: “[192.168.1.0/24]”
```



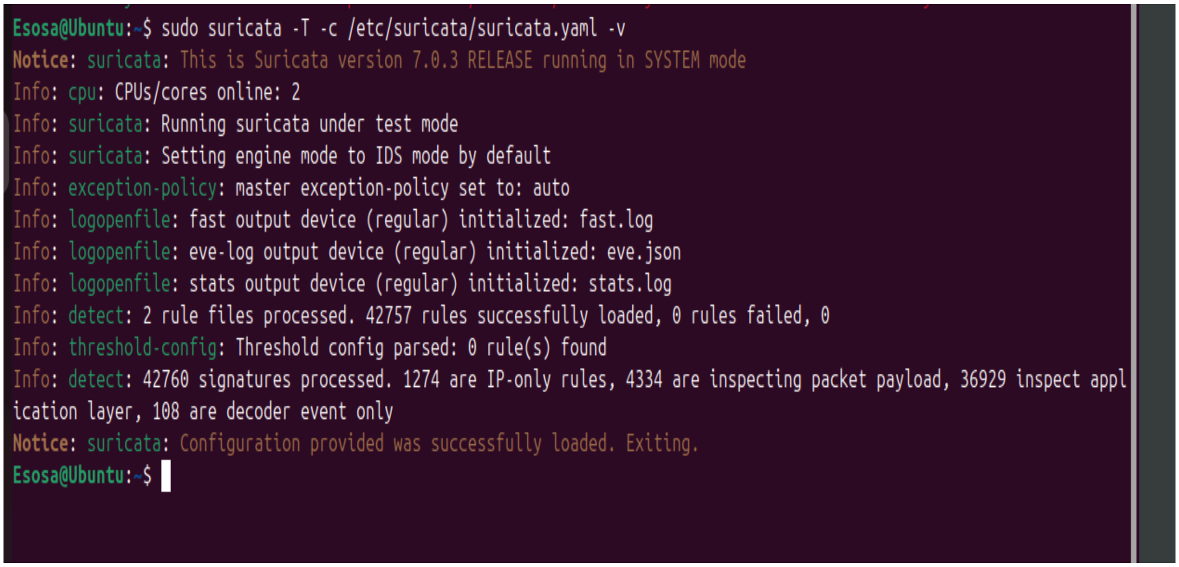
```
  GNU nano 7.2                          /etc/suricata/suricata.yaml *
%YAML 1.1
---

# Suricata configuration file. In addition to the comments describing all
# options in this file, full documentation can be found at:
# https://docs.suricata.io/en/latest/configuration/suricata-yaml.html

# This configuration file generated by Suricata 7.0.3.
suricata-version: "7.0"

##
## Step 1: Inform Suricata about your network
##

vars:
  # more specific is better for alert accuracy and performance
  address-groups:
    HOME_NET: "[192.168.1.0/24]"
    #HOME_NET: "[192.168.0.0/16]"
    #HOME_NET: "[10.0.0.0/8]"
    #HOME_NET: "[172.16.0.0/12]"
    #HOME_NET: "any"

    EXTERNAL_NET: "!$HOME_NET"
    #EXTERNAL_NET: "any"

^G Help       ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo      M-A Set Mark
^X Exit       ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^/ Go To Line M-E Redo      M-6 Copy
```

Tested the configuration:

Bash

```
sudo suricata -T -c  /etc/suricata/suricata.yaml -v
```

The test was successful, and the output below was generated:



```
Esosa@Ubuntu:~$ sudo suricata -T -c /etc/suricata/suricata.yaml -v
Notice: suricata: This is Suricata version 7.0.3 RELEASE running in SYSTEM mode
Info: cpu: CPUs/cores online: 2
Info: suricata: Running suricata under test mode
Info: suricata: Setting engine mode to IDS mode by default
Info: exception-policy: master exception-policy set to: auto
Info: logopenfile: fast output device (regular) initialized: fast.log
Info: logopenfile: eve-log output device (regular) initialized: eve.json
Info: logopenfile: stats output device (regular) initialized: stats.log
Info: detect: 2 rule files processed. 42757 rules successfully loaded, 0 rules failed, 0
Info: threshold-config: Threshold config parsed: 0 rule(s) found
Info: detect: 42760 signatures processed. 1274 are IP-only rules, 4334 are inspecting packet payload, 36929 inspect appl
ication layer, 108 are decoder event only
Notice: suricata: Configuration provided was successfully loaded. Exiting.
Esosa@Ubuntu:~$
```

PHASE 2: Creating a Custom Suricata Rule to Detect SYN Scans

Created a Custom Rule:

A custom.rules file was created in the `/var/lib/suricata/rules` directory and a custom rule to detect Nmap SYN scans was added.

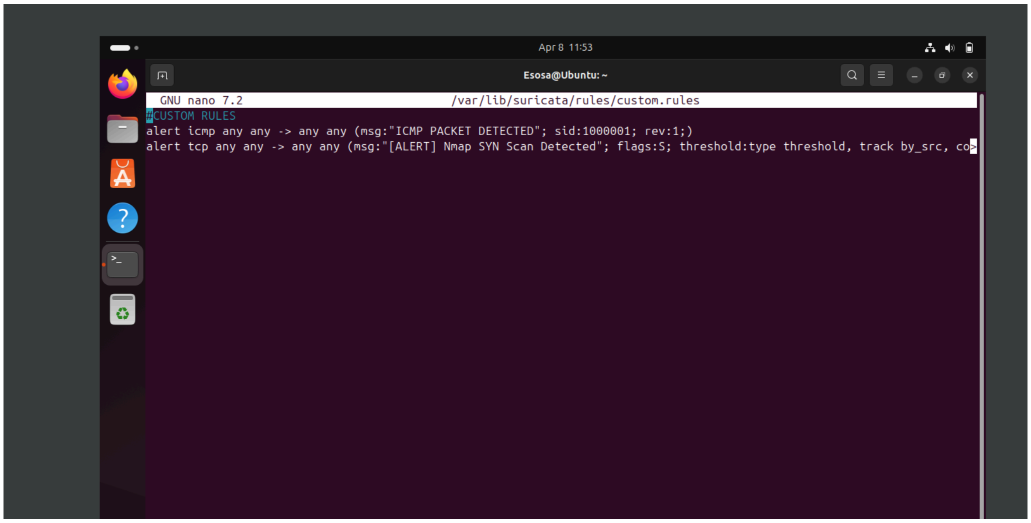
Bash

```bash
sudo nano /var/lib/suricata/rules/custom.rules
```

Rule:

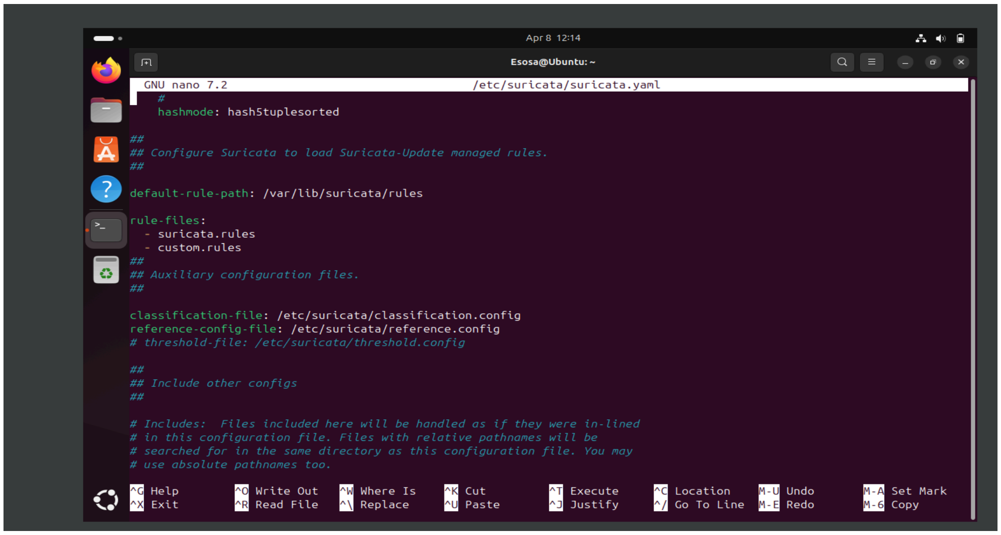
```
alert tcp any any -> any any (msg:" [ALERT] Nmap SYN Scan Detected"; flags:S; threshold: type threshold,  track by_src, count 5, seconds 10; sid:1000002; rev:1;)
```

- flags:S — Detects packets with only SYN flag
- threshold — Limits false positives: 5 packets in 10 seconds
- sid — Unique signature ID



```
  GNU nano 7.2                                /var/lib/suricata/rules/custom.rules
#CUSTOM RULES
alert icmp any any -> any any (msg:"ICMP PACKET DETECTED"; sid:1000001; rev:1;)
alert tcp any any -> any any (msg:"[ALERT] Nmap SYN Scan Detected"; flags:S; threshold:type threshold, track by_src, co>
```

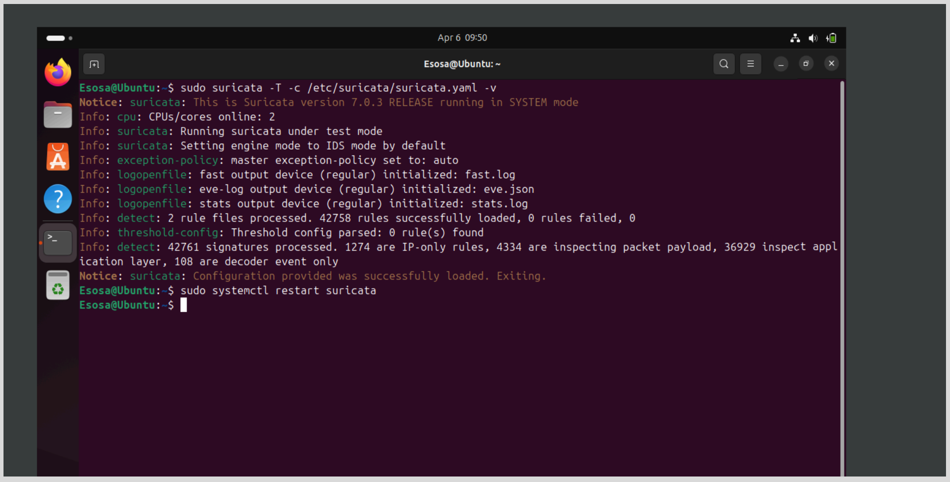
The Suricata config file was updated to include the custom rule file if it wasn't already:



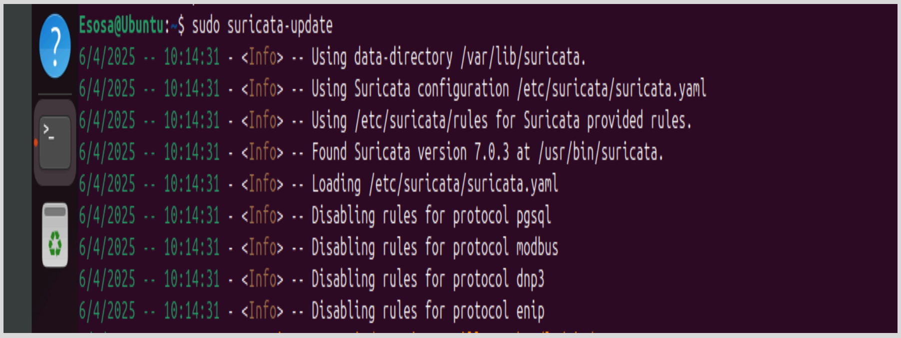
```
  GNU nano 7.2                                        /etc/suricata/suricata.yaml
    #
    hashmode: hash5tuplesorted

##
## Configure Suricata to load Suricata-Update managed rules.
##

default-rule-path: /var/lib/suricata/rules

rule-files:
  - suricata.rules
  - custom.rules
##
## Auxiliary configuration files.
##

classification-file: /etc/suricata/classification.config
reference-config-file: /etc/suricata/reference.config
# threshold-file: /etc/suricata/threshold.config

##
## Include other configs
##

# Includes:  Files included here will be handled as if they were in-lined
# in this configuration file. Files with relative pathnames will be
# searched for in the same directory as this configuration file. You may
# use absolute pathnames too.
```

The new configuration was tested, and Suricata was updated and restarted to load the new rule.

```bash
sudo suricata -T -c  /etc/suricata/suricata.yaml -v

sudo suricata-update

sudo systemctl restart suricata
```



```
Esosa@Ubuntu:~$ sudo suricata -T -c /etc/suricata/suricata.yaml -v
Notice: suricata: This is Suricata version 7.0.3 RELEASE running in SYSTEM mode
Info: cpu: CPUs/cores online: 2
Info: suricata: Running suricata under test mode
Info: suricata: Setting engine mode to IDS mode by default
Info: exception-policy: master exception-policy set to: auto
Info: logopenfile: fast output device (regular) initialized: fast.log
Info: logopenfile: eve-log output device (regular) initialized: eve.json
Info: logopenfile: stats output device (regular) initialized: stats.log
Info: detect: 2 rule files processed. 42758 rules successfully loaded, 0 rules failed, 0
Info: threshold-config: Threshold config parsed: 0 rule(s) found
Info: detect: 42761 signatures processed. 1274 are IP-only rules, 4334 are inspecting packet payload, 36929 inspect appl
ication layer, 108 are decoder event only
Notice: suricata: Configuration provided was successfully loaded. Exiting.
Esosa@Ubuntu:~$ sudo systemctl restart suricata
Esosa@Ubuntu:~$ 
```



```
Esosa@Ubuntu:~$ sudo suricata-update
6/4/2025 -- 10:14:31 - <Info> -- Using data-directory /var/lib/suricata.
6/4/2025 -- 10:14:31 - <Info> -- Using Suricata configuration /etc/suricata/suricata.yaml
6/4/2025 -- 10:14:31 - <Info> -- Using /etc/suricata/rules for Suricata provided rules.
6/4/2025 -- 10:14:31 - <Info> -- Found Suricata version 7.0.3 at /usr/bin/suricata.
6/4/2025 -- 10:14:31 - <Info> -- Loading /etc/suricata/suricata.yaml
6/4/2025 -- 10:14:31 - <Info> -- Disabling rules for protocol pgsql
6/4/2025 -- 10:14:31 - <Info> -- Disabling rules for protocol modbus
6/4/2025 -- 10:14:31 - <Info> -- Disabling rules for protocol dnp3
6/4/2025 -- 10:14:31 - <Info> -- Disabling rules for protocol enip
```

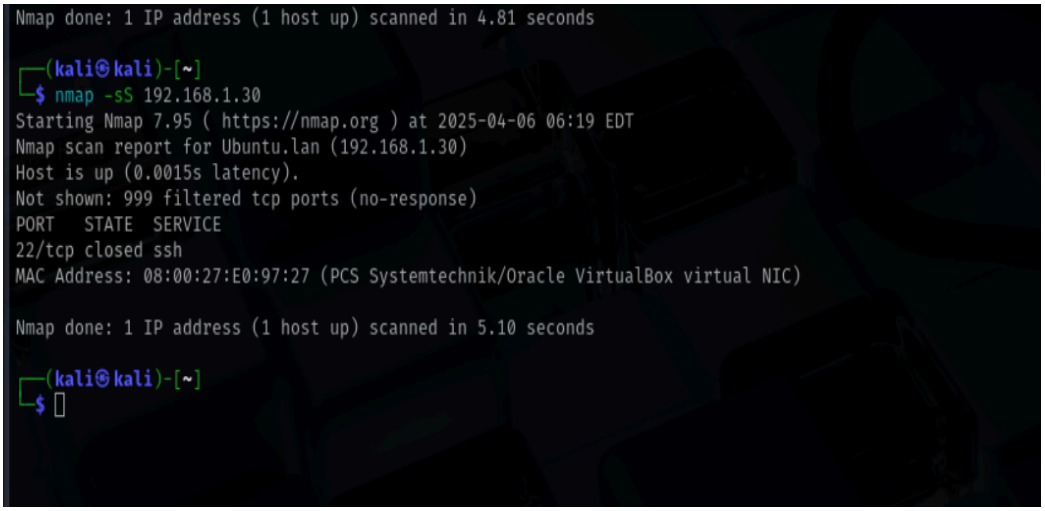
PHASE 3: Simulating an Nmap Scan from Kali Linux (Attacker Machine)

Nmap Scan:

On Kali Linux, the victim was scanned:

```bash
nmap -sS 192.168.1.30
```

This triggered TCP SYN packets to various ports.



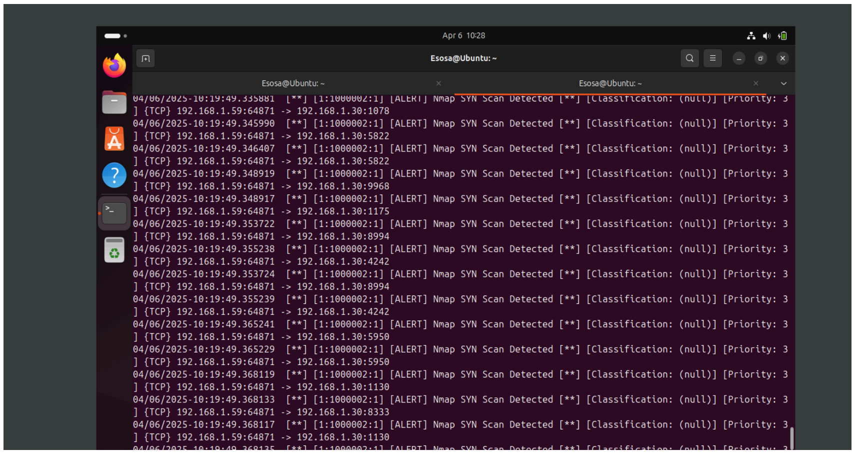
```
Nmap done: 1 IP address (1 host up) scanned in 4.81 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -sS 192.168.1.30
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-06 06:19 EDT
Nmap scan report for Ubuntu.lan (192.168.1.30)
Host is up (0.0015s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE  SERVICE
22/tcp closed ssh
MAC Address: 08:00:27:E0:97:27 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 5.10 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

Monitoring Logs in fast.log:

Once the scan was successful, Suricata began to log alerts to **fast.log** file by default:

```Bash
sudo nano /var/log/suricata/fast.log
```

Log output:



```
04/06/2025-10:19:49.335881  [**] [1:1000002:1] [ALERT] Nmap SYN Scan Detected [**] [Classification: (null)] [Priority: 3
] {TCP} 192.168.1.59:64871 -> 192.168.1.30:1078
04/06/2025-10:19:49.345990  [**] [1:1000002:1] [ALERT] Nmap SYN Scan Detected [**] [Classification: (null)] [Priority: 3
] {TCP} 192.168.1.59:64871 -> 192.168.1.30:5822
04/06/2025-10:19:49.346407  [**] [1:1000002:1] [ALERT] Nmap SYN Scan Detected [**] [Classification: (null)] [Priority: 3
] {TCP} 192.168.1.59:64871 -> 192.168.1.30:5822
04/06/2025-10:19:49.348919  [**] [1:1000002:1] [ALERT] Nmap SYN Scan Detected [**] [Classification: (null)] [Priority: 3
] {TCP} 192.168.1.59:64871 -> 192.168.1.30:9968
04/06/2025-10:19:49.348917  [**] [1:1000002:1] [ALERT] Nmap SYN Scan Detected [**] [Classification: (null)] [Priority: 3
] {TCP} 192.168.1.59:64871 -> 192.168.1.30:1175
04/06/2025-10:19:49.353722  [**] [1:1000002:1] [ALERT] Nmap SYN Scan Detected [**] [Classification: (null)] [Priority: 3
] {TCP} 192.168.1.59:64871 -> 192.168.1.30:8994
04/06/2025-10:19:49.355238  [**] [1:1000002:1] [ALERT] Nmap SYN Scan Detected [**] [Classification: (null)] [Priority: 3
] {TCP} 192.168.1.59:64871 -> 192.168.1.30:4242
04/06/2025-10:19:49.353724  [**] [1:1000002:1] [ALERT] Nmap SYN Scan Detected [**] [Classification: (null)] [Priority: 3
] {TCP} 192.168.1.59:64871 -> 192.168.1.30:8994
04/06/2025-10:19:49.355239  [**] [1:1000002:1] [ALERT] Nmap SYN Scan Detected [**] [Classification: (null)] [Priority: 3
] {TCP} 192.168.1.59:64871 -> 192.168.1.30:4242
04/06/2025-10:19:49.365241  [**] [1:1000002:1] [ALERT] Nmap SYN Scan Detected [**] [Classification: (null)] [Priority: 3
] {TCP} 192.168.1.59:64871 -> 192.168.1.30:5950
04/06/2025-10:19:49.365229  [**] [1:1000002:1] [ALERT] Nmap SYN Scan Detected [**] [Classification: (null)] [Priority: 3
] {TCP} 192.168.1.59:64871 -> 192.168.1.30:5950
04/06/2025-10:19:49.368119  [**] [1:1000002:1] [ALERT] Nmap SYN Scan Detected [**] [Classification: (null)] [Priority: 3
] {TCP} 192.168.1.59:64871 -> 192.168.1.30:1130
04/06/2025-10:19:49.368133  [**] [1:1000002:1] [ALERT] Nmap SYN Scan Detected [**] [Classification: (null)] [Priority: 3
] {TCP} 192.168.1.59:64871 -> 192.168.1.30:8333
04/06/2025-10:19:49.368117  [**] [1:1000002:1] [ALERT] Nmap SYN Scan Detected [**] [Classification: (null)] [Priority: 3
] {TCP} 192.168.1.59:64871 -> 192.168.1.30:1130
04/06/2025-10:19:49.368135  [**] [1:1000002:1] [ALERT] Nmap SYN Scan Detected [**] [Classification: (null)] [Priority: 3
```

PHASE 4: Installing and Configuring Splunk Universal Forwarder

Installed Splunk Universal forwarder:

Splunk Universal Forwarder was installed on the Victim VM with the procedure below:

- Download the .deb file
- Run `sudo dpkg -i splunkforwarder-<version>.deb`
- Run `sudo /opt/splunkforwarder/bin/splunk start --accept-license`

Configured Splunk Forwarder to Monitor Log File:

Splunk forwarder was configured to monitor the fast.log suricata log file using the command below:

Bash

```
sudo /opt/splunkforwarder/bin/splunk add monitor /var/log/suricata/fast.log -sourcetype suricata:fast
```

This command sets the sourcetype to **suricata:fast** so it'll be easy to search on Splunk.

Configured Splunk Forwarder to forward logs:

Splunk Forwarder was configured to forward logs to the Splunk server using the command below:

Bash

```
sudo /opt/splunkforwarder/bin/splunk add forward-server 192.168.1.200:9997
```

Enabled Splunk Forwarder to start on boot:

To enable splunk forwarder start on boot, the commands below were used:

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

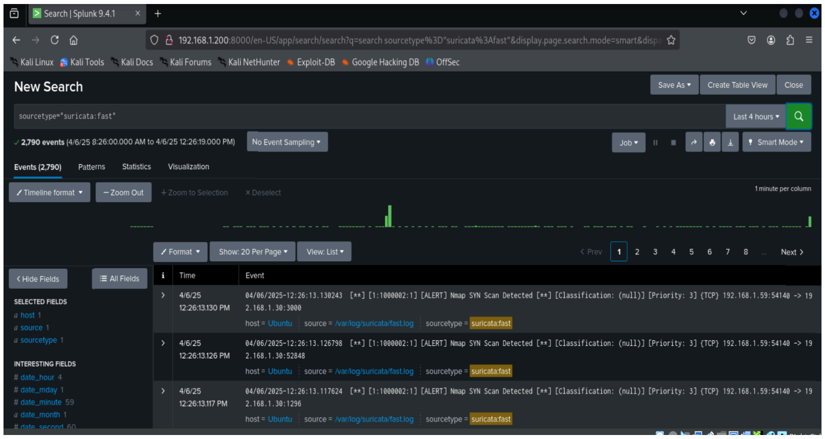
```
sudo /opt/splunkforwarder/bin/splunk enable boot-start
```

Visualizing Alerts in Splunk:

The query below was issued on splunk to visualize the contents of the fast.log file.

Spl

```
sourcetype="suricata:fast”
```

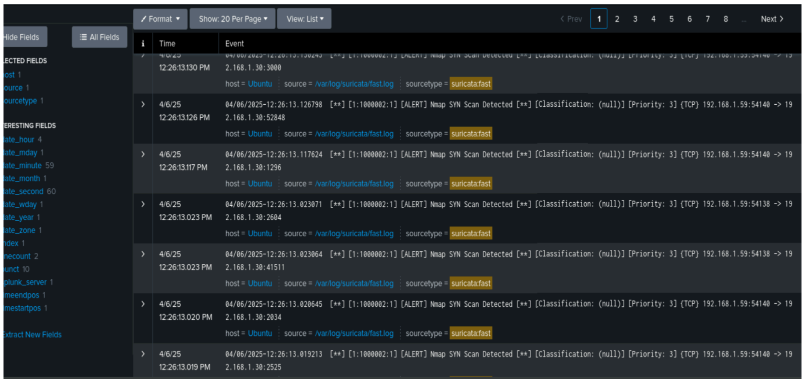


192.168.1.200:8000/en-US/app/search/search?q=search sourcetype%3D"suricata%3Afast"&display.page.search.mode=smart&dispa

```
sourcetype="suricata:fast"
```

✓ 2,790 events (4/6/25 8:26:00.000 AM to 4/6/25 12:26:19.000 PM)

i	Time	Event
›	4/6/25 12:26:13.130 PM	04/06/2025-12:26:13.130243 [**] [1:1000002:1] [ALERT] Nmap SYN Scan Detected [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.1.59:54140 -> 192.168.1.30:3000 host = Ubuntu source = /var/log/suricata/fast.log sourcetype = suricata:fast
›	4/6/25 12:26:13.126 PM	04/06/2025-12:26:13.126798 [**] [1:1000002:1] [ALERT] Nmap SYN Scan Detected [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.1.59:54140 -> 192.168.1.30:52848 host = Ubuntu source = /var/log/suricata/fast.log sourcetype = suricata:fast
›	4/6/25 12:26:13.117 PM	04/06/2025-12:26:13.117624 [**] [1:1000002:1] [ALERT] Nmap SYN Scan Detected [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.1.59:54140 -> 192.168.1.30:1296 host = Ubuntu source = /var/log/suricata/fast.log sourcetype = suricata:fast



i	Time	Event
	12:26:13.130 PM	2.168.1.30:3000 host = Ubuntu source = /var/log/suricata/fast.log sourcetype = suricata:fast
›	4/6/25 12:26:13.126 PM	04/06/2025-12:26:13.126798 [**] [1:1000002:1] [ALERT] Nmap SYN Scan Detected [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.1.59:54140 -> 192.168.1.30:52848 host = Ubuntu source = /var/log/suricata/fast.log sourcetype = suricata:fast
›	4/6/25 12:26:13.117 PM	04/06/2025-12:26:13.117624 [**] [1:1000002:1] [ALERT] Nmap SYN Scan Detected [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.1.59:54140 -> 192.168.1.30:1296 host = Ubuntu source = /var/log/suricata/fast.log sourcetype = suricata:fast
›	4/6/25 12:26:13.023 PM	04/06/2025-12:26:13.023071 [**] [1:1000002:1] [ALERT] Nmap SYN Scan Detected [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.1.59:54138 -> 192.168.1.30:2604 host = Ubuntu source = /var/log/suricata/fast.log sourcetype = suricata:fast
›	4/6/25 12:26:13.023 PM	04/06/2025-12:26:13.023064 [**] [1:1000002:1] [ALERT] Nmap SYN Scan Detected [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.1.59:54138 -> 192.168.1.30:41511 host = Ubuntu source = /var/log/suricata/fast.log sourcetype = suricata:fast
›	4/6/25 12:26:13.020 PM	04/06/2025-12:26:13.020645 [**] [1:1000002:1] [ALERT] Nmap SYN Scan Detected [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.1.59:54140 -> 192.168.1.30:2034 host = Ubuntu source = /var/log/suricata/fast.log sourcetype = suricata:fast
›	4/6/25 12:26:13.019 PM	04/06/2025-12:26:13.019213 [**] [1:1000002:1] [ALERT] Nmap SYN Scan Detected [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.1.59:54140 -> 192.168.1.30:2525

CONCLUSION

This project successfully demonstrated how an IDS (Suricata) and a SIEM (Splunk) can work together to detect reconnaissance attacks. By simulating an Nmap SYN scan from Kali Linux and creating a custom detection rule in Suricata, I was able to generate alerts that were forwarded and visualized in Splunk.

This mirrors real-world SOC workflows where early detection of unauthorized scans enables faster investigation and response, preventing attackers from progressing further in the Cyber kill chain.