PREPARED BY: ZAINAB ARIF

Exploring Suricata

What is Suricata?

INTRODUCTION TO SURICATA:

It is open source/free threat detection software/tool include IDS, IPS, and network monitoring.

Widely used in both private and public organizations.

Developed by community run /non-profit organization OSIF (Open Information Security Foundation).

Suricata has two operational modes:

1)Active(IPS) : Used to alert, log and block network traffic that matches specific rules.

2)Passive(IDS) : Used to identify, alert and log suspicious network traffic within a network.

Note: We cannot choose IPS directly instead of IDS because in IPS we might come across a lot of false positive cases or multiple issues, so initially we start with IDS.

Network Monitoring: Suricata analyze and log network traffic for troubleshooting and security insights.

HOW SURICATA WORKS :

It can be deployed as IDS on network to monitor network traffic.
It can be deployed as IPS in in-line mode to detect and stop malicious network traffic.

It identify malicious network traffic by predefined or set rules, when malicious network matched against a rule or set of rules, alert will generated and traffic will be logged.

SURICATA KEY FEATURES :

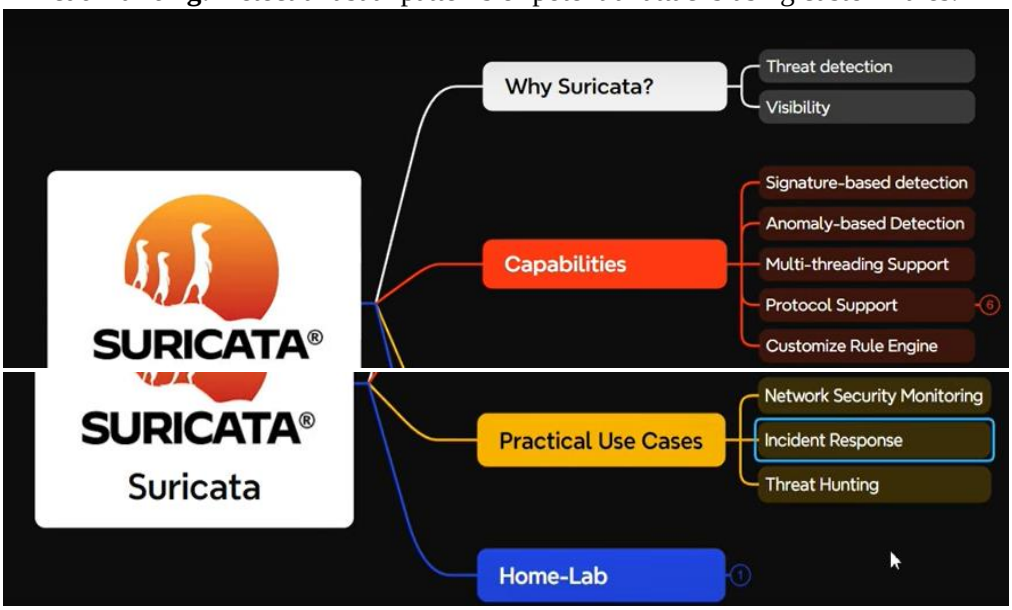
Protocol Detection: Detects protocols (like HTTP) on any port to spot malware and threats.

Fast Performance: Uses multiple cores for quick and efficient traffic monitoring.

Detailed Logging: Logs data for HTTP, DNS, and other protocols for easier analysis.

Compliance Auditing: Monitor networks to ensure adherence to security policies.

Threat Hunting: Detect unusual patterns or potential attacks using custom rules.



How install and configure it?

Installing it on Ubuntu.

Commands for Installation on Ubuntu:

sudo apt-get install software-properties-common

sudo add-apt-repository ppa:oisf/suricata-stable

sudo apt-get update

Then can install the latest stable with:

sudo apt-get install suricata

```
Jan 1 19:31
zainab@zainab-VMware-Virtual-Platform: ~
zainab@zainab-VMware-Virtual-Platform:~$ sudo apt-get install software-properties-common
sudo add-apt-repository ppa:oisf/suricata-stable
sudo apt-get update
[sudo] password for zainab:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
software-properties-common is already the newest version (0.99.48).
0 upgraded, 0 newly installed, 0 to remove and 3 not upgraded.
Repository: 'Types: deb
URIs: https://ppa.launchpadcontent.net/oisf/suricata-stable/ubuntu/
Suites: noble
Components: main
'
Description:
Suricata IDS/IPS/NSM stable packages
h suricata.io/
h oisf.net/

Suricata IDS/IPS/NSM - Suricata is a high performance Intrusion Detection and Prevention System and Network Security Mon
itoring engine.

Open Source and owned by a community run non-profit foundation, the Open Information Security Foundation (OISF). Suricat
a is developed by the OISF, its supporting vendors and the community.

This Engine supports:

- Multi-Threading - provides for extremely fast and flexible operation on multicore systems.
- Multi Tenancy - Per vlan/Per interface
- Uses Rust for most protocol detection/parsing
- TLS/SSL certificate matching/logging
- JA3 TLS client fingerprinting
- JA3S TLS server fingerprinting
```



```
Jan 1 19:32
zainab@zainab-VMware-Virtual-Platform: ~
- File MD5/SHA1/SHA256 matching
- Gzip Decompression
- Fast IP Matching
- Datasets matching
- Rustlang enabled protocol detection
- Lua scripting

and many more great features -
https://suricata.io/features/all-features/
More info: https://launchpad.net/~oisf/+archive/ubuntu/suricata-stable
Adding repository.
Press [ENTER] to continue or Ctrl-c to cancel.
Found existing deb entry in /etc/apt/sources.list.d/oisf-ubuntu-suricata-stable-noble.sources
Hit:1 http://pk.archive.ubuntu.com/ubuntu noble InRelease
Hit:2 http://pk.archive.ubuntu.com/ubuntu noble-updates InRelease
Hit:3 http://pk.archive.ubuntu.com/ubuntu noble-backports InRelease
Hit:4 https://ppa.launchpadcontent.net/oisf/suricata-stable/ubuntu noble InRelease
Hit:5 http://security.ubuntu.com/ubuntu noble-security InRelease
Reading package lists... Done
Hit:1 http://pk.archive.ubuntu.com/ubuntu noble InRelease
Hit:2 http://pk.archive.ubuntu.com/ubuntu noble-updates InRelease
Hit:3 http://pk.archive.ubuntu.com/ubuntu noble-backports InRelease
Hit:4 http://security.ubuntu.com/ubuntu noble-security InRelease
Hit:5 https://ppa.launchpadcontent.net/oisf/suricata-stable/ubuntu noble InRelease
Reading package lists... Done
zainab@zainab-VMware-Virtual-Platform:~$ sudo apt-get install suricata
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
suricata is already the newest version (1:7.0.8-0ubuntu0).
0 upgraded, 0 newly installed, 0 to remove and 3 not upgraded.
zainab@zainab-VMware-Virtual-Platform:~$
```


SURICATA SET UP:

Suricata is installed as see files in this

```
bash: /etc/suricata: Is a directory
zainab@zainab-VMware-Virtual-Platform:~$ cd /etc/suricata
zainab@zainab-VMware-Virtual-Platform:/etc/suricata$ ls
classification.config  reference.config  rules  suricata.yaml  suricata.yaml.dpkg-dist  threshold.config
zainab@zainab-VMware-Virtual-Platform:/etc/suricata$
```


Download and extract the Emerging Threats Suricata ruleset:

Jan 2 00:19

zainab@zainab-VMware-Virtual-Platform: /

```
zainab@zainab-VMware-Virtual-Platform:/etc/suricata$ cd ..
zainab@zainab-VMware-Virtual-Platform:/etc$ cd ..
zainab@zainab-VMware-Virtual-Platform:/$ cd /tmp/ && curl -LO https://rules.emergingthreats.net/open/suricata-6.0.8/emer
ging.rules.tar.gz
sudo tar -xvzf emerging.rules.tar.gz && sudo mv rules/*.rules /etc/suricata/rules/
sudo chmod 640 /etc/suricata/rules/*.rules
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
  0     0    0     0    0     0      0      0 --:--:--  0:00:01 --:--:--     0
```

Terminal

zainab@zainab-VMware-Virtual-Platform: /tmp

```
sudo tar -xvzf emerging.rules.tar.gz && sudo mv rules/*.rules /etc/suricata/rules/
sudo chmod 640 /etc/suricata/rules/*.rules
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 4593k  100 4593k    0     0  80562      0  0:00:58  0:00:58 --:--:-- 53658
[sudo] password for zainab:
rules/
rules/3coresec.rules
rules/BSD-License.txt
rules/LICENSE
rules/botcc.portgrouped.rules
rules/botcc.rules
rules/ciarmy.rules
rules/classification.config
rules/compromised-ips.txt
rules/compromised.rules
rules/drop.rules
rules/dshield.rules
rules/emerging-activex.rules
rules/emerging-adware_pup.rules
rules/emerging-attack_response.rules
rules/emerging-chat.rules
rules/emerging-coinminer.rules
rules/emerging-current_events.rules
rules/emerging-deleted.rules
rules/emerging-dns.rules
rules/emerging-dos.rules
rules/emerging-exploit.rules
rules/emerging-exploit_kit.rules
rules/emerging-ftp.rules
rules/emerging-games.rules
rules/emerging-hunting.rules
rules/emerging-icmp.rules
```

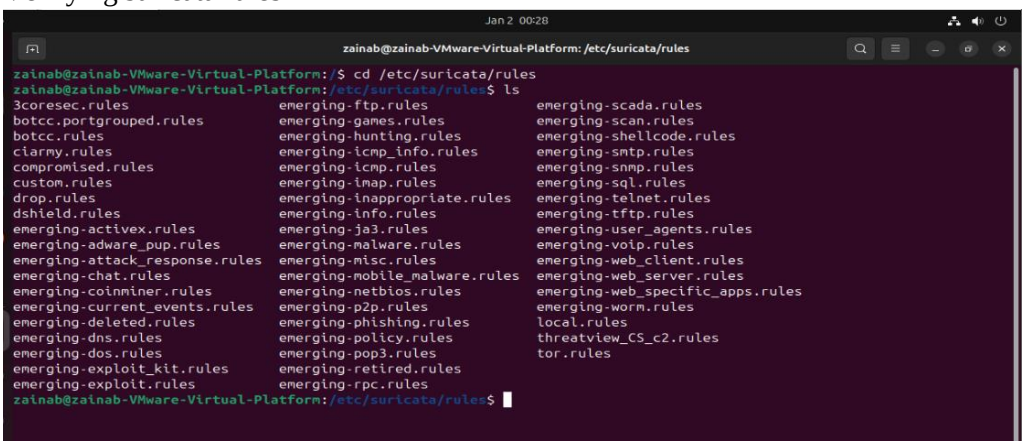
CDROM

zainab@zainab-VMware-Virtual-Platform: /tmp

```
rules/emerging-info.rules
rules/emerging-ja3.rules
rules/emerging-malware.rules
rules/emerging-misc.rules
rules/emerging-mobile_malware.rules
rules/emerging-netbios.rules
rules/emerging-p2p.rules
rules/emerging-phishing.rules
rules/emerging-policy.rules
rules/emerging-pop3.rules
rules/emerging-retired.rules
rules/emerging-rpc.rules
rules/emerging-scada.rules
rules/emerging-scan.rules
rules/emerging-shellcode.rules
rules/emerging-smtp.rules
rules/emerging-snmp.rules
rules/emerging-sql.rules
rules/emerging-telnet.rules
rules/emerging-tftp.rules
rules/emerging-user_agents.rules
rules/emerging-voip.rules
rules/emerging-web_client.rules
rules/emerging-web_server.rules
rules/emerging-web_specific_apps.rules
rules/emerging-worm.rules
rules/gpl-2.0.txt
rules/sid-msg.map
rules/suricata-5.0-enhanced-open.txt
rules/threatview_CS_c2.rules
rules/tor.rules
zainab@zainab-VMware-Virtual-Platform:/tmp$
```

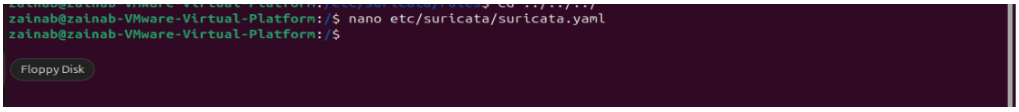
Floppy Disk

Verifying suricata rules



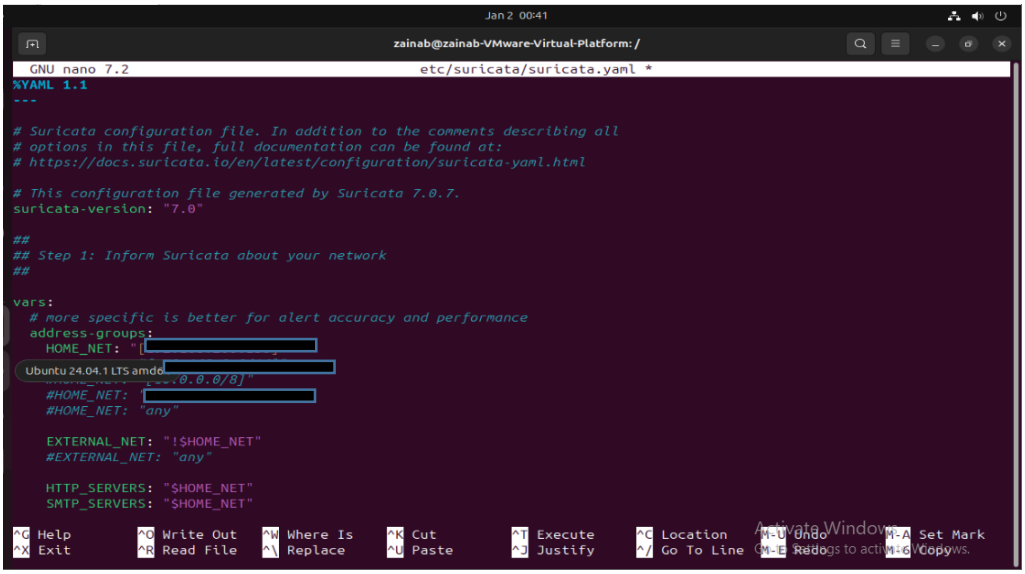
First copy ip address of Ubuntu through if config

Modify Suricata settings in the /etc/suricata/suricata.yaml file and set the following variables:
Run this command to open file



Under file do following changes

HOME_NET: "<UBUNTU_IP>"



because our server will be in public network so we we don't

know from what would be the external network right so will keep it any.So Uncomment it.

EXTERNAL_NET: "any"

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

    HTTP_SERVERS: "$HOME_NET"
    SMTP_SERVERS: "$HOME_NET"
```

default-rule-path: /etc/suricata/rules

rule-files:

- "*.rules"

Changes this

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

rule-files:
  - /etc/suricata/rules/local.rules
  - /etc/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
```

To this

```
##

default-rule-path: /etc/suricata/rules

rule-files:
  - "*.rules"
##
## Auxiliary configuration files.
```

Global stats configuration

stats:

enabled: Yes

it is default set

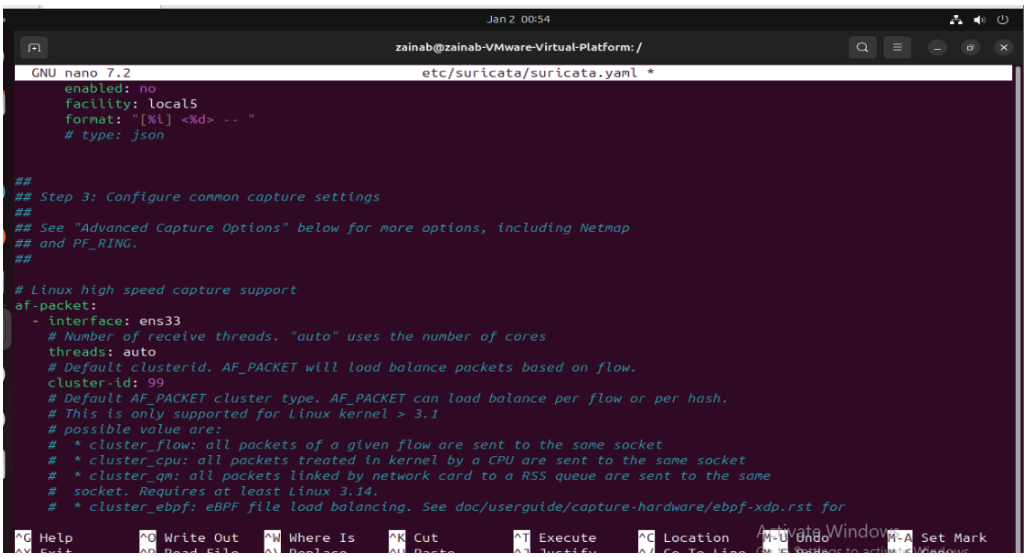
```
# Global stats configuration
stats:
  enabled: yes
  # The interval field (in seconds) controls the interval at
  # which stats are updated in the log.
  interval: 8
  # Add decode events to stats.
  CDROM
  # Add decoder event prefix in stats. Has been 'decoder' before, but that leads
  # to missing events in the eve.stats records. See issue #2225.
  #decoder-events-prefix: "decoder.event"
  # Add stream events as stats.
  #stream-events: false

                                [ Search Wrapped ]
^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
```

Linux high speed capture support

af-packet:

- interface: ens33 (change this according to your ip)



press ctrl+O then enter to save.
press ctrl+x to exit.

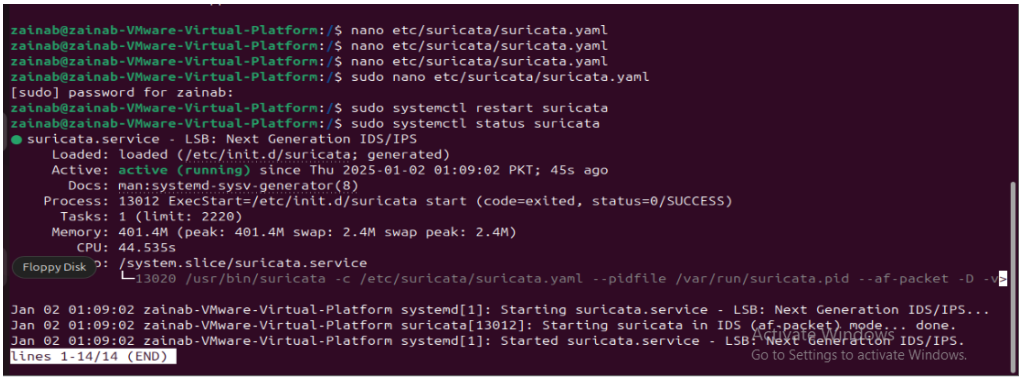
Note:If it deny permission to make changes then use sudo:

sudo nano etc/suricata/suricata.yaml

Restart the Suricata service:

sudo systemctl restart suricata

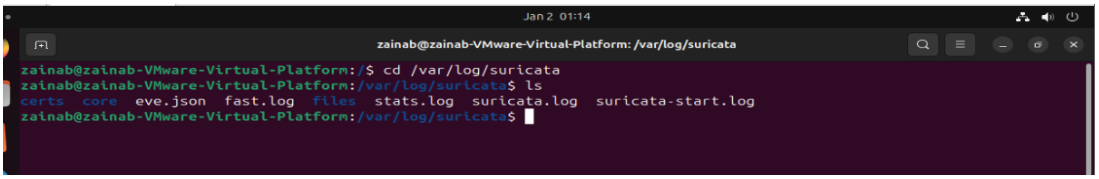
sudo systemctl status suricata



perfect as see it's active and running so all good ..

we can also verify the different logs , that's a better way of

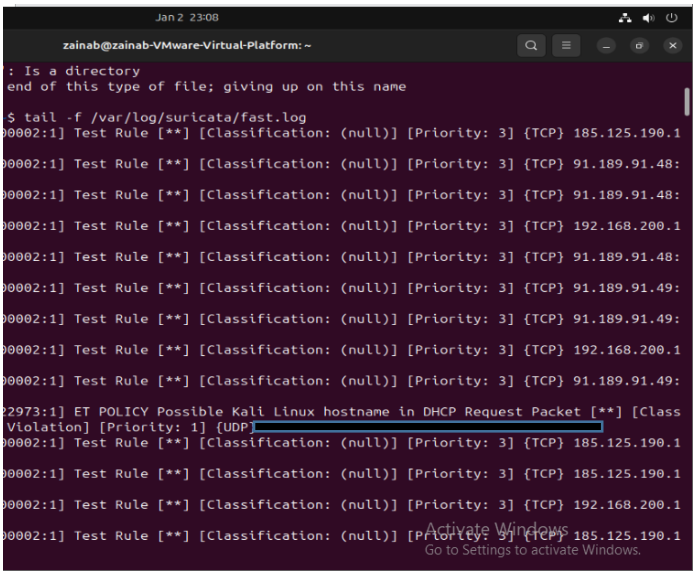
verifying it as the logs are stored in a different directory.
we can try by
cd /var/log/suricata



<u>View Logs:</u>

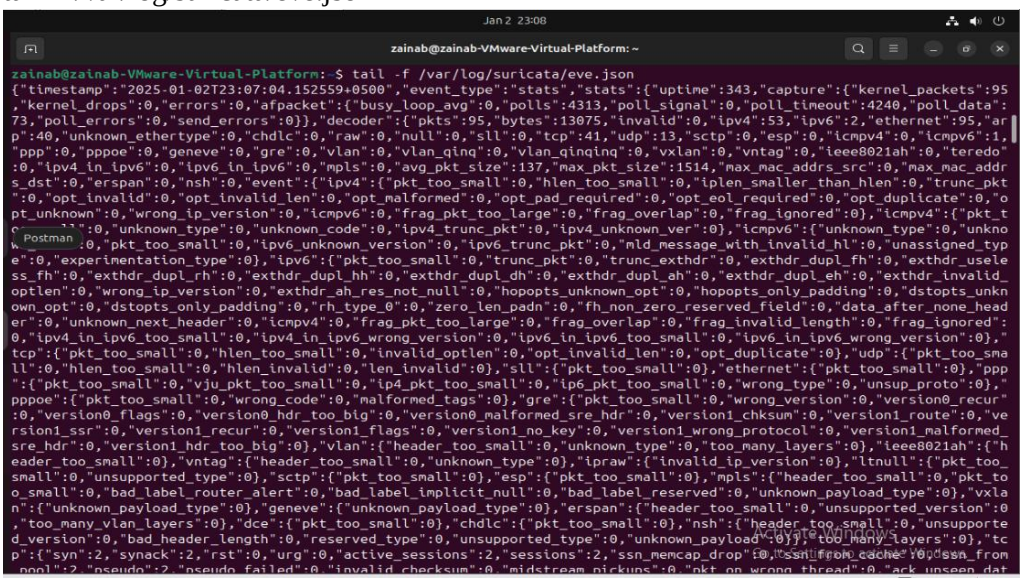
Open fast.log for quick alerts:

tail -f /var/log/suricata/fast.log



For detailed logs, use eve.json:

tail -f /var/log/suricata/eve.json



TESTING SURICATA:

Generate network traffic to test its capabilities:

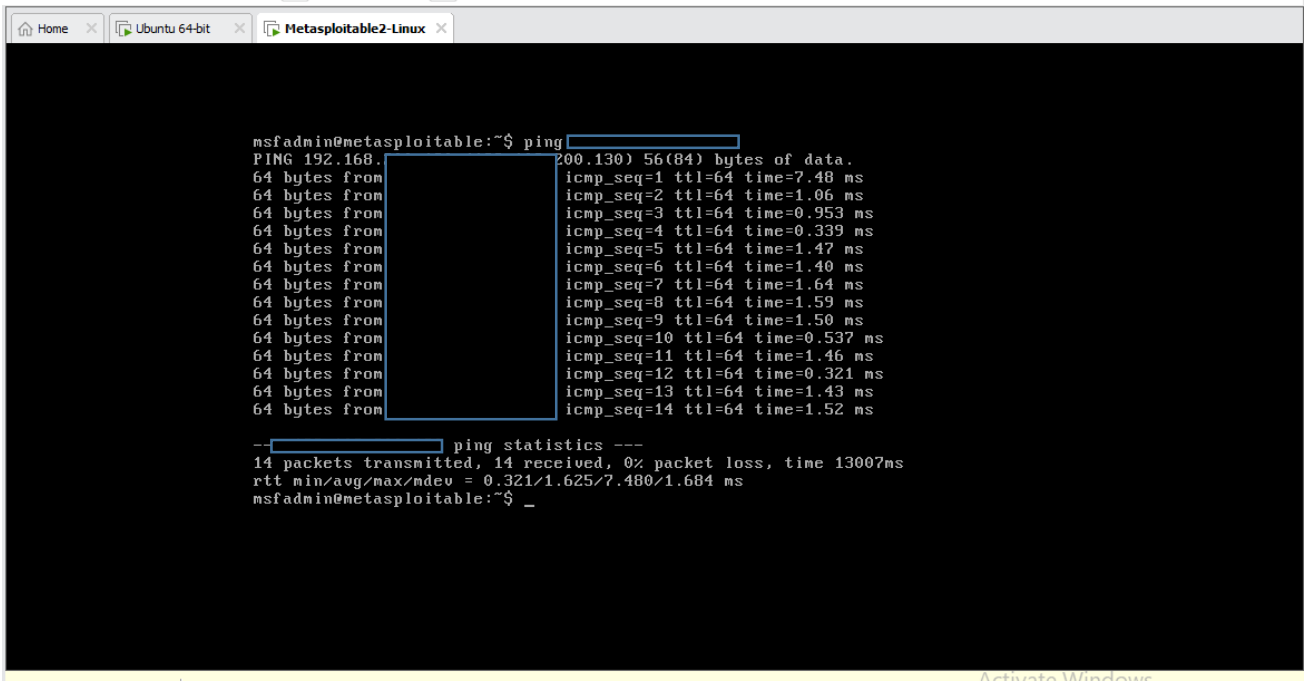
Ping Test

Ping your Ubuntu system

On another device metasploitable (on the same network), open a terminal and run:

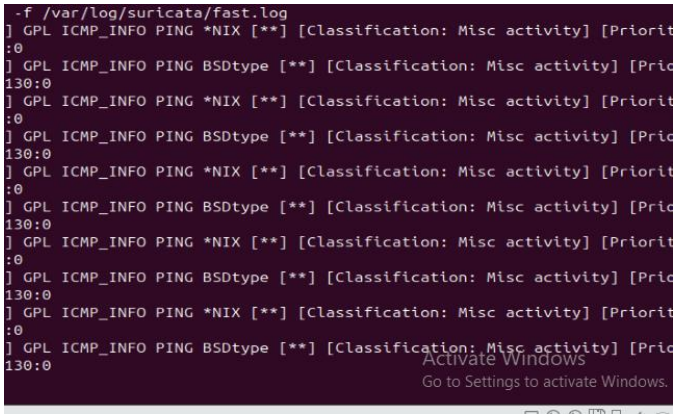
ping <Ubuntu_IP>

Replace <Ubuntu_IP> with the IP address of your Ubuntu system.



Check Suricata logs
Run the following command on your Ubuntu system to see the logs:

tail -f /var/log/suricata/fast.log



```
 -f /var/log/suricata/fast.log
] GPL ICMP_INFO PING *NIX [**] [Classification: Misc activity] [Priorit
:0
] GPL ICMP_INFO PING BSDtype [**] [Classification: Misc activity] [Pric
130:0
] GPL ICMP_INFO PING *NIX [**] [Classification: Misc activity] [Priorit
:0
] GPL ICMP_INFO PING BSDtype [**] [Classification: Misc activity] [Pric
130:0
] GPL ICMP_INFO PING *NIX [**] [Classification: Misc activity] [Priorit
:0
] GPL ICMP_INFO PING BSDtype [**] [Classification: Misc activity] [Pric
130:0
] GPL ICMP_INFO PING *NIX [**] [Classification: Misc activity] [Priorit
:0
] GPL ICMP_INFO PING BSDtype [**] [Classification: Misc activity] [Pric
130:0
] GPL ICMP_INFO PING *NIX [**] [Classification: Misc activity] [Priorit
:0
] GPL ICMP_INFO PING BSDtype [**] [Classification: Misc activity] [Pric
130:0
```

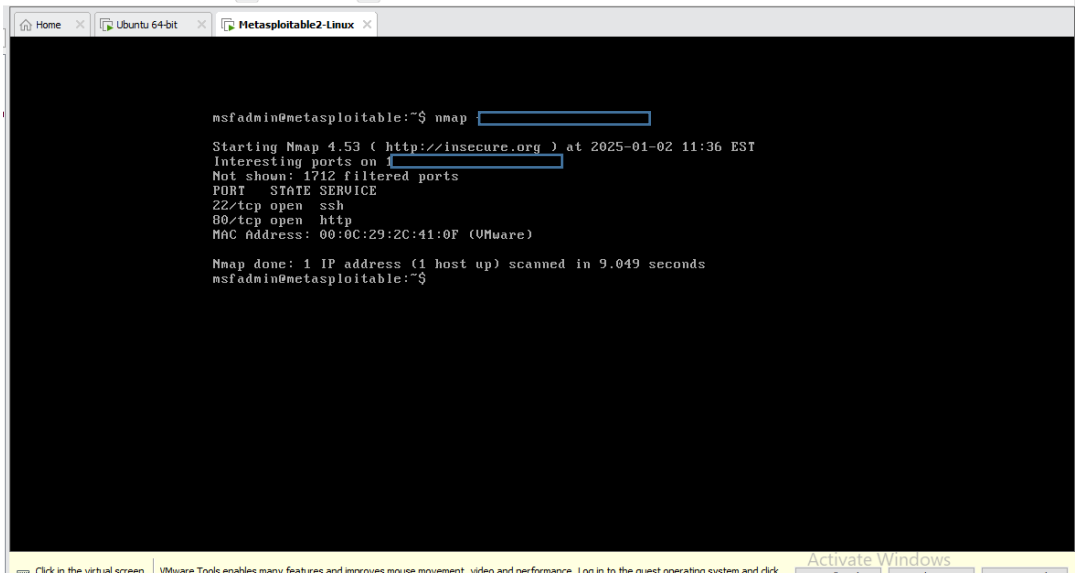
Look for entries related to ICMP traffic.

Port Scan

Run an nmap scan

From another device, use nmap to perform a SYN scan on your Ubuntu machine:bash

nmap -sS <Ubuntu_IP>



```
msfadmin@metasploitable:~$ nmap [redacted]

Starting Nmap 4.53 ( http://insecure.org ) at 2025-01-02 11:36 EST
Interesting ports on [redacted]
Not shown: 1712 filtered ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 00:0C:29:2C:41:0F (VMware)

Nmap done: 1 IP address (1 host up) scanned in 9.049 seconds
msfadmin@metasploitable:~$
```

Check Suricata logs

On your Ubuntu system, monitor the logs again for port scan alerts:

tail -f /var/log/suricata/fast.log

You should see alerts related to the port scanning activity.

What did you learn about Suricata rules?

Custom Rules for Threat Detection:

Objective: This demonstrates Suricata's flexibility, allowing us to detect specific attack patterns such as port scans, suspicious network traffic, or even application layer vulnerabilities.

Learn the structure of Suricata rules:

Action (e.g., alert)

Protocol (e.g., TCP, UDP)

Source IP, destination IP

Source port, destination port

Payload conditions (patterns in the data)

Steps to Implement Custom Rules

Step 1: Understand Suricata's Rule Syntax:
Suricata uses a simple and intuitive rule syntax to identify malicious or suspicious traffic patterns. These rules help detect everything from basic port scans to more complex attack vectors. The first step in our project is to familiarize ourselves with this syntax to create custom rules for detecting specific threats.

Step 2: Identify a Threat:

Next, we'll identify a network threat that we want Suricata to detect. This could be something simple, like a port scan

Step 3: Create a Custom Suricata Rule:

With Suricata, we can write rules to detect specific types of traffic. For detecting a port scan, we would write a rule that looks for an unusually high number of connection attempts to different ports in a short time frame. This rule would alert Suricata whenever this pattern is detected."

Basic structure of a Suricata rule:

alert <protocol> <source_ip> <source_port> -> <destination_ip> <destination_port>
(msg:"<alert_message>"; <options>; sid:<unique_id>;)

Step 4: Working

Develop custom Suricata rules to detect specific threats (e.g., port scans, suspicious traffic, or unauthorized access attempts) and test their effectiveness using a simulated environment.

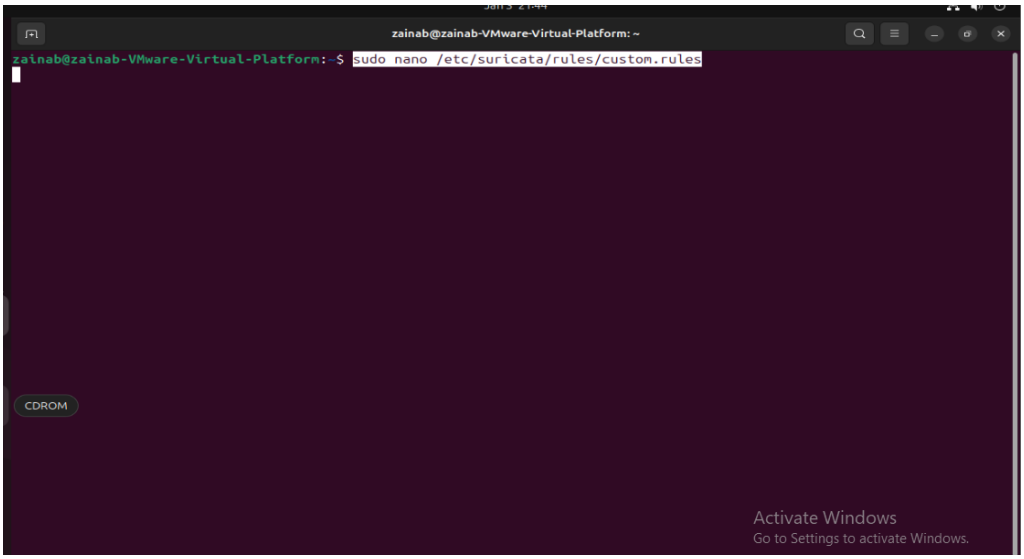
Test the Rules

Add the Rules to Suricata**:**

Create a new custom rules file:

sudo nano /etc/suricata/rules/custom.rules

Add the rules to this file.



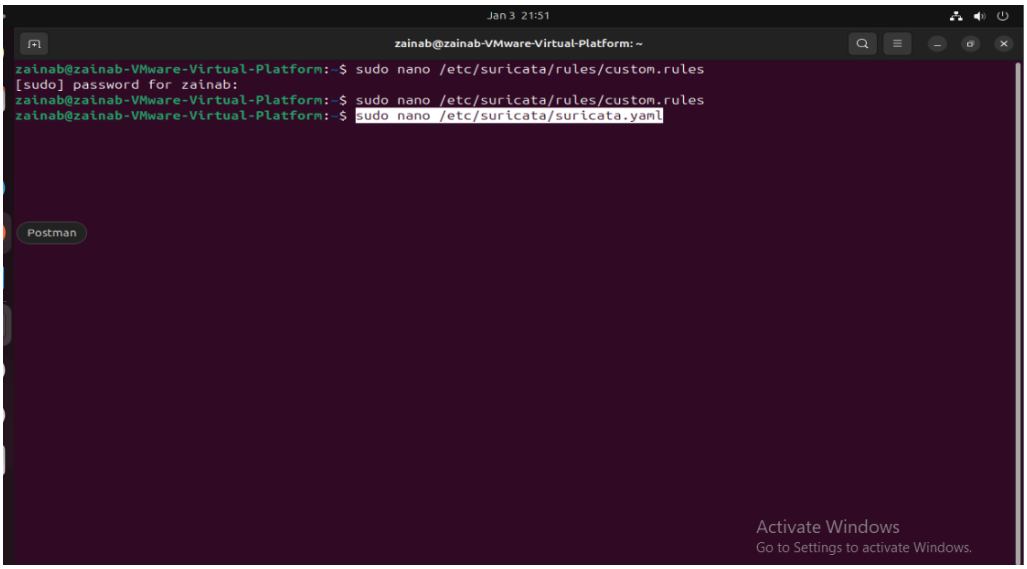
- Example 1: Detect Port Scans:

alert tcp any any -> $HOME_NET any (msg:"Possible Port Scan"; flags:S; threshold:type both, track by_dst, count 10, seconds 5; sid:100001;)

Update Suricata Configuration:

Edit the Suricata configuration file:

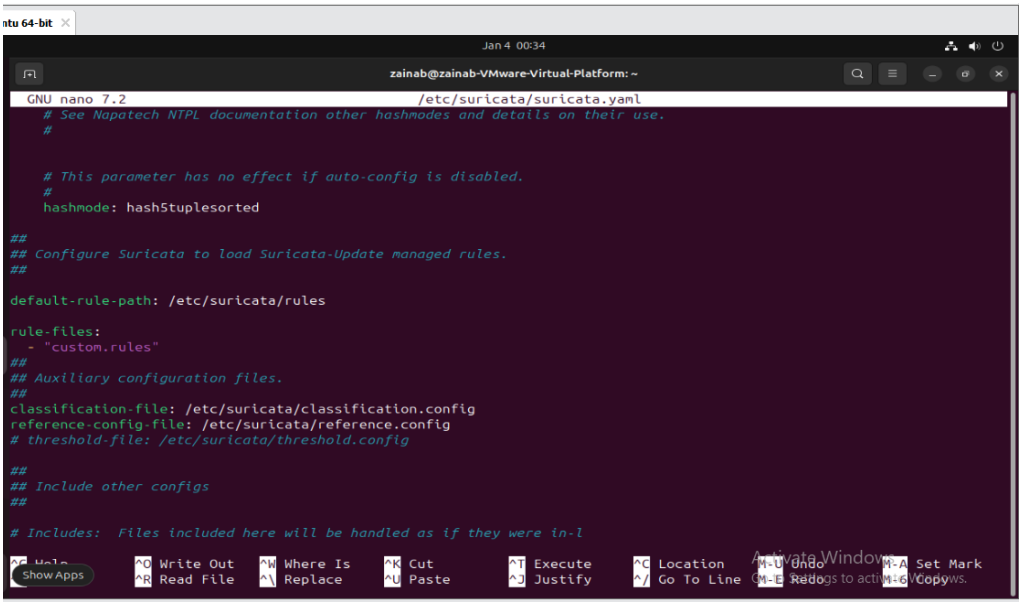
sudo nano /etc/suricata/suricata.yaml



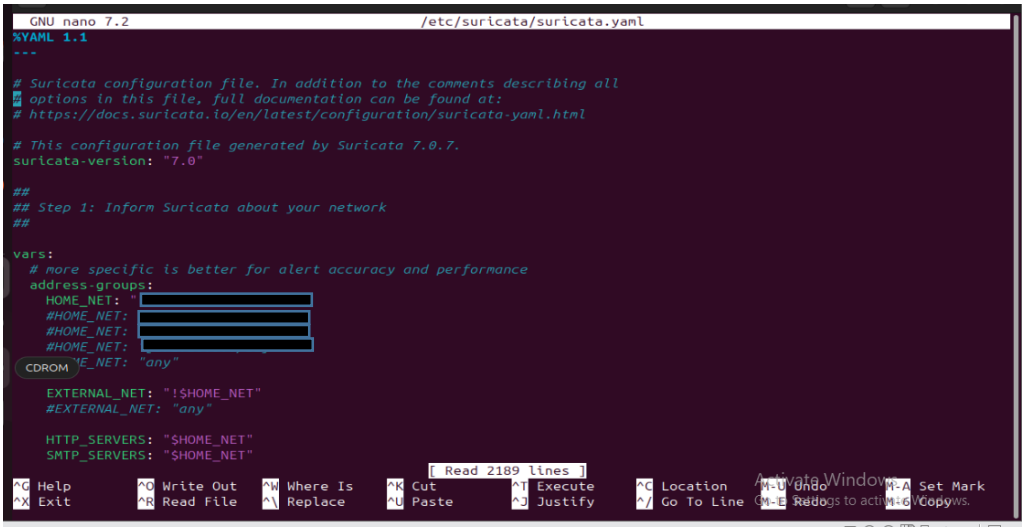
Ensure the custom rules file is included:

rule-files:

- custom.rules

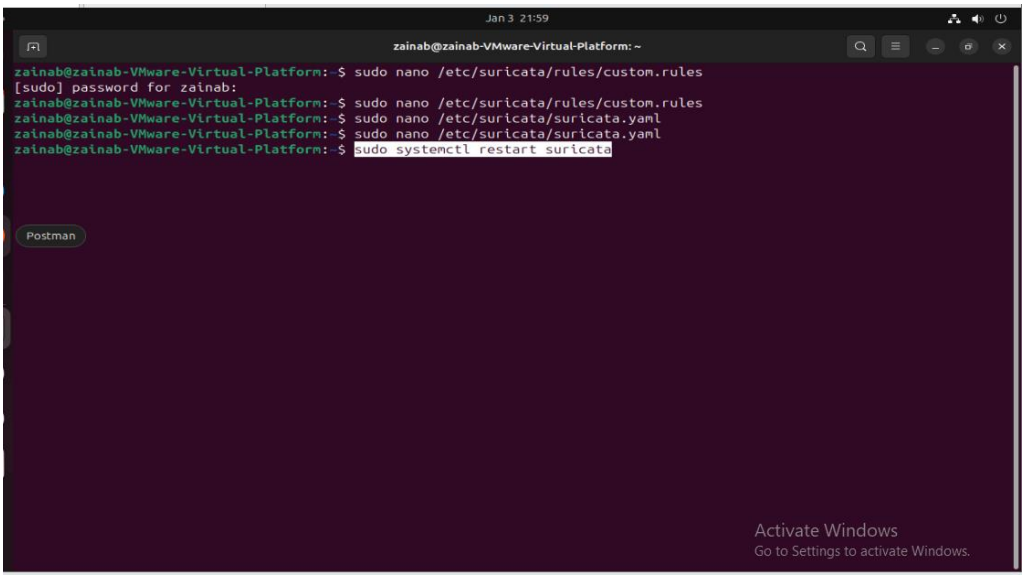


set address-groups as below:



Restart Suricata:

sudo systemctl restart suricata

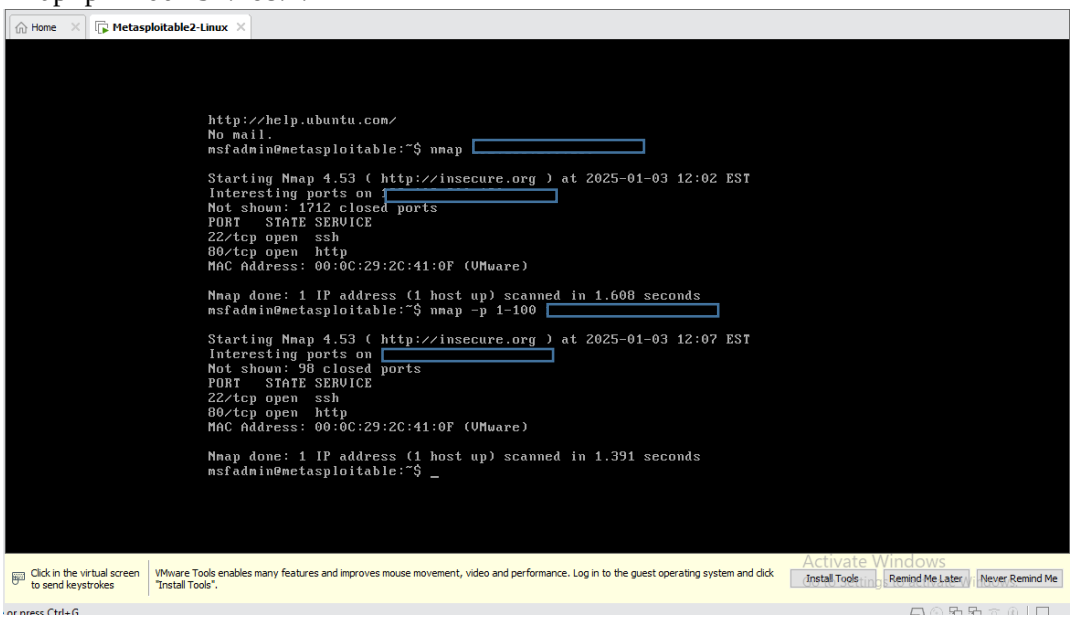


Simulate Attacks

On Metasploitable, scan port

Nmap Port Scan**:**

nmap -p 1-100 192.168.x.x



Analyze Logs

View alerts:

tail -f /var/log/suricata/fast.log

Check for matches with your custom rules:

Alerts for port scans should include:

text

[**] [1:100001:1] Possible Port Scan [**]

How to Match the Expected Port Scan Alert:

- Custom Rule Match:

The rule with sid:100001 is matching and generating alerts for possible port scans:

[1:100001:0] Possible Port Scan

This indicates that traffic matching the flags:S and threshold conditions is being detected as a port scan.

- Alerts in Logs:

These lines from your logs confirm the rule is firing:

01/03/2025-22:06:55.167636 [**] [1:100001:0] Possible Port Scan [**] [Classification: (null)] [Priority: 3] {TCP} 19[redacted]1:49309 -> 1[redacted]0:95

- Other Rules:

The logs also show other rules matching, such as the ET SCAN rules:

[1:2010937:3] ET SCAN Suspicious inbound to mySQL port 3306

Conclusion:

By completing these steps, created a custom Suricata rule, tested it using nmap to generate a port scan, and monitored Suricata's logs for the detection. This is a simple demonstration of how flexible Suricata is in detecting specific threats using custom rules.

Conclusion:

By following these steps can:

1. Set up Suricata as an IDS/IPS.
2. Create and test custom rules.
3. Analyze logs for threat detection.

This demonstrates the flexibility and power of Suricata for real-time threat detection and network security.