**PART 1.**

A screenshot of a computer

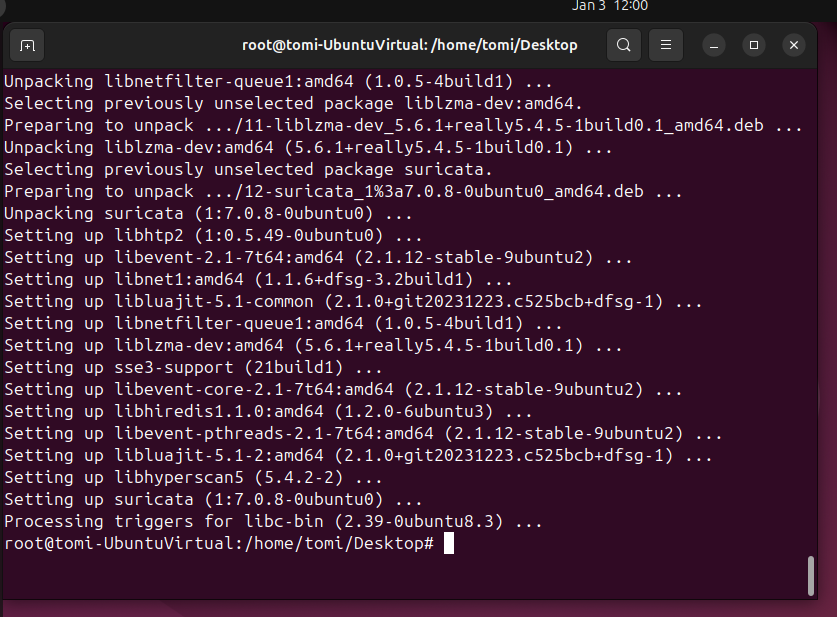
Description automatically generated

Suricata package repository being installed.

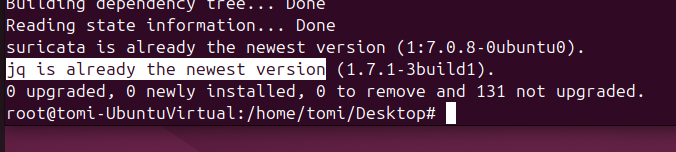
A screenshot of a computer

Description automatically generated

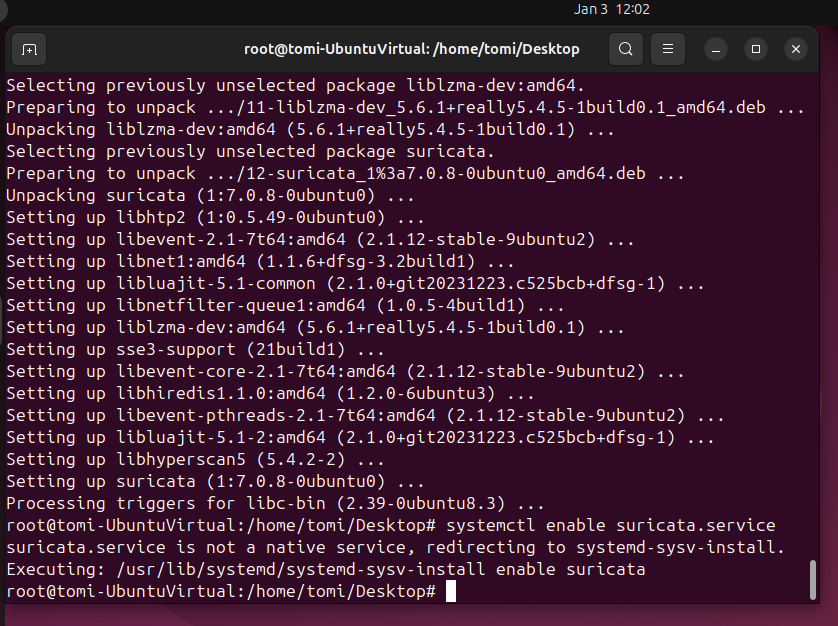
Package repository installed.



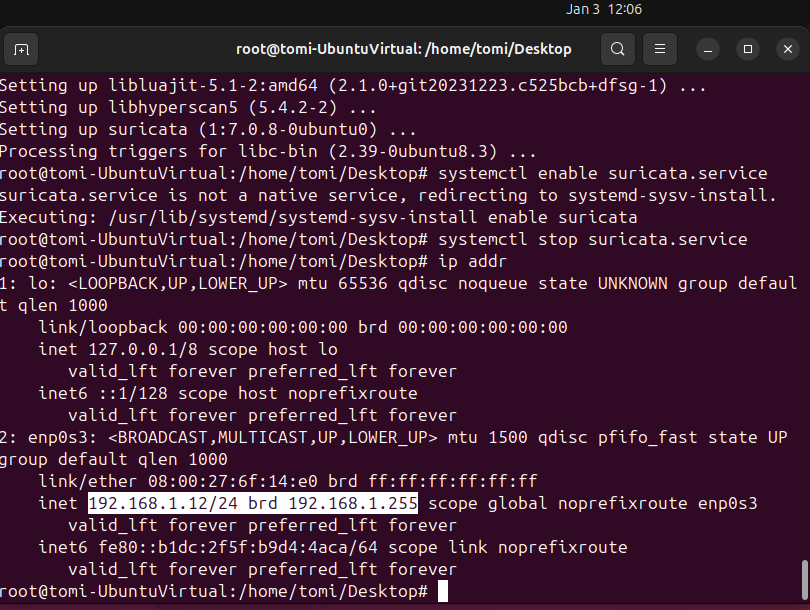
With command ‘apt install suricata jq’ (information data processing program)



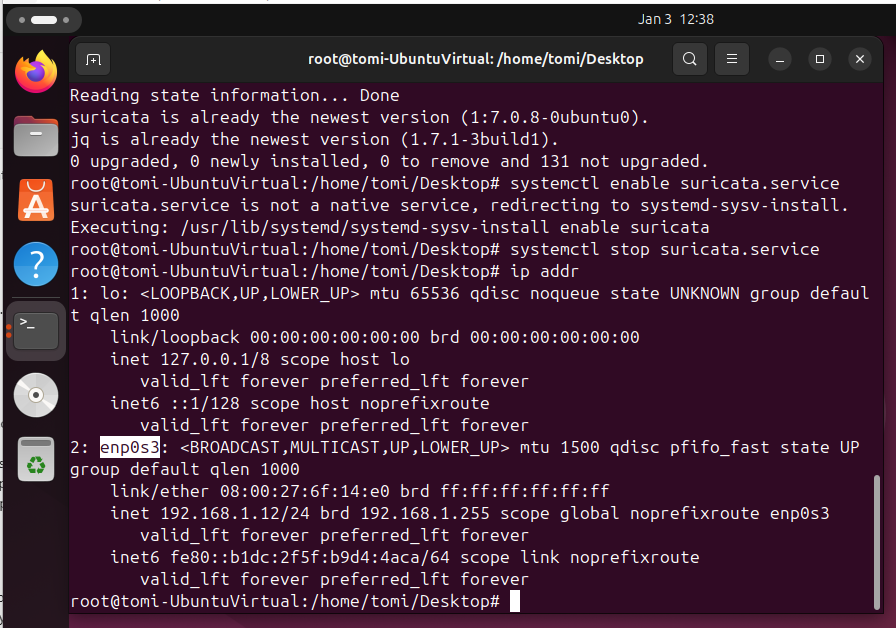
Data processing program installed.



Suricata service started.



Confirming the IP address.

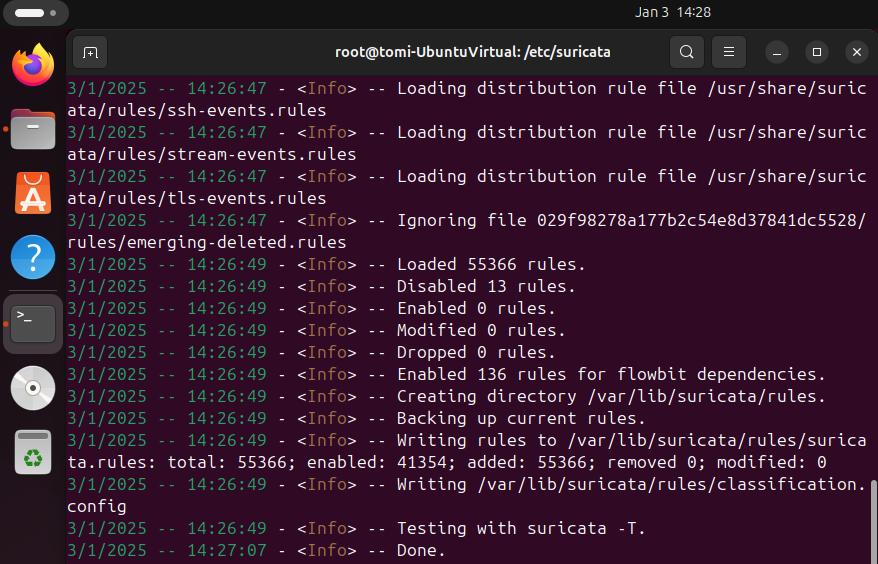


The interface highlighted.

A screenshot of a computer

Description automatically generated

The default interface to be changed to ‘enp0s3’.



Suricata software on Ubuntu VM successfully installed.

A screenshot of a computer

Description automatically generated

My firewall and Ubuntu VM targeted from the GVM scanner.

A screenshot of a computer

Description automatically generated

Attack on the Ubuntu VM from Kali Linux returned zero detection and indicates no anomaly.

**PART 2.**

1.

* I had a seamless installation of the Suricata software, but I had difficulty in overwriting on the default configuration when I tried to change the default interface of ‘eth0’ to the generated interface of ‘enp0s3’. I needed to read through the QuickStart guide for me to figure out how to overwrite the configuration.

A close up of a white background

Description automatically generated

* On all my VMs, I cannot directly use the snipping tool without popping up the icon.
* I still could not properly use my installed GVM as it kept on freezing on OpenVAS.

3.

Network forensics involves the monitoring, capturing and analysis of network traffic to detect and investigate security incidents. Some methodologies are: -

* Packet Capture – involves intercepting and logging traffic that passes over a network using tools like Wireshark. Full Packet capture (the comprehensive network traffic) and Selective Packet Capture (only specific traffic like IP addresses or protocols) are the two types of packet capture.
* Deep Packet Inspection – identifies and analyzes a payload of packets, hence able to detect malicious activities, going beyond only examining the contents of packets.
* Analysis of Protocols – involves examining the behavior and structure of protocols to identify unusual patterns or deviations from normal behavior. Protocols like HTTPS, SMTP, SFTP, TCP/IP are analyzed and examined. The method involves capturing network traffic for later analysis and real-time monitoring and analysis. (Kostadinov, D., 2020.)

4.

My GVM scanner did not indicate any anomaly or malicious activity.

5.

IDS and IPS play vital roles in network security by monitoring system activities and detecting potential attacks by utilizing various detection methods to identify and respond to security threats effectively. (Palmer, G., 2023.) However, analytic methodologies, both qualitative and quantitative, can significantly enhance the capabilities of these systems to predict and communicate network anomalies.

Qualitative methods use pattern recognition like signature-based detection (by comparing network traffic against a database of known signatures) and behavioral analysis (by observing and analyzing system and user behaviors to detect deviations from the norm.). Qualitative methods also use expert analysis like reviewing incident reports and threat intelligence to identify anomalies and detect emerging threats and vulnerabilities.

Quantitative methods use statistical analysis and models to establish baselines of network behavior so that deviations and unusual activity can be identified and detected.

**References.**

# Bdair-AIghuraibawi, A., Abdullah, R., Manickam, S., & Alkareem-Alyasseri, Z., (2021). Detection of ICMPv6-based DDoS Attacks Using Anomaly based Intrusion Detection System.

# <https://doi-org.lopes.idm.oclc.org/10.11591/ijece.v11i6.pp5216-5228>

Kostadinov, D., 2020, Apr. 14. Network Forensics Overview.

<https://www.infosecinstitute.com/resources/digital-forensics/network-forensics-overview/>

Palmer, G., 2023, Jun. 16. IDS/IDPS Detection Methods: Anomaly, Signature and Stateful Protocol Analysis.

<https://zymitry.com/ids-idps-detection-methods/>