International Journal of Scientific Research and Engineering Development-– Volume 8 Issue 4, July Year 2025
Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

Real-Time Network Intrusion Detection Using Snort

Nisha Ajay Pawar*
*(Lecturer in Computer Engineering Department, PES Polytechnic,
Chh. Sambhajinagar (Aurangabad), Maharashtra. India)
Email: pawarnisha1797@gmail.com)

----------**********----------

Abstract:

This project focuses on the implantation of real-time network intrusion detection system using Snort. It includes Configuration of Snort which explore how rule-based detection can identify suspicious network behaviour such as ICMP flooding, port scanning, and malformed packets. The objective is to design a low-cost, configurable IDS setup that helps in understanding real-world security operations and defensive monitoring system.

Keywords — Intrusion, Snort, Network, Intrusion Detection System (IDS), cmd (command prompt)

----------**********----------

I. INTRODUCTION

In today's word, cyber-attacks and threads are rising, so to handle unauthorized access and malicious activities Intrusion Detection Systems (IDS) play an important role in this area.

To Understand Intrusion Detection system first we have to understand following concepts :

Intruder
|
Intrusion
|
Intrusion Detection System (IDS)

Intruder : Intruder is a person who is trying get unauthorized access with criminal intension.

Intrusion : Unauthorized access by an Intruder is known as Intrusion.

Intrusion Detection System (IDS) : It is a system who identify the Intruders who is trying to access data. It works at backend. It send alert messages to admin.

This project implements Snort, a widely-used open-source IDS, to detect various network-based attacks using custom rule sets. The goal is to provide hands-on understanding of IDS functioning and improve the ability to detect potential threats. Now we are going to install and configure snort for intrusion detection.

II. LITERATURE SURVEY

Number of studies have proven the importance of ids in network security. snort, is one of the most popular tools, has been integrated into all environments like academic, enterprise. compared to traditional systems, snort offers flexibility and customization through its rule-based engine. research also highlights the growing need for intelligent threat detection using open-source technologies.

III. SYSTEM DESIGN

A) System Architecture:

Attacker PC → Target VM → Snort IDS → Alert Logs

B) Software Requirements:

- OS: Kali Linux / Ubuntu.
- Snort 2.9.x.
- Tools: Nmap, Wireshark, Netcat.

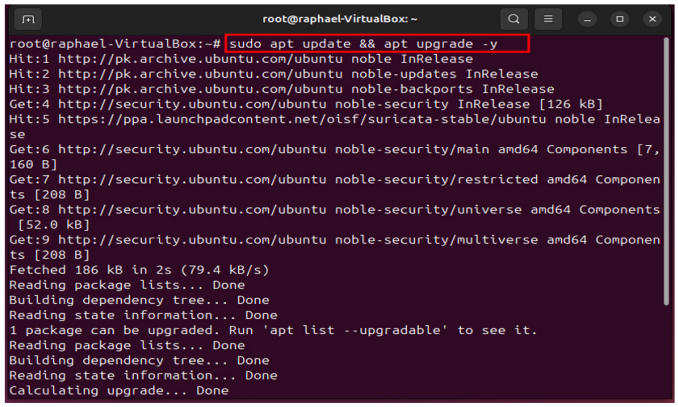
C) Hardware Requirements:

- CPU: i3/i5 or higher.
- RAM: 4GB+
- VirtualBox or any VM.

IV. IMPLEMENTATION

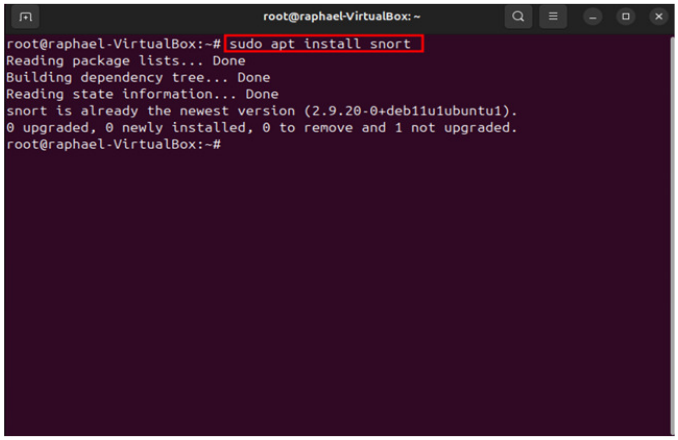
- Install VMWARE and add Ubuntu OS.
- Open your terminal and run this command so that your Ubuntu is up to date :

sudo apt update && apt upgrade –y



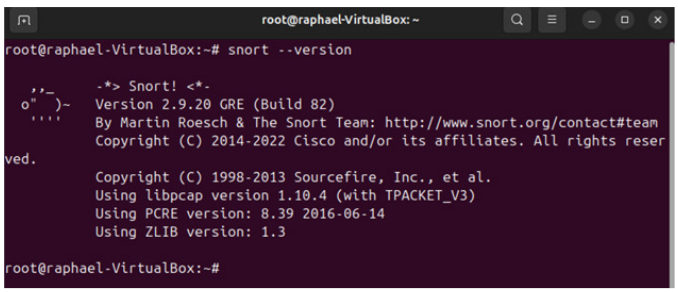
- Now run this command to install snort on Ubuntu

sudo apt install snort

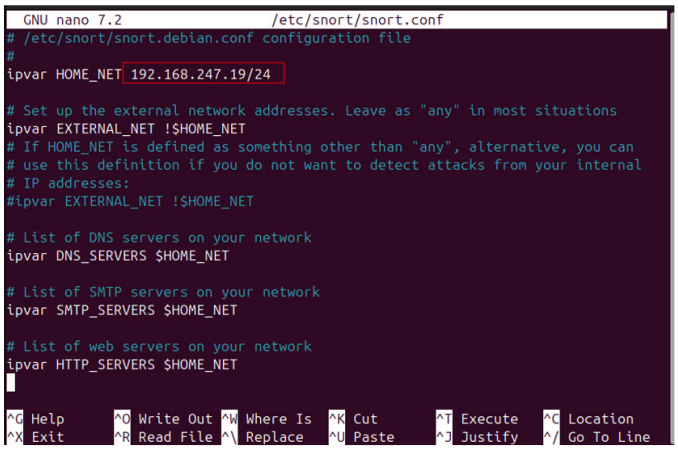


- To check if snort has been installed input this command to check the version of snort

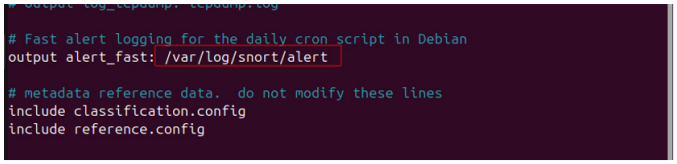
snort –version



- If snort has been installed enter this command to configure snort settings and enable alerts of your network
- Edit the snort.conf file using nano command and change these settings according to your IP and interface
  sudo nano /etc/snort/snort.conf
- Set network variables (HOME_NET):

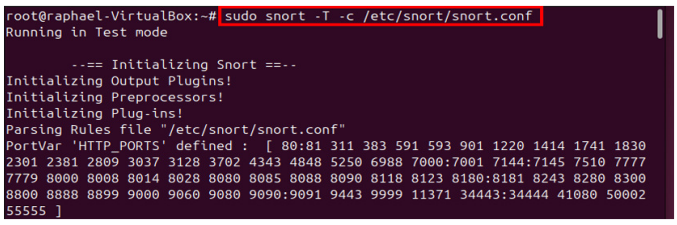


- Include rule paths:

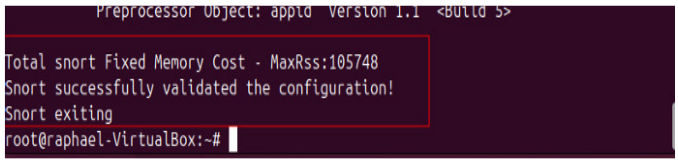


- The configuration file defines the environment (e.g., monitored network) and specifies rule files.
- Now press Ctrl + S and then Ctrl + X
- Now run this command to test the configuration

sudo snort -T -c/etc/snort/snort.conf

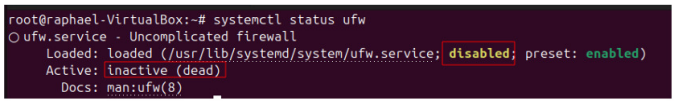


- If the configuration is successful then this will be displayed in the terminal



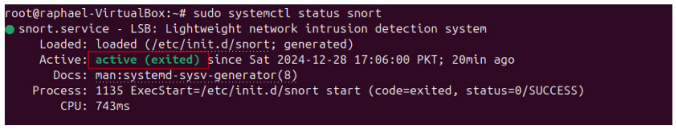
- Validates the configuration file for errors before running Snort.
- Before starting the snort make sure to check If the ufw is enabled or not

systemctl status ufw



- if it is enabled then run this command
  systemctl stop ufw
- Check if the Snort service is enabled and is up and running by inputting this command

sudo systemctl status snort



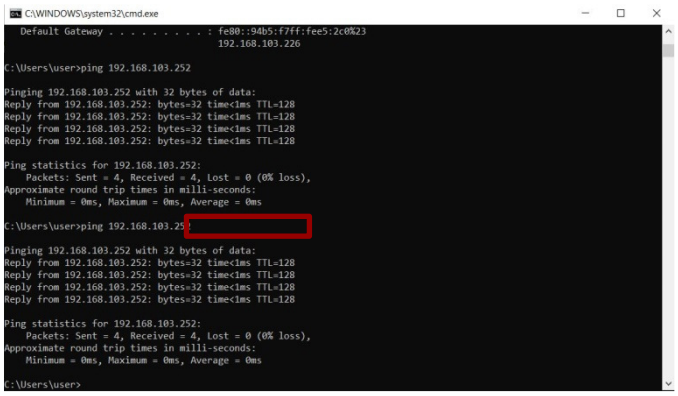
- Now run command to install apache
  sudo apt –get install apache2
- Now run following command to set FTP server
  sudo apt -get install vsftpd
- To configure Firewall(UFW) on Ubuntu system to allow traffic on specific ports use following command
  sudo ufw allow 21/tcp
  sudo ufw allow 80/tcp
- Now create rules file in /etc/snort/rules
  sudo nano local.rules
- Write rule using following syntax :
  Action Protocol Source IP Source port -> Destination IP Destination port (options)
  Sample rule :

alert ip any any -> any any (ms:"Message tobe print")

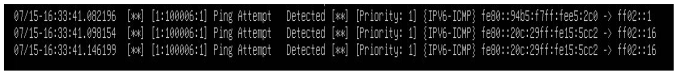
- Now run snort in the Terminal, Enter this command

sudo snort -A console -q -c etc/snort/snort.conf -I ens33

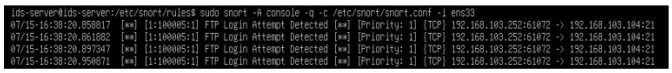
- Now start the snort system for monitor the intrusion. To generate alert messages I will enter the simple ping command in windows cmd.



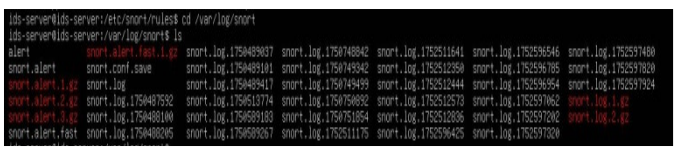
- When you enter above command in cmd then snort will give you alert message.



- For second alert message I open cmd and try to access ftp port 21 to get alert message in snort.



- This alter message is called as real time network intrusion detection using snort.
- All this alert messages are saved in snort log file to see alert log first stop snort and enter below command :



- This are all log files that save all alert messages in it.

V. CONCLUSION

This project can effectively demonstrate Snort as an actual real-time network intrusion detection system. By implementing and testing user-defined

rules, the system can identify common network attacks and port scans. The setup enhances the knowledge of IDS deployment in real-world applications. The Real-Time Intrusion Detection System using SNORT successfully demonstrates the ability to monitor and examine network traffic for possible vulnerability in real time. Employing the effective rule-based detection engine of SNORT and open-source code, the system offers a practical and cost-efficient solution to network security enhancement. With proper setup, integration with visualization tools, and real-time alerting, the system is capable of detecting malicious traffic via port scans, denial-of-service, and attempts at accessing. This gives administrators an early chance to block new threats and harden the network infrastructure. In general, SNORT is a great place to begin intrusion detection in small and enterprise environments. Combined with log analysis, port mirroring, and add-on machine learning modules, it can dramatically enhance the responsiveness and effectiveness of network defence mechanisms for detection

ACKNOWLEDGMENT

We would like to extend our sincerest thanks to Department of Computer Engineering, P.E.S. Polytechnic College Chh. Sambhaji Nagar, Maharashtra for supporting and guiding us in our project.

REFERENCES

[1] *Snort guideline and download Website* https://www.snort.org

[2] *To study snort in detail website* https://www.fortinet.com

[3] *To study snort installation website* https://hackertarget.com

[4] *"The study on network intrusion detection system of Snort," in Proc. IEEE Conf., 2025.*

[5] *"Research on intelligent intrusion prevention system based on Snort," in Proc. IEEE Conf., 2025.*

