Department of Computer Science & Engineering

Bangladesh University of Engineering & Technology

CSE406 - Computer Security Sessional

Report On Snort

September 13, 2023

Supervisor:

Abdur Rashid Tushar
Lecturer

Prepared By:

Fabiha Tasneem
1805072
Level-4, Term-1

Sumaiya Sultana
1805079
Level-4, Term-1

Abstract

Snort, created by Martin Roesch in 1998, is a versatile IDS/IPS that offers real-time analysis of network traffic to detect and respond to potentially malicious activities. It operates on a rule-based system, where users can define custom rules or employ pre-existing rule sets to identify and mitigate threats. Snort's rule-based approach allows it to monitor network traffic at both the network and application layers, thereby offering comprehensive protection against a wide range of network-based attacks and vulnerabilities.

Snort represents a vital asset in the arsenal of network security tools. Its rule-based detection, adaptability, and open-source philosophy have established it as a trusted solution for identifying and mitigating network threats. As cyber threats continue to evolve, Snort's role in defending against these threats remains indispensable, ensuring the resilience of modern network infrastructures.

Contents

List of Figures

1 Introduction

1.1 What Is Snort?

Snort is a popular free and open-source IDS/ IPS system that is used to perform traffic/ protocol analysis and content matching. Snort can be used to detect and prevent various attacks based on *predefined rules*.

1.2 Snort Operations

- **Packet Sniffing:** Analyzes the actual network traffic in real-time
- **Network Intrusion Detection:** Analyzes packets and matches traffic against signatures
- **Packet Logging:** Collects and logs network traffic into a log file
- **Network Intrusion Prevention:** Takes specific actions to block identified threats

1.3 How Does Snort Work?

Snort detects malicious traffic or attacks by leveraging pattern matching. When active, Snort captures packets, reassembles them, analyzes them, and determines what needs to be done to the packet based on predefined rules.
Snort has a large number of rule sets created by the community that are very useful to begin with. Snort rules are very similar to a typical firewall rule, whereby, they are used to match network activity against specific patterns or signatures and consequently make a decision as to whether to send an alert or drop the traffic (in the case of IPS).

1.4 Snort Rules

Snort has 4 types of rule sets:

- **Community Rules:** Free rule sets created by the Snort community.
- **Registered Rules:** Free rule sets created by Talos. In order to use them, a user must register for an account.
- **Subscription Only Rules:** These rule sets require an active paid subscription in order to be accessed and used.
- **Customized Rules:** We can write our own rules based on our requirements.

A Snort Rule is very simple and easy to write. The syntax goes like this:

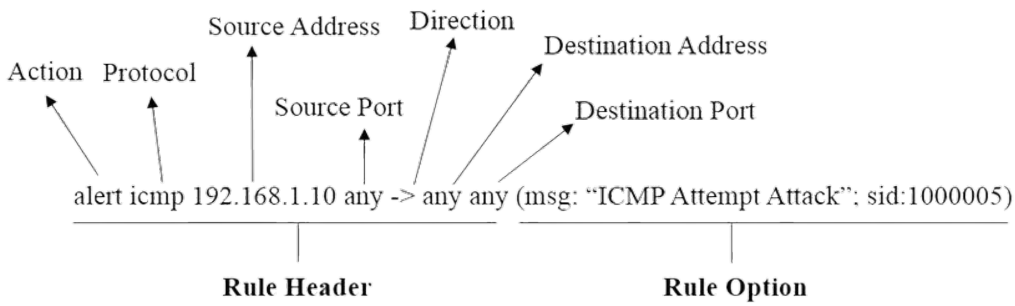

Figure 1: Snort Rule Syntax

2 Prerequisites

2.1 Virtual Machine Setup

Here is the list of Virtual Machines that we are going to use:

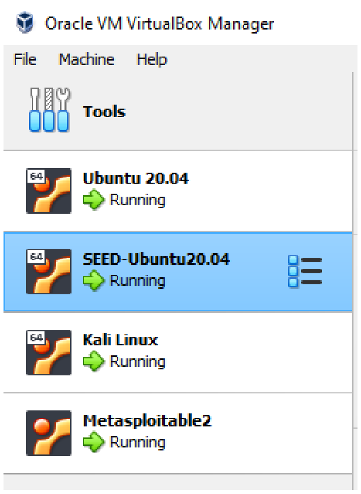

Figure 2: List of the VMs

The roles of all these virtual machines are:

- **Ubuntu 20.04:** This is where we will install Snort
- **Kali Linux:** Attacker Virtual Machine
- **SEED-Ubuntu 20.04:** A vulnerable Victim Virtual Machine
- **Metasploitable:** Another more vulnerable Victim Virtual Machine

The IP addresses of all of the Virtual Machines must be in promiscuous mode to connect with each other.

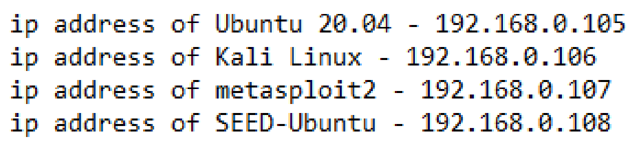

Figure 3: IP Addresses

2.2 Snort Installation

To install Snort on Ubuntu 22.04, we can simply run **"sudo apt-get install -y snort"**. We have installed Snort 2.0 instead of Snort 3.0 because it is more stable and has rich resources available.

Then we can test the Snort installation to ensure it's functioning correctly, which is crucial for effective intrusion detection and prevention.

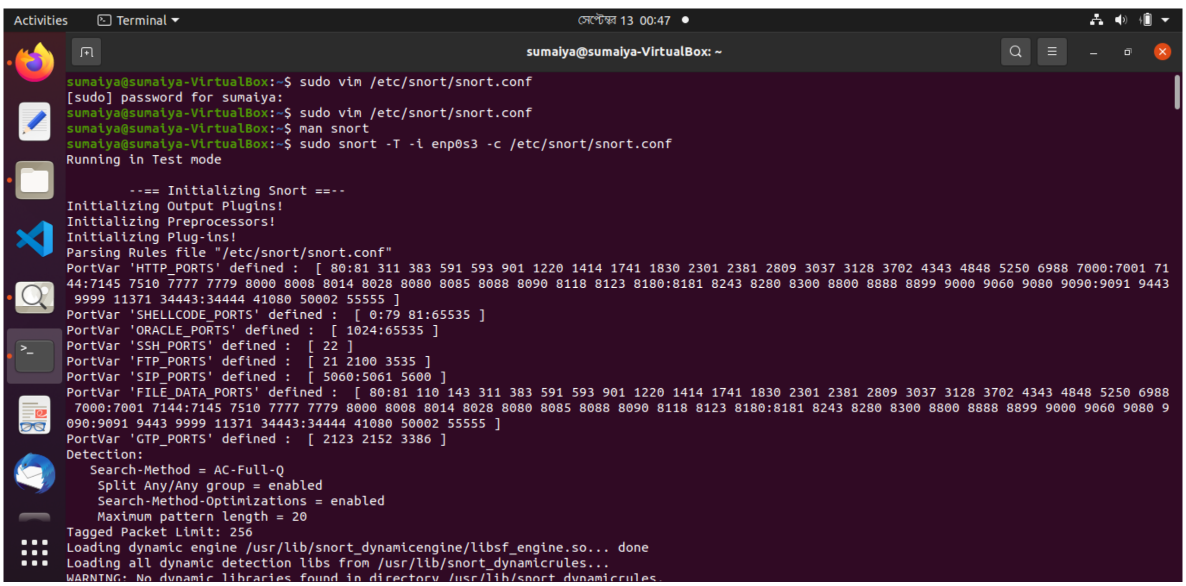

Figure 4: Testing Snort

The image below displays the total number of rules installed in Snort, highlighting the extensive rule set that helps identify and respond to various network threats.

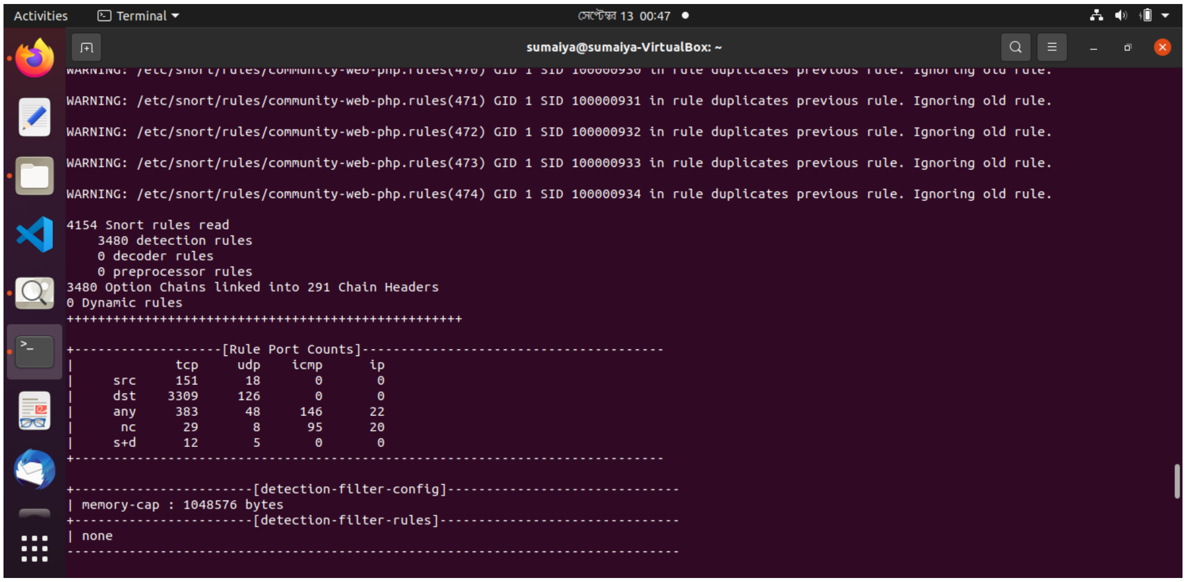

Figure 5: Total Rules Installed

Inside the **etc/snort/** folder:

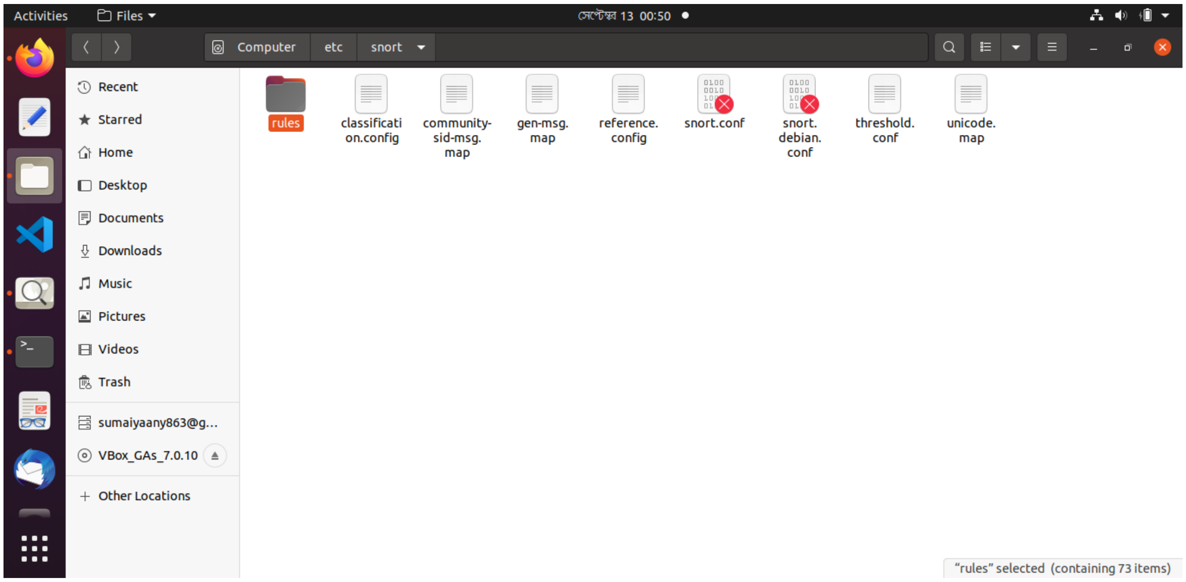

Figure 6: Snort Folder

The image below provides a glimpse into the configuration file **etc/snort/snort.conf**, where Snort's settings are defined:

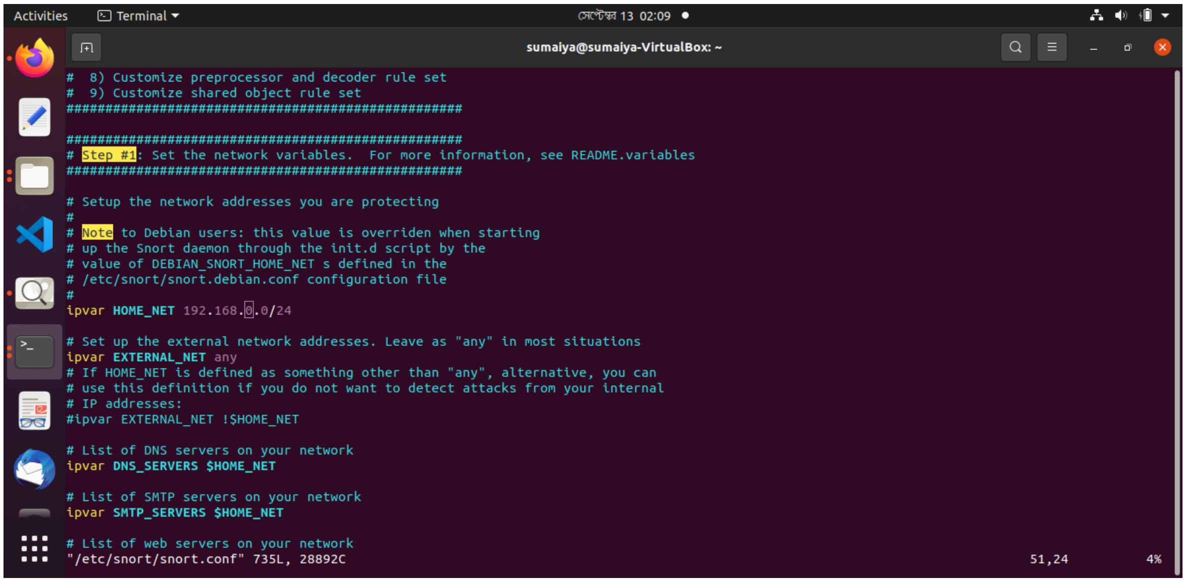

Figure 7: Configuration File

The Rules folder contains a collection of rule sets that Snort uses to detect known attack patterns:

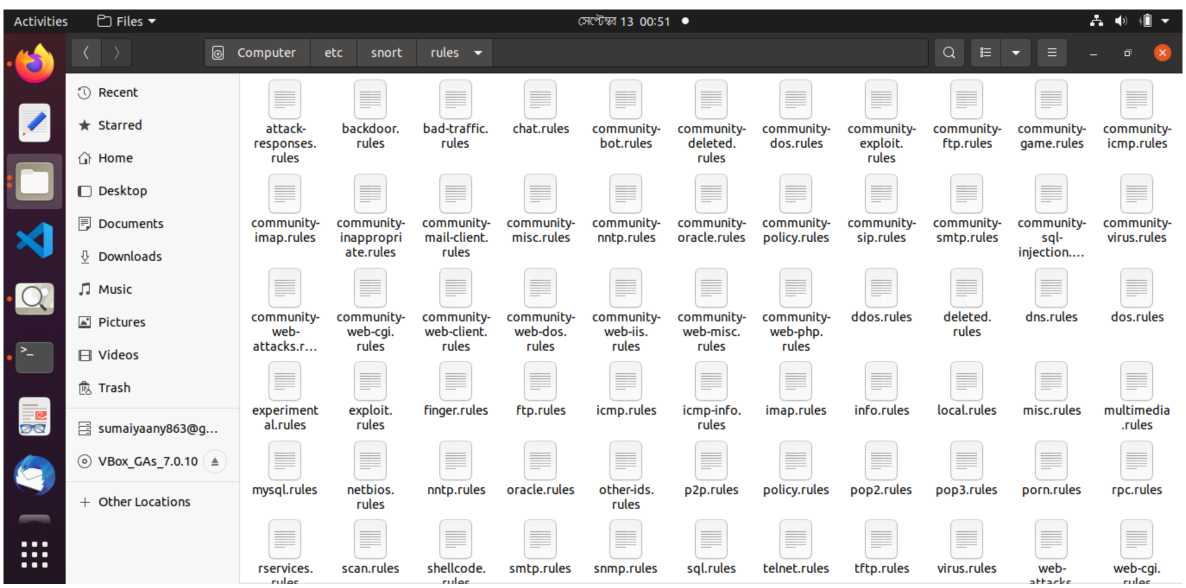

Figure 8: Rules Folder

Here, you can see the contents of the Community Rules File which is free for everybody:

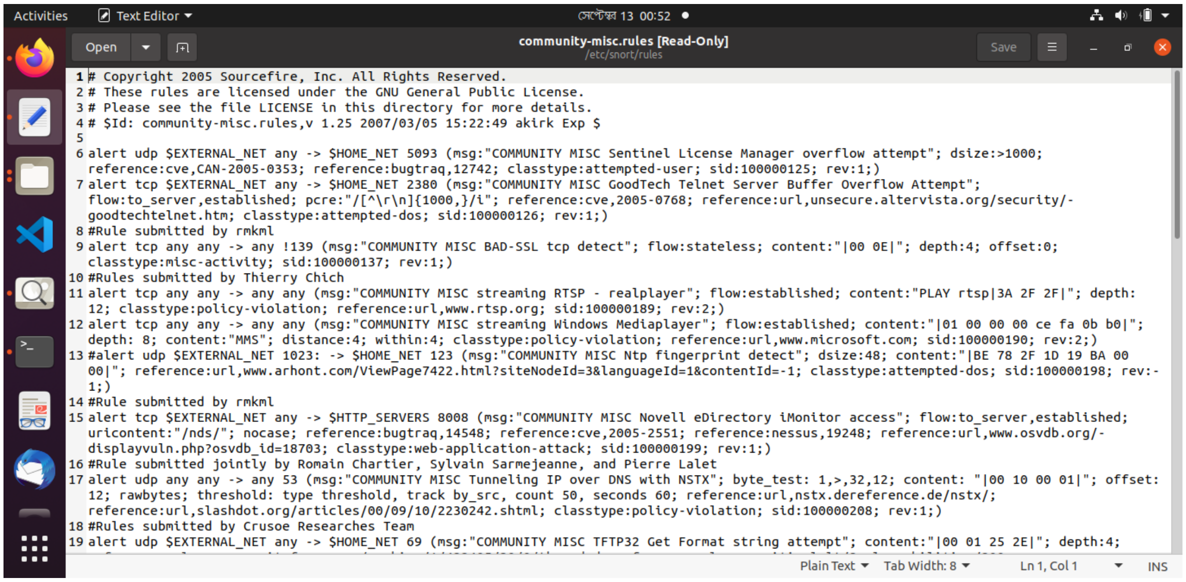

Figure 9: Community Rules File

The command to see local rules:

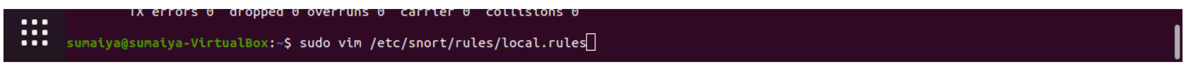

Figure 10: Command for Local Rules

Inside Local Rules File:

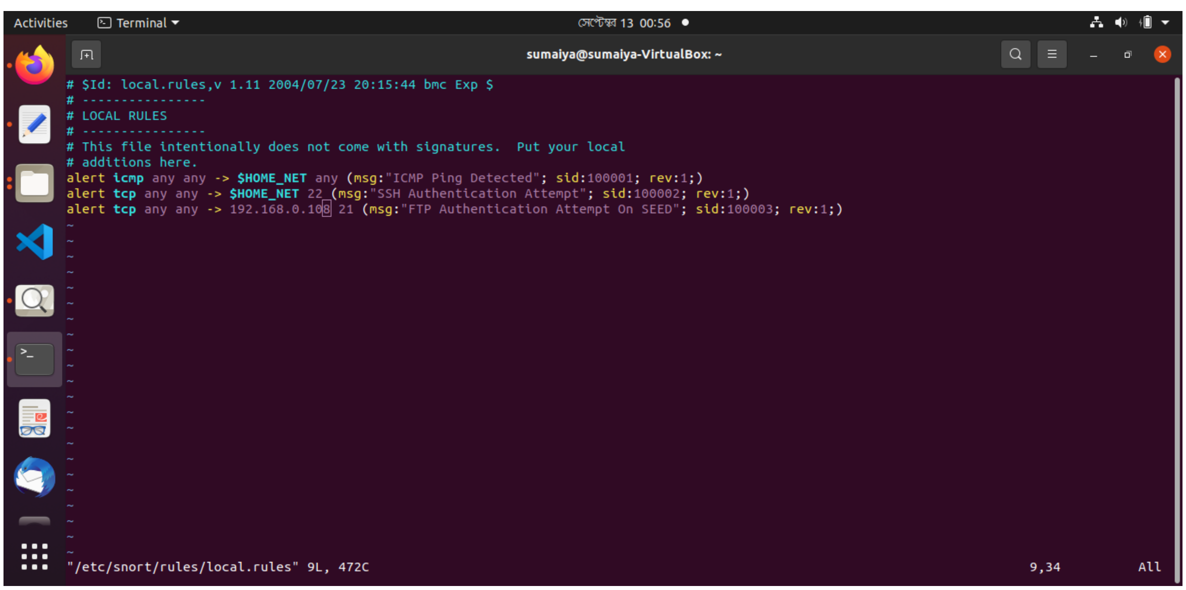

Figure 11: Local rules file

3 Demonstration

3.1 Packet Sniffing

Packet sniffing in Snort refers to the capability of the Snort Intrusion Detection System (IDS) to capture and inspect network packets as they traverse a network interface. It is one of the fundamental functions of Snort, allowing it to analyze network traffic in real-time for the detection of suspicious or malicious activity.

Packet sniffing specifically refers to the process of capturing and inspecting network packets as they traverse a network interface. This is the initial step where the IDS monitors the raw network traffic for any suspicious or malicious activity. So, we are not demonstrating this feature separately and we are jumping to Intrusion Detection directly.

3.2 Network Intrusion Detection

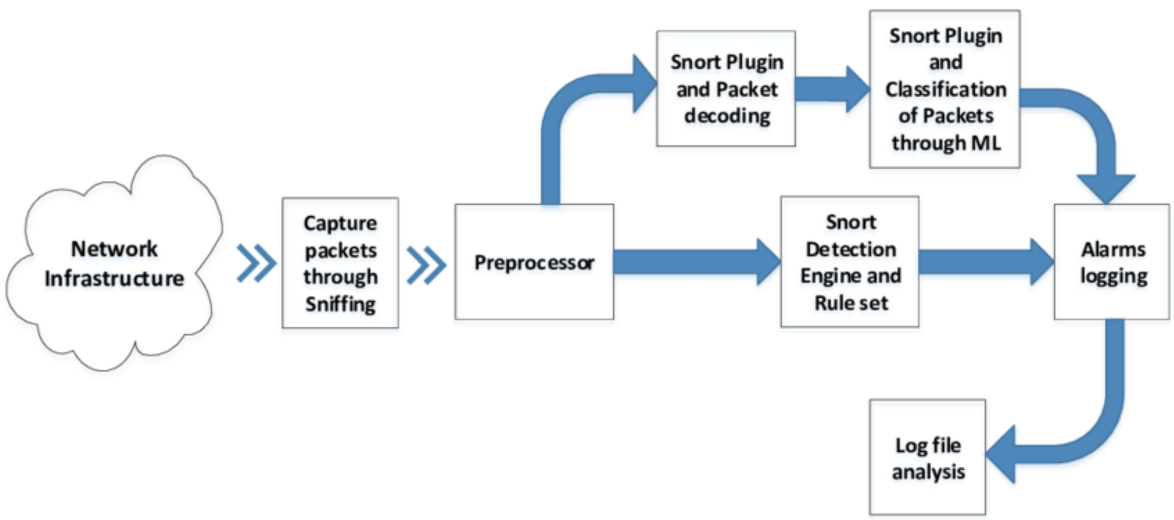

Figure 12: IDS Workflow

Intrusion detection is the process of actively discovering threats/attacks/intrusions on a network, different hosts, or services. An Intrusion Detection System (IDS) is a system/host planted within a network to capture traffic and identify malicious activity based on predefined rules, after which, this malicious activity is logged, and a notification is sent to the relevant parties informing them of an intrusion.
There are 2 types of IDS solutions based on the placement:

- **HIDS:** A Host-based IDS (HIDS) is set up on an individual host on a network.
- **NIDS:** A Network IDS (NIDS) is placed within a network to monitor traffic to and from all hosts on a network.

Intrusion detection systems are typically coupled with the functionality to also perform intrusion prevention, whereby specific rules can be set to drop packets that are malicious or intrusive.

We first write some rules for our demonstration:

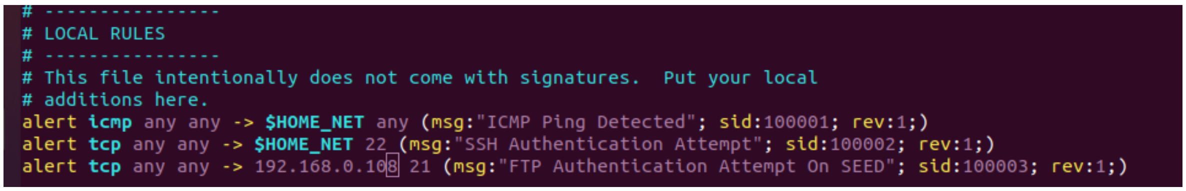

Figure 13: IDS Rules

Here we use a tool named **Snorpy** to write the rules easily:

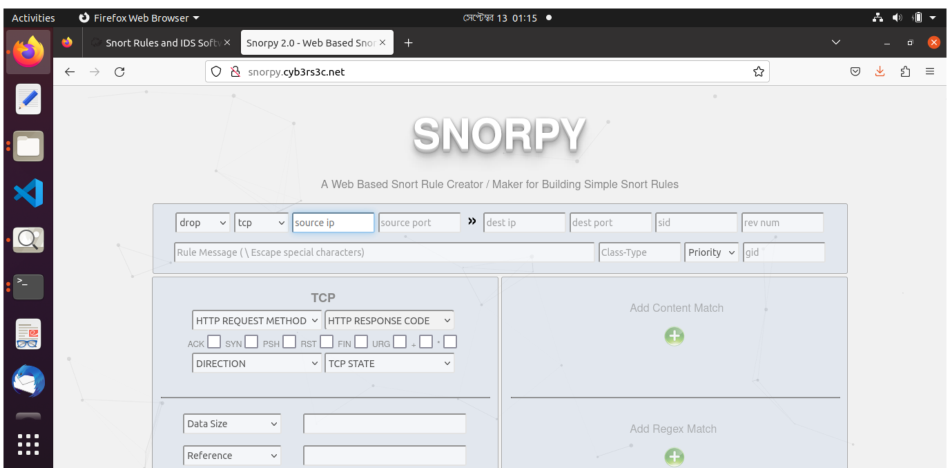

Figure 14: Snorpy

This screenshot displays the command used to start the Snort Intrusion Detection System in our Ubuntu 22.04 VM:

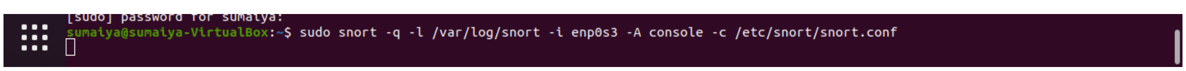

Figure 15: Command to Run Snort

A ping command is being executed from Kali Linux to test the connectivity to our Ubuntu 20.04. Ping tests help ensure network connectivity and are often used as part of network troubleshooting processes.

```
┌──(sumaiya㉿kali)-[~]
└─$ ping 192.168.0.105
PING 192.168.0.105 (192.168.0.105) 56(84) bytes of data.
64 bytes from 192.168.0.105: icmp_seq=1 ttl=64 time=0.839 ms
64 bytes from 192.168.0.105: icmp_seq=2 ttl=64 time=0.746 ms
64 bytes from 192.168.0.105: icmp_seq=3 ttl=64 time=1.24 ms
64 bytes from 192.168.0.105: icmp_seq=4 ttl=64 time=1.42 ms
64 bytes from 192.168.0.105: icmp_seq=5 ttl=64 time=1.22 ms
^C
--- 192.168.0.105 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4042ms
rtt min/avg/max/mdev = 0.746/1.092/1.418/0.256 ms
```

Figure 16: Pinging Ubuntu 20.04

To establish an SSH connection to Metasploit2 with specific configuration options:

```
┌──(sumaiya㉿kali)-[~]
└─$ ssh -oHostKeyAlgorithms=+ssh-dss msfadmin@192.168.0.107
msfadmin@192.168.0.107's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
Last login: Wed Sep  6 00:53:28 2023 from 192.168.0.106
msfadmin@metasploitable:~$ ls
vulnerable
msfadmin@metasploitable:~$ exit
logout
Connection to 192.168.0.107 closed.
```

Figure 17: SSH to Metasploit2

To initiate an FTP (File Transfer Protocol) connection to our SEED VM on port 21:

```
┌──(sumaiya㉿kali)-[~]
└─$ ftp 192.168.0.108 21
Connected to 192.168.0.108.
220 (vsFTPd 3.0.3)
Name (192.168.0.108:sumaiya): seed
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Figure 18: FTP to SEED

Ensuring the rules are correctly configured:

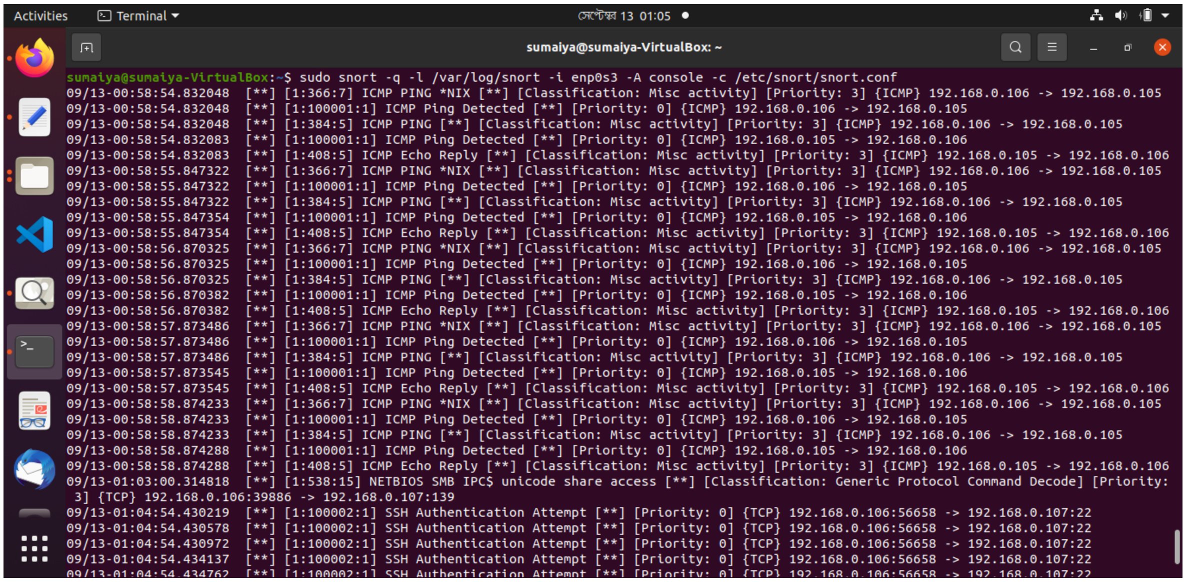

Figure 19: Verifying Local Rules (1)

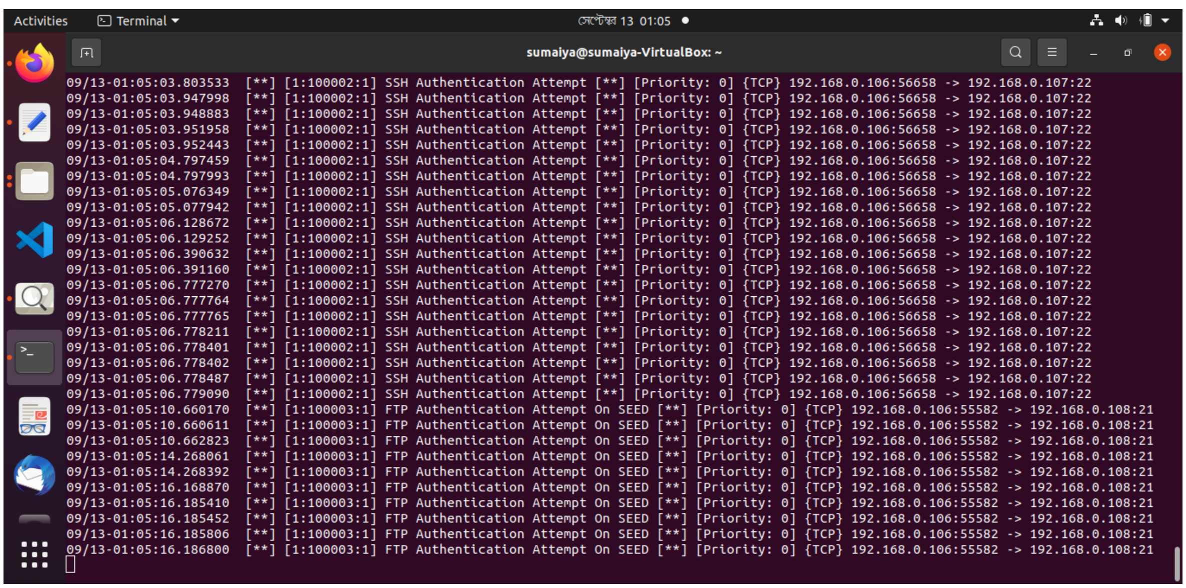

Figure 20: Verifying Local Rules (2)

Now we check the log for any intrusion:

Figure 21: Command to Log Alerts

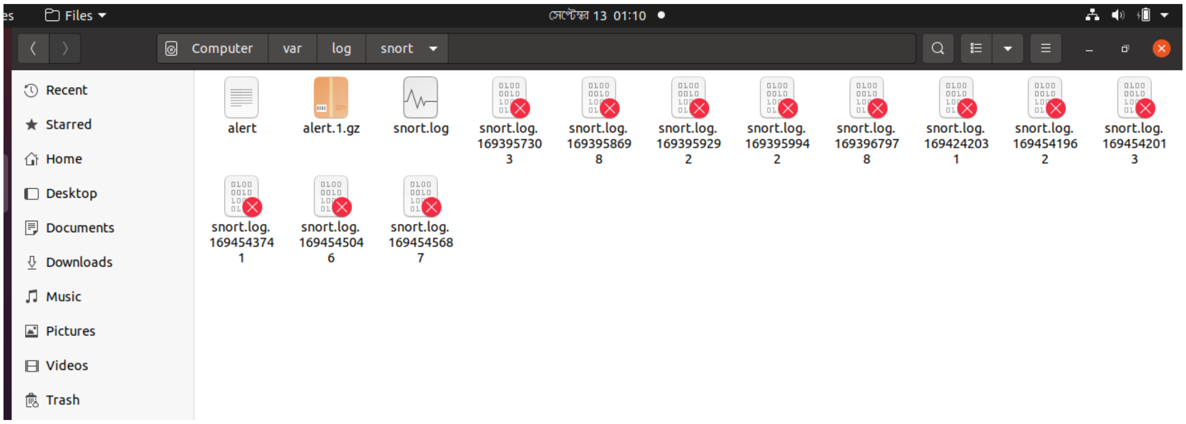

Figure 22: Snort Log Folder

We can see the alert has been generated by Snort after detecting an intrusion. All the logs are saved too.

3.3 Packet Logging

Packet logging in Snort refers to the process of capturing and recording network packets that match specific rules or signatures defined in the Snort intrusion detection system (IDS) configuration. Here we will use a tool named **Wireshark** for logging.

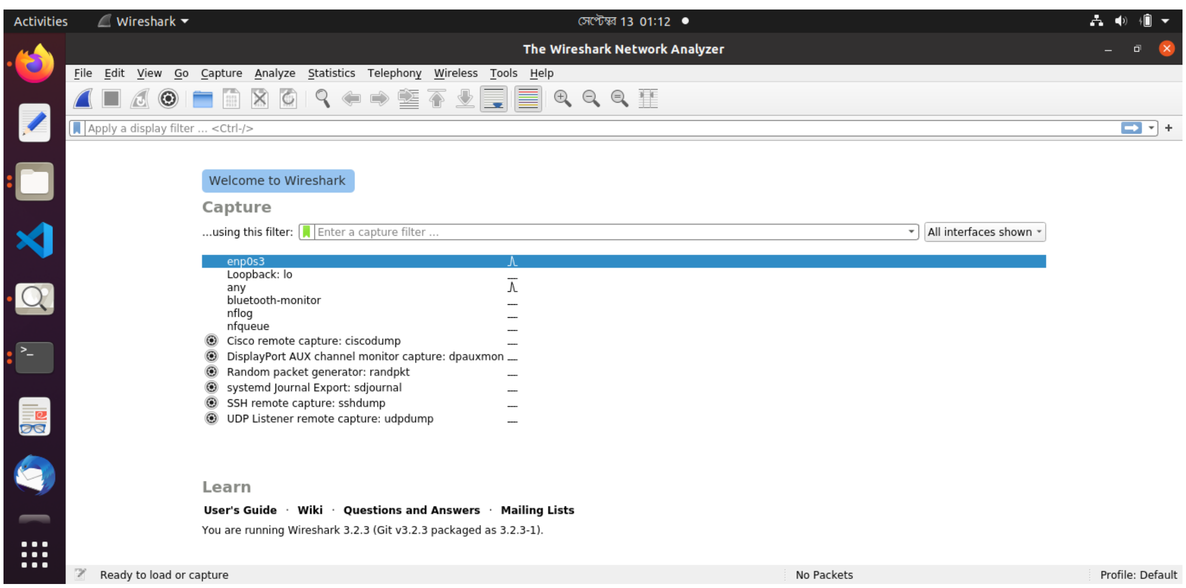

Figure 23: Wireshark

We open the last log file generated:

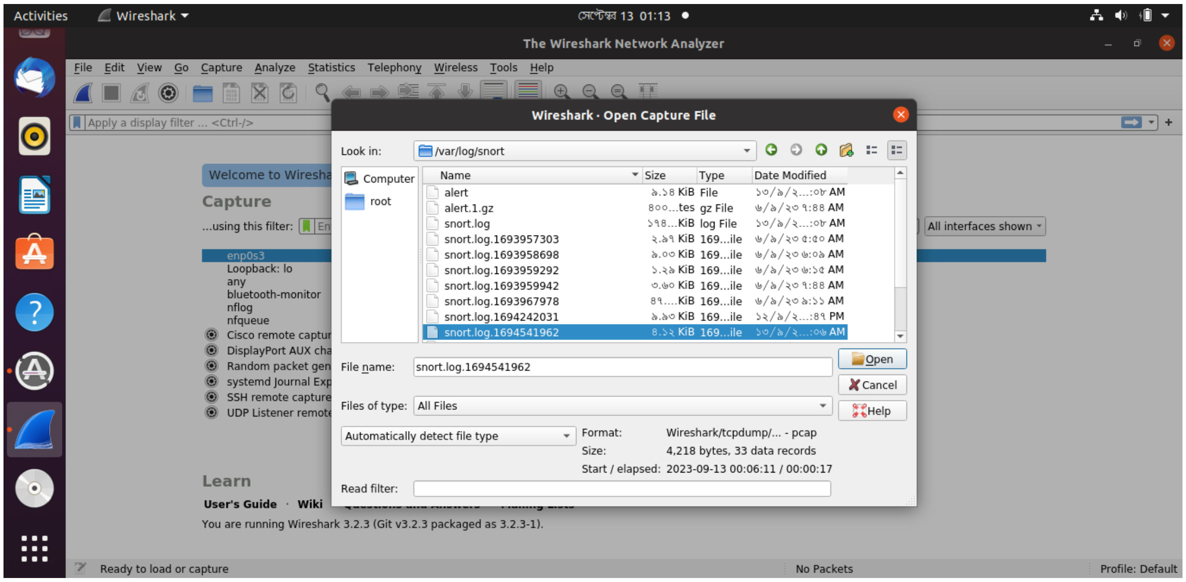

Figure 24: Open Capture File in Wireshark

Here, we can see the detailed information of every alert:

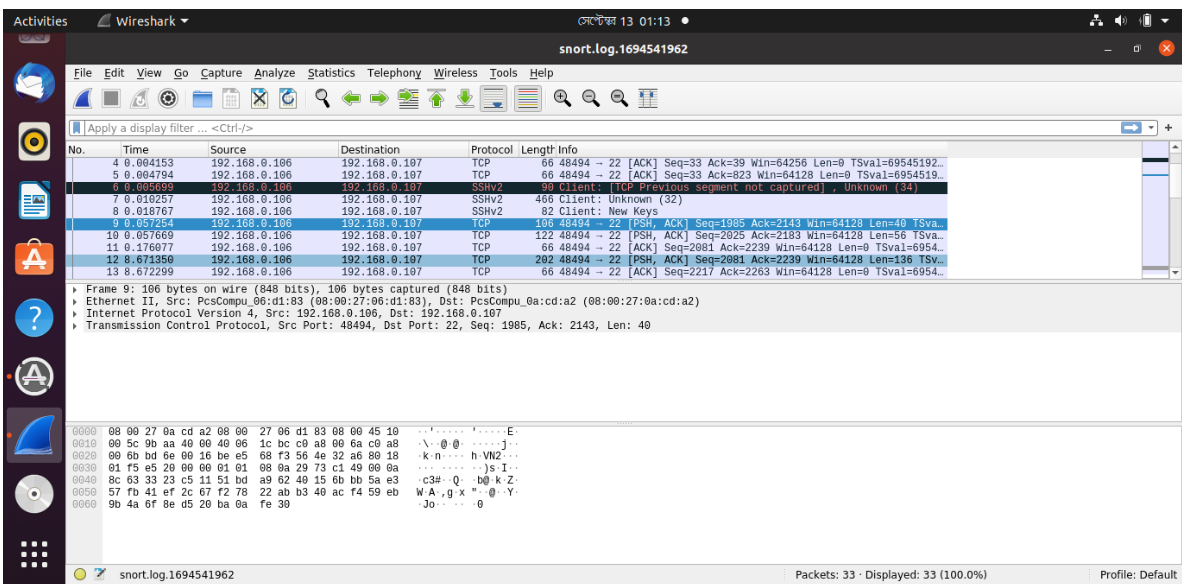

Figure 25: Logging in Wireshark

From here, we can do any kind of analysis we want.

4 Conclusion

In conclusion, Snort is a powerful and versatile intrusion detection and prevention system that plays a crucial role in network security. It operates based on predefined rules and can analyze network traffic in real-time, making it effective in detecting and responding to a wide range of malicious activities. Whether used for packet logging, packet sniffing, network intrusion detection, or network intrusion prevention, Snort provides valuable insights into network traffic and helps organizations defend against evolving cyber threats. Its open-source nature and extensive community support make it a valuable tool in the arsenal of network security solutions, ensuring the continued resilience of modern network infrastructures.

Resources:

- Snort Official Website
- Youtube Playlist on Snort By HackerSploit