REPORT

ON

INFORMATION AND NETWORK SECURITY MINI PROJECT

Submitted to

NMAM INSTITUTE OF TECHNOLOGY, NITTE

(Deemed to be University)

In partial fulfilment of the requirements for the award of the

Degree of Bachelor of Technology

In

Information Science & Engineering

By

SAMRUDDI NG

USN NNM22IS136

Under the guidance of

Dr. Jason Elroy Martis

Associate Professor

CERTIFICATE

This is to certify that the "INS Mini Project Report" submitted by Miss. Samruddi NG bearing USN NNM22IS136 of 6th semester B-Tech., a bonafide student of NMAM Institute of Technology, Nitte, fulfilling the partial requirements for the award of degree of Bachelor of Engineering in Information Science & Engineering at NMAM Institute of Technology, Nitte.

Name and Signature of Professor

Signature of HOD

ABSTRACT

Network security is an essential part of any information system in the digital world. Introduction This project aims on setting up an IDS i.e. bluntly Snort, it's a well-known and open-source network-based IDS tool. In most cases, their principal purpose is to analyze network traffic in order to identify suspicious activities or possible threats. As for the project, everything is done in a virtual machine as you are using VirtualBox and Ubuntu Server, so the things are easier to be set because everything is in a simulated environment.

When dealing with attacks or not, attackers tend to use ICMP traffic while communicating with a network so we then configure the IDS to alert us of ICMP traffic. A default Snort config file is set and a custom rule that will be used to inspect traffic for ICMP echo requests (ping) is added to the config file. We tested the system by sending out a ping operation simulating an attack. Upon detecting ICMP traffic, Snort generates and displays a real-time alert on the console. This shows that the IDS is working and able to detect certain types of network activity.

As well as showcasing the technical how to of setting up and configuring an IDS, this project teaches you how these things actually work in practice in terms of detecting and responding to potential threats on network. This project not only provides real-world experience communicating with Snort, but also demonstrates how intrusion detection can be used as a preemptive measure to stay secure when it comes to cybersecurity.

OBJECTIVES

The primary objectives of this project are:

- **To understand the fundamental concepts of Intrusion Detection Systems (IDS)** and their role in enhancing network security.
- **To set up a virtualized network environment** using VirtualBox and Ubuntu Server for safely deploying and testing the IDS.
- **To install and configure Snort**, an open-source Network-based Intrusion Detection System (NIDS), on a Linux-based virtual machine.
- **To create and implement custom Snort rules** for detecting specific types of network traffic, such as ICMP echo requests (ping).
- **To simulate network traffic** that mimics potential intrusion attempts in order to test the effectiveness of the IDS.
- **To verify Snort's ability to detect and alert** on suspicious activity in real time based on the custom rules.
- **To analyze and document the detection results**, demonstrating how Snort processes and reports network anomalies.
- **To gain hands-on experience in network security monitoring** and understand how IDS tools are applied in real-world environments.

METHODOLOGY

This project involves the setup, configuration, and demonstration of an Intrusion Detection System (IDS) using **Snort** in a simulated network environment.
The overall process is divided into several key process:

1. Environment Setup

- **VirtualBox** is installed to create a virtual environment.
- An **Ubuntu Server ISO** is downloaded and used to set up a virtual machine.
- The Ubuntu Server is updated to ensure all packages are current.

2. Snort Installation

- Snort is installed using the package manager:

```
sudo apt update && sudo apt install snort -y
```

- During installation, the network interface (enp0s3) is specified for Snort to monitor.
- The Snort version is verified to ensure successful installation.

3. Rule Configuration

- The local rules file located at /etc/snort/rules/local.rules is edited.
- A custom rule is added to detect ICMP traffic (ping):

```
alert icmp any any -> any any (msg:"ICMP test detected"; sid:1000001; rev:1;)
```

4. Testing and Demonstration

- Snort is run in IDS mode using:

```
sudo snort -A console -q -c /etc/snort/snort.conf -i enp0s3
```

- In another terminal or from the host machine, a ping is sent to the Snort machine:

```
ping <Snort_VM_IP>
```

- If the rule is correctly configured, Snort generates an alert:

```
[**] [1:1000001:1] ICMP test detected [**]
```

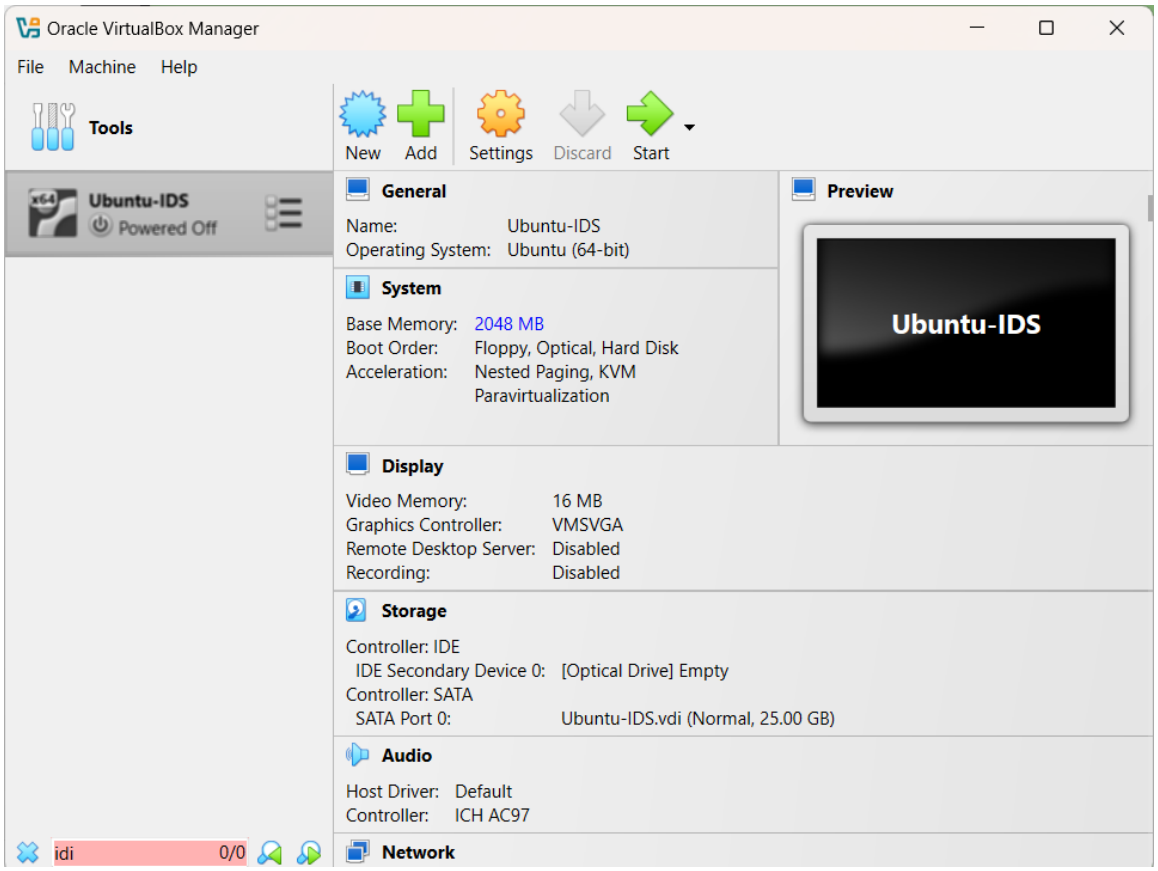
5. Analysis

- The alerts are reviewed in the console to confirm that Snort is actively monitoring and detecting traffic.
- Screenshots of the alert output and rules are captured for documentation.

RESULTS

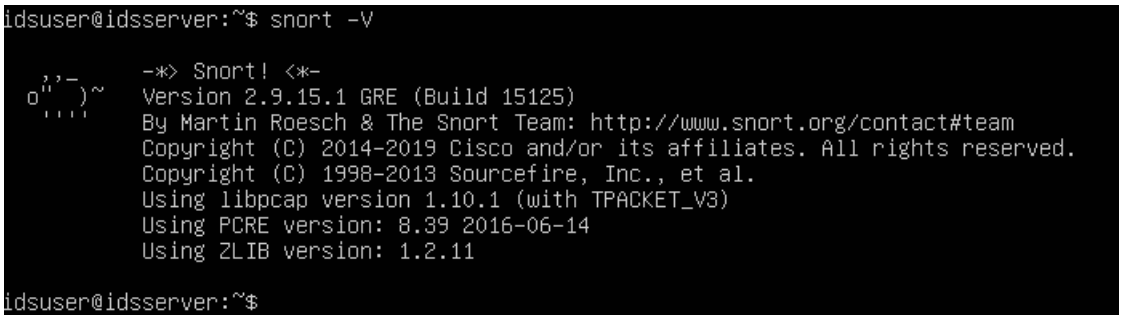
1. Virtual environment setup

- Installed Ubuntu Server



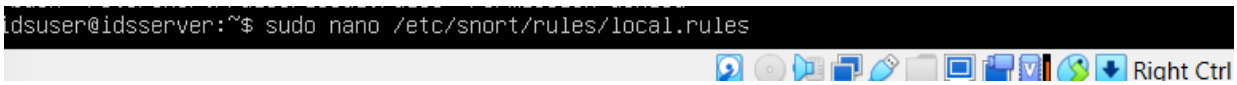
2. System and Snort Setup

- Output of snort -V showing version and successful installation



3. Rule Configuration

- Open the local.rules file:



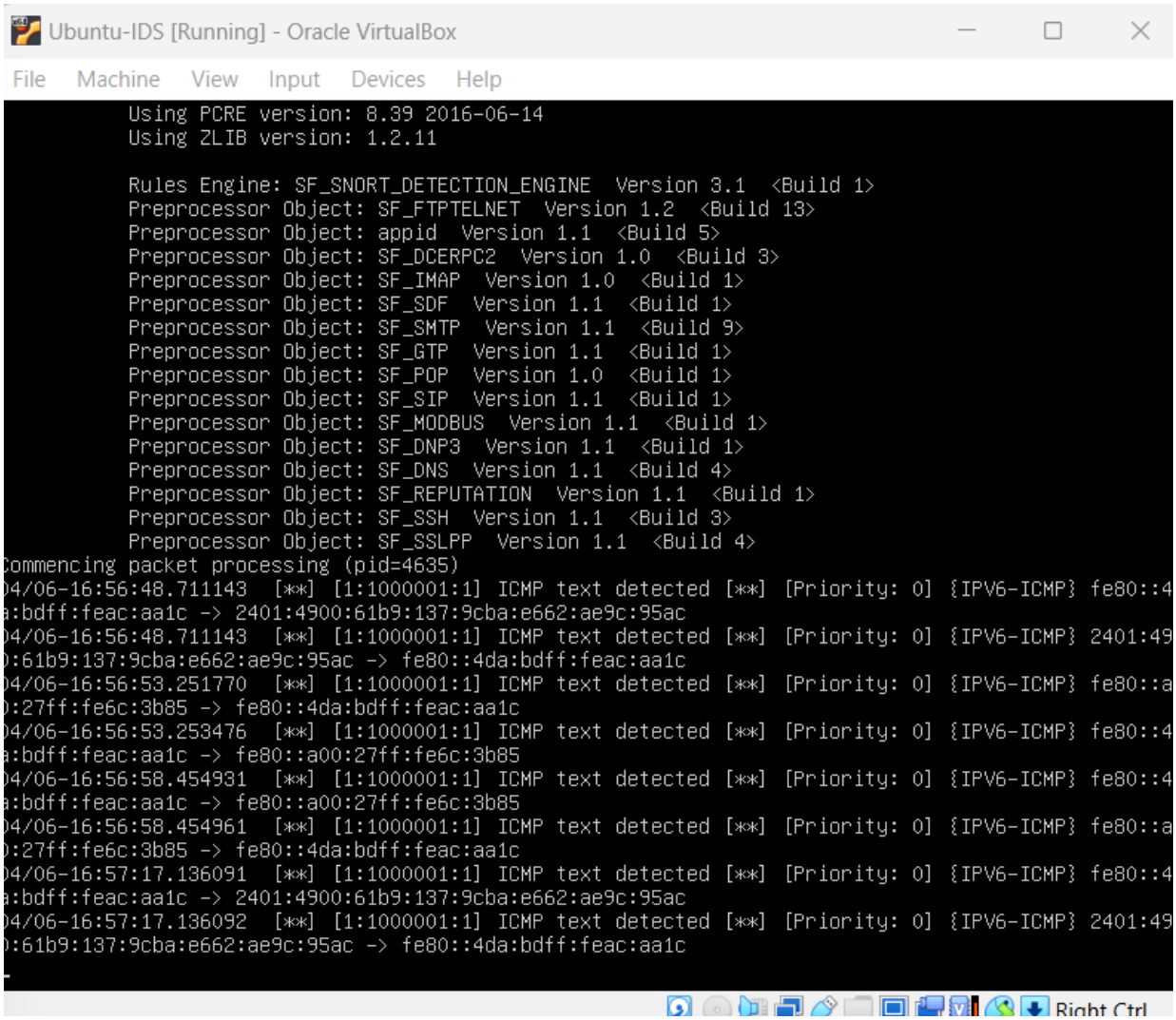
- custom ICMP rule and save the rule file.

```
 GNU nano 6.2                        /etc/snort/rules/local.rules
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
# ----------------
# LOCAL RULES
# ----------------
# This file intentionally does not come with signatures.  Put your local
# additions here.
alert icmp any any -> any any (msg:"ICMP text detected"; sid:1000001; rev:1;)
```

4. Running Snort

- Running Snort in IDS mode with the command:

```
idsuser@idsserver:~$ sudo snort -i enp0s3 -A console -c /etc/snort/snort.conf
```



5. Simulated an Attack

- From the same VM (or another terminal):

```
idsuser@idsserver:~$ ping -c 1 8.8.8.8
```

6. Snort Detection

- Snort console showing alert output:

```
04/06-18:14:35.523502  [**] [1:1000001:1] ICMP text detected [**] [Priority: 0] {IPV6-ICMP} fe80::4d
a:bdff:feac:aa1c -> 2401:4900:61b9:137:9cba:e662:ae9c:95ac
04/06-18:14:35.523502  [**] [1:1000001:1] ICMP text detected [**] [Priority: 0] {IPV6-ICMP} 2401:490
0:61b9:137:9cba:e662:ae9c:95ac -> fe80::4da:bdff:feac:aa1c
04/06-18:14:54.468234  [**] [1:1000001:1] ICMP text detected [**] [Priority: 0] {IPV6-ICMP} fe80::4d
a:bdff:feac:aa1c -> 2401:4900:61b9:137:9cba:e662:ae9c:95ac
04/06-18:14:54.468235  [**] [1:1000001:1] ICMP text detected [**] [Priority: 0] {IPV6-ICMP} 2401:490
0:61b9:137:9cba:e662:ae9c:95ac -> fe80::4da:bdff:feac:aa1c
```

CONCLUSION

A successful implementation and demonstration of an IDS using Snort provided beneficial insight into the inner workings of modern network security systems. The hands-on experience with this project provided a deep dive into how IDS tools operate in real time for monitoring, analyzing, and responding to malicious or questionable traffic. We achieved this by creating a simulated controlled environment with Virtual Box and Ubuntu Server that allowed us to experiment in a realistic network environment without harming any real systems.

As one of the most powerful and flexible open-source IDS, Snort gave us the advantage of configuring custom detection rules: one that will catch all ICMP traffic (typically used in ping sweep reconnaissance attacks). Snort was monitoring the interface we configured correctly and responding appropriately, considering the alert triggered after sending a simulated ping command. It obviously showed how security professionals are able to identify, and possibly stop, malicious traffic before damage can be done.
Furthermore, this project polished our hands-on experience on:

- Configure a Linux based system
- Network analysis: interface and traffic
- Implementing custom detection rules through writing and deployment

Understanding alert logs and what the responses mean
Having participated in every part of the IDS lifecycle, including installation, configuration, testing, and validation, we now have a better sense of how intrusion detection systems can be deployed in production networks for defense against an ever-evolving threat landscape.
This project provides a solid starting point to gain an understanding of the basic mechanics of deeper cybersecurity concepts, such as advanced intrusion detection, threat hunting, and security information and event management (SIEM) systems

Github link:
https://github.com/03NgSam/Information-Network-Security/upload/main/IDS-%20Snort%20Project

Demo Video link :
https://drive.google.com/file/d/1FS9Og6Px6-K-bcK2XvlDGvXlJ5ZhXIBj/view?usp=sharing