Task 4: Network Intrusion Detection System

# Objective

To set up a Network Intrusion Detection System (NIDS) using Snort to monitor network traffic, detect suspicious or malicious activities, and optionally visualize the detected attacks using dashboards.

# Tools Used

- Snort – NIDS Engine  
- Elastic Stack (ELK) – For log collection and visualization (Elasticsearch, Logstash, Kibana)  
- Ubuntu Linux (Recommended)  
- tcpdump/Wireshark – For packet analysis (optional)

# Step 1: Install Snort on Ubuntu

## 1.1 Update System

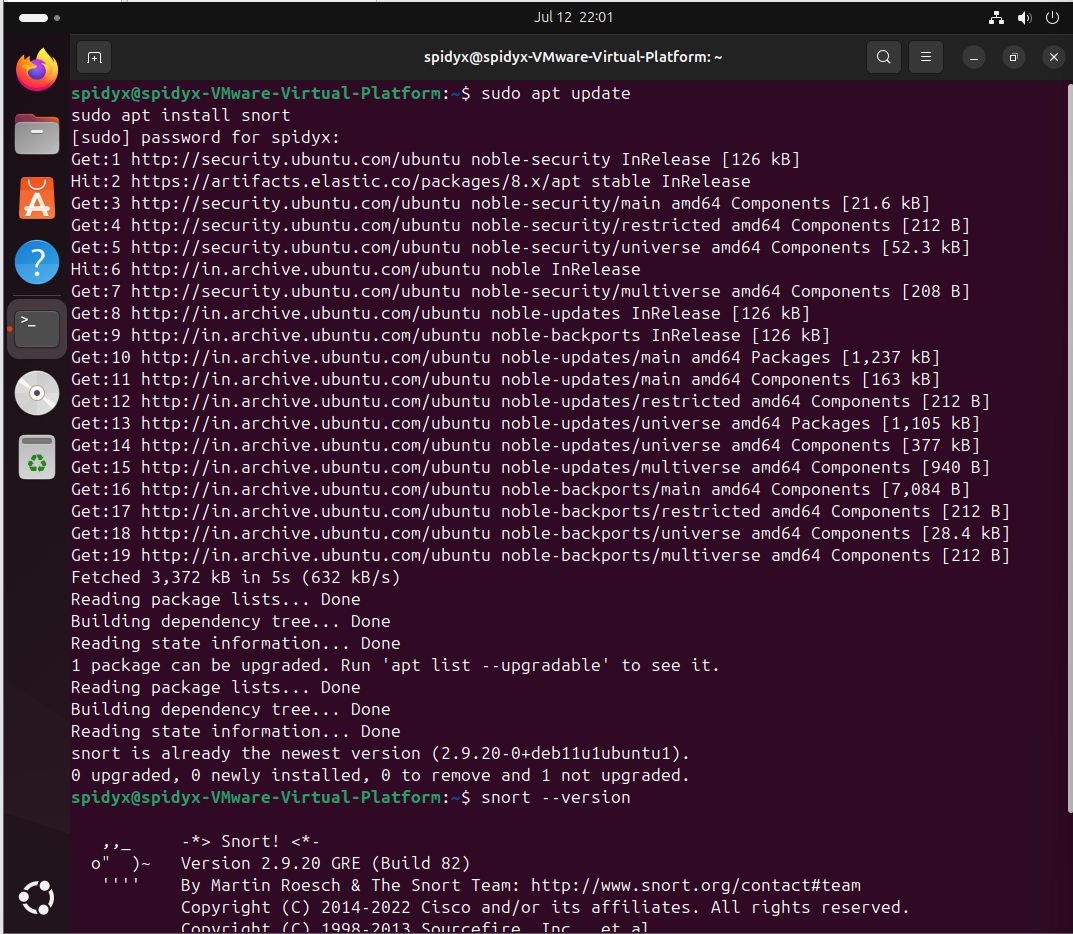
sudo apt update && sudo apt upgrade -y

## 1.2 Install Required Packages

sudo apt install -y build-essential libpcap-dev libpcre3-dev libdumbnet-dev bison flex zlib1g-dev liblzma-dev openssl libssl-dev

## 1.3 Download and Install DAQ

wget https://www.snort.org/downloads/snort/daq-2.0.7.tar.gz  
tar -xvzf daq-2.0.7.tar.gz  
cd daq-2.0.7  
./configure && make && sudo make install



## 1.4 Download and Install Snort

cd ~  
wget https://www.snort.org/downloads/snort/snort-2.9.20.tar.gz  
tar -xvzf snort-2.9.20.tar.gz  
cd snort-2.9.20  
./configure --enable-sourcefire && make && sudo make install

## 1.5 Configure Snort Environment

sudo ldconfig  
sudo ln -s /usr/local/bin/snort /usr/sbin/snort

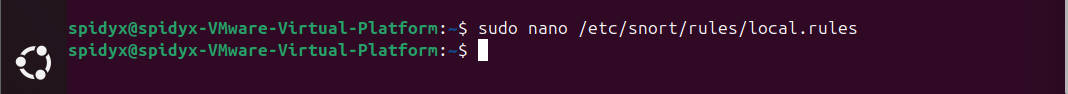
# Step 2: Configure Snort

## 2.1 Create Snort Directory Structure

sudo mkdir -p /etc/snort/rules  
sudo mkdir /var/log/snort  
sudo mkdir /usr/local/lib/snort\_dynamicrules

## 2.2 Create Empty Rule Files

sudo touch /etc/snort/rules/local.rules

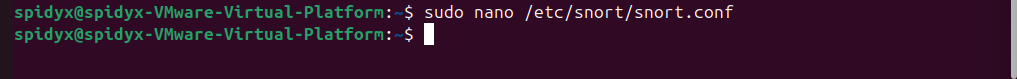


A screenshot of a computer

AI-generated content may be incorrect.  
sudo touch /etc/snort/rules/white\_list.rules  
sudo touch /etc/snort/rules/black\_list.rules

## 2.3 Configure snort.conf

cp ~/snort-2.9.20/etc/snort.conf /etc/snort/  
sudo nano /etc/snort/snort.conf



A screenshot of a computer

AI-generated content may be incorrect.  
  
Update:  
var RULE\_PATH /etc/snort/rules  
include $RULE\_PATH/local.rules

# Step 3: Create and Test Custom Rules

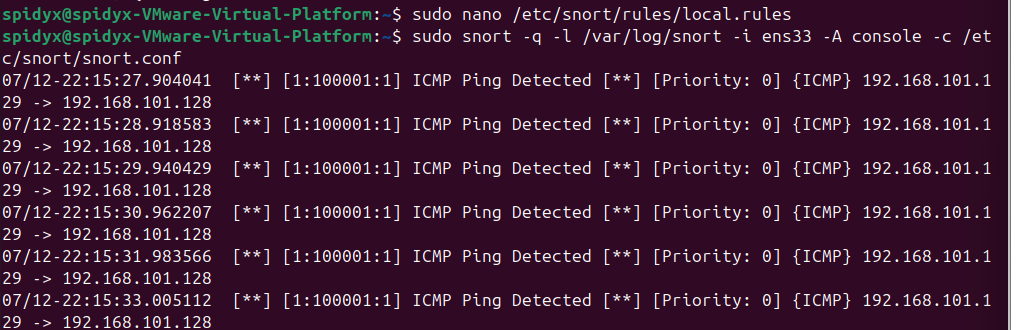
## Example Rule (ICMP Ping Detection)

alert icmp any any -> any any (msg:"ICMP Packet Detected"; sid:1000001; rev:1;)

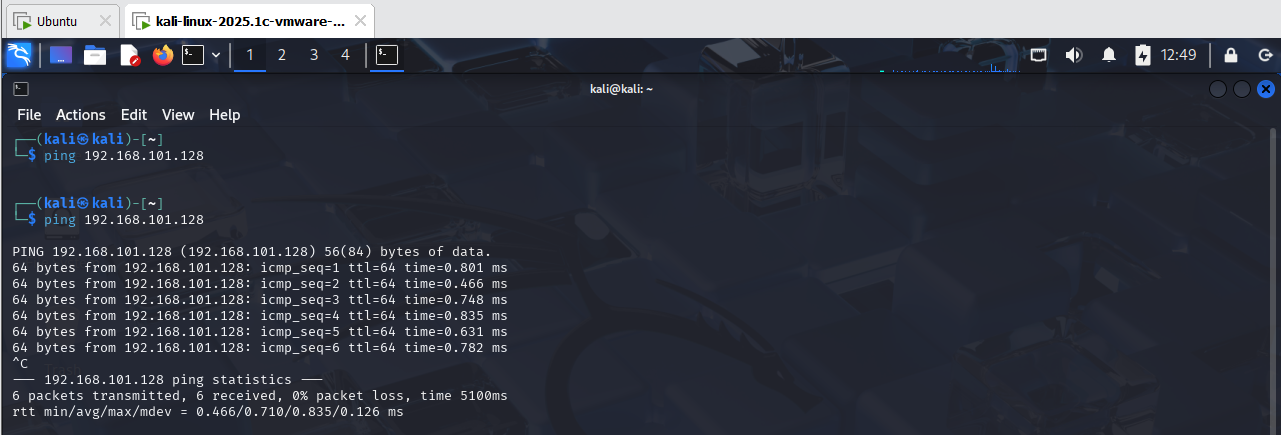
A screenshot of a computer program

AI-generated content may be incorrect.

## Test Rule with Ping

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

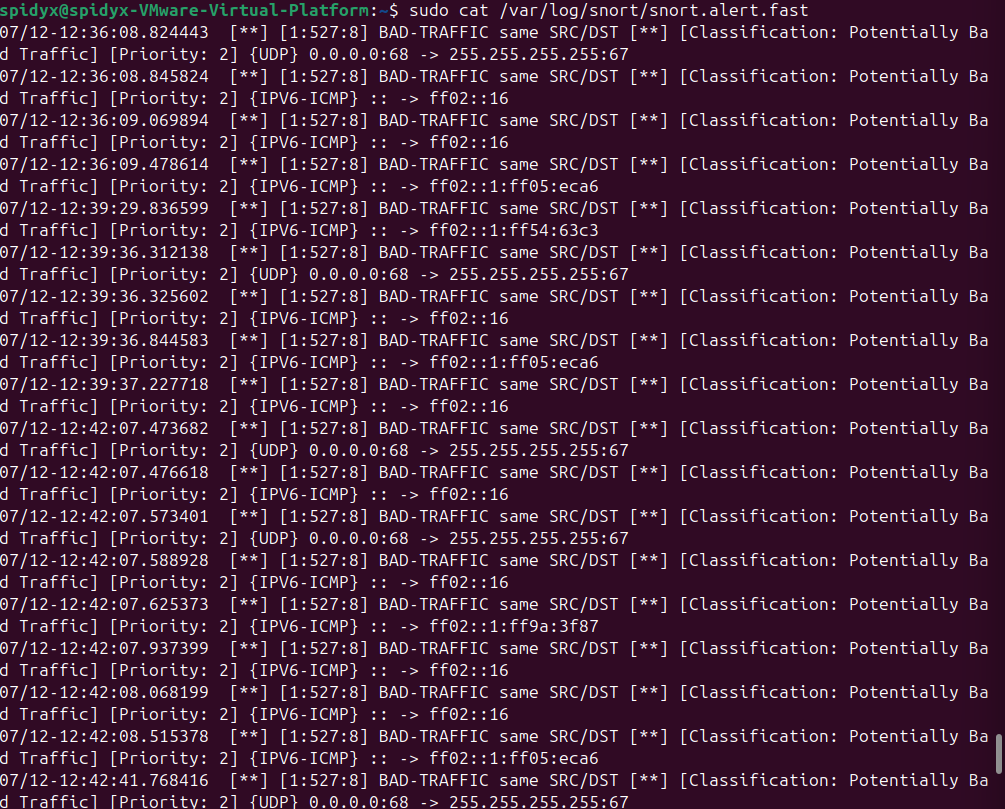
ping <your\_snort\_machine\_ip>



# Step 4: Monitor Network Traffic

## Continuous Monitoring Mode Using Nmap

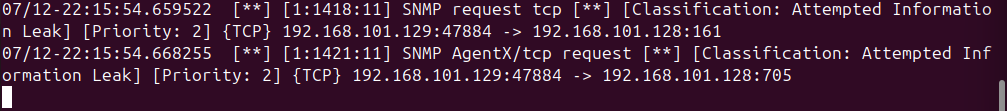
sudo snort -A fast -c /etc/snort/snort.conf -i ens33 -l /var/log/snort/



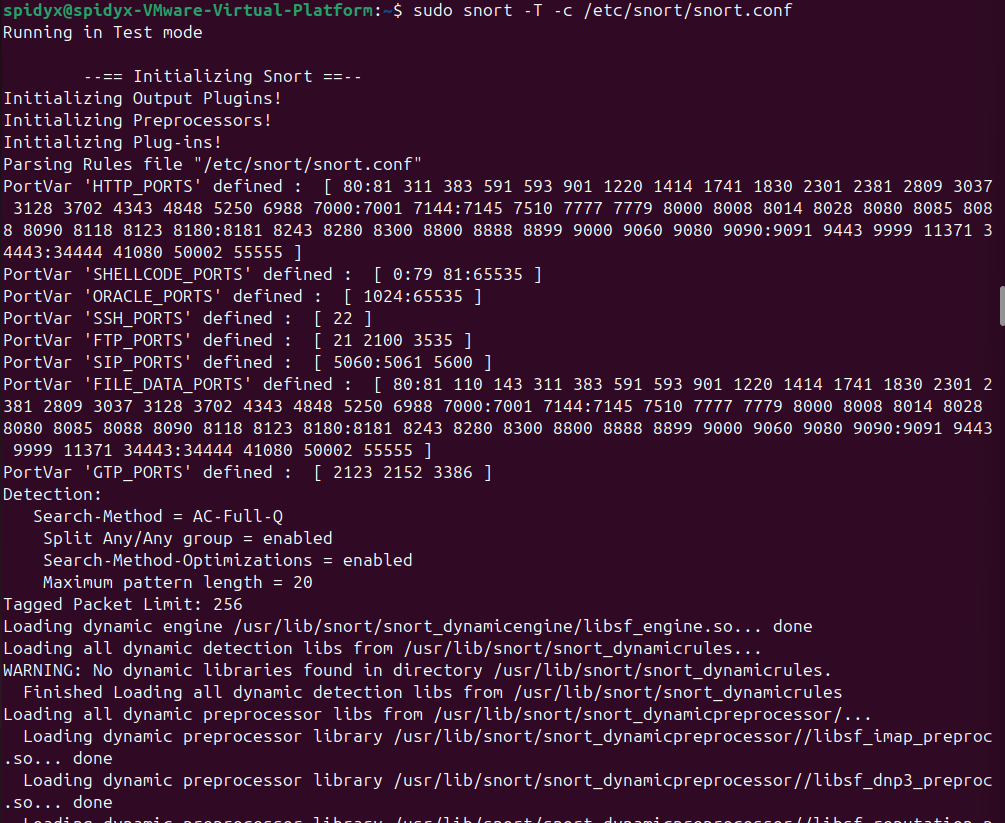
It monitors all the traffic using the alerts  
Alerts will be saved to /var/log/snort/snort.alert.fast

A black object on a surface

AI-generated content may be incorrect.



To know snort in working properly with all rules or not



It will show Snort successfully validated the configuration

A screenshot of a computer

AI-generated content may be incorrect.

# Step 5: Implement Response Mechanisms Using Mailing

Use Swatch or OSSEC to trigger scripts based on Snort alerts.  
Set up email alerts using log monitoring tools like inotify or logwatch.

Install Mailutils:

A screenshot of a computer

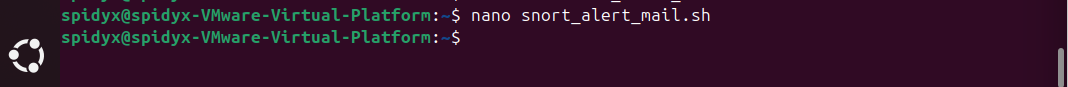
AI-generated content may be incorrect.

Check mail.log is working or not

A screenshot of a computer program

AI-generated content may be incorrect.

Then set a snort alert mail



A screenshot of a computer

AI-generated content may be incorrect.

Then set a timmer using contrab -e

A screen shot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

# Conclusion

This task successfully demonstrates the configuration and deployment of a Network Intrusion Detection System using Snort. It includes:  
- Detection of network-based threats  
- Rule configuration for known signatures  
- Continuous traffic monitoring  
  
This setup enhances an organization’s ability to detect, respond, and understand network threats in real time.