Snort IDS Installation and Configuration Report

# 1. Introduction

This report outlines the process of installing, configuring, and running Snort as an Intrusion Detection System (IDS) on a Kali Linux machine. It includes steps followed, commands executed, encountered issues, and how they were resolved.

# 2. Objectives

The goal was to build and configure Snort from source and set it up to run in IDS mode, monitoring network traffic for suspicious activity.

# 3. Installation and Configuration Steps

## Update and upgrade system packages

sudo apt update && sudo apt upgrade -y

## Install required dependencies

sudo apt install -y build-essential libpcap-dev libpcre3-dev libdumbnet-dev bison flex zlib1g-dev liblzma-dev openssl libssl-dev pkg-config libhwloc-dev cmake libc-ares-dev libluajit-5.1-dev libnghttp2-dev libdnet autoconf libtool

## Download Snort source code

wget https://www.snort.org/downloads/snort/snort-2.9.20.tar.gz

## Extract and navigate to Snort source

tar -xvzf snort-2.9.20.tar.gz && cd snort-2.9.20

## Configure and compile Snort

./configure && make && sudo make install

## Create Snort directories

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

## Copy configuration files

sudo cp etc/\*.conf\* /etc/snort && sudo cp etc/\*.map /etc/snort

## Update snort.conf with correct network range

ip a # to find your IP, then set HOME\_NET in snort.conf accordingly (e.g., 10.0.2.0/24)

## Run Snort in IDS mode

sudo snort -A console -q -c /etc/snort/snort.conf -i eth0

# 4. Common Issues and Fixes

## Issue: 404 Errors fetching packages

Run: sudo apt update --fix-missing

## Issue: Missing libpcap, pcre, dnet, daq\_static, or luajit

Install with apt, or compile manually from source if not available.

## Issue: rpc/rpc.h not found

Install rpc headers: sudo apt install libtirpc-dev

## Issue: Snort service not found

Run Snort manually or set up a custom systemd service.

## Issue: Dynamic rules path error

Create the missing directory: sudo mkdir /usr/local/lib/snort\_dynamicrules

# 5. Conclusion

By following these steps, we successfully compiled and configured Snort IDS on Kali Linux. We resolved dependency issues, configured the network range, and validated Snort's ability to run in IDS mode.