**Title**: Snort-Based Intrusion Detection System (IDS)   
**Author**: Ravindra Pandit Ahire  
**Channel**: CyberTechX\_ravin  
**Date**: April 11, 2025  
**Email**: Ravindraahire897@gmail.com

**📝 Overview**

This guide outlines the complete setup of a Snort-based Intrusion Detection System (IDS) on Ubuntu, including prerequisites, installation, configuration, and testing procedures.

**✅ Prerequisites**

* Ubuntu 20.04 or later
* sudo/root access
* Snort-compatible network interface
* Network connection
* Secondary machine (e.g., Kali Linux) for testing

sudo apt update && sudo apt upgrade -y

**🛠️ Step 1: Install Required Dependencies**

sudo apt install -y build-essential libpcap-dev libpcre3-dev libdnet-dev zlib1g-dev

**📥 Step 2: Download & Install Snort**

wget https://www.snort.org/downloads/snort/snort-2.9.X.tar.gz

tar -xvzf snort-2.9.X.tar.gz

cd snort-2.9.X

./configure --enable-sourcefire

make

sudo make install

Check installation:

snort -V

**⚙️ Step 3: Configuration Directories**

sudo mkdir /etc/snort

sudo cp etc/\* /etc/snort/

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

sudo chmod -R 5775 /etc/snort /var/log/snort /usr/local/lib/snort\_dynamicrules

**⚙️ Step 4: Edit snort.conf**

sudo nano /etc/snort/snort.conf

Inside snort.conf, set:

var HOME\_NET 192.168.1.0/24

var EXTERNAL\_NET !$HOME\_NET

include $RULE\_PATH/local.rules

**✍️ Step 5: Create Custom Rules**

sudo nano /etc/snort/rules/local.rules

Add these rules:

alert icmp any any -> $HOME\_NET any (msg:"ICMP Ping Detected"; sid:1000001; rev:1;)

alert tcp any any -> $HOME\_NET 21 (msg:"FTP Connection Attempt"; sid:1000002; rev:1;)

alert tcp any any -> $HOME\_NET 80 (msg:"HTTP Connection Attempt"; sid:1000003; rev:1;)

alert udp any any -> $HOME\_NET 53 (msg:"UDP Port 53 Access Detected"; sid:1000004; rev:1;)

**🚀 Step 6: Run Snort in IDS Mode**

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

To check interface name:

ip addr

**🧪 Step 7: Simulate Attacks (From Kali Linux)**

ping <Snort-IP>

nmap -sS <Snort-IP>

echo 'test' | nc -u <Snort-IP> 53

**🎯 Conclusion**

After following these steps, your Snort IDS will be running and capable of detecting suspicious activities. You can now showcase this in your cybersecurity portfolio or demo it on your YouTube channel.