Snort Installation in Ubuntu

1. Prerequisites

System Requirements

- **Ubuntu 20.04/22.04** (or any Debian-based Linux)
- Minimum **2GB RAM**, **Dual-core CPU**
- **Internet connection** to install dependencies

Tools Required

- **Snort** (Network IDS)
- **Wireshark** (for packet analysis, optional)
- **Tcpdump** (for traffic capture)
- **iptables** (for firewall rules)

---

2. Install Snort on Ubuntu

Step 1: Update System

```
sudo apt update && sudo apt upgrade -y
```

Step 2: Install Dependencies

```
sudo apt install -y snort tcpdump libpcre3 libpcre3-dev zlib1g zlib1g-dev
libluajit-5.1-dev
```

Step 3: Verify Snort Installation

```
snort -V
```

You should see Snort's version details.

---

3. Configure Snort

Step 1: Find Network Interface

Find your active network interface:

```
ip a
```

Example output:

```
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500
```

Here, **ens33** is the interface.

Step 2: Edit Snort Configuration

Open the Snort config file:

```
sudo nano /etc/snort/snort.conf
```

Modify:

- **Set network range**
  Find:

  ```
  ipvar HOME_NET any
  ```

  Replace `any` with your subnet (find with `ip a` command). Example:

  ```
  ipvar HOME_NET 192.168.1.0/24
  ```

- **Enable Rule Path**
  Locate:

  ```
  var RULE_PATH ../rules
  ```

  Change to:

  ```
  var RULE_PATH /etc/snort/rules
  ```

Step 3: Create Snort Rule File

Create a custom rule file:

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

Add a test rule:

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

Save and exit.

---

4. Running Snort

Step 1: Test Snort Configuration

```
sudo snort -T -i ens33 -c /etc/snort/snort.conf
```

Ensure no errors appear.

Step 2: Start Snort in IDS Mode

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

- `-A console`: Shows alerts on the terminal
- `-q`: Runs in quiet mode (only logs alerts)

Step 3: Generate a Test Attack (ICMP Ping)

From another machine, ping your Ubuntu system:

```
ping -c 4 192.168.1.10
```

Snort should detect and alert:

```
[**] [1:1000001:1] ICMP Ping Detected [**]
```

---

5. Reporting & Logs

Snort logs alerts in:

```
cat /var/log/snort/alert
```

For real-time monitoring:

```
tail -f /var/log/snort/alert
```