Network Intrusion Detection System

🌐 What is an Intrusion Detection System (IDS)?

An **Intrusion Detection System (IDS)** is like a security guard for your computer or network. It **watches everything happening**—like who's trying to get in, what they're doing, and if something **suspicious or dangerous** is going on, it raises an alarm.

Think of it like a CCTV camera system:

- It doesn't stop the thief.
- But it **alerts you** if someone is trying to break in.

Type Of IDS :

1. Network Intrusion Detection System
2. Host Intrusion Detection System

🔍 What is a Network Intrusion Detection System (NIDS)?

A **Network IDS (NIDS)** is a specific kind of IDS that **monitors an entire network** instead of just one computer. It sits in a **strategic place** on the network (like near the firewall) and watches **all incoming and outgoing traffic**, looking for bad stuff.

Imagine a security guard **watching all the roads** into a city rather than just one building. That's a NIDS.

📋 NIDS Project Report – Kali Linux Version

Tool Used: Snort
System: Kali Linux 2024
Interface Monitored: eth0 *(or check with `ip a`)*
Network Range: 192.168.1.0/24

✅ Custom Rules Created:

Rule Type	Rule Snort Syntax	Purpose
ICMP Alert	`alert icmp any any -> any any (msg:"ICMP Ping Detected"; sid:1000001; rev:1;)`	Detect ping packets
Port Scan	`alert tcp any any -> any 22 (msg:"Port 22 Access"; sid:1000002; rev:1;)`	Detect SSH port scan

🛠️ Testing Performed:

- ✅ Sent ICMP ping to Kali machine → **Alert triggered**
- ✅ Used Nmap to scan SSH port (22) → **Alert triggered**

Key Learnings:

- Learned how to configure Snort and write basic detection rules.
- Understood how to monitor real-time traffic on Kali Linux.
- Saw how easily Snort can detect common suspicious behaviors.
- Identified how to test alerts using `ping` and `nmap`.

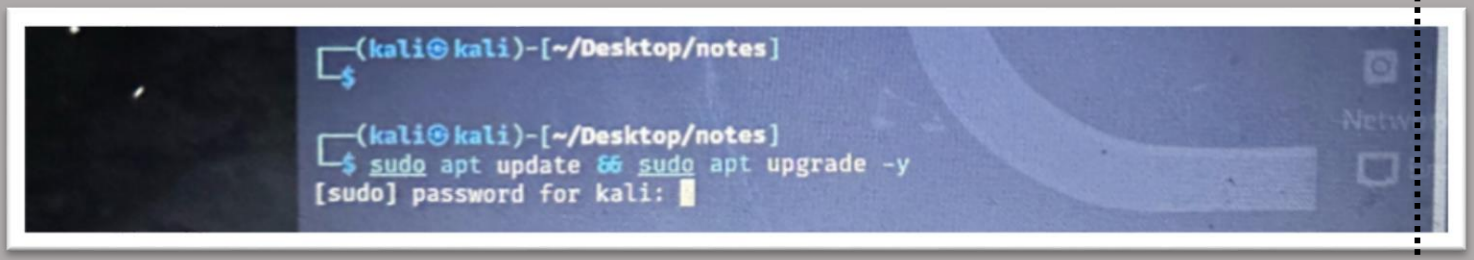
Steps:

There are the few steps that use for the network Intrusion Detection System.

Step 1: Update Your System

You're making sure everything in Kali is up to date before installing anything.

☞ Run this in the terminal:



✅ Step 2: Install Snort

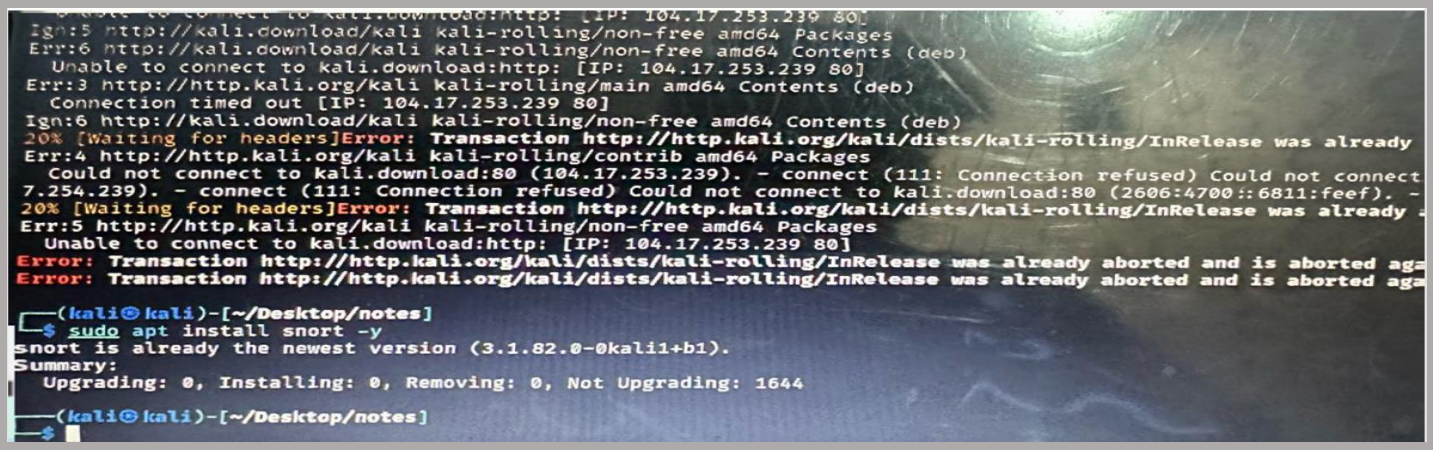
You're installing the main tool, **Snort**.

👉 Run this:

```
sudo apt install snort -y
```

During installation:

- It'll ask for your **network interface** (like `eth0` or `wlan0`). You can check which one you're using by typing:



✅ Step 3: Check Snort Version

Just to confirm that Snort was installed correctly:

👉 Type this:

```
Bash

snort -V
```

✅ Step 4: Create a Detection Rule

Now, you're writing your **own rule** that tells Snort:

“If someone sends a ping to any device, show an alert.”

👉 Open the rule file:

```
Bash

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

👉 Add this line:

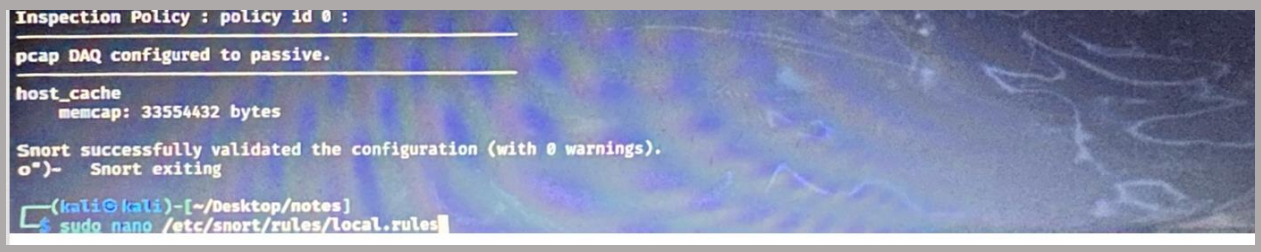
```
bash
```

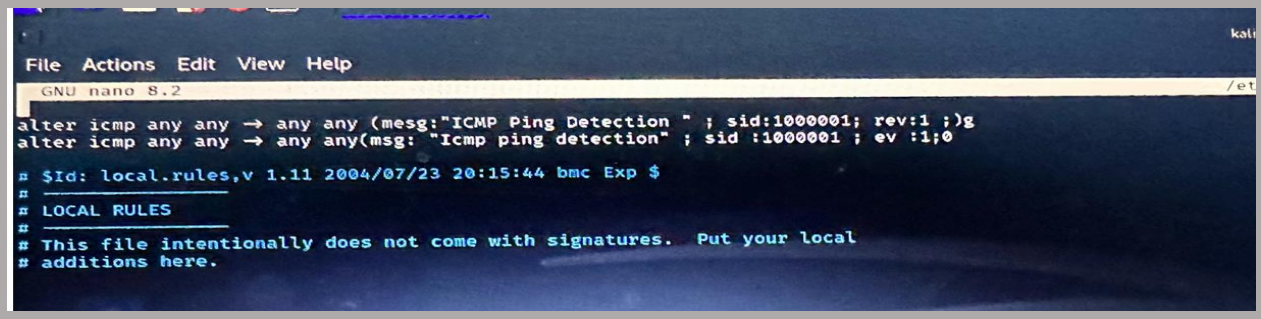
```
alert icmp any any -> any any (msg:"ICMP Ping Detected"; sid:1000001; rev:1;)
```

This means:

- **ICMP** = type of traffic used for ping
- **msg** = the message you'll see when this rule is triggered

Then save by pressing:
`CTRL + X`, then `Y`, then `Enter`





✅ Step 5: Link Your Rule File to Snort

You now make sure Snort **uses your rule**.

👉 Open this file:

```
bash

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

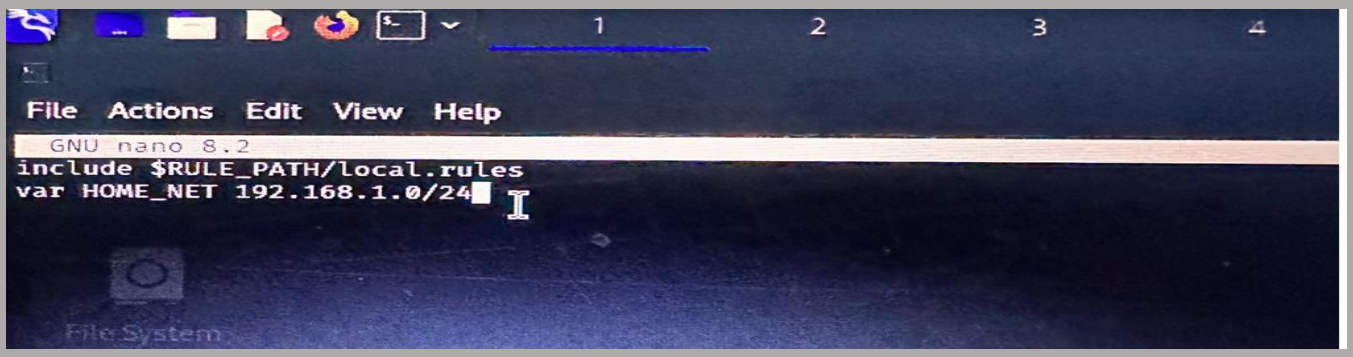
Make sure this line is NOT commented (remove any #):

```
Bash

include $RULE_PATH/local.rules
```

Also look for:

```
bash

var HOME_NET 192.168.1.0/24
```

Make sure it matches your network range.



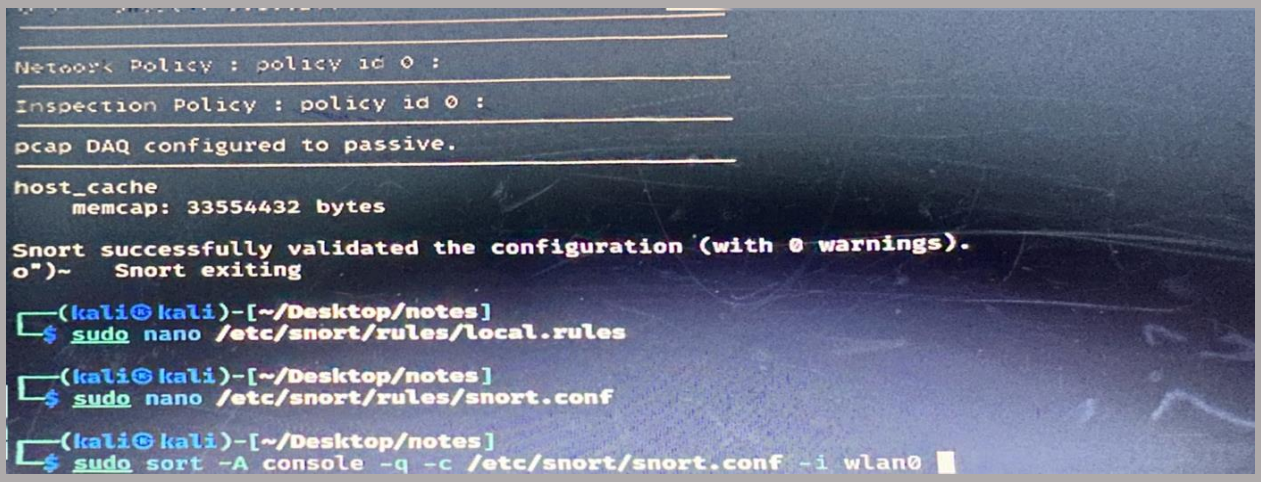
✅ Step 6: Run Snort in IDS Mode

Now, you're telling Snort to **start watching traffic**.

👉 Run this:

```
bash

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

- `-A console` = show alerts in terminal
- `-q` = quiet (don't show extra logs)
- `-c` = use your config file
- `-i eth0` = use your network interface (use `ip a` to check if it's `eth0`, `wlan0`, etc.)



✅ Step 7: Test Your Rule

Now go to another system on the same network (or a second terminal if you have one) and **ping your Kali machine**:

```
bash
CopyEdit
ping 192.168.1.15  # Replace with your Kali IP address
```

If it works, you'll see this in the Snort terminal:

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

That means your IDS is working and **detecting real-time activity**!

📊 Bonus: Visualize It (Optional)

If you want to go next-level:

- Use **Wireshark** (already in Kali) to inspect packets
- Or install **Kibana + Elasticsearch** to build a dashboard

✅ Summary: What You Did

Step	What You Did
Updated Kali	So everything is fresh
Installed Snort	The core IDS tool
Wrote a Rule	To detect ping (ICMP) packets
Ran Snort	In monitoring mode
Tested it	By sending a ping to yourself

Step	What You Did
Saw an Alert	Which means success 🎉