

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	<pre>alert icmp any any -> any any (msg:"ICMP Ping Detected"; sid:1000001; rev:1;)</pre>	Detect ping packets
Port Scan	<pre>alert tcp any any -> any 22 (msg:"Port 22 Access"; sid:1000002; rev:1;)</pre>	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`.

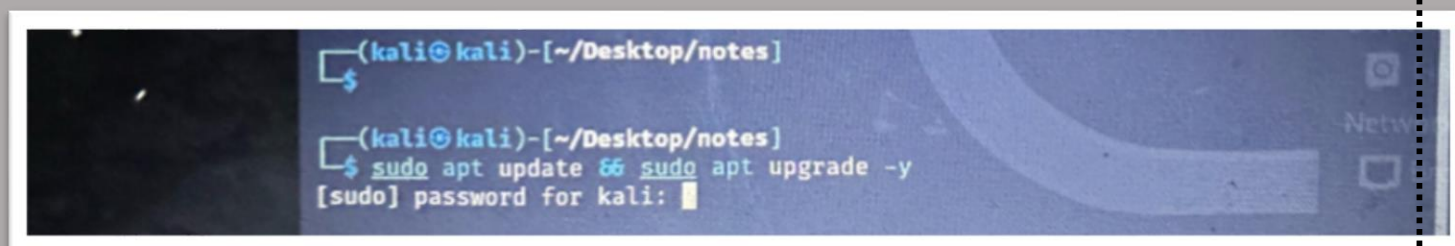
Steps:

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:

A screenshot of a Kali Linux terminal window. The prompt is `(kali㉿kali)-[~/Desktop/notes]`. The first command entered is `$`. The second command is `$ sudo apt update && sudo apt upgrade -y`. The third line shows the prompt `[sudo] password for kali:` followed by a cursor. The terminal has a dark background with a blue and white logo on the right side.

```
(kali㉿kali)-[~/Desktop/notes]
$
(kali㉿kali)-[~/Desktop/notes]
$ sudo apt update && sudo apt upgrade -y
[sudo] password for kali:
```

✓ Step 2: Install Snort

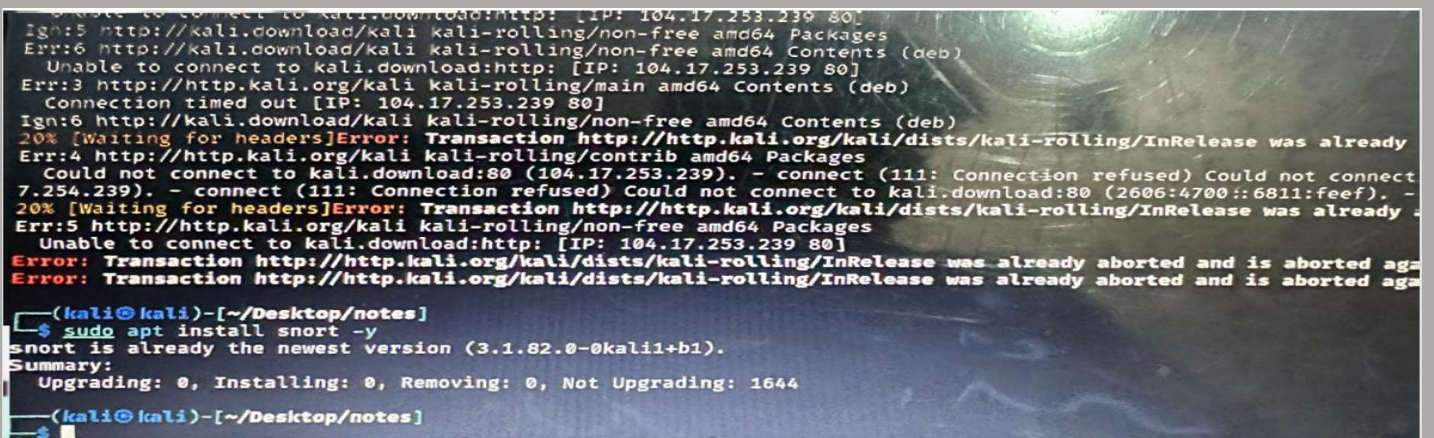
You're installing the main tool, **Snort**.

👉 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:



```
(kali㉿kali)-[~/Desktop/notes]
$ sudo apt install snort -y
snort is already the newest version (3.1.82.0-0kali1+b1).
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 1644
(kali㉿kali)-[~/Desktop/notes]
$
```

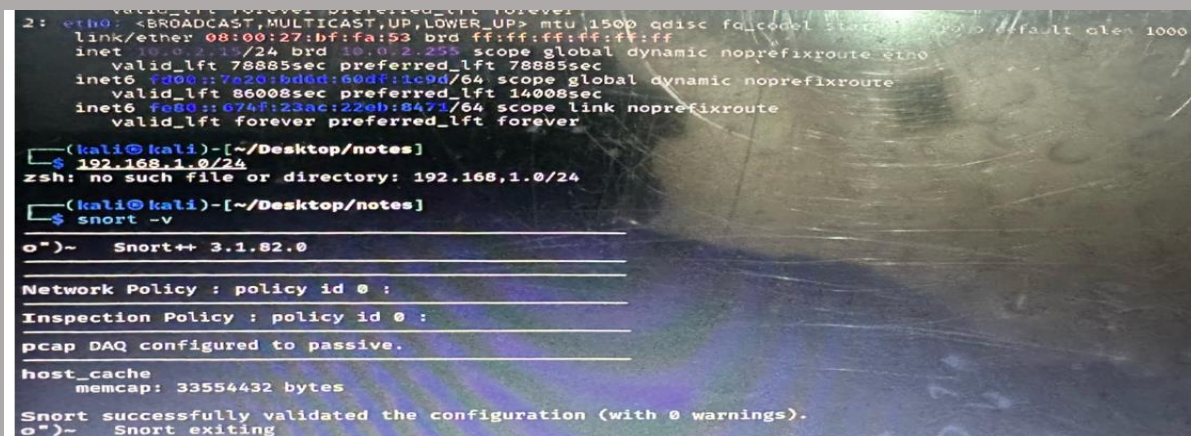
✓ Step 3: Check Snort Version

Just to confirm that Snort was installed correctly:

☞ Type this:

Bash

```
snort -V
```



```
2: veth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP default qlen 1000
    link/ether 08:00:27:b7:fa:53 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.0/24 brd 192.168.1.255 scope global dynamic noprefixroute veth0
        valid_lft 78885sec preferred_lft 78885sec
    inet6 fd00::7a20:bd4d:60df:1c9d/64 scope global dynamic noprefixroute
        valid_lft 86008sec preferred_lft 14008sec
    inet6 fe80::674f:23ac:22eb:8473/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

(kali@kali)-[~/Desktop/notes]
$ 192.168.1.0/24
zsh: no such file or directory: 192.168.1.0/24

(kali@kali)-[~/Desktop/notes]
$ snort -v
o*)~  Snort++ 3.1.82.0

Network Policy : policy id 0 :
Inspection Policy : policy id 0 :
pcap DAQ configured to passive.

host_cache
  memcap: 33554432 bytes

Snort successfully validated the configuration (with 0 warnings).
o*)~  Snort exiting
```

✓ 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
```

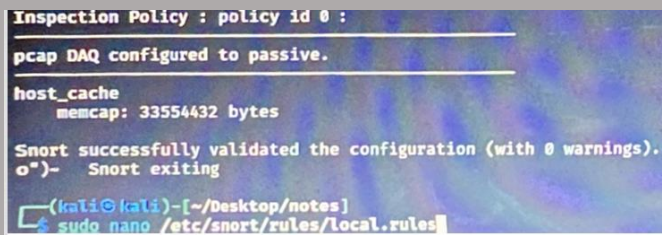
```
alert icmp any any -> any any (msg:"ICMP Ping Detected"; sid:1000001; rev:1;)
```

This means:

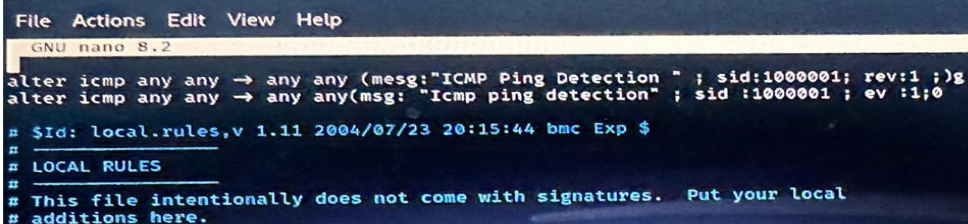
- **ICMP** = type of traffic used for ping
- **msg** = the message you'll see when this rule is triggered

Then save by pressing:

CTRL + X, then Y, then Enter



```
Inspection Policy : policy id 0 :  
pcap DAQ configured to passive.  
host_cache  
  memcap: 33554432 bytes  
Snort successfully validated the configuration (with 0 warnings).  
o")-  Snort exiting  
(kali@kali)-[~/Desktop/notes]  
$ sudo nano /etc/snort/rules/local.rules
```



```
File Actions Edit View Help  
GNU nano 8.2 /etc/snort/rules/local.rules  
alter icmp any any -> any any (msg:"ICMP Ping Detection " ; sid:1000001; rev:1 ;)g  
alter icmp any any -> any any(msg: "Icmp ping detection" ; sid :1000001 ; ev :1;0  
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $  
#  
# LOCAL RULES  
#  
# This file intentionally does not come with signatures.  Put your local  
# additions here.
```

✓ 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
```

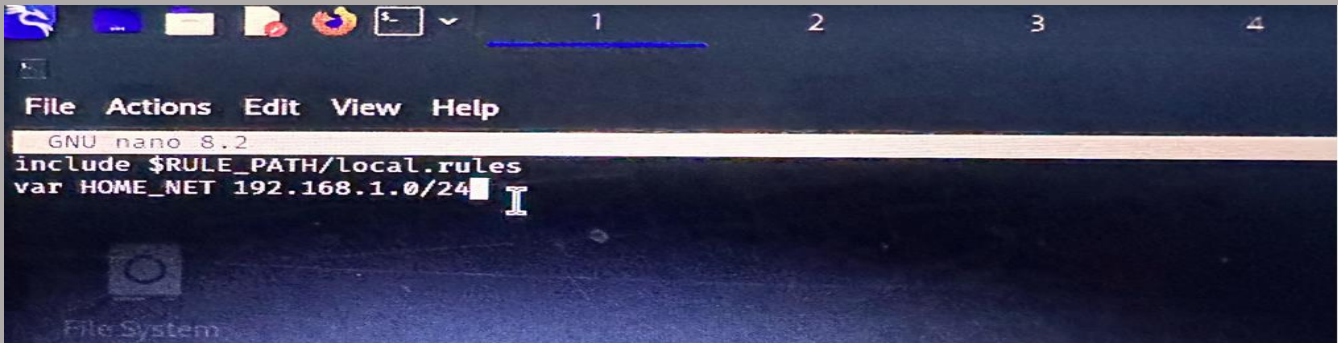
```
include $RULE_PATH/local.rules
```

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

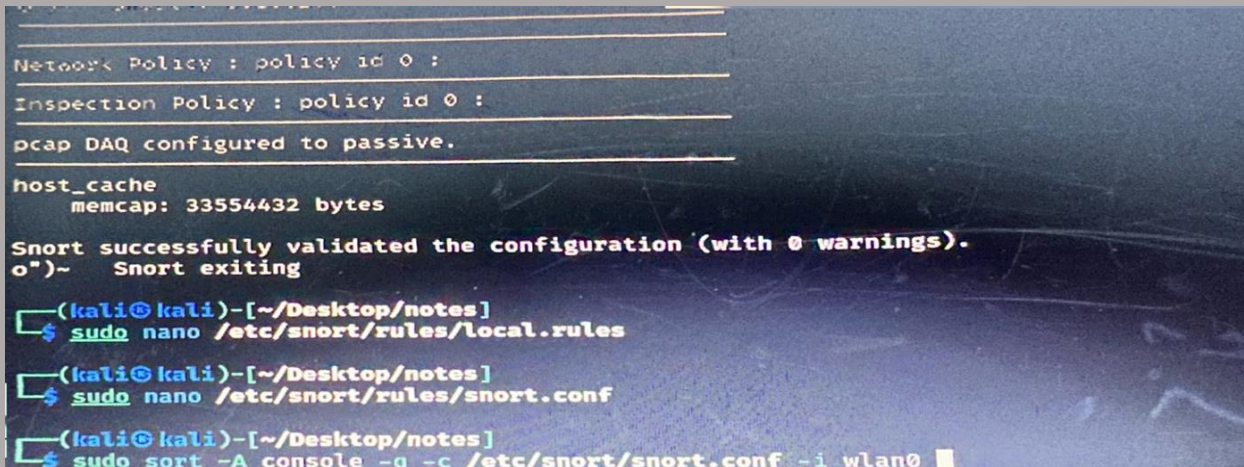
Now, you're telling Snort to **start watching traffic**.

🔗 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 🎉