" We’re going to set up a Network Intrusion Detection System using Suricata on Kali Linux.  
We’ll go slowly, step-by-step, so even if you’re new to Linux, you can follow along."

**2. What is a NIDS?**

"A Network Intrusion Detection System — or NIDS — watches network traffic for suspicious activity.  
Think of it like a CCTV camera for your network. Suricata is the software we’ll use to do this."

**3. Step 1 – Open the Terminal**

"First, open the Terminal. This is where we type our commands. On Kali Linux, the terminal icon is usually on the top bar or side panel."

**4. Step 2 – Install Suricata**

**Commands:**

sudo apt update

sudo apt install -y suricata jq

"Type sudo apt update to refresh the list of available packages. Then type sudo apt install -y suricata jq to install Suricata and jq, which helps us read JSON output.  
Press **Enter** after each command. You might be asked for your password — type it and press Enter."

**5. Step 3 – Find Your Network Range**

**Command:**

ip a

"We need to know our network range, called a subnet.  
Type ip a and look for your active network interface — usually eth0 or ens33.  
If your IP is 192.138.24.224, your range is 192.138.24.0/24."

**6. Step 4 – Edit Suricata’s Configuration**

**Command:**

sudo nano /etc/suricata/suricata.yaml

"Now we’ll open Suricata’s main configuration file in a text editor called nano.  
In the terminal, type sudo nano /etc/suricata/suricata.yaml and press Enter.  
Use the arrow keys to move the cursor.  
Find the line that starts with HOME\_NET and change it to match your network range, like this:"

yaml

HOME\_NET: "[192.138.24.0/24]"

"Press **Ctrl + O** to save, then Enter, then **Ctrl + X** to exit."

**7. Step 5 – Add a Custom Rule**

**Command:**

sudo tee /var/lib/suricata/rules/local.rules <<'EOF'

alert icmp any any -> any any (msg:"SURICATA-TEST ICMP detected"; sid:1000001; rev:1;)

EOF

"Now we’ll add a custom rule. This rule will detect ICMP traffic — that’s ping traffic — and log an alert.  
sid is a unique rule number, and rev is the revision number."

**8. Step 6 – Make Sure the Rule is Loaded**

**Command:**

sudo nano /etc/suricata/suricata.yaml

"Open the config file again, scroll to the rule-files section, and make sure it lists local.rules like this:"

yaml

rule-files:

- suricata.rules

- local.rules

"Save and exit with Ctrl + O, Enter, Ctrl + X."

**9. Step 7 – Restart Suricata**

**Command:**

sudo systemctl restart suricata

"Restart Suricata so it loads our changes. If there are no errors, we’re good to go."

**10. Step 8 – Testing from Another Machine**

"Now, when I say *another machine*, I mean a different computer or virtual machine on the same network.  
It could be another VM in VirtualBox or VMware, or a real PC connected to the same router."

**On the attacker machine:**

sudo apt install hping3

sudo hping3 --icmp --flood 192.138.24.224

"Here, we install hping3 and use it to flood our sensor with ping packets. Replace the IP with your Kali sensor’s IP."

**11. Step 9 – Viewing Alerts**

**Command:**

sudo tail -f /var/log/suricata/fast.log

"Back on our Kali sensor, we watch the alert log with tail -f /var/log/suricata/fast.log.  
You’ll see alerts popping up for every detected ping. That means our rule worked!"

**12. Step 10 – Wrap Up**

"And that’s it! You’ve set up a Suricata-based NIDS, added a custom detection rule, and tested it from another machine.  
Remember: never run attack tools on public networks — always use a safe lab."