# Network Intrusion Detection System (NIDS) Setup Report

## 1. Set Up a Network-Based Intrusion Detection System

Tool Used: Snort

Platform: Linux (Ubuntu)

Installation Command:

sudo apt update

sudo apt install snort -y

Configure network interface (e.g., eth0) and home network (e.g., 192.168.1.0/24)

## 2. Configure Rules and Alerts

Snort Rule Example (Detect ICMP Ping):

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

Save in: /etc/snort/rules/local.rules

Ensure 'include $RULE_PATH/local.rules' is active in snort.conf

## 3. Monitor Network Traffic for Potential Threats

Run Snort in IDS mode:

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

Check alerts at: /var/log/snort/alert

## 4. Implement Response Mechanisms

Tools:

- fail2ban: blocks IPs based on logs
- iptables: manual blocking
- Custom scripts

Example Email Alert Script:

```
tail -n0 -F /var/log/snort/alert | while read line; do
  echo "Alert: $line" | mail -s "Snort Alert" you@example.com
done
```

### 5. Visualize Detected Attacks (Optional)

Visualization Tools:

- Snorby, BASE, Kibana + Elasticsearch + Logstash
- Python with Matplotlib or Google Sheets for basic charts

Example Table:

| Date | Attack Type | Count |
|---|---|---|
| 2025-06-19 | ICMP Ping | 12 |
| 2025-06-19 | Port Scan | 5 |

### Summary Table

| Step | Description |
|---|---|
| 1 | Installed and configured Snort |
| 2 | Wrote custom rules and loaded them |
| 3 | Monitored real-time alerts |
| 4 | Suggested response scripts and tools |
| 5 | Explained optional visualization tools |