Project Report: Network Intrusion Detection System (NIDS)

Objective

To deploy and configure a Network-Based Intrusion Detection System (NIDS) that detects and alerts on malicious or suspicious activities on a network using Snort or Suricata.

Tools & Technologies Used

- Operating System: Ubuntu 20.04 LTS
- IDS Tool: Snort 3 / Suricata
- Visualization: ELK Stack (Elasticsearch, Logstash, Kibana)
- Scripting: Bash
- Firewall: UFW / iptables

Implementation Steps

1. Installation of IDS Tool (Snort or Suricata)
Command:
```
sudo apt update
sudo apt install snort  # or suricata
```
Interface set in promiscuous mode: ifconfig eth0 promisc

2. Configuration of Rules and Alerts
Example Snort Rule:
```
alert tcp any any -> any 80 (msg:"Possible Web Attack"; sid:1000001; rev:1;)
```
File: /etc/snort/rules/local.rules
Enabled in snort.conf or suricata.yaml

3. Monitoring Network Traffic
Command to start:
```
sudo snort -A console -q -c /etc/snort/snort.conf -i eth0
```
Output: Logs to /var/log/snort/alert

4. Intrusion Response
Auto-blocking with firewall:
```
sudo iptables -A INPUT -s <suspicious_IP> -j DROP
```
Alert forwarding: Configured to send email/syslog messages

5. Visualization Dashboard (Optional)
Installed ELK Stack:
```
sudo apt install elasticsearch logstash kibana
```
Snort logs piped to Logstash and visualized on Kibana

Sample Configuration Files

Project Report: Network Intrusion Detection System (NIDS)

Snort Config Snippet (snort.conf):

```
include $RULE_PATH/local.rules
output alert_fast: alert.fast
var HOME_NET [192.168.1.0/24]
```

Suricata Config Snippet (suricata.yaml):

```
rule-files:
  - local.rules
outputs:
  - fast:
      enabled: yes
      filename: fast.log
```

Results and Conclusion

- NIDS was successfully deployed and configured.
- System identified and alerted on test intrusion scenarios (e.g., port scan using nmap).
- Response mechanisms blocked intrusions in real-time.
- Optional visualization provided clear insights into network behavior.

Future Enhancements

- Integration with real-time threat intelligence feeds.
- Email/SMS alerts for critical threats.
- Scheduled log/report generation.

Folder Structure to Submit

```
NIDS_Project/
??? Report.pdf
??? config/
?   ??? snort.conf
?   ??? local.rules
?   ??? suricata.yaml
??? screenshots/
?   ??? snort_console.png
?   ??? alert_log.png
?   ??? rules_file.png
?   ??? kibana_dashboard.png
??? logs/
    ??? sample_alerts.log
```