Network Intrusion Detection System (NIDS) Using Snort

A Project on Intrusion Detection with Snort

By Syed Mujtaba Ahmed

Introduction

- A Network Intrusion Detection System (NIDS) monitors network traffic to detect suspicious activity.
- Snort is an open-source IDS that inspects network packets and generates alerts for malicious activities.

Tools & Technologies Used

- – Operating System: Ubuntu/Kali Linux
- – IDS Tool: Snort
- – Additional Tools: Wireshark, Nmap, Hping3
- – Visualization: ELK Stack (Elasticsearch, Logstash, Kibana)

Snort Installation & Configuration

- 1. Install Snort:
- sudo apt update && sudo apt install snort -y

- 2. Verify Installation:
- snort -V

- 3. Configure Rules:
- sudo nano /etc/snort/rules/local.rules

Example Snort Rule

- Detect ICMP Ping Scans:
- alert icmp any any -> any any (msg:"ICMP Packet Detected"; sid:1000001;)

Running Snort in IDS Mode

- Use the following command to start Snort in detection mode:

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

Testing & Generating Alerts

- 1. Nmap SYN Scan:
- nmap -sS -p 22 <your-IP>

- 2. Hping3 SYN Flood Attack:
- hping3 -S -p 80 --flood <your-IP>

- Snort should log these activities and trigger alerts.

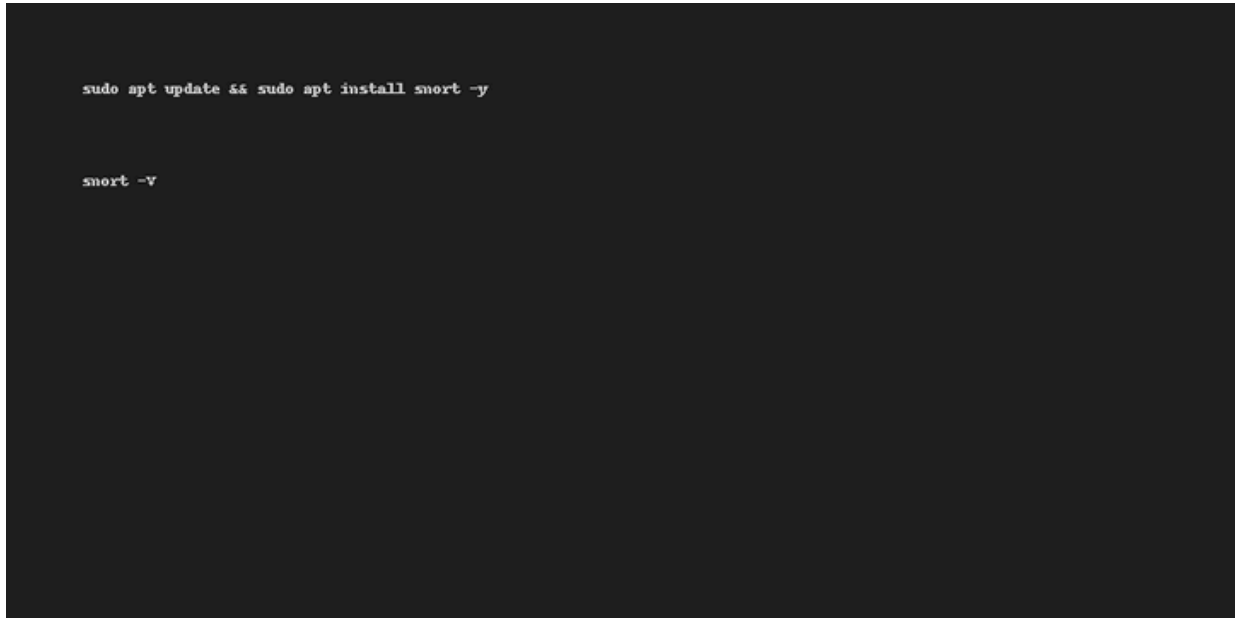
Visualizing Alerts with ELK

- 1. Store logs in Elasticsearch
- 2. Parse logs using Logstash
- 3. Use Kibana for real-time visualization of Snort alerts.

Conclusion & Future Scope

- • Successfully detected and logged network attacks using Snort.
- • Future Enhancements:
- – Automate response actions.
- – Integrate with SIEM tools like Splunk for better analysis.

Snort Installation Output



Snort Rule Configuration

Running Snort in IDS Mode

Testing Network Attacks