**Snort Installation and Configuration Lab**

****

**Author:** Taha Zaheer  
**Platform:** Parrot OS (for Snort configuration) and Kali Linux (for attack simulation)  
**Tool Used:** **Snort, Scapy, Snorpy**, Hping3

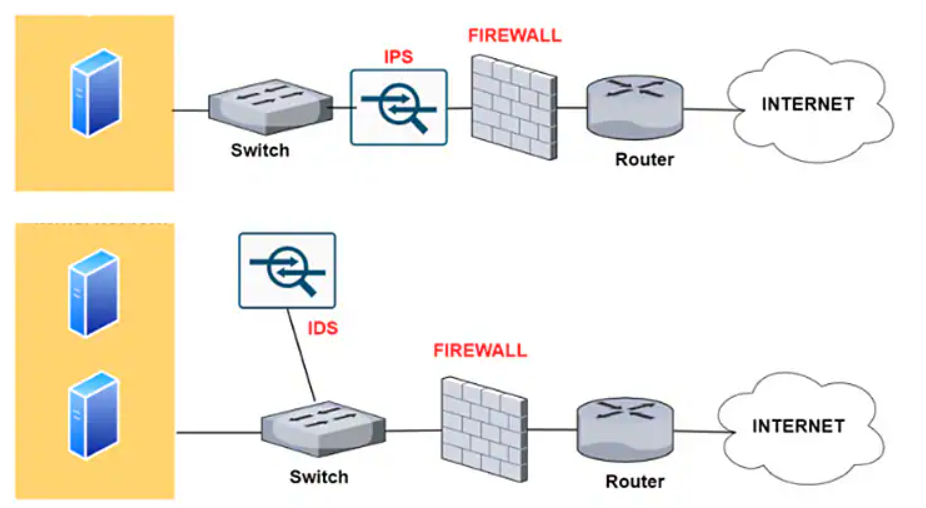
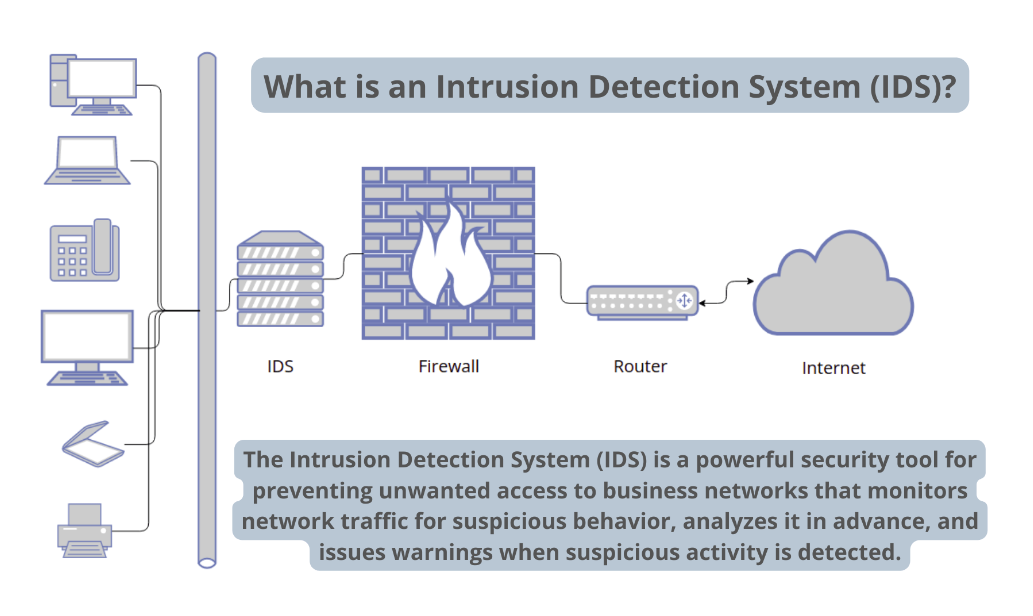
**Purpose:** To demonstrate the installation, configuration, and testing of **Snort** as an Intrusion Detection and Prevention System (IDS/IPS), and verify its detection capabilities using ICMP and SYN flood attacks.

**Objective**

The objective of this lab is to install and configure **Snort**, an open-source Intrusion Detection System, to monitor and analyze network traffic. The lab further demonstrates how Snort can detect different types of attacks based on predefined or custom rules, such as ICMP packet monitoring and SYN flood attacks.

**1. Understanding IDS and IPS**

* **Intrusion Detection System (IDS):**  
  An IDS monitors network traffic or system activities to detect unauthorized access, malicious activity, or policy violations. It operates passively by alerting the administrator upon detection of suspicious events.
* **Intrusion Prevention System (IPS):**  
  An IPS is an advanced form of IDS that not only detects but also blocks or mitigates threats in real time. It operates **inline** within the network flow, actively responding to malicious packets.



**Comparison Summary:**

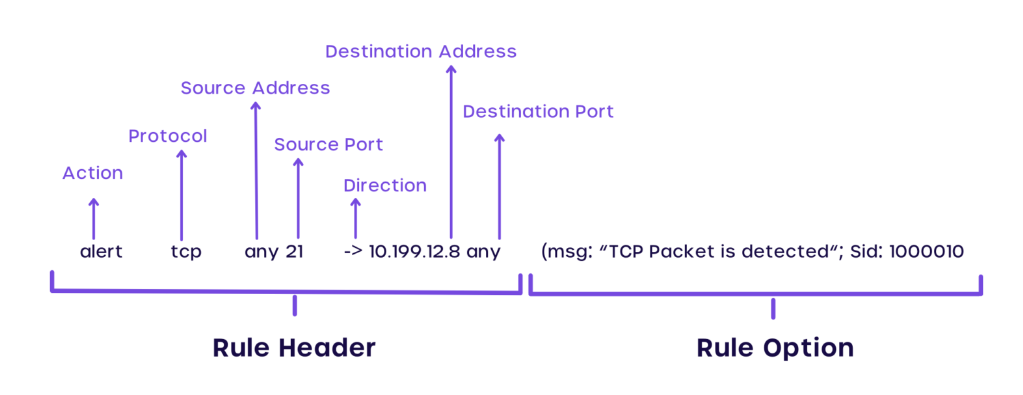
| **Aspect** | **IDS** | **IPS** |
| --- | --- | --- |
| Function | Detects and alerts | Detects and blocks |
| Mode | Passive | Active (Inline) |
| Action | No prevention | Can prevent attacks |

**2. Introduction to Snort**

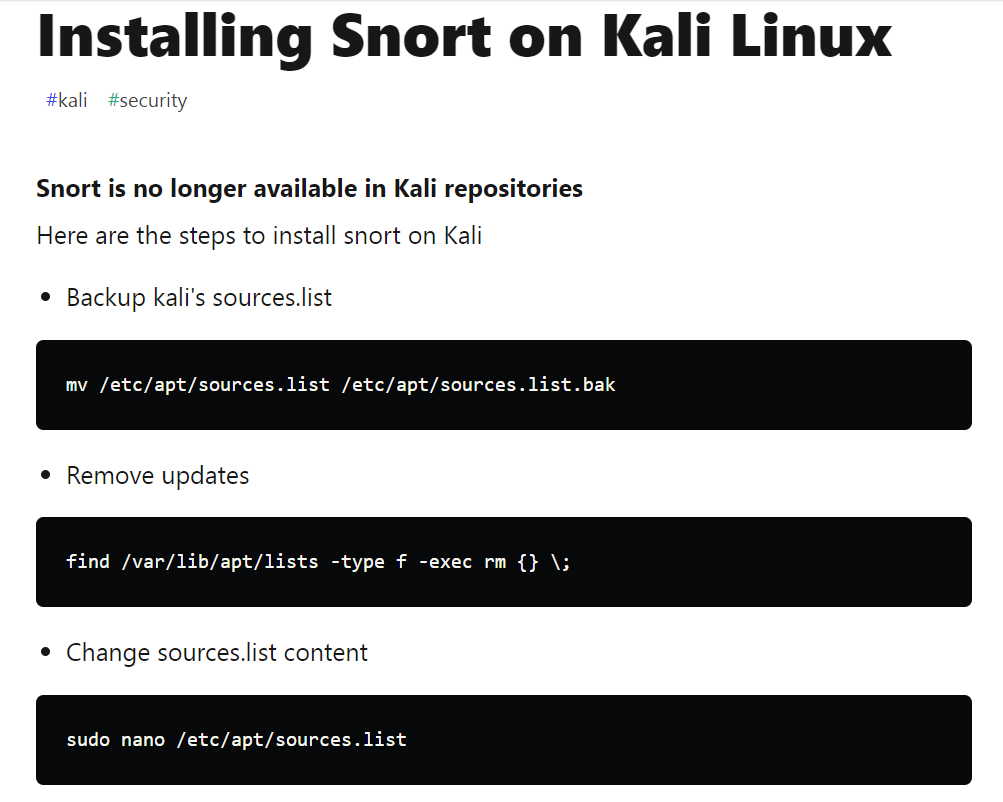
**Snort** is an open-source **Network Intrusion Detection and Prevention System (NIDS/NIPS)** developed by **Martin Roesch (1998)** and maintained by **Cisco**. It uses a **rule-based detection engine** to identify malicious network traffic.

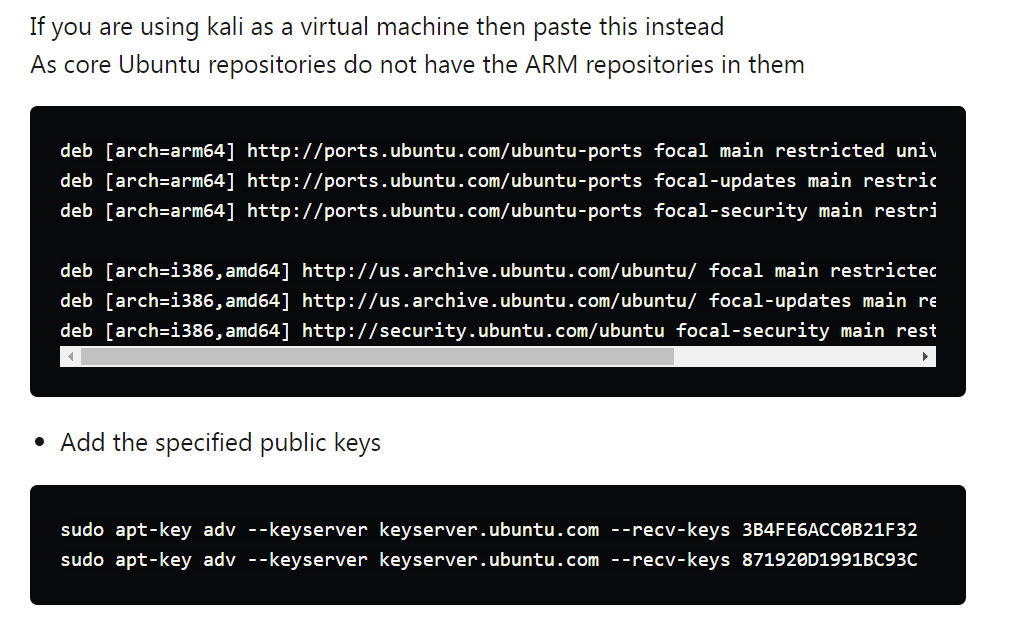
**Modes of Operation:**

1. **Sniffer Mode:** Displays network packets on the console in real time.
2. **Packet Logger Mode:** Logs packets to disk for analysis.
3. **Network IDS/IPS Mode:** Monitors and analyzes packets based on rules to detect and prevent intrusions.

****

**3. Snort Installation**

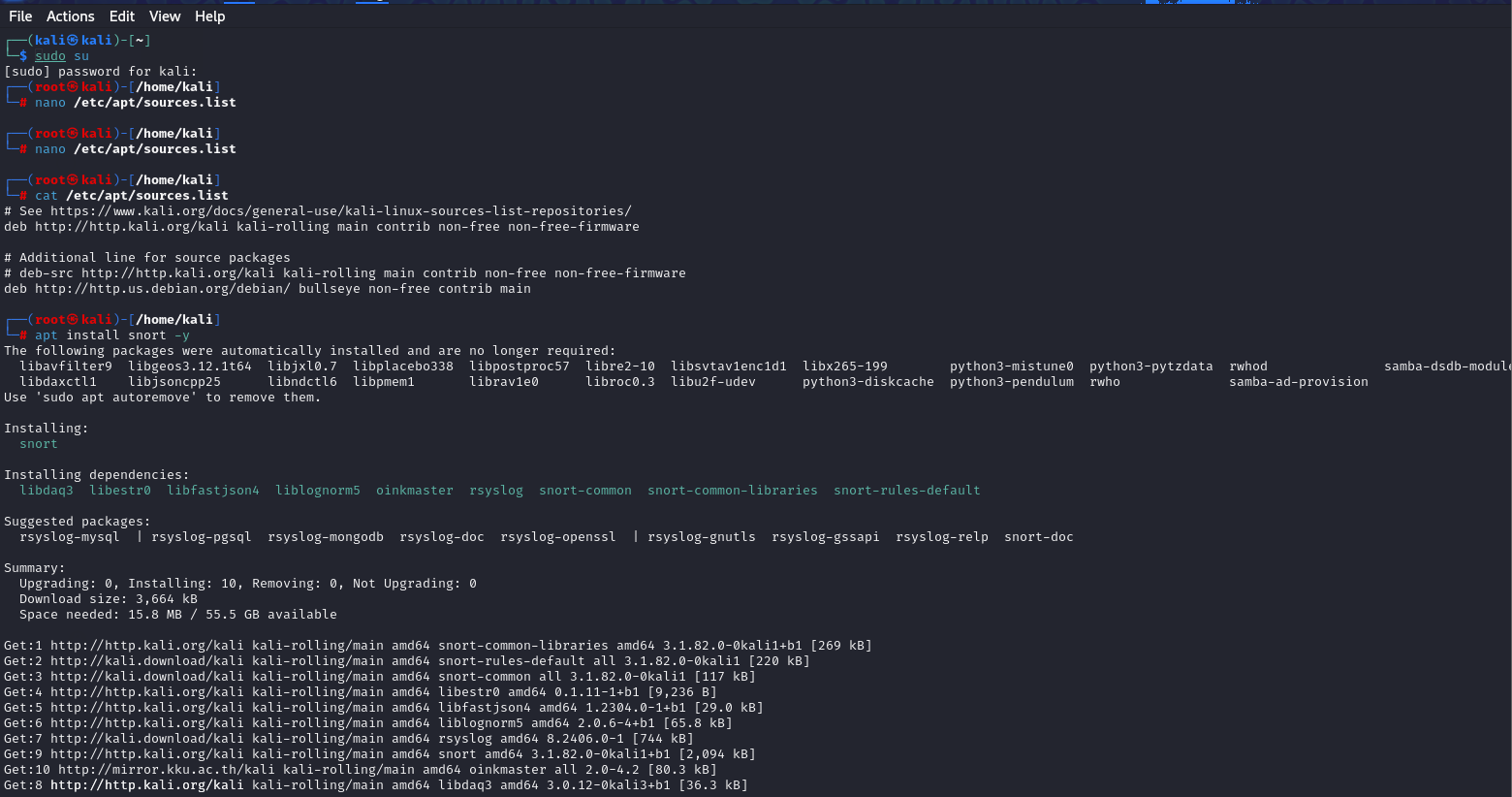






Verify installation:

snort --version



**4. Configuring Snort**

**Step 2: Edit the Configuration File**

Open the Snort configuration file:

sudo nano /etc/snort/snort.conf

Set the home network variable:

ipvar HOME\_NET 150.1.7.0/24

Define log directory:

config logdir: /var/log/snort

**5. Creating and Managing Snort Rules**

Navigate to the rules directory:

cd /etc/snort/rules

Create a new ICMP rule file:

sudo nano icmp.rules

Add a custom detection rule for ICMP packets:

alert icmp any any -> 150.1.7.0/24 (msg:"ICMP Packet Found"; sid:10000001;)

Save and exit.

**6. Running Snort**

Run Snort in console mode to monitor ICMP packets in real time:

sudo snort -A console -q -u snort -g snort -c /etc/snort/snort.conf -i ens34

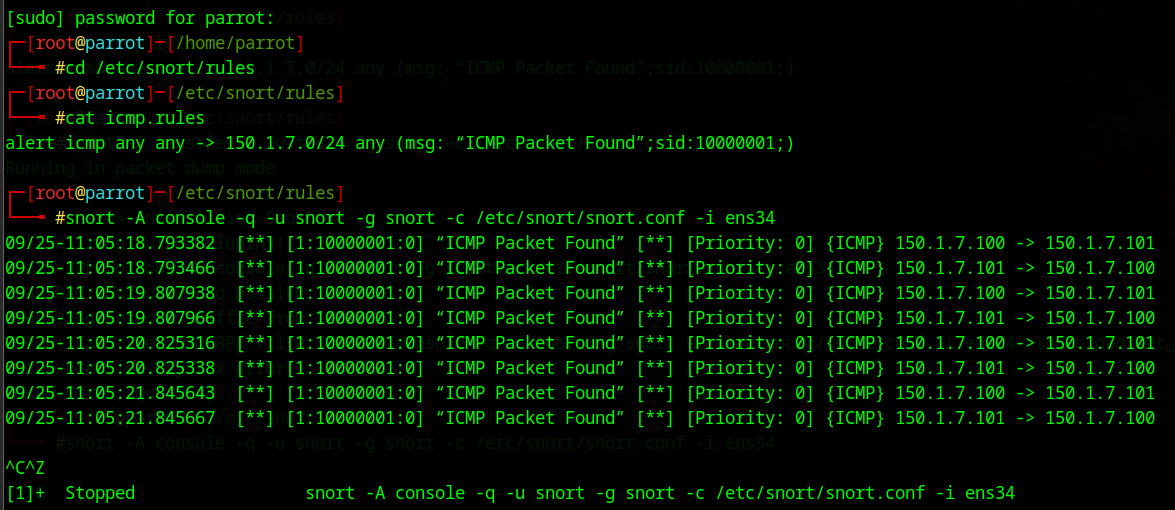
From another machine, send ICMP requests:

ping -n 2 150.1.7.104

**7. Testing Snort with Attack Simulations**

**A. ICMP Attack Detection**

Snort successfully detected ICMP packets sent to the configured HOME\_NET and displayed alerts in the console with the message “ICMP Packet Found.”

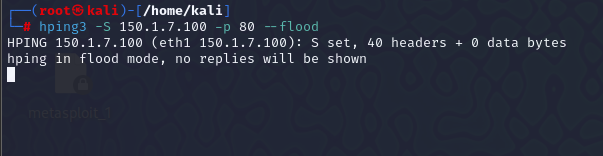


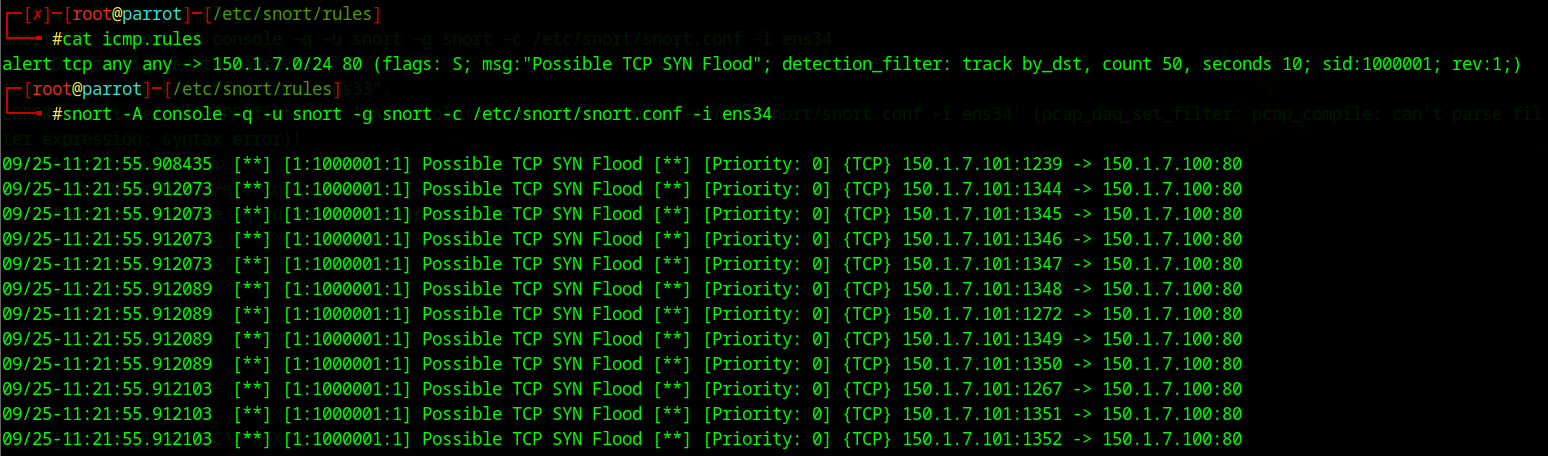
**B. SYN Flood Attack Using hping3**

Simulate a SYN Flood attack using the hping3 tool from Kali Linux:

sudo hping3 -S --flood -V -p 22 150.1.7.104

Snort detects the flood of SYN packets based on its internal or user-defined rules and raises alerts for potential denial-of-service activity.

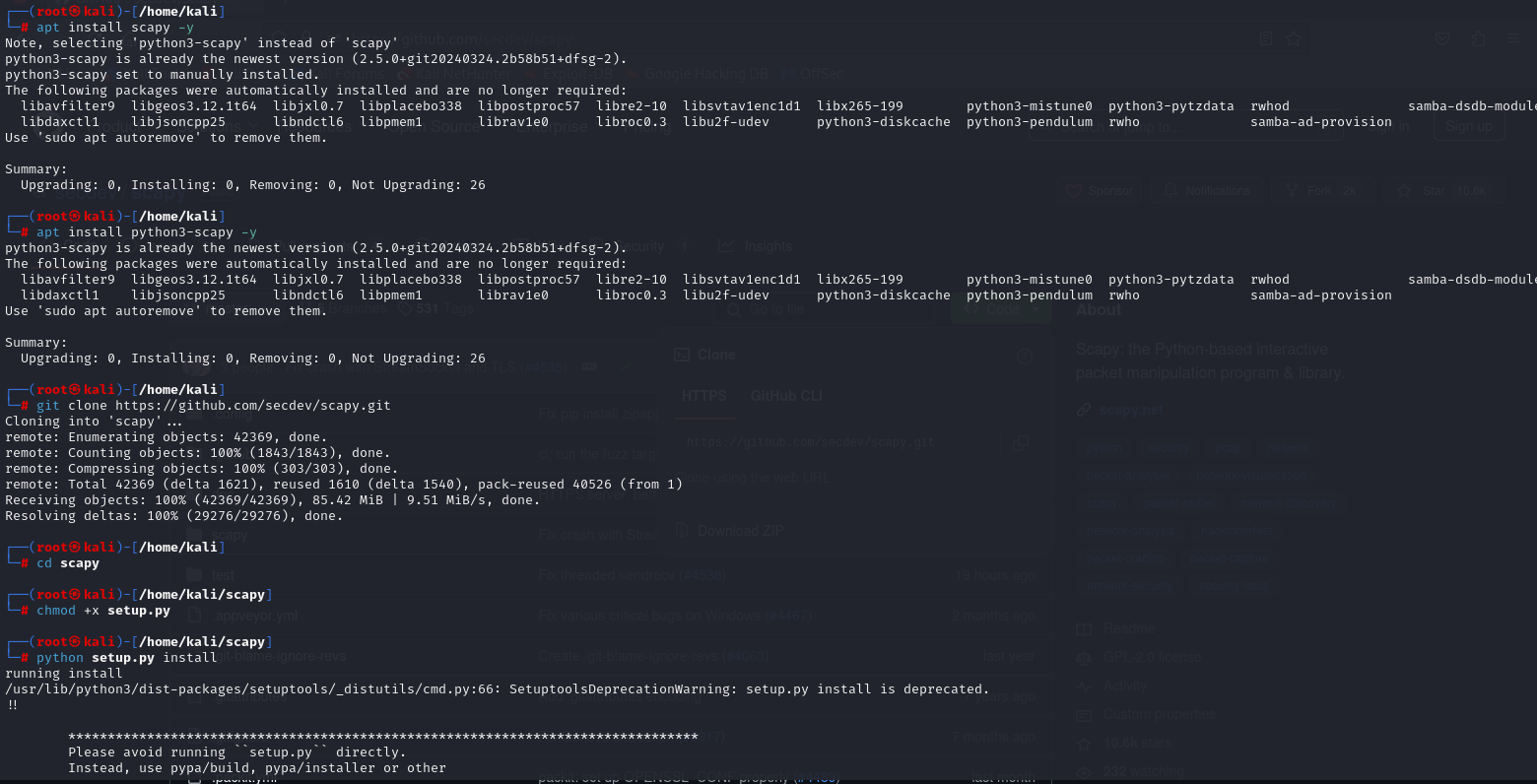


****

**C. SYN Flood Attack Using Scapy**

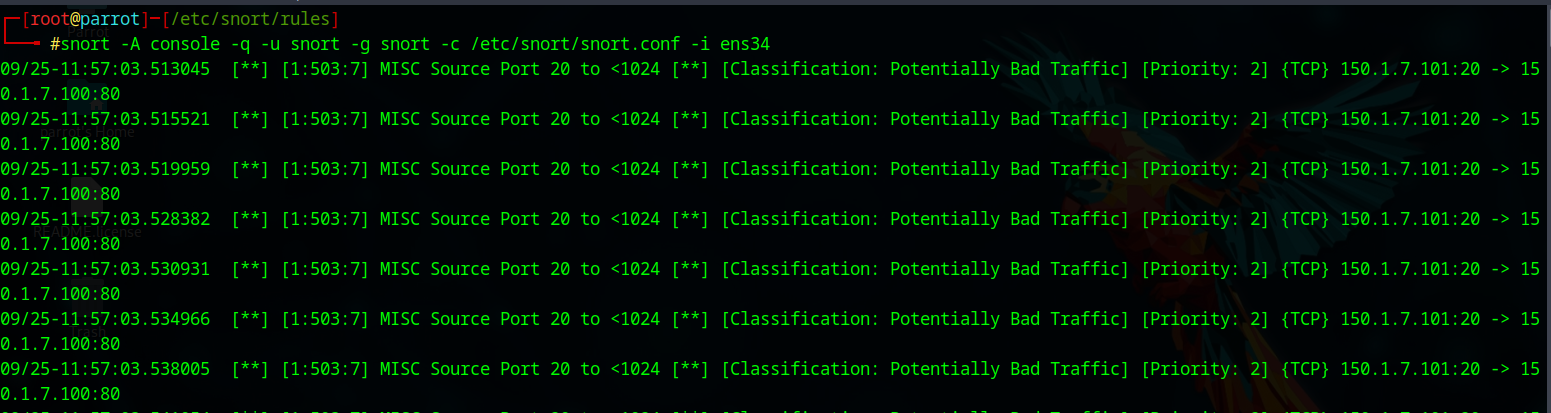
Install Scapy for packet crafting:

sudo apt install python3-scapy

****

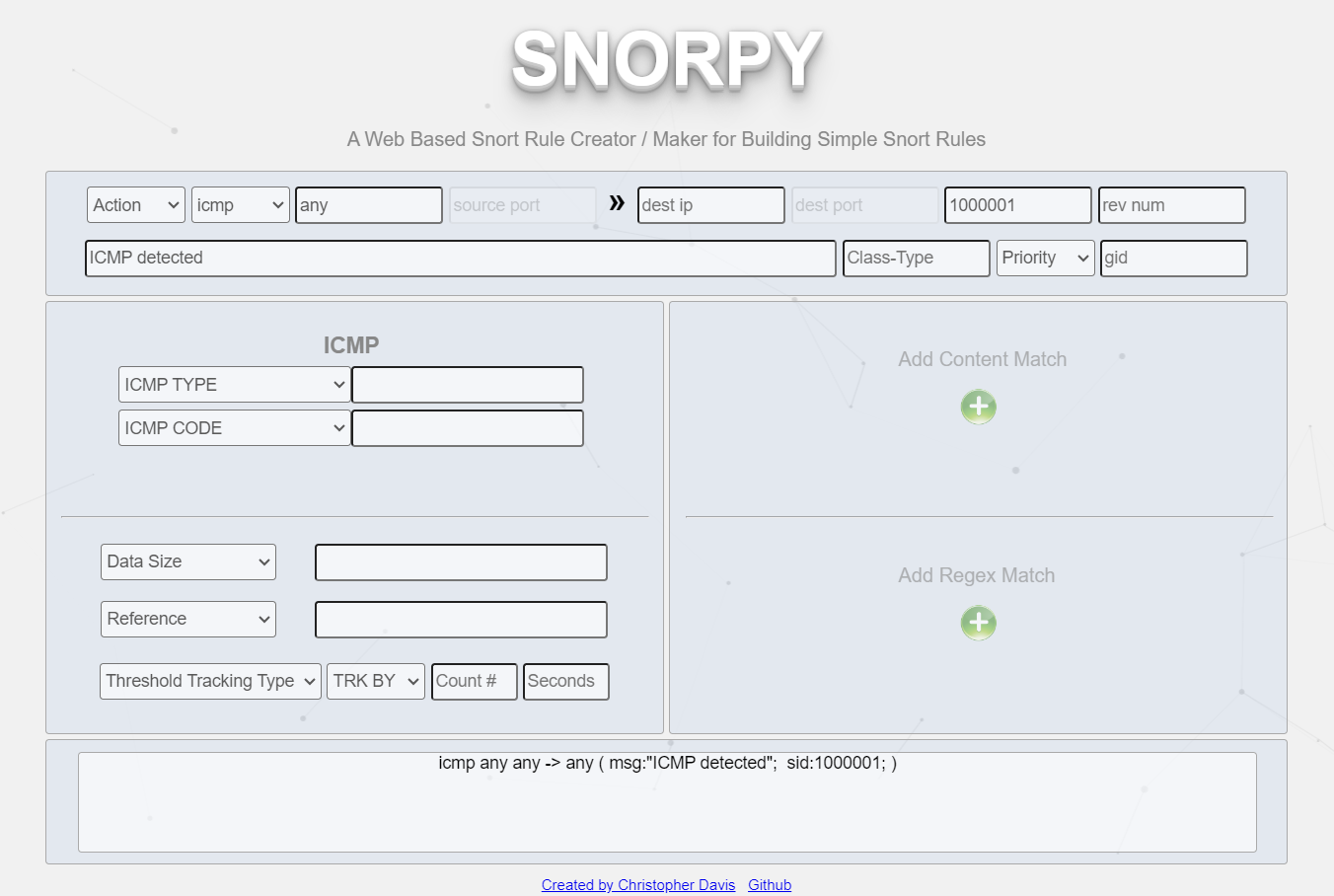
Then execute a SYN flood attack script (example from Scapy documentation) to verify Snort’s response.

****

****

**8. Using Snorpy for Rule Generation**

To simplify custom rule creation, **Snorpy**, a web-based Snort rule generator, can be used. It provides a GUI interface for defining conditions and outputs a properly formatted Snort rule.



**Conclusion**

This lab demonstrates the **complete installation, configuration, and testing of Snort IDS/IPS**.  
Snort was able to detect ICMP and SYN flood attacks successfully, validating its capability as a robust, open-source intrusion detection solution.