ATTACKS_DETECTED IN SNORT

DOS ATTACK: DoS Attack Detection using Snort

What is Dos attack?

A Denial of Service (DoS) attack is a cyberattack where an attacker floods a network, server, or website with excessive traffic or malicious requests, making it unavailable to legitimate users.

Types of DoS Attacks

1)Volume-Based Attacks (Flood Attacks)

- Overload bandwidth with massive traffic.
- **Examples:**
    - **ICMP Flood** (Ping Flood)
    - **UDP Flood**
    - **SYN Flood**

2)Protocol Attacks

- Exploit vulnerabilities in network protocols.
- **Examples:**
    - **SYN Flood** (Exploits TCP handshake)
    - **Smurf Attack** (Amplifies ICMP traffic)

3)Application-Layer Attacks

- Target specific applications like HTTP, DNS.
- **Examples:**
    - **Slowloris Attack** (Keeps connections open)
    - **HTTP Flood** (Massive fake web requests)

How to Prevent DoS Attacks?

1) Firewall & Rate Limiting (Limit traffic requests)
2)intrusion Detection Systems (IDS/IPS) (e.g., Snort, Suricata)
3)Load Balancers (Distribute traffic evenly.

DoS Attack in Kali Linux with Alert Trigger in Ubuntu

Step-by-Step Process:

Step 1: Set Up the Lab Environment

1. Install **Kali Linux** and **Ubuntu** as virtual machines or on separate systems.
2. Ensure both machines are on the same network (e.g., same Wi-Fi or VirtualBox/VMware bridged adapter).

Step 2: Install DoS Attack Tool in Kali Linux

Using hping3

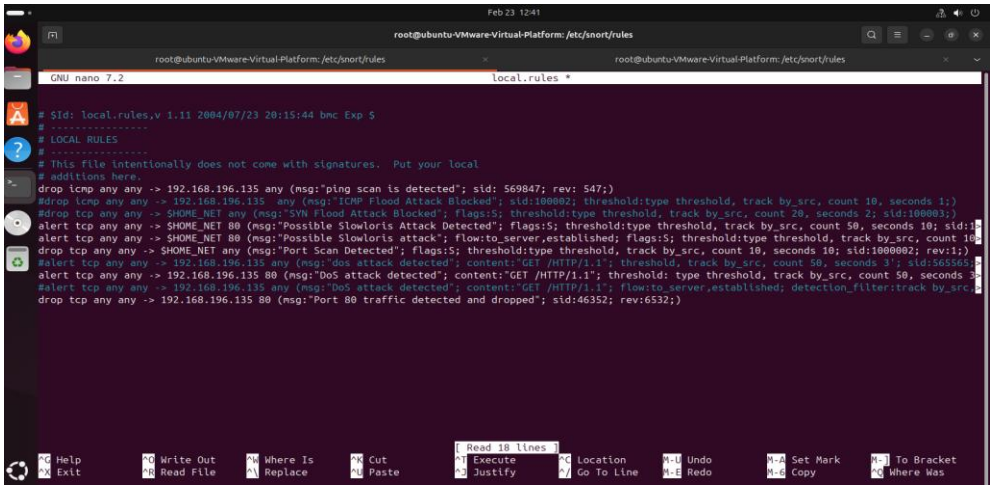
1. Install Hping3

2. Command:**sudo apt install hping3**

Step 3: Locate and Edit local.rules

Command : sudo nano /etc/snort/rules/local.rules

Rule : alert tcp any any -> 192.168.196.135 80 (flags:S; msg:"DOS ATTACK DETECTED”; threshold:type threshold, track by_src, count 50, seconds 10; sid:1000001; rev:1;)



Step 4 : Run Snort in live monitoring mode:

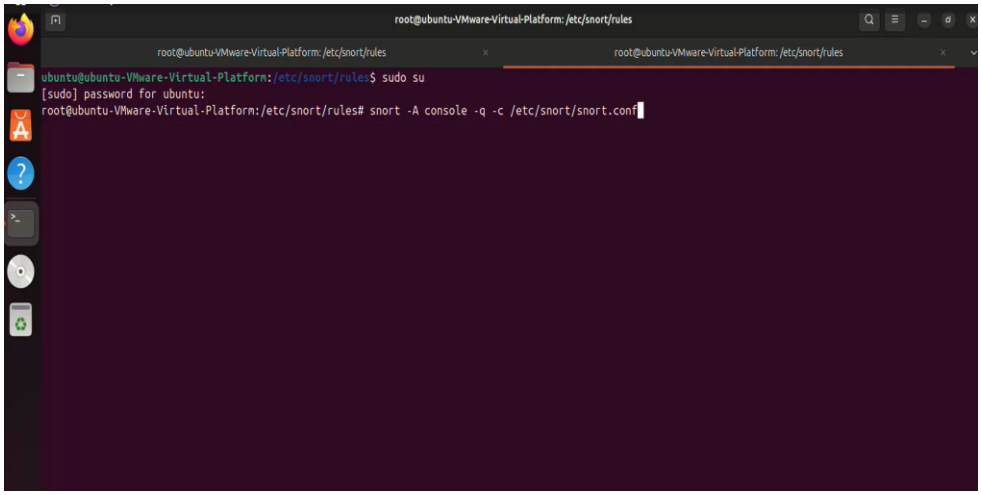
Once you have configured your **Snort rules** (including local.rules), you need to start Snort in **listening mode** to detect attacks and generate alerts.

Command : sudo snort -A console -q -c /etc/snort/snort.conf

· -A console → Shows alerts in the terminal.

· -q → Runs in quiet mode (hides unnecessary messages).

· -c /etc/snort/snort.conf → Loads Snort configuration.



Step 5 : DoS Attack Using hping3 in Kali Linux

In Kali Linux, you can use **hping3** to perform a **SYN flood attack** or other types of DoS attacks on the target Ubuntu machine.

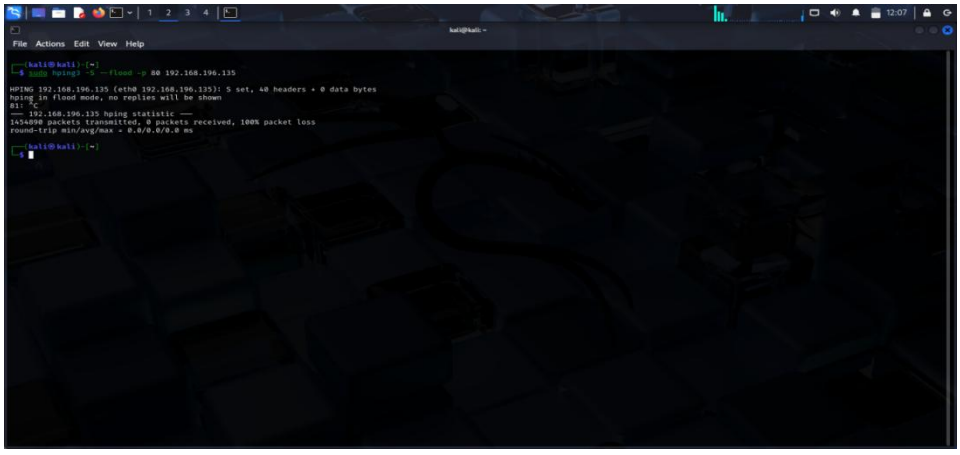
.Run **hping3** to Perform a DoS Attack

Command : sudo hping3 -S --flood -p 80 192.168.196.135

· -S → Sends SYN packets.

· --flood → Sends packets as fast as possible.

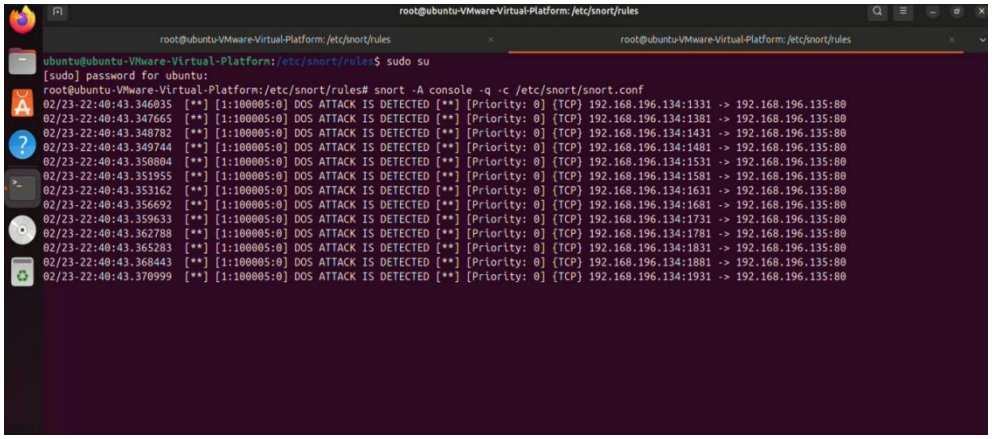
· -p 80 → Targets **port 80**

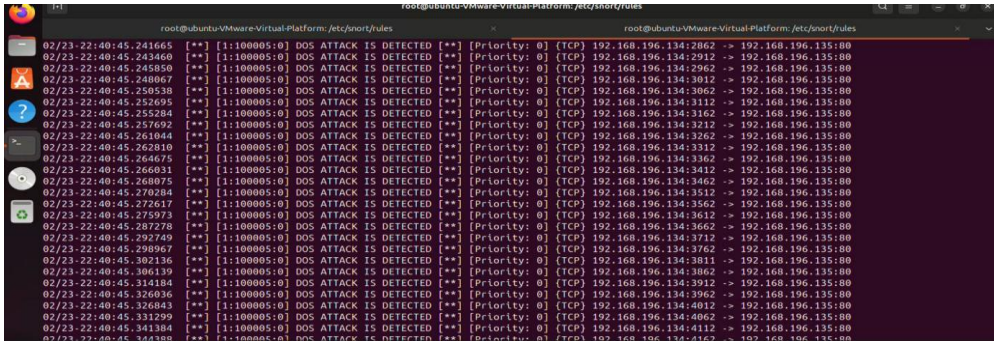


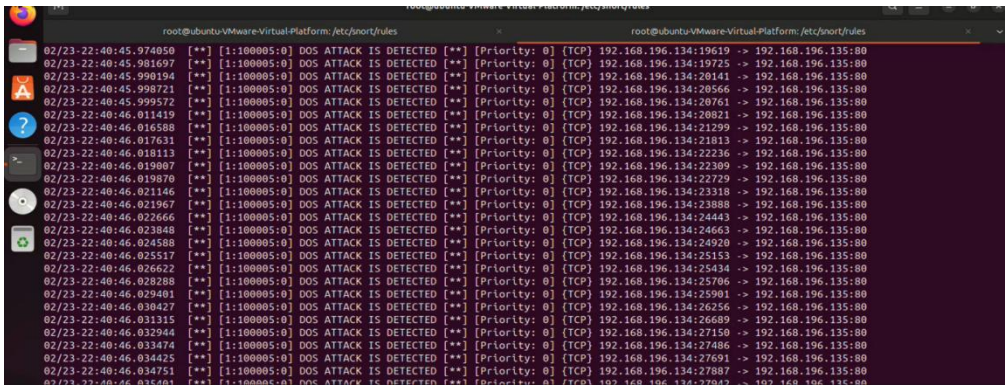
Step 6 : Start the Attack and Generate Alerts on Ubuntu

Now that both **Kali Linux (attacker)** and **Ubuntu (target with Snort IDS)** are set up, it's time to **start the attack and check for alerts on Ubuntu.**

Command : sudo snort -A console -q -c /etc/snort/snort.conf







Now that the **DoS attack from Kali Linux** has been successfully launched, your **Ubuntu machine has detected it** using **Snort IDS**

Step 7 : Stop the Attack and Analyze the Logs

Stop the attack on Kali Linux : **CTRL + C**

Check the logs on Ubuntu to analyze the attack patterns

Apply firewall rules using iptables to block malicious traffic:

Command : sudo iptables -A INPUT -s 192.168.196.135 -j DROP

Brute-Force Attack : Brute-Force Attack Detection using Snort

What is Brute-Force Attack?

A **Brute-Force Attack** is a method where an attacker systematically tries multiple passwords, usernames, or encryption keys to gain unauthorized access to a system, account, or service. It relies on the idea of **"guessing" credentials** until the correct combination is found.

Types of Brute-Force Attacks:

1)Simple Brute-Force – Tries every possible password **without any logic** (e.g., aaa, aab, aac...).

2)Dictionary Attack – Uses a **predefined list** of common passwords (e.g., password123, admin, qwerty).

3)Hybrid Attack – Combines dictionary words with variations (e.g., P@ssw0rd, Admin2024!).

4)Reverse Brute-Force – The attacker starts with a common password and **tests it against multiple usernames**.

5)Credential Stuffing – Uses **leaked username-password combos** from data breaches to log into other accounts.

How to Prevent Brute-Force Attacks

Use Strong Passwords (mix of uppercase, lowercase, numbers, symbols).
Enable Account Lockout (after 3-5 failed attempts).
Use Two-Factor Authentication (2FA) for extra security.
Limit Login Attempts using iptables.
Use Captchas to stop automated bots.
Monitor Logs for repeated failed login attempts.

Step-by-Step Process:

Step 1: Set Up the Lab Environment

3. Install **Kali Linux** and **Ubuntu** as virtual machines or on separate systems.
4. Ensure both machines are on the same network (e.g., same Wi-Fi or VirtualBox/VMware bridged adapter).

Step 2: Install brute-froce Attack Tool in Kali Linux

Using hydra

3. Install hydra

4. Command:**sudo apt install hydra**

Step 3: Locate and Edit local.rules

Command : sudo nano /etc/snort/rules/local.rules

Rule : alert tcp any any -> 192.168.196.135 any (msg:"BRUTE-FORCE ATTACK DETECTED"; flags:S; threshold:type threshold, track by_src, count 5, seconds 10; sid:1000002; rev:1;)

Step 4 : Run Snort in live monitoring mode:

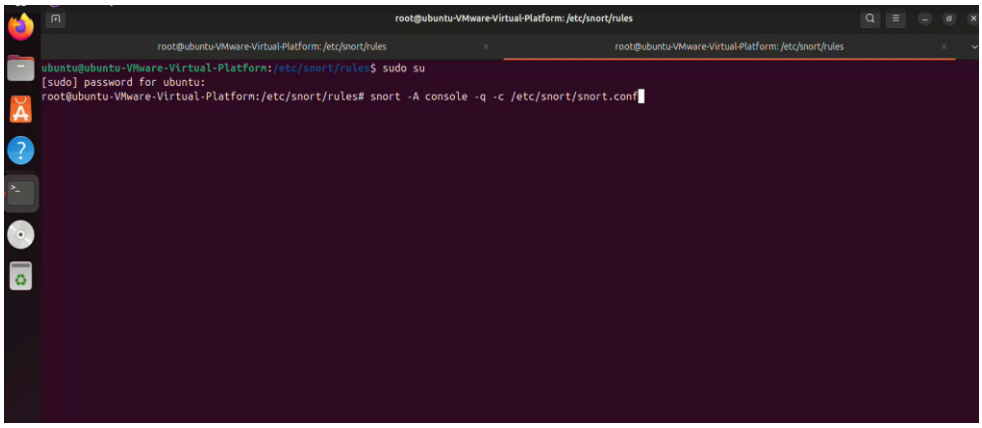
Once you have configured your **Snort rules** (including local.rules), you need to start Snort in **listening mode** to detect attacks and generate alerts.

Command : sudo snort -A console -q -c /etc/snort/snort.conf

· -A console → Shows alerts in the terminal.

· -q → Runs in quiet mode (hides unnecessary messages).

· -c /etc/snort/snort.conf → Loads Snort configuration.



Step 5: Brute-Force Attack Using Hydra in Kali Linux

In Kali Linux, you can use **Hydra** to perform a **Brute-Force Attack** on the **SSH service (port 22)** of the target Ubuntu machine

Command : sudo hydra -l root -P /usr/share/wordlists/rockyou.txt 192.168.196.135 ssh

· -l root → Tries **root** as the username.

· -P /usr/share/wordlists/rockyou.txt → Uses **RockYou** password list.

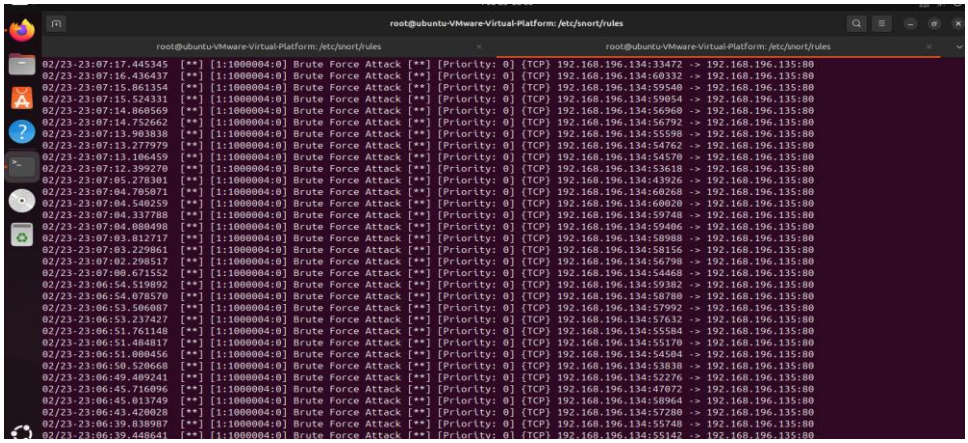
· 192.168.196.135 → Target Ubuntu machine's **IP address**.

· ssh → Specifies that **SSH login (port 22)** is being attacked.

Step 6 : Start the Attack and Generate Alerts on Ubuntu

Now that both **Kali Linux (attacker)** and **Ubuntu (target with Snort IDS)** are set up, it's time to **start the attack and check for alerts on Ubuntu.**

Command : sudo snort -A console -q -c /etc/snort/snort.conf



Now that the brute-froce **attack from Kali Linux** has been successfully launched, your **Ubuntu machine has detected it** using **Snort IDS.**

Step 7 : Stop the Attack and Analyze the Logs

Stop the attack on Kali Linux : **CTRL + C**

Check the logs on Ubuntu to analyze the attack patterns

Apply firewall rules using iptables to block malicious traffic:

Command : sudo iptables -A INPUT -s 192.168.196.135 -j DROP.