

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

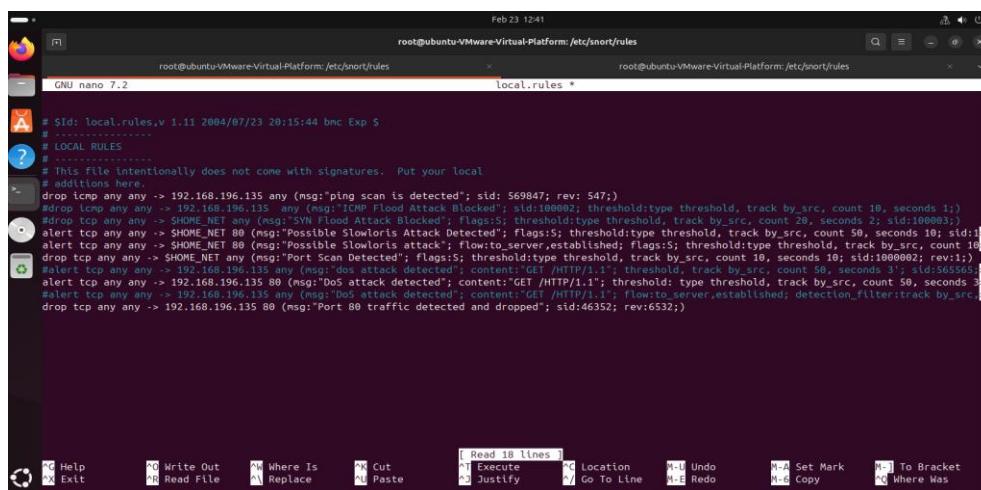
Using hping3

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;)`



```
# Std: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $  
# .....  
# LOCAL RULES  
# .....  
# This file intentionally does not come with signatures. Put your local  
# additions here.  
#drop icmp any any -> 192.168.196.135 any (msg:"ping scan is detected"; sid:569847; rev: 547;)  
#drop icmp any any -> 192.168.196.135 any (msg:"ICMP Flood Attack Blocked"; sid:1000002; threshold:type threshold, track by_src, count 10, seconds 1;)  
#drop tcp any any -> SHOME_NET any (msg:"SYN Flood Attack Blocked"; flags:S; threshold:type threshold, track by_src, count 20, seconds 2; sid:1000003;)  
alert tcp any any -> SHOME_NET 80 (msg:"Possible Slowloris Attack Detected"; flags:S; threshold:type threshold, track by_src, count 50, seconds 10; sid:1000004; rev:1;)  
alert tcp any any -> SHOME_NET 80 (msg:"Possible Slowloris attack"; flowto_server,established; flags:S; threshold:type threshold, track by_src, count 10;)  
drop tcp any any -> SHOME_NET any (msg:"Port Scan Detected"; flags:S; threshold:type threshold, track by_src, count 10, seconds 10; sid:1000005; rev:1;)  
#alert tcp any any -> 192.168.196.135 any (msg:"dos attack detected"; content:"GET /HTTP/1.1"; threshold, track by_src, count 50, seconds 3; sid:565565; rev:1;)  
#alert tcp any any -> 192.168.196.135 80 (msg:"DoS attack detected"; content:"GET /HTTP/1.1"; threshold: type threshold, track by_src, count 50, seconds 3; sid:565565; rev:1;)  
#alert tcp any any -> 192.168.196.135 any (msg:"DOS attack detected"; content:"GET /HTTP/1.1"; flowto_server,established; detection_filter:track by_src, count 50, seconds 3; sid:46352; rev:652;)  
drop tcp any any -> 192.168.196.135 80 (msg:"Port 80 traffic detected and dropped"; sid:46352; rev:652;)
```

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.

The screenshot shows two terminal windows side-by-side. Both windows have the title 'root@ubuntu-VMware-Virtual-Platform:/etc/snort/rules'. The left window contains the command 'sudo su' followed by a password prompt. The right window contains the command 'snort -A console -q -c /etc/snort/snort.conf'. The terminal interface includes a dark background with light-colored text, standard Linux file icons in the top bar, and a vertical dock on the left.

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**

The screenshot shows a terminal window with a dark background. The command 'sudo hping3 -S --flood -p 80 192.168.196.135' is entered and executed. The output shows the attack parameters and statistics: 'HPING 192.168.196.135 (eth0 192.168.196.135) 5 set, 40 headers + 0 data bytes', 'Host is up (0.000000ms latency)', '1654008 packets transmitted, 0 packets received, 100% packet loss', and 'round-trip min/avg/max = 0.0/0.0/0.0 ms'. The terminal interface includes a dark background with light-colored text, standard Linux file icons in the top bar, and a vertical dock on the left.

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

```

root@ubuntu:~/Desktop$ sudo su
[sudo] password for ubuntu:
root@ubuntu:~/Desktop$ /etc/snort/rules# snort -A console -q -c /etc/snort/snort.conf
02/23/22:40:43.346035 [**] [1:100005:0] DOS ATTACK IS DETECTED [**] [Priority: 0] [TCP] 192.168.196.134:1331 -> 192.168.196.135:80
02/23/22:40:43.347665 [**] [1:100005:0] DOS ATTACK IS DETECTED [**] [Priority: 0] [TCP] 192.168.196.134:1381 -> 192.168.196.135:80
02/23/22:40:43.348782 [**] [1:100005:0] DOS ATTACK IS DETECTED [**] [Priority: 0] [TCP] 192.168.196.134:1431 -> 192.168.196.135:80
02/23/22:40:43.349744 [**] [1:100005:0] DOS ATTACK IS DETECTED [**] [Priority: 0] [TCP] 192.168.196.134:1481 -> 192.168.196.135:80
02/23/22:40:43.350804 [**] [1:100005:0] DOS ATTACK IS DETECTED [**] [Priority: 0] [TCP] 192.168.196.134:1531 -> 192.168.196.135:80
02/23/22:40:43.351955 [**] [1:100005:0] DOS ATTACK IS DETECTED [**] [Priority: 0] [TCP] 192.168.196.134:1581 -> 192.168.196.135:80
02/23/22:40:43.353162 [**] [1:100005:0] DOS ATTACK IS DETECTED [**] [Priority: 0] [TCP] 192.168.196.134:1631 -> 192.168.196.135:80
02/23/22:40:43.356692 [**] [1:100005:0] DOS ATTACK IS DETECTED [**] [Priority: 0] [TCP] 192.168.196.134:1681 -> 192.168.196.135:80
02/23/22:40:43.359633 [**] [1:100005:0] DOS ATTACK IS DETECTED [**] [Priority: 0] [TCP] 192.168.196.134:1731 -> 192.168.196.135:80
02/23/22:40:43.362788 [**] [1:100005:0] DOS ATTACK IS DETECTED [**] [Priority: 0] [TCP] 192.168.196.134:1781 -> 192.168.196.135:80
02/23/22:40:43.365283 [**] [1:100005:0] DOS ATTACK IS DETECTED [**] [Priority: 0] [TCP] 192.168.196.134:1831 -> 192.168.196.135:80
02/23/22:40:43.368443 [**] [1:100005:0] DOS ATTACK IS DETECTED [**] [Priority: 0] [TCP] 192.168.196.134:1881 -> 192.168.196.135:80
02/23/22:40:43.370999 [**] [1:100005:0] DOS ATTACK IS DETECTED [**] [Priority: 0] [TCP] 192.168.196.134:1931 -> 192.168.196.135:80

```

```

root@ubuntu:~/Desktop$ sudo su
[sudo] password for ubuntu:
root@ubuntu:~/Desktop$ /etc/snort/rules# snort -A console -q -c /etc/snort/snort.conf
02/23/22:40:45.241665 [**] [1:100005:0] DOS ATTACK IS DETECTED [**] [Priority: 0] [TCP] 192.168.196.134:2082 -> 192.168.196.135:80
02/23/22:40:45.243460 [**] [1:100005:0] DOS ATTACK IS DETECTED [**] [Priority: 0] [TCP] 192.168.196.134:2912 -> 192.168.196.135:80
02/23/22:40:45.245850 [**] [1:100005:0] DOS ATTACK IS DETECTED [**] [Priority: 0] [TCP] 192.168.196.134:2962 -> 192.168.196.135:80
02/23/22:40:45.248067 [**] [1:100005:0] DOS ATTACK IS DETECTED [**] [Priority: 0] [TCP] 192.168.196.134:3012 -> 192.168.196.135:80
02/23/22:40:45.250538 [**] [1:100005:0] DOS ATTACK IS DETECTED [**] [Priority: 0] [TCP] 192.168.196.134:3062 -> 192.168.196.135:80
02/23/22:40:45.252099 [**] [1:100005:0] DOS ATTACK IS DETECTED [**] [Priority: 0] [TCP] 192.168.196.134:3112 -> 192.168.196.135:80
02/23/22:40:45.255284 [**] [1:100005:0] DOS ATTACK IS DETECTED [**] [Priority: 0] [TCP] 192.168.196.134:3162 -> 192.168.196.135:80
02/23/22:40:45.257692 [**] [1:100005:0] DOS ATTACK IS DETECTED [**] [Priority: 0] [TCP] 192.168.196.134:3212 -> 192.168.196.135:80
02/23/22:40:45.261044 [**] [1:100005:0] DOS ATTACK IS DETECTED [**] [Priority: 0] [TCP] 192.168.196.134:3262 -> 192.168.196.135:80
02/23/22:40:45.262910 [**] [1:100005:0] DOS ATTACK IS DETECTED [**] [Priority: 0] [TCP] 192.168.196.134:3312 -> 192.168.196.135:80
02/23/22:40:45.264679 [**] [1:100005:0] DOS ATTACK IS DETECTED [**] [Priority: 0] [TCP] 192.168.196.134:3362 -> 192.168.196.135:80
02/23/22:40:45.266081 [**] [1:100005:0] DOS ATTACK IS DETECTED [**] [Priority: 0] [TCP] 192.168.196.134:3412 -> 192.168.196.135:80
02/23/22:40:45.268075 [**] [1:100005:0] DOS ATTACK IS DETECTED [**] [Priority: 0] [TCP] 192.168.196.134:3462 -> 192.168.196.135:80
02/23/22:40:45.270284 [**] [1:100005:0] DOS ATTACK IS DETECTED [**] [Priority: 0] [TCP] 192.168.196.134:3512 -> 192.168.196.135:80
02/23/22:40:45.272617 [**] [1:100005:0] DOS ATTACK IS DETECTED [**] [Priority: 0] [TCP] 192.168.196.134:3562 -> 192.168.196.135:80
02/23/22:40:45.274773 [**] [1:100005:0] DOS ATTACK IS DETECTED [**] [Priority: 0] [TCP] 192.168.196.134:3612 -> 192.168.196.135:80
02/23/22:40:45.276729 [**] [1:100005:0] DOS ATTACK IS DETECTED [**] [Priority: 0] [TCP] 192.168.196.134:3662 -> 192.168.196.135:80
02/23/22:40:45.282749 [**] [1:100005:0] DOS ATTACK IS DETECTED [**] [Priority: 0] [TCP] 192.168.196.134:3712 -> 192.168.196.135:80
02/23/22:40:45.289867 [**] [1:100005:0] DOS ATTACK IS DETECTED [**] [Priority: 0] [TCP] 192.168.196.134:3762 -> 192.168.196.135:80
02/23/22:40:45.302136 [**] [1:100005:0] DOS ATTACK IS DETECTED [**] [Priority: 0] [TCP] 192.168.196.134:3811 -> 192.168.196.135:80
02/23/22:40:45.304184 [**] [1:100005:0] DOS ATTACK IS DETECTED [**] [Priority: 0] [TCP] 192.168.196.134:3861 -> 192.168.196.135:80
02/23/22:40:45.314184 [**] [1:100005:0] DOS ATTACK IS DETECTED [**] [Priority: 0] [TCP] 192.168.196.134:3911 -> 192.168.196.135:80
02/23/22:40:45.326036 [**] [1:100005:0] DOS ATTACK IS DETECTED [**] [Priority: 0] [TCP] 192.168.196.134:3962 -> 192.168.196.135:80
02/23/22:40:45.326843 [**] [1:100005:0] DOS ATTACK IS DETECTED [**] [Priority: 0] [TCP] 192.168.196.134:4012 -> 192.168.196.135:80
02/23/22:40:45.331299 [**] [1:100005:0] DOS ATTACK IS DETECTED [**] [Priority: 0] [TCP] 192.168.196.134:4062 -> 192.168.196.135:80
02/23/22:40:45.343184 [**] [1:100005:0] DOS ATTACK IS DETECTED [**] [Priority: 0] [TCP] 192.168.196.134:4112 -> 192.168.196.135:80
02/23/22:40:45.346399 [**] [1:100005:0] DOS ATTACK IS DETECTED [**] [Priority: 0] [TCP] 192.168.196.134:4162 -> 192.168.196.135:80

```

```

root@ubuntu:~/Desktop$ sudo su
[sudo] password for ubuntu:
root@ubuntu:~/Desktop$ /etc/snort/rules# snort -A console -q -c /etc/snort/snort.conf
02/23/22:40:45.974050 [**] [1:100005:0] DOS ATTACK IS DETECTED [**] [Priority: 0] [TCP] 192.168.196.134:1919 -> 192.168.196.135:80
02/23/22:40:45.981697 [**] [1:100005:0] DOS ATTACK IS DETECTED [**] [Priority: 0] [TCP] 192.168.196.134:19725 -> 192.168.196.135:80
02/23/22:40:45.990194 [**] [1:100005:0] DOS ATTACK IS DETECTED [**] [Priority: 0] [TCP] 192.168.196.134:20141 -> 192.168.196.135:80
02/23/22:40:45.998721 [**] [1:100005:0] DOS ATTACK IS DETECTED [**] [Priority: 0] [TCP] 192.168.196.134:20556 -> 192.168.196.135:80
02/23/22:40:45.999572 [**] [1:100005:0] DOS ATTACK IS DETECTED [**] [Priority: 0] [TCP] 192.168.196.134:20761 -> 192.168.196.135:80
02/23/22:40:46.011419 [**] [1:100005:0] DOS ATTACK IS DETECTED [**] [Priority: 0] [TCP] 192.168.196.134:20821 -> 192.168.196.135:80
02/23/22:40:46.016588 [**] [1:100005:0] DOS ATTACK IS DETECTED [**] [Priority: 0] [TCP] 192.168.196.134:2199 -> 192.168.196.135:80
02/23/22:40:46.017631 [**] [1:100005:0] DOS ATTACK IS DETECTED [**] [Priority: 0] [TCP] 192.168.196.134:21813 -> 192.168.196.135:80
02/23/22:40:46.018113 [**] [1:100005:0] DOS ATTACK IS DETECTED [**] [Priority: 0] [TCP] 192.168.196.134:22236 -> 192.168.196.135:80
02/23/22:40:46.0196907 [**] [1:100005:0] DOS ATTACK IS DETECTED [**] [Priority: 0] [TCP] 192.168.196.134:22309 -> 192.168.196.135:80
02/23/22:40:46.020854 [**] [1:100005:0] DOS ATTACK IS DETECTED [**] [Priority: 0] [TCP] 192.168.196.134:22310 -> 192.168.196.135:80
02/23/22:40:46.021146 [**] [1:100005:0] DOS ATTACK IS DETECTED [**] [Priority: 0] [TCP] 192.168.196.134:23319 -> 192.168.196.135:80
02/23/22:40:46.021967 [**] [1:100005:0] DOS ATTACK IS DETECTED [**] [Priority: 0] [TCP] 192.168.196.134:23590 -> 192.168.196.135:80
02/23/22:40:46.021967 [**] [1:100005:0] DOS ATTACK IS DETECTED [**] [Priority: 0] [TCP] 192.168.196.134:23888 -> 192.168.196.135:80
02/23/22:40:46.022666 [**] [1:100005:0] DOS ATTACK IS DETECTED [**] [Priority: 0] [TCP] 192.168.196.134:24443 -> 192.168.196.135:80
02/23/22:40:46.0232848 [**] [1:100005:0] DOS ATTACK IS DETECTED [**] [Priority: 0] [TCP] 192.168.196.134:24663 -> 192.168.196.135:80
02/23/22:40:46.023588 [**] [1:100005:0] DOS ATTACK IS DETECTED [**] [Priority: 0] [TCP] 192.168.196.134:24920 -> 192.168.196.135:80
02/23/22:40:46.025517 [**] [1:100005:0] DOS ATTACK IS DETECTED [**] [Priority: 0] [TCP] 192.168.196.134:25153 -> 192.168.196.135:80
02/23/22:40:46.026622 [**] [1:100005:0] DOS ATTACK IS DETECTED [**] [Priority: 0] [TCP] 192.168.196.134:25434 -> 192.168.196.135:80
02/23/22:40:46.028288 [**] [1:100005:0] DOS ATTACK IS DETECTED [**] [Priority: 0] [TCP] 192.168.196.134:25706 -> 192.168.196.135:80
02/23/22:40:46.029401 [**] [1:100005:0] DOS ATTACK IS DETECTED [**] [Priority: 0] [TCP] 192.168.196.134:25901 -> 192.168.196.135:80
02/23/22:40:46.030427 [**] [1:100005:0] DOS ATTACK IS DETECTED [**] [Priority: 0] [TCP] 192.168.196.134:26256 -> 192.168.196.135:80
02/23/22:40:46.031315 [**] [1:100005:0] DOS ATTACK IS DETECTED [**] [Priority: 0] [TCP] 192.168.196.134:26689 -> 192.168.196.135:80
02/23/22:40:46.031374 [**] [1:100005:0] DOS ATTACK IS DETECTED [**] [Priority: 0] [TCP] 192.168.196.134:27045 -> 192.168.196.135:80
02/23/22:40:46.033474 [**] [1:100005:0] DOS ATTACK IS DETECTED [**] [Priority: 0] [TCP] 192.168.196.134:27486 -> 192.168.196.135:80
02/23/22:40:46.034425 [**] [1:100005:0] DOS ATTACK IS DETECTED [**] [Priority: 0] [TCP] 192.168.196.134:27691 -> 192.168.196.135:80
02/23/22:40:46.034751 [**] [1:100005:0] DOS ATTACK IS DETECTED [**] [Priority: 0] [TCP] 192.168.196.134:27887 -> 192.168.196.135:80
02/23/22:40:46.035401 [**] [1:100005:0] DOS ATTACK IS DETECTED [**] [Priority: 0] [TCP] 192.168.196.134:27947 -> 192.168.196.135:80

```

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-force 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`

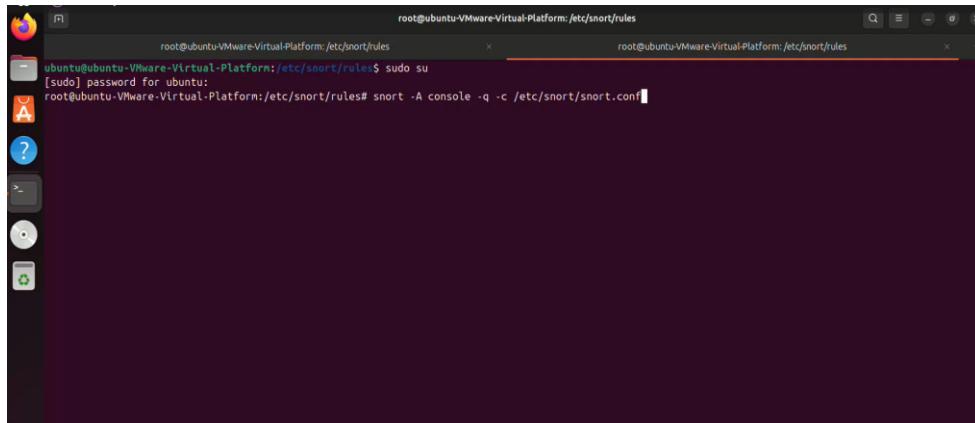
Rule : `alert tcp any any -> 192.168.196.135 any (msg:"BRUTE-FORCE ATTACK DETECTED"; flags:S; threshold:type threshold, track by_src, count 5, seconds 10; sid:1000002; rev:1;)`

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.



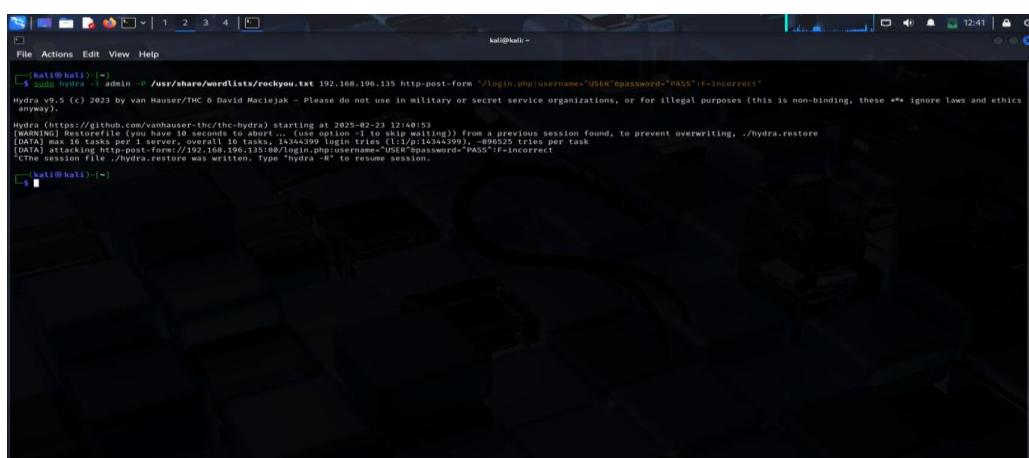
The screenshot shows a terminal window with two tabs. The left tab is titled 'ubuntu@ubuntu-Virtual-Platform:/etc/snort/rules' and contains the command [sudo] password for ubuntu: followed by the command 'root@ubuntu-Virtual-Platform:/etc/snort/rules# snort -A console -q -c /etc/snort/snort.conf'. The right tab is titled 'root@ubuntu-Virtual-Platform:/etc/snort/rules' and shows the command being run. The terminal has a dark background with light-colored text.

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.

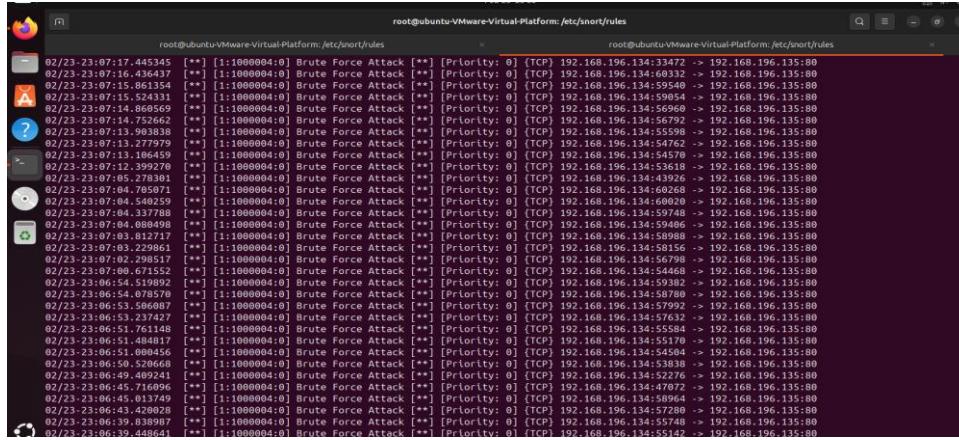


The screenshot shows a terminal window with a dark background. It displays the command 'kali@kali:~\$ sudo hydra -l admin -P /usr/share/wordlists/rockyou.txt 192.168.196.135 http-post-form "/Login.php?username=%USER%&password=%PASS%" -f -incorrect' followed by the output of the Hydra attack. The output includes warning messages about restore files and session resumption. The terminal has a dark background with light-colored text.

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



```
root@Ubuntu-VMware-Virtual-Platform:/etc/snort/rules
root@Ubuntu-VMware-Virtual-Platform:/etc/snort/rules

02/23-23:07:17.445345 [*] [1:1060004:0] Brute Force Attack [**] [Priority: 0] [TCP] 192.168.196.134:33472 -> 192.168.196.135:80
02/23-23:07:16.436437 [*] [1:1060004:0] Brute Force Attack [**] [Priority: 0] [TCP] 192.168.196.134:60332 -> 192.168.196.135:80
02/23-23:07:15.524434 [*] [1:1060004:0] Brute Force Attack [**] [Priority: 0] [TCP] 192.168.196.134:50054 -> 192.168.196.135:80
02/23-23:07:15.524331 [*] [1:1060004:0] Brute Force Attack [**] [Priority: 0] [TCP] 192.168.196.134:59054 -> 192.168.196.135:80
02/23-23:07:14.868956 [*] [1:1060004:0] Brute Force Attack [**] [Priority: 0] [TCP] 192.168.196.134:56968 -> 192.168.196.135:80
02/23-23:07:14.752662 [*] [1:1060004:0] Brute Force Attack [**] [Priority: 0] [TCP] 192.168.196.134:56792 -> 192.168.196.135:80
02/23-23:07:13.908388 [*] [1:1060004:0] Brute Force Attack [**] [Priority: 0] [TCP] 192.168.196.134:55598 -> 192.168.196.135:80
02/23-23:07:13.898388 [*] [1:1060004:0] Brute Force Attack [**] [Priority: 0] [TCP] 192.168.196.134:54579 -> 192.168.196.135:80
02/23-23:07:13.898388 [*] [1:1060004:0] Brute Force Attack [**] [Priority: 0] [TCP] 192.168.196.134:54579 -> 192.168.196.135:80
02/23-23:07:12.399276 [*] [1:1060004:0] Brute Force Attack [**] [Priority: 0] [TCP] 192.168.196.134:53618 -> 192.168.196.135:80
02/23-23:07:05.278301 [*] [1:1060004:0] Brute Force Attack [**] [Priority: 0] [TCP] 192.168.196.134:43926 -> 192.168.196.135:80
02/23-23:07:04.785071 [*] [1:1060004:0] Brute Force Attack [**] [Priority: 0] [TCP] 192.168.196.134:60268 -> 192.168.196.135:80
02/23-23:07:04.540259 [*] [1:1060004:0] Brute Force Attack [**] [Priority: 0] [TCP] 192.168.196.134:60028 -> 192.168.196.135:80
02/23-23:07:04.080000 [*] [1:1060004:0] Brute Force Attack [**] [Priority: 0] [TCP] 192.168.196.134:59044 -> 192.168.196.135:80
02/23-23:07:04.080000 [*] [1:1060004:0] Brute Force Attack [**] [Priority: 0] [TCP] 192.168.196.134:59046 -> 192.168.196.135:80
02/23-23:07:03.831717 [*] [1:1060004:0] Brute Force Attack [**] [Priority: 0] [TCP] 192.168.196.134:58998 -> 192.168.196.135:80
02/23-23:07:02.229861 [*] [1:1060004:0] Brute Force Attack [**] [Priority: 0] [TCP] 192.168.196.134:58158 -> 192.168.196.135:80
02/23-23:07:02.298517 [*] [1:1060004:0] Brute Force Attack [**] [Priority: 0] [TCP] 192.168.196.134:56798 -> 192.168.196.135:80
02/23-23:07:02.671552 [*] [1:1060004:0] Brute Force Attack [**] [Priority: 0] [TCP] 192.168.196.134:54468 -> 192.168.196.135:80
02/23-23:06:59.806456 [*] [1:1060004:0] Brute Force Attack [**] [Priority: 0] [TCP] 192.168.196.134:52776 -> 192.168.196.135:80
02/23-23:06:54.078570 [*] [1:1060004:0] Brute Force Attack [**] [Priority: 0] [TCP] 192.168.196.134:50780 -> 192.168.196.135:80
02/23-23:06:53.506067 [*] [1:1060004:0] Brute Force Attack [**] [Priority: 0] [TCP] 192.168.196.134:57992 -> 192.168.196.135:80
02/23-23:06:53.237427 [*] [1:1060004:0] Brute Force Attack [**] [Priority: 0] [TCP] 192.168.196.134:57632 -> 192.168.196.135:80
02/23-23:06:51.761148 [*] [1:1060004:0] Brute Force Attack [**] [Priority: 0] [TCP] 192.168.196.134:55178 -> 192.168.196.135:80
02/23-23:06:51.484841 [*] [1:1060004:0] Brute Force Attack [**] [Priority: 0] [TCP] 192.168.196.134:55178 -> 192.168.196.135:80
02/23-23:06:49.526056 [*] [1:1060004:0] Brute Force Attack [**] [Priority: 0] [TCP] 192.168.196.134:53828 -> 192.168.196.135:80
02/23-23:06:49.409241 [*] [1:1060004:0] Brute Force Attack [**] [Priority: 0] [TCP] 192.168.196.134:52276 -> 192.168.196.135:80
02/23-23:06:45.716096 [*] [1:1060004:0] Brute Force Attack [**] [Priority: 0] [TCP] 192.168.196.134:47872 -> 192.168.196.135:80
02/23-23:06:45.013749 [*] [1:1060004:0] Brute Force Attack [**] [Priority: 0] [TCP] 192.168.196.134:58964 -> 192.168.196.135:80
02/23-23:06:43.426928 [*] [1:1060004:0] Brute Force Attack [**] [Priority: 0] [TCP] 192.168.196.134:57280 -> 192.168.196.135:80
02/23-23:06:39.838987 [*] [1:1060004:0] Brute Force Attack [**] [Priority: 0] [TCP] 192.168.196.134:55748 -> 192.168.196.135:80
02/23-23:06:39.446641 [*] [1:1060004:0] Brute Force Attack [**] [Priority: 0] [TCP] 192.168.196.134:55142 -> 192.168.196.135:80
```

Now that the brute-force **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.