I. INTRODUCTION

Snort is an open source network intrusion prevention system, capable of performing real-time traffic analysis and packet logging on IP networks. It can perform protocol analysis, content searching/matching, and can be used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, OS fingerprinting attempts, and much more.

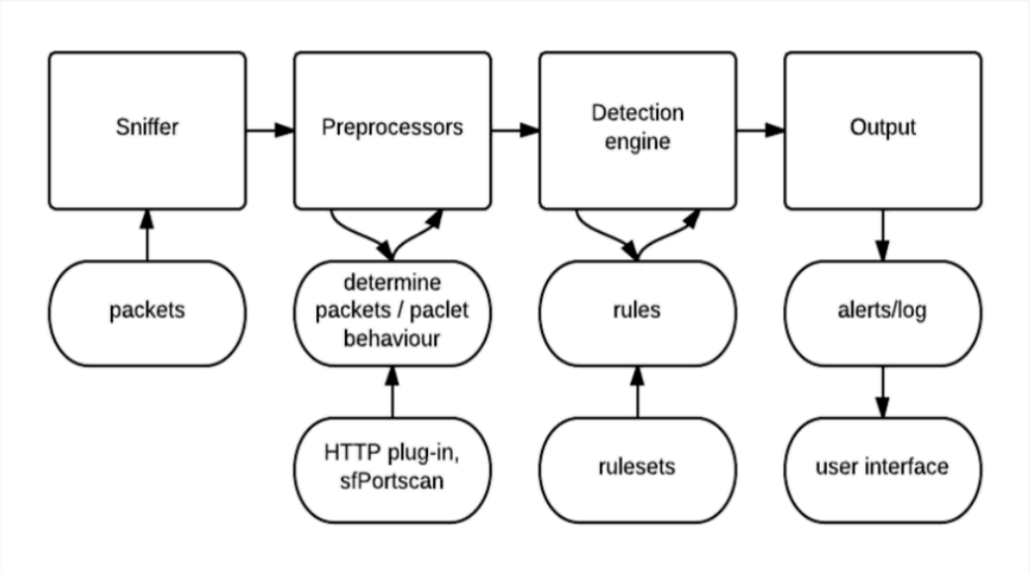
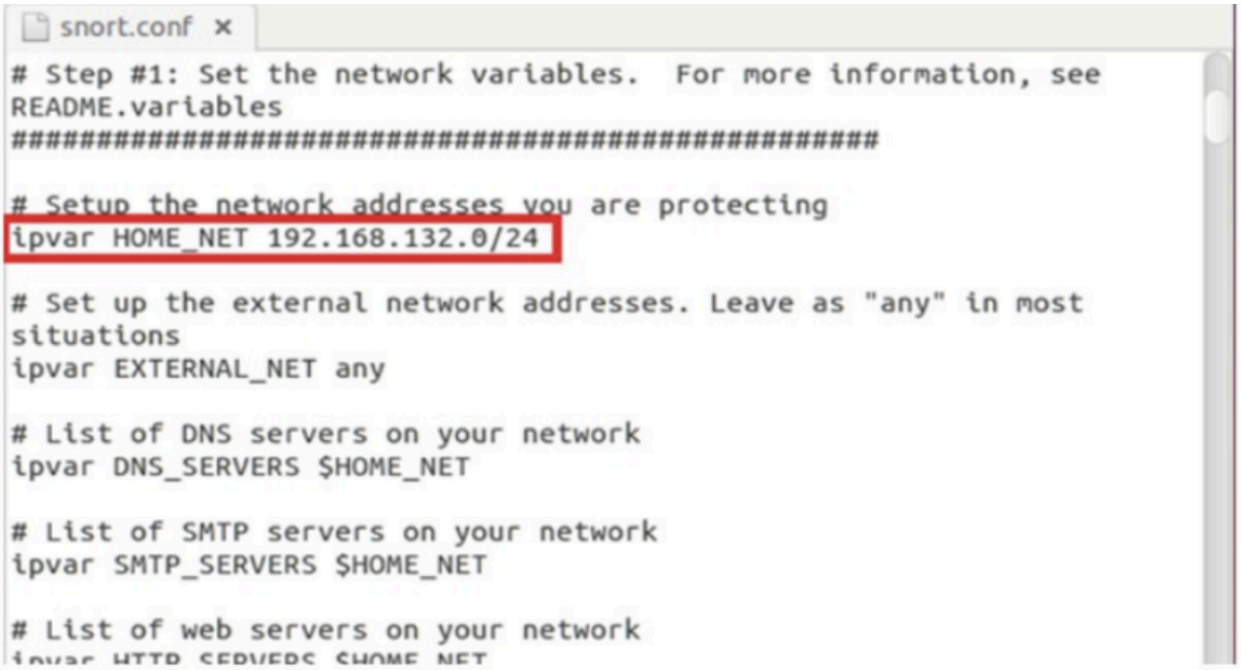


Fig: Snort Architecture

Snort Version

```
   ,,_     -*> Snort++ <*-
  o"  )~   Version 3.1.84.0
   ''''    By Martin Roesch & The Snort Team
           http://snort.org/contact#team
           Copyright (C) 2014-2024 Cisco and/or its affiliates. All rights reser
ved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using DAQ version 3.0.14
           Using LuaJIT version 2.1.1710088188
           Using OpenSSL 3.3.0 9 Apr 2024
           Using libpcap version 1.10.4
           Using PCRE version 8.45 2021-06-15
           Using ZLIB version 1.2.12
           Using Hyperscan version 5.4.11 2023-11-21
           Using LZMA version 5.6.1
```

Changing the ip address to the hom_net address



Rule Header

- alert – Rule action. Snort will generate an alert when the set condition is met.

- any – Source IP. Snort will look at all sources.
- any – Source port. Snort will look at all ports.
- -> – Direction. From source to destination.
- $HOME_NET – Destination IP. We are using the HOME_NET value from the snort.conf file.
- any – Destination port. Snort will look at all ports on the protected network

Rule Options

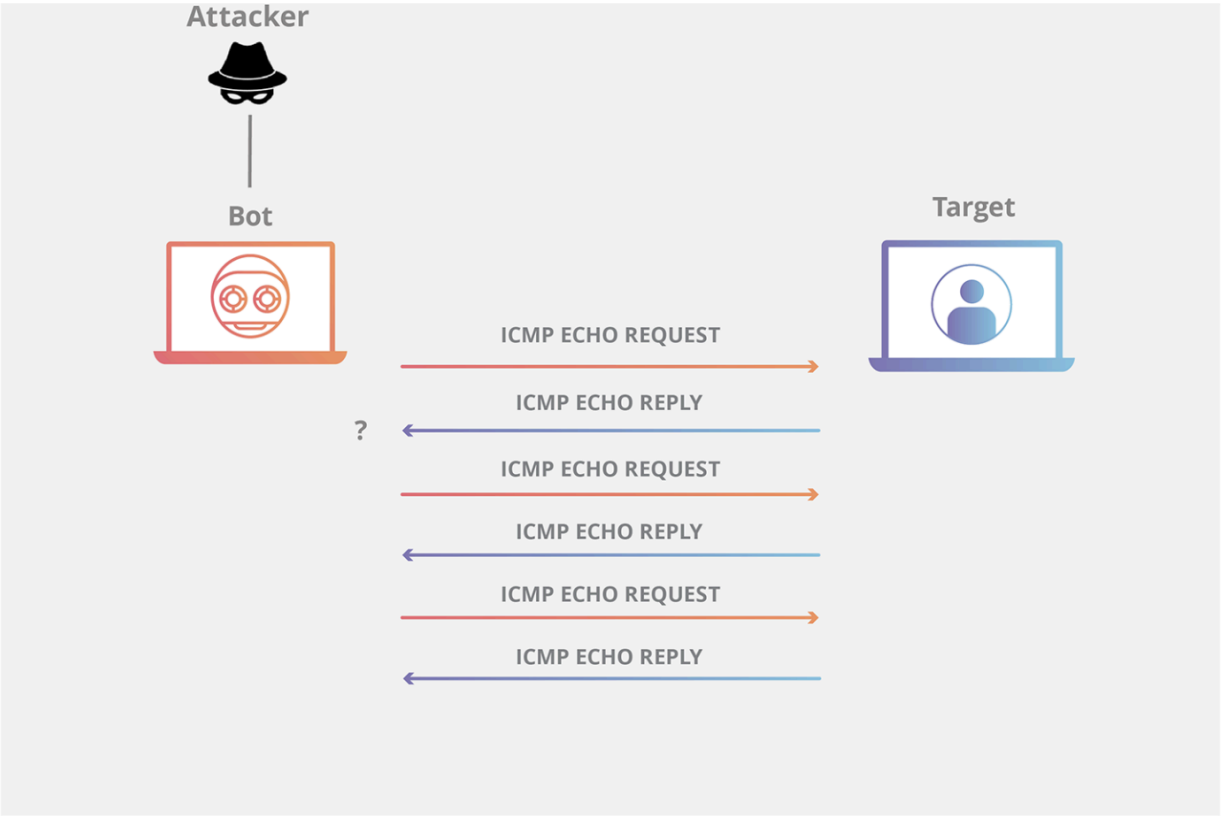
- msg:"ICMP flood" – Snort will include this message with the alert.
- sid:1000001 – Snort rule ID. Remember all numbers < 1,000,000 are reserved, this is why we are starting with 1000001 (you may use any number, as long as it's greater than 1,000,000).
- rev:1 – Revision number. This option allows for easier rule maintenance.
- classtype:icmp-event – Categorizes the rule as an "icmp-event", one of the predefined Snort categories. This option helps with rule organization.
- detection_filter:track by_dst - Snort tracks the destination IP address for detection.
- seconds 3 - sampling period is set to 3 seconds
- count 500 - if during the sampling period Snort detects more than 500 requests then we will receive the alert.

Now, let's start Snort in IDS mode and tell it to display alerts to the console:

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

Here we are pointing Snort to the configuration file it should use (**-c**) and specifying the interface (**-i eth0**). The **-A console** option prints alerts to standard output. We don't see any output when we enter the command because Snort hasn't detected any activity specified in the rule we wrote. We generate some activity and see if our rule is working. We launch our VM.

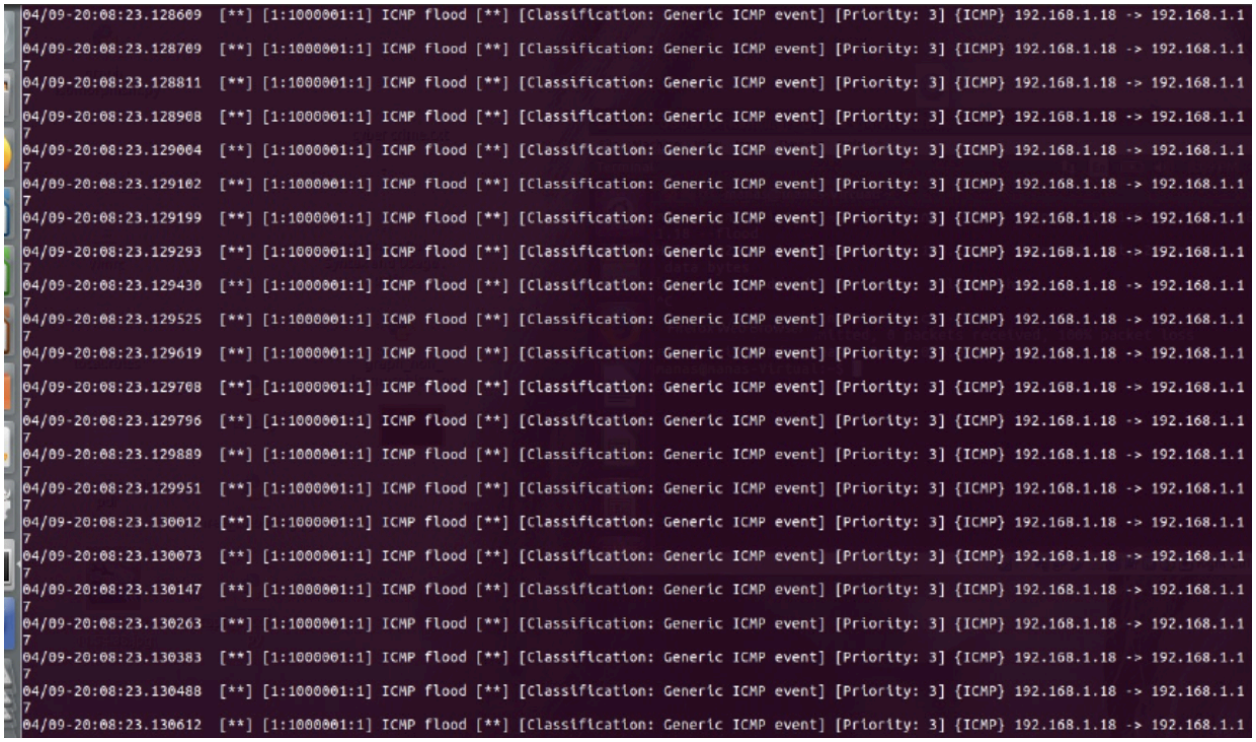
Then we run a tool called **hping3** to launch an ICMP flooding attack on our local host. We see alerts generated for every ICMP echo request past the specified count value within the sampling period with the message text we specified in the **msg** option.

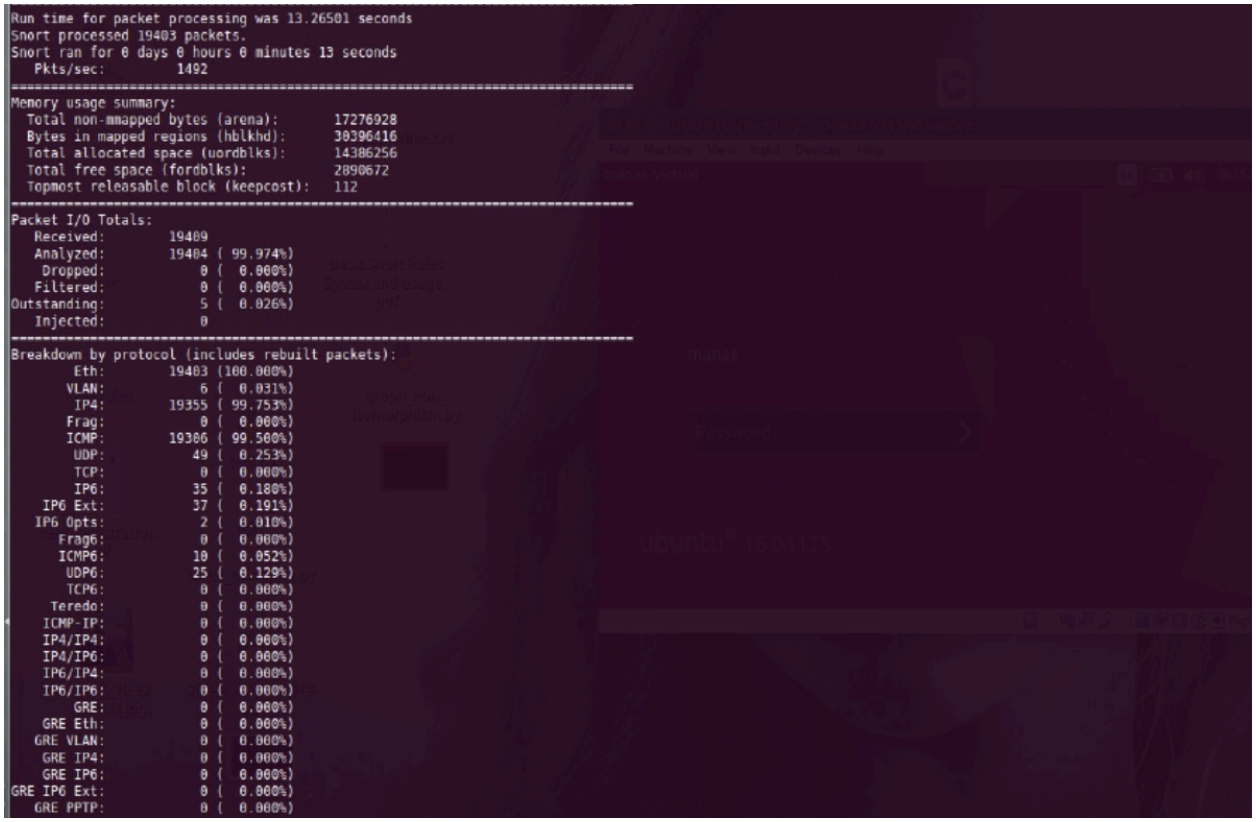


alert icmp any any -> $HOME_NET any (msg:"ICMP flood"; sid:1000001; rev:1; classtype:icmp-event; detection_filter:track by_dst, count 500, seconds 3;)

An Internet Control Message Protocol (ICMP) flood attack is a common distributed denial-of-service (DDoS) attack where malicious actors try to overwhelm a server or network device with ICMP pings, or echo-request packets.

DETECTION OF DDOS USING SNORT



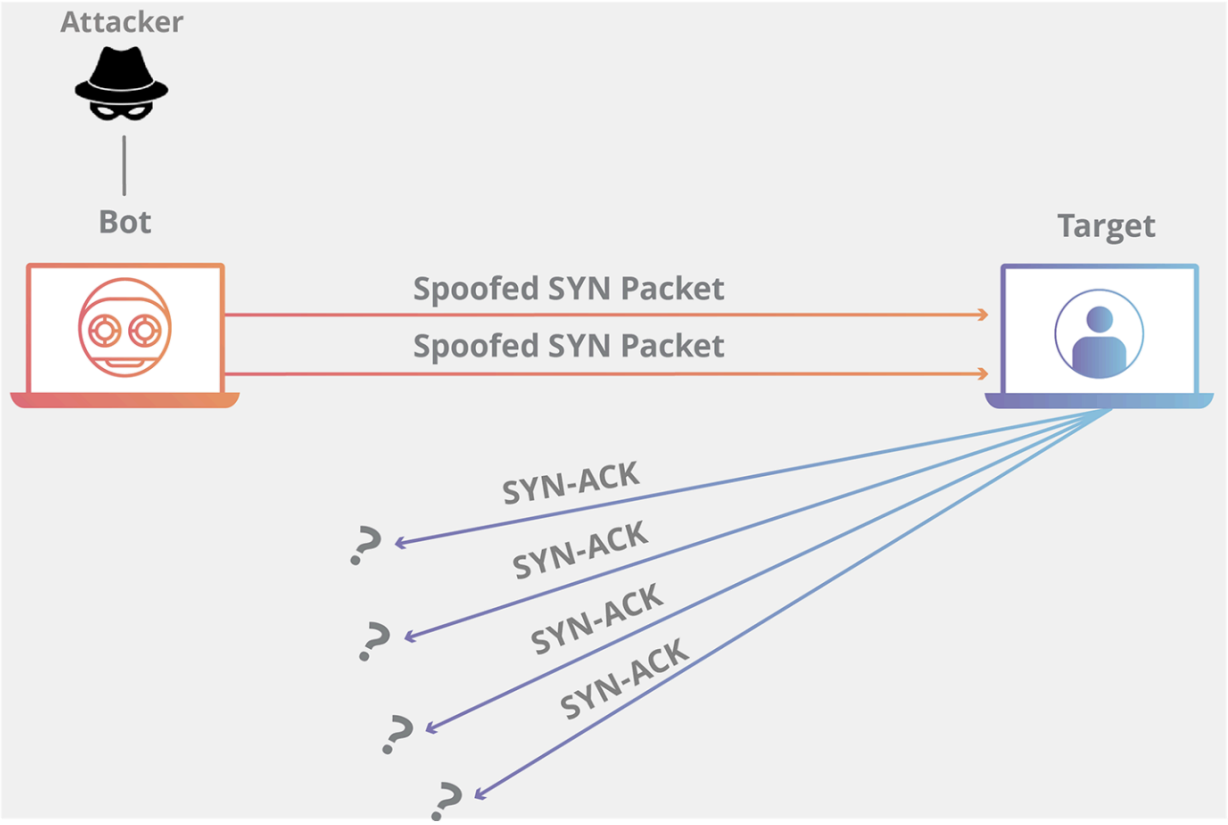


```
Run time for packet processing was 13.26501 seconds
Snort processed 19403 packets.
Snort ran for 0 days 0 hours 0 minutes 13 seconds
   Pkts/sec:         1492
===============================================================================
Memory usage summary:
  Total non-mmapped bytes (arena):       17276928
  Bytes in mapped regions (hblkhd):      30396416
  Total allocated space (uordblks):      14386256
  Total free space (fordblks):           2890672
  Topmost releasable block (keepcost):   112
===============================================================================
Packet I/O Totals:
   Received:        19409
   Analyzed:        19404 ( 99.974%)
    Dropped:            0 (  0.000%)
   Filtered:            0 (  0.000%)
Outstanding:            5 (  0.026%)
   Injected:            0
===============================================================================
Breakdown by protocol (includes rebuilt packets):
        Eth:        19403 (100.000%)
       VLAN:            6 (  0.031%)
        IP4:        19355 ( 99.753%)
       Frag:            0 (  0.000%)
       ICMP:        19306 ( 99.500%)
        UDP:           49 (  0.253%)
        TCP:            0 (  0.000%)
        IP6:           35 (  0.180%)
    IP6 Ext:           37 (  0.191%)
   IP6 Opts:            2 (  0.010%)
      Frag6:            0 (  0.000%)
      ICMP6:           10 (  0.052%)
       UDP6:           25 (  0.129%)
       TCP6:            0 (  0.000%)
     Teredo:            0 (  0.000%)
    ICMP-IP:            0 (  0.000%)
    IP4/IP4:            0 (  0.000%)
    IP4/IP6:            0 (  0.000%)
    IP6/IP4:            0 (  0.000%)
    IP6/IP6:            0 (  0.000%)
        GRE:            0 (  0.000%)
    GRE Eth:            0 (  0.000%)
   GRE VLAN:            0 (  0.000%)
    GRE IP4:            0 (  0.000%)
    GRE IP6:            0 (  0.000%)
GRE IP6 Ext:            0 (  0.000%)
    GRE PPTP:           0 (  0.000%)
```

SYN ATTACK

alert tcp any any -> $HOME_NET 80 (flags: S; msg:"Possible DoS Attack Type : SYNflood"; flow:stateless; sid:3; detection_filter:track by_dst, count 20, seconds 10;)

DETECTION OF DDOS USING SNORT




```
        Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
        Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
        Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
Commencing packet processing (pid=3432)
04/09-20:28:31.737660  [**] [1:3:0] Possible DoS Attack    Type : SYN flood [**] [Priority: 0] {TCP} 242.233.115.149:2700 -> 192.168.1.17:80
04/09-20:28:32.738992  [**] [1:3:0] Possible DoS Attack    Type : SYN flood [**] [Priority: 0] {TCP} 212.125.55.42:2701 -> 192.168.1.17:80
04/09-20:28:33.739468  [**] [1:3:0] Possible DoS Attack    Type : SYN flood [**] [Priority: 0] {TCP} 58.6.187.140:2702 -> 192.168.1.17:80
04/09-20:28:34.739962  [**] [1:3:0] Possible DoS Attack    Type : SYN flood [**] [Priority: 0] {TCP} 213.168.252.70:2703 -> 192.168.1.17:80
04/09-20:28:35.744141  [**] [1:3:0] Possible DoS Attack    Type : SYN flood [**] [Priority: 0] {TCP} 55.138.201.229:2704 -> 192.168.1.17:80
04/09-20:28:36.744410  [**] [1:3:0] Possible DoS Attack    Type : SYN flood [**] [Priority: 0] {TCP} 154.253.253.72:2705 -> 192.168.1.17:80
04/09-20:28:37.744965  [**] [1:3:0] Possible DoS Attack    Type : SYN flood [**] [Priority: 0] {TCP} 29.50.223.167:2706 -> 192.168.1.17:80
04/09-20:28:38.749986  [**] [1:3:0] Possible DoS Attack    Type : SYN flood [**] [Priority: 0] {TCP} 53.163.186.189:2707 -> 192.168.1.17:80
04/09-20:28:39.750350  [**] [1:3:0] Possible DoS Attack    Type : SYN flood [**] [Priority: 0] {TCP} 217.115.230.201:2708 -> 192.168.1.17:80
04/09-20:28:40.750910  [**] [1:3:0] Possible DoS Attack    Type : SYN flood [**] [Priority: 0] {TCP} 126.25.76.213:2709 -> 192.168.1.17:80
04/09-20:28:41.751335  [**] [1:3:0] Possible DoS Attack    Type : SYN flood [**] [Priority: 0] {TCP} 151.57.191.244:2710 -> 192.168.1.17:80
04/09-20:28:42.751872  [**] [1:3:0] Possible DoS Attack    Type : SYN flood [**] [Priority: 0] {TCP} 109.119.236.197:2711 -> 192.168.1.17:80
04/09-20:28:43.752498  [**] [1:3:0] Possible DoS Attack    Type : SYN flood [**] [Priority: 0] {TCP} 126.81.2.193:2712 -> 192.168.1.17:80
04/09-20:28:44.752913  [**] [1:3:0] Possible DoS Attack    Type : SYN flood [**] [Priority: 0] {TCP} 109.37.126.197:2713 -> 192.168.1.17:80
04/09-20:28:45.753562  [**] [1:3:0] Possible DoS Attack    Type : SYN flood [**] [Priority: 0] {TCP} 18.244.55.187:2714 -> 192.168.1.17:80
04/09-20:28:46.754074  [**] [1:3:0] Possible DoS Attack    Type : SYN flood [**] [Priority: 0] {TCP} 223.161.222.123:2715 -> 192.168.1.17:80
04/09-20:28:47.754501  [**] [1:3:0] Possible DoS Attack    Type : SYN flood [**] [Priority: 0] {TCP} 191.55.182.126:2716 -> 192.168.1.17:80
04/09-20:28:48.755045  [**] [1:3:0] Possible DoS Attack    Type : SYN flood [**] [Priority: 0] {TCP} 71.97.233.27:2717 -> 192.168.1.17:80
04/09-20:28:49.755526  [**] [1:3:0] Possible DoS Attack    Type : SYN flood [**] [Priority: 0] {TCP} 104.212.14.139:2718 -> 192.168.1.17:80
04/09-20:28:50.756035  [**] [1:3:0] Possible DoS Attack    Type : SYN flood [**] [Priority: 0] {TCP} 147.239.198.148:2719 -> 192.168.1.17:80
04/09-20:28:51.756495  [**] [1:3:0] Possible DoS Attack    Type : SYN flood [**] [Priority: 0] {TCP} 239.70.249.55:2720 -> 192.168.1.17:80
04/09-20:28:52.756887  [**] [1:3:0] Possible DoS Attack    Type : SYN flood [**] [Priority: 0] {TCP} 68.162.197.123:2721 -> 192.168.1.17:80
04/09-20:28:53.757365  [**] [1:3:0] Possible DoS Attack    Type : SYN flood [**] [Priority: 0] {TCP} 219.103.204.120:2722 -> 192.168.1.17:80
04/09-20:28:54.757847  [**] [1:3:0] Possible DoS Attack    Type : SYN flood [**] [Priority: 0] {TCP} 21.42.2.168:2723 -> 192.168.1.17:80
04/09-20:28:55.758303  [**] [1:3:0] Possible DoS Attack    Type : SYN flood [**] [Priority: 0] {TCP} 97.55.235.214:2724 -> 192.168.1.17:80
04/09-20:28:56.758862  [**] [1:3:0] Possible DoS Attack    Type : SYN flood [**] [Priority: 0] {TCP} 193.95.179.48:2725 -> 192.168.1.17:80
04/09-20:28:57.759381  [**] [1:3:0] Possible DoS Attack    Type : SYN flood [**] [Priority: 0] {TCP} 152.187.55.227:2726 -> 192.168.1.17:80
04/09-20:28:58.759845  [**] [1:3:0] Possible DoS Attack    Type : SYN flood [**] [Priority: 0] {TCP} 161.152.62.219:2727 -> 192.168.1.17:80
04/09-20:28:59.760632  [**] [1:3:0] Possible DoS Attack    Type : SYN flood [**] [Priority: 0] {TCP} 240.136.101.249:2728 -> 192.168.1.17:80
04/09-20:29:00.761056  [**] [1:3:0] Possible DoS Attack    Type : SYN flood [**] [Priority: 0] {TCP} 126.138.29.93:2729 -> 192.168.1.17:80
04/09-20:29:01.761671  [**] [1:3:0] Possible DoS Attack    Type : SYN flood [**] [Priority: 0] {TCP} 13.110.242.42:2730 -> 192.168.1.17:80
04/09-20:29:02.762162  [**] [1:3:0] Possible DoS Attack    Type : SYN flood [**] [Priority: 0] {TCP} 187.230.21.129:2731 -> 192.168.1.17:80
04/09-20:29:03.762649  [**] [1:3:0] Possible DoS Attack    Type : SYN flood [**] [Priority: 0] {TCP} 191.214.235.161:2732 -> 192.168.1.17:80
04/09-20:29:04.763112  [**] [1:3:0] Possible DoS Attack    Type : SYN flood [**] [Priority: 0] {TCP} 110.139.252.238:2733 -> 192.168.1.17:80
04/09-20:29:05.763766  [**] [1:3:0] Possible DoS Attack    Type : SYN flood [**] [Priority: 0] {TCP} 72.126.203.25:2734 -> 192.168.1.17:80
04/09-20:29:06.764336  [**] [1:3:0] Possible DoS Attack    Type : SYN flood [**] [Priority: 0] {TCP} 110.93.168.252:2735 -> 192.168.1.17:80
04/09-20:29:07.764923  [**] [1:3:0] Possible DoS Attack    Type : SYN flood [**] [Priority: 0] {TCP} 213.125.64.182:2736 -> 192.168.1.17:80
04/09-20:29:08.765498  [**] [1:3:0] Possible DoS Attack    Type : SYN flood [**] [Priority: 0] {TCP} 109.153.122.123:2737 -> 192.168.1.17:80
04/09-20:29:09.766173  [**] [1:3:0] Possible DoS Attack    Type : SYN flood [**] [Priority: 0] {TCP} 58.174.154.233:2738 -> 192.168.1.17:80
^C*** Caught Int-Signal
===============================================================================
Run time for packet processing was 51.6087 seconds
Snort processed 381 packets.
Snort ran for 0 days 0 hours 0 minutes 51 seconds
   Pkts/sec:           7
```

DETECTION OF DDOS USING SNORT