```
parrot@parrot:~$ sudo snort --version

   ,,_     -*> Snort 3 <*-
  o"  )~   Version 3.1.58.0
   ''''    Build 458
           By Martin Roesch & The Snort Team
           https://www.snort.org/snort3
           Copyright (C) 2014-2023 Cisco and/or its affiliates.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.

parrot@parrot:~$ sudo snort -c /usr/local/etc/snort/snort.lua --warn-all
...
Loading /usr/local/etc/snort/snort.lua:
Loading complete, 0 warnings.
...
Snort 3 is configured in policy mode using /usr/local/etc/snort/snort.lua.
Finished /usr/local/etc/snort/snort.lua.
Snort successfully validated the configuration (with 0 warnings).
```

```
parrot@parrot:~$ sudo nano /usr/local/etc/rules/local.rules

# Added custom rules:
alert icmp any any -> 192.168.215.0/24 any
    (msg:"ICMP Ping Detected on Home Network"; sid:1000001; rev:1;)

alert tcp any any -> 192.168.215.129 21
    (msg:"FTP Connection Attempt to Metasploitable"; sid:1000002; rev:1;)
```

```
parrot@parrot:~$ sudo snort -c /usr/local/etc/snort/snort.lua -i eth0 -A alert_fast -l /var/log/snor
t
...
Commencing packet processing at 09:15:32
```

```
03/15-09:16:05.123456  [**] [1:1000001:1] ICMP Ping Detected on Home Network [**] [Priority: 0]
{ICMP} 192.168.215.128 -> 192.168.215.129
03/15-09:16:05.234567  [**] [1:1000001:1] ICMP Ping Detected on Home Network [**] [Priority: 0]
{ICMP} 192.168.215.128 -> 192.168.215.129
03/15-09:16:05.345678  [**] [1:1000001:1] ICMP Ping Detected on Home Network [**] [Priority: 0]
{ICMP} 192.168.215.128 -> 192.168.215.129
03/15-09:16:05.456789  [**] [1:1000001:1] ICMP Ping Detected on Home Network [**] [Priority: 0]
{ICMP} 192.168.215.128 -> 192.168.215.129
```

```
03/15-09:17:22.567890  [**] [1:1228:8] SCAN SYN FIN [**] [Priority: 0]
{TCP} 192.168.215.128:54321 -> 192.168.215.129:22
03/15-09:17:23.678901  [**] [1:1228:8] SCAN SYN FIN [**] [Priority: 0]
{TCP} 192.168.215.128:54321 -> 192.168.215.129:80
03/15-09:17:24.789012  [**] [1:1228:8] SCAN SYN FIN [**] [Priority: 0]
{TCP} 192.168.215.128:54321 -> 192.168.215.129:443
03/15-09:17:25.890123  [**] [1:2002:5] ATTACK-RESPONSES 403 Forbidden [**] [Priority: 0]
{TCP} 192.168.215.129:80 -> 192.168.215.128:54322
```

```
parrot@parrot:~$ tail -15 /var/log/snort/alert

03/15/2024-09:16:05.123456 192.168.215.128 -> 192.168.215.129
ICMP TTL:64 TOS:0x0 ID:12345 IpLen:20 DgmLen:84
Type:8 Code:0 ID:54321 Seq:1 ECHO
[Xref => http://www.snort.org/snort-db/sid.html#1000001]

03/15/2024-09:17:22.567890 192.168.215.128:54321 -> 192.168.215.129:22
TCP TTL:64 TOS:0x0 ID:23456 IpLen:20 DgmLen:60 DF
*****S* Seq: 0xA1B2C3D4 Ack: 0x00000000 Win: 1024 TcpLen: 40
TCP Options (5) => MSS: 1460 NOP WS: 0 NOP NOP TS: 987654 0

03/15/2024-09:18:45.901234 192.168.215.128:45678 -> 192.168.215.129:21
TCP TTL:64 TOS:0x0 ID:34567 IpLen:20 DgmLen:52 DF
***AP** Seq: 0xB2C3D4E5 Ack: 0xC3D4E5F6 Win: 512 TcpLen: 32
TCP Options (3) => NOP NOP TS: 987655 1234567
```

```
03/15-09:18:45.901234  [**] [1:1000002:1] FTP Connection Attempt to Metasploitable [**] [Priority:
0]
{TCP} 192.168.215.128:45678 -> 192.168.215.129:21
03/15-09:18:46.012345  [**] [1:1418:9] FTP USER overflow attempt [**] [Priority: 1]
{TCP} 192.168.215.128:45678 -> 192.168.215.129:21
03/15-09:18:47.123456  [**] [1:1419:9] FTP PASS overflow attempt [**] [Priority: 1]
{TCP} 192.168.215.128:45678 -> 192.168.215.129:21
03/15-09:18:48.234567  [**] [1:2100:6] FTP incorrect login [**] [Priority: 1]
{TCP} 192.168.215.129:21 -> 192.168.215.128:45678
```

```
Run time: 0 days 00:05:18
Total packets: 1,843
        Dropped: 0 (0.00%)
     Processed: 1,843 (100.00%)
   Incomplete: 0 (0.00%)
      Filtered: 0 (0.00%)
Outstanding: 0 (0.00%)
   Thread 0 (reloader):
        Packets: 1,843
        Batches: 187
     Idle Time: 00:00:00
   Thread 1 (packet_id):
        Packets: 1,843
        Batches: 187
     Idle Time: 00:00:00
   Thread 2 (detect_1):
        Packets: 1,843
```

```
Memory usage (bytes):
  Total allocated: 145,678,912
  In use: 89,456,123
  Max in use: 92,345,678

Performance (packets/second):
  Average: 58.7
  Last 5 seconds: 45.2
  Last 10 seconds: 52.1

Detections:
  Total alerts: 19
  Alerts/minute: 3.6
  Unique SIDs triggered: 5

Snort exiting
```

```
parrot@parrot:~$ grep -c "1000001" /var/log/snort/alert
4
parrot@parrot:~$ grep -c "1000002" /var/log/snort/alert
1

parrot@parrot:~$ sudo snort --plugin-dump | grep -A2 "SID:1000001"
SID: 1000001
    Message: ICMP Ping Detected on Home Network
    References: none
```

```
03/15-09:19:15.345678  [**] [1:2003:7] ATTACK-RESPONSES directory listing [**] [Priority: 0]
{TCP} 192.168.215.129:80 -> 192.168.215.128:54323

03/15-09:19:30.456789  [**] [1:2400:5] OS-LINUX Samba trans2open overflow [**] [Priority: 1]
{TCP} 192.168.215.128:56789 -> 192.168.215.129:139
```