```
└─$ snort -c /usr/local/etc/snort/snort.lua
--------------------------------------------------
o")~  Snort++ 3.1.74.0
--------------------------------------------------
Loading /usr/local/etc/snort/snort.lua:
Loading snort_defaults.lua:
Finished snort_defaults.lua:
    active
    alerts
    daq
    decode
    host_cache
    host_tracker
    hosts
    network
    packets
    search_engine
    so_proxy
    stream
    stream_ip
    stream_icmp
    stream_tcp
    stream_user
    stream_file
    arp_spoof
    back_orifice
    dns
    imap
```

netflow

normalizer

rpc_decode

sip

ssh

telnet

cip

dnp3

iec104

mms

modbus

s7commplus

dce_smb

dce_tcp

dce_udp

dce_http_proxy

gtp_inspect

port_scan

ftp_server

http_inspect

http2_inspect

file_policy

appid

wizard

trace

ips

classifications

references

```
    binder
    js_norm
    file_id
    ftp_data
    ftp_client
    smtp
    dce_http_server
    ssl
    pop
    stream_udp
    process
    output
Finished /usr/local/etc/snort/snort.lua:
Loading file_id.rules_file:
Loading file_magic.rules:
Finished file_magic.rules:
Finished file_id.rules_file:
--------------------------------------------------
ips policies rule stats
          id  loaded  shared enabled    file
           0    208      0    208    /usr/local/etc/snort/snort.lua
--------------------------------------------------
rule counts
     total rules loaded: 208
           text rules: 208
         option chains: 208
         chain headers: 1
--------------------------------------------------
```

```
service rule counts        to-srv  to-cli
             file_id:     208    208
               total:     208    208
-------------------------------------------------
fast pattern groups
            to_server: 1
            to_client: 1
-------------------------------------------------
search engine (ac_bnfa)
             instances: 2
              patterns: 416
          pattern chars: 2508
             num states: 1778
        num match states: 370
           memory scale: KB
           total memory: 68.5879
         pattern memory: 18.6973
       match list memory: 27.3281
       transition memory: 22.3125
appid: MaxRss diff: 2220
appid: patterns loaded: 300
-------------------------------------------------
pcap DAQ configured to passive.


Snort successfully validated the configuration (with 0 warnings).
o")~  Snort exiting
```

_____

_____

┌──(virus㉿virus)-[~/snort/snort3-3.1.74.0/build]

└─$ sudo snort -c /usr/local/etc/snort/snort.lua -i eth0 -A alert_fast

---

o")~ Snort++ 3.1.74.0

Loading /usr/local/etc/snort/snort.lua:

Loading snort_defaults.lua:

Finished snort_defaults.lua:

port_scan

smtp

ftp_server

http_inspect

http2_inspect

file_policy

js_norm

appid

wizard

binder

ips

classifications

references

file_id

ftp_data

ftp_client

dce_udp

modbus

active

daq

decode

host_cache

normalizer

netflow

imap

dns

back_orifice

arp_spoof

stream_file

stream_user

stream_udp

stream_tcp

stream_icmp

stream_ip

stream

alerts

output

host_tracker

network

packets

search_engine

trace

hosts

process

so_proxy

```
    pop
    rpc_decode
    sip
    ssh
    ssl
    telnet
    cip
    dnp3
    iec104
    mms
    s7commplus
    dce_smb
    dce_tcp
    dce_http_proxy
    dce_http_server
    gtp_inspect
Finished /usr/local/etc/snort/snort.lua:
Loading file_id.rules_file:
Loading file_magic.rules:
Finished file_magic.rules:
Finished file_id.rules_file:
Loading /usr/local/etc/rules/local.rules:
Finished /usr/local/etc/rules/local.rules:
-------------------------------------------------
ips policies rule stats
        id  loaded  shared enabled    file
         0    831     0    831    /usr/local/etc/snort/snort.lua
-------------------------------------------------
```

```
rule counts
      total rules loaded: 831
            text rules: 209
          builtin rules: 622
          option chains: 831
          chain headers: 3
-------------------------------------------------
port rule counts
         tcp    udp   icmp     ip
    any   622      0      1      0
  total   622      0      1      0
-------------------------------------------------
service rule counts        to-srv  to-cli
             file_id:     208    208
               total:     208    208
-------------------------------------------------
fast pattern groups
             to_server: 1
             to_client: 1
-------------------------------------------------
search engine (ac_bnfa)
             instances: 2
              patterns: 416
          pattern chars: 2508
            num states: 1778
         num match states: 370
           memory scale: KB
           total memory: 68.5879
```

pattern memory: 18.6973

match list memory: 27.3281

transition memory: 22.3125

appid: MaxRss diff: 2268

appid: patterns loaded: 300

---

pcap DAQ configured to passive.

Commencing packet processing

++ [0] eth0

07/31-15:41:25.289717 [**] [116:444:1] "(ipv4) IPv4 option set" [**] [Priority: 3] {IP} 192.168.0.1 -> 224.0.0.1

07/31-15:41:27.937727 [**] [116:444:1] "(ipv4) IPv4 option set" [**] [Priority: 3] {IP} 192.168.0.104 -> 224.0.0.251

07/31-15:41:28.774075 [**] [116:444:1] "(ipv4) IPv4 option set" [**] [Priority: 3] {IP} 192.168.0.107 -> 224.0.0.252

07/31-15:41:28.774365 [**] [116:444:1] "(ipv4) IPv4 option set" [**] [Priority: 3] {IP} 192.168.0.107 -> 239.255.255.250

07/31-15:42:12.714785 [**] [116:444:1] "(ipv4) IPv4 option set" [**] [Priority: 3] {IP} 192.168.0.104 -> 224.0.0.2

07/31-15:42:12.714892 [**] [1:1000001:0] "ICMP Detected" [**] [Priority: 0] {ICMP} fe80::5029:d1ff:fe73:b9c1 -> ff02::16

07/31-15:42:13.479088 [**] [1:1000001:0] "ICMP Detected" [**] [Priority: 0] {ICMP} fe80::5029:d1ff:fe73:b9c1 -> ff02::16

07/31-15:43:30.274027 [**] [116:444:1] "(ipv4) IPv4 option set" [**] [Priority: 3] {IP} 192.168.0.1 -> 224.0.0.1

07/31-15:43:33.264545 [**] [116:444:1] "(ipv4) IPv4 option set" [**] [Priority: 3] {IP} 192.168.0.107 -> 224.0.0.252

07/31-15:43:34.265200 [**] [116:444:1] "(ipv4) IPv4 option set" [**] [Priority: 3] {IP} 192.168.0.107 -> 239.255.255.250

07/31-15:43:39.767163 [**] [116:444:1] "(ipv4) IPv4 option set" [**] [Priority: 3] {IP} 192.168.0.107 -> 224.0.0.251

07/31-15:44:24.369457 [**] [1:1000001:0] "ICMP Detected" [**] [Priority: 0] {ICMP} 192.168.0.107 -> 192.168.0.101

07/31-15:44:24.369487 [**] [1:1000001:0] "ICMP Detected" [**] [Priority: 0] {ICMP} 192.168.0.101 -> 192.168.0.107

07/31-15:44:25.378253 [**] [1:1000001:0] "ICMP Detected" [**] [Priority: 0] {ICMP} 192.168.0.107 -> 192.168.0.101

07/31-15:44:25.378379 [**] [1:1000001:0] "ICMP Detected" [**] [Priority: 0] {ICMP} 192.168.0.101 -> 192.168.0.107

07/31-15:44:26.392734 [**] [1:1000001:0] "ICMP Detected" [**] [Priority: 0] {ICMP} 192.168.0.107 -> 192.168.0.101

07/31-15:44:26.392876 [**] [1:1000001:0] "ICMP Detected" [**] [Priority: 0] {ICMP} 192.168.0.101 -> 192.168.0.107

07/31-15:44:27.404456 [**] [1:1000001:0] "ICMP Detected" [**] [Priority: 0] {ICMP} 192.168.0.107 -> 192.168.0.101

07/31-15:44:27.404696 [**] [1:1000001:0] "ICMP Detected" [**] [Priority: 0] {ICMP} 192.168.0.101 -> 192.168.0.107

07/31-15:44:29.661393 [**] [112:1:1] "(arp_spoof) unicast ARP request" [**] [Priority: 3] {ARP} ->

07/31-15:45:28.219697 [**] [1:1000001:0] "ICMP Detected" [**] [Priority: 0] {ICMP} fe80::a00:27ff:fe45:d497 -> ff02::2

07/31-15:45:35.335144 [**] [116:444:1] "(ipv4) IPv4 option set" [**] [Priority: 3] {IP} 192.168.0.1 -> 224.0.0.1

07/31-15:45:38.826752 [**] [116:444:1] "(ipv4) IPv4 option set" [**] [Priority: 3] {IP} 192.168.0.107 -> 239.255.255.250

07/31-15:45:41.329942 [**] [116:444:1] "(ipv4) IPv4 option set" [**] [Priority: 3] {IP} 192.168.0.107 -> 224.0.0.252

07/31-15:45:41.829154 [**] [116:444:1] "(ipv4) IPv4 option set" [**] [Priority: 3] {IP} 192.168.0.107 -> 224.0.0.251

---

^C** caught int signal

== stopping

-- [0] eth0

Packet Statistics

---

daq

received: 379

analyzed: 379

allow: 379

rx_bytes: 87111

---

codec

total: 379 (100.000%)

other: 1 (0.264%)

arp: 101 (26.649%)

eth: 379 (100.000%)

icmp4: 8 (2.111%)

icmp6: 3 (0.792%)

igmp: 13 (3.430%)

ipv4: 247 (65.172%)

ipv6: 30 (7.916%)

ipv6_hop_opts: 2 (0.528%)

udp: 253 (66.755%)

Module Statistics

---

appid

packets: 277

processed_packets: 277

total_sessions: 27

service_cache_adds: 4

bytes_in_use: 608

items_in_use: 4

---

arp_spoof

packets: 101

---

back_orifice

packets: 253

---

binder

raw_packets: 102

new_flows: 16

inspects: 118

---

detection

analyzed: 379

hard_evals: 11

alerts: 25

total_alerts: 25

logged: 25

---

port_scan

packets: 277

trackers: 23

---

search_engine

qualified_events: 11

---

stream

flows: 16

total_prunes: 6

idle_prunes_proto_timeout: 6

---

stream_icmp

sessions: 3

max: 3

created: 3

released: 3

---

stream_ip

sessions: 6

max: 6

created: 13

released: 13

timeouts: 7

total_bytes: 104

---

stream_udp

```
            sessions: 7
                max: 7
             created: 11
            released: 11
            timeouts: 4
          total_bytes: 69795
--------------------------------------------------
wizard
            udp_scans: 7
           udp_misses: 7
--------------------------------------------------
Appid Statistics
--------------------------------------------------
detected apps and services
          Application: Services  Clients  Users    Payloads  Misc     Referred
              unknown: 7         0        0        0         0        0
--------------------------------------------------
Summary Statistics
--------------------------------------------------
process
            signals: 1
--------------------------------------------------
timing
            runtime: 00:05:16
            seconds: 316.933602
o")~  Snort exiting
```