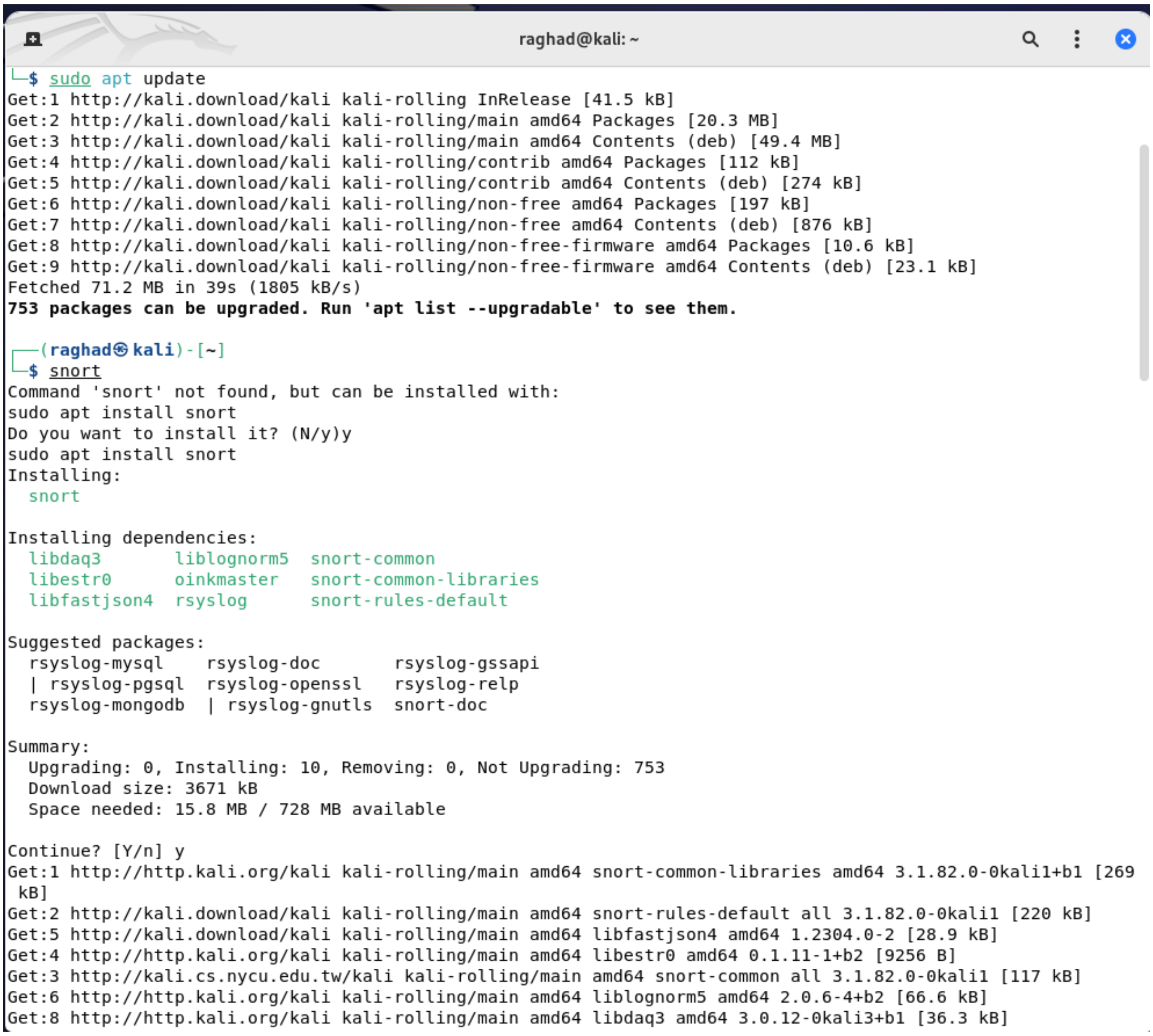
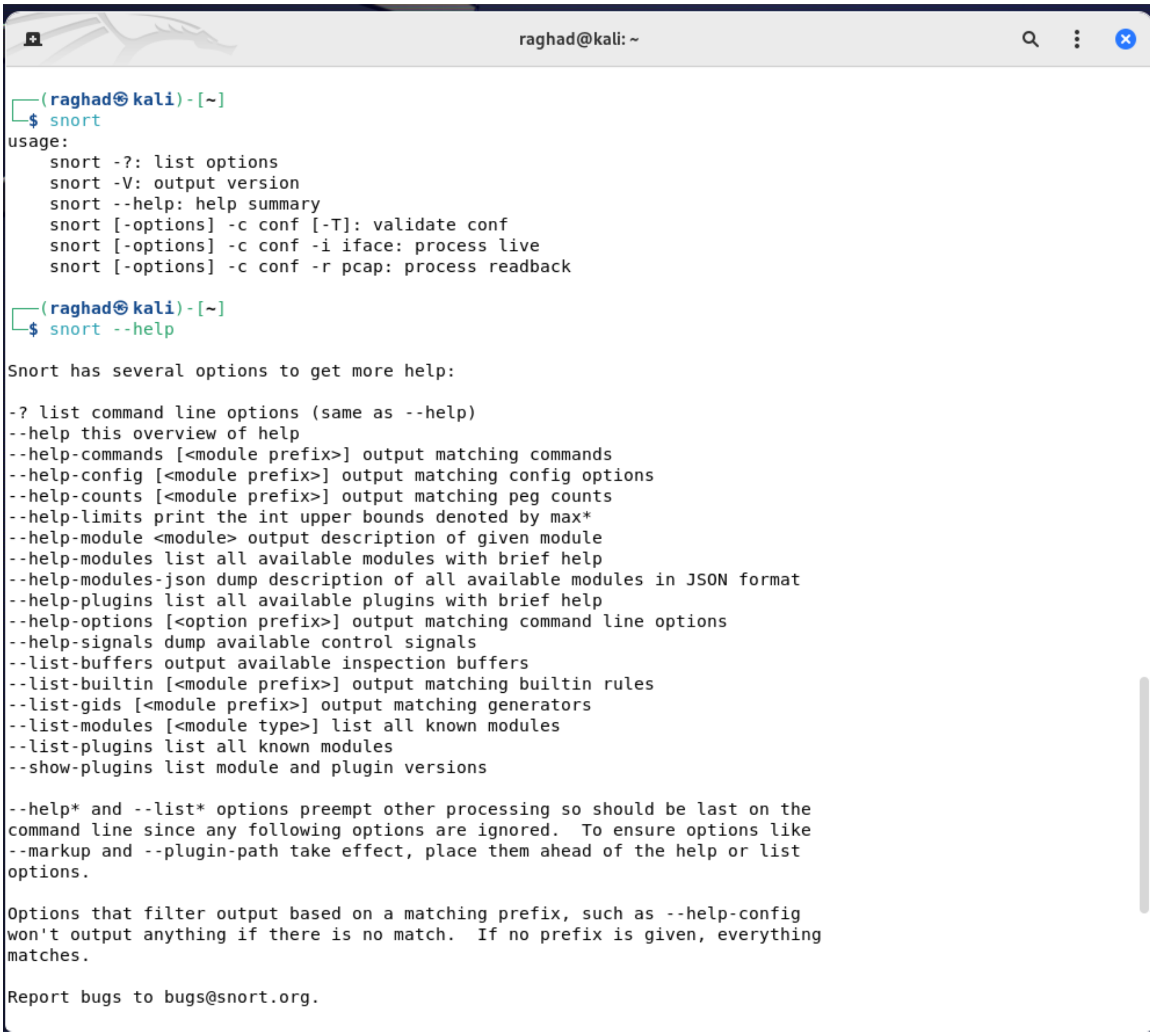
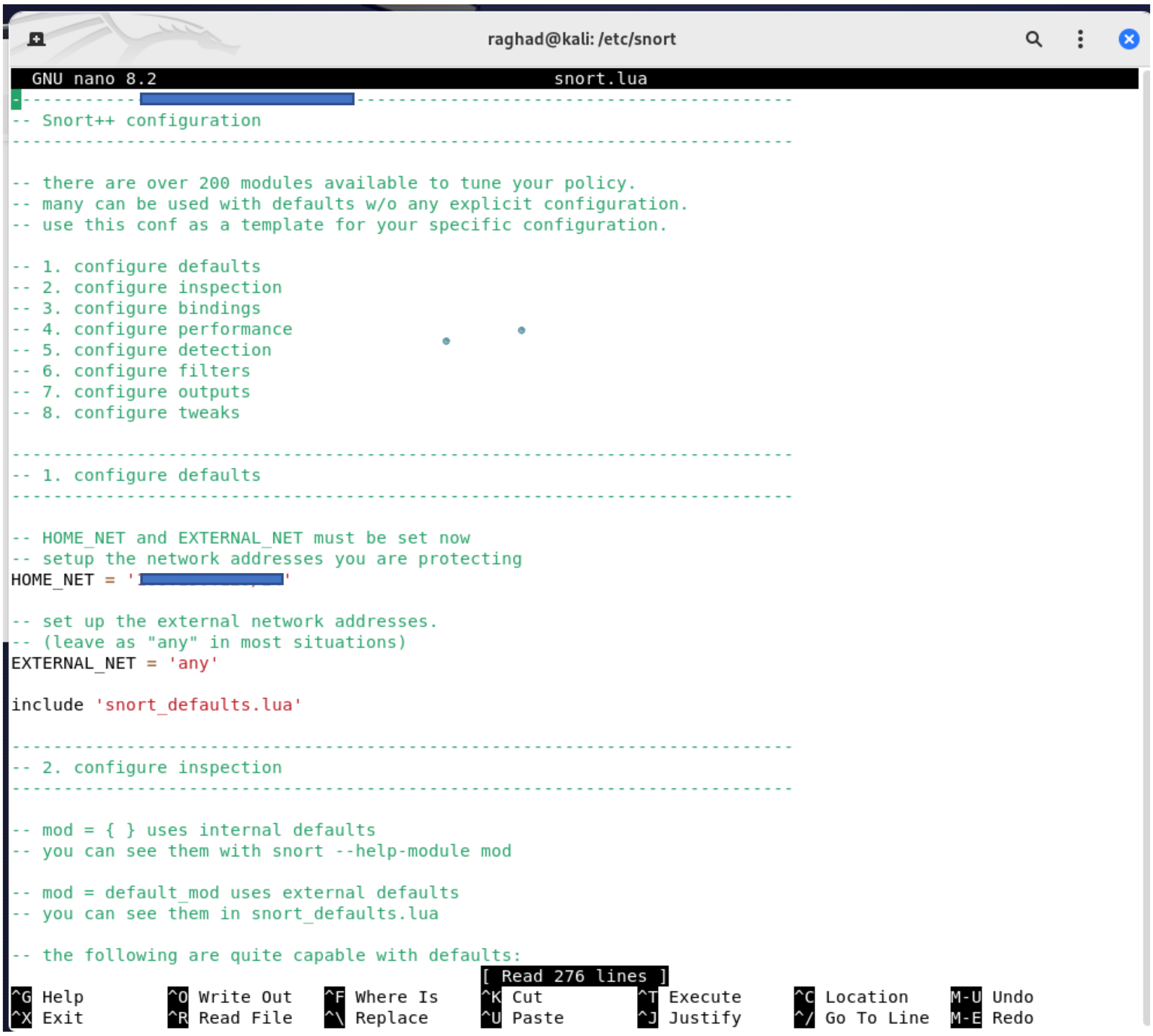


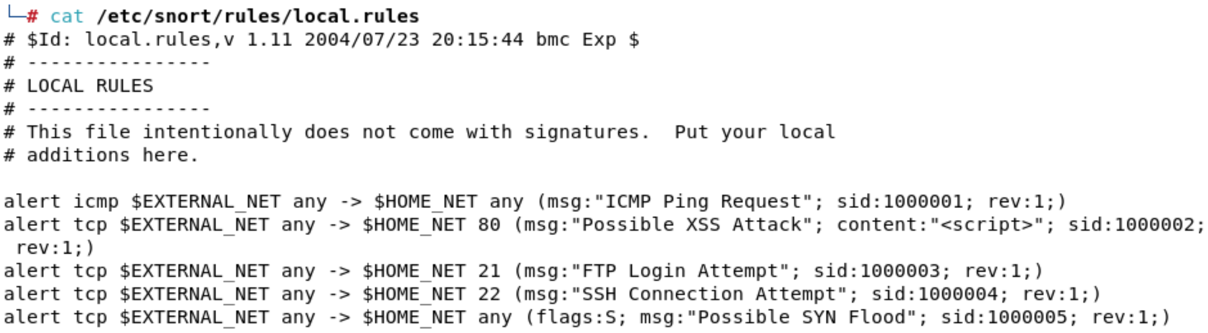
```
└─$ sudo apt update
Get:1 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [20.3 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [49.4 MB]
Get:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [112 kB]
Get:5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [274 kB]
Get:6 http://kali.download/kali kali-rolling/non-free amd64 Packages [197 kB]
Get:7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [876 kB]
Get:8 http://kali.download/kali kali-rolling/non-free-firmware amd64 Packages [10.6 kB]
Get:9 http://kali.download/kali kali-rolling/non-free-firmware amd64 Contents (deb) [23.1 kB]
Fetched 71.2 MB in 39s (1805 kB/s)
753 packages can be upgraded. Run 'apt list --upgradable' to see them.

┌──(raghad㉿kali)-[~]
└─$ snort
Command 'snort' not found, but can be installed with:
sudo apt install snort
Do you want to install it? (N/y)y
sudo apt install snort
Installing:
  snort

Installing dependencies:
  libdaq3       liblognorm5  snort-common
  libestr0      oinkmaster   snort-common-libraries
  libfastjson4  rsyslog      snort-rules-default

Suggested packages:
  rsyslog-mysql    rsyslog-doc       rsyslog-gssapi
  | rsyslog-pgsql  rsyslog-openssl   rsyslog-relp
  rsyslog-mongodb  | rsyslog-gnutls  snort-doc

Summary:
  Upgrading: 0, Installing: 10, Removing: 0, Not Upgrading: 753
  Download size: 3671 kB
  Space needed: 15.8 MB / 728 MB available

Continue? [Y/n] y
Get:1 http://http.kali.org/kali kali-rolling/main amd64 snort-common-libraries amd64 3.1.82.0-0kali1+b1 [269
 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 snort-rules-default all 3.1.82.0-0kali1 [220 kB]
Get:5 http://kali.download/kali kali-rolling/main amd64 libfastjson4 amd64 1.2304.0-2 [28.9 kB]
Get:4 http://http.kali.org/kali kali-rolling/main amd64 libestr0 amd64 0.1.11-1+b2 [9256 B]
Get:3 http://kali.cs.nycu.edu.tw/kali kali-rolling/main amd64 snort-common all 3.1.82.0-0kali1 [117 kB]
Get:6 http://http.kali.org/kali kali-rolling/main amd64 liblognorm5 amd64 2.0.6-4+b2 [66.6 kB]
Get:8 http://http.kali.org/kali kali-rolling/main amd64 libdaq3 amd64 3.0.12-0kali3+b1 [36.3 kB]
```



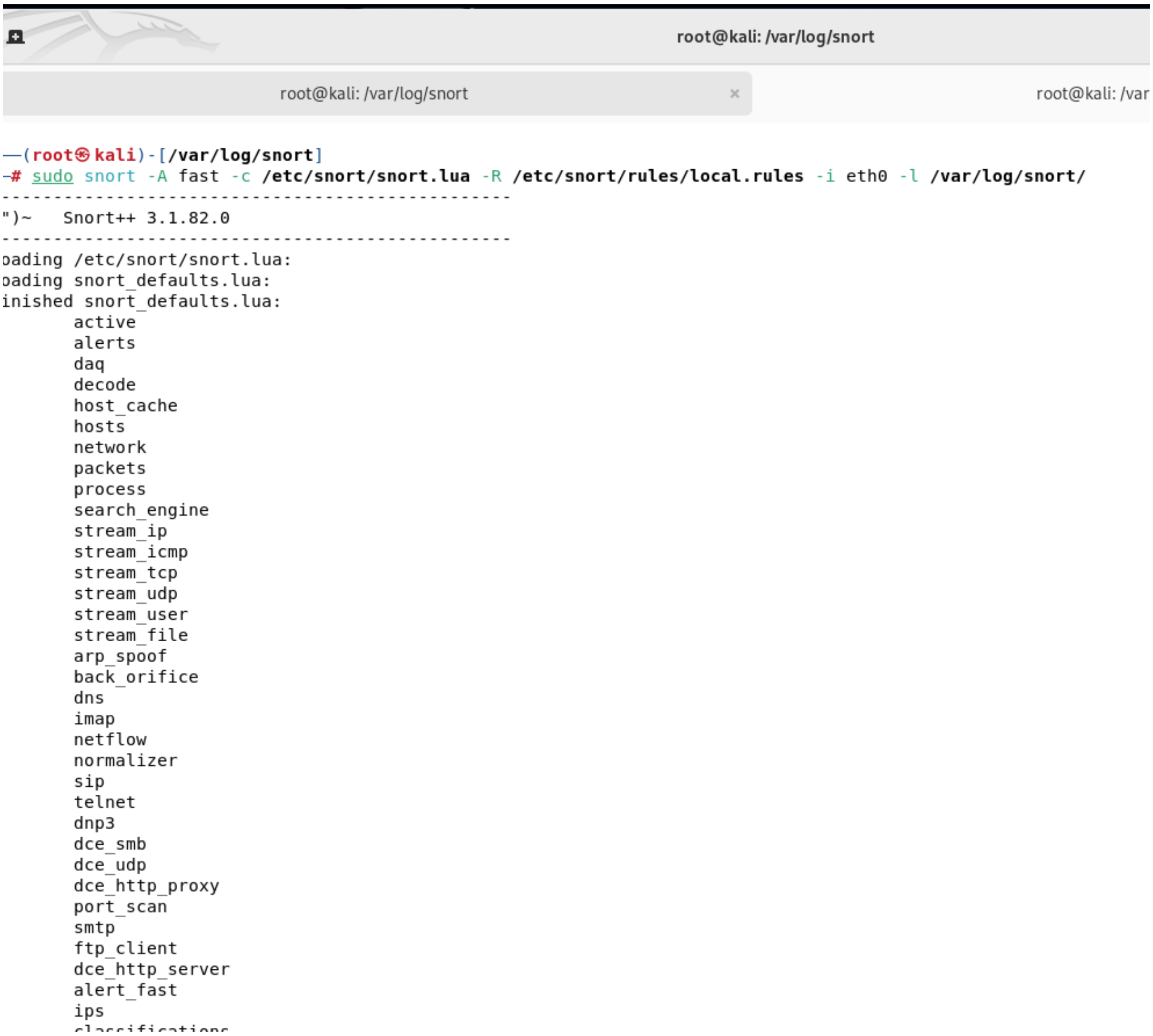
```
┌──(raghad㉿kali)-[~]
└─$ snort
usage:
    snort -?: list options
    snort -V: output version
    snort --help: help summary
    snort [-options] -c conf [-T]: validate conf
    snort [-options] -c conf -i iface: process live
    snort [-options] -c conf -r pcap: process readback

┌──(raghad㉿kali)-[~]
└─$ snort --help

Snort has several options to get more help:

-? list command line options (same as --help)
--help this overview of help
--help-commands [<module prefix>] output matching commands
--help-config [<module prefix>] output matching config options
--help-counts [<module prefix>] output matching peg counts
--help-limits print the int upper bounds denoted by max*
--help-module <module> output description of given module
--help-modules list all available modules with brief help
--help-modules-json dump description of all available modules in JSON format
--help-plugins list all available plugins with brief help
--help-options [<option prefix>] output matching command line options
--help-signals dump available control signals
--list-buffers output available inspection buffers
--list-builtin [<module prefix>] output matching builtin rules
--list-gids [<module prefix>] output matching generators
--list-modules [<module type>] list all known modules
--list-plugins list all known modules
--show-plugins list module and plugin versions

--help* and --list* options preempt other processing so should be last on the
command line since any following options are ignored.  To ensure options like
--markup and --plugin-path take effect, place them ahead of the help or list
options.

Options that filter output based on a matching prefix, such as --help-config
won't output anything if there is no match.  If no prefix is given, everything
matches.

Report bugs to bugs@snort.org.
```



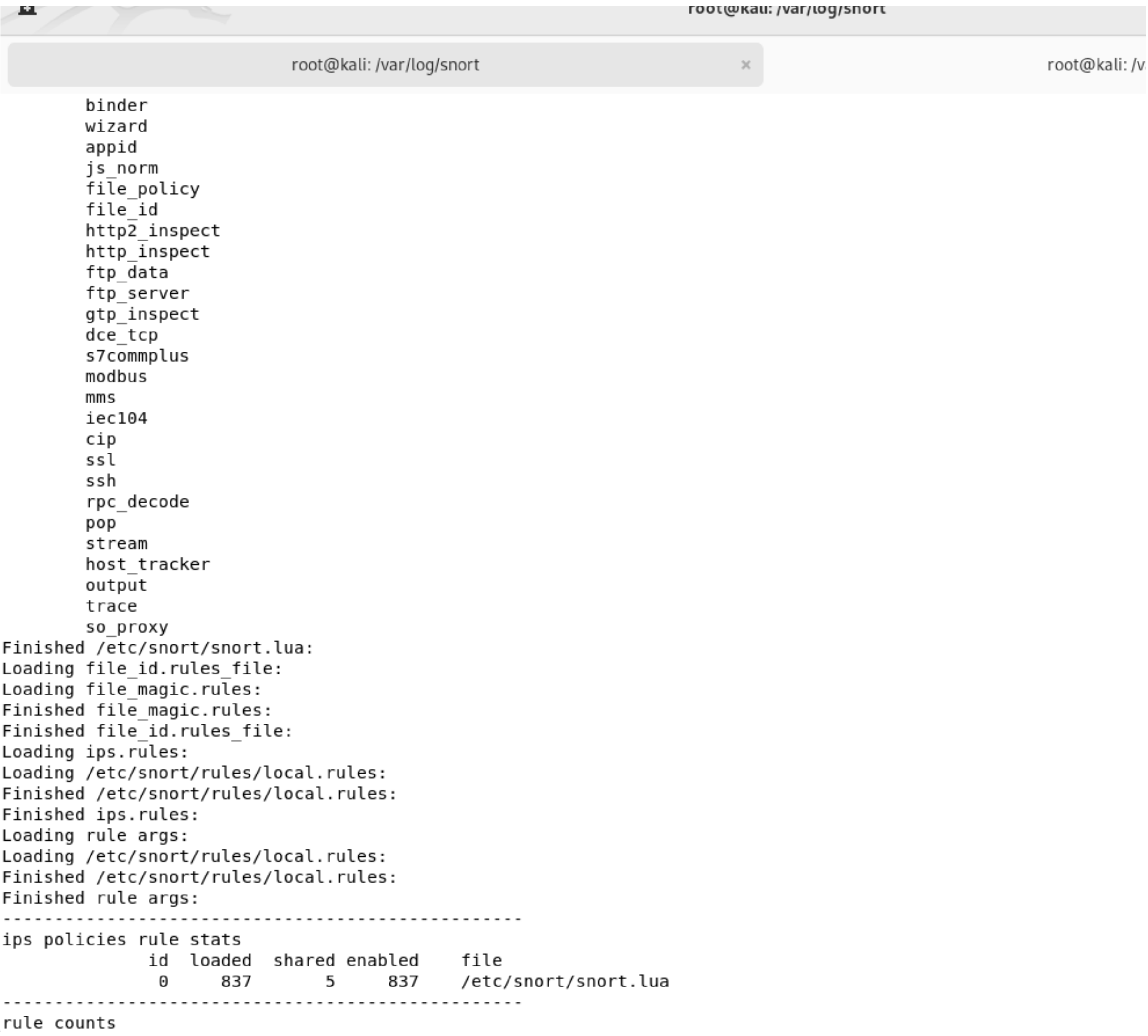
```
 GNU nano 8.2                                    snort.lua
------------[redacted]------------------------------------------
-- Snort++ configuration
---------------------------------------------------------------------------

-- there are over 200 modules available to tune your policy.
-- many can be used with defaults w/o any explicit configuration.
-- use this conf as a template for your specific configuration.

-- 1. configure defaults
-- 2. configure inspection
-- 3. configure bindings
-- 4. configure performance
-- 5. configure detection
-- 6. configure filters
-- 7. configure outputs
-- 8. configure tweaks

---------------------------------------------------------------------------
-- 1. configure defaults
---------------------------------------------------------------------------

-- HOME_NET and EXTERNAL_NET must be set now
-- setup the network addresses you are protecting
HOME_NET = '[redacted]'

-- set up the external network addresses.
-- (leave as "any" in most situations)
EXTERNAL_NET = 'any'

include 'snort_defaults.lua'

---------------------------------------------------------------------------
-- 2. configure inspection
---------------------------------------------------------------------------

-- mod = { } uses internal defaults
-- you can see them with snort --help-module mod

-- mod = default_mod uses external defaults
-- you can see them in snort_defaults.lua

-- the following are quite capable with defaults:
                                        [ Read 276 lines ]
^G Help         ^O Write Out    ^F Where Is     ^K Cut          ^T Execute      ^C Location     M-U Undo
^X Exit         ^R Read File    ^\ Replace      ^U Paste        ^J Justify      ^/ Go To Line   M-E Redo
```



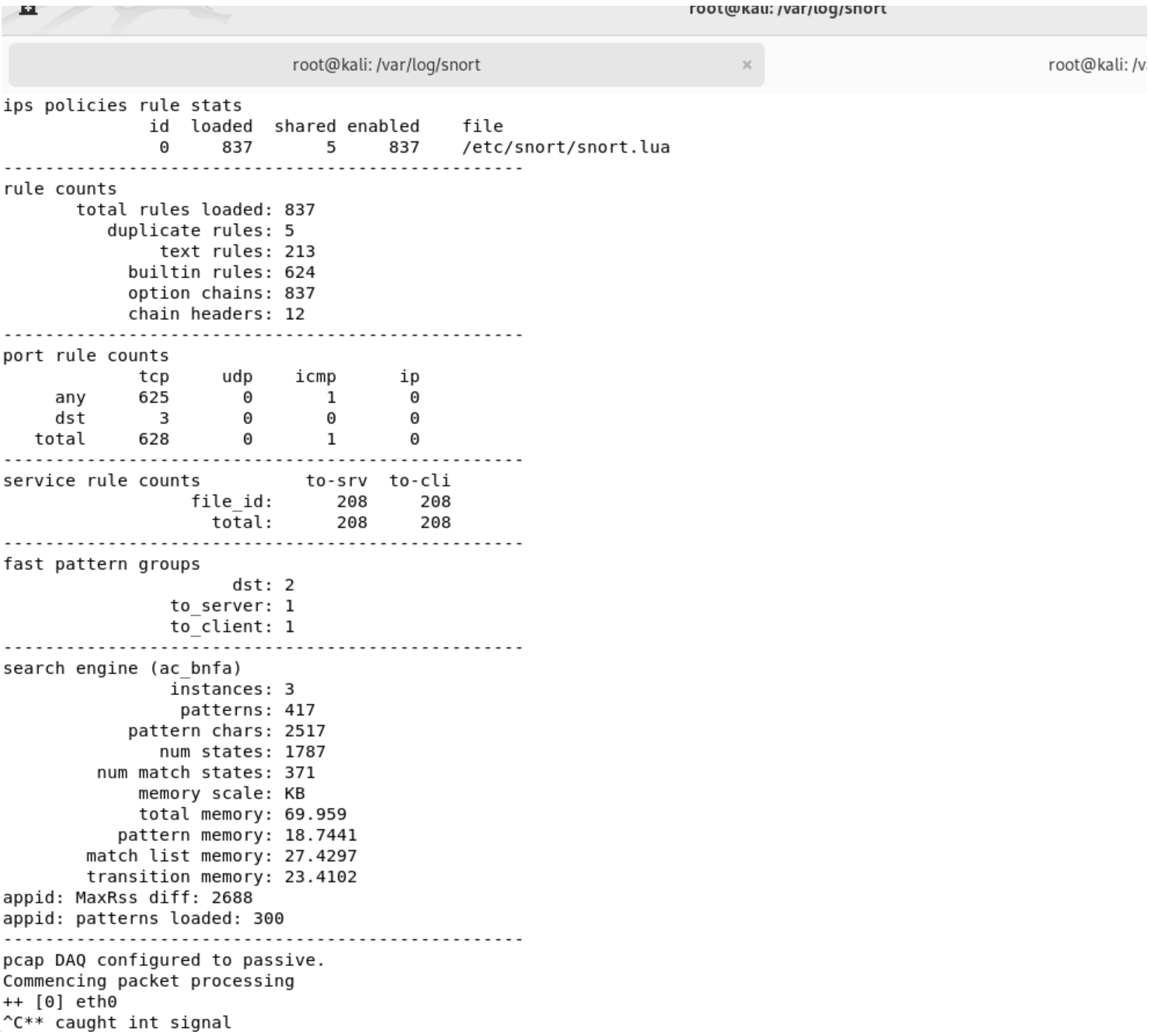
```
└─# cat /etc/snort/rules/local.rules
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
# ----------------
# LOCAL RULES
# ----------------
# This file intentionally does not come with signatures.  Put your local
# additions here.

alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Ping Request"; sid:1000001; rev:1;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 80 (msg:"Possible XSS Attack"; content:"<script>"; sid:1000002;
 rev:1;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP Login Attempt"; sid:1000003; rev:1;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 22 (msg:"SSH Connection Attempt"; sid:1000004; rev:1;)
alert tcp $EXTERNAL_NET any -> $HOME_NET any (flags:S; msg:"Possible SYN Flood"; sid:1000005; rev:1;)
```



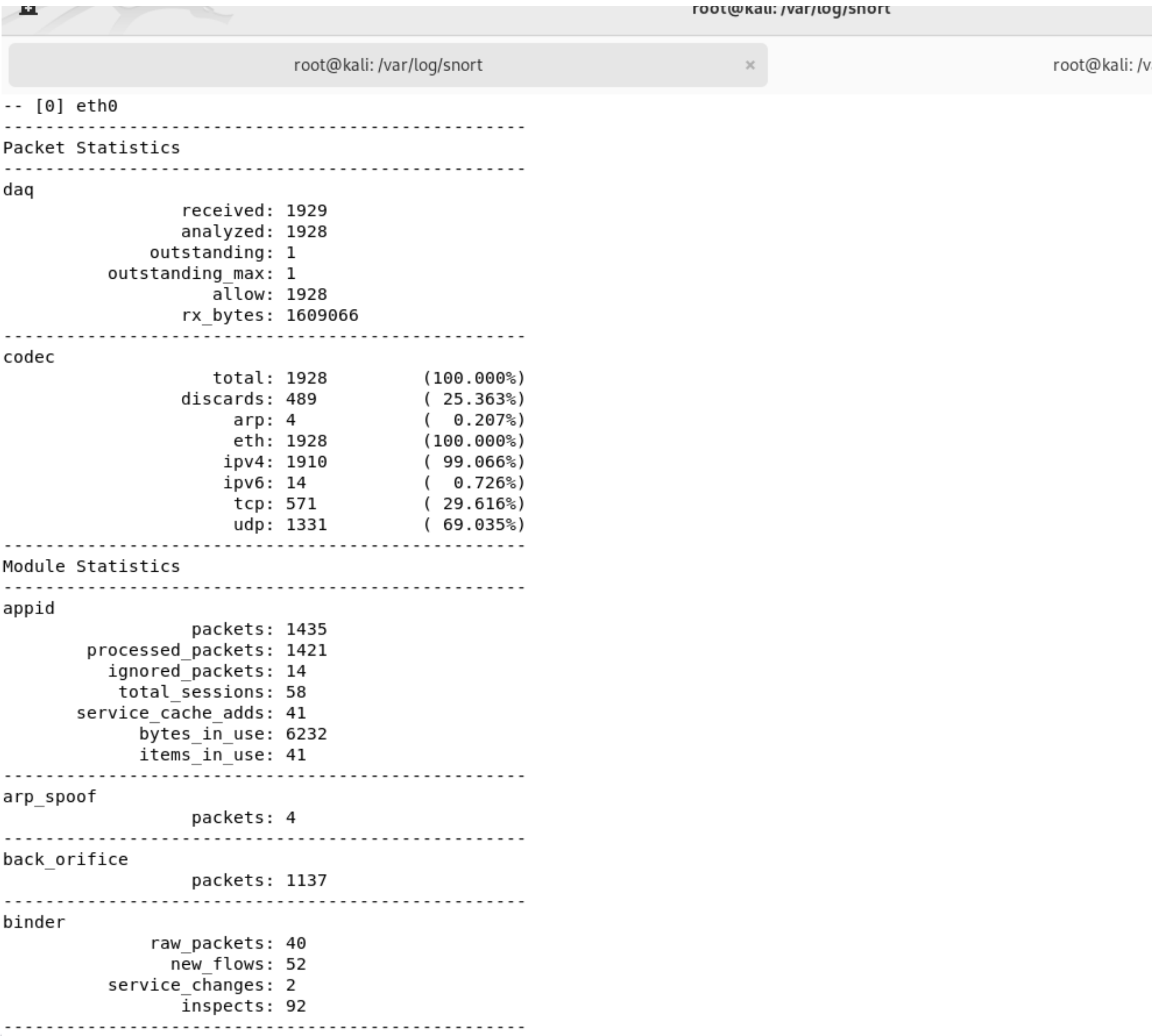
```
—(root㉿kali)-[/var/log/snort]
-# sudo snort -A fast -c /etc/snort/snort.lua -R /etc/snort/rules/local.rules -i eth0 -l /var/log/snort/
--------------------------------------------------
")~   Snort++ 3.1.82.0
--------------------------------------------------
oading /etc/snort/snort.lua:
oading snort_defaults.lua:
inished snort_defaults.lua:
       active
       alerts
       daq
       decode
       host_cache
       hosts
       network
       packets
       process
       search_engine
       stream_ip
       stream_icmp
       stream_tcp
       stream_udp
       stream_user
       stream_file
       arp_spoof
       back_orifice
       dns
       imap
       netflow
       normalizer
       sip
       telnet
       dnp3
       dce_smb
       dce_udp
       dce_http_proxy
       port_scan
       smtp
       ftp_client
       dce_http_server
       alert_fast
       ips
       classifications
```



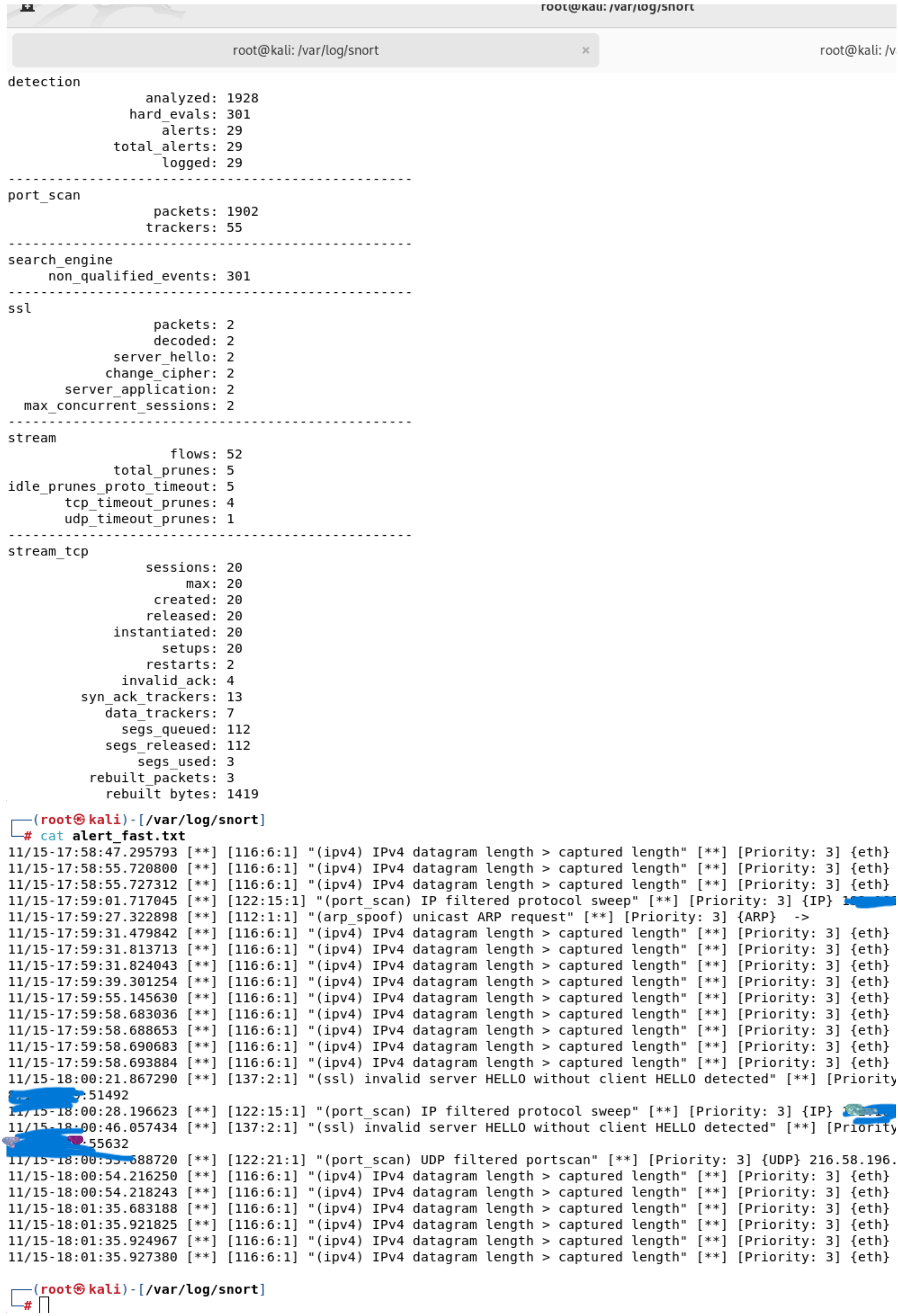
```
        binder
        wizard
        appid
        js_norm
        file_policy
        file_id
        http2_inspect
        http_inspect
        ftp_data
        ftp_server
        gtp_inspect
        dce_tcp
        s7commplus
        modbus
        mms
        iec104
        cip
        ssl
        ssh
        rpc_decode
        pop
        stream
        host_tracker
        output
        trace
        so_proxy
Finished /etc/snort/snort.lua:
Loading file_id.rules_file:
Loading file_magic.rules:
Finished file_magic.rules:
Finished file_id.rules_file:
Loading ips.rules:
Loading /etc/snort/rules/local.rules:
Finished /etc/snort/rules/local.rules:
Finished ips.rules:
Loading rule args:
Loading /etc/snort/rules/local.rules:
Finished /etc/snort/rules/local.rules:
Finished rule args:
--------------------------------------------------
ips policies rule stats
              id  loaded  shared enabled    file
               0     837       5     837    /etc/snort/snort.lua
--------------------------------------------------
rule counts
```



```
ips policies rule stats
              id  loaded  shared enabled    file
               0     837       5     837    /etc/snort/snort.lua
--------------------------------------------------
rule counts
       total rules loaded: 837
          duplicate rules: 5
               text rules: 213
            builtin rules: 624
            option chains: 837
            chain headers: 12
--------------------------------------------------
port rule counts
             tcp     udp    icmp      ip
     any     625       0       1       0
     dst       3       0       0       0
   total     628       0       1       0
--------------------------------------------------
service rule counts          to-srv  to-cli
                  file_id:      208     208
                    total:      208     208
--------------------------------------------------
fast pattern groups
                      dst: 2
                to_server: 1
                to_client: 1
--------------------------------------------------
search engine (ac_bnfa)
                instances: 3
                 patterns: 417
            pattern chars: 2517
               num states: 1787
         num match states: 371
             memory scale: KB
             total memory: 69.959
           pattern memory: 18.7441
        match list memory: 27.4297
        transition memory: 23.4102
appid: MaxRss diff: 2688
appid: patterns loaded: 300
--------------------------------------------------
pcap DAQ configured to passive.
Commencing packet processing
++ [0] eth0
^C** caught int signal
```



```
-- [0] eth0
--------------------------------------------------
Packet Statistics
--------------------------------------------------
daq
                 received: 1929
                 analyzed: 1928
              outstanding: 1
          outstanding_max: 1
                    allow: 1928
                 rx_bytes: 1609066
--------------------------------------------------
codec
                    total: 1928         (100.000%)
                 discards: 489          ( 25.363%)
                      arp: 4            (  0.207%)
                      eth: 1928         (100.000%)
                     ipv4: 1910         ( 99.066%)
                     ipv6: 14           (  0.726%)
                      tcp: 571          ( 29.616%)
                      udp: 1331         ( 69.035%)
--------------------------------------------------
Module Statistics
--------------------------------------------------
appid
                  packets: 1435
        processed_packets: 1421
          ignored_packets: 14
           total_sessions: 58
       service_cache_adds: 41
             bytes_in_use: 6232
             items_in_use: 41
--------------------------------------------------
arp_spoof
                  packets: 4
--------------------------------------------------
back_orifice
                  packets: 1137
--------------------------------------------------
binder
              raw_packets: 40
                new_flows: 52
          service_changes: 2
                 inspects: 92
--------------------------------------------------
```



```
detection
                 analyzed: 1928
               hard_evals: 301
                   alerts: 29
             total_alerts: 29
                   logged: 29
--------------------------------------------------
port_scan
                  packets: 1902
                 trackers: 55
--------------------------------------------------
search_engine
     non_qualified_events: 301
--------------------------------------------------
ssl
                  packets: 2
                  decoded: 2
             server_hello: 2
            change_cipher: 2
       server_application: 2
  max_concurrent_sessions: 2
--------------------------------------------------
stream
                    flows: 52
             total_prunes: 5
idle_prunes_proto_timeout: 5
       tcp_timeout_prunes: 4
       udp_timeout_prunes: 1
--------------------------------------------------
stream_tcp
                 sessions: 20
                      max: 20
                  created: 20
                 released: 20
             instantiated: 20
                   setups: 20
                 restarts: 2
              invalid_ack: 4
         syn_ack_trackers: 13
            data_trackers: 7
              segs_queued: 112
            segs_released: 112
                segs_used: 3
          rebuilt_packets: 3
            rebuilt bytes: 1419

┌──(root㉿kali)-[/var/log/snort]
└─# cat alert_fast.txt
11/15-17:58:47.295793 [**] [116:6:1] "(ipv4) IPv4 datagram length > captured length" [**] [Priority: 3] {eth}
11/15-17:58:55.720800 [**] [116:6:1] "(ipv4) IPv4 datagram length > captured length" [**] [Priority: 3] {eth}
11/15-17:58:55.727312 [**] [116:6:1] "(ipv4) IPv4 datagram length > captured length" [**] [Priority: 3] {eth}
11/15-17:59:01.717045 [**] [122:15:1] "(port_scan) IP filtered protocol sweep" [**] [Priority: 3] {IP} [redacted]
11/15-17:59:27.322898 [**] [112:1:1] "(arp_spoof) unicast ARP request" [**] [Priority: 3] {ARP}  ->
11/15-17:59:31.479842 [**] [116:6:1] "(ipv4) IPv4 datagram length > captured length" [**] [Priority: 3] {eth}
11/15-17:59:31.813713 [**] [116:6:1] "(ipv4) IPv4 datagram length > captured length" [**] [Priority: 3] {eth}
11/15-17:59:31.824043 [**] [116:6:1] "(ipv4) IPv4 datagram length > captured length" [**] [Priority: 3] {eth}
11/15-17:59:39.301254 [**] [116:6:1] "(ipv4) IPv4 datagram length > captured length" [**] [Priority: 3] {eth}
11/15-17:59:55.145630 [**] [116:6:1] "(ipv4) IPv4 datagram length > captured length" [**] [Priority: 3] {eth}
11/15-17:59:58.683036 [**] [116:6:1] "(ipv4) IPv4 datagram length > captured length" [**] [Priority: 3] {eth}
11/15-17:59:58.688653 [**] [116:6:1] "(ipv4) IPv4 datagram length > captured length" [**] [Priority: 3] {eth}
11/15-17:59:58.690683 [**] [116:6:1] "(ipv4) IPv4 datagram length > captured length" [**] [Priority: 3] {eth}
11/15-17:59:58.693884 [**] [116:6:1] "(ipv4) IPv4 datagram length > captured length" [**] [Priority: 3] {eth}
11/15-18:00:21.867290 [**] [137:2:1] "(ssl) invalid server HELLO without client HELLO detected" [**] [Priority
[redacted]:51492
11/15-18:00:28.196623 [**] [122:15:1] "(port_scan) IP filtered protocol sweep" [**] [Priority: 3] {IP} [redacted]
11/15-18:00:46.057434 [**] [137:2:1] "(ssl) invalid server HELLO without client HELLO detected" [**] [Priority
[redacted]:55632
688720 [**] [122:21:1] "(port_scan) UDP filtered portscan" [**] [Priority: 3] {UDP} 216.58.196.
11/15-18:00:54.216250 [**] [116:6:1] "(ipv4) IPv4 datagram length > captured length" [**] [Priority: 3] {eth}
11/15-18:00:54.218243 [**] [116:6:1] "(ipv4) IPv4 datagram length > captured length" [**] [Priority: 3] {eth}
11/15-18:01:35.683188 [**] [116:6:1] "(ipv4) IPv4 datagram length > captured length" [**] [Priority: 3] {eth}
11/15-18:01:35.921825 [**] [116:6:1] "(ipv4) IPv4 datagram length > captured length" [**] [Priority: 3] {eth}
11/15-18:01:35.924967 [**] [116:6:1] "(ipv4) IPv4 datagram length > captured length" [**] [Priority: 3] {eth}
11/15-18:01:35.927380 [**] [116:6:1] "(ipv4) IPv4 datagram length > captured length" [**] [Priority: 3] {eth}

┌──(root㉿kali)-[/var/log/snort]
└─#
```