C&NS Lab Assignment 14

Onkar Santosh Gavali (2019BTECS00037)

Batch B2

Index

Snort

- Explain Intrusion Detection System.
- Implement Intrusion Detection System using snort.

Intrusion Detection System

SNORT

Snort is the world's foremost Open Source Intrusion Prevention System (IPS). Snort IPS uses a series of rules that help define malicious network activity and uses those rules to find packets that match against them and generates alerts for users. Snort can be deployed inline to stop these packets, as well. Snort has three primary uses: As a packet sniffer like tcpdump, as a packet logger — which is useful for network traffic debugging or can be used as a full-blown network intrusion prevention system. Snort can be downloaded and configured for personal and business use alike.

Snort

Snort is an open source and popular Intrusion Detection System (IDS). It works by actively monitoring of network traffic parsing each packet and alerting system administrator of any anomalous behavior that goes against the snort rules configured by the administrator according to the security policies of an organization.

Install snort in windows:

https://zaeemjaved10.medium.com/installing-configuring-snort-2-9-17-on-windows-10-26f73e342780

Snort installed

Output

Step 1:

Install winpcap ,npcap and snort and snort rules same version

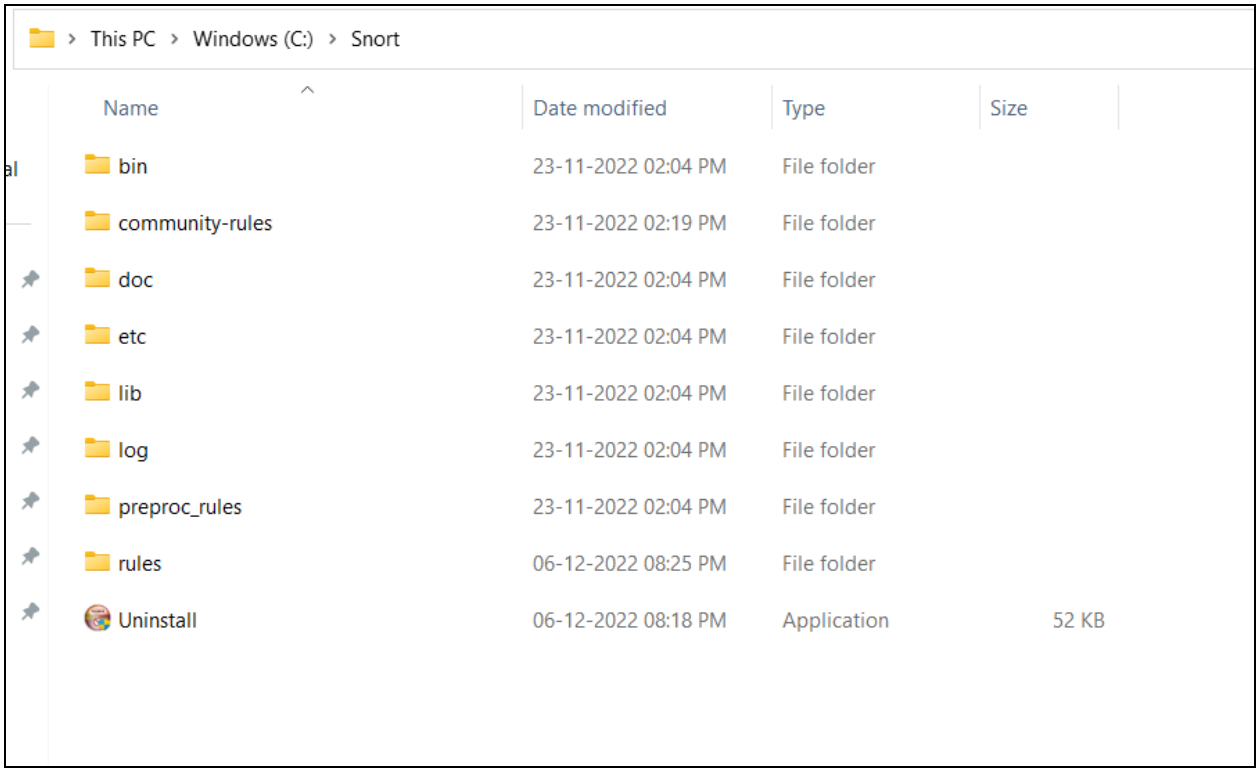
https://www.winpcap.org/install/

https://npcap.com/#download

https://snort.org/downloads

https://snort.org/downloads#rules

Unzip the rules and replaces rules and preproc_rules folder



Go to file

"C:\Snort\etc\snort.conf"

Go to line 45

Change “any” to your network address

```
# Step #1: Set the network variables.  For more information, see READM
##################################################

# Setup the network addresses you are protecting
ipvar HOME_NET any

# Set up the external network addresses. Leave as "any" in most situat
ipvar EXTERNAL_NET any

# List of DNS servers on your network
```

Our network

```
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Default Gateway . . . . . . . . . : fe80::b6a7:c6ff:fe7d:2fbc%20
                                    192.168.29.1
```

Changed to

```
# Step #1: Set the network variables.  For more information, se
##################################################

# Setup the network addresses you are protecting
ipvar HOME_NET 192.168.29.0/24

# Set up the external network addresses. Leave as "any" in most
ipvar EXTERNAL_NET any
```

Change external network value to !$HOME_NET

```
# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET any

# List of DNS servers on your network
```

```
# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET !$HOME_NET
```

Change path

```
# Path to your rules files (this can be a relative path)
# Note for Windows users:  You are advised to make this an absolute path,
# such as:  c:\snort\rules
var RULE_PATH ../rules
var SO_RULE_PATH ../so_rules
var PREPROC_RULE_PATH ../preproc_rules

# If you are using reputation preprocessor set these
# Currently there is a bug with relative paths, they are relative to where snort is
# not relative to snort.conf like the above variables
# This is completely inconsistent with how other vars work, BUG 89986
# Set the absolute path appropriately
var WHITE_LIST_PATH ../rules
var BLACK_LIST_PATH ../rules
```

To

```
# Path to your rules files (this can be a relative path)
# Note for Windows users:  You are advised to make this an absolute path,
# such as:  c:\snort\rules
var RULE_PATH c:\Snort\rules
# var SO_RULE_PATH ../so_rules
var PREPROC_RULE_PATH c:\Snort\preproc_rules

# If you are using reputation preprocessor set these
# Currently there is a bug with relative paths, they are relative to where snort is
# not relative to snort.conf like the above variables
# This is completely inconsistent with how other vars work, BUG 89986
# Set the absolute path appropriately
var WHITE_LIST_PATH c:\Snort\rules
var BLACK_LIST_PATH c:\Snort\rules
```

Find lofdir

```
# Configure default log directory for snort to log to.  For more information see snort -h command line options (-l)
#
# config logdir:
```

And change it to

```
# Configure default log directory for snort to log to.  For more information see snort -h command line options (-l)
#
config logdir: C:\Snort\log
```

```
# path to dynamic preprocessor libraries
dynamicpreprocessor directory /usr/local/lib/snort_dynamicpreprocessor/

# path to base preprocessor engine
dynamicengine /usr/local/lib/snort_dynamicengine/libsf_engine.so

# path to dynamic rules libraries
dynamicdetection directory /usr/local/lib/snort_dynamicrules
```

Change it to

```
# path to dynamic preprocessor libraries
dynamicpreprocessor directory C:\Snort\lib\snort_dynamicpreprocessor

# path to base preprocessor engine
dynamicengine C:\Snort\lib\snort_dynamicengine\sf_engine.dll

# path to dynamic rules libraries
# dynamicdetection directory /usr/local/lib/snort_dynamicrules
```

Comment lines from 265 to 269,335

```
# Inline packet normalization. For more information, see README.normalize
# Does nothing in IDS mode
# preprocessor normalize_ip4
# preprocessor normalize_tcp: ips ecn stream
# preprocessor normalize_icmp4
# preprocessor normalize_ip6
# preprocessor normalize_icmp6
```

```
# Back Orifice detection.
# preprocessor bo
```

Uncomment the line 418

```
    xlink2state { enabled }

# Portscan detection.  For more information, see README.sfportscan
preprocessor sfportscan: proto  { all } memcap { 10000000 } sense_level { low }

# ARP spoof detection.  For more information, see the Snort Manual - Configuring Snort - Preprocessors
```

Now got line 507

```
    check_crc

# Reputation preprocessor. For more information see README.reputation
preprocessor reputation: \
    memcap 500, \
    priority whitelist, \
    nested_ip inner, \
    whitelist $WHITE_LIST_PATH/white_list.rules, \
    blacklist $BLACK_LIST_PATH/black_list.rules
```

Here if we search blacklist.rules file in c:/snort/rules/ folder

We can find it but whitelist.rules file is missing

So we just need to create one

snort.conf | blacklist.rules | whitelist.rules

C: > Snort > rules > blacklist.rules

```
# Copyright 2001-2022 Sourcefire, Inc. All Rights Reserved.
#
# This file contains (i) proprietary rules that were created, tested and certified by
# Sourcefire, Inc. (the "VRT Certified Rules") that are distributed under the VRT
# Certified Rules License Agreement (v 2.0), and (ii) rules that were created by
# Sourcefire and other third parties (the "GPL Rules") that are distributed under the
# GNU General Public License (GPL), v2.
#
# The VRT Certified Rules are owned by Sourcefire, Inc. The GPL Rules were created
# by Sourcefire and other third parties. The GPL Rules created by Sourcefire are
# owned by Sourcefire, Inc., and the GPL Rules not created by Sourcefire are owned by
# their respective creators. Please see http://www.snort.org/snort/snort-team/ for a
# list of third party owners and their respective copyrights.
#
# In order to determine what rules are VRT Certified Rules or GPL Rules, please refer
# to the VRT Certified Rules License Agreement (v2.0).
#
#----------------
# BLACKLIST RULES
#----------------

```

And create whitelist.rules

snort.conf | blacklist.rules | whitelist.rules

C: > Snort > rules > whitelist.rules > # WHITELIST RULES

```
# Copyright 2001-2022 Sourcefire, Inc. All Rights Reserved.
#
# This file contains (i) proprietary rules that were created, tested and certified by
# Sourcefire, Inc. (the "VRT Certified Rules") that are distributed under the VRT
# Certified Rules License Agreement (v 2.0), and (ii) rules that were created by
# Sourcefire and other third parties (the "GPL Rules") that are distributed under the
# GNU General Public License (GPL), v2.
#
# The VRT Certified Rules are owned by Sourcefire, Inc. The GPL Rules were created
# by Sourcefire and other third parties. The GPL Rules created by Sourcefire are
# owned by Sourcefire, Inc., and the GPL Rules not created by Sourcefire are owned by
# their respective creators. Please see http://www.snort.org/snort/snort-team/ for a
# list of third party owners and their respective copyrights.
#
# In order to determine what rules are VRT Certified Rules or GPL Rules, please refer
# to the VRT Certified Rules License Agreement (v2.0).
#
#----------------
# WHITELIST RULES
#----------------
```

Also made changes in snort.conf

```
505
506 # Reputation preprocessor. For more information see README.reputation
507 preprocessor reputation: \
508    memcap 500, \
509    priority whitelist, \
510    nested_ip inner, \
511    whitelist $WHITE_LIST_PATH\whitelist.rules, \
512    blacklist $BLACK_LIST_PATH\blacklist.rules
513
```

From line no 546 to 651

Change every / with \

```
# site specific rules
include $RULE_PATH\local.rules

include $RULE_PATH\app-detect.rules
include $RULE_PATH\attack-responses.rules
include $RULE_PATH\backdoor.rules
include $RULE_PATH\bad-traffic.rules
include $RULE_PATH\blacklist.rules
include $RULE_PATH\botnet-cnc.rules
include $RULE_PATH\browser-chrome.rules
include $RULE_PATH\browser-firefox.rules
include $RULE_PATH\browser-ie.rules
include $RULE_PATH\browser-other.rules
include $RULE_PATH\browser-plugins.rules
include $RULE_PATH\browser-webkit.rules
include $RULE_PATH\chat.rules
include $RULE_PATH\content-replace.rules
include $RULE_PATH\ddos.rules
include $RULE_PATH\dns.rules
include $RULE_PATH\dos.rules
include $RULE_PATH\experimental.rules
```

```
include $RULE_PATH\telnet.rules
include $RULE_PATH\tftp.rules
include $RULE_PATH\virus.rules
include $RULE_PATH\voip.rules
include $RULE_PATH\web-activex.rules
include $RULE_PATH\web-attacks.rules
include $RULE_PATH\web-cgi.rules
include $RULE_PATH\web-client.rules
include $RULE_PATH\web-coldfusion.rules
include $RULE_PATH\web-frontpage.rules
include $RULE_PATH\web-iis.rules
include $RULE_PATH\web-misc.rules
include $RULE_PATH\web-php.rules
include $RULE_PATH\x11.rules

##################################################
```

Fromm line 659 to 661 uncomment lines and use \ in directory path

```
656  ##################################################
657
658  # decoder and preprocessor event rules
659  include $PREPROC_RULE_PATH\preprocessor.rules
660  include $PREPROC_RULE_PATH\decoder.rules
661  include $PREPROC_RULE_PATH\sensitive-data.rules
662
663  ##################################################
```

```
Administrator: Command Prompt

C:\Snort\bin>snort -V

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.20-WIN64 GRE (Build 82)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using PCRE version: 8.10 2010-06-25
           Using ZLIB version: 1.2.11
```

snort -i 1 -c C:\Snort\etc\snort.conf -T

```
Administrator: Command Prompt

C:\Snort\bin>snort -i 1 -c C:\Snort\etc\snort.conf -T
Running in Test mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "C:\Snort\etc\snort.conf"
PortVar 'HTTP_PORTS' defined :  [ 80:81 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 3702 4343 4848 5250 6988 7000:7001 71
44:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091 9443
 9999 11371 34443:34444 41080 50002 55555 ]
PortVar 'SHELLCODE_PORTS' defined :  [ 0:79 81:65535 ]
PortVar 'ORACLE_PORTS' defined :  [ 1024:65535 ]
PortVar 'SSH_PORTS' defined :  [ 22 ]
PortVar 'FTP_PORTS' defined :  [ 21 2100 3535 ]
PortVar 'SIP_PORTS' defined :  [ 5060:5061 5600 ]
PortVar 'FILE_DATA_PORTS' defined :  [ 80:81 110 143 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 3702 4343 4848 5250 6988
 7000:7001 7144:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300 8800 8888 8899 9000 9060 9080 9
090:9091 9443 9999 11371 34443:34444 41080 50002 55555 ]
PortVar 'GTP_PORTS' defined :  [ 2123 2152 3386 ]
Detection:
   Search-Method = AC-Full-Q
    Split Any/Any group = enabled
    Search-Method-Optimizations = enabled
    Maximum pattern length = 20
Tagged Packet Limit: 256
Loading dynamic engine C:\Snort\lib\snort_dynamicengine\sf_engine.dll... done
Loading all dynamic preprocessor libs from C:\Snort\lib\snort_dynamicpreprocessor...
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_dce2.dll... done
```

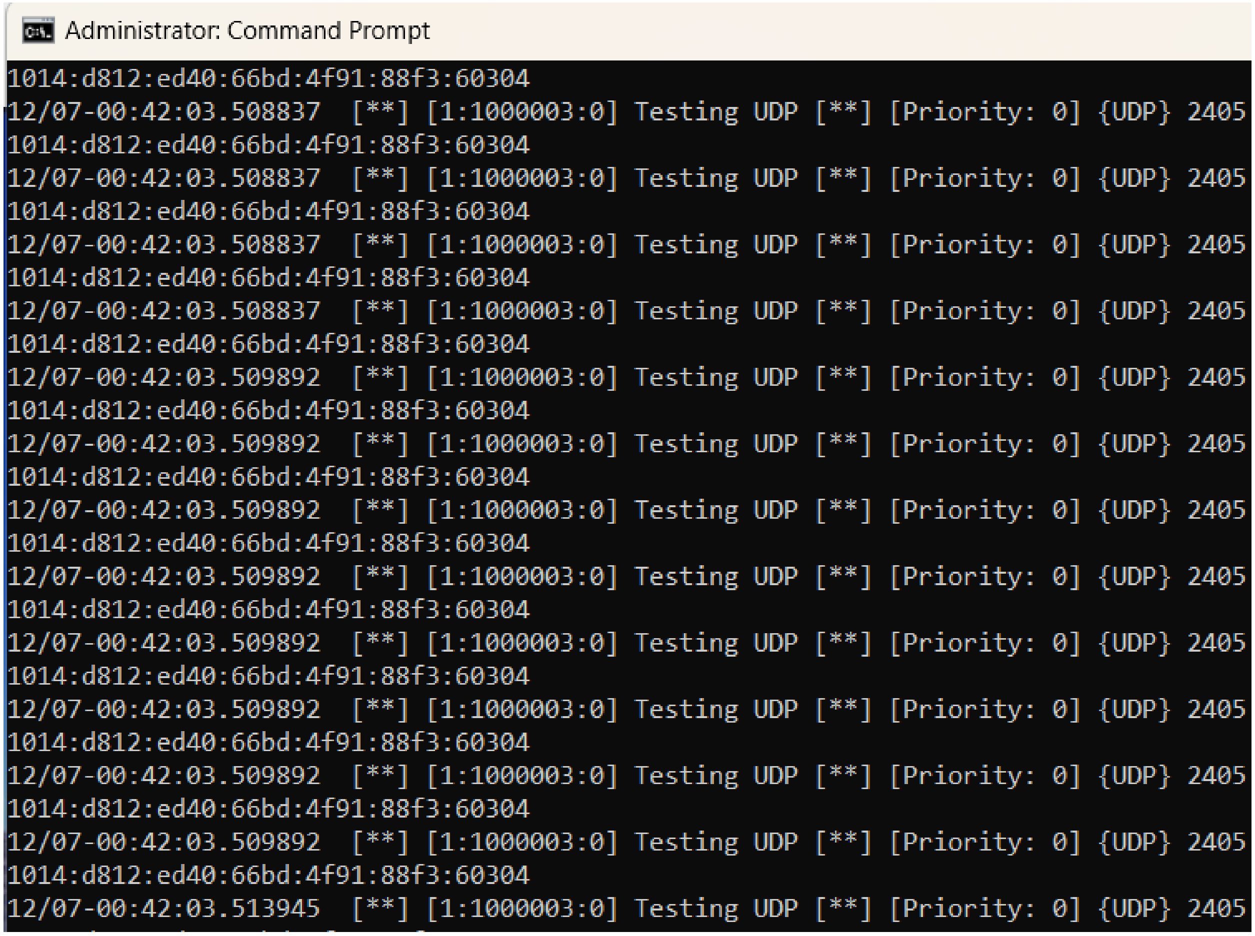
```
Administrator: Command Prompt

  ,,_     -*> Snort! <*-
 o" )~    Version 2.9.20-WIN64 GRE (Build 82)
  ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
          Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
          Copyright (C) 1998-2013 Sourcefire, Inc., et al.
          Using PCRE version: 8.10 2010-06-25
          Using ZLIB version: 1.2.11

          Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 3.2  <Build 1>
          Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
          Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
          Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
          Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
          Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
          Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
          Preprocessor Object: SF_POP  Version 1.0  <Build 1>
          Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
          Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
          Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
          Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
          Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
          Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
          Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>

Total snort Fixed Memory Cost - MaxRss:897266336
Snort successfully validated the configuration!
Snort exiting

C:\Snort\bin>
```

Added rules in local.ruoles

```
# list of third party owners and their respective copyrights.
#
# In order to determine what rules are VRT Certified Rules or GPL Rules, please
# to the VRT Certified Rules License Agreement (v2.0).
#
#-------------
# LOCAL RULES
#-------------
alert icmp any any -> any any (msg:"Testing ICMP";sid:1000001;)
alert tcp any any -> any any (msg:"Testing TCP";sid:1000002;)
alert udp any any -> any any (msg:"Testing UDP";sid:1000003;)
```

If we want to say result in pingtest.txt

snort -i 1 -c c:\snort\etc\snort.conf -A console > c:\snort\log\pingtest.txt



```
1014:d812:ed40:66bd:4f91:88f3:60304
12/07-00:42:03.508837  [**] [1:1000003:0] Testing UDP [**] [Priority: 0] {UDP} 2405
1014:d812:ed40:66bd:4f91:88f3:60304
12/07-00:42:03.508837  [**] [1:1000003:0] Testing UDP [**] [Priority: 0] {UDP} 2405
1014:d812:ed40:66bd:4f91:88f3:60304
12/07-00:42:03.508837  [**] [1:1000003:0] Testing UDP [**] [Priority: 0] {UDP} 2405
1014:d812:ed40:66bd:4f91:88f3:60304
12/07-00:42:03.508837  [**] [1:1000003:0] Testing UDP [**] [Priority: 0] {UDP} 2405
1014:d812:ed40:66bd:4f91:88f3:60304
12/07-00:42:03.509892  [**] [1:1000003:0] Testing UDP [**] [Priority: 0] {UDP} 2405
1014:d812:ed40:66bd:4f91:88f3:60304
12/07-00:42:03.509892  [**] [1:1000003:0] Testing UDP [**] [Priority: 0] {UDP} 2405
1014:d812:ed40:66bd:4f91:88f3:60304
12/07-00:42:03.509892  [**] [1:1000003:0] Testing UDP [**] [Priority: 0] {UDP} 2405
1014:d812:ed40:66bd:4f91:88f3:60304
12/07-00:42:03.509892  [**] [1:1000003:0] Testing UDP [**] [Priority: 0] {UDP} 2405
1014:d812:ed40:66bd:4f91:88f3:60304
12/07-00:42:03.509892  [**] [1:1000003:0] Testing UDP [**] [Priority: 0] {UDP} 2405
1014:d812:ed40:66bd:4f91:88f3:60304
12/07-00:42:03.509892  [**] [1:1000003:0] Testing UDP [**] [Priority: 0] {UDP} 2405
1014:d812:ed40:66bd:4f91:88f3:60304
12/07-00:42:03.509892  [**] [1:1000003:0] Testing UDP [**] [Priority: 0] {UDP} 2405
1014:d812:ed40:66bd:4f91:88f3:60304
12/07-00:42:03.509892  [**] [1:1000003:0] Testing UDP [**] [Priority: 0] {UDP} 2405
1014:d812:ed40:66bd:4f91:88f3:60304
12/07-00:42:03.513945  [**] [1:1000003:0] Testing UDP [**] [Priority: 0] {UDP} 2405
```

```
*** Caught Int-Signal
===============================================================================
Run time for packet processing was 3.92000 seconds
Snort processed 1948 packets.
Snort ran for 0 days 0 hours 0 minutes 3 seconds
   Pkts/sec:          649
===============================================================================
Packet I/O Totals:
   Received:         1959
   Analyzed:         1948 ( 99.438%)
    Dropped:            0 (  0.000%)
   Filtered:            0 (  0.000%)
Outstanding:           11 (  0.562%)
   Injected:            0
===============================================================================
Breakdown by protocol (includes rebuilt packets):
        Eth:         1949 (100.000%)
       VLAN:            0 (  0.000%)
        IP4:           30 (  1.539%)
       Frag:            0 (  0.000%)
       ICMP:            0 (  0.000%)
        UDP:            2 (  0.103%)
```