```
het@Snort:~$ sudo apt install -y snort
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following package was automatically installed and is no longer required:
  libllvm19
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  libdaq2t64 libdumbnet1 libluajit-5.1-2 libluajit-5.1-common libnetfilter-queue1 libpcre3 net-tools oinkmaster
  snort-common snort-common-libraries snort-rules-default
Suggested packages:
  snort-doc
The following NEW packages will be installed:
  libdaq2t64 libdumbnet1 libluajit-5.1-2 libluajit-5.1-common libnetfilter-queue1 libpcre3 net-tools oinkmaster snort
  snort-common snort-common-libraries snort-rules-default
0 upgraded, 12 newly installed, 0 to remove and 0 not upgraded.
Need to get 2,870 kB of archives.
After this operation, 12.2 MB of additional disk space will be used.
Get:1 http://in.archive.ubuntu.com/ubuntu noble/universe amd64 libluajit-5.1-common all 2.1.0+git20231223.c525bcb+dfsg-1 [49.2 kB]
Get:2 http://in.archive.ubuntu.com/ubuntu noble/universe amd64 libluajit-5.1-2 amd64 2.1.0+git20231223.c525bcb+dfsg-1 [275 kB]
Get:3 http://in.archive.ubuntu.com/ubuntu noble/universe amd64 libpcre3 amd64 2:8.39-15build1 [248 kB]
Get:4 http://in.archive.ubuntu.com/ubuntu noble/universe amd64 snort-common-libraries amd64 2.9.20-0+deb11u1ubuntu1 [899 kB]
Get:5 http://in.archive.ubuntu.com/ubuntu noble/universe amd64 snort-rules-default all 2.9.20-0+deb11u1ubuntu1 [144 kB]
Get:6 http://in.archive.ubuntu.com/ubuntu noble/universe amd64 snort-common all 2.9.20-0+deb11u1ubuntu1 [47.7 kB]
Get:7 http://in.archive.ubuntu.com/ubuntu noble-updates/main amd64 net-tools amd64 2.10-0.1ubuntu4.4 [204 kB]
Get:8 http://in.archive.ubuntu.com/ubuntu noble/universe amd64 libdumbnet1 amd64 1.17.0-1ubuntu2 [30.7 kB]
Get:9 http://in.archive.ubuntu.com/ubuntu noble/universe amd64 libnetfilter-queue1 amd64 1.0.5-4build1 [15.1 kB]
Get:10 http://in.archive.ubuntu.com/ubuntu noble/universe amd64 libdaq2t64 amd64 2.0.7-5.1build3 [92.9 kB]
Get:11 http://in.archive.ubuntu.com/ubuntu noble/universe amd64 snort amd64 2.9.20-0+deb11u1ubuntu1 [791 kB]
Get:12 http://in.archive.ubuntu.com/ubuntu noble/universe amd64 oinkmaster all 2.0-4.2 [71.9 kB]
Fetched 2,870 kB in 5s (622 kB/s)
Preconfiguring packages ...
Snort configuration: interface default not set, using 'enp0s3'
Selecting previously unselected package libluajit-5.1-common.
(Reading database ... 152746 files and directories currently installed.)
Preparing to unpack .../00-libluajit-5.1-common_2.1.0+git20231223.c525bcb+dfsg-1_all.deb ...
Unpacking libluajit-5.1-common (2.1.0+git20231223.c525bcb+dfsg-1) ...
Selecting previously unselected package libluajit-5.1-2:amd64.
Preparing to unpack .../01-libluajit-5.1-2_2.1.0+git20231223.c525bcb+dfsg-1_amd64.deb ...
Unpacking libluajit-5.1-2:amd64 (2.1.0+git20231223.c525bcb+dfsg-1) ...
Selecting previously unselected package libpcre3:amd64.
Preparing to unpack .../02-libpcre3_2%3a8.39-15build1_amd64.deb ...
Unpacking libpcre3:amd64 (2:8.39-15build1) ...
```

```
Unpacking snort-common-libraries (2.9.20-0+deb11u1ubuntu1) ...
Selecting previously unselected package snort-rules-default.
Preparing to unpack .../04-snort-rules-default_2.9.20-0+deb11u1ubuntu1_all.deb ...
Unpacking snort-rules-default (2.9.20-0+deb11u1ubuntu1) ...
Selecting previously unselected package snort-common.
Preparing to unpack .../05-snort-common_2.9.20-0+deb11u1ubuntu1_all.deb ...
Unpacking snort-common (2.9.20-0+deb11u1ubuntu1) ...
Selecting previously unselected package net-tools.
Preparing to unpack .../06-net-tools_2.10-0.1ubuntu4.4_amd64.deb ...
Unpacking net-tools (2.10-0.1ubuntu4.4) ...
Selecting previously unselected package libdumbnet1:amd64.
Preparing to unpack .../07-libdumbnet1_1.17.0-1ubuntu2_amd64.deb ...
Unpacking libdumbnet1:amd64 (1.17.0-1ubuntu2) ...
Selecting previously unselected package libnetfilter-queue1:amd64.
Preparing to unpack .../08-libnetfilter-queue1_1.0.5-4build1_amd64.deb ...
Unpacking libnetfilter-queue1:amd64 (1.0.5-4build1) ...
Selecting previously unselected package libdaq2t64.
Preparing to unpack .../09-libdaq2t64_2.0.7-5.1build3_amd64.deb ...
Unpacking libdaq2t64 (2.0.7-5.1build3) ...
Selecting previously unselected package snort.
Preparing to unpack .../10-snort_2.9.20-0+deb11u1ubuntu1_amd64.deb ...
Unpacking snort (2.9.20-0+deb11u1ubuntu1) ...
Selecting previously unselected package oinkmaster.
Preparing to unpack .../11-oinkmaster_2.0-4.2_all.deb ...
Unpacking oinkmaster (2.0-4.2) ...
Setting up oinkmaster (2.0-4.2) ...
Setting up net-tools (2.10-0.1ubuntu4.4) ...
Setting up snort-common (2.9.20-0+deb11u1ubuntu1) ...
Setting up libpcre3:amd64 (2:8.39-15build1) ...
Setting up libluajit-5.1-common (2.1.0+git20231223.c525bcb+dfsg-1) ...
Setting up libnetfilter-queue1:amd64 (1.0.5-4build1) ...
Setting up libdumbnet1:amd64 (1.17.0-1ubuntu2) ...
Setting up snort-rules-default (2.9.20-0+deb11u1ubuntu1) ...
Setting up libdaq2t64 (2.0.7-5.1build3) ...
Setting up libluajit-5.1-2:amd64 (2.1.0+git20231223.c525bcb+dfsg-1) ...
Setting up snort-common-libraries (2.9.20-0+deb11u1ubuntu1) ...
Setting up snort (2.9.20-0+deb11u1ubuntu1) ...
Snort configuration: interface default not set, using 'enp0s3'
Processing triggers for man-db (2.12.0-4build2) ...
Processing triggers for libc-bin (2.39-0ubuntu8.6) ...
het@Snort:~$
```

```
Unpacking net-tools (2.10-0.1ubuntu4.4) ...
Selecting previously unselected package libdumbnet1:amd64.
Preparing to unpack .../07-libdumbnet1_1.17.0-1ubuntu2_amd64.deb ...
Unpacking libdumbnet1:amd64 (1.17.0-1ubuntu2) ...
Selecting previously unselected package libnetfilter-queue1:amd64.
Preparing to unpack .../08-libnetfilter-queue1_1.0.5-4build1_amd64.deb ...
Unpacking libnetfilter-queue1:amd64 (1.0.5-4build1) ...
Selecting previously unselected package libdaq2t64.
Preparing to unpack .../09-libdaq2t64_2.0.7-5.1build3_amd64.deb ...
Unpacking libdaq2t64 (2.0.7-5.1build3) ...
Selecting previously unselected package snort.
Preparing to unpack .../10-snort_2.9.20-0+deb11u1ubuntu1_amd64.deb ...
Unpacking snort (2.9.20-0+deb11u1ubuntu1) ...
Selecting previously unselected package oinkmaster.
Preparing to unpack .../11-oinkmaster_2.0-4.2_all.deb ...
Unpacking oinkmaster (2.0-4.2) ...
Setting up oinkmaster (2.0-4.2) ...
Setting up net-tools (2.10-0.1ubuntu4.4) ...
Setting up snort-common (2.9.20-0+deb11u1ubuntu1) ...
Setting up libpcre3:amd64 (2:8.39-15build1) ...
Setting up libluajit-5.1-common (2.1.0+git20231223.c525bcb+dfsg-1) ...
Setting up libnetfilter-queue1:amd64 (1.0.5-4build1) ...
Setting up libdumbnet1:amd64 (1.17.0-1ubuntu2) ...
Setting up snort-rules-default (2.9.20-0+deb11u1ubuntu1) ...
Setting up libdaq2t64 (2.0.7-5.1build3) ...
Setting up libluajit-5.1-2:amd64 (2.1.0+git20231223.c525bcb+dfsg-1) ...
Setting up snort-common-libraries (2.9.20-0+deb11u1ubuntu1) ...
Setting up snort (2.9.20-0+deb11u1ubuntu1) ...
Snort configuration: interface default not set, using 'enp0s3'
Processing triggers for man-db (2.12.0-4build2) ...
Processing triggers for libc-bin (2.39-0ubuntu8.6) ...
het@Snort:~$ snort -V

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.20 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 libpcap version 1.10.4 (with TPACKET_V3)
           Using PCRE version: 8.39 2016-06-14
           Using ZLIB version: 1.3

het@Snort:~$
```

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

# Setup the network addresses you are protecting
#
# Note to Debian users: this value is overriden when starting
# up the Snort daemon through the init.d script by the
# value of DEBIAN_SNORT_HOME_NET s defined in the
# /etc/snort/snort.debian.conf configuration file
#
ipvar HOME_NET any

# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET any
# If HOME_NET is defined as something other than "any", alternative, you can
# use this definition if you do not want to detect attacks from your internal
# IP addresses:
#ipvar EXTERNAL_NET !$HOME_NET

# List of DNS servers on your network
ipvar DNS_SERVERS $HOME_NET

# List of SMTP servers on your network
ipvar SMTP_SERVERS $HOME_NET

# List of web servers on your network
ipvar HTTP_SERVERS $HOME_NET

# List of sql servers on your network
ipvar SQL_SERVERS $HOME_NET

# List of telnet servers on your network
ipvar TELNET_SERVERS $HOME_NET

# List of ssh servers on your network
ipvar SSH_SERVERS $HOME_NET

# List of ftp servers on your network
ipvar FTP_SERVERS $HOME_NET

# List of sip servers on your network
```

```
# other variables, these should not be modified
ipvar AIM_SERVERS [64.12.24.0/23,64.12.28.0/23,64.12.161.0/24,64.12.163.0/24,64.12.200.0/24,205.188.3.0/24,205.188.5.0/24,205.188.7.0/24,205.188.9.0/24,205.188.153.0/24,205.188

# 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 /etc/snort/rules
var SO_RULE_PATH /etc/snort/so_rules
var PREPROC_RULE_PATH /etc/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 /etc/snort/rules
var BLACK_LIST_PATH /etc/snort/rules

##################################################
# Step #2: Configure the decoder.  For more information, see README.decode
##################################################

# Stop generic decode events:
config disable_decode_alerts

# Stop Alerts on experimental TCP options
config disable_tcpopt_experimental_alerts

# Stop Alerts on obsolete TCP options
config disable_tcpopt_obsolete_alerts

# Stop Alerts on T/TCP alerts
config disable_tcpopt_ttcp_alerts

# Stop Alerts on all other TCPOption type events:
config disable_tcpopt_alerts

# Stop Alerts on invalid ip options
config disable_ipopt_alerts
```

GNU nano 7.2 /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.

# ICMP Ping Detection
alert icmp any any -> $HOME_NET any (msg:"ICMP Ping Detected"; sid:1000001; rev:1;)

# SSH Connection Attempt
alert tcp any any -> $HOME_NET 22 (msg:"SSH Connection Attempt"; flags:S; sid:1000002; rev:1;)

# HTTP Traffic Detection
alert tcp any any -> $HOME_NET 80 (msg:"HTTP Traffic Detected"; sid:1000003; rev:1;)

# FTP Connection Attempt
alert tcp any any -> $HOME_NET 21 (msg:"FTP Connection Attempt"; sid:1000004; rev:1;)

# Telnet Connection Attempt
alert tcp any any -> $HOME_NET 23 (msg:"Telnet Attempt Detected"; sid:1000005; rev:1;)

# DNS Query Detection
alert udp any any -> $HOME_NET 53 (msg:"DNS Query Detected"; sid:1000006; rev:1;)
```

```
het@Snort:/etc/snort$ sudo nano /etc/snort/rules/local.rules
het@Snort:/etc/snort$ sudo snort -T -c /etc/snort/snort.conf
Running in Test mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "/etc/snort/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 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 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 8
008 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 '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 /usr/lib/snort/snort_dynamicengine/libsf_engine.so... done
Loading all dynamic detection libs from /usr/lib/snort/snort_dynamicrules...
WARNING: No dynamic libraries found in directory /usr/lib/snort/snort_dynamicrules.
  Finished Loading all dynamic detection libs from /usr/lib/snort/snort_dynamicrules
Loading all dynamic preprocessor libs from /usr/lib/snort/snort_dynamicpreprocessor/...
  Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_pop_preproc.so... done
  Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_ftptelnet_preproc.so... done
  Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_dce2_preproc.so... done
  Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_ssl_preproc.so... done
  Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_sip_preproc.so... done
  Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_appid_preproc.so... done
  Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_gtp_preproc.so... done
  Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_s7commplus_preproc.so... done
  Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_ssh_preproc.so... done
  Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_dnp3_preproc.so... done
  Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_sdf_preproc.so... done
  Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_imap_preproc.so... done
  Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_smtp_preproc.so... done
```

```
|   Patterns        : 0.51
|   Match Lists     : 1.01
|   DFA
|     1 byte states : 1.02
|     2 byte states : 13.96
|     4 byte states : 0.00
+-------------------------------------------------------------
[ Number of patterns truncated to 20 bytes: 1038 ]

MaxRss at the end of detection rules:106588

        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.20 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 libpcap version 1.10.4 (with TPACKET_V3)
           Using PCRE version: 8.39 2016-06-14
           Using ZLIB version: 1.3

           Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 3.2  <Build 1>
           Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
           Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
           Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
           Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
           Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
           Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
           Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
           Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
           Preprocessor Object: SF_S7COMMPLUS  Version 1.0  <Build 1>
           Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
           Preprocessor Object: appid  Version 1.1  <Build 5>
           Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
           Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
           Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
           Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
           Preprocessor Object: SF_POP  Version 1.0  <Build 1>

Total snort Fixed Memory Cost - MaxRss:106588
Snort successfully validated the configuration!
Snort exiting
het@Snort:/etc/snort$
```

```
    inet6 fd17:625c:f037:2:a00:27ff:fe40:1d4f/64 scope global dynamic mngtmpaddr
       valid_lft 85949sec preferred_lft 13949sec
    inet6 fe80::a00:27ff:fe40:1d4f/64 scope link
       valid_lft forever preferred_lft forever
het@Snort:/etc/snort$ sudo snort -A console -q -c /etc/snort/snort.conf -i enp0s3

01/24-12:13:43.329642  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {IPV6-ICMP} fe80::2 -> ff02::1
01/24-12:23:26.586280  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {IPV6-ICMP} fe80::2 -> ff02::1
01/24-12:24:10.652222  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 10.0.2.15 -> 142.251.43.14
01/24-12:24:10.714294  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 142.251.43.14 -> 10.0.2.15
01/24-12:24:11.657282  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 10.0.2.15 -> 142.251.43.14
01/24-12:24:11.691767  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 142.251.43.14 -> 10.0.2.15
01/24-12:24:12.658443  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 10.0.2.15 -> 142.251.43.14
01/24-12:24:12.701956  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 142.251.43.14 -> 10.0.2.15
01/24-12:24:13.660427  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 10.0.2.15 -> 142.251.43.14
01/24-12:24:13.702441  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 142.251.43.14 -> 10.0.2.15
01/24-12:24:14.722520  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 10.0.2.15 -> 142.251.43.14
01/24-12:24:14.761226  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 142.251.43.14 -> 10.0.2.15
01/24-12:24:15.724980  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 10.0.2.15 -> 142.251.43.14
01/24-12:24:15.778322  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 142.251.43.14 -> 10.0.2.15
01/24-12:24:16.746488  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 10.0.2.15 -> 142.251.43.14
01/24-12:24:16.794526  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 142.251.43.14 -> 10.0.2.15
01/24-12:24:17.747441  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 10.0.2.15 -> 142.251.43.14
01/24-12:24:17.791311  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 142.251.43.14 -> 10.0.2.15
01/24-12:24:18.748012  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 10.0.2.15 -> 142.251.43.14
01/24-12:24:18.811459  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 142.251.43.14 -> 10.0.2.15
01/24-12:24:19.749153  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 10.0.2.15 -> 142.251.43.14
01/24-12:24:19.801952  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 142.251.43.14 -> 10.0.2.15
01/24-12:24:20.781454  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 10.0.2.15 -> 142.251.43.14
01/24-12:24:20.822051  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 142.251.43.14 -> 10.0.2.15
01/24-12:24:21.783343  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 10.0.2.15 -> 142.251.43.14
01/24-12:24:21.822713  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 142.251.43.14 -> 10.0.2.15
01/24-12:24:22.814350  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 10.0.2.15 -> 142.251.43.14
01/24-12:24:22.861629  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 142.251.43.14 -> 10.0.2.15
01/24-12:24:23.815540  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 10.0.2.15 -> 142.251.43.14
01/24-12:24:23.851893  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 142.251.43.14 -> 10.0.2.15
01/24-12:24:24.817434  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 10.0.2.15 -> 142.251.43.14
01/24-12:24:24.882621  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 142.251.43.14 -> 10.0.2.15
01/24-12:24:25.836928  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 10.0.2.15 -> 142.251.43.14
01/24-12:24:25.901156  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 142.251.43.14 -> 10.0.2.15
01/24-12:24:26.839518  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 10.0.2.15 -> 142.251.43.14
01/24-12:24:27.260068  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 142.251.43.14 -> 10.0.2.15
```

```
01/24-12:24:46.996482  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 10.0.2.15 -> 142.251.43.14
01/24-12:24:47.030672  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 142.251.43.14 -> 10.0.2.15
01/24-12:24:47.998506  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 10.0.2.15 -> 142.251.43.14
01/24-12:24:48.027469  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 142.251.43.14 -> 10.0.2.15
01/24-12:24:48.998607  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 10.0.2.15 -> 142.251.43.14
01/24-12:24:49.035430  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 142.251.43.14 -> 10.0.2.15
01/24-12:24:50.000317  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 10.0.2.15 -> 142.251.43.14
01/24-12:24:50.031108  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 142.251.43.14 -> 10.0.2.15
01/24-12:24:51.002164  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 10.0.2.15 -> 142.251.43.14
01/24-12:24:51.029912  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 142.251.43.14 -> 10.0.2.15
01/24-12:24:52.004193  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 10.0.2.15 -> 142.251.43.14
01/24-12:24:52.036735  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 142.251.43.14 -> 10.0.2.15
01/24-12:24:53.006540  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 10.0.2.15 -> 142.251.43.14
01/24-12:24:53.037465  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 142.251.43.14 -> 10.0.2.15
01/24-12:24:54.009293  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 10.0.2.15 -> 142.251.43.14
01/24-12:24:54.040753  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 142.251.43.14 -> 10.0.2.15
01/24-12:24:55.011313  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 10.0.2.15 -> 142.251.43.14
01/24-12:24:55.046320  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 142.251.43.14 -> 10.0.2.15
01/24-12:24:56.012716  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 10.0.2.15 -> 142.251.43.14
01/24-12:24:56.044170  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 142.251.43.14 -> 10.0.2.15
01/24-12:24:57.015246  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 10.0.2.15 -> 142.251.43.14
01/24-12:24:57.040425  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 142.251.43.14 -> 10.0.2.15
01/24-12:24:58.016898  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 10.0.2.15 -> 142.251.43.14
01/24-12:24:58.045953  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 142.251.43.14 -> 10.0.2.15
01/24-12:24:59.020485  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 10.0.2.15 -> 142.251.43.14
01/24-12:24:59.050823  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 142.251.43.14 -> 10.0.2.15
01/24-12:25:00.022198  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 10.0.2.15 -> 142.251.43.14
01/24-12:25:00.053399  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 142.251.43.14 -> 10.0.2.15
01/24-12:25:01.022791  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 10.0.2.15 -> 142.251.43.14
01/24-12:25:01.045437  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 142.251.43.14 -> 10.0.2.15
01/24-12:25:02.025498  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 10.0.2.15 -> 142.251.43.14
01/24-12:25:02.061240  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 142.251.43.14 -> 10.0.2.15
01/24-12:25:03.043470  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 10.0.2.15 -> 142.251.43.14
01/24-12:25:03.071052  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 142.251.43.14 -> 10.0.2.15
01/24-12:25:04.044741  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 10.0.2.15 -> 142.251.43.14
01/24-12:25:04.075318  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 142.251.43.14 -> 10.0.2.15
01/24-12:28:23.351716  [**] [1:1000003:1] HTTP Traffic Detected [**] [Priority: 0] {TCP} 10.0.2.15:56528 -> 185.125.190.98:80
01/24-12:29:21.308481  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {IPV6-ICMP} fe80::2 -> ff02::1
01/24-12:33:14.713266  [**] [1:1000003:1] HTTP Traffic Detected [**] [Priority: 0] {TCP} 10.0.2.15:54802 -> 185.125.190.82:80
01/24-12:33:32.029409  [**] [1:1000003:1] HTTP Traffic Detected [**] [Priority: 0] {TCP} 10.0.2.15:45170 -> 104.18.27.120:80
01/24-12:34:18.366764  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {IPV6-ICMP} fe80::2 -> ff02::1
```

het@Snort: ~

```
het@snort:-$ sudo snort -A console -q -c /etcsnort/snort.conf -i
etC-Snort snoft -a

[01/24-15:00:14.676437] [ICMP Ping Detected [**]
Priority: 0
[ICMP] 127.0.0.1 -> 127.0.0.1
   ICMP TTL:255 TOS:0x0 ID:2212 Ip.2212 IpLen:20 DgmLen: 84 Type: 8 Code:0 ID:41 Seq:1


[01/24-15:00:17.231166] [Telnet Attempt Detected [**]
Priority: 0
[TCP] 127.00.0.1:45086 -> 127.0.0.1:23
   Seq: 0x375D5B7B Ack:0x0 Win:65535 TcpLen:0

[01/24-15:00:23:305419] [DNS Query Detected [**]
Priority: 0
[UDP] 127.0.0.1:48790 -> 127.0.0.1:53
   UDP TTL:64 TOS:0x0 ID:0 IpLen:56 DgmLen:36 9TTL-:0

[01/24-15:00:25:251953] [HTTP Traffic Detected [**]
Priority: 0
[TCP] 127.0.0.1:32933 -> 127.0.0.1:80
   Seq: 0x3CAF7EDF Ack:0x0 Win: 65476 TcpLen:36 TcpLen:32

[01/24-15:00:43.988332] [SSH Connection Attempt [**]
Priority: 0
[TCP] 127.0.0.1:48692 -> 127.0.0.1:23
   Seq: 0x6023CDC5 Ack:0x0 Win: 05468 TCP :65469 TcpLen:0

het@snort:~$
```