

INTERNSHIP ORGANIZED BY CYBER SECURITY CLUB

Project Report on

Setting up an Intrusion Detection System (IDS)

and Intrusion Prevention System (IPS)

BACHELOR OF ENGINEERING

IN

COMPUTER ENGINEERING

BY

Saitwadekar Valay Angar (Roll No. 49)

TE CMPN

DEPARTMENT OF COMPUTER ENGINEERING



**CYBER SECURITY CLUB
(SWDC)**

Accredited by NBA for 3 years w.e.f. 1st July 2022

SHREE L. R. TIWARI COLLEGE OF ENGINEERING
SHREE L.R. TIWARI EDUCATIONAL CAMPUS, MIRA ROAD (East),
THANE - 401 107, MAHARASHTRA.

University of Mumbai

(AY 2022-23)

Table of Contents

Table of Contents.....	1
Introduction.....	2
Hardware/Software Details.....	3
Procedure/Steps.....	3
Output.....	10
References.....	12

Introduction

Intrusion detection is the process of monitoring your network traffic and analyzing it for signs of possible intrusions, such as exploit attempts and incidents that may be imminent threats to your network. For its part, intrusion prevention is the process of performing intrusion detection and then stopping the detected incidents, typically done by dropping packets or terminating sessions. These security measures are available as intrusion detection systems (IDS) and intrusion prevention systems (IPS), which are part of network security measures taken to detect and stop potential incidents and are included functionality within next-generation firewalls (NGFW).

IDS/IPS monitors all traffic on the network to identify any known malicious behavior. One of the ways in which an attacker will try to compromise a network is by exploiting a vulnerability within a device or within software. IDS/IPS identifies those exploit attempts and blocks them before they successfully compromise any endpoints within the network. IDS/IPS are necessary security technologies, both at the network edge and within the data center, precisely because they can stop attackers while they are gathering information about your network.

Both systems can:

Monitor. After setup, these programs can look over traffic within parameters you specify, and they will work until you turn them off.

Alert. Both programs will send a notification to those you specify when a problem has been spotted.

Learn. Both can use machine learning to understand patterns and emerging threats.

Log. Both will keep records of attacks and responses, so you can adjust your protections accordingly.

But they differ due to:

Response. An IDS is passive, while an IPS is an active control system. You must take action after an IDS alerts you, as your system is still under attack.

Protection. Arguably, an IDS offers less help when you're under threat. You must figure out what to do, when to do it, and how to clean up the mess. An IPS does all of this for you.

False positives. If an IDS gives you an alert about something that isn't troublesome at all, you're the only one inconvenienced. If an IPS shuts down traffic, many people could be impacted.

Hardware/Software Details

An IDS/IPS is usually run on a Dedicated Server type of Hardware with Networking Capabilities. It uses special Proprietary Software on a Linux/Unix based Operating System.

In my case, I have used Kali Linux running on a local machine along with SNORT which is an Open Source IPS and IDS Solution.

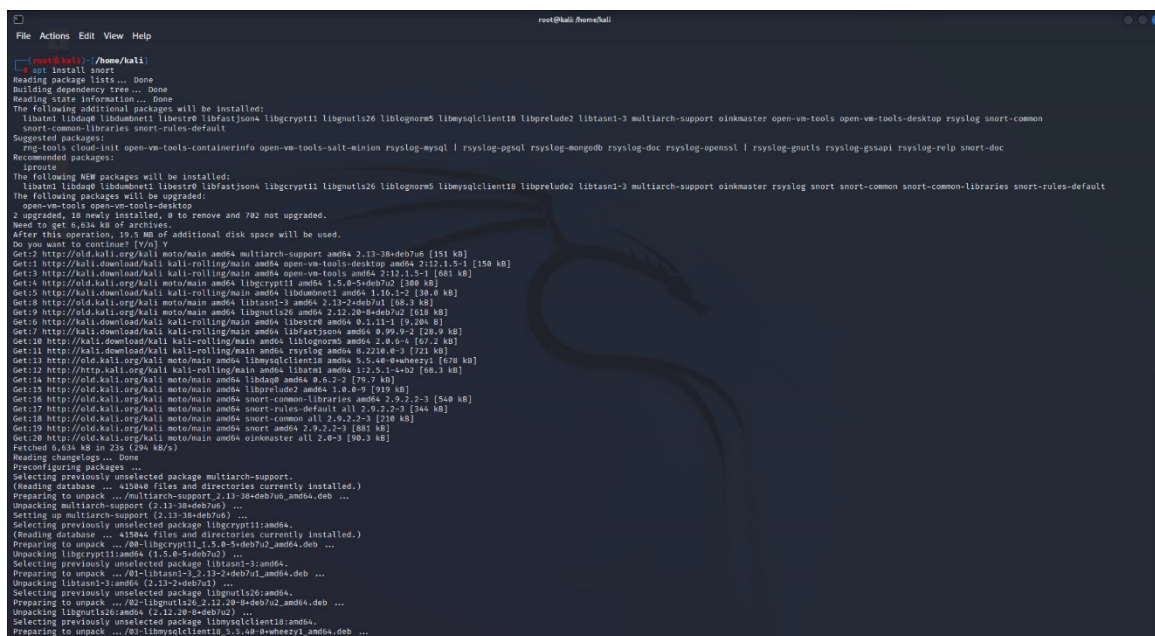
Procedure/Steps

First we Install the Snort Packages and Update our Kali Linux Dependencies.

We are in Super User mode so we avoid all the sudo commands.

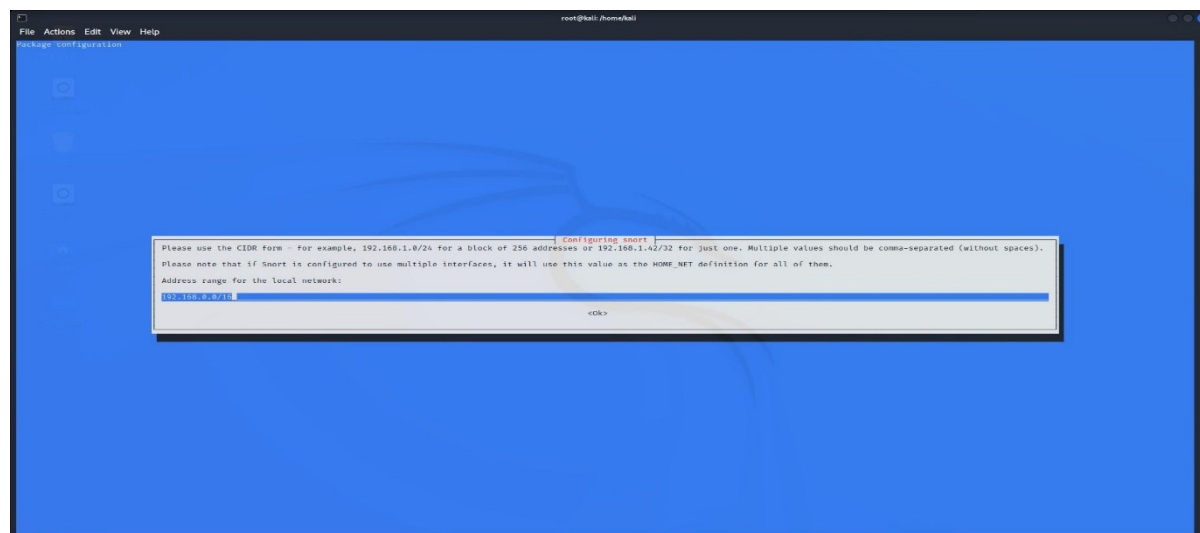
To Setup Snort as IDS:

1) apt install snort

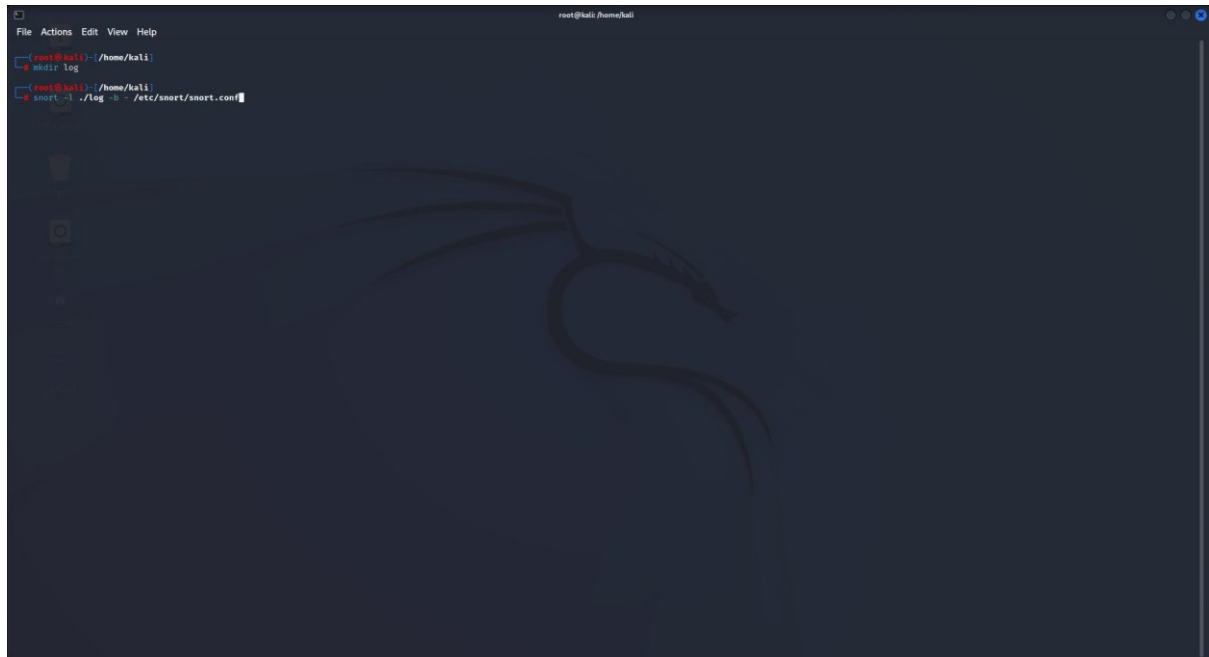


```
root@kali:~/home/kali# apt install snort
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libatsn1 libdumbnet1 libestr0 libfastjson4 libgcrypt11 libgnutls26 libhogweed5 libidn2-3 libltdl7 libnettle11 libnss3 libp11-kit0 libtasn1-3 libunistring2 libusb-1.0-0 libx11-6 libx11-xcb1 libxkbcommon0 libxslt1.1 libzstd1
Suggested packages:
  rng-tools cloud-init openvm-tools-containerinfo openvm-tools-salt-minion rsyslog-mysql | rsyslog-ngsql rsyslog-mongodb rsyslog-dbg rsyslog-openssl | rsyslog-gnutls rsyslog-gssapi rsyslog-relp snort-doc
Recommended packages:
  libseccomp2
The following NEW packages will be installed:
  libatsn1 libdumbnet1 libestr0 libfastjson4 libgcrypt11 libgnutls26 libhogweed5 libidn2-3 libltdl7 libnettle11 libnss3 libp11-kit0 libtasn1-3 libunistring2 libusb-1.0-0 libx11-6 libx11-xcb1 libxkbcommon0 libxslt1.1 libzstd1
The following packages will be upgraded:
  openvm-tools openvm-tools-desktop
2 upgraded, 18 newly installed, 0 to remove and 782 not upgraded.
Need to get 6,634 kB of archives.
After this operation, 19.5 MB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:2 http://old.kali.org/kali/moto/main amd64 multiarch-support amd64 2.13-38deb7u6 [151 kB]
Get:3 http://old.kali.org/kali/kali-rolling/main amd64 openvm-tools amd64 2.12.1-5-1 [158 kB]
Get:4 http://old.kali.org/kali/kali-rolling/main amd64 openvm-tools amd64 2.12.1-5-1 [681 kB]
Get:5 http://old.kali.org/kali/moto/main amd64 libgcrypt11 amd64 1.5.0-5-deb7u2 [388 kB]
Get:6 http://old.kali.org/kali/kali-rolling/main amd64 libdumbnet1 amd64 1.16-1-2 [38.8 kB]
Get:7 http://old.kali.org/kali/moto/main amd64 libatsn1-3 amd64 2.13-2-deb7u1 [88.3 kB]
Get:8 http://old.kali.org/kali/moto/main amd64 libgnutls26 amd64 2.12.20-8-deb7u2 [518 kB]
Get:9 http://old.kali.org/kali/kali-rolling/main amd64 libestr0 amd64 0.1.11-1 [9,204 B]
Get:10 http://old.kali.org/kali/kali-rolling/main amd64 libfastjson4 amd64 0.99.9-2 [28.9 kB]
Get:11 http://old.kali.org/kali/kali-rolling/main amd64 libhogweed5 amd64 2.8.4-4 [67.2 kB]
Get:12 http://old.kali.org/kali/moto/main amd64 libidn2-3 amd64 2.2.0-4 [72.1 kB]
Get:13 http://old.kali.org/kali/kali-rolling/main amd64 libtasn1-3 amd64 4.16.2-3 [121 kB]
Get:14 http://old.kali.org/kali/moto/main amd64 libdumbnet1 amd64 1.16-1-2 [38.8 kB]
Get:15 http://old.kali.org/kali/moto/main amd64 libunistring2 amd64 1.0.0-3 [549 kB]
Get:16 http://old.kali.org/kali/moto/main amd64 libx11-6 amd64 2.9.2-2-3 [344 kB]
Get:17 http://old.kali.org/kali/moto/main amd64 libx11-xcb1 amd64 2.9.2-2-3 [170 kB]
Get:18 http://old.kali.org/kali/moto/main amd64 libxkbcommon0 amd64 2.9.2-2-3 [88.1 kB]
Get:19 http://old.kali.org/kali/moto/main amd64 libnss3 amd64 2.6.3-3 [108.3 kB]
Get:20 http://old.kali.org/kali/moto/main amd64 libp11-kit0 amd64 0.26.3-3 [108.3 kB]
Fetched 6,634 kB in 23s (294 kB/s)
Reading changelogs... Done
Preconfiguring packages ...
Selecting previously unselected package multiarch-support.
(Reading database ... 41866 files and directories currently installed.)
Preparing to unpack .../multiarch-support_2.13-38deb7u6_amd64.deb ...
Unpacking multiarch-support (2.13-38deb7u6) ...
Setting up multiarch-support (2.13-38deb7u6) ...
Selecting previously unselected package libgcrypt11:amd64.
(Reading database ... 41866 files and directories currently installed.)
Preparing to unpack .../libgcrypt11_1.5.0-5-deb7u2_amd64.deb ...
Unpacking libgcrypt11:amd64 (1.5.0-5-deb7u2) ...
Selecting previously unselected package libtasn1-3:amd64.
(Reading database ... 41866 files and directories currently installed.)
Preparing to unpack .../libtasn1-3_2.13-2-deb7u1_amd64.deb ...
Unpacking libtasn1-3:amd64 (2.13-2-deb7u1) ...
Selecting previously unselected package libgnutls26:amd64.
Preparing to unpack .../libgnutls26_2.12.20-8-deb7u2_amd64.deb ...
Unpacking libgnutls26:amd64 (2.12.20-8-deb7u2) ...
Selecting previously unselected package libidn2-3:amd64.
Preparing to unpack .../libidn2-3_2.2.0-4_amd64.deb ...
Unpacking libidn2-3:amd64 (2.2.0-4) ...
Preparing to unpack .../libunistring2_1.0.0-3_amd64.deb ...
Unpacking libunistring2:amd64 (1.0.0-3) ...
Preparing to unpack .../libx11-6_2.9.2-2-3_amd64.deb ...
Unpacking libx11-6:amd64 (2.9.2-2-3) ...
Preparing to unpack .../libx11-xcb1_2.9.2-2-3_amd64.deb ...
Unpacking libx11-xcb1:amd64 (2.9.2-2-3) ...
Preparing to unpack .../libxkbcommon0_2.9.2-2-3_amd64.deb ...
Unpacking libxkbcommon0:amd64 (2.9.2-2-3) ...
Preparing to unpack .../libnss3_2.6.3-3_amd64.deb ...
Unpacking libnss3:amd64 (2.6.3-3) ...
Preparing to unpack .../libp11-kit0_0.26.3-3_amd64.deb ...
Unpacking libp11-kit0:amd64 (0.26.3-3) ...
```

It asks for Address Range of Local Network while performing Configuration

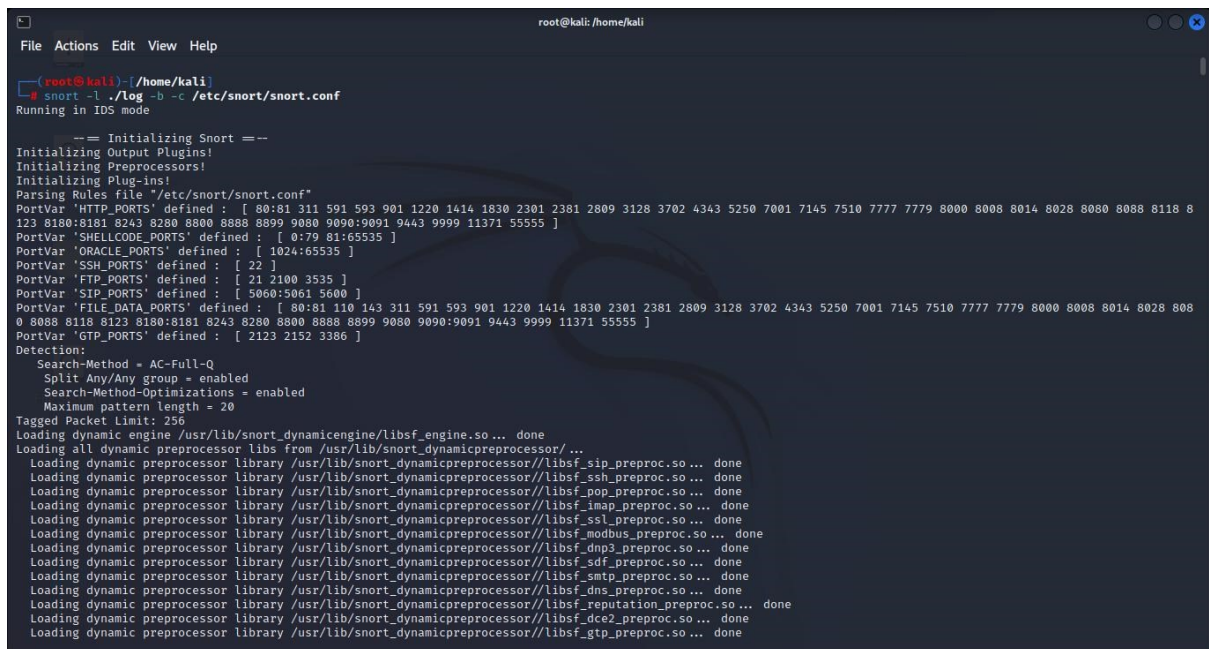


2) Create a Folder for storing Logs and Create a new Log for the Current Session



```
root@kali: /home/kali
File Actions Edit View Help
root@kali:~# mkdir log
root@kali:~# snort -l ./log -b -c /etc/snort/snort.conf
```

3) Run Snort to check if it is working



```
root@kali: /home/kali
File Actions Edit View Help
root@kali:~# snort -l ./log -b -c /etc/snort/snort.conf
Running in IDS mode

-- Initializing Snort --
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-Ins!
Parsing Rules File "/etc/snort/snort.conf"
PortVar 'HTTP_PORTS' defined : [ 80:81 311 591 593 901 1220 1414 1830 2301 2381 2809 3128 3702 4343 5250 7001 7145 7510 7777 7779 8000 8008 8014 8028 8080 8088 8118 8123 8180:8181 8243 8280 8800 8888 8899 9080 9090:9091 9443 9999 11371 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 : [ 80:81 110 143 311 591 593 901 1220 1414 1830 2301 2381 2809 3128 3702 4343 5250 7001 7145 7510 7777 7779 8000 8008 8014 8028 8080 8088 8118 8123 8180:8181 8243 8280 8800 8888 8899 9080 9090:9091 9443 9999 11371 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_dynamicengine/libsf_engine.so... done
Loading all dynamic preprocessor libs from /usr/lib/snort_dynamicpreprocessor/...
Loading dynamic preprocessor library /usr/lib/snort_dynamicpreprocessor/libsf_sip_preproc.so... done
Loading dynamic preprocessor library /usr/lib/snort_dynamicpreprocessor/libsf_ssh_preproc.so... done
Loading dynamic preprocessor library /usr/lib/snort_dynamicpreprocessor/libsf_pop_preproc.so... done
Loading dynamic preprocessor library /usr/lib/snort_dynamicpreprocessor/libsf_imap_preproc.so... done
Loading dynamic preprocessor library /usr/lib/snort_dynamicpreprocessor/libsf_ssl_preproc.so... done
Loading dynamic preprocessor library /usr/lib/snort_dynamicpreprocessor/libsf_modbus_preproc.so... done
Loading dynamic preprocessor library /usr/lib/snort_dynamicpreprocessor/libsf_dmp3_preproc.so... done
Loading dynamic preprocessor library /usr/lib/snort_dynamicpreprocessor/libsf_sdf_preproc.so... done
Loading dynamic preprocessor library /usr/lib/snort_dynamicpreprocessor/libsf_smtp_preproc.so... done
Loading dynamic preprocessor library /usr/lib/snort_dynamicpreprocessor/libsf_dns_preproc.so... done
Loading dynamic preprocessor library /usr/lib/snort_dynamicpreprocessor/libsf_reputation_preproc.so... done
Loading dynamic preprocessor library /usr/lib/snort_dynamicpreprocessor/libsf_dce2_preproc.so... done
Loading dynamic preprocessor library /usr/lib/snort_dynamicpreprocessor/libsf_gtp_preproc.so... done
```

```
root@kali: /home/kali/log
File Actions Edit View Help
=====
SMTP Preprocessor Statistics
Total sessions          : 0
Max concurrent sessions : 0
=====
dcerpc2 Preprocessor Statistics
Total sessions: 0
=====
SSL Preprocessor:
SSL packets decoded: 12
Client Hello: 2
Server Hello: 2
Certificate: 0
Server Done: 0
Client Key Exchange: 0
Server Key Exchange: 0
Change Cipher: 3
Finished: 0
Client Application: 4
Server Application: 4
Alert: 2
Unrecognized records: 0
Completed handshakes: 0
Bad handshakes: 0
Sessions ignored: 3
Detection disabled: 0
=====
SIP Preprocessor Statistics
Total sessions: 0
=====
Snort exiting
root@kali)-[/home/kali]
# cd log
root@kali)-[/home/kali/log]
# ls
alert  snort.log.1672518527
root@kali)-[/home/kali/log]
```

Checking for current Logs

4) Open the Configuration File

```
root@kali: /home/kali/log
File Actions Edit View Help
=====
GNU nano 6.4 /etc/snort/snort.conf
#
# VRT Rule Packages Snort.conf
#
# For more information visit us at:
# http://www.snort.org           Snort Website
# http://vrt-sourcefire.blogspot.com/ Sourcefire VRT Blog
#
# Mailing list Contact:  snort-sigs@lists.sourceforge.net
# False Positive reports: fp@sourcefire.com
# Snort bugs:           bugs@snort.org
#
# Compatible with Snort Versions:
# VERSIONS : 2.9.2.2
#
# Snort build options:
# OPTIONS : --enable-ipv6 --enable-gre --enable-mpls --enable-targetbased --enable-decoder-preprocessor-rules --enable-ppm --enable-perfprofiling --enable-zlib
#
# Additional information:
# This configuration file enables active response, to run snort in
# test mode -T you are required to supply an interface -i <interface>
# or test mode will fail to fully validate the configuration and
# exit with a FATAL error
#
#####
# This file contains a sample snort configuration.
# You should take the following steps to create your own custom configuration:
#
# 1) Set the network variables.
# 2) Configure the decoder
# 3) Configure the base detection engine
# 4) Configure dynamic loaded libraries
# 5) Configure preprocessors
# 6) Configure output plugins
# 7) Customize your rule set
# 8) Customize preprocessor and decoder rule set
# 9) Customize shared object rule set
#
[ Read 680 lines ]
# Help      # Write Out  # Where Is   # Cut        # Execute   # Location  # Undo       # Set Mark   # To Bracket # Previous
# Exit      # Read File  # Replace    # Paste      # Justify   # Go To Line # Redo       # Copy       # Where Was  # Next
```

nano etc/snort/snort.conf


```
root@kali: /home/kali
File Actions Edit View Help
[ Number of patterns truncated to 20 bytes: 1038 ]
pcap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "wlan0".
Reload thread starting...
Reload thread started, thread 0x7f90ee9f56c0 (21254)
Decoding Ethernet

== Initialization Complete ==

--> Snort! <*-
o''-)- Version 2.9.2.2 IPv6 GRE (Build 121)
****- By Martin Roesch & The Snort Team: http://www.snort.org/snort/snort-team
      Copyright (C) 1998-2012 Sourcefire, Inc., et al.
      Using libpcap version 1.10.1 (with TPACKET_V3)
      Using PCRE version: 8.39 2016-06-14
      Using ZLIB version: 1.2.11

Rules Engine: SF_SNORT_DETECTION_ENGINE Version 1.15 <Build 18>
Preprocessor Object: SF_FTPTELNET (IPv6) Version 1.2 <Build 13>
Preprocessor Object: SF_GTP (IPv6) Version 1.1 <Build 1>
Preprocessor Object: SF_DCERPC2 (IPv6) Version 1.0 <Build 3>
Preprocessor Object: SF_REPUTATION (IPv6) Version 1.1 <Build 1>
Preprocessor Object: SF_DNS (IPv6) Version 1.1 <Build 4>
Preprocessor Object: SF_SMTP (IPv6) Version 1.1 <Build 9>
Preprocessor Object: SF_SDF (IPv6) Version 1.1 <Build 1>
Preprocessor Object: SF_DNP3 (IPv6) Version 1.1 <Build 1>
Preprocessor Object: SF_MODBUS (IPv6) Version 1.1 <Build 1>
Preprocessor Object: SF_SSLPP (IPv6) Version 1.1 <Build 4>
Preprocessor Object: SF_IMAP (IPv6) Version 1.0 <Build 1>
Preprocessor Object: SF_POP (IPv6) Version 1.0 <Build 1>
Preprocessor Object: SF_SSH (IPv6) Version 1.1 <Build 3>
Preprocessor Object: SF_STP (IPv6) Version 1.1 <Build 1>
Commencing packet processing (pid=21254)
12/31-20:37:42.286042 [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.29.164 → 192.168.29.1
12/31-20:39:25.096260 [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.29.164 → 192.168.29.1
12/31-20:39:35.540238 [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 → 255.255.255.255:67
12/31-20:39:35.540338 [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 → 255.255.255.255:67
```

Snort is Monitoring the Traffic and showing Logs

IDS is Setup

To setup Snort as both IPS and IDS:

- 1) Configure Snort to run in “inline” mode and in afpacket daq

```
root@kali: /home/kali
File Actions Edit View Help
GNU nano 6.4 /etc/snort/snort.conf *
# Configure maximum number of flowbit references.  For more information, see README.flowbits
# config flowbits_size: 64

# Configure ports to ignore
# config ignore_ports: tcp 21 6667:6671 1356
# config ignore_ports: udp 1:17 53

# Configure active response for non inline operation.  For more information, see README.active
# config response: eth0 attempts 2

# Configure DAQ related options for inline operation.  For more information, see README.daq
#
# config daq: <type>
# config daq_dir: <dir>
# config daq_mode: <mode>
# config daq_var: <var>
# config daq: afpacket
# config daq_mode: inline

# <type> ::= pcap | afpacket | dump | nfq | ipq | ipfw
# <mode> ::= read-file | passive | inline
# <var> ::= arbitrary <name>=<value passed to DAQ
# <dir> ::= path as to where to look for DAQ module so's

# Configure specific UID and GID to run snort as after dropping privs.  For more information see snort -h command line options
#
# config set_gid:
# config set_uid:

# Configure default snaplen.  Snort defaults to MTU of in use interface.  For more information see README
#
# config snaplen:

# Configure default bpf_file to use for filtering what traffic reaches snort.  For more information see snort -h command line options (-F)
#
# config bpf_file:

^G Help      ^O Write Out  ^W Where Is   ^X Cut        ^E Execute    ^L Location   ^U Undo       ^M Set Mark   ^_] To Bracket  ^_C Previous
^X Exit      ^O Read File  ^W Replace    ^X Paste      ^E Justify    ^L Go To Line ^U Redo       ^M Copy       ^_] Where Was  ^_N Next
```


2) Run Snort in Test Mode to check if it works in “inline”

```
root@kali: /home/kali
File Actions Edit View Help

root@kali:~/home/kali# sudo snort -T -c /etc/snort/snort.conf -Q -i eth1:eth2
Enabling inline operation
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 : [ 80:81 311 591 593 901 1220 1414 1830 2301 2381 2809 3128 3702 4343 5250 7001 7145 7510 7777 7779 8000 8008 8014 8028 8080 8088 8118 8123 8180:8181 8243 8280 8800 8888 8899 9080 9090:9091 9443 9999 11371 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 : [ 80:81 110 143 311 591 593 901 1220 1414 1830 2301 2381 2809 3128 3702 4343 5250 7001 7145 7510 7777 7779 8000 8008 8014 8028 8080 8088 8118 8123 8180:8181 8243 8280 8800 8888 8899 9080 9090:9091 9443 9999 11371 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_dynamicengine/libsf_engine.so... done
Loading all dynamic preprocessor libs from /usr/lib/snort_dynamicpreprocessor/...
Loading dynamic preprocessor library /usr/lib/snort_dynamicpreprocessor/libsf_sip_preproc.so... done
Loading dynamic preprocessor library /usr/lib/snort_dynamicpreprocessor/libsf_ssh_preproc.so... done
Loading dynamic preprocessor library /usr/lib/snort_dynamicpreprocessor/libsf_pop_preproc.so... done
Loading dynamic preprocessor library /usr/lib/snort_dynamicpreprocessor/libsf_imap_preproc.so... done
Loading dynamic preprocessor library /usr/lib/snort_dynamicpreprocessor/libsf_ssl_preproc.so... done
Loading dynamic preprocessor library /usr/lib/snort_dynamicpreprocessor/libsf_modbus_preproc.so... done
Loading dynamic preprocessor library /usr/lib/snort_dynamicpreprocessor/libsf_dnp3_preproc.so... done
Loading dynamic preprocessor library /usr/lib/snort_dynamicpreprocessor/libsf_sdf_preproc.so... done
Loading dynamic preprocessor library /usr/lib/snort_dynamicpreprocessor/libsf_smtp_preproc.so... done
Loading dynamic preprocessor library /usr/lib/snort_dynamicpreprocessor/libsf_dns_preproc.so... done
Loading dynamic preprocessor library /usr/lib/snort_dynamicpreprocessor/libsf_reputation_preproc.so... done
Loading dynamic preprocessor library /usr/lib/snort_dynamicpreprocessor/libsf_dce2_preproc.so... done
```

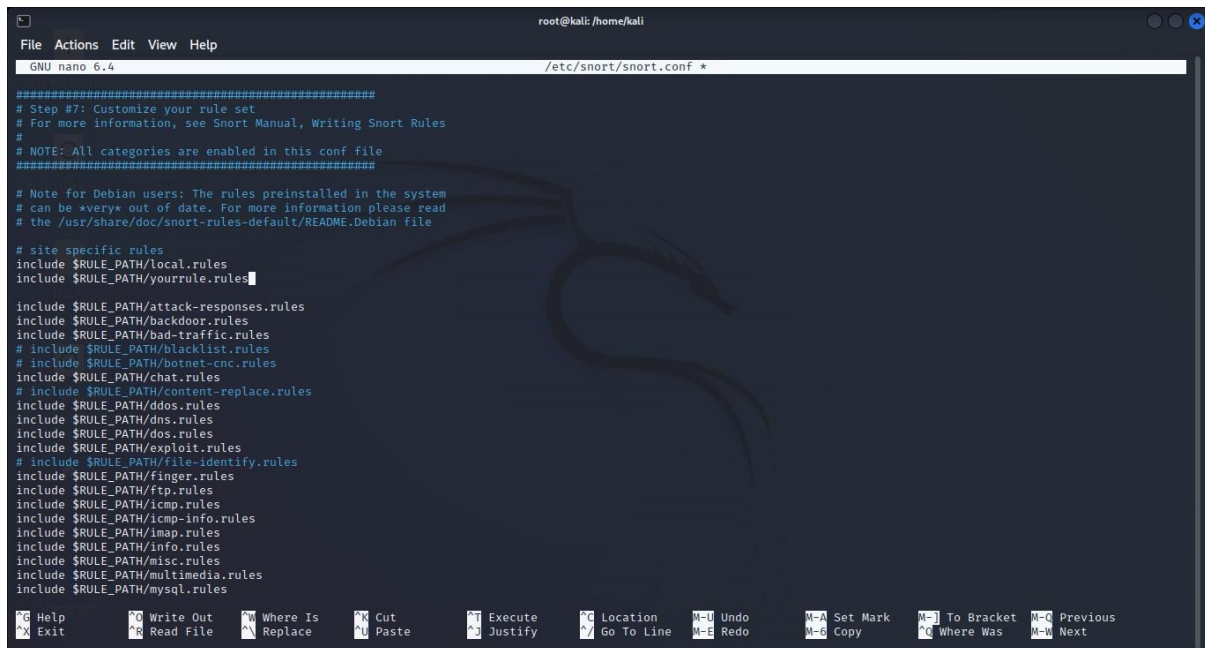
3) Add Rule to drop ICMP and TCP Packets

```
root@kali: /home/kali
File Actions Edit View Help

GNU nano 6.4 /etc/snort/rules/yourrule.rules *
alert icmp any any -> $HOME_NET any (msg:"ICMP test detected"; GID:1; sid:10000001; rev:001; classtype:icmp-event;)

File Name to Write: /etc/snort/rules/yourrule.rules
M-C Help M-D DOS Format M-A Append M-B Backup File
M-C Cancel M-M Mac Format M-P Prepend M-T Browse
```

4) Add the rules file to the main conf file



```
root@kali: /home/kali
File Actions Edit View Help
GNU nano 6.4 /etc/snort/snort.conf *
#####
# Step #7: Customize your rule set
# For more information, see Snort Manual, Writing Snort Rules
#
# NOTE: All categories are enabled in this conf file
#####

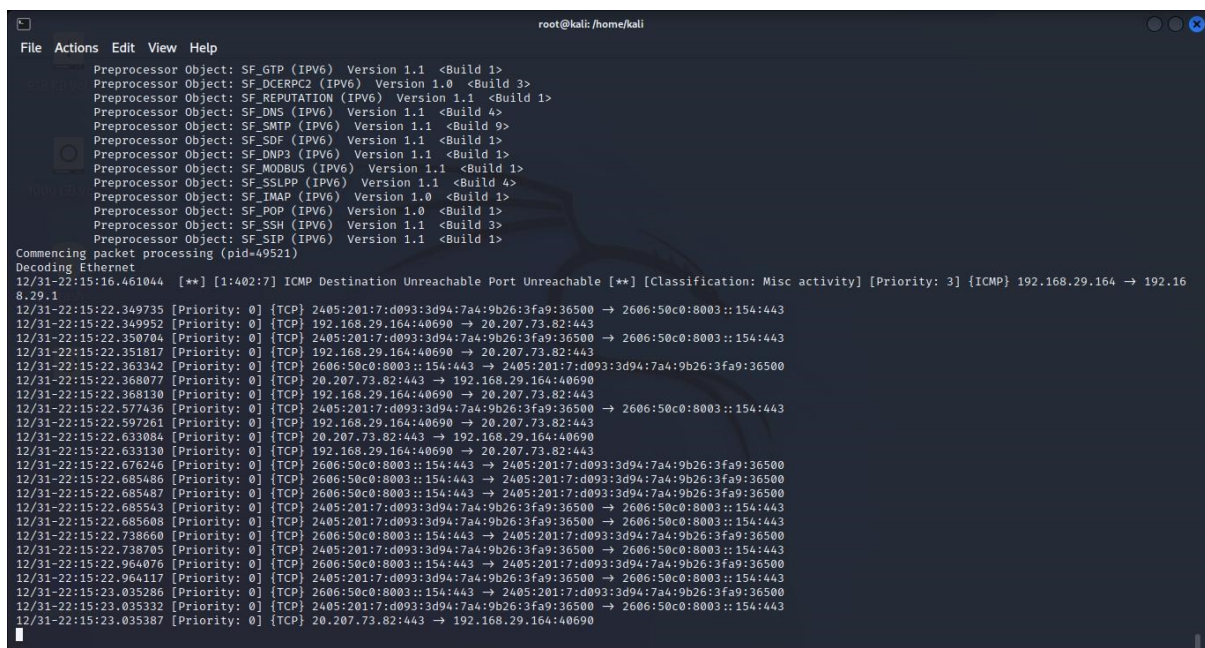
# Note for Debian users: The rules preinstalled in the system
# can be *very* out of date. For more information please read
# the /usr/share/doc/snort-rules-default/README.Debian file

# site specific rules
include $RULE_PATH/local.rules
include $RULE_PATH/yourrule.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/chat.rules
# include $RULE_PATH/content-replace.rules
include $RULE_PATH/ddos.rules
include $RULE_PATH/dns.rules
include $RULE_PATH/exploit.rules
# include $RULE_PATH/file-identify.rules
include $RULE_PATH/finger.rules
include $RULE_PATH/ftp.rules
include $RULE_PATH/icmp.rules
include $RULE_PATH/icmp-info.rules
include $RULE_PATH/imap.rules
include $RULE_PATH/misc.rules
include $RULE_PATH/multimedia.rules
include $RULE_PATH/mysql.rules

[Help] [Write Out] [Where Is] [Cut] [Execute] [Location] [Undo] [Set Mark] [To Bracket] [Previous]
[Exit] [Read File] [Replace] [Paste] [Justify] [Go To Line] [Redo] [Copy] [Where Was] [Next]
```

5) Save the file and run Snort to work as both IPS and IDS.



```
root@kali: /home/kali
File Actions Edit View Help
Preprocessor Object: SF_GTP (IPv6) Version 1.1 <Build 1>
Preprocessor Object: SF_DCEP2 (IPv6) Version 1.0 <Build 3>
Preprocessor Object: SF_REPUTATION (IPv6) Version 1.1 <Build 1>
Preprocessor Object: SF_DNS (IPv6) Version 1.1 <Build 4>
Preprocessor Object: SF_SMTP (IPv6) Version 1.1 <Build 9>
Preprocessor Object: SF_SDF (IPv6) Version 1.1 <Build 1>
Preprocessor Object: SF_DNP3 (IPv6) Version 1.1 <Build 1>
Preprocessor Object: SF_MODBUS (IPv6) Version 1.1 <Build 1>
Preprocessor Object: SF_SSLPP (IPv6) Version 1.1 <Build 4>
Preprocessor Object: SF_IMAP (IPv6) Version 1.0 <Build 1>
Preprocessor Object: SF_POP (IPv6) Version 1.0 <Build 1>
Preprocessor Object: SF_SSH (IPv6) Version 1.1 <Build 3>
Preprocessor Object: SF_STP (IPv6) Version 1.1 <Build 1>
Commencing packet processing (pid=49521)
Decoding Ethernet
12/31-22:15:16.461044 [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.29.164 → 192.168.29.1
12/31-22:15:22.349735 [Priority: 0] {TCP} 2405:201:7:d093:3d94:7a4:9b26:3fa9:36500 → 2606:50c0:8003::154:443
12/31-22:15:22.349952 [Priority: 0] {TCP} 192.168.29.164:40690 → 20.207.73.82:443
12/31-22:15:22.360704 [Priority: 0] {TCP} 2405:201:7:d093:3d94:7a4:9b26:3fa9:36500 → 2606:50c0:8003::154:443
12/31-22:15:22.351817 [Priority: 0] {TCP} 192.168.29.164:40690 → 20.207.73.82:443
12/31-22:15:22.363342 [Priority: 0] {TCP} 2606:50c0:8003::154:443 → 2405:201:7:d093:3d94:7a4:9b26:3fa9:36500
12/31-22:15:22.368077 [Priority: 0] {TCP} 20.207.73.82:443 → 192.168.29.164:40690
12/31-22:15:22.368130 [Priority: 0] {TCP} 192.168.29.164:40690 → 20.207.73.82:443
12/31-22:15:22.577436 [Priority: 0] {TCP} 2405:201:7:d093:3d94:7a4:9b26:3fa9:36500 → 2606:50c0:8003::154:443
12/31-22:15:22.597261 [Priority: 0] {TCP} 192.168.29.164:40690 → 20.207.73.82:443
12/31-22:15:22.633084 [Priority: 0] {TCP} 20.207.73.82:443 → 192.168.29.164:40690
12/31-22:15:22.633130 [Priority: 0] {TCP} 192.168.29.164:40690 → 20.207.73.82:443
12/31-22:15:22.676246 [Priority: 0] {TCP} 2606:50c0:8003::154:443 → 2405:201:7:d093:3d94:7a4:9b26:3fa9:36500
12/31-22:15:22.685486 [Priority: 0] {TCP} 2606:50c0:8003::154:443 → 2405:201:7:d093:3d94:7a4:9b26:3fa9:36500
12/31-22:15:22.685487 [Priority: 0] {TCP} 2606:50c0:8003::154:443 → 2405:201:7:d093:3d94:7a4:9b26:3fa9:36500
12/31-22:15:22.685543 [Priority: 0] {TCP} 2405:201:7:d093:3d94:7a4:9b26:3fa9:36500 → 2606:50c0:8003::154:443
12/31-22:15:22.685608 [Priority: 0] {TCP} 2405:201:7:d093:3d94:7a4:9b26:3fa9:36500 → 2606:50c0:8003::154:443
12/31-22:15:22.738660 [Priority: 0] {TCP} 2606:50c0:8003::154:443 → 2405:201:7:d093:3d94:7a4:9b26:3fa9:36500
12/31-22:15:22.738705 [Priority: 0] {TCP} 2405:201:7:d093:3d94:7a4:9b26:3fa9:36500 → 2606:50c0:8003::154:443
12/31-22:15:22.964076 [Priority: 0] {TCP} 2606:50c0:8003::154:443 → 2405:201:7:d093:3d94:7a4:9b26:3fa9:36500
12/31-22:15:22.964117 [Priority: 0] {TCP} 2405:201:7:d093:3d94:7a4:9b26:3fa9:36500 → 2606:50c0:8003::154:443
12/31-22:15:23.035286 [Priority: 0] {TCP} 2606:50c0:8003::154:443 → 2405:201:7:d093:3d94:7a4:9b26:3fa9:36500
12/31-22:15:23.035332 [Priority: 0] {TCP} 2405:201:7:d093:3d94:7a4:9b26:3fa9:36500 → 2606:50c0:8003::154:443
12/31-22:15:23.035387 [Priority: 0] {TCP} 20.207.73.82:443 → 192.168.29.164:40690
```

Snort is Monitoring the Traffic and showing Logs.

Snort is Setup as both IPS and IDS.

Output

Performing nmap from other device on the IDS that we setup

```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
└─$ sudo nmap -v -sT -O 192.168.29.164  
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-31 20:45 UTC  
Initiating Parallel DNS resolution of 1 host. at 20:45  
Completed Parallel DNS resolution of 1 host. at 20:45, 0.01s elapsed  
Initiating Connect Scan at 20:45  
Scanning 192.168.29.164 [1000 ports]  
Completed Connect Scan at 20:45, 0.03s elapsed (1000 total ports)  
Initiating OS detection (try #1) against 192.168.29.164  
Retrying OS detection (try #2) against 192.168.29.164  
Nmap scan report for 192.168.29.164  
Host is up (0.000086s latency).  
All 1000 scanned ports on 192.168.29.164 are in ignored states.  
Not shown: 1000 closed tcp ports (conn-refused)  
Too many fingerprints match this host to give specific OS details  
Network Distance: 0 hops  
  
Read data files from: /usr/bin/./share/nmap  
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 1.79 seconds  
Raw packets sent: 12 (1.668KB) | Rcvd: 22 (2.616KB)  
  
(kali@kali)-[~]  
└─$
```

Snort Detecting and showing Bad Traffic in Logs

```
root@kali: /home/kali  
File Actions Edit View Help  
  
[ Number of patterns truncated to 20 bytes: 1038 ]  
pcap DAQ configured to passive.  
The DAQ version does not support reload.  
Acquiring network traffic from "wlan0".  
Reload thread starting...  
Reload thread started, thread 0x7f90ee9f56c0 (21254)  
Decoding Ethernet  
  
-- Initialization Complete --  
  
--> Snort! <--  
o'')- Version 2.9.2.2 IPv6 GRE (Build 121)  
.... By Martin Roesch & The Snort Team: http://www.snort.org/snort/snort-team  
Copyright (C) 1998-2012 Sourcefire, Inc., et al.  
Using libpcap version 1.10.1 (with TPACKET_V3)  
Using PCRE version: 8.39 2016-06-14  
Using ZLIB version: 1.2.11  
  
Rules Engine: SF_SNORT_DETECTION_ENGINE Version 1.15 <Build 18>  
Preprocessor Object: SF_FTPTELNET (IPv6) Version 1.2 <Build 13>  
Preprocessor Object: SF_GTP (IPv6) Version 1.1 <Build 1>  
Preprocessor Object: SF_DCERPC2 (IPv6) Version 1.0 <Build 3>  
Preprocessor Object: SF_REPUTATION (IPv6) Version 1.1 <Build 1>  
Preprocessor Object: SF_DNS (IPv6) Version 1.1 <Build 4>  
Preprocessor Object: SF_SMTP (IPv6) Version 1.1 <Build 9>  
Preprocessor Object: SF_SDF (IPv6) Version 1.1 <Build 1>  
Preprocessor Object: SF_DNP3 (IPv6) Version 1.1 <Build 1>  
Preprocessor Object: SF_MODBUS (IPv6) Version 1.1 <Build 1>  
Preprocessor Object: SF_SSLPP (IPv6) Version 1.1 <Build 4>  
Preprocessor Object: SF_IMAP (IPv6) Version 1.0 <Build 1>  
Preprocessor Object: SF_POP (IPv6) Version 1.0 <Build 1>  
Preprocessor Object: SF_SSH (IPv6) Version 1.1 <Build 3>  
Preprocessor Object: SF_STP (IPv6) Version 1.1 <Build 1>  
  
Commencing packet processing (pid=21254)  
12/31-20:37:42.286042 [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.29.164 → 192.168.29.1  
12/31-20:39:25.096260 [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.29.164 → 192.168.29.1  
12/31-20:39:35.540338 [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 → 255.255.255.255:67  
12/31-20:39:35.540338 [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 → 255.255.255.255:67
```


Performing 2 attacks to check if Snort drops the Packets

```
kali@kali: ~  
File Actions Edit View Help  
[kali@kali]~$ sudo nmap -v -sT -O 192.168.29.164  
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-31 21:54 UTC  
Initiating Parallel DNS resolution of 1 host. at 21:54  
Completed Parallel DNS resolution of 1 host. at 21:54, 0.00s elapsed  
Initiating Connect Scan at 21:54  
Scanning 192.168.29.164 [1000 ports]  
Completed Connect Scan at 21:54, 0.03s elapsed (1000 total ports)  
Initiating OS detection (try #1) against 192.168.29.164  
Retrying OS detection (try #2) against 192.168.29.164  
Nmap scan report for 192.168.29.164  
Host is up (0.00012s latency).  
All 1000 scanned ports on 192.168.29.164 are in ignored states.  
Not shown: 1000 closed tcp ports (conn-refused)  
Too many fingerprints match this host to give specific OS details  
Network Distance: 0 hops  
  
Read data files from: /usr/bin/./share/nmap  
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 1.81 seconds  
Raw packets sent: 12 (1.668KB) | Rcvd: 22 (2.616KB)  
  
[kali@kali]~$ sudo hping3 -C 10000 -d 120 -S -w 64 -p 21 --flood --rand-source 192.168.29.164  
HPING 192.168.29.164 (wlan0 192.168.29.164): S set, 40 headers + 120 data bytes  
hping in flood mode, no replies will be shown
```

Snort Drops all Packages and returns 0 packets

```
root@kali: /home/kali  
File Actions Edit View Help  
12/31-22:22:58.580910 [**] [1:528:5] BAD-Traffic loopback traffic [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 127.64.200.23:19192 → 192.168.2  
9.1:21  
12/31-22:22:58.632925 [**] [1:528:5] BAD-Traffic loopback traffic [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 127.243.163.157:19460 → 192.168  
.29.1:21  
12/31-22:22:58.719245 [**] [1:528:5] BAD-Traffic loopback traffic [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 127.185.219.154:20238 → 192.168  
.29.1:21  
12/31-22:22:58.726613 [**] [1:528:5] BAD-Traffic loopback traffic [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 127.53.13.157:20326 → 192.168.2  
9.1:21  
12/31-22:22:58.727254 [**] [1:528:5] BAD-Traffic loopback traffic [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 127.79.158.226:20335 → 192.168.  
29.1:21  
12/31-22:22:58.730935 [**] [1:528:5] BAD-Traffic loopback traffic [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 127.8.142.54:20381 → 192.168.29  
.1:21  
12/31-22:22:58.743365 [**] [1:528:5] BAD-Traffic loopback traffic [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 127.216.17.7:20523 → 192.168.29  
.1:21  
12/31-22:22:58.752979 [**] [1:528:5] BAD-Traffic loopback traffic [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 127.172.177.254:20720 → 192.168  
.29.1:21  
12/31-22:22:58.947257 [**] [1:528:5] BAD-Traffic loopback traffic [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 127.15.92.123:21397 → 192.168.2  
9.1:21  
12/31-22:22:59.001997 [**] [1:528:5] BAD-Traffic loopback traffic [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 127.13.44.45:21849 → 192.168.29  
.1:21  
12/31-22:22:59.022352 [**] [1:528:5] BAD-Traffic loopback traffic [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 127.7.166.223:22461 → 192.168.2  
9.1:21  
12/31-22:22:59.023087 [**] [1:528:5] BAD-Traffic loopback traffic [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 127.142.174.165:22504 → 192.168  
.29.1:21  
12/31-22:22:59.027651 [**] [1:528:5] BAD-Traffic loopback traffic [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 127.152.45.222:22638 → 192.168.  
29.1:21  
12/31-22:22:59.039160 [**] [1:528:5] BAD-Traffic loopback traffic [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 127.60.1.32:22882 → 192.168.29.  
1:21  
12/31-22:22:59.041071 [**] [1:528:5] BAD-Traffic loopback traffic [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 127.4.139.231:22995 → 192.168.2  
9.1:21  
12/31-22:22:59.044007 [**] [1:528:5] BAD-Traffic loopback traffic [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 127.189.180.145:23116 → 192.168  
.29.1:21  
12/31-22:22:59.044718 [**] [1:528:5] BAD-Traffic loopback traffic [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 127.242.75.162:23146 → 192.168.  
29.1:21  
12/31-22:22:59.048397 [**] [1:528:5] BAD-Traffic loopback traffic [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 127.242.162.199:23230 → 192.168  
29.1:21  
12/31-22:22:59.052681 [**] [1:528:5] BAD-Traffic loopback traffic [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 127.245.205.126:23377 → 192.168  
.29.1:21  
12/31-22:22:59.055429 [**] [1:528:5] BAD-Traffic loopback traffic [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 127.39.243.107:23409 → 192.168.  
29.1:21
```

References

1. <https://www.snort.org/>
2. <https://www.snort.org/#documents>
3. <https://serverfault.com/questions/tagged/snort>
4. <https://security.stackexchange.com/questions/tagged/snort>
5. <https://github.com/snort3/snort3>
6. <https://suricata.io/>