INTEGRATION OF IDS (SNORT) AND SPLUNK

Cybersecurity IDS & SIEM

2025

MICHAEL MUSOKE

Contents

Intrusion Detection System (Snort) and System Information Event Management (Splunk)

Abstract

Intrusion Detection Systems (IDS) play an important role in modern cybersecurity by identifying malicious activity and potential threats in real-time. This demo will illustrate the configuration of an IDS (SNORT). The alerts generated based on the custom rules set will be forwarded to an SIEM Splunk for further analysis. The demo will be divided into two parts.

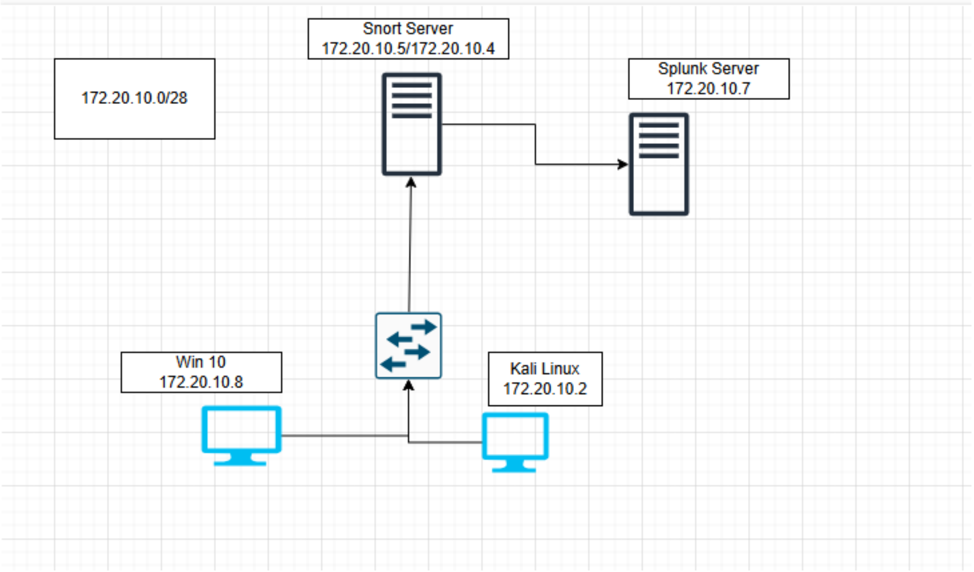
1. Configure IDS with custom rules
2. Forward the alerts generated to SIEM for analysis

Objectives

1. Configure SNORT used to detect intrusion (IDS)
2. Configure SPLUNK used to analyse data. (SIEM)
3. Configure rules that will used to flag unauthorised activity.

The setup comprises: 2 Ubuntu (Snort and Splunk), 1 Kali Linux and 1 Windows 10

Topology

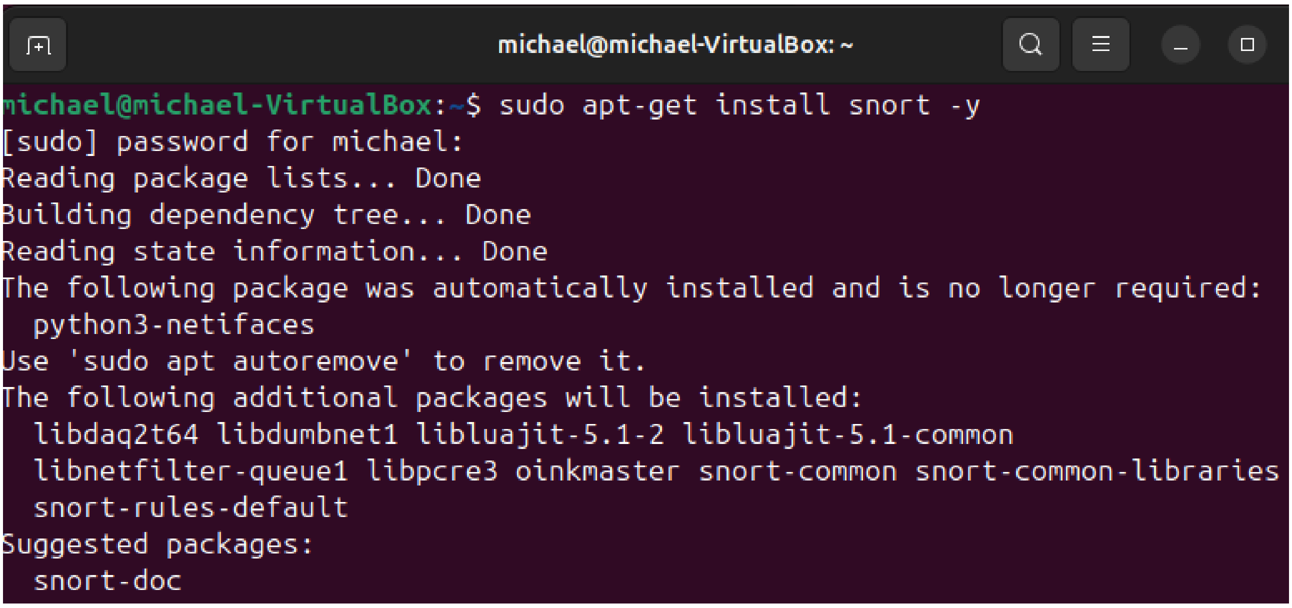


Introduction

Snort is an open-source network Intrusion Detection and prevention System (IDS/IPS) that monitors networks in real-time. It uses rule-based instructions to analyse packets and data and identify suspicious patterns. Snort, as an IDS, generates alerts for detected threats that can be logged locally or forwarded to a System Information Event Management (SIEM). Snort is widely used in enterprise and research environments for network security monitoring. In this demo, Snort will be used as an IDS.

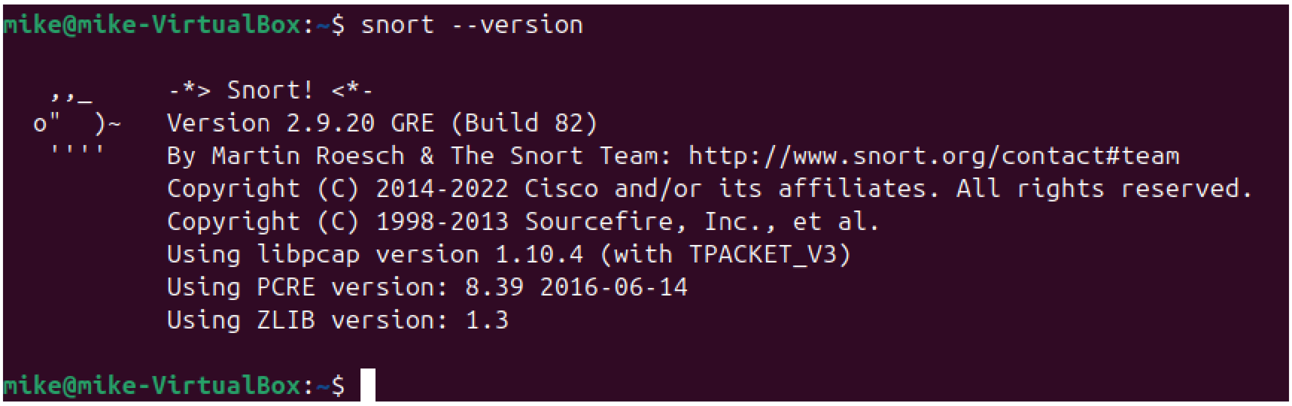
Installing and Configuring Snort.

Log on to an Ubuntu device and run the update and upgrade commands to get latest versions of the repositories onto your device. **sudo apt-get update && sudo apt-get upgrade -y.**
With the update and upgrade done run the command to install snort **sudo apt-get install snort -y**



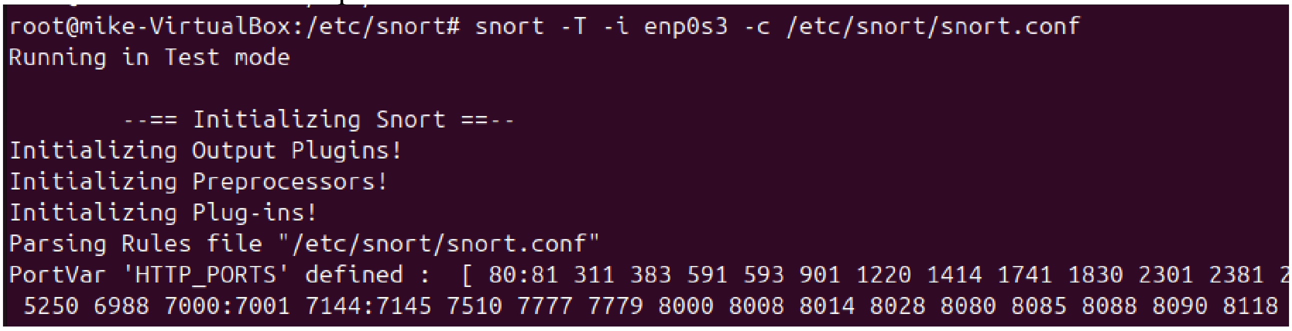
```
michael@michael-VirtualBox:~$ sudo apt-get install snort -y
[sudo] password for michael:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following package was automatically installed and is no longer required:
  python3-netifaces
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  libdaq2t64 libdumbnet1 libluajit-5.1-2 libluajit-5.1-common
  libnetfilter-queue1 libpcre3 oinkmaster snort-common snort-common-libraries
  snort-rules-default
Suggested packages:
  snort-doc
```

After the installation is complete check that snort was installed properly by using the next tow commands. **snort –version**. This will display the version of snort installed.



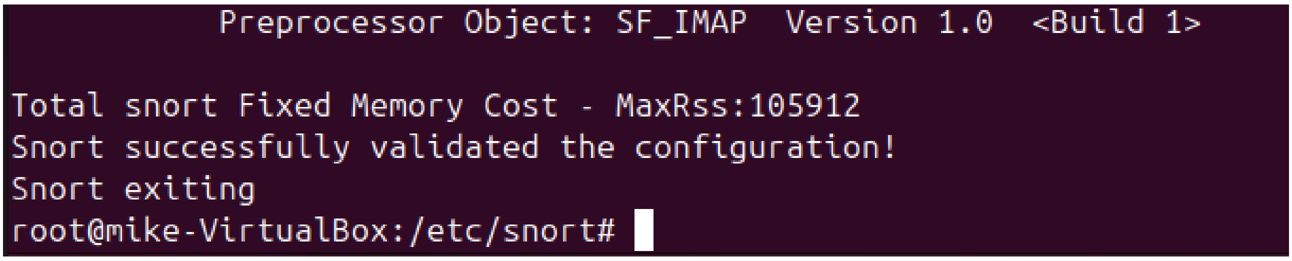
```
mike@mike-VirtualBox:~$ snort --version

   ,,_     -*> 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

mike@mike-VirtualBox:~$ 
```

Start snort in test mode to validate the configuration using the command **snort -T -i enp0s3 -c /etc/snort/snort.conf**. (-T = test mode, -i = network interface, -c = configuration file). Use man snort to read about extra options



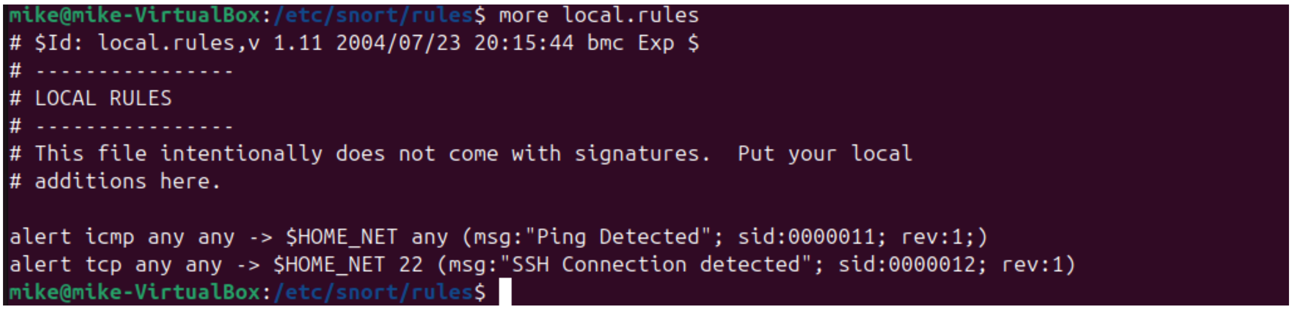
```
root@mike-VirtualBox:/etc/snort# snort -T -i enp0s3 -c /etc/snort/snort.conf
Running in Test mode

        --== 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 2
 5250 6988 7000:7001 7144:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118
```

After this is complete snort will exit



```
           Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>

Total snort Fixed Memory Cost - MaxRss:105912
Snort successfully validated the configuration!
Snort exiting
root@mike-VirtualBox:/etc/snort#
```

Navigate to the file **local.rules** to custom rules for this demo. The intention is to detect **ICMP** pings and **SSH** connections to any device on the network. The local.rules files is the in **/etc/snort/rules** directory

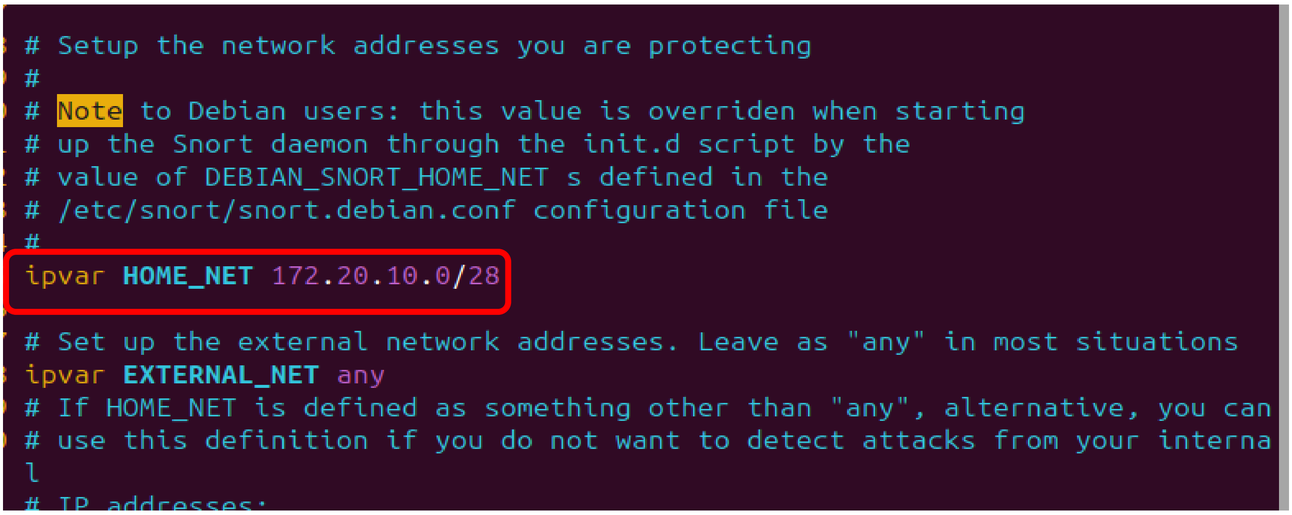


```
mike@mike-VirtualBox:/etc/snort/rules$ more local.rules
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
# ----------------
# LOCAL RULES
# ----------------
# This file intentionally does not come with signatures.  Put your local
# additions here.

alert icmp any any -> $HOME_NET any (msg:"Ping Detected"; sid:0000011; rev:1;)
alert tcp any any -> $HOME_NET 22 (msg:"SSH Connection detected"; sid:0000012; rev:1)
mike@mike-VirtualBox:/etc/snort/rules$
```

Using a test editor type in the rule **alert icmp any any -> $HOME_NET any (msg: “Ping Detected”; sid:00000011; rev:1;)** and **alert tcp any any -> $HOME_NET 22 (msg: “SSH Connection detected”; sid:00000012; rev1)**

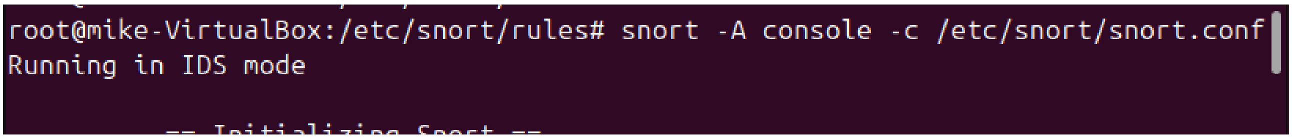
rule 1 means raise an alert if/when an ICMP from any device from any source address -> to. $HOME_NET any msg to display Ping Detected sid is the signature Identification number rev is the revision number. NB for the sid the number has to be one million and above as any number below may clash with one of the community rules
Rule 2 is the same as rule 1 but is particularly concerned with port 22 SSH. Save and exit the file

In the **/etc/snort/snort.conf** make sure the that network that needs to to monitored is configured and the external_net is any since an attack can be initiated from any IP address.



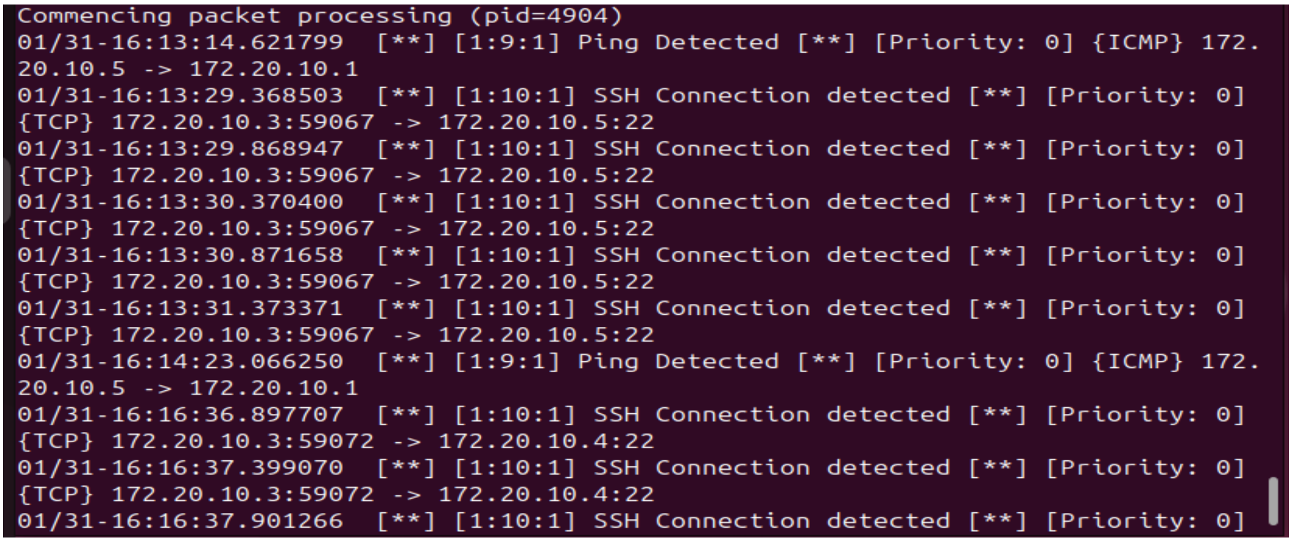
```
# Setup the network addresses you are protecting
#
# Note to Debian users: this value is overriden when starting
# up the Snort daemon through the init.d script by the
# value of DEBIAN_SNORT_HOME_NET s defined in the
# /etc/snort/snort.debian.conf configuration file
#
ipvar HOME_NET 172.20.10.0/28

# 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 interna
l
# IP addresses:
```

Start snort in detection mode using the command **snort -A console -c /etc/snort/snort.conf**



```
root@mike-VirtualBox:/etc/snort/rules# snort -A console -c /etc/snort/snort.conf
Running in IDS mode

        == Initializing Snort ==
```

Form a device on the network and ping any other device on the network. In this demo snort server pings the default gateway and from the host device SSH to the snort server.



```
Commencing packet processing (pid=4904)
01/31-16:13:14.621799  [**] [1:9:1] Ping Detected [**] [Priority: 0] {ICMP} 172.
20.10.5 -> 172.20.10.1
01/31-16:13:29.368503  [**] [1:10:1] SSH Connection detected [**] [Priority: 0]
{TCP} 172.20.10.3:59067 -> 172.20.10.5:22
01/31-16:13:29.868947  [**] [1:10:1] SSH Connection detected [**] [Priority: 0]
{TCP} 172.20.10.3:59067 -> 172.20.10.5:22
01/31-16:13:30.370400  [**] [1:10:1] SSH Connection detected [**] [Priority: 0]
{TCP} 172.20.10.3:59067 -> 172.20.10.5:22
01/31-16:13:30.871658  [**] [1:10:1] SSH Connection detected [**] [Priority: 0]
{TCP} 172.20.10.3:59067 -> 172.20.10.5:22
01/31-16:13:31.373371  [**] [1:10:1] SSH Connection detected [**] [Priority: 0]
{TCP} 172.20.10.3:59067 -> 172.20.10.5:22
01/31-16:14:23.066250  [**] [1:9:1] Ping Detected [**] [Priority: 0] {ICMP} 172.
20.10.5 -> 172.20.10.1
01/31-16:16:36.897707  [**] [1:10:1] SSH Connection detected [**] [Priority: 0]
{TCP} 172.20.10.3:59072 -> 172.20.10.4:22
01/31-16:16:37.399070  [**] [1:10:1] SSH Connection detected [**] [Priority: 0]
{TCP} 172.20.10.3:59072 -> 172.20.10.4:22
01/31-16:16:37.901266  [**] [1:10:1] SSH Connection detected [**] [Priority: 0]
```

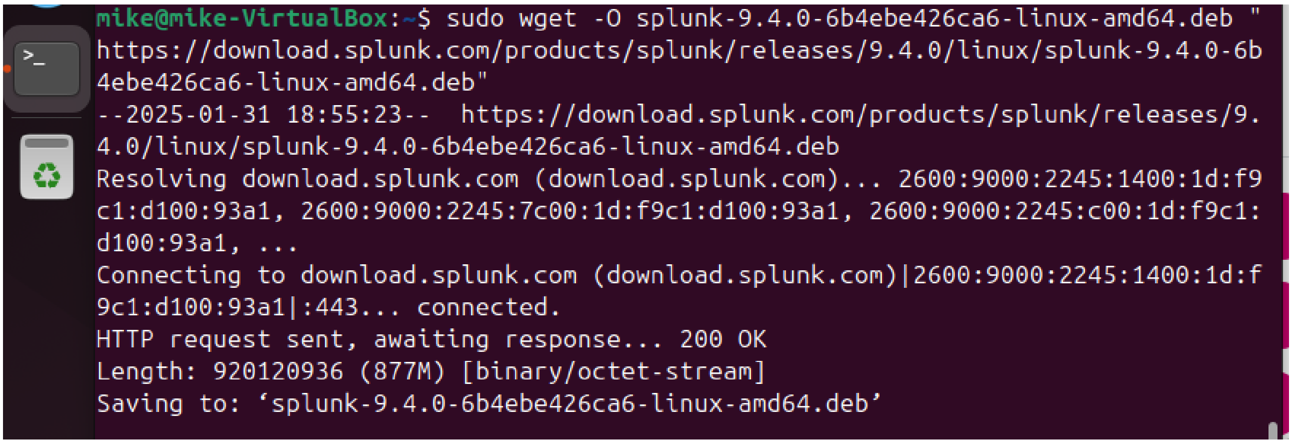
Snort server 172.20.10.5, gateway 172.20.10.1, host= 172.20.10.3

Part 2 - Installing and Configuring Splunk

In part 2 of this documentation, configuring Splunk to analyse the data collected on the snort IDS will be the main focus.

Splunk is a Security information event management platform that collects, analyses and visualises data from various sources such as logs, network traffic and security events. It helps security teams in organisations gain real-time insights into their infrastructure, detect threats and streamline incident response.
Splunk works by ingesting data from multiple sources, indexing it and allowing authorised users to search, correlate and produce visual representation of the information collected. By using Splunk Query Language (SPL) dashboards, alerts and automated responses are used to enhance threat detection and operational efficiency.
Splunk is commonly used for log analysis, intrusion detection, compliance monitoring, and forensic investigations. Its ability to integrate with IDS tools like snort makes it a valuable asset for security teams to centralise and analyse security events effectively

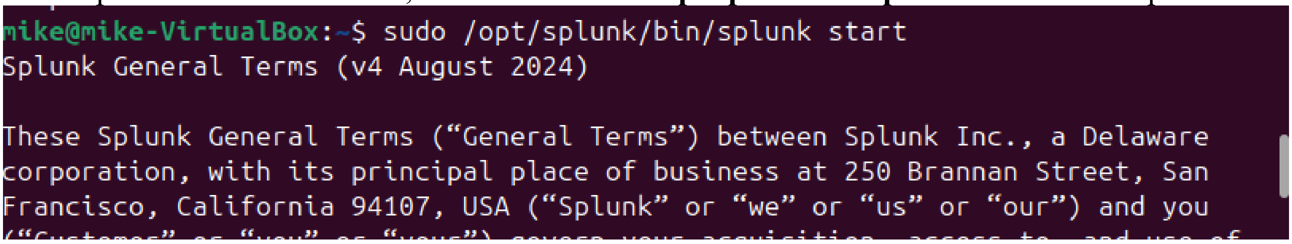
On the other Ubuntu VM, install Splunk. To download Splunk an active email address is required to download Splunk software. Using the **wget** command download the latest Splunk package.



```
mike@mike-VirtualBox:~$ sudo wget -O splunk-9.4.0-6b4ebe426ca6-linux-amd64.deb "
https://download.splunk.com/products/splunk/releases/9.4.0/linux/splunk-9.4.0-6b
4ebe426ca6-linux-amd64.deb"
--2025-01-31 18:55:23--  https://download.splunk.com/products/splunk/releases/9.
4.0/linux/splunk-9.4.0-6b4ebe426ca6-linux-amd64.deb
Resolving download.splunk.com (download.splunk.com)... 2600:9000:2245:1400:1d:f9
c1:d100:93a1, 2600:9000:2245:7c00:1d:f9c1:d100:93a1, 2600:9000:2245:c00:1d:f9c1:
d100:93a1, ...
Connecting to download.splunk.com (download.splunk.com)|2600:9000:2245:1400:1d:f
9c1:d100:93a1|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 920120936 (877M) [binary/octet-stream]
Saving to: ‘splunk-9.4.0-6b4ebe426ca6-linux-amd64.deb’
```

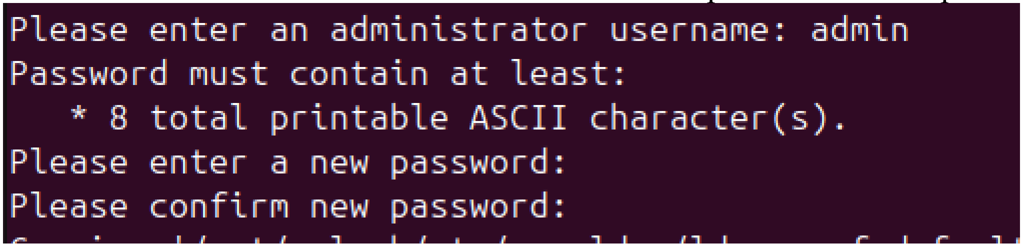
Install the splunk package using the command **dpkg -i <splunk package>**

After Splunk has been installed, use the command **/opt/splunk/bin/splunk** start to start Splunk



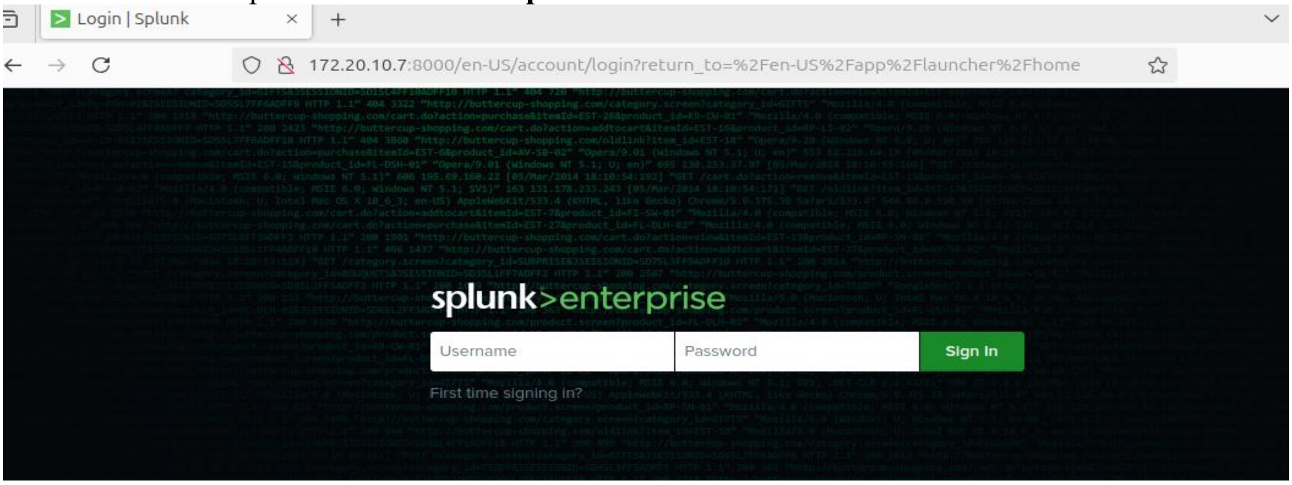
```
mike@mike-VirtualBox:~$ sudo /opt/splunk/bin/splunk start
Splunk General Terms (v4 August 2024)

These Splunk General Terms (“General Terms”) between Splunk Inc., a Delaware
corporation, with its principal place of business at 250 Brannan Street, San
Francisco, California 94107, USA (“Splunk” or “we” or “us” or “our”) and you
(“Customer” or “you” or “your”) governs your acquisition, access to, and use of
```

Type Y at the prompt when required to agree to the license agreement Press the space bar through the terms and conditions. Provide an administrator username and password for the splunk login.



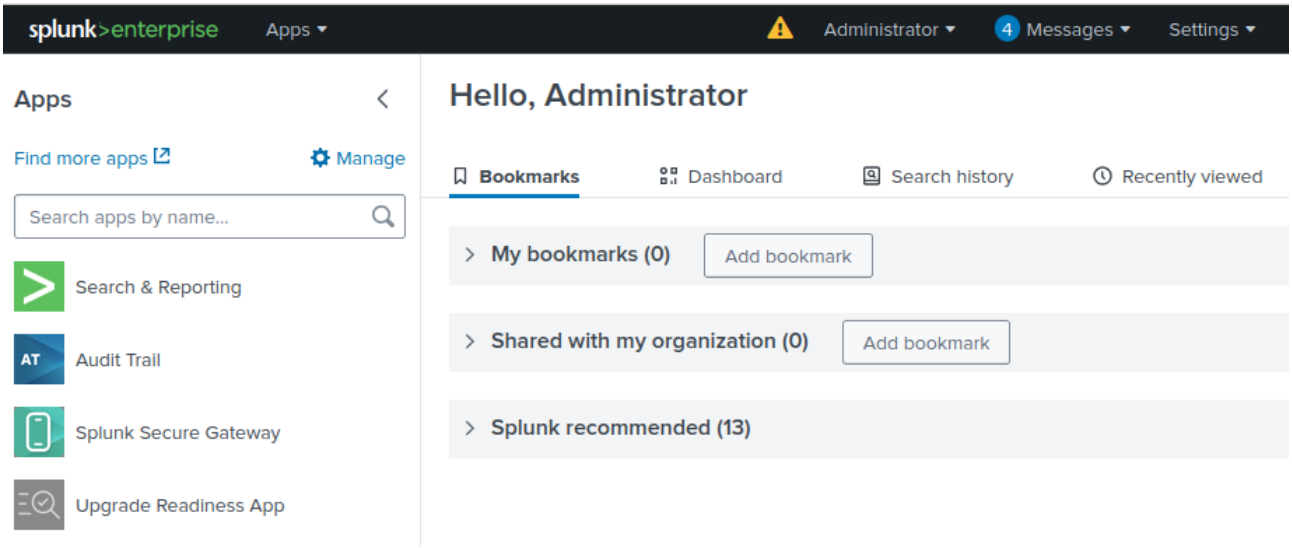
```
Please enter an administrator username: admin
Password must contain at least:
   * 8 total printable ASCII character(s).
Please enter a new password:
Please confirm new password:
```

Once the installation is complete. On a web browser type the IP address of the server followed by the port number to access Splunk on the web. **http://<IP address:8000>**

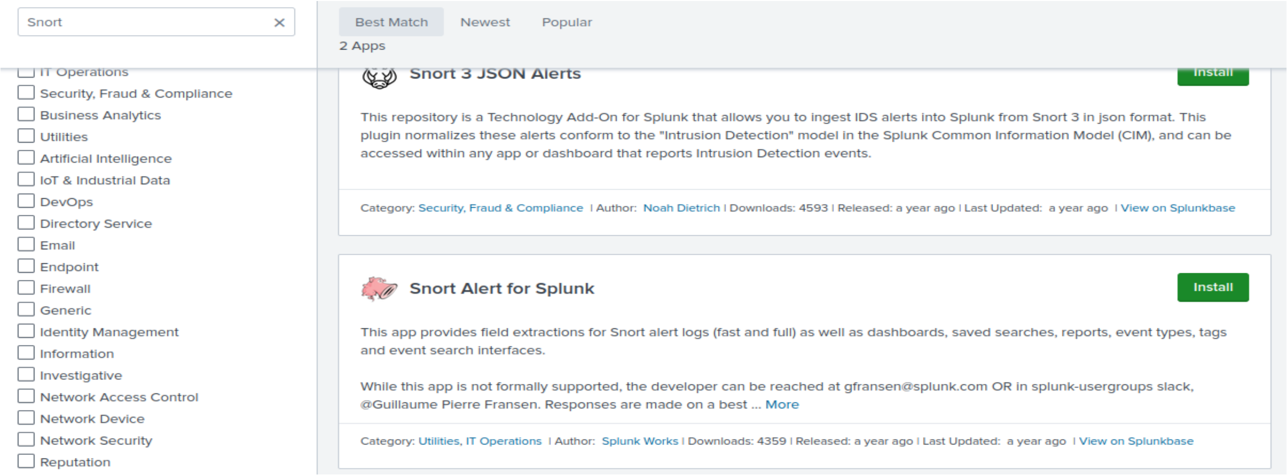


Login | Splunk
172.20.10.7:8000/en-US/account/login?return_to=%2Fen-US%2Fapp%2Flauncher%2Fhome
splunk>enterprise
Username
Password
Sign In
First time signing in?

With username and password submitted during the installation log into Splunk.



Splunk has the ability to integrate with various other technologies snort being one of them. Under apps snort API can be installed.



Snort 3 JSON Alerts

This repository is a Technology Add-On for Splunk that allows you to ingest IDS alerts into Splunk from Snort 3 in json format. This plugin normalizes these alerts conform to the "Intrusion Detection" model in the Splunk Common Information Model (CIM), and can be accessed within any app or dashboard that reports Intrusion Detection events.

Category: Security, Fraud & Compliance | Author: Noah Dietrich | Downloads: 4593 | Released: a year ago | Last Updated: a year ago | View on Splunkbase

Snort Alert for Splunk

This app provides field extractions for Snort alert logs (fast and full) as well as dashboards, saved searches, reports, event types, tags and event search interfaces.

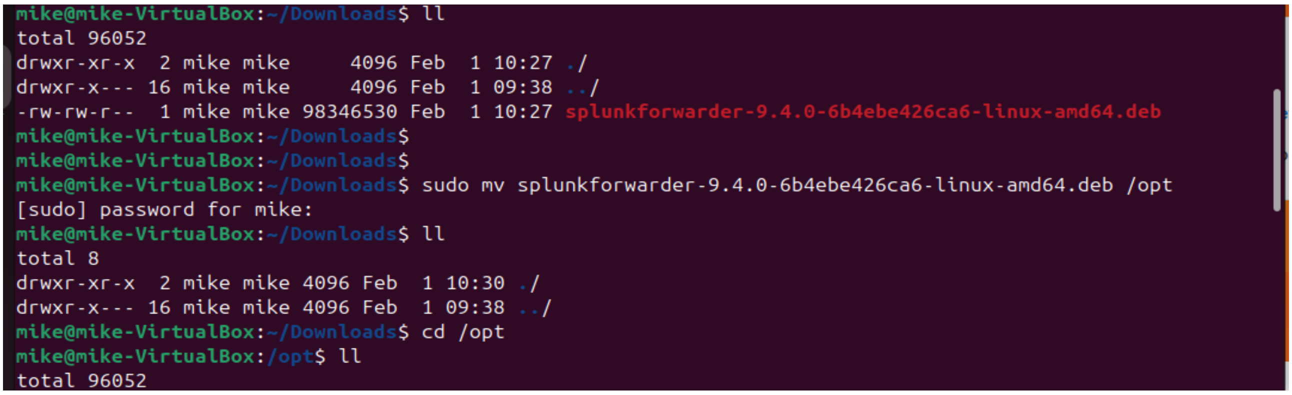
While this app is not formally supported, the developer can be reached at gfransen@splunk.com OR in splunk-usergroups slack, @Guillaume Pierre Fransen. Responses are made on a best ... More

Category: Utilities, IT Operations | Author: Splunk Works | Downloads: 4359 | Released: a year ago | Last Updated: a year ago | View on Splunkbase

Click Install and allow them the import of data through port 9997

Next, a universal data forwarder will need to be installed on the snort server. This is to help export the data collected from the log files into the Splunk server.

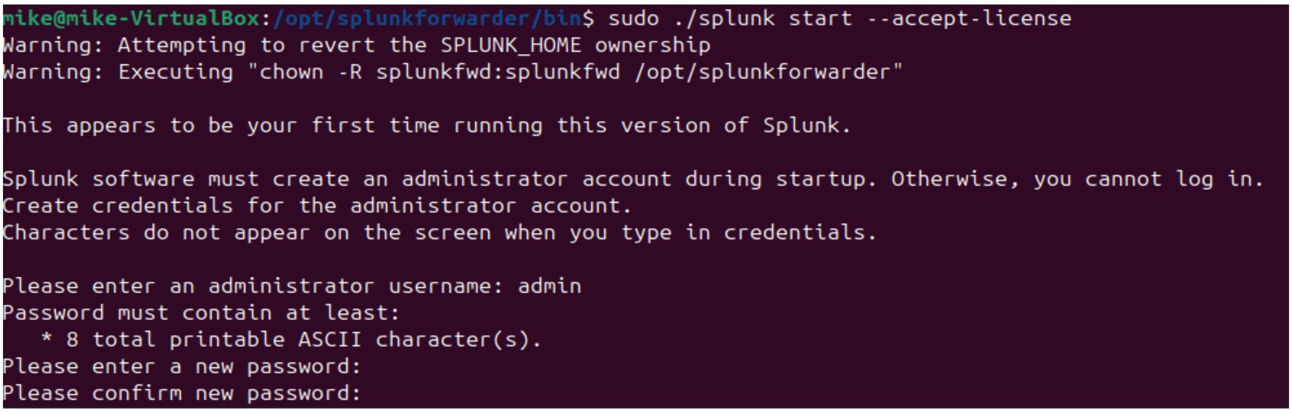
On the snort server download Splunk forwarder for the Splunk website, using the **wget** command.



```
mike@mike-VirtualBox:~/Downloads$ ll
total 96052
drwxr-xr-x  2 mike mike     4096 Feb  1 10:27 ./
drwxr-x--- 16 mike mike     4096 Feb  1 09:38 ../
-rw-rw-r--  1 mike mike 98346530 Feb  1 10:27 splunkforwarder-9.4.0-6b4ebe426ca6-linux-amd64.deb
mike@mike-VirtualBox:~/Downloads$
mike@mike-VirtualBox:~/Downloads$
mike@mike-VirtualBox:~/Downloads$ sudo mv splunkforwarder-9.4.0-6b4ebe426ca6-linux-amd64.deb /opt
[sudo] password for mike:
mike@mike-VirtualBox:~/Downloads$ ll
total 8
drwxr-xr-x  2 mike mike 4096 Feb  1 10:30 ./
drwxr-x--- 16 mike mike 4096 Feb  1 09:38 ../
mike@mike-VirtualBox:~/Downloads$ cd /opt
mike@mike-VirtualBox:/opt$ ll
total 96052
```

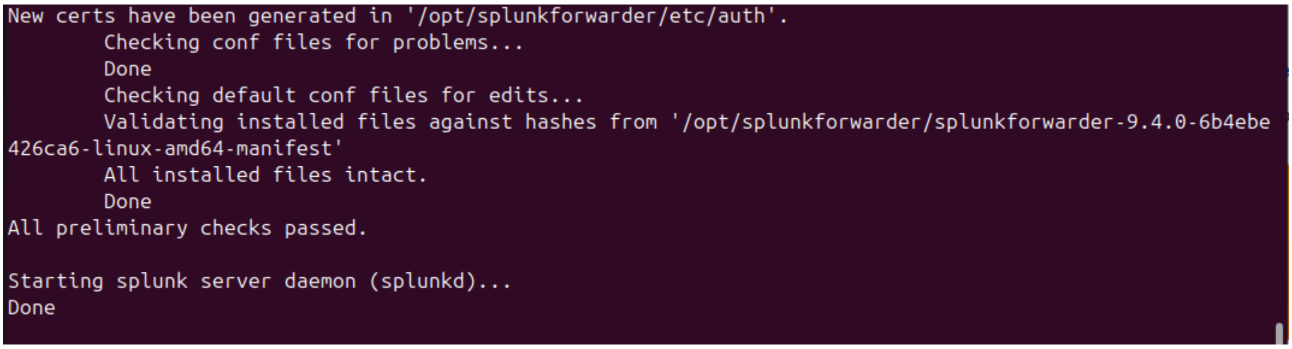
Install the splunkforwarder using the dpkg command i.e. **dpkg -i <name of splunkforwarder>**

When the installation is complete start the forwarder navigate to the forwarder binary folder use the command **./splunk start –accept-license**



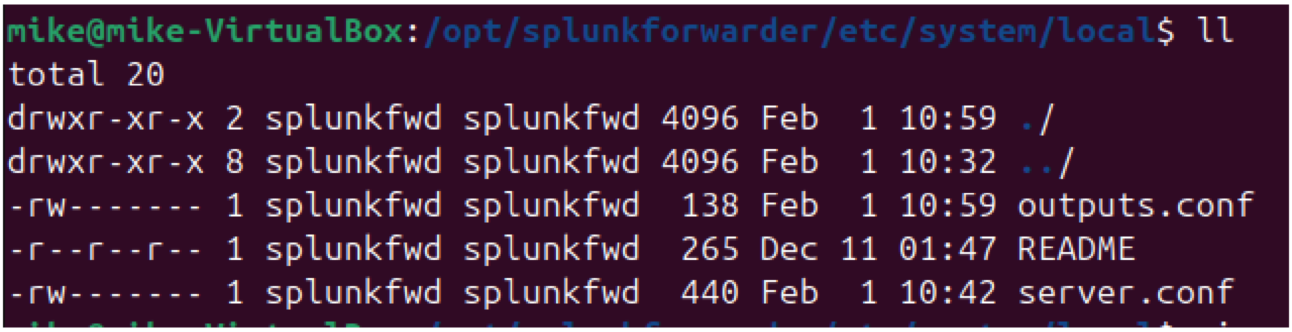
```
mike@mike-VirtualBox:/opt/splunkforwarder/bin$ sudo ./splunk start --accept-license
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"

This appears to be your first time running this version of Splunk.

Splunk software must create an administrator account during startup. Otherwise, you cannot log in.
Create credentials for the administrator account.
Characters do not appear on the screen when you type in credentials.

Please enter an administrator username: admin
Password must contain at least:
   * 8 total printable ASCII character(s).
Please enter a new password:
Please confirm new password:
```

Provide an administrator username and password.
After the installation is complete check there not errors in the preliminary checks



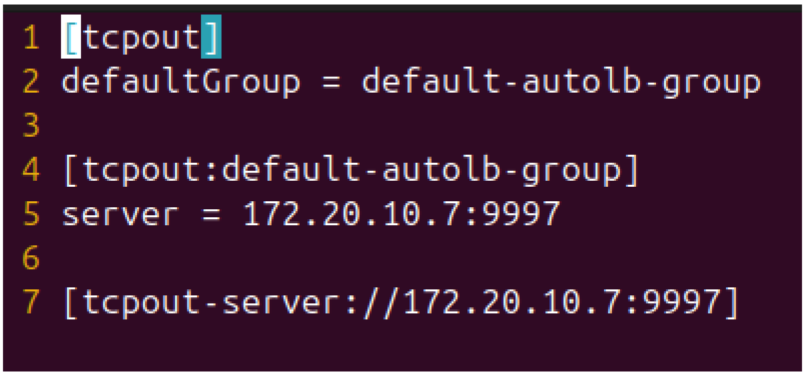
```
New certs have been generated in '/opt/splunkforwarder/etc/auth'.
        Checking conf files for problems...
        Done
        Checking default conf files for edits...
        Validating installed files against hashes from '/opt/splunkforwarder/splunkforwarder-9.4.0-6b4ebe
426ca6-linux-amd64-manifest'
        All installed files intact.
        Done
All preliminary checks passed.

Starting splunk server daemon (splunkd)...
Done
```

Navigate to **/opt/splunkforwarder/etc/system/local** and edit the outputs.conf file



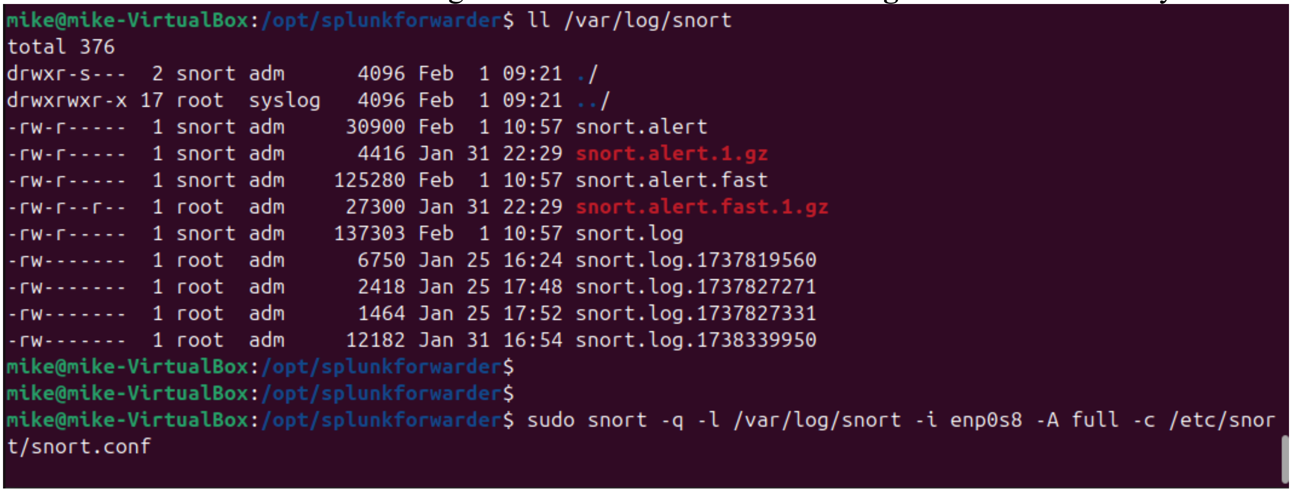
```
mike@mike-VirtualBox:/opt/splunkforwarder/etc/system/local$ ll
total 20
drwxr-xr-x 2 splunkfwd splunkfwd 4096 Feb  1 10:59 ./
drwxr-xr-x 8 splunkfwd splunkfwd 4096 Feb  1 10:32 ../
-rw------- 1 splunkfwd splunkfwd  138 Feb  1 10:59 outputs.conf
-r--r--r-- 1 splunkfwd splunkfwd  265 Dec 11 01:47 README
-rw------- 1 splunkfwd splunkfwd  440 Feb  1 10:42 server.conf
```

Make sure that the details in the file are correct. server = <IP address of the splunk server>:port number. And the **tcpout** is also correct



```
[tcpout]
defaultGroup = default-autolb-group

[tcpout:default-autolb-group]
server = 172.20.10.7:9997

[tcpout-server://172.20.10.7:9997]
```

If the details are correct test that log file can be created in the **/var/log/snort/alert** directory



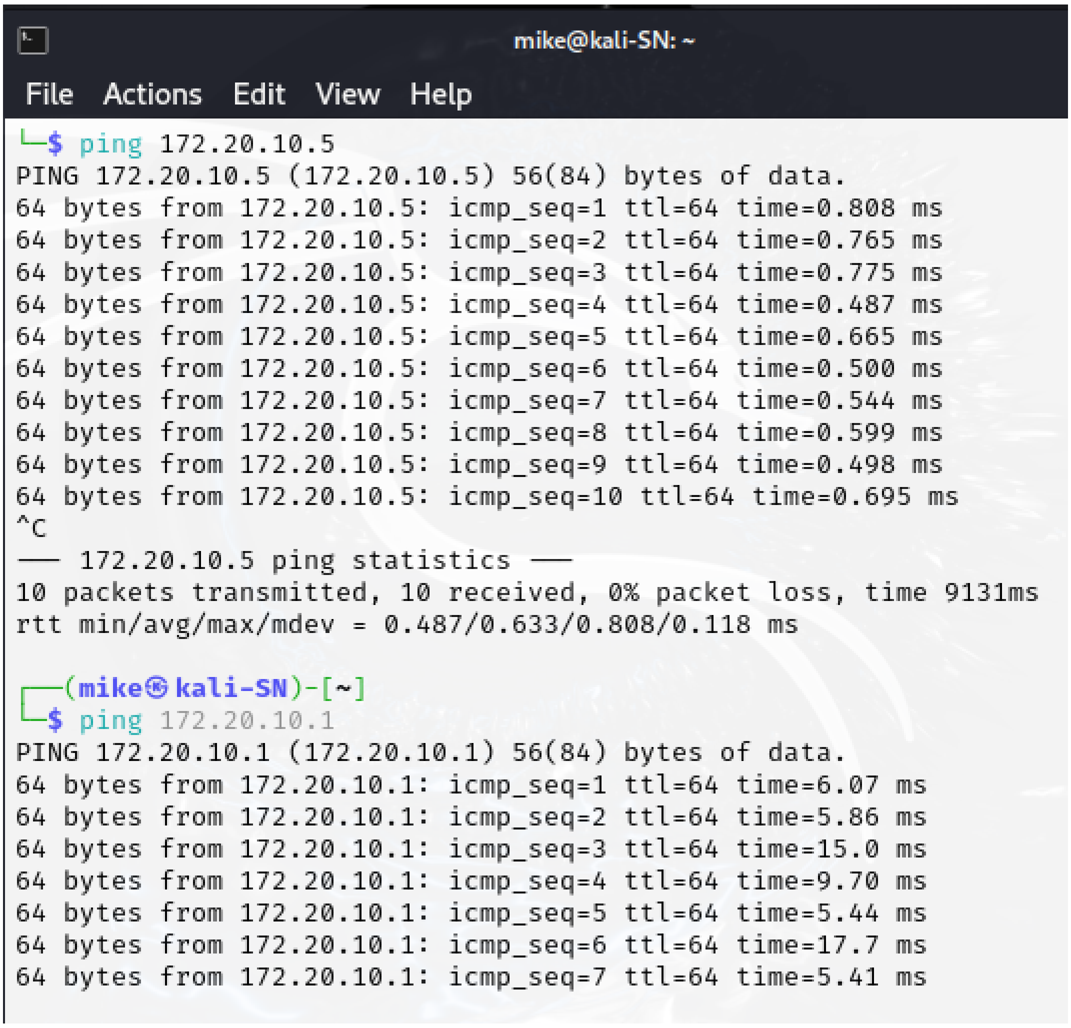
```
mike@mike-VirtualBox:/opt/splunkforwarder$ ll /var/log/snort
total 376
drwxr-s---  2 snort adm      4096 Feb  1 09:21 ./
drwxrwxr-x 17 root  syslog   4096 Feb  1 09:21 ../
-rw-r-----  1 snort adm     30900 Feb  1 10:57 snort.alert
-rw-r-----  1 snort adm      4416 Jan 31 22:29 snort.alert.1.gz
-rw-r-----  1 snort adm    125280 Feb  1 10:57 snort.alert.fast
-rw-r--r--  1 root  adm     27300 Jan 31 22:29 snort.alert.fast.1.gz
-rw-r-----  1 snort adm    137303 Feb  1 10:57 snort.log
-rw-------  1 root  adm      6750 Jan 25 16:24 snort.log.1737819560
-rw-------  1 root  adm      2418 Jan 25 17:48 snort.log.1737827271
-rw-------  1 root  adm      1464 Jan 25 17:52 snort.log.1737827331
-rw-------  1 root  adm     12182 Jan 31 16:54 snort.log.1738339950
mike@mike-VirtualBox:/opt/splunkforwarder$
mike@mike-VirtualBox:/opt/splunkforwarder$
mike@mike-VirtualBox:/opt/splunkforwarder$ sudo snort -q -l /var/log/snort -i enp0s8 -A full -c /etc/snor
t/snort.conf
```

start the snort server with the l option so the logs are created. Use the command **snort -q -l /var/log/snort -i <network interface> -A full -c <snort configuration file>**

-q = quiet mode
-l = record logs to the file
-i = network interface
-A = generate alerts
-c = configuration file

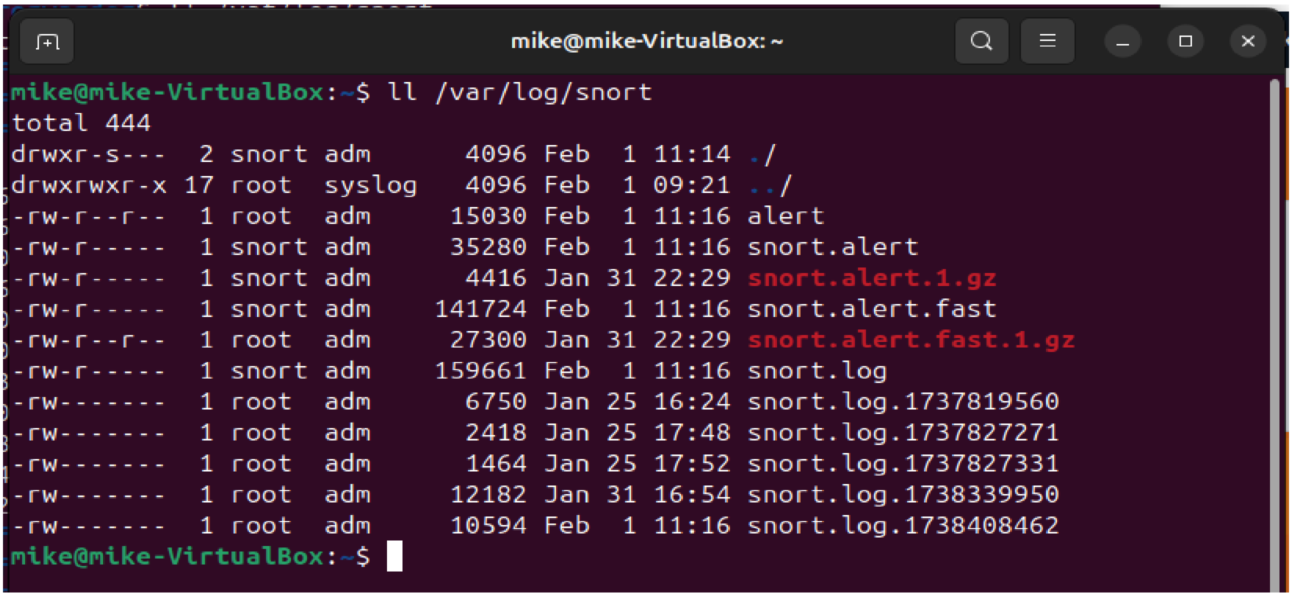
Integration of Snort and Splunk Servers

To test log on the Kali Linux, ping some of the devices on the network so some data is generated



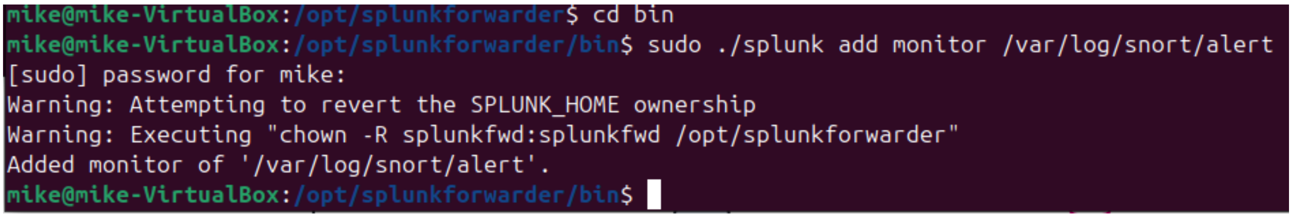
```
└─$ ping 172.20.10.5
PING 172.20.10.5 (172.20.10.5) 56(84) bytes of data.
64 bytes from 172.20.10.5: icmp_seq=1 ttl=64 time=0.808 ms
64 bytes from 172.20.10.5: icmp_seq=2 ttl=64 time=0.765 ms
64 bytes from 172.20.10.5: icmp_seq=3 ttl=64 time=0.775 ms
64 bytes from 172.20.10.5: icmp_seq=4 ttl=64 time=0.487 ms
64 bytes from 172.20.10.5: icmp_seq=5 ttl=64 time=0.665 ms
64 bytes from 172.20.10.5: icmp_seq=6 ttl=64 time=0.500 ms
64 bytes from 172.20.10.5: icmp_seq=7 ttl=64 time=0.544 ms
64 bytes from 172.20.10.5: icmp_seq=8 ttl=64 time=0.599 ms
64 bytes from 172.20.10.5: icmp_seq=9 ttl=64 time=0.498 ms
64 bytes from 172.20.10.5: icmp_seq=10 ttl=64 time=0.695 ms
^C
── 172.20.10.5 ping statistics ──
10 packets transmitted, 10 received, 0% packet loss, time 9131ms
rtt min/avg/max/mdev = 0.487/0.633/0.808/0.118 ms

┌──(mike㉿kali-SN)-[~]
└─$ ping 172.20.10.1
PING 172.20.10.1 (172.20.10.1) 56(84) bytes of data.
64 bytes from 172.20.10.1: icmp_seq=1 ttl=64 time=6.07 ms
64 bytes from 172.20.10.1: icmp_seq=2 ttl=64 time=5.86 ms
64 bytes from 172.20.10.1: icmp_seq=3 ttl=64 time=15.0 ms
64 bytes from 172.20.10.1: icmp_seq=4 ttl=64 time=9.70 ms
64 bytes from 172.20.10.1: icmp_seq=5 ttl=64 time=5.44 ms
64 bytes from 172.20.10.1: icmp_seq=6 ttl=64 time=17.7 ms
64 bytes from 172.20.10.1: icmp_seq=7 ttl=64 time=5.41 ms
```

Navigate to the /var/log/snort can check that the **alert file** has been created



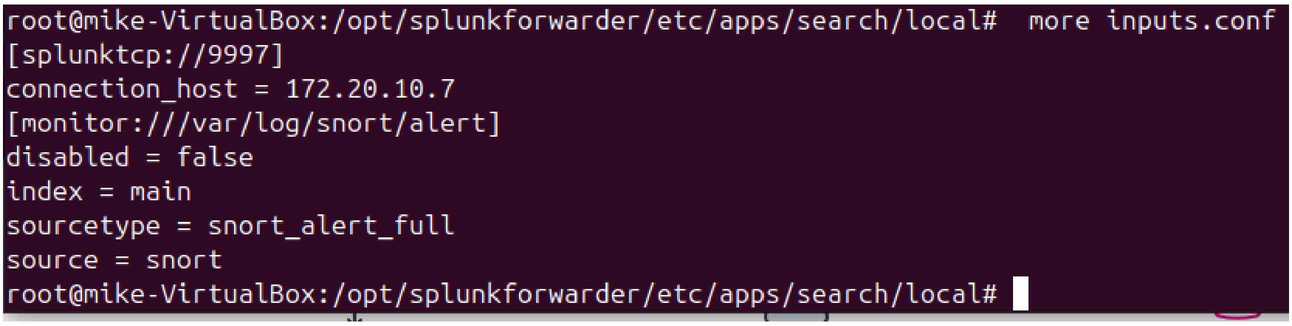
```
mike@mike-VirtualBox:~$ ll /var/log/snort
total 444
drwxr-s---  2 snort adm      4096 Feb  1 11:14 ./
drwxrwxr-x 17 root  syslog   4096 Feb  1 09:21 ../
-rw-r--r--  1 root  adm     15030 Feb  1 11:16 alert
-rw-r-----  1 snort adm     35280 Feb  1 11:16 snort.alert
-rw-r-----  1 snort adm      4416 Jan 31 22:29 snort.alert.1.gz
-rw-r-----  1 snort adm    141724 Feb  1 11:16 snort.alert.fast
-rw-r--r--  1 root  adm     27300 Jan 31 22:29 snort.alert.fast.1.gz
-rw-r-----  1 snort adm    159661 Feb  1 11:16 snort.log
-rw-------  1 root  adm      6750 Jan 25 16:24 snort.log.1737819560
-rw-------  1 root  adm      2418 Jan 25 17:48 snort.log.1737827271
-rw-------  1 root  adm      1464 Jan 25 17:52 snort.log.1737827331
-rw-------  1 root  adm     12182 Jan 31 16:54 snort.log.1738339950
-rw-------  1 root  adm     10594 Feb  1 11:16 snort.log.1738408462
mike@mike-VirtualBox:~$
```

Next is to add the alert file to be monitored use the command in the bin directory **./splunk add monitor <name of the file to be monitored>**



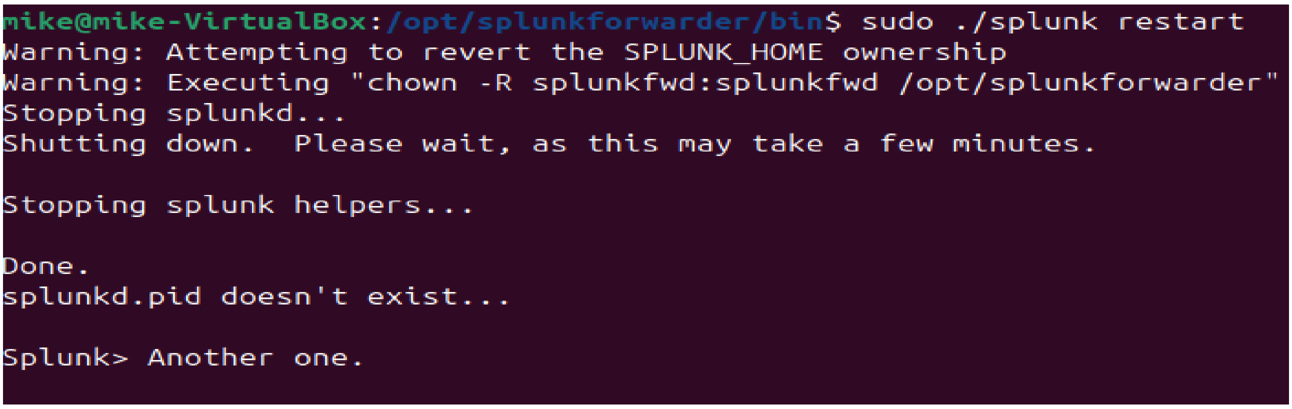
```
mike@mike-VirtualBox:/opt/splunkforwarder$ cd bin
mike@mike-VirtualBox:/opt/splunkforwarder/bin$ sudo ./splunk add monitor /var/log/snort/alert
[sudo] password for mike:
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Added monitor of '/var/log/snort/alert'.
mike@mike-VirtualBox:/opt/splunkforwarder/bin$ 
```

Next, check that the inputs.conf file has the correct details. This is the file that that forwarder will refer to for the details of the connection to the Splunk server and port, file to be monitored.



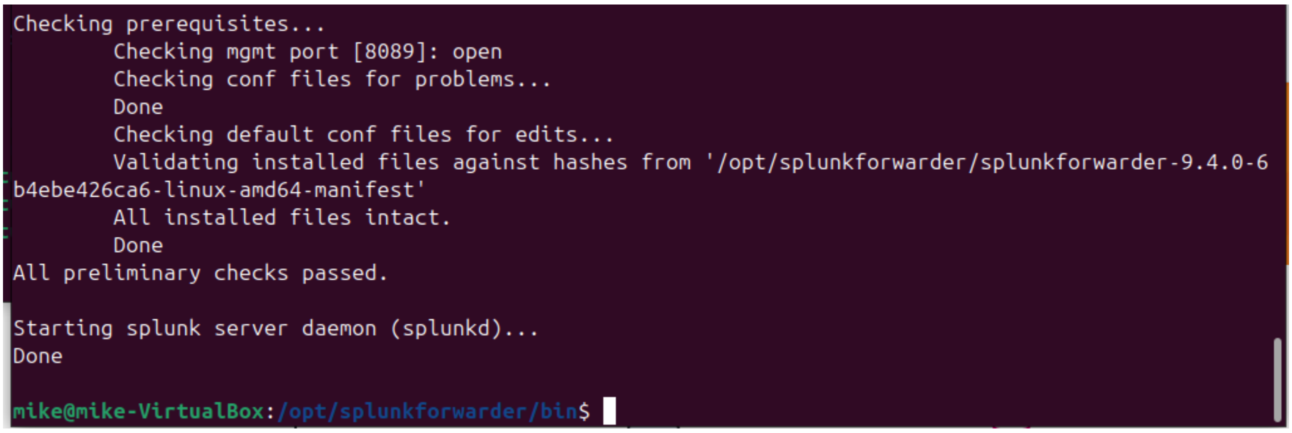
```
root@mike-VirtualBox:/opt/splunkforwarder/etc/apps/search/local#  more inputs.conf
[splunktcp://9997]
connection_host = 172.20.10.7
[monitor:///var/log/snort/alert]
disabled = false
index = main
sourcetype = snort_alert_full
source = snort
root@mike-VirtualBox:/opt/splunkforwarder/etc/apps/search/local# 
```

If any change is made to the inputs.conf file, splunkforwarder will need to be restarted



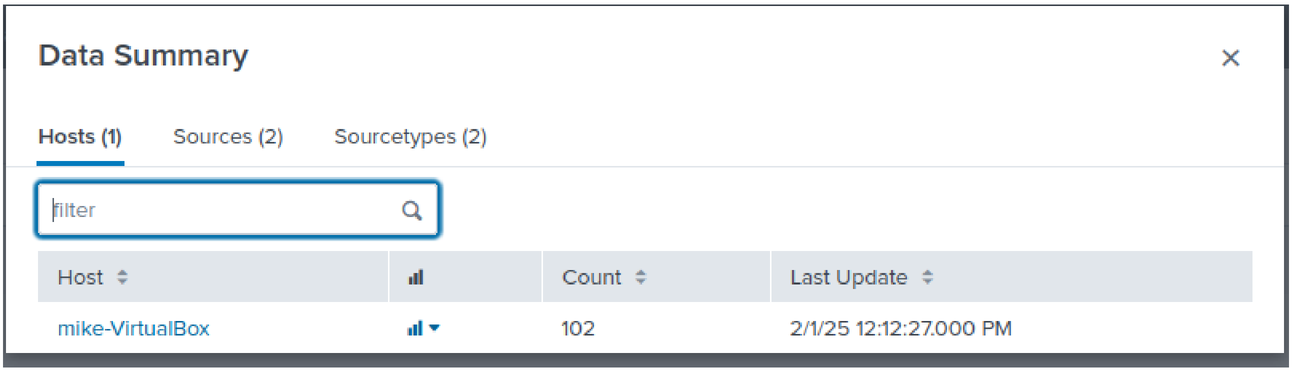
```
mike@mike-VirtualBox:/opt/splunkforwarder/bin$ sudo ./splunk restart
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Stopping splunkd...
Shutting down.  Please wait, as this may take a few minutes.

Stopping splunk helpers...

Done.
splunkd.pid doesn't exist...

Splunk> Another one.
```

Again, make sure that there are no errors in the configuration



```
Checking prerequisites...
        Checking mgmt port [8089]: open
        Checking conf files for problems...
        Done
        Checking default conf files for edits...
        Validating installed files against hashes from '/opt/splunkforwarder/splunkforwarder-9.4.0-6
b4ebe426ca6-linux-amd64-manifest'
        All installed files intact.
        Done
All preliminary checks passed.

Starting splunk server daemon (splunkd)...
Done

mike@mike-VirtualBox:/opt/splunkforwarder/bin$ 
```

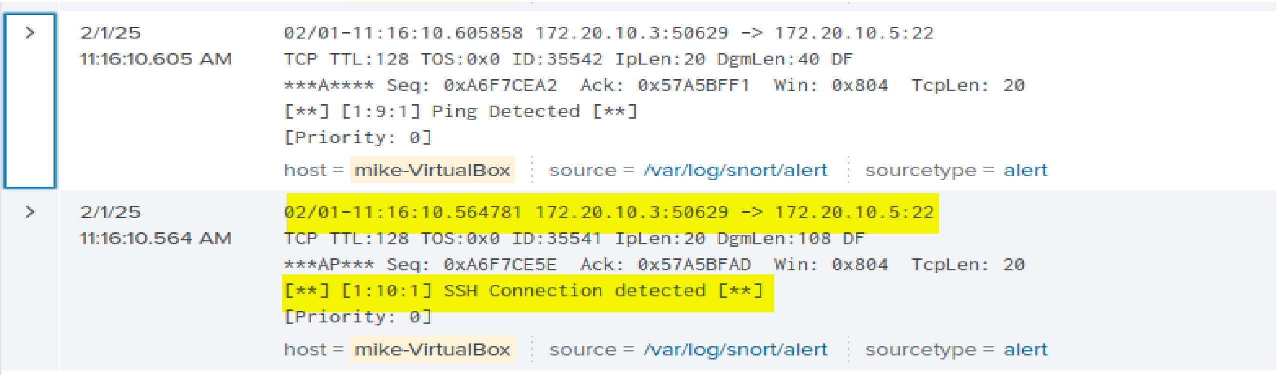
On the Splunk server under Search and Reporting > Data summary, the imported file should be available



Host		Count	Last Update
mike-VirtualBox		102	2/1/25 12:12:27.000 PM

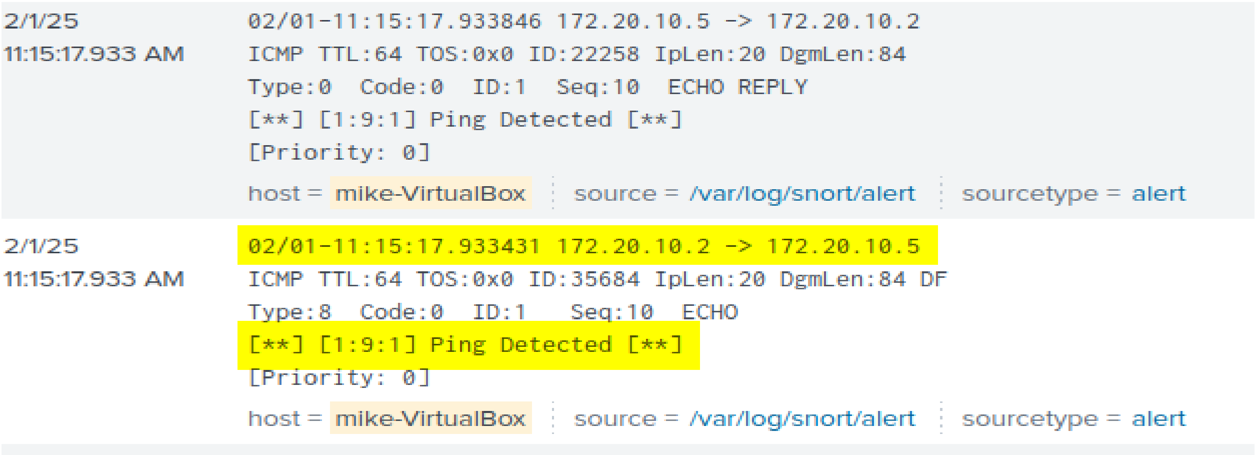
Click on the file to open it (mike-VirtualBox)

The ssh connection was detected from the host device to the snort server



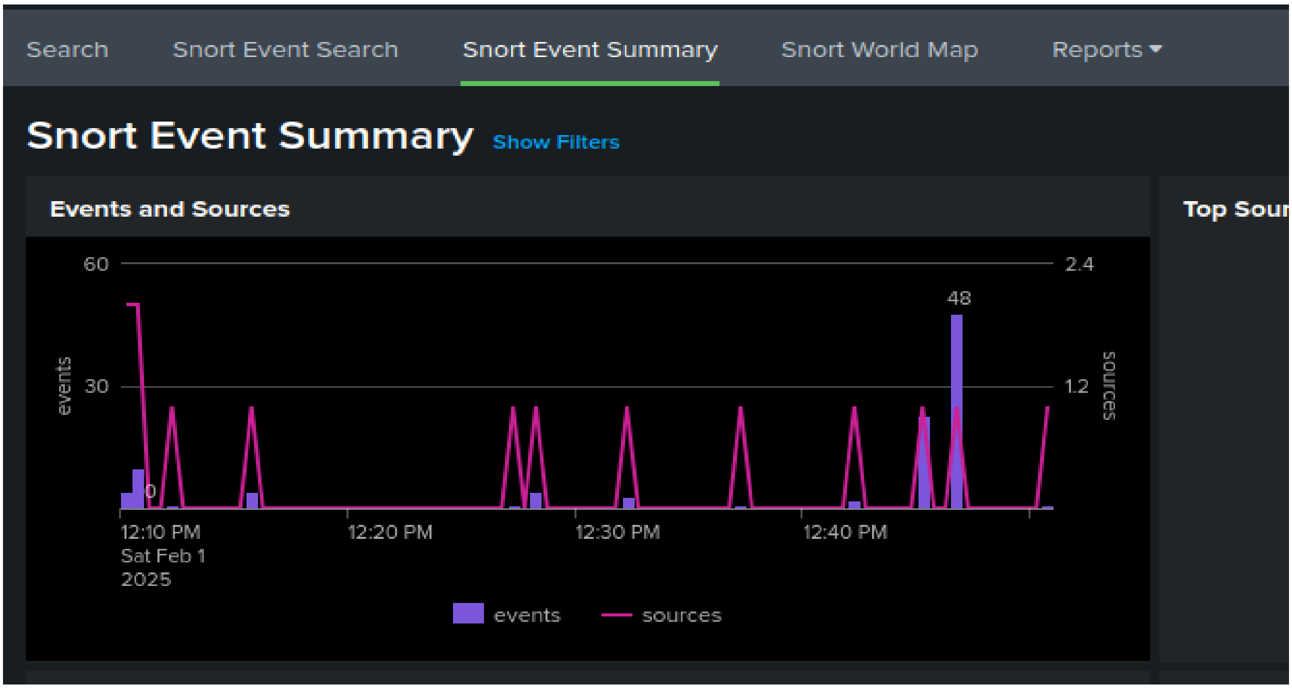
```
2/1/25            02/01-11:16:10.605858 172.20.10.3:50629 -> 172.20.10.5:22
11:16:10.605 AM   TCP TTL:128 TOS:0x0 ID:35542 IpLen:20 DgmLen:40 DF
                  ***A**** Seq: 0xA6F7CEA2  Ack: 0x57A5BFF1  Win: 0x804  TcpLen: 20
                  [**] [1:9:1] Ping Detected [**]
                  [Priority: 0]
                  host = mike-VirtualBox   source = /var/log/snort/alert   sourcetype = alert

2/1/25            02/01-11:16:10.564781 172.20.10.3:50629 -> 172.20.10.5:22
11:16:10.564 AM   TCP TTL:128 TOS:0x0 ID:35541 IpLen:20 DgmLen:108 DF
                  ***AP*** Seq: 0xA6F7CE5E  Ack: 0x57A5BFAD  Win: 0x804  TcpLen: 20
                  [**] [1:10:1] SSH Connection detected [**]
                  [Priority: 0]
                  host = mike-VirtualBox   source = /var/log/snort/alert   sourcetype = alert
```

Ping detected from snort server to Kali Linux

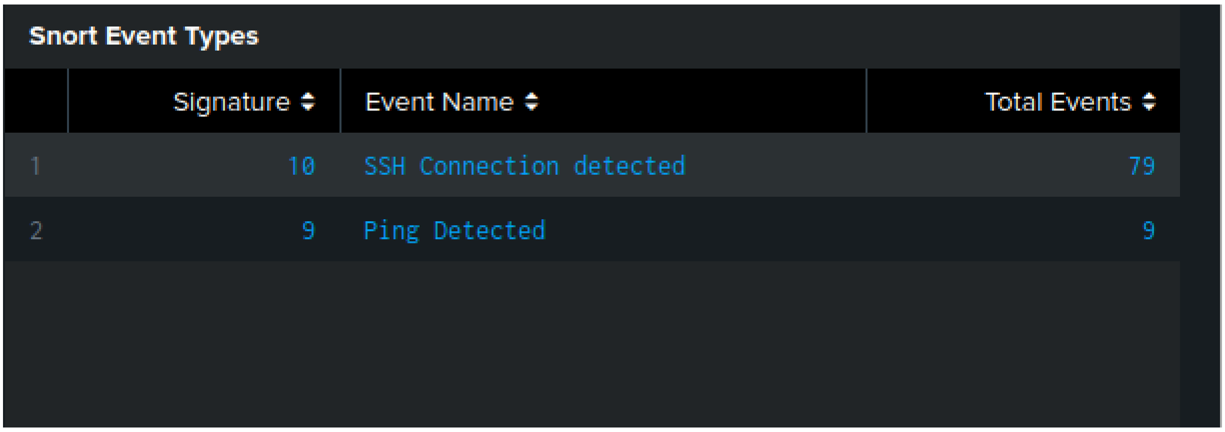


```
2/1/25            02/01-11:15:17.933846 172.20.10.5 -> 172.20.10.2
11:15:17.933 AM   ICMP TTL:64 TOS:0x0 ID:22258 IpLen:20 DgmLen:84
                  Type:0  Code:0  ID:1  Seq:10  ECHO REPLY
                  [**] [1:9:1] Ping Detected [**]
                  [Priority: 0]
                  host = mike-VirtualBox   source = /var/log/snort/alert   sourcetype = alert

2/1/25            02/01-11:15:17.933431 172.20.10.2 -> 172.20.10.5
11:15:17.933 AM   ICMP TTL:64 TOS:0x0 ID:35684 IpLen:20 DgmLen:84 DF
                  Type:8  Code:0  ID:1   Seq:10  ECHO
                  [**] [1:9:1] Ping Detected [**]
                  [Priority: 0]
                  host = mike-VirtualBox   source = /var/log/snort/alert   sourcetype = alert
```

In the snort app that was installed, under snort event summary a graphical representation is generated



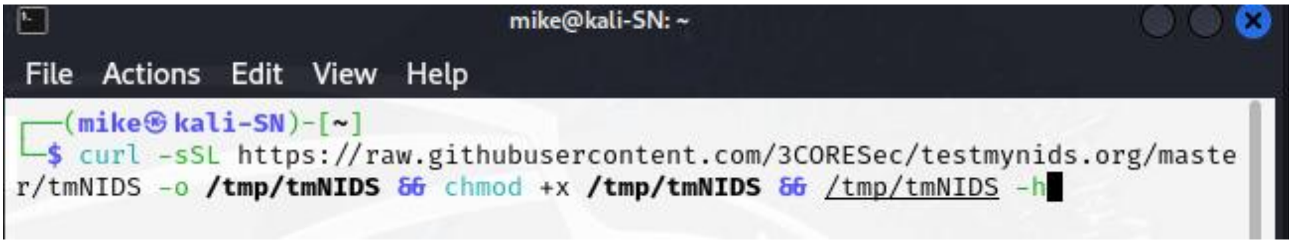
Under snort event types. The type of events can be viewed.



Snort Event Types

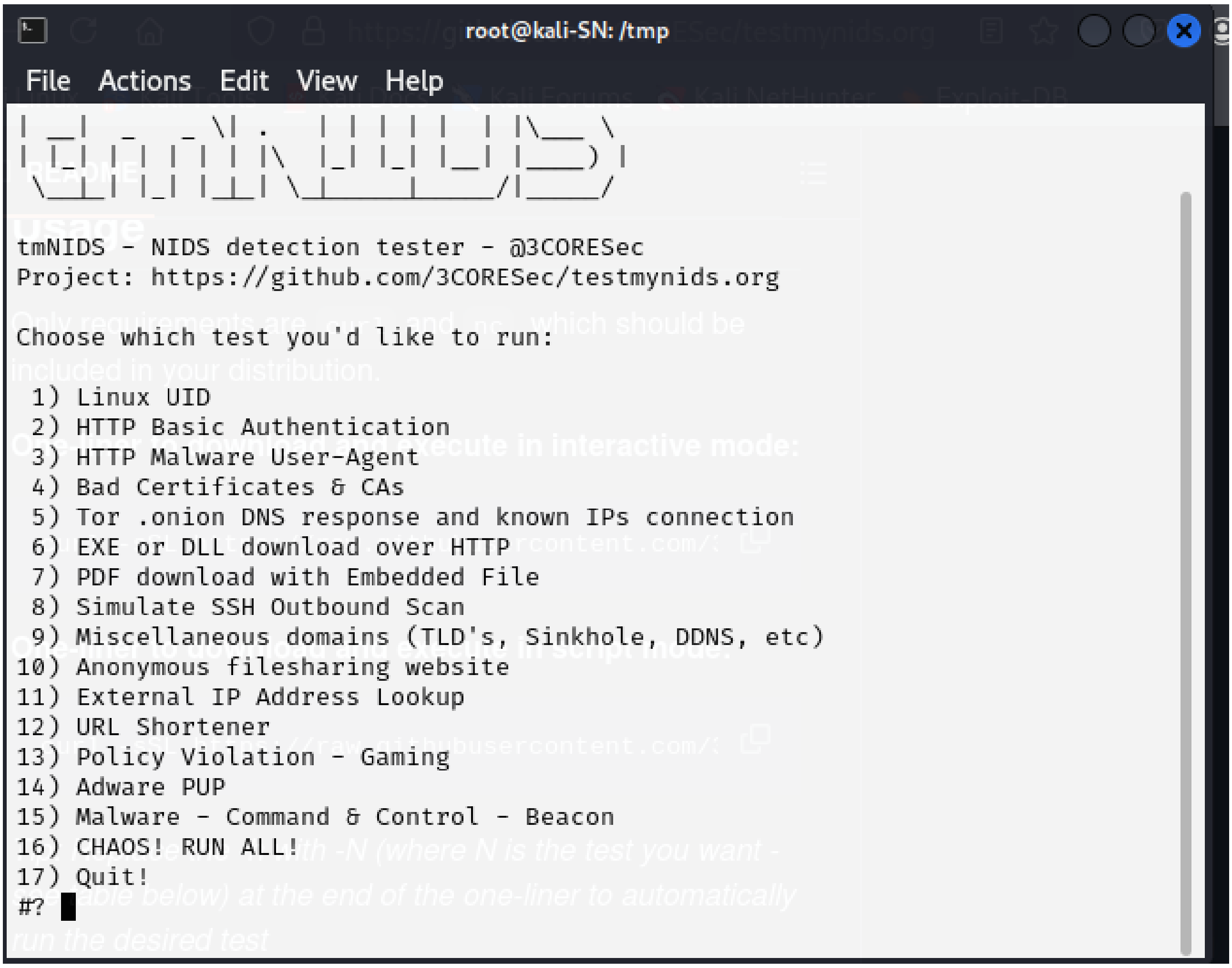
	Signature ⇕	Event Name ⇕	Total Events ⇕
1	10	SSH Connection detected	79
2	9	Ping Detected	9

To test the reaction of the system towards alerts other than pings and ssh this document used a binary provided by 3CORESec which can be downloaded from their GitHub page



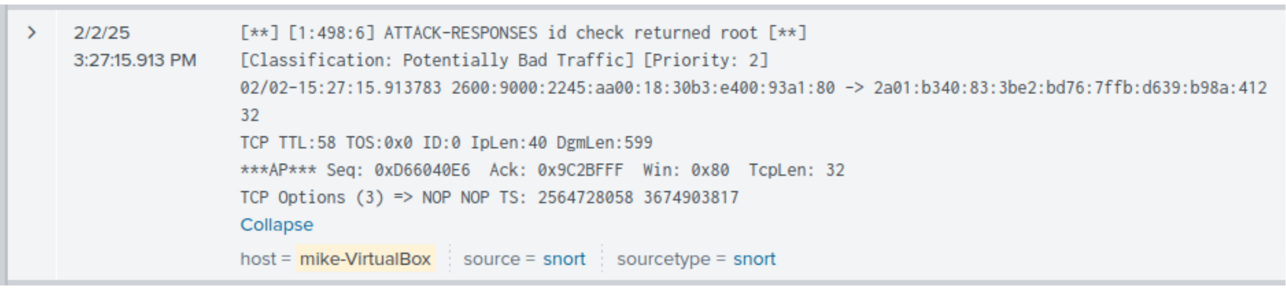
```
┌──(mike㉿kali-SN)-[~]
└─$ curl -sSL https://raw.githubusercontent.com/3CORESec/testmynids.org/maste
r/tmNIDS -o /tmp/tmNIDS && chmod +x /tmp/tmNIDS && /tmp/tmNIDS -h
```

Once downloaded navigate to the tmp folder and run it.



```
| __|  _   _ \| .   | | | | |  | |\___ \
| |_| | | | | | |\  |_| |_| |__| |____) |
 \___| |_| |_|_| \_|_______|_____/|_____/

tmNIDS - NIDS detection tester - @3CORESec
Project: https://github.com/3CORESec/testmynids.org

Choose which test you'd like to run:
 1) Linux UID
 2) HTTP Basic Authentication
 3) HTTP Malware User-Agent
 4) Bad Certificates & CAs
 5) Tor .onion DNS response and known IPs connection
 6) EXE or DLL download over HTTP
 7) PDF download with Embedded File
 8) Simulate SSH Outbound Scan
 9) Miscellaneous domains (TLD's, Sinkhole, DDNS, etc)
10) Anonymous filesharing website
11) External IP Address Lookup
12) URL Shortener
13) Policy Violation - Gaming
14) Adware PUP
15) Malware - Command & Control - Beacon
16) CHAOS! RUN ALL!
17) Quit!
#? 
```

Run any one of the scripts e.g. 8.
Check the Splunk server if any data has been imported



```
>   2/2/25          [**] [1:498:6] ATTACK-RESPONSES id check returned root [**]
    3:27:15.913 PM  [Classification: Potentially Bad Traffic] [Priority: 2]
                    02/02-15:27:15.913783 2600:9000:2245:aa00:18:30b3:e400:93a1:80 -> 2a01:b340:83:3be2:bd76:7ffb:d639:b98a:412
                    32
                    TCP TTL:58 TOS:0x0 ID:0 IpLen:40 DgmLen:599
                    ***AP*** Seq: 0xD66040E6  Ack: 0x9C2BFFF  Win: 0x80  TcpLen: 32
                    TCP Options (3) => NOP NOP TS: 2564728058 3674903817
                    Collapse
                    host = mike-VirtualBox | source = snort | sourcetype = snort
```

The above data was imported just after running script number 8.

Conclusion

In this demonstration a successful deployment of Snort an IDS to monitor network traffic and detect potential threats based on the rules configured. The logs are then forwarded to Spunk where it was analysed in a friendly centralised human-readable interface.

This integration provides a powerful security monitoring solution enabling security teams to detect, investigate, and respond to threats more effectively. By leveraging Snort in real-time detection capabilities and Splunk's advanced analytics and search functionalities organisations can enhance their security posture and incident response ability.

For future demos, inclusion of a firewall device, customising more snort rules setting up and automated alert system in Splunk and integrating additional intelligence sources to improve accuracy and reduce false positives e.g. MITRE ATT&CK, User and Entity Behaviour Analytics (UEBA)

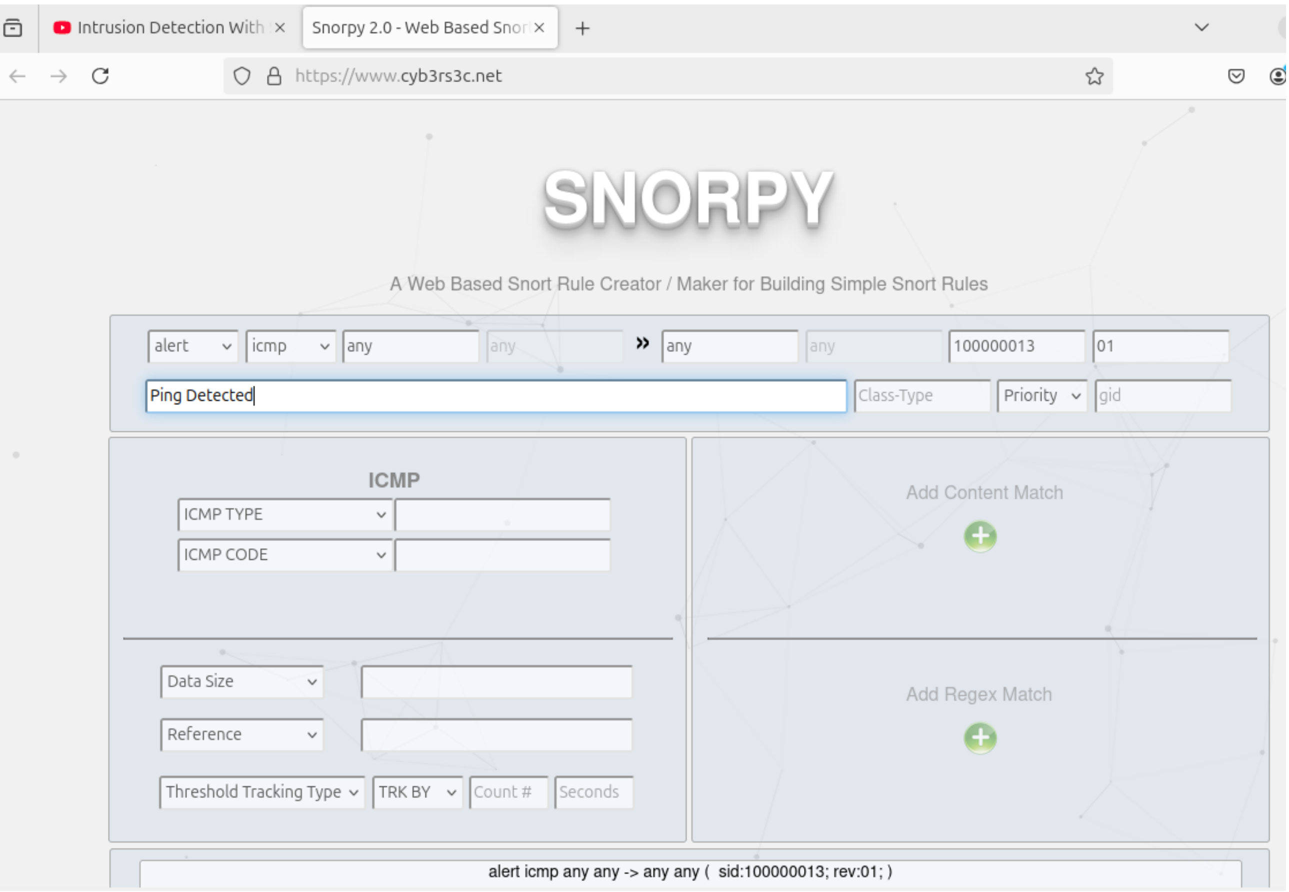
Lessons learned

1. Installation and configuration of IDS – Snort
2. Installation and configuration of SIEM – Splunk
3. Installation and configuration of Splunk forwarder on the snort server
4. Customising rules for Snort
5. Importing logs files into Splunk form the IDS

Appendix

Additional material

To help write rules the website SNORPY (https://www.cyb3rs3c.net) can be very helpful



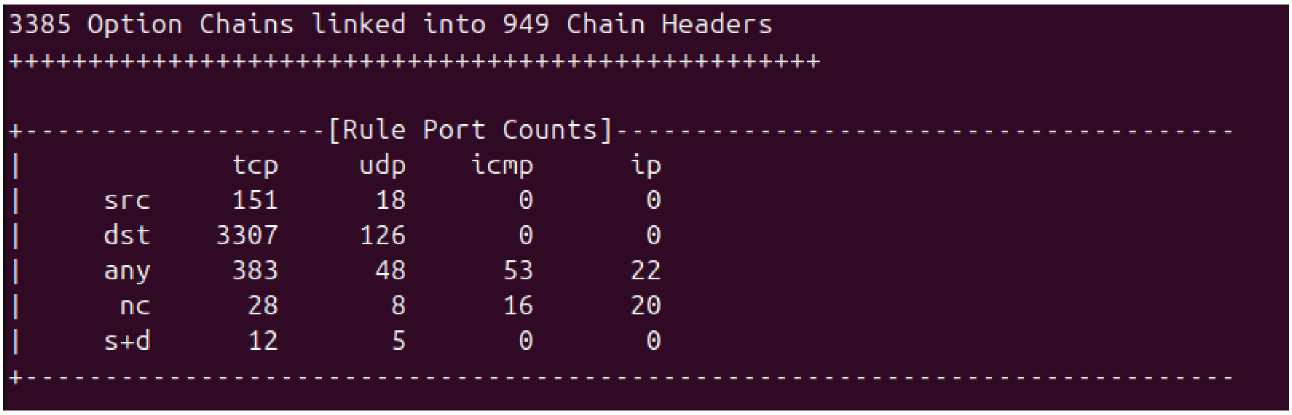
alert | icmp | any | any » any | any | 100000013 | 01

Ping Detected

```
alert icmp any any -> any any ( sid:100000013; rev:01; )
```

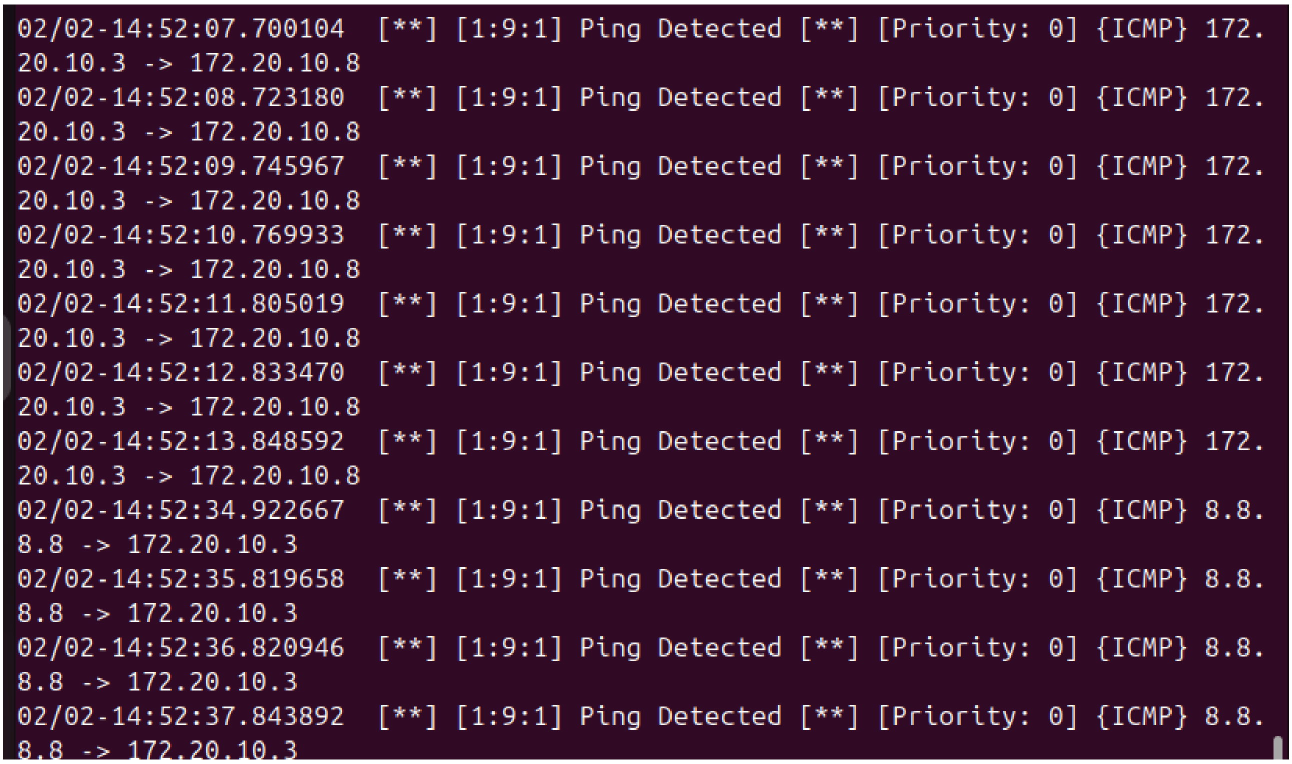
Fill in the desired rule. At the bottom of the page copy and paste the rule in **/etc/snort/rules/local.rules**

Summary of the number rules that will be used to monitor the network



```
3385 Option Chains linked into 949 Chain Headers
+++++++++++++++++++++++++++++++++++++++++++++++++++

+-------------------[Rule Port Counts]---------------------------------------
|             tcp     udp    icmp      ip
|     src     151      18       0       0
|     dst    3307     126       0       0
|     any     383      48      53      22
|      nc      28       8      16      20
|     s+d      12       5       0       0
+----------------------------------------------------------------------------
```

Other pings detected by snort between Host device and Win 10 and the host device to the google DNS servers 8.8.8.8



```
02/02-14:52:07.700104  [**] [1:9:1] Ping Detected [**] [Priority: 0] {ICMP} 172.
20.10.3 -> 172.20.10.8
02/02-14:52:08.723180  [**] [1:9:1] Ping Detected [**] [Priority: 0] {ICMP} 172.
20.10.3 -> 172.20.10.8
02/02-14:52:09.745967  [**] [1:9:1] Ping Detected [**] [Priority: 0] {ICMP} 172.
20.10.3 -> 172.20.10.8
02/02-14:52:10.769933  [**] [1:9:1] Ping Detected [**] [Priority: 0] {ICMP} 172.
20.10.3 -> 172.20.10.8
02/02-14:52:11.805019  [**] [1:9:1] Ping Detected [**] [Priority: 0] {ICMP} 172.
20.10.3 -> 172.20.10.8
02/02-14:52:12.833470  [**] [1:9:1] Ping Detected [**] [Priority: 0] {ICMP} 172.
20.10.3 -> 172.20.10.8
02/02-14:52:13.848592  [**] [1:9:1] Ping Detected [**] [Priority: 0] {ICMP} 172.
20.10.3 -> 172.20.10.8
02/02-14:52:34.922667  [**] [1:9:1] Ping Detected [**] [Priority: 0] {ICMP} 8.8.
8.8 -> 172.20.10.3
02/02-14:52:35.819658  [**] [1:9:1] Ping Detected [**] [Priority: 0] {ICMP} 8.8.
8.8 -> 172.20.10.3
02/02-14:52:36.820946  [**] [1:9:1] Ping Detected [**] [Priority: 0] {ICMP} 8.8.
8.8 -> 172.20.10.3
02/02-14:52:37.843892  [**] [1:9:1] Ping Detected [**] [Priority: 0] {ICMP} 8.8.
8.8 -> 172.20.10.3
```