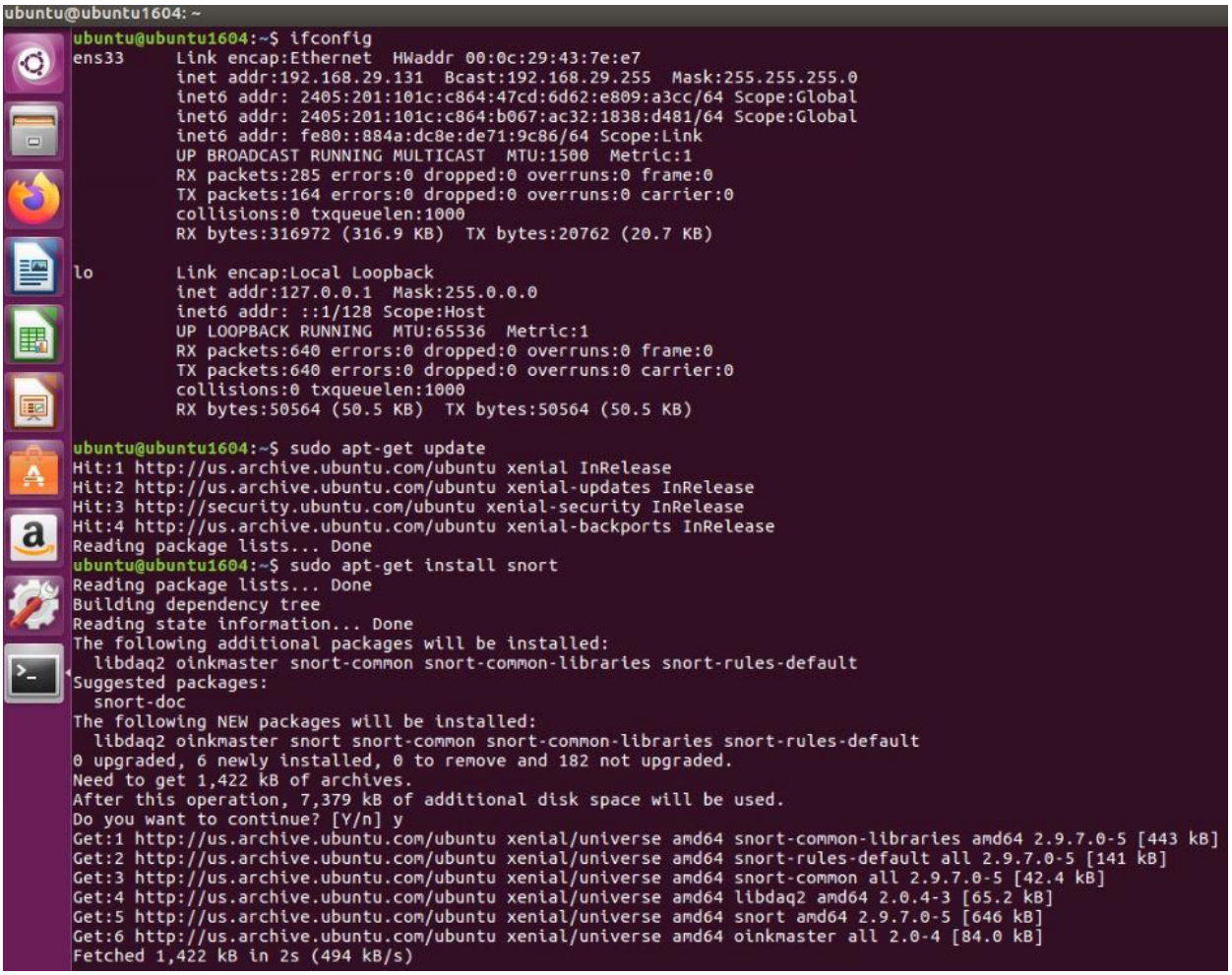
Splunk Enterprise Project

Configure and Forward logs of Snort IDS to Splunk Enterprise

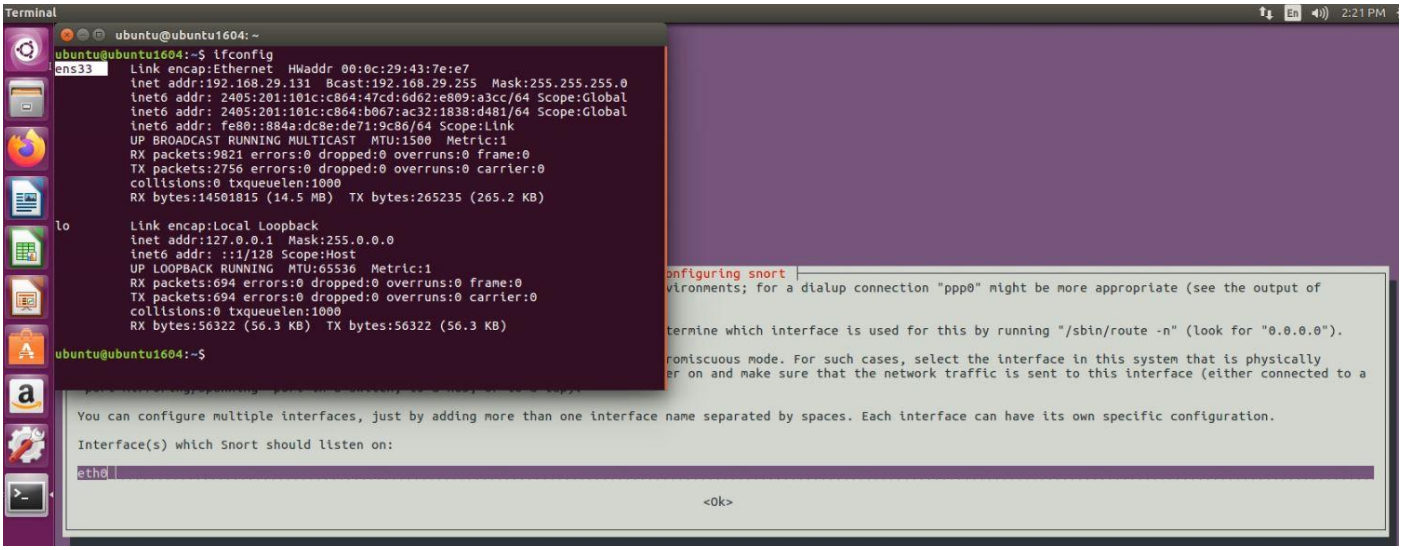
In this write up, I will be setting up and configuring Snort (In Ubuntu), a Splunk server(In Windows OS), and Splunk's universal forwarder. I will be documenting most of the configuration needed for this environment. Towards the end we will be using our fully working environment to play around with both Splunk and Snort. Along with using a tool to launch attacks that we can monitor and log in splunk.

Step 1 – We will install and configure Snort IDS in Ubuntu System. Follow the steps in given image.

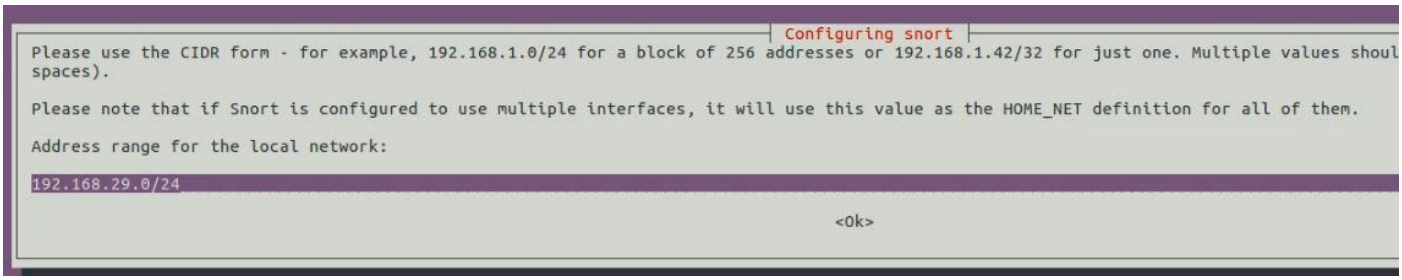


```
ubuntu@ubuntu1604: ~
ubuntu@ubuntu1604:~$ ifconfig
ens33     Link encap:Ethernet  HWaddr 00:0c:29:43:7e:e7
          inet addr:192.168.29.131  Bcast:192.168.29.255  Mask:255.255.255.0
          inet6 addr: 2405:201:101c:c864:47cd:6d62:e809:a3cc/64 Scope:Global
          inet6 addr: 2405:201:101c:c864:b067:ac32:1838:d481/64 Scope:Global
          inet6 addr: fe80::884a:dc8e:de71:9c86/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:285 errors:0 dropped:0 overruns:0 frame:0
          TX packets:164 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:316972 (316.9 KB)  TX bytes:20762 (20.7 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:640 errors:0 dropped:0 overruns:0 frame:0
          TX packets:640 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:50564 (50.5 KB)  TX bytes:50564 (50.5 KB)

ubuntu@ubuntu1604:~$ sudo apt-get update
Hit:1 http://us.archive.ubuntu.com/ubuntu xenial InRelease
Hit:2 http://us.archive.ubuntu.com/ubuntu xenial-updates InRelease
Hit:3 http://security.ubuntu.com/ubuntu xenial-security InRelease
Hit:4 http://us.archive.ubuntu.com/ubuntu xenial-backports InRelease
Reading package lists... Done
ubuntu@ubuntu1604:~$ sudo apt-get install snort
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libdaq2 oinkmaster snort-common snort-common-libraries snort-rules-default
Suggested packages:
  snort-doc
The following NEW packages will be installed:
  libdaq2 oinkmaster snort snort-common snort-common-libraries snort-rules-default
0 upgraded, 6 newly installed, 0 to remove and 182 not upgraded.
Need to get 1,422 kB of archives.
After this operation, 7,379 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://us.archive.ubuntu.com/ubuntu xenial/universe amd64 snort-common-libraries amd64 2.9.7.0-5 [443 kB]
Get:2 http://us.archive.ubuntu.com/ubuntu xenial/universe amd64 snort-rules-default all 2.9.7.0-5 [141 kB]
Get:3 http://us.archive.ubuntu.com/ubuntu xenial/universe amd64 snort-common all 2.9.7.0-5 [42.4 kB]
Get:4 http://us.archive.ubuntu.com/ubuntu xenial/universe amd64 libdaq2 amd64 2.0.4-3 [65.2 kB]
Get:5 http://us.archive.ubuntu.com/ubuntu xenial/universe amd64 snort amd64 2.9.7.0-5 [646 kB]
Get:6 http://us.archive.ubuntu.com/ubuntu xenial/universe amd64 oinkmaster all 2.0-4 [84.0 kB]
Fetched 1,422 kB in 2s (494 kB/s)
```

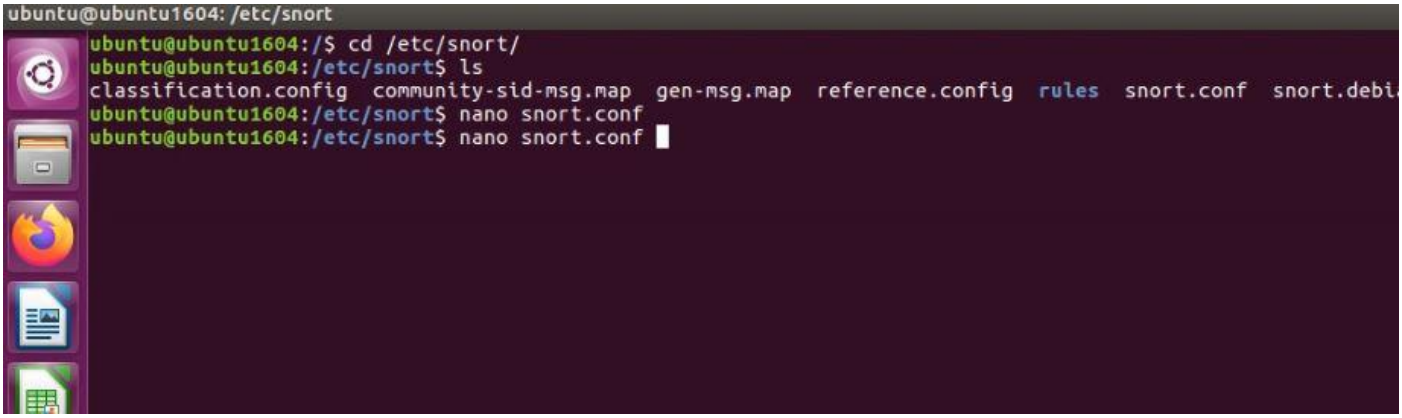
Enter the Interface which snort should listen on,



Enter this command to find Address Range – “ip a s”



Step 2 – Make changes in snort.conf file



Set the Network Variables in after HOME_NET. Enter this command to find it– “ip a s”

```
ubuntu@ubuntu1604: /etc/snort
  GNU nano 2.5.3                                          File: snort.conf

# 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
##################################################

##################################################
# Step #1: Set the network variables.  For more information, see README.variable
##################################################

# 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 192.16

# 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
```

Run the Snort in Test Mode

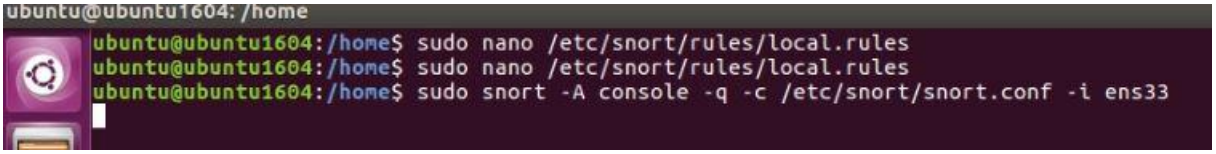
```
ubuntu@ubuntu1604: /home
ubuntu@ubuntu1604:/home$ cd /home
ubuntu@ubuntu1604:/home$ sudo snort -T -i ens33 -c /etc/snort/snort.conf
Running in Test mode

        --== 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 4
 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371
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 312
000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091 94
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 detection libs from /usr/lib/snort_dynamicrules...
WARNING: No dynamic libraries found in directory /usr/lib/snort_dynamicrules.
  Finished Loading all dynamic detection libs from /usr/lib/snort_dynamicrules
Loading all dynamic preprocessor libs from /usr/lib/snort_dynamicpreprocessor/...
  Loading dynamic preprocessor library /usr/lib/snort_dynamicpreprocessor//libsf_gtp_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_dns_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_sdf_preproc.so... done
  Loading dynamic preprocessor library /usr/lib/snort_dynamicpreprocessor//libsf_sip_preproc.so... done
```

Step 3 – We need to add rule in local.rules file.

Enter this command to navigate file – “sudo nano /etc/snort/rules/local.rules”

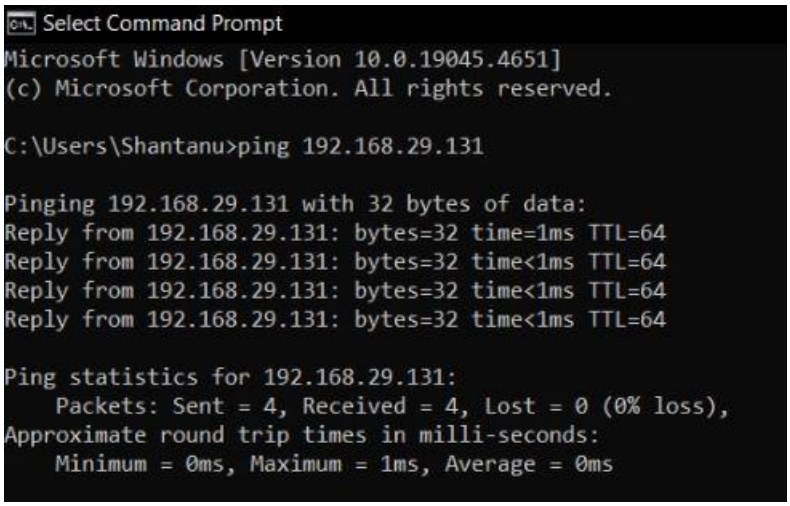
Add the rule for Ping command.

Start the Snort IDS using this command – “sudo snort -A console -q -c /etc/snort/snort.conf -I ens33”



Snort IDS will Successfully Start.

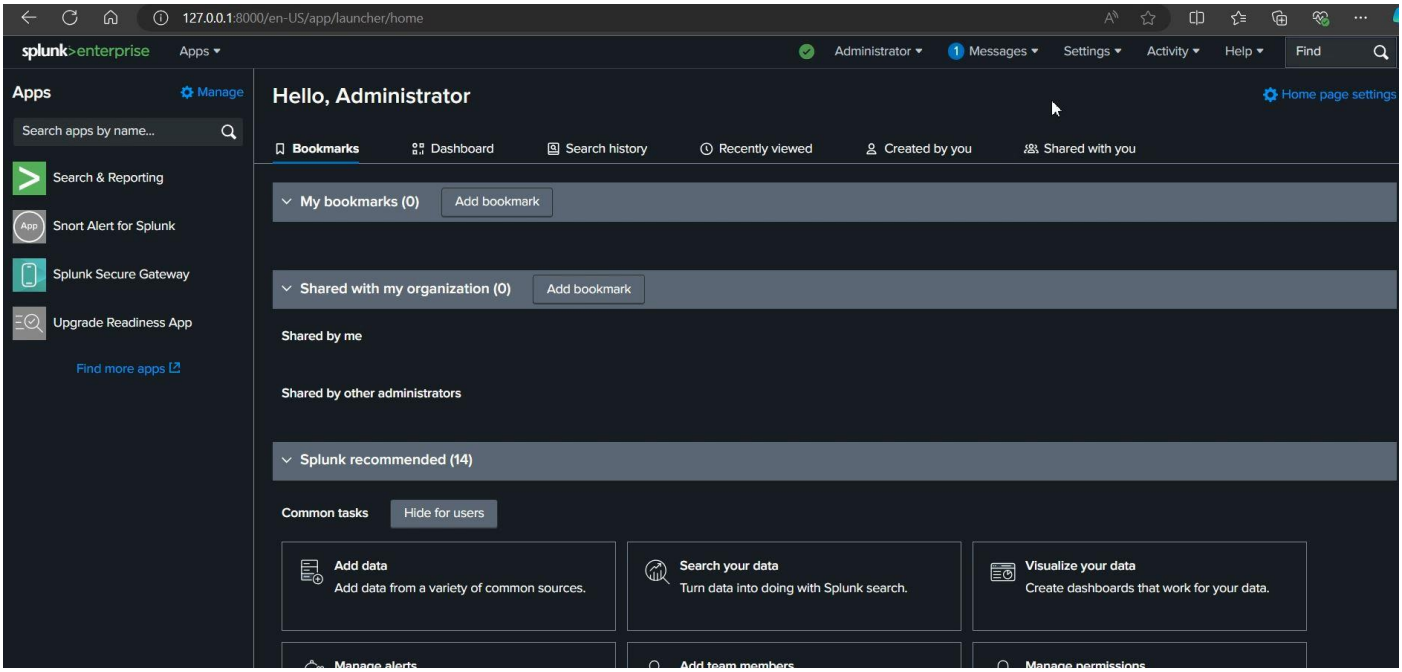
Step 4 - Ping the Ubuntu System from other system.



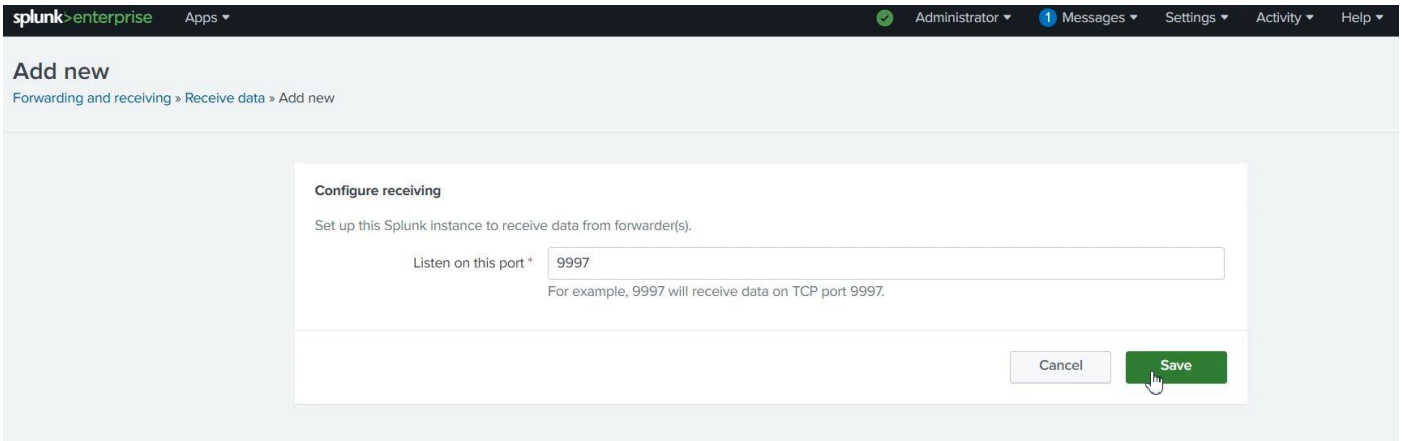
The Snort IDS will alert about the ping.

```
ubuntu@ubuntu1604: /home
ubuntu@ubuntu1604:/home$ sudo nano /etc/snort/rules/local.rules
ubuntu@ubuntu1604:/home$ sudo nano /etc/snort/rules/local.rules
ubuntu@ubuntu1604:/home$ sudo snort -A console -q -c /etc/snort/snort.conf -i ens33
08/04-14:55:41.166807  [**] [1:1005:1] PING ATTEMPTED BY SOMEONE [**] [Priority: 0] {IPV6-ICMP} fe80::6edf:fbff:fe27:6b93 -> ff02::1
08/04-14:55:41.166855  [**] [1:1005:1] PING ATTEMPTED BY SOMEONE [**] [Priority: 0] {IPV6-ICMP} fe80::6edf:fbff:fe27:6b93 -> ff02::1
08/04-14:55:41.166861  [**] [1:1005:1] PING ATTEMPTED BY SOMEONE [**] [Priority: 0] {IPV6-ICMP} fe80::6edf:fbff:fe27:6b93 -> ff02::1
08/04-14:55:47.198939  [**] [1:1005:1] PING ATTEMPTED BY SOMEONE [**] [Priority: 0] {IPV6-ICMP} fe80::6edf:fbff:fe27:6b93 -> 2405:201:101c:c864:b0
08/04-14:55:47.199010  [**] [1:1005:1] PING ATTEMPTED BY SOMEONE [**] [Priority: 0] {IPV6-ICMP} 2405:201:101c:c864:b067:ac32:1838:d481 -> fe80::6e
08/04-14:55:54.888619  [**] [1:1005:1] PING ATTEMPTED BY SOMEONE [**] [Priority: 0] {IPV6-ICMP} fe80::6edf:fbff:fe27:6b93 -> ff02::1
08/04-14:55:55.092361  [**] [1:1005:1] PING ATTEMPTED BY SOMEONE [**] [Priority: 0] {IPV6-ICMP} fe80::6edf:fbff:fe27:6b93 -> ff02::1
08/04-14:55:55.092560  [**] [1:1005:1] PING ATTEMPTED BY SOMEONE [**] [Priority: 0] {IPV6-ICMP} fe80::6edf:fbff:fe27:6b93 -> ff02::1
08/04-14:55:55.453945  [**] [1:382:7] ICMP PING Windows [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.29.162 -> 192.168.29.131
08/04-14:55:55.453945  [**] [1:1005:1] PING ATTEMPTED BY SOMEONE [**] [Priority: 0] {ICMP} 192.168.29.162 -> 192.168.29.131
08/04-14:55:55.453945  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.29.162 -> 192.168.29.131
08/04-14:55:55.453972  [**] [1:1005:1] PING ATTEMPTED BY SOMEONE [**] [Priority: 0] {ICMP} 192.168.29.131 -> 192.168.29.162
08/04-14:55:55.453972  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.29.131 -> 192.168.29.162
08/04-14:55:56.465840  [**] [1:382:7] ICMP PING Windows [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.29.162 -> 192.168.29.131
08/04-14:55:56.465840  [**] [1:1005:1] PING ATTEMPTED BY SOMEONE [**] [Priority: 0] {ICMP} 192.168.29.162 -> 192.168.29.131
08/04-14:55:56.465840  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.29.162 -> 192.168.29.131
08/04-14:55:56.465874  [**] [1:1005:1] PING ATTEMPTED BY SOMEONE [**] [Priority: 0] {ICMP} 192.168.29.131 -> 192.168.29.162
08/04-14:55:56.465874  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.29.131 -> 192.168.29.162
08/04-14:55:57.480035  [**] [1:382:7] ICMP PING Windows [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.29.162 -> 192.168.29.131
08/04-14:55:57.480035  [**] [1:1005:1] PING ATTEMPTED BY SOMEONE [**] [Priority: 0] {ICMP} 192.168.29.162 -> 192.168.29.131
08/04-14:55:57.480035  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.29.162 -> 192.168.29.131
08/04-14:55:57.480061  [**] [1:1005:1] PING ATTEMPTED BY SOMEONE [**] [Priority: 0] {ICMP} 192.168.29.131 -> 192.168.29.162
08/04-14:55:57.480061  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.29.131 -> 192.168.29.162
08/04-14:55:58.493449  [**] [1:382:7] ICMP PING Windows [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.29.162 -> 192.168.29.131
08/04-14:55:58.493449  [**] [1:1005:1] PING ATTEMPTED BY SOMEONE [**] [Priority: 0] {ICMP} 192.168.29.162 -> 192.168.29.131
08/04-14:55:58.493449  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.29.162 -> 192.168.29.131
08/04-14:55:58.493482  [**] [1:1005:1] PING ATTEMPTED BY SOMEONE [**] [Priority: 0] {ICMP} 192.168.29.131 -> 192.168.29.162
08/04-14:55:58.493482  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.29.131 -> 192.168.29.162
```

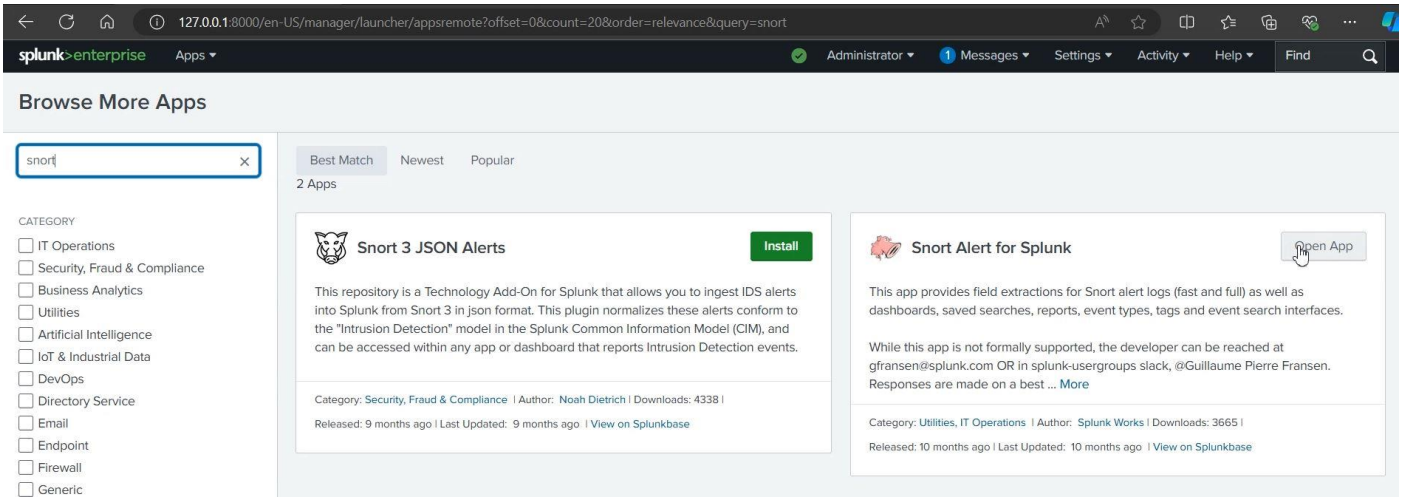
Now, Let's start with Splunk enterprise. After Installing and Configuring Splunk. Login to Splunk



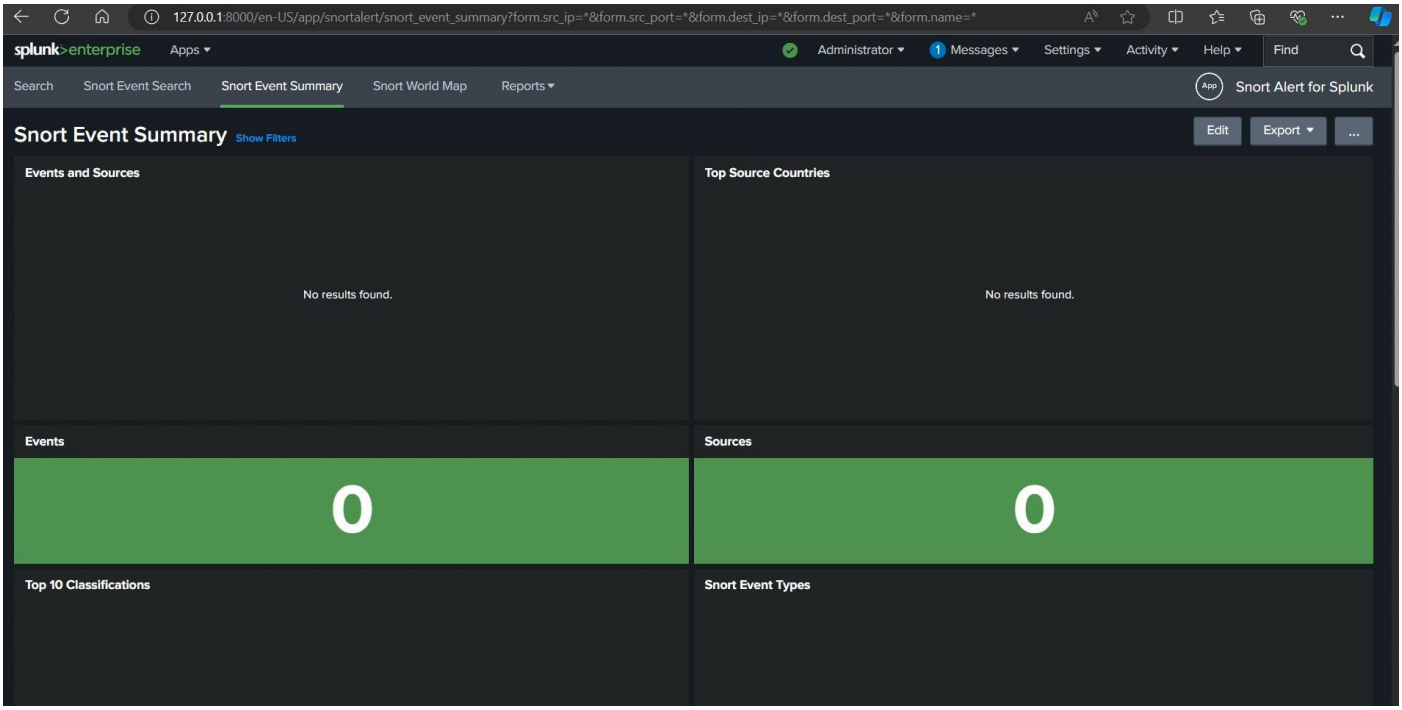
Step 5 - Go to Settings→Forwarding and receiving→In receive data click Add new→enter port no. and save.



Step 6 – Go to home page → Apps → Find More Apps → search snort → Install.

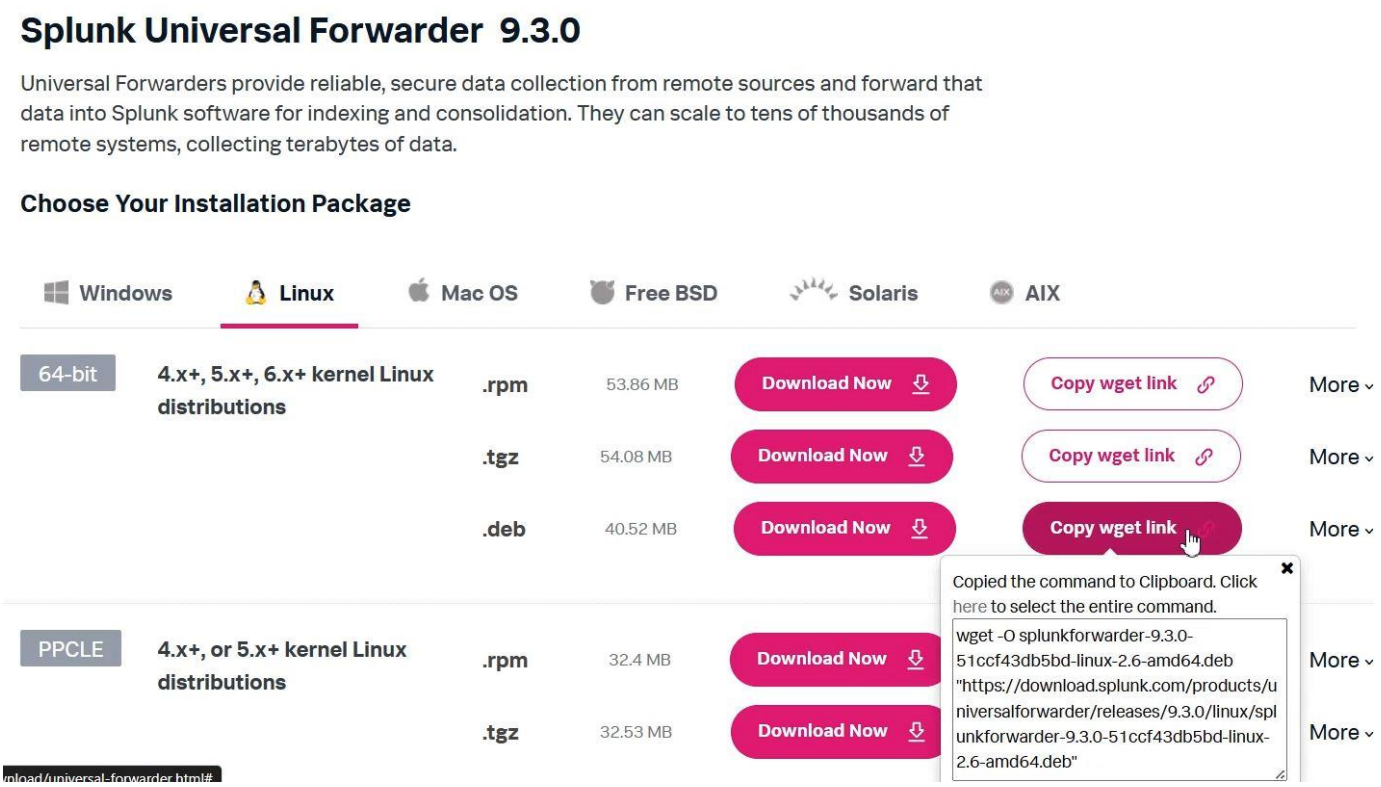


Go to home page and click Snort Alert for Splunk.

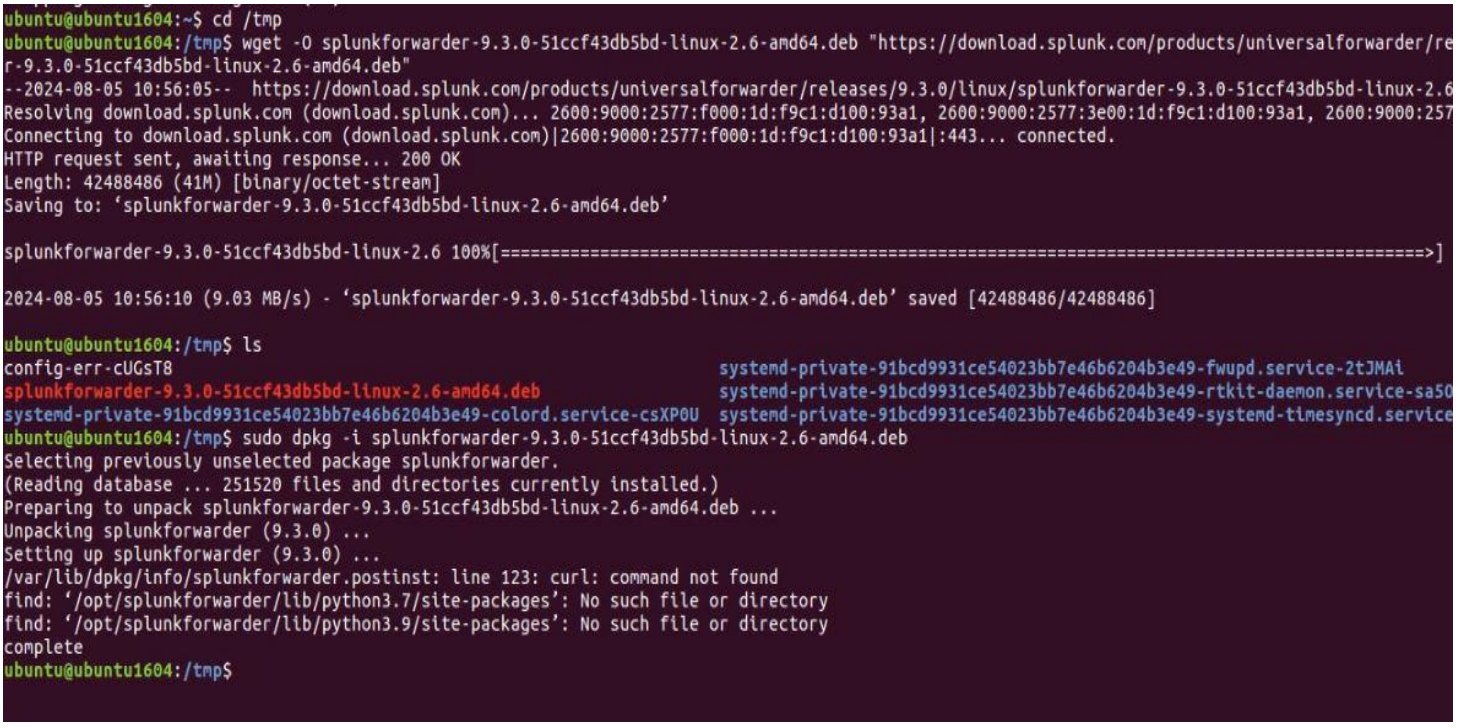


Go to Ubuntu System and add the ufw rules

Step 7 - Go to splunk.com → login account → Products → Free Trials & Downloads →In Universal Forwarder click “Get my Free Download” → Copy link as shown in given image.



Go to Ubuntu system, enter wget -O and paste the link and enter command. And follow command as below



```
ubuntu@ubuntu1604:~$ cd /tmp
ubuntu@ubuntu1604:/tmp$ wget -O splunkforwarder-9.3.0-51ccf43db5bd-linux-2.6-amd64.deb "https://download.splunk.com/products/universalforwarder/re
r-9.3.0-51ccf43db5bd-linux-2.6-amd64.deb"
--2024-08-05 10:56:05--  https://download.splunk.com/products/universalforwarder/releases/9.3.0/linux/splunkforwarder-9.3.0-51ccf43db5bd-linux-2.6
Resolving download.splunk.com (download.splunk.com)... 2600:9000:2577:f000:1d:f9c1:d100:93a1, 2600:9000:2577:3e00:1d:f9c1:d100:93a1, 2600:9000:257
Connecting to download.splunk.com (download.splunk.com)|2600:9000:2577:f000:1d:f9c1:d100:93a1|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 42488486 (41M) [binary/octet-stream]
Saving to: ‘splunkforwarder-9.3.0-51ccf43db5bd-linux-2.6-amd64.deb’

splunkforwarder-9.3.0-51ccf43db5bd-linux-2.6 100%[===================================================================================>]

2024-08-05 10:56:10 (9.03 MB/s) - ‘splunkforwarder-9.3.0-51ccf43db5bd-linux-2.6-amd64.deb’ saved [42488486/42488486]

ubuntu@ubuntu1604:/tmp$ ls
config-err-cUGsT8                                                  systemd-private-91bcd9931ce54023bb7e46b6204b3e49-fwupd.service-2tJMAi
splunkforwarder-9.3.0-51ccf43db5bd-linux-2.6-amd64.deb             systemd-private-91bcd9931ce54023bb7e46b6204b3e49-rtkit-daemon.service-sa50
systemd-private-91bcd9931ce54023bb7e46b6204b3e49-colord.service-csXP0U  systemd-private-91bcd9931ce54023bb7e46b6204b3e49-systemd-timesyncd.service
ubuntu@ubuntu1604:/tmp$ sudo dpkg -i splunkforwarder-9.3.0-51ccf43db5bd-linux-2.6-amd64.deb
Selecting previously unselected package splunkforwarder.
(Reading database ... 251520 files and directories currently installed.)
Preparing to unpack splunkforwarder-9.3.0-51ccf43db5bd-linux-2.6-amd64.deb ...
Unpacking splunkforwarder (9.3.0) ...
Setting up splunkforwarder (9.3.0) ...
/var/lib/dpkg/info/splunkforwarder.postinst: line 123: curl: command not found
find: ‘/opt/splunkforwarder/lib/python3.7/site-packages’: No such file or directory
find: ‘/opt/splunkforwarder/lib/python3.9/site-packages’: No such file or directory
complete
ubuntu@ubuntu1604:/tmp$
```

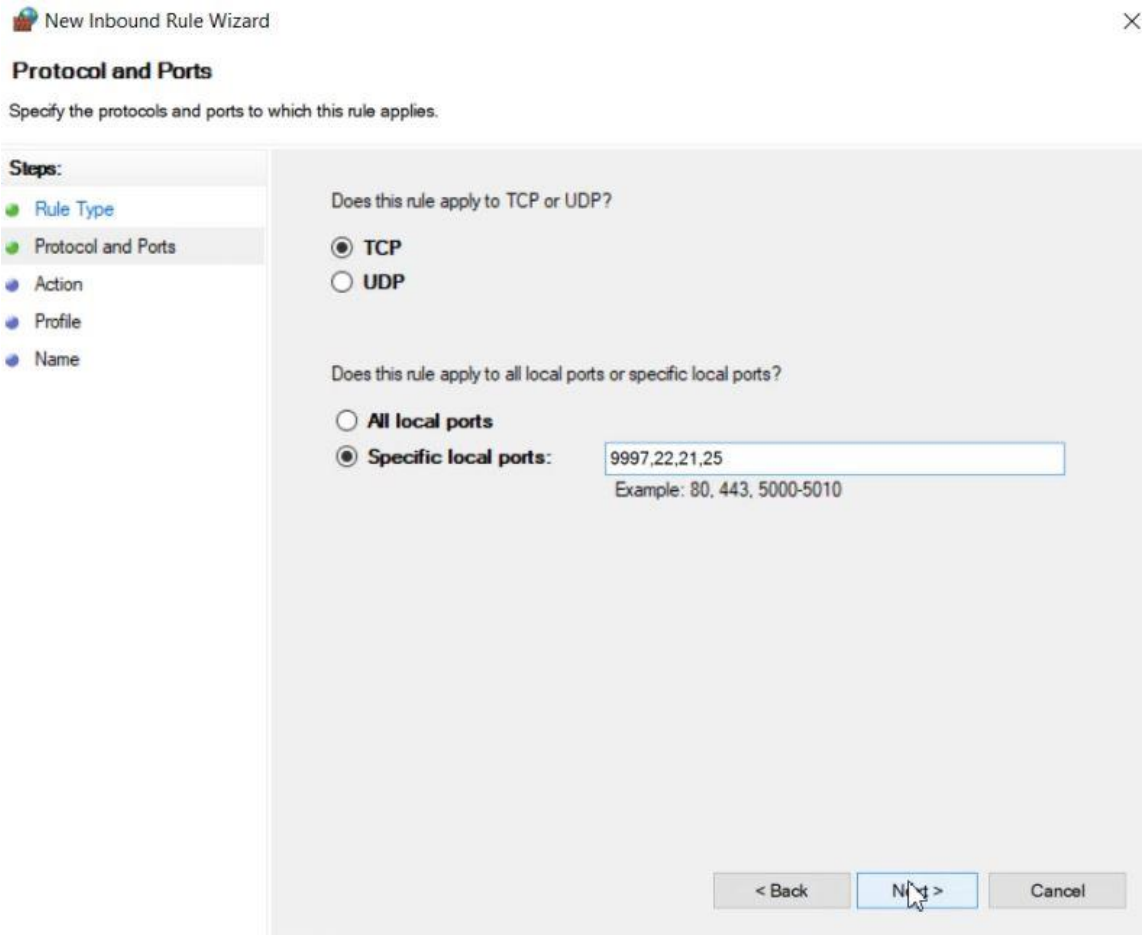
Enter the below command.

```
ubuntu@ubuntu1604: /opt/splunkforwarder/bin
ubuntu@ubuntu1604:/tmp$ cd /opt/splunkforwarder/bin/
ubuntu@ubuntu1604:/opt/splunkforwarder/bin$ sudo ./splunk start --accept-lisence
```

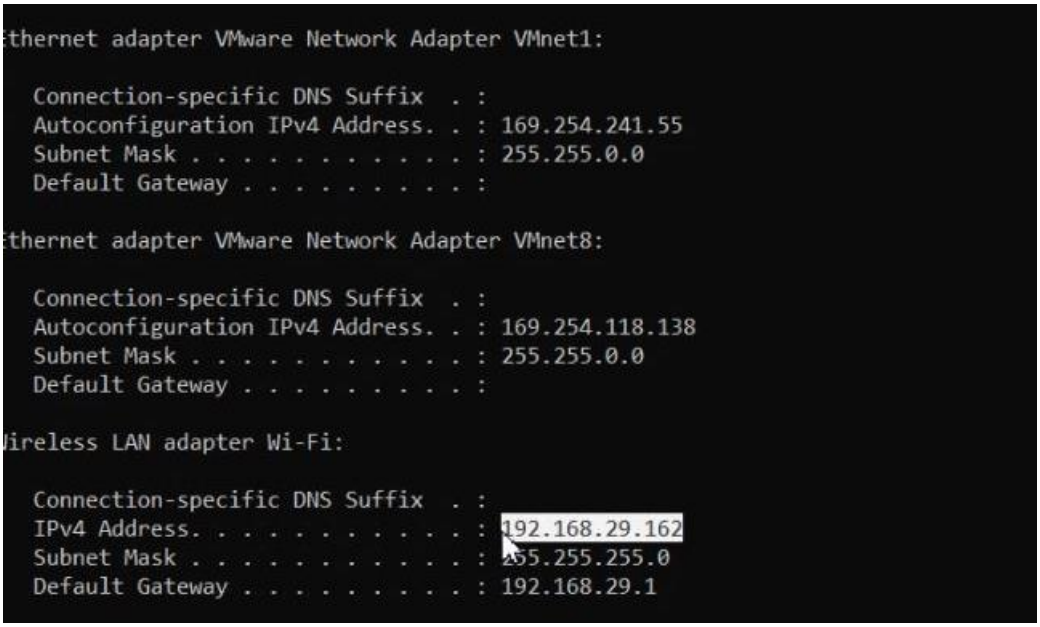
Output -

```
ubuntu@ubuntu1604: /opt/splunkforwarder/bin

"Statement of Work" means the statements of work and/or any and all applicable
Orders, that describe the specific services to be performed by Splunk,
including any materials and deliverables to be delivered by Splunk.

Do you agree with this license? [y/n]:     y
Do you agree with this license? [y/n]: y

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: splunkuf
Password must contain at least:
   * 8 total printable ASCII character(s).
Please enter a new password:
Please confirm new password:
Creating unit file...
Important: splunk will start under systemd as user: splunkfwd
The unit file has been created.


Splunk> See your world.  Maybe wish you hadn't.

Checking prerequisites...
        Checking mgmt port [8089]: open
                Creating: /opt/splunkforwarder/var/lib/splunk
                Creating: /opt/splunkforwarder/var/run/splunk
                Creating: /opt/splunkforwarder/var/run/splunk/appserver/i18n
                Creating: /opt/splunkforwarder/var/run/splunk/appserver/modules/static/css
                Creating: /opt/splunkforwarder/var/run/splunk/upload
                Creating: /opt/splunkforwarder/var/run/splunk/search_telemetry
                Creating: /opt/splunkforwarder/var/run/splunk/search_log
                Creating: /opt/splunkforwarder/var/spool/splunk
                Creating: /opt/splunkforwarder/var/spool/dirmoncache
                Creating: /opt/splunkforwarder/var/lib/splunk/authDb
                Creating: /opt/splunkforwarder/var/lib/splunk/hashDb
                Creating: /opt/splunkforwarder/var/run/splunk/sessions
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-9.3.0-5
        All installed files intact.
        Done
All preliminary checks passed.

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

Step 8 – In Windows OS go to Firewall & Network Protection →Advance Settings →Inbound Rules → New Rule →Port → TCP, Enter port no. “9997,22,21,25” →Next →Next→Give name → Finish



Step 9 - Copy IP address of Windows OS.

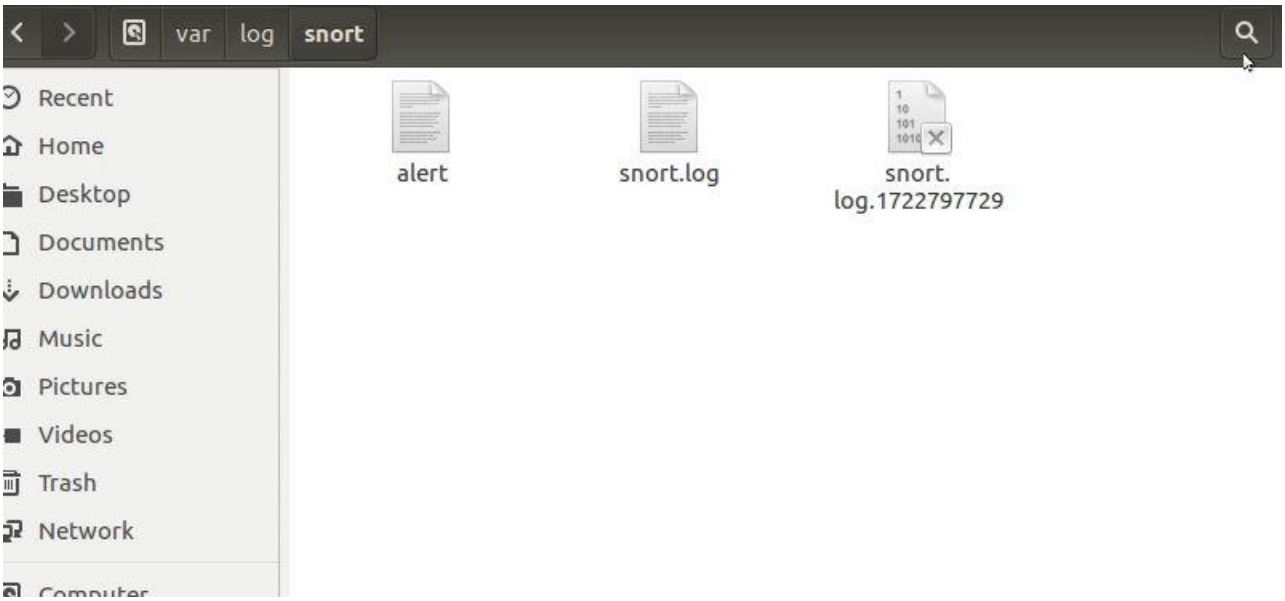


Enter Below Commands, Check if the server address is same as Windows OS ip address in outputs.conf

```
ubuntu@ubuntu1604: /opt/splunkforwarder/etc/system/local
ubuntu@ubuntu1604:/opt/splunkforwarder/bin$ sudo ./splunk add forward-server 192.168.29.162:9997
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Splunk username: splunkuf
Password:
Added forwarding to: 192.168.29.162:9997.
ubuntu@ubuntu1604:/opt/splunkforwarder/bin$ cd /opt/splunkforwarder/etc/system/local/
ubuntu@ubuntu1604:/opt/splunkforwarder/etc/system/local$ ls
outputs.conf  README  server.conf
ubuntu@ubuntu1604:/opt/splunkforwarder/etc/system/local$ sudo nano outputs.conf
ubuntu@ubuntu1604:/opt/splunkforwarder/etc/system/local$
```

Enter the command “sudo snort -q -l /var/log/snort/ -i ens33 -A full -c /etc/snort/snort.conf” in ubuntu.

And check in /var/log/snort if alert file is created.



Add the alert file to monitor in splunk using this command.

```
ubuntu@ubuntu1604: /opt/splunkforwarder/bin
ubuntu@ubuntu1604:/opt/splunkforwarder/etc/system$ cd ..
ubuntu@ubuntu1604:/opt/splunkforwarder/etc$ cd ..
ubuntu@ubuntu1604:/opt/splunkforwarder$ cd /bin
ubuntu@ubuntu1604:/bin$ cd /opt/splunkforwarder/bin/
ubuntu@ubuntu1604:/opt/splunkforwarder/bin$ ls
2to3-3.7  bzip2          genSignedServerCert.sh  idle3.9       pip     prichunkpng  pripamtopng
2to3-3.9  classify       genWebCert.sh           openssl       pip3    priforgepng  pripnglsch
btool     copyright.txt  idle3                   pcre2-config  pip3.7  prigreypng   pripngtopam
btprobe   genRootCA.sh   idle3.7                 pid_check.sh  pip3.9  pripalpng    priweavepng
ubuntu@ubuntu1604:/opt/splunkforwarder/bin$ sudo ./splunk add monitor /var/log/snort/alert
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Added monitor of '/var/log/snort/alert'.
ubuntu@ubuntu1604:/opt/splunkforwarder/bin$
```

Go to inputs.conf

```
root@ubuntu1604: /opt/splunkforwarder/etc/apps/search/local
ubuntu@ubuntu1604:/opt/splunkforwarder/etc/apps/search$ sudo su
root@ubuntu1604:/opt/splunkforwarder/etc/apps/search# cd local/
root@ubuntu1604:/opt/splunkforwarder/etc/apps/search/local# ls
inputs.conf
root@ubuntu1604:/opt/splunkforwarder/etc/apps/search/local# nano inputs.conf
```

And make this changes to inputs.conf file, enter ip address of Windows OS in host.

```
root@ubuntu1604: /opt/splunkforwarder/etc/apps/search/local
  GNU nano 2.5.3                                          File: inputs.conf

[splunktcp://9997]
connection_host = 192.168.29.162
[monitor:///var/log/snort/alert]
disabled = false
index = main
sourcetype = snort_alert_full
source = snort
```

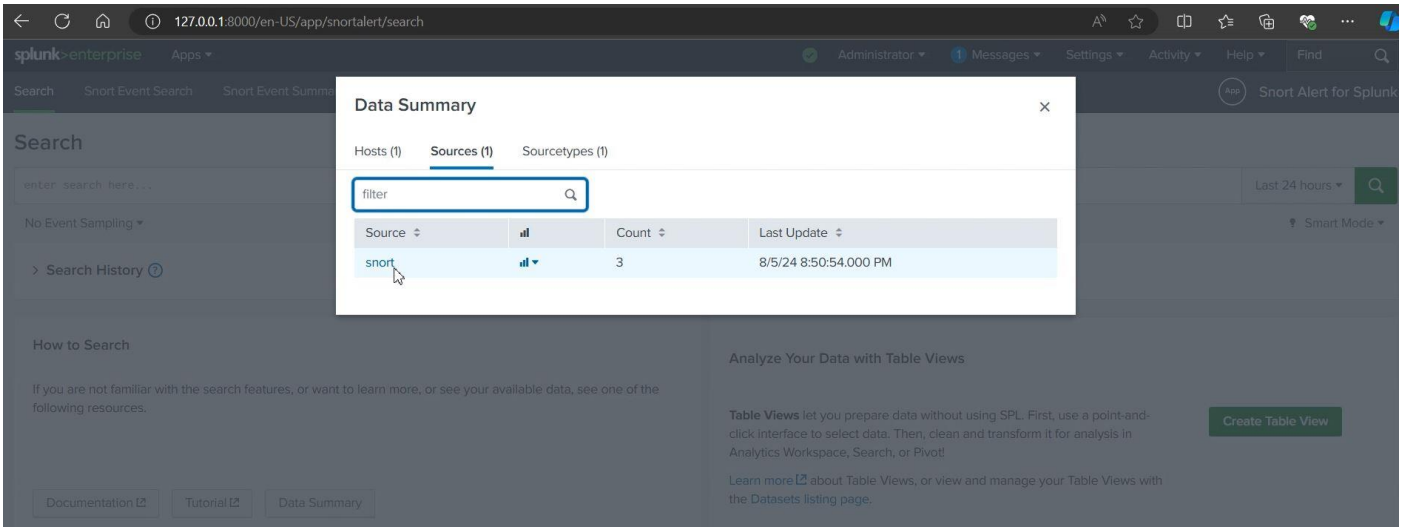
Restart the Splunk server

```
ubuntu@ubuntu1604: /opt/splunkforwarder/bin
ubuntu@ubuntu1604:/opt/splunkforwarder$ cd bin/
ubuntu@ubuntu1604:/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> See your world.  Maybe wish you hadn't.

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.
        All installed files intact.
        Done
All preliminary checks passed.

Starting splunk server daemon (splunkd)...
Done

ubuntu@ubuntu1604:/opt/splunkforwarder/bin$
```

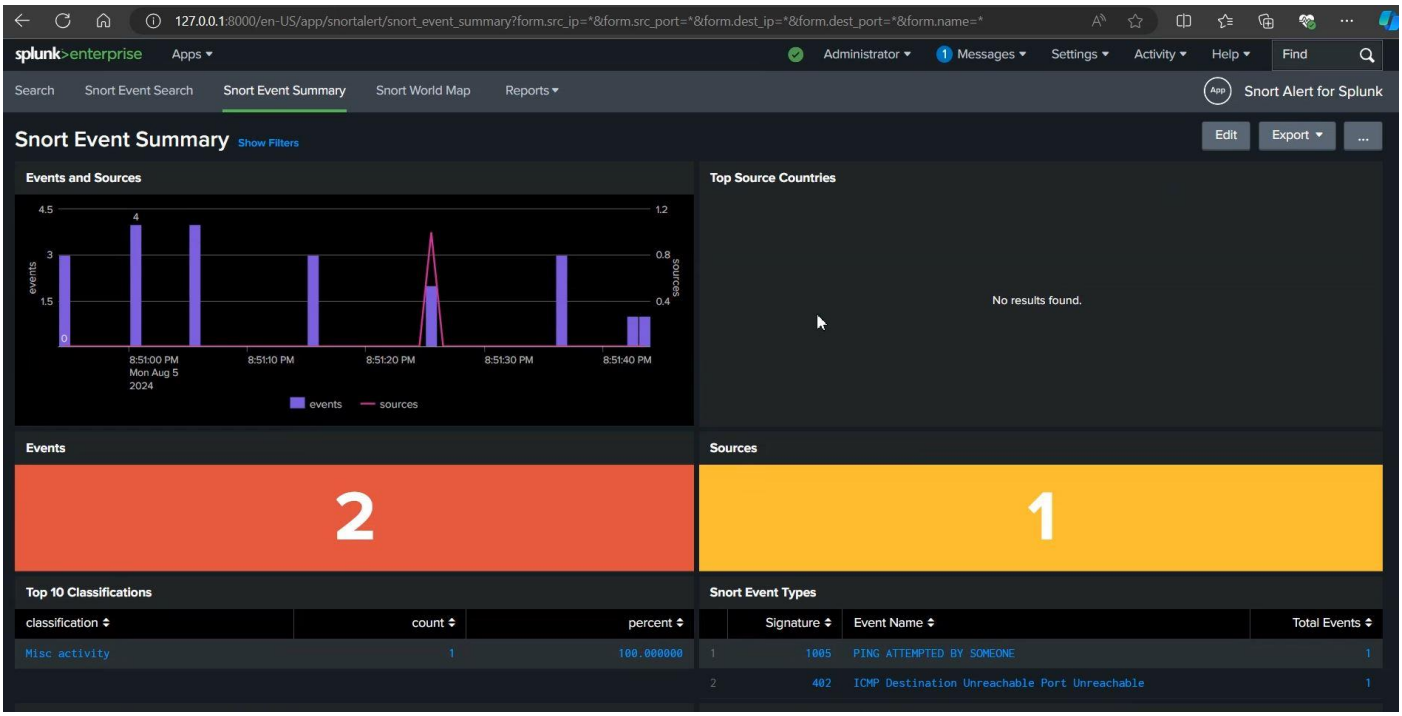
Enter the command “sudo snort -q -l /var/log/snort/ -i ens33 -A full -c /etc/snort/snort.conf” in ubuntu

To start Snort in Ubuntu System.

Step 10 – Go to Splunk server → Search → Data Summary → snort.



We can see the logs of snort of Ubuntu system are forwarding in Splunk.



Step 10 – Let's attack Ubuntu system and check if the logs are forwarding in Splunk.

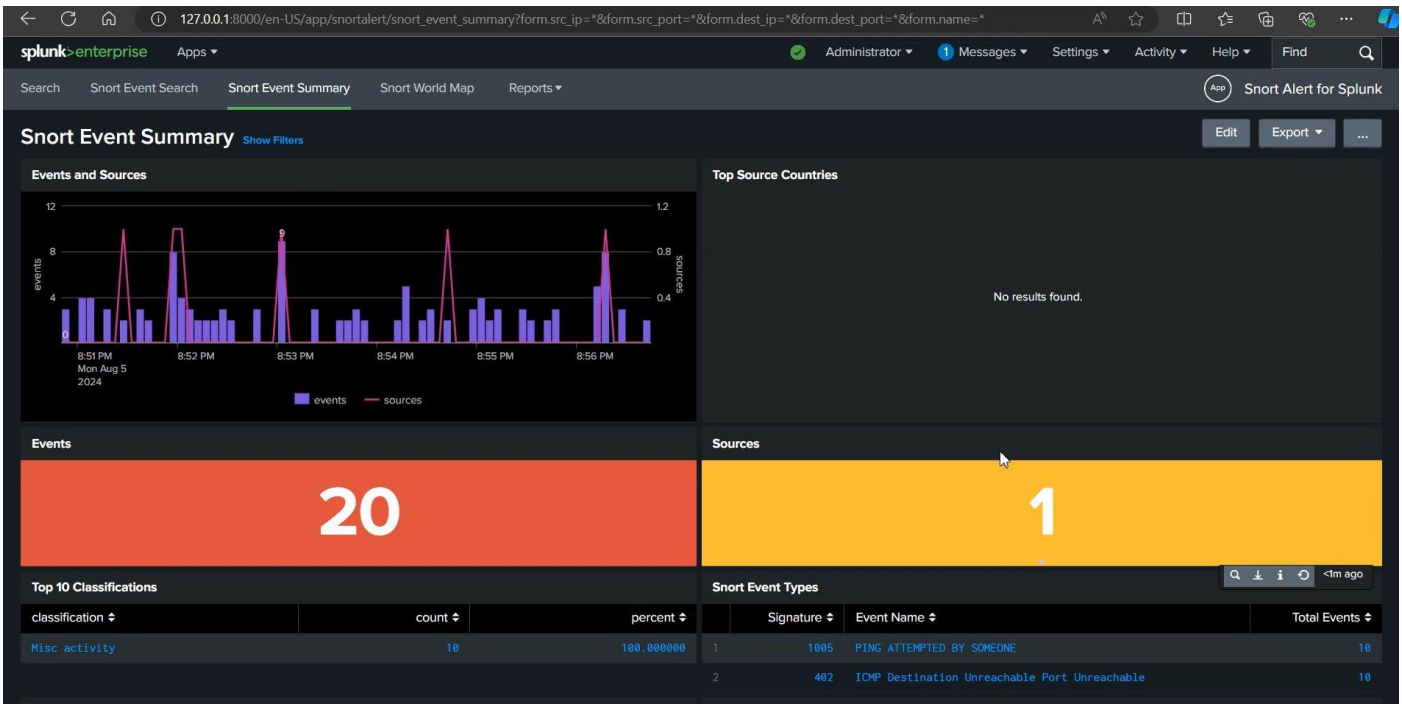
Go to your browser and search "github tmnids." Open it and copy tool link → then follow below Steps.

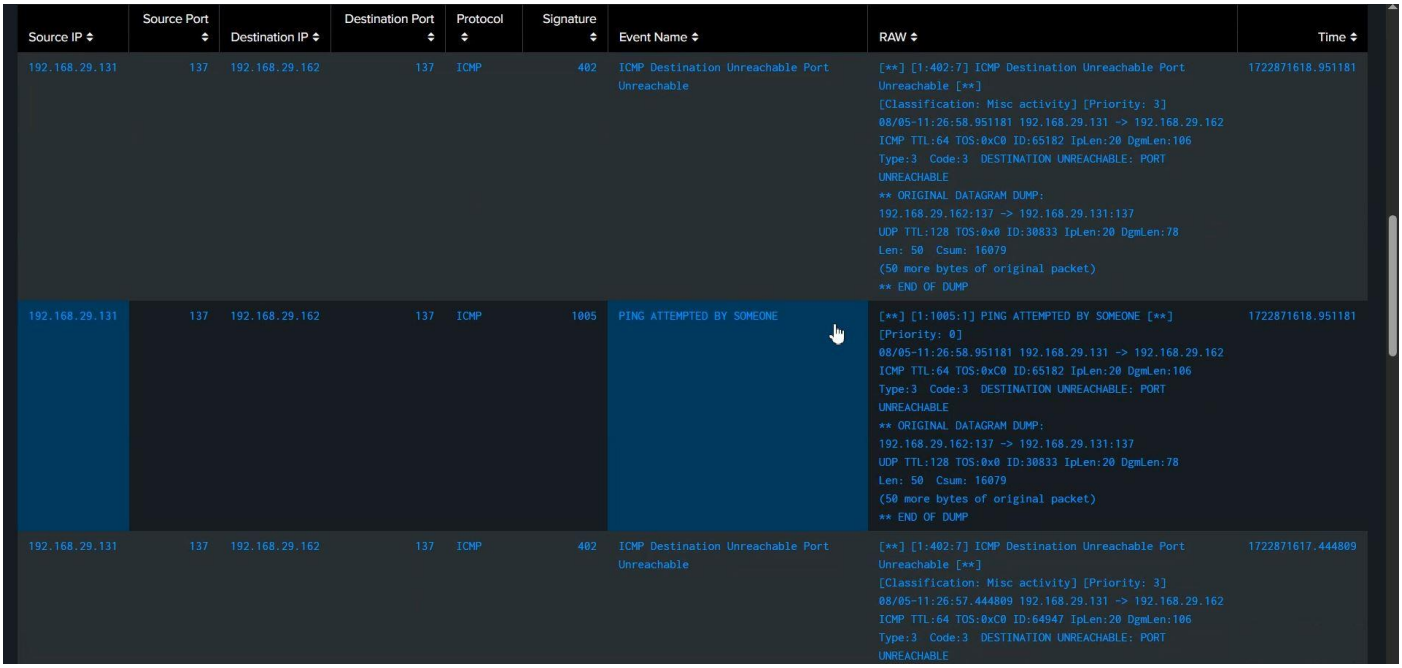
```
ubuntu@ubuntu1604: ~/testmynids.org
ubuntu@ubuntu1604:~$ git clone https://github.com/0xtf/testmynids.org.git
Cloning into 'testmynids.org'...
remote: Enumerating objects: 216, done.
remote: Counting objects: 100% (48/48), done.
remote: Compressing objects: 100% (39/39), done.
remote: Total 216 (delta 18), reused 19 (delta 9), pack-reused 168
Receiving objects: 100% (216/216), 5.51 MiB | 3.11 MiB/s, done.
Resolving deltas: 100% (65/65), done.
Checking connectivity... done.
ubuntu@ubuntu1604:~$ ls
Desktop  Documents  Downloads  examples.desktop  Music  Pictures  Public  Templates  testmynids.org  Videos
ubuntu@ubuntu1604:~$ cd testmynids.org/
ubuntu@ubuntu1604:~/testmynids.org$ ./tmnids
```

Enter Attack no. 11.

```
ubuntu@ubuntu1604: ~/testmynids.org
 _              _   _ _____ _____   _____
| |            | \ | |_   _|  __ \ / ____|
| |_ _ __ ___ |  \| | | | | |  | | (___
| __|  _   _ \| .   | | | | |  | |\___ \
| |_| | | | | | |\  |_| |_| |__| |____) |
 \__|_| |_| |_|_| \_|_____|_____/|_____/

tmNIDS - NIDS detection tester - @0xtf
Project: https://github.com/0xtf/testmynids.org

Choose which test you'd like to run:

 1) Linux UID
 2) HTTP Basic Authentication
 3) HTTP Malware User-Agent
 4) Bad Certificate Authorities
 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) MD5 in TLS Certificate Signature
11) CHAOS! RUN ALL!
12) Quit!
#? 11
./tmNIDS: line 23: curl: command not found
./tmNIDS: line 27: curl: command not found
./tmNIDS: line 31: curl: command not found
./tmNIDS: line 32: curl: command not found
./tmNIDS: line 33: curl: command not found
./tmNIDS: line 34: curl: command not found
./tmNIDS: line 35: curl: command not found
./tmNIDS: line 39: curl: command not found
./tmNIDS: line 40: curl: command not found
sort: cannot read: /tmp/tor.list: No such file or directory
rm: cannot remove '/tmp/tor.list': No such file or directory
./tmNIDS: line 59: curl: command not found
./tmNIDS: line 63: curl: command not found
rm: cannot remove '/tmp/tmnidspdf.pdf': No such file or directory
```

We can see the attach logs are being detected live in Splunk.





Conclusion

We now have a working Splunk environment with snort, that will allow us to monitor and create logs within our virtual machines. Setting up these tools from scratch helps you get familiar with both of these tools.