National College of Ireland

Configuration Manual

MSc Research Project
MSc. in Cybersecurity

Likhith Umesh Salian
Student ID: 23205237

School of Computing
National College of Ireland

Supervisor: Khadija Hafeez

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Likhith Umesh Salian		
Student ID:	23205237		
Programme:	MSc. in Cybersecurity	**Year:**	2024
Module:	Practicum Part 2		
Lecturer:	Khadija Hafeez		
Submission Due Date:	12/12/2024		
Project Title:	Efficient Cyber threat Intelligence Automation using Machine Learning		
Word Count: 697	**Page Count:** 13		

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: LIKHITH UMESH SALIAN

Date: 12/12/2024

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

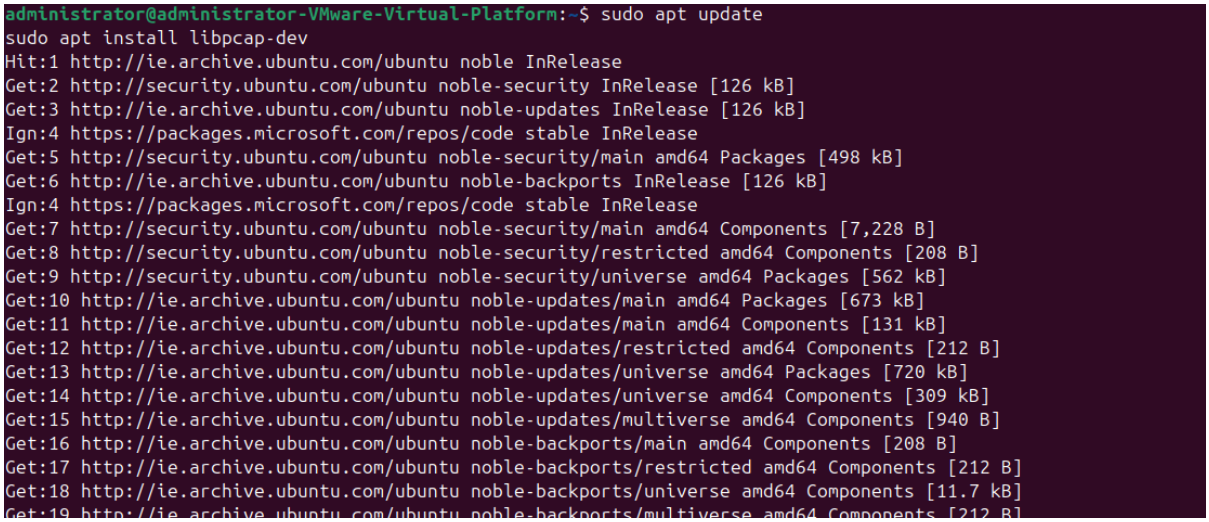
Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

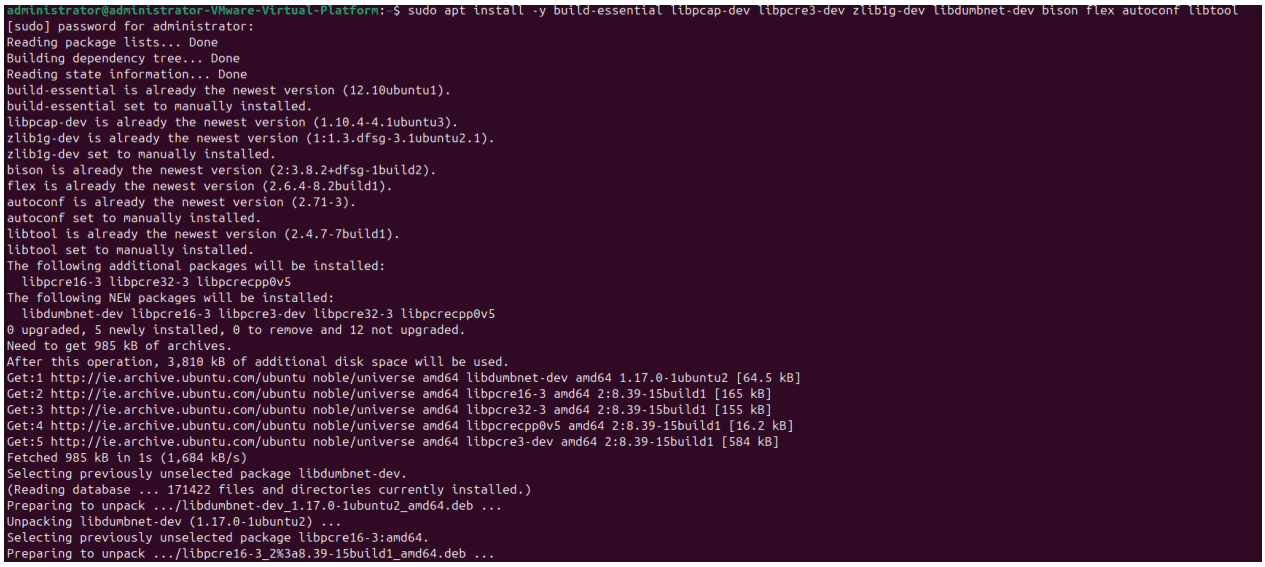
Configuration Manual

Likhith Umesh Salian
Student ID: 23205237

1 Preliminary configurations

1) Preliminary configurations require preliminary configurations for the installation of dependency files on the system to install snort successfully. The dependency files include the libpcap, DAQ and check files which needs to be installed. Update the Ubuntu operating system to enable the packages to be updated. The configurations are installed by fetching the necessary details from the OS.





```
administrator@administrator-VMware-Virtual-Platform:~/Downloads$ wget https://www.snort.org/downloads/archive/snort/daq-2.0.7.tar.gz
--2024-12-07 22:31:40--  https://www.snort.org/downloads/archive/snort/daq-2.0.7.tar.gz
Resolving www.snort.org (www.snort.org)... 104.19.222.12, 104.19.221.12, 2606:4700::6813:dd0c, ...
Connecting to www.snort.org (www.snort.org)|104.19.222.12|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://snort-org-site.s3.amazonaws.com/production/release_files/files/000/013/420/original/daq-2.0.7.tar.gz?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAU7AK5ITMMOX
GB2W5%2F20241207%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20241207T223143Z&X-Amz-Expires=3600&X-Amz-SignedHeaders=host&X-Amz-Signature=dfee12f5fbaf40342a9c728313870856cc7f3403a883064
107d88b080d0d7ec4 [following]
--2024-12-07 22:31:43--  https://snort-org-site.s3.amazonaws.com/production/release_files/files/000/013/420/original/daq-2.0.7.tar.gz?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=
AKIAU7AK5ITMMOXGB2W5%2F20241207%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20241207T223143Z&X-Amz-Expires=3600&X-Amz-SignedHeaders=host&X-Amz-Signature=dfee12f5fbaf40342a9c728313870856
cc7f3403a883064107d88b080d0d7ec4
Resolving snort-org-site.s3.amazonaws.com (snort-org-site.s3.amazonaws.com)... 52.216.204.75, 3.5.28.146, 16.15.177.183, ...
Connecting to snort-org-site.s3.amazonaws.com (snort-org-site.s3.amazonaws.com)|52.216.204.75|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 520287 (508K) [binary/octet-stream]
Saving to: ‘daq-2.0.7.tar.gz’

daq-2.0.7.tar.gz                    100%[=========================================================================================>] 508.09K   172KB/s    in 2.9s

2024-12-07 22:31:49 (172 KB/s) - ‘daq-2.0.7.tar.gz’ saved [520287/520287]

administrator@administrator-VMware-Virtual-Platform:~/Downloads$ tar -xvzf daq-2.0.7.tar.gz
cd daq-2.0.7
daq-2.0.7/
daq-2.0.7/config.h.in
daq-2.0.7/config.guess
daq-2.0.7/api/
daq-2.0.7/api/daq.h
daq-2.0.7/api/Makefile.am
daq-2.0.7/api/daq_common.h
daq-2.0.7/api/daq_base.c
daq-2.0.7/api/daq_api.h
daq-2.0.7/api/daq_mod_ops.c
daq-2.0.7/api/Makefile.in
daq-2.0.7/config.sub
```

```
administrator@administrator-VMware-Virtual-Platform:~/Downloads/daq-2.0.7$ ./configure
make
sudo make install
checking for a BSD-compatible install... /usr/bin/install -c
checking whether build environment is sane... yes
checking for a thread-safe mkdir -p... /usr/bin/mkdir -p
checking for gawk... no
checking for mawk... mawk
checking whether make sets $(MAKE)... yes
checking whether make supports nested variables... yes
checking for gcc... gcc
checking whether the C compiler works... yes
checking for C compiler default output file name... a.out
checking for suffix of executables...
checking whether we are cross compiling... no
checking for suffix of object files... o
checking whether we are using the GNU C compiler... yes
checking whether gcc accepts -g... yes
checking for gcc option to accept ISO C89... none needed
checking whether gcc understands -c and -o together... yes
checking for style of include used by make... GNU
checking dependency style of gcc... gcc3
checking build system type... x86_64-unknown-linux-gnu
checking host system type... x86_64-unknown-linux-gnu
checking how to print strings... printf
checking for a sed that does not truncate output... /usr/bin/sed
checking for grep that handles long lines and -e... /usr/bin/grep
checking for egrep... /usr/bin/grep -E
checking for fgrep... /usr/bin/grep -F
checking for ld used by gcc... /usr/bin/ld
checking if the linker (/usr/bin/ld) is GNU ld... yes
```

2 Install snort on Ubuntu

Install snort after the update is complete. If the snort packages are installed previously then then the output shows snort is already in the newest version.

```
administrator@administrator-VMware-Virtual-Platform:~$ sudo apt install snort
[sudo] password for administrator:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
snort is already the newest version (2.9.20-0+deb11u1ubuntu1).
0 upgraded, 0 newly installed, 0 to remove and 12 not upgraded.
```

3 Alter the ownership of the directory

The alerts are generated and saved on the /var/log/snort. Enable the snort logs alerts generated to gain the unprivileged access to the files to perform analysis when required. The ownership of the /var/log/snort directory is set to snort and administrator.

```
administrator@administrator-VMware-Virtual-Platform:~$ sudo mkdir -p /etc/snort/rules /var/log/snort /usr/local/lib/snort_dynamicrules
sudo touch /etc/snort/rules/local.rules
administrator@administrator-VMware-Virtual-Platform:~$ sudo chmod -R 5775 /var/log/snort
sudo chmod -R 5775 /etc/snort
administrator@administrator-VMware-Virtual-Platform:~$ ls -la /var/log/snort
total 320
drwsrwsr-t  2 snort administrator  4096 Dec  7 13:07 .
drwxrwxr-x 17 root  syslog         4096 Dec  7 22:24 ..
-rwsrwxr-t  1 snort administrator 93951 Dec  1 19:28 alert
-rwsrwxr-t  1 snort administrator 10598 Dec  5 19:56 'nmap and ping.txt'
-rwsrwxr-t  1 snort adm               0 Dec  7 22:24 snort.alert
-rwsrwxr-t  1 snort administrator   180 Dec  6 01:24 snort.alert.1.gz
-rwsrwxr-t  1 snort administrator    59 Dec  3 22:09 snort.alert.2.gz
-rwsrwxr-t  1 snort administrator   637 Dec  2 23:00 snort.alert.3.gz
-rwsrwxr-t  1 snort administrator   837 Nov 27 23:20 snort.alert.4.gz
-rwsrwxr-t  1 snort administrator    90 Nov 26 23:09 snort.alert.5.gz
-rwsrwxr-t  1 snort administrator   108 Nov 22 23:53 snort.alert.6.gz
-rwsrwxr-t  1 snort adm             374 Dec  7 19:40 snort.alert.fast
-rwsrwxr-t  1 snort administrator   259 Dec  6 01:24 snort.alert.fast.1.gz
-rwsrwxr-t  1 snort administrator   416 Dec  5 19:33 snort.alert.fast.2.gz
-rwsrwxr-t  1 snort administrator   115 Dec  3 22:09 snort.alert.fast.3.gz
-rwsrwxr-t  1 snort administrator   627 Dec  2 23:00 snort.alert.fast.4.gz
-rwsrwxr-t  1 snort administrator  4831 Dec  1 21:03 snort.alert.fast.5.gz
-rwsrwxr-t  1 snort administrator   717 Nov 27 23:20 snort.alert.fast.6.gz
-rwsrwxr-t  1 snort administrator   145 Nov 26 23:09 snort.alert.fast.7.gz
-rwsrwxr-t  1 snort adm               0 Dec  7 22:24 snort.log
-rwsrwxr-t  1 root  administrator   978 Dec  7 13:07 snort.log.06122024.pcap
-rwsrwxr-t  1 snort administrator  6408 Nov 27 23:20 snort.log.1732749568
-rwsrwxr-t  1 snort administrator   654 Dec  1 19:04 snort.log.1733078537
-rwsrwxr-t  1 snort administrator 68082 Dec  1 19:27 snort.log.1733080754
-rwsrwxr-t  1 snort administrator  7320 Dec  1 19:28 snort.log.1733081278
-rwsrwxr-t  1 snort administrator  4812 Dec  1 19:34 snort.log.1733081623
-rwsrwxr-t  1 snort administrator   204 Dec  1 20:50 snort.log.1733086215
-rwsrwxr-t  1 snort administrator   114 Dec  1 20:55 snort.log.1733086491
-rwsrwxr-t  1 snort administrator  3258 Dec  5 19:33 snort.log.1733427061
```

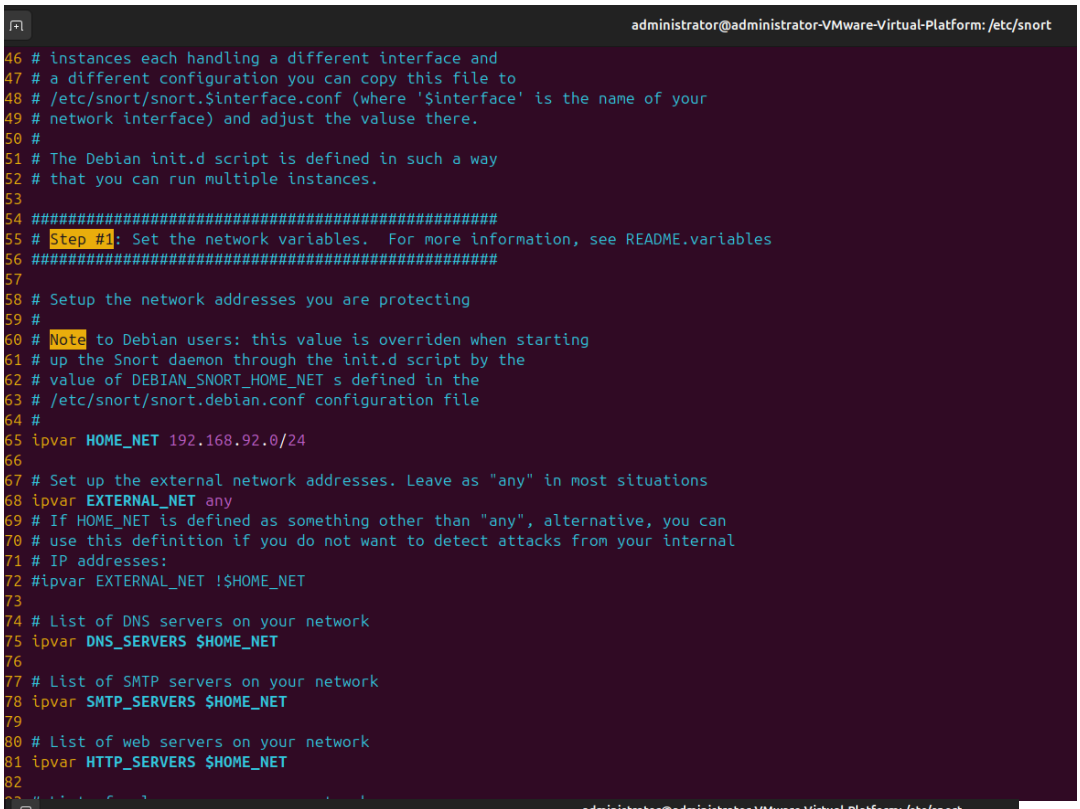
4 Identify the local IP address of the system

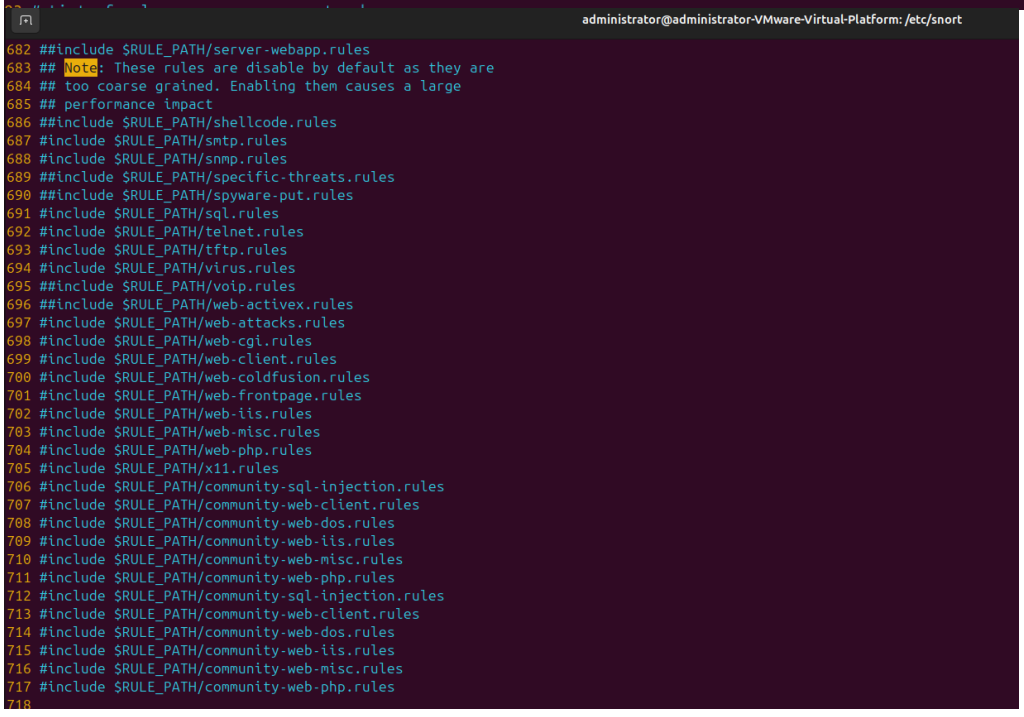
Identify the system inferface name for the IP address by using “ip a s” command. The system IP address for the interface being used here is the ens33 with IP address 192.168.92.129 with port 24.

```
administrator@administrator-VMware-Virtual-Platform:~$ ip a s
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:1b:17:d4 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.92.129/24 brd 192.168.92.255 scope global dynamic noprefixroute ens33
       valid_lft 1413sec preferred_lft 1413sec
    inet6 fe80::20c:29ff:fe1b:17d4/64 scope link
```

5 Configurations in snort.conf file

Make configurations in the snort file with right IP address and appropriate configurations to prevent the warning appearing on the system. Firstly configure the HOME_NET IP address with exact port number. The warnings on the validation snort testing can be overcome by commenting lines 597 to 717 using the *"vim"* tool to edit snort.conf in order to clear the warnings appearing. The vim prompt ***:/^/597,717s/#/*** will comment the lines and the changes are saved using ESC then enter *:wq* the write and quit from the snort.conf file using vim.





6 Test the snort functioning

The snort is tested using the snort command with -T with defined interface and console represented by -i and -c respectively.

```
administrator@administrator-VMware-Virtual-Platform: $ sudo snort -T -c /etc/snort/snort.conf -i ens33
Running in Test mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "/etc/snort/snort.conf"
PortVar 'HTTP_PORTS' defined :  [ 80:81 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 3702 4343 4848 5250 6988 7000:7001 7144
 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 50002 55555 ]
PortVar 'SHELLCODE_PORTS' defined :  [ 0:79 81:65535 ]
PortVar 'ORACLE_PORTS' defined :  [ 1024:65535 ]
PortVar 'SSH_PORTS' defined :  [ 22 ]
PortVar 'FTP_PORTS' defined :  [ 21 2100 3535 ]
PortVar 'SIP_PORTS' defined :  [ 5060:5061 5600 ]
PortVar 'FILE_DATA_PORTS' defined :  [ 80:81 110 143 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 3702 4343 4848 5250 6988 7
008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 5
PortVar 'GTP_PORTS' defined :  [ 2123 2152 3386 ]
Detection:
   Search-Method = AC-Full-Q
    Split Any/Any group = enabled
    Search-Method-Optimizations = enabled
    Maximum pattern length = 20
Tagged Packet Limit: 256
Loading dynamic engine /usr/lib/snort/snort_dynamicengine/libsf_engine.so... done
Loading all dynamic detection libs from /usr/lib/snort/snort_dynamicrules...
WARNING: No dynamic libraries found in directory /usr/lib/snort/snort_dynamicrules.
  Finished Loading all dynamic detection libs from /usr/lib/snort/snort_dynamicrules
Loading all dynamic preprocessor libs from /usr/lib/snort/snort_dynamicpreprocessor/...
  Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_pop_preproc.so... done
  Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_dnp3_preproc.so... done
  Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_ssl_preproc.so... done
  Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_ssh_preproc.so... done
  Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_ftptelnet_preproc.so... done
  Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_modbus_preproc.so... done
  Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_s7commplus_preproc.so... done
  Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_sdf_preproc.so... done
  Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_appid_preproc.so... done
```

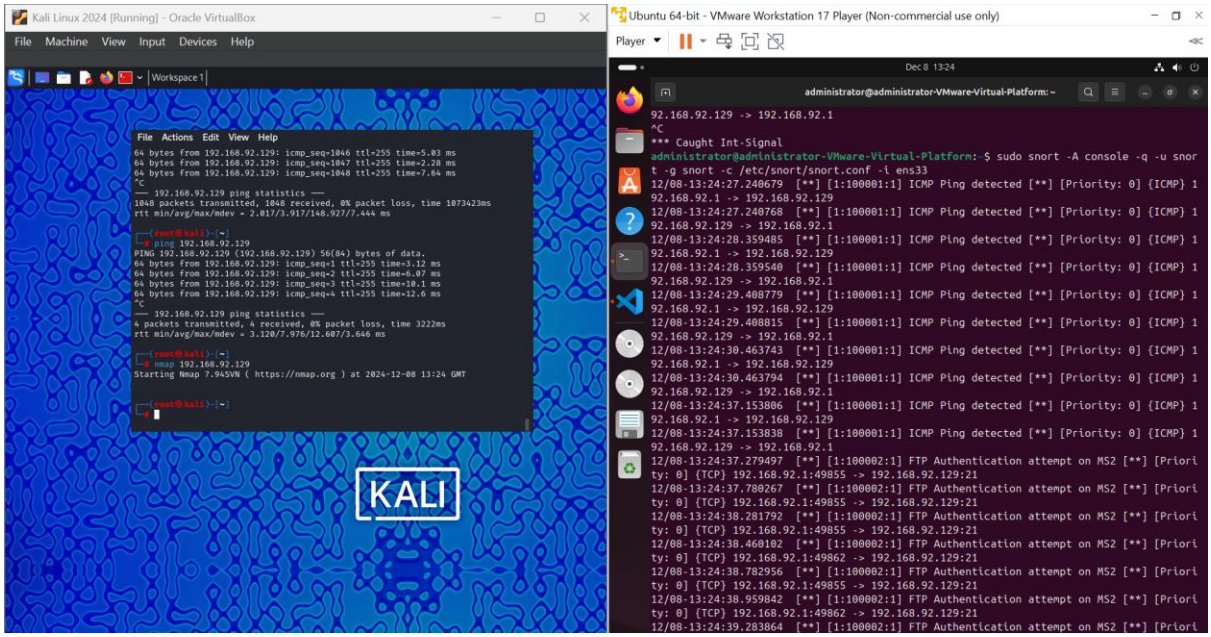
```
  Finished Loading all dynamic preprocessor libs from /usr/lib/snort/snort_dynamicpreprocessor/
Log directory = /var/log/snort
WARNING: ip4 normalizations disabled because not inline.
WARNING: tcp normalizations disabled because not inline.
WARNING: icmp4 normalizations disabled because not inline.
WARNING: ip6 normalizations disabled because not inline.
WARNING: icmp6 normalizations disabled because not inline.
Frag3 global config:
    Max frags: 65536
    Fragment memory cap: 4194304 bytes
Frag3 engine config:
    Bound Address: default
    Target-based policy: WINDOWS
    Fragment timeout: 180 seconds
    Fragment min_ttl:   1
    Fragment Anomalies: Alert
    Overlap Limit:     10
    Min fragment Length:     100
      Max Expected Streams: 768
Stream global config:
    Track TCP sessions: ACTIVE
    Max TCP sessions: 262144
    TCP cache pruning timeout: 30 seconds
    TCP cache nominal timeout: 3600 seconds
    Memcap (for reassembly packet storage): 8388608
    Track UDP sessions: ACTIVE
    Max UDP sessions: 131072
    UDP cache pruning timeout: 30 seconds
    UDP cache nominal timeout: 180 seconds
    Track ICMP sessions: INACTIVE
    Track IP sessions: INACTIVE
    Log info if session memory consumption exceeds 1048576
    Send up to 2 active responses
    Wait at least 5 seconds between responses
    Protocol Aware Flushing: ACTIVE
        Maximum Flush Point: 16000
Stream TCP Policy config:
    Bound Address: default
```

```
DCE/RPC 2 Preprocessor Configuration
  Global Configuration
    DCE/RPC Defragmentation: Enabled
    Memcap: 102400 KB
    Events: co
    SMB Fingerprint policy: Disabled
  Server Default Configuration
    Policy: WinXP
    Detect ports (PAF)
      SMB: 139 445
      TCP: 135
      UDP: 135
      RPC over HTTP server: 593
      RPC over HTTP proxy: None
    Autodetect ports (PAF)
      SMB: None
      TCP: 1025-65535
      UDP: 1025-65535
      RPC over HTTP server: 1025-65535
      RPC over HTTP proxy: None
    Invalid SMB shares: C$ D$ ADMIN$
    Maximum SMB command chaining: 3 commands
    SMB file inspection: Disabled
DNS config:
    DNS Client rdata txt Overflow Alert: ACTIVE
    Obsolete DNS RR Types Alert: INACTIVE
    Experimental DNS RR Types Alert: INACTIVE
    Ports: 53
SSLPP config:
    Encrypted packets: not inspected
    Ports:
      443      465      563      636      989
      992      993      994      995     7801
     7802     7900     7901     7902     7903
     7904     7905     7906     7907     7908
     7909     7910     7911     7912     7913
```

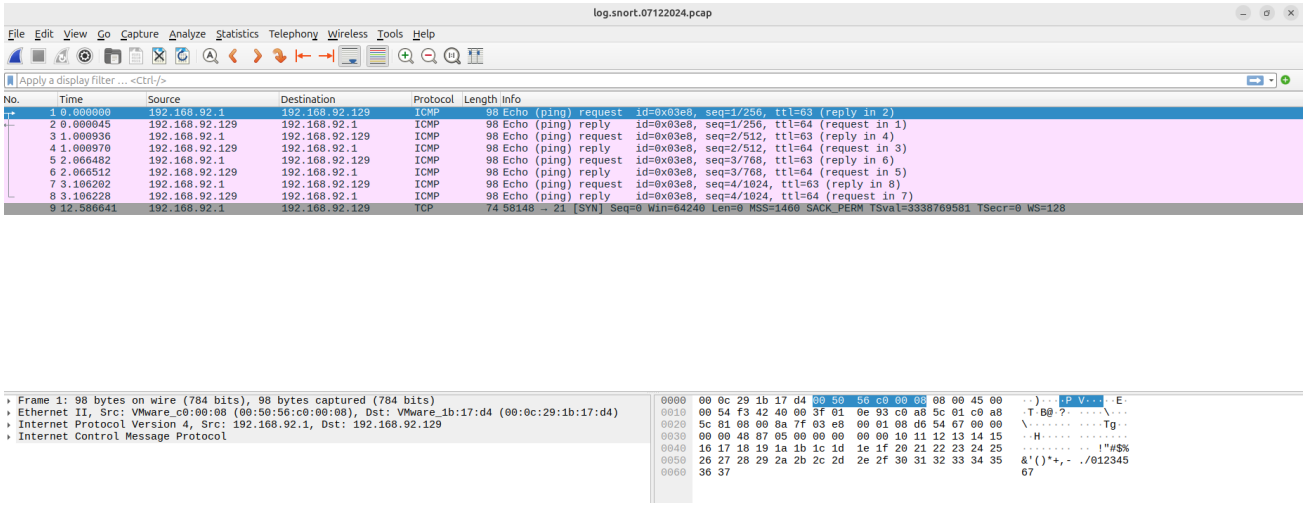
```
Acquiring network traffic from "eth0".

        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.20 GRE (Build 82)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using libpcap version 1.10.4 (with TPACKET_V3)
           Using PCRE version: 8.39 2016-06-14
           Using ZLIB version: 1.3

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

Total snort Fixed Memory Cost - MaxRss:49024
Snort successfully validated the configuration!
Snort exiting
```

7 Monitor the local network using Snort

The logs are monitored using the snort command with console (-c) and interface (-i) specified. The alerts are generated by performing ping and the network mapping over the network.



The generated logs are available in the /var/log/snort directory of the linux file system. The logs can be viewed and changed to pcap file format using the Wireshark tool.



8 Attacker machine configurations

The attacker machine using the Kali Linux Virtual machine using the NAT network configurrations and similar performance capabilities as the target machine (Ubuntu VM). Ensure that all the tools are setup to normal working conditions to perform threat analysis.

```
File  Actions  Edit  View  Help
┌──(root㉿kali)-[~]
└─# ip a s
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def
ault qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g
roup default qlen 1000
    link/ether 00:0c:29:48:4e:cc brd ff:ff:ff:ff:ff:ff
    inet 192.168.92.128/24 brd 192.168.92.255 scope global dynamic noprefixro
ute eth0
       valid_lft 1649sec preferred_lft 1649sec
    inet6 fe80::20c:29ff:fe48:4ecc/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

Setup Kali Linux VM with Metasploit Framework to generate the security alerts in the Linux. For our instance we are choosing Ubuntu hosted on Windows WSL. After the installation, run the Metasploit framework using the command “msfconsole”.

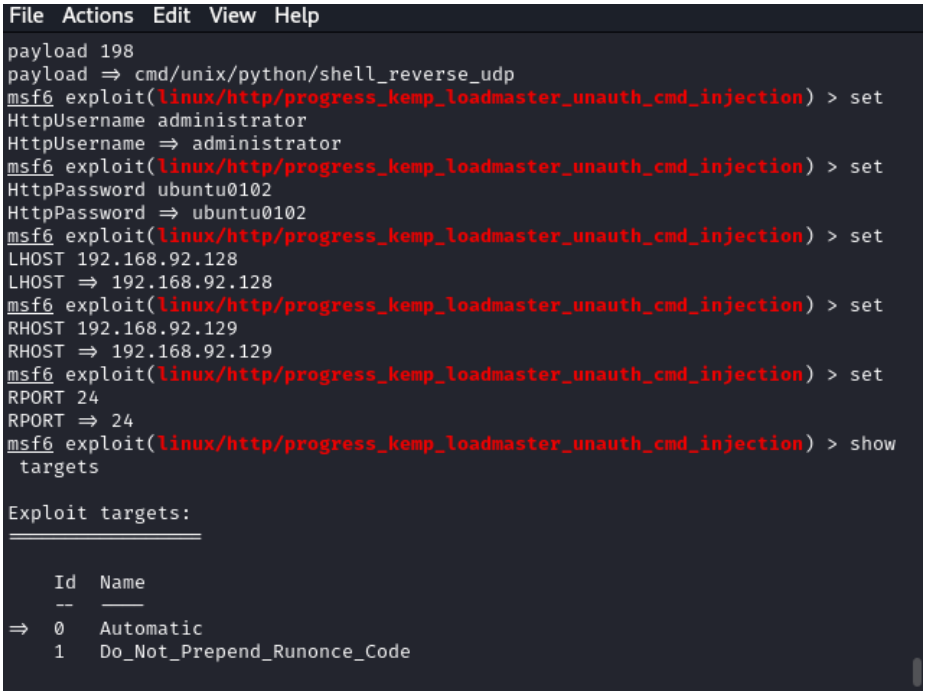
```
┌──(root㉿kali)-[~]
└─# msfconsole
Metasploit tip: You can use help to view all available commands

                .;lxO0KXXXK0Oxl:.
            ,o0WMMMMMMMMMMMMMMMMMMKd,
         'xNMMMMMMMMMMMMMMMMMMMMMMMMWx,
      :KMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMK:
    .KMMMMMMMMMMMMMMMWNNNWMMMMMMMMMMMMMMX,
   lWMMMMMMMMMMXd:..      ..;dKMMMMMMMMMMMo
  xMMMMMMMMMMWd.               .oNMMMMMMMMMk
 oMMMMMMMMMMx.                   dMMMMMMMMMx
.WMMMMMMMM:                       :MMMMMMMM,
xMMMMMMMMo                         lMMMMMMMO
NMMMMMMMW                      ,ccccoMMMMMMMWlccccc;
MMMMMMMX                       ;KMMMMMMMMMMMMMMMX:
NMMMMMMW.                        ;KMMMMMMMMMMMX:
xMMMMMMMd                          ,0MMMMMMMMK;
.WMMMMMMMc                           'OMMMMM0,
 lMMMMMMMk.                            .kMO'
  dMMMMMMMWd'                           ..
   cWMMMMMMMMMNxc'.                ##########
    .0MMMMMMMMMMMMMMMWc            #+#    #+#
      ;0MMMMMMMMMMMMMo.           +:+
        .dNMMMMMMMMMMo           +#++:++#+
           'oOWMMMMMMMo                +:+
               .,cdkO0K;         :+:    :+:
```

Search for the latest vulnerability with the type as exploit for the Linux operating system.

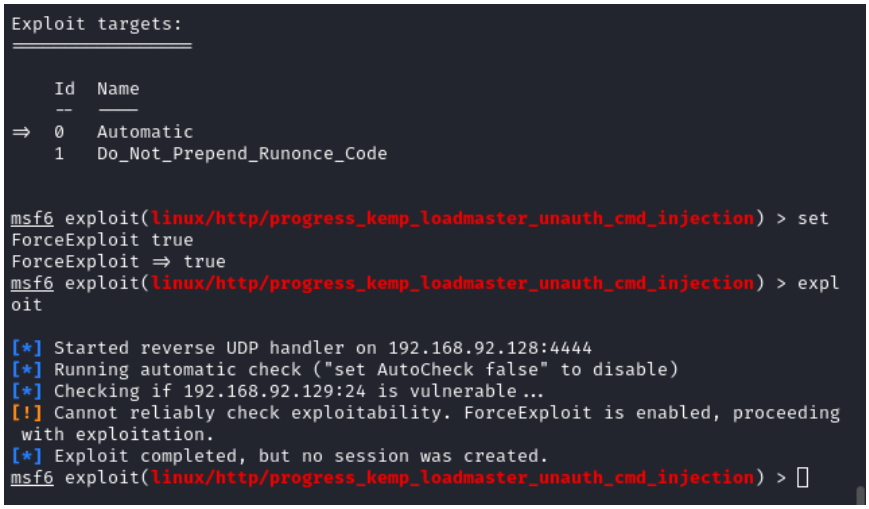
```
msf6 > search cve:2024 type:exploit platform:Linux

Matching Modules
================

   #   Name                                                                  D
isclosure Date  Rank       Check  Description
   -   ----                                                                  -
----------------  ----       -----  -----------
   0   exploit/multi/http/avideo_wwbnindex_unauth_rce                        2
024-04-09       excellent  Yes    AVideo WWBNIndex Plugin Unauthenticated RCE
   1     \_ target: Automatic                                                .
               .          .      .
   2     \_ target: PHP In-Memory                                            .
               .          .      .
   3     \_ target: Unix In-Memory                                           .
               .          .      .
   4     \_ target: Windows In-Memory                                        .
               .          .      .
   5   exploit/linux/http/apache_hugegraph_gremlin_rce                       2
024-04-22       excellent  Yes    Apache HugeGraph Gremlin RCE
   6   exploit/multi/http/apache_ofbiz_forgot_password_directory_traversal   2
024-05-30       excellent  Yes    Apache OFBiz forgotPassword/ProgramExport R
CE
   7     \_ target: Linux Command                                            .
```

```
File  Actions  Edit  View  Help
e Escalation


Interact with a module by name or index. For example info 97, use 97 or use e
xploit/linux/local/runc_cwd_priv_esc

msf6 > use 60
[*] Using configured payload cmd/linux/http/x64/meterpreter_reverse_tcp
msf6 exploit(linux/http/progress_kemp_loadmaster_unauth_cmd_injection) > show
 payloads

Compatible Payloads
===================

   #    Name                                                    Disclosur
e Date  Rank    Check  Description                             ---------
   -    ----    -----  -----------
------  ----    -----  -----------
   0    payload/cmd/linux/http/mips64/meterpreter_reverse_http      .
        normal  No     HTTP Fetch
   1    payload/cmd/linux/http/mips64/meterpreter_reverse_https     .
        normal  No     HTTP Fetch
   2    payload/cmd/linux/http/mips64/meterpreter_reverse_tcp       .
        normal  No     HTTP Fetch
   3    payload/cmd/linux/http/x64/exec                             .
        normal  No     HTTP Fetch, Linux Execute Command
   4    payload/cmd/linux/http/x64/meterpreter/bind_tcp             .
```

Set target and host details such as Http username, password, and IP address where necessary.



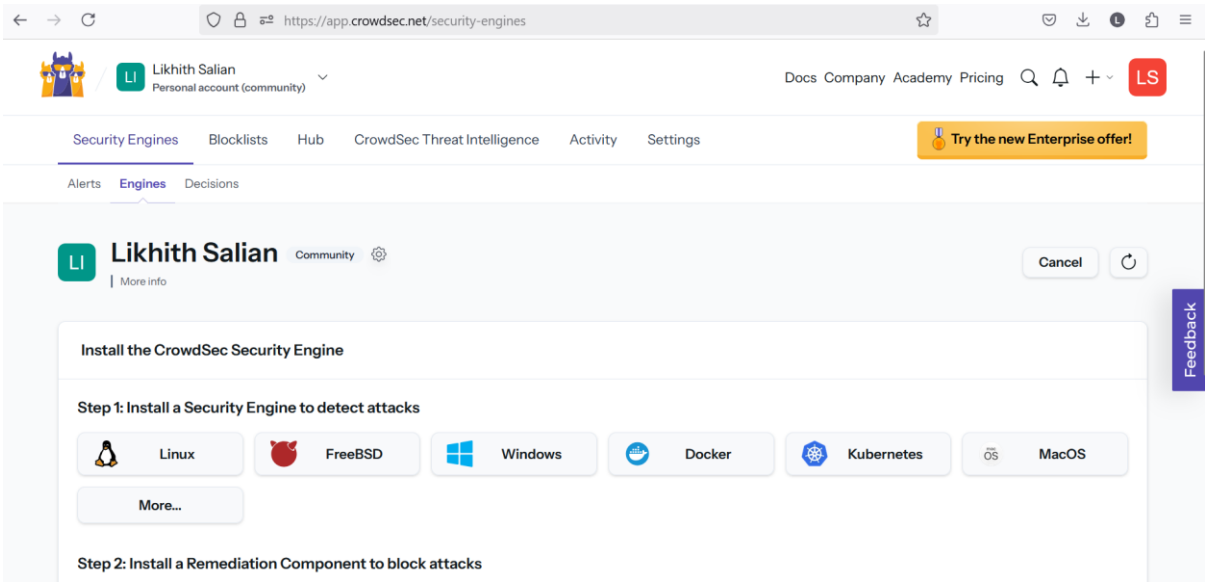
After choosing the exploit types, set target and payload. Set LHOST and set force exploit as true.



The logs with respect to the simulted incident are generated and can be identified as a unauthorised command injection attempt if the rules are pre-defined in the IDS system. Else the snort generates the logs with outcome ‘undefined incident with defined priority 0’ is shown.

9 Cloud CTI API key generation

The CTI API is necessary for the machine learning to identify the threats in the cyber threat landscape. The CrowdSec API platform is used for the threat analysis with crowdsec API installated on the system. This is an optional functionality to add on.

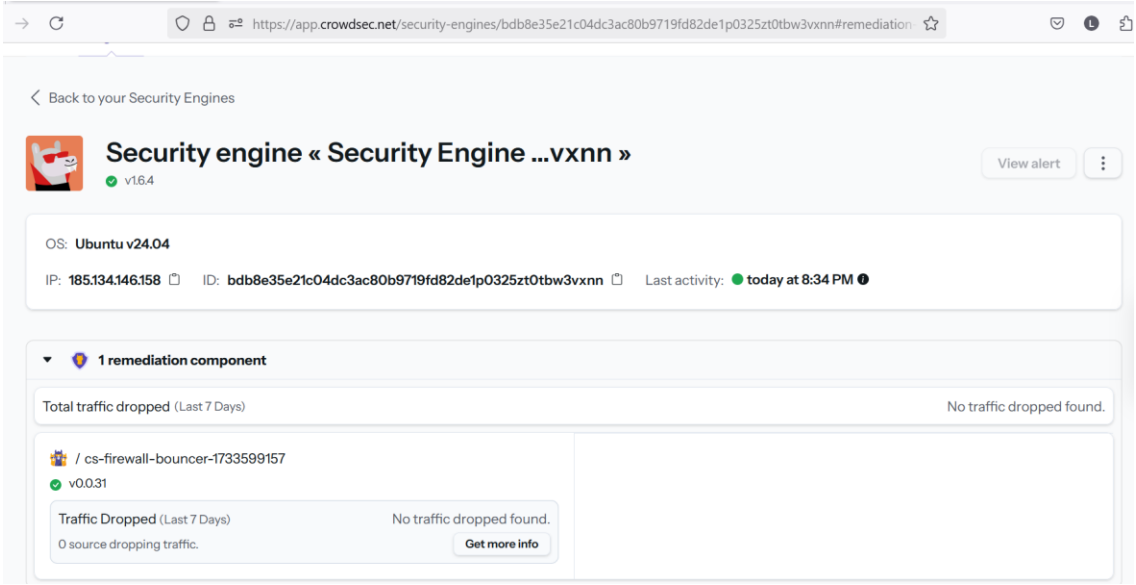



```
administrator@administrator-VMware-Virtual-Platform:~$ curl -s https://install.crowdsec.net | sudo sh
[sudo] password for administrator:
Detected operating system as ubuntu/24.
Detected apt version as 2.7.14
Checking for gpg...
Detected gpg...
Checking for curl...
Detected curl...

Importing packagecloud gpg key...

Packagecloud gpg key imported to /etc/apt/keyrings/crowdsec_crowdsec-archive-keyring.gpg

Installing /etc/apt/sources.list.d/crowdsec_crowdsec.list...
```

Upon completion of the installation of the crowdsec CTI, restart the crowdsec cloud API.

```
administrator@administrator-VMware-Virtual-Platform:~$ systemctl restart crowdsec
```

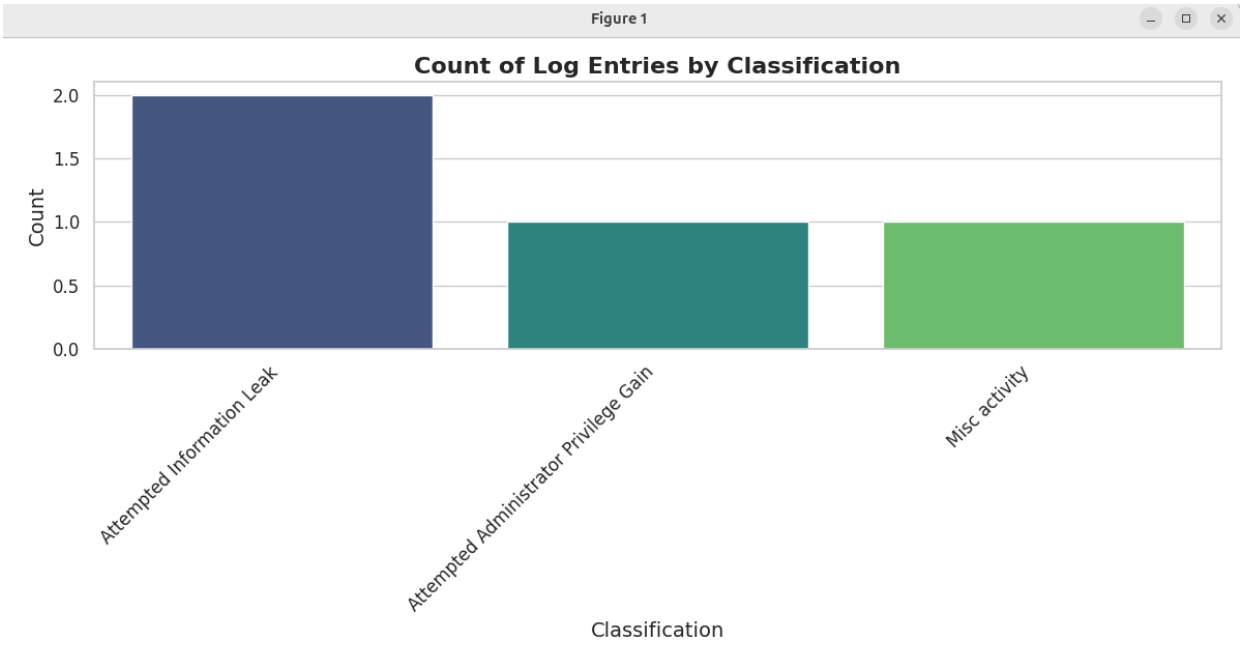
Integrate the API key provided with the Ubuntu Virtual Machine using the command. Upon integration of CrowdSec Cloud API the security engine shows connected.



10 Code execution and output

The primary step towards the log analysis includes the parsing and structuring the log data into the necessary format. The parsed logs are then classified into required formats to generate the graphical data as an output. The graphs represent the number of log entry classification and log count on priorities of the security incident to be addressed.

```
(.venv) administrator@administrator-VMware-Virtual-Platform:~$ /home/administrator/.venv/bin/python "/home/administrator/Thesis project/log_parsing.py"
          sid                  message                    classification  priority protocol         src_ip src_port         dest_ip dest_port
0  1:2000001:1       ICMP PING detected             Attempted Information Leak         2     ICMP  192.168.92.128     None  192.168.92.129      None
1  1:2000003:1  SSH Brute Force attempt  Attempted Administrator Privilege Gain         1      TCP  192.168.92.128       22  192.168.92.129        22
2  1:2000004:1    Suspicious UDP packet                          Misc activity         3      UDP   192.168.1.150     5353   192.168.1.255      5353
3  1:2000005:1  TCP port scan detected             Attempted Information Leak         3      TCP   192.168.1.150       22   192.168.1.255        22
/home/administrator/Thesis project/log_parsing.py:73: FutureWarning:

Passing `palette` without assigning `hue` is deprecated and will be removed in v0.14.0. Assign the `x` variable to `hue` and set `legend=False` for the same effect.

  sns.barplot(
/home/administrator/Thesis project/log_parsing.py:88: FutureWarning:

Passing `palette` without assigning `hue` is deprecated and will be removed in v0.14.0. Assign the `x` variable to `hue` and set `legend=False` for the same effect.
```



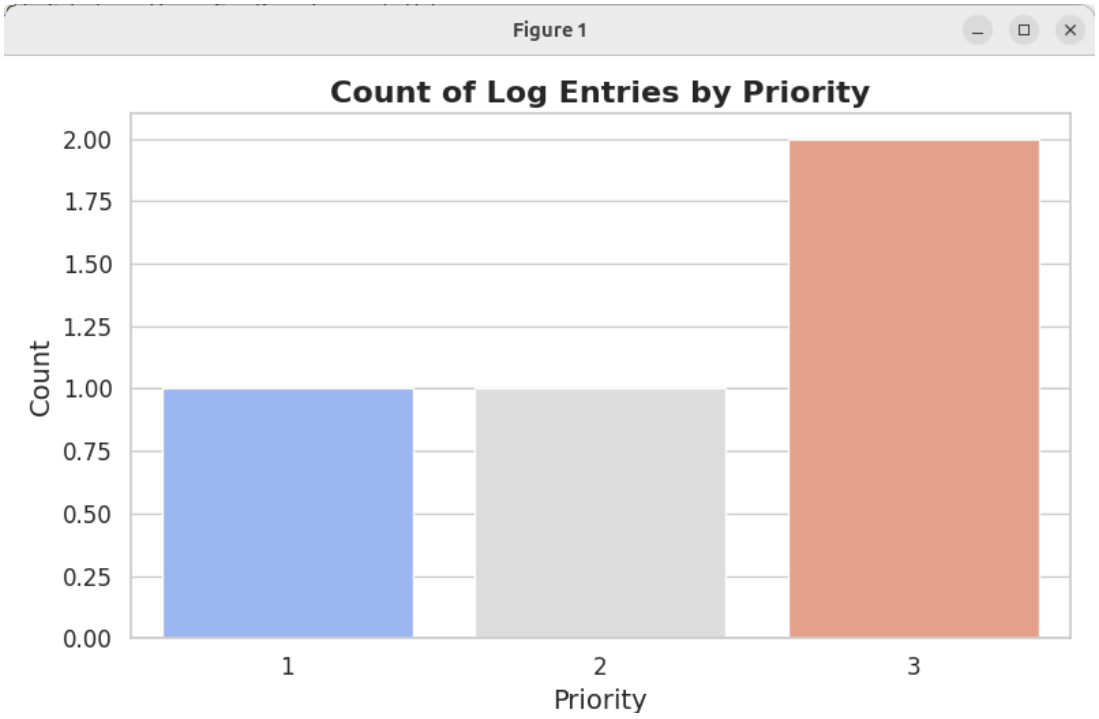


Figure 1
Count of Log Entries by Priority
2.00
1.75
1.50
1.25
1.00
0.75
0.50
0.25
0.00
Count
1
2
3
Priority