Detecting ICMP Traffic with Snort and Suricata- A Beginner's Guide.

I’ll walk you through how to set up two powerful open-source network intrusion detection systems—Snort and Suricata—to detect ICMP (ping) traffic using custom rules. Whether you’re new to NIDS or brushing up your skills, this guide has you covered with step-by-step instructions and commands tested on Ubuntu.

Snort and Suricata are both popular Network Intrusion Detection and Prevention Systems (NIDS/NIPS). They monitor network traffic in real time and generate alerts (or even block malicious packets) based on predefined or custom rules.

Prerequisites

- Operating System: Ubuntu (tested on 20.04/22.04)
- Network Interface: A configured network interface (e.g., enp0s3 or eth0)
- Network Range: Knowledge of your local network subnet (e.g.,192.168.1.0/24)
- Root Access: Administrative privileges (sudo) for installation and configuration
- Internet Access: Required for package downloads and updates

INSTALLATION AND CONFIGURATION OF SNORT

Step 1: Install Snort :

Update your system and install Snort:

```
sudo apt update && sudo apt install -y snort
```

During installation, select the correct network interface (e.g., enp0s3 or eth0) and set your local network range (e.g., 192.168.1.0/24).

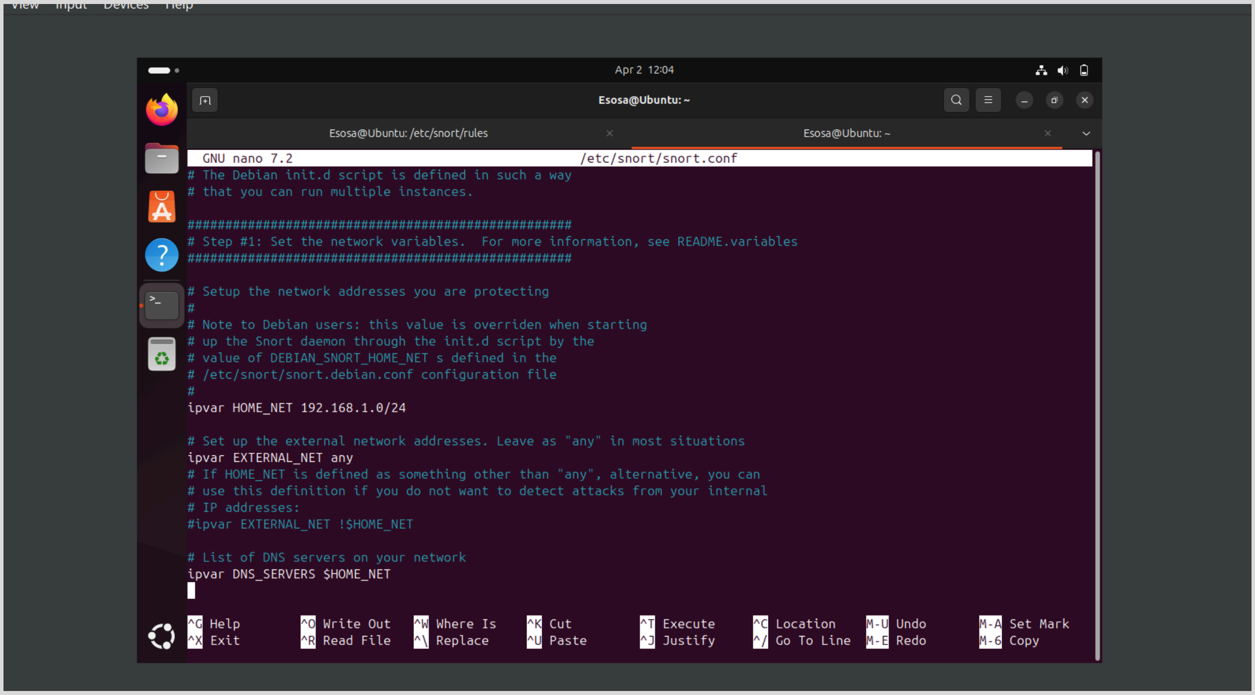
Step 2: Configure Snort:

Edit the main configuration file:

```
sudo nano /etc/snort/snort.conf
```

Find the line starting with ipvar HOME_NET and set your subnet:

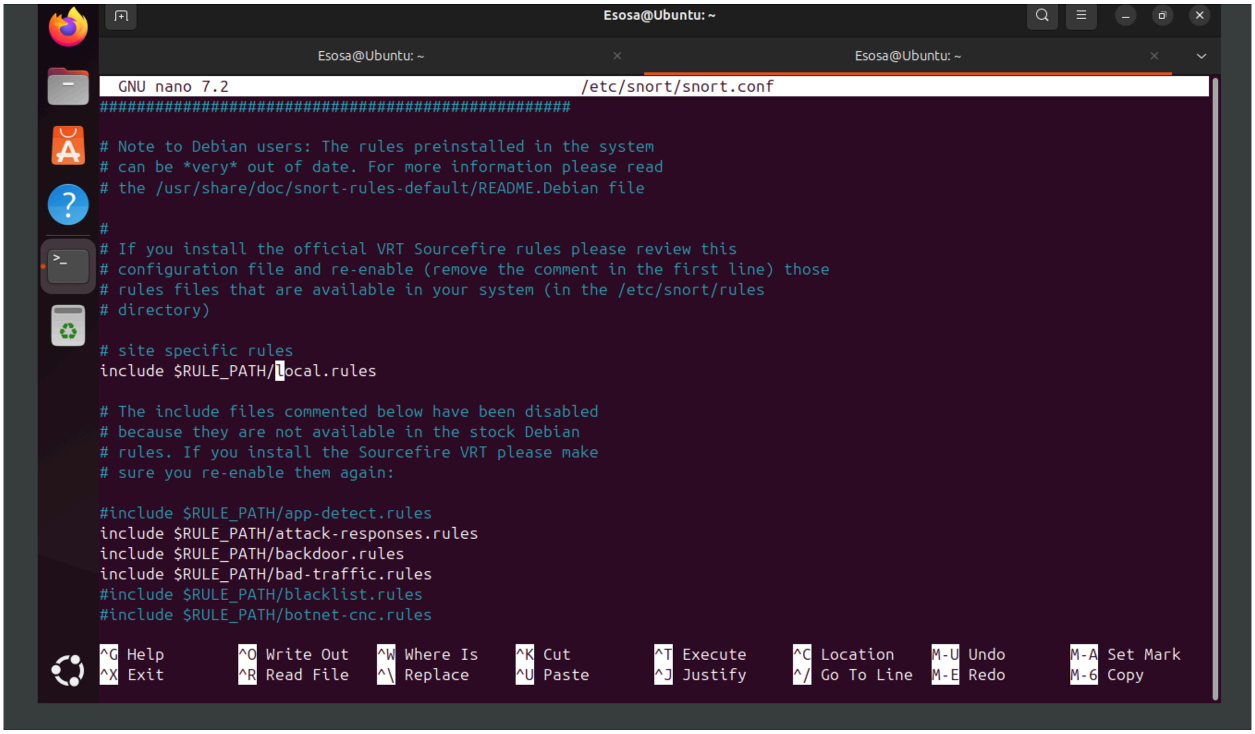
ipvar HOME_NET 192.168.1.0/24



```
  GNU nano 7.2                              /etc/snort/snort.conf
# The Debian init.d script is defined in such a way
# that you can run multiple instances.

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

# 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 192.168.1.0/24

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

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


^G Help       ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo      M-A Set Mark
^X Exit       ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^/ Go To Line M-E Redo      M-6 Copy
```

Also, make sure the following line is included (to enable your local rules):

include $RULE_PATH/local.rules

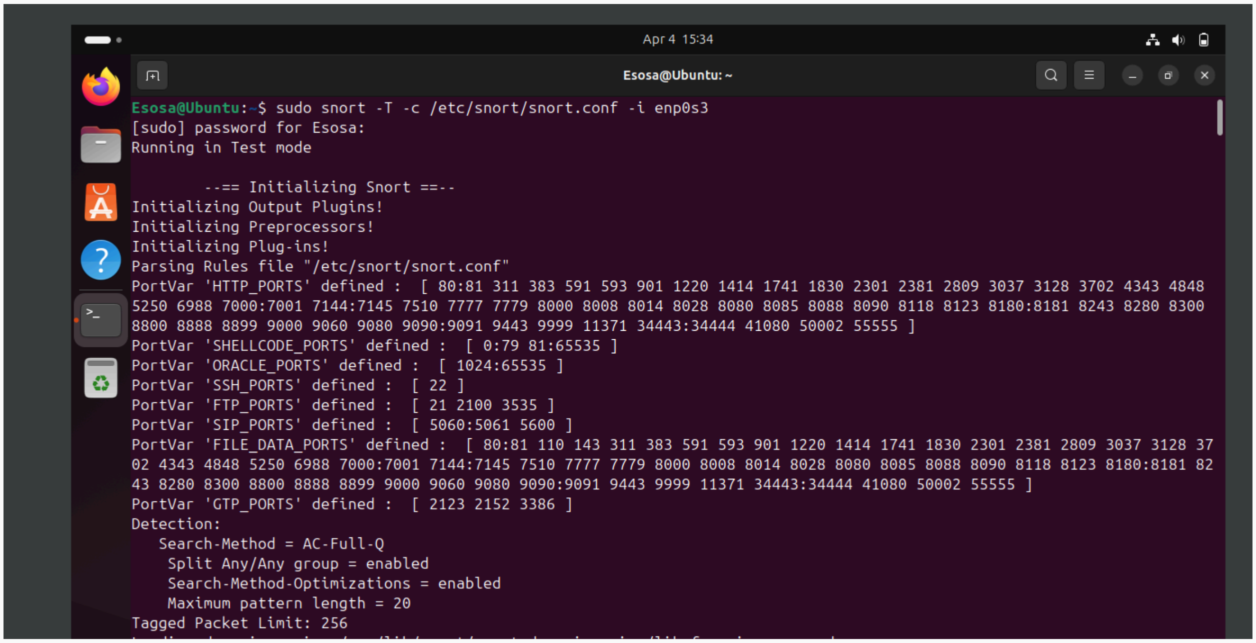


```
  GNU nano 7.2                                    /etc/snort/snort.conf
###################################################

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

#
# If you install the official VRT Sourcefire rules please review this
# configuration file and re-enable (remove the comment in the first line) those
# rules files that are available in your system (in the /etc/snort/rules
# directory)

# site specific rules
include $RULE_PATH/local.rules

# The include files commented below have been disabled
# because they are not available in the stock Debian
# rules. If you install the Sourcefire VRT please make
# sure you re-enable them again:

#include $RULE_PATH/app-detect.rules
include $RULE_PATH/attack-responses.rules
include $RULE_PATH/backdoor.rules
include $RULE_PATH/bad-traffic.rules
#include $RULE_PATH/blacklist.rules
#include $RULE_PATH/botnet-cnc.rules
```

Step 3: Test Snort configuration:

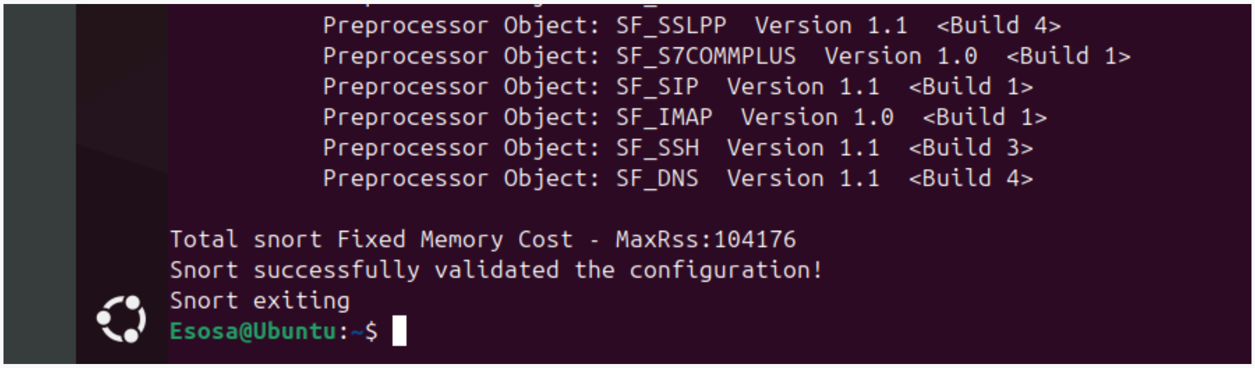
```
sudo snort -T -c /etc/snort/snort.conf -i enp0s3
```

Where -T is Test mode, -c is the path to the configuration file, and -i is the specified network interface.



```
Esosa@Ubuntu:~$ sudo snort -T -c /etc/snort/snort.conf -i enp0s3
[sudo] password for Esosa:
Running in Test mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "/etc/snort/snort.conf"
PortVar 'HTTP_PORTS' defined :  [ 80:81 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 3702 4343 4848
5250 6988 7000:7001 7144:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300
8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 50002 55555 ]
PortVar 'SHELLCODE_PORTS' defined :  [ 0:79 81:65535 ]
PortVar 'ORACLE_PORTS' defined :  [ 1024:65535 ]
PortVar 'SSH_PORTS' defined :  [ 22 ]
PortVar 'FTP_PORTS' defined :  [ 21 2100 3535 ]
PortVar 'SIP_PORTS' defined :  [ 5060:5061 5600 ]
PortVar 'FILE_DATA_PORTS' defined :  [ 80:81 110 143 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 37
02 4343 4848 5250 6988 7000:7001 7144:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 82
43 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 50002 55555 ]
PortVar 'GTP_PORTS' defined :  [ 2123 2152 3386 ]
Detection:
   Search-Method = AC-Full-Q
    Split Any/Any group = enabled
    Search-Method-Optimizations = enabled
    Maximum pattern length = 20
Tagged Packet Limit: 256
```

If successful, you should see this:



```
            Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
            Preprocessor Object: SF_S7COMMPLUS  Version 1.0  <Build 1>
            Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
            Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
            Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
            Preprocessor Object: SF_DNS  Version 1.1  <Build 4>

Total snort Fixed Memory Cost - MaxRss:104176
Snort successfully validated the configuration!
Snort exiting
Esosa@Ubuntu:~$ 
```

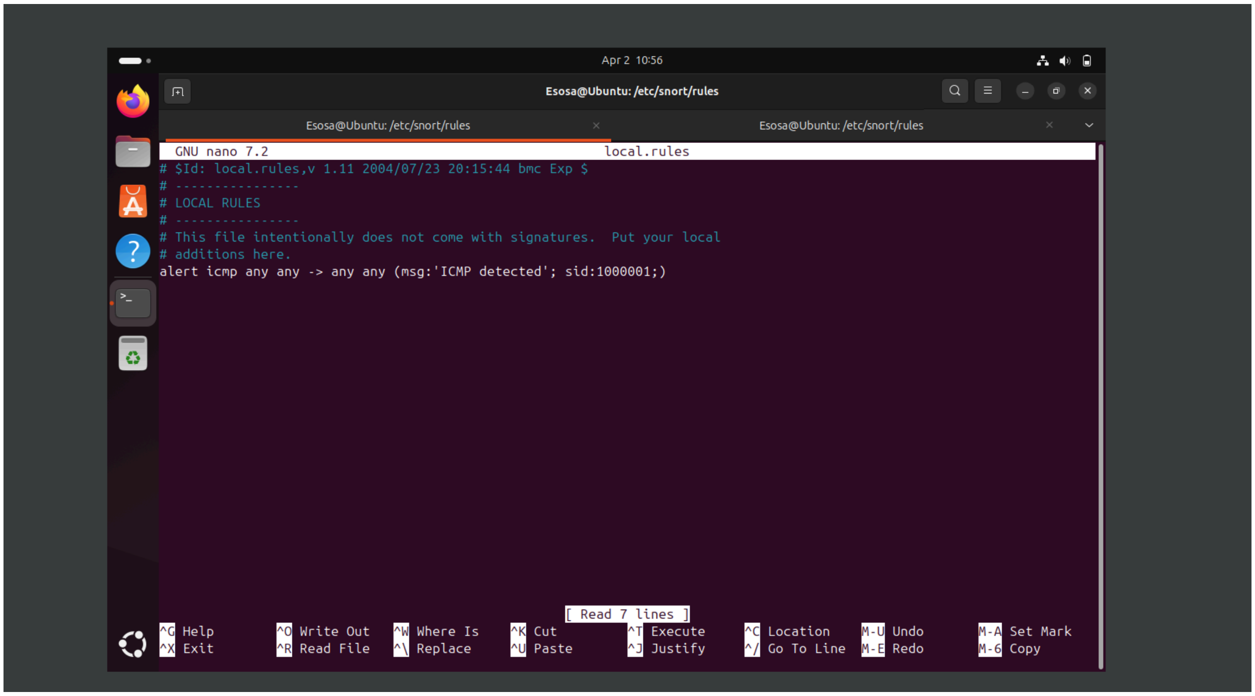
Step 4: Create a custom ICMP rule :

Edit the rule file: /etc/snort/rules/local.rules:

```
sudo nano /etc/snort/rules/local.rules
```

Add this rule to detect all ICMP traffic:

```
alert icmp any any -> any any (msg:"ICMP detected"; sid:1000001; rev:1;
```



Apr 2 10:56
Esosa@Ubuntu: /etc/snort/rules
Esosa@Ubuntu: /etc/snort/rules
Esosa@Ubuntu: /etc/snort/rules

```
  GNU nano 7.2                                      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 -> any any (msg:'ICMP detected'; sid:1000001;)
```

```
                                                    [ Read 7 lines ]
^G Help          ^O Write Out     ^W Where Is      ^K Cut           ^T Execute       ^C Location      M-U Undo         M-A Set Mark
^X Exit          ^R Read File     ^\ Replace       ^U Paste         ^J Justify       ^/ Go To Line    M-E Redo         M-6 Copy
```

Save and Exit.

Step 5: Run Snort in IDS Mode :

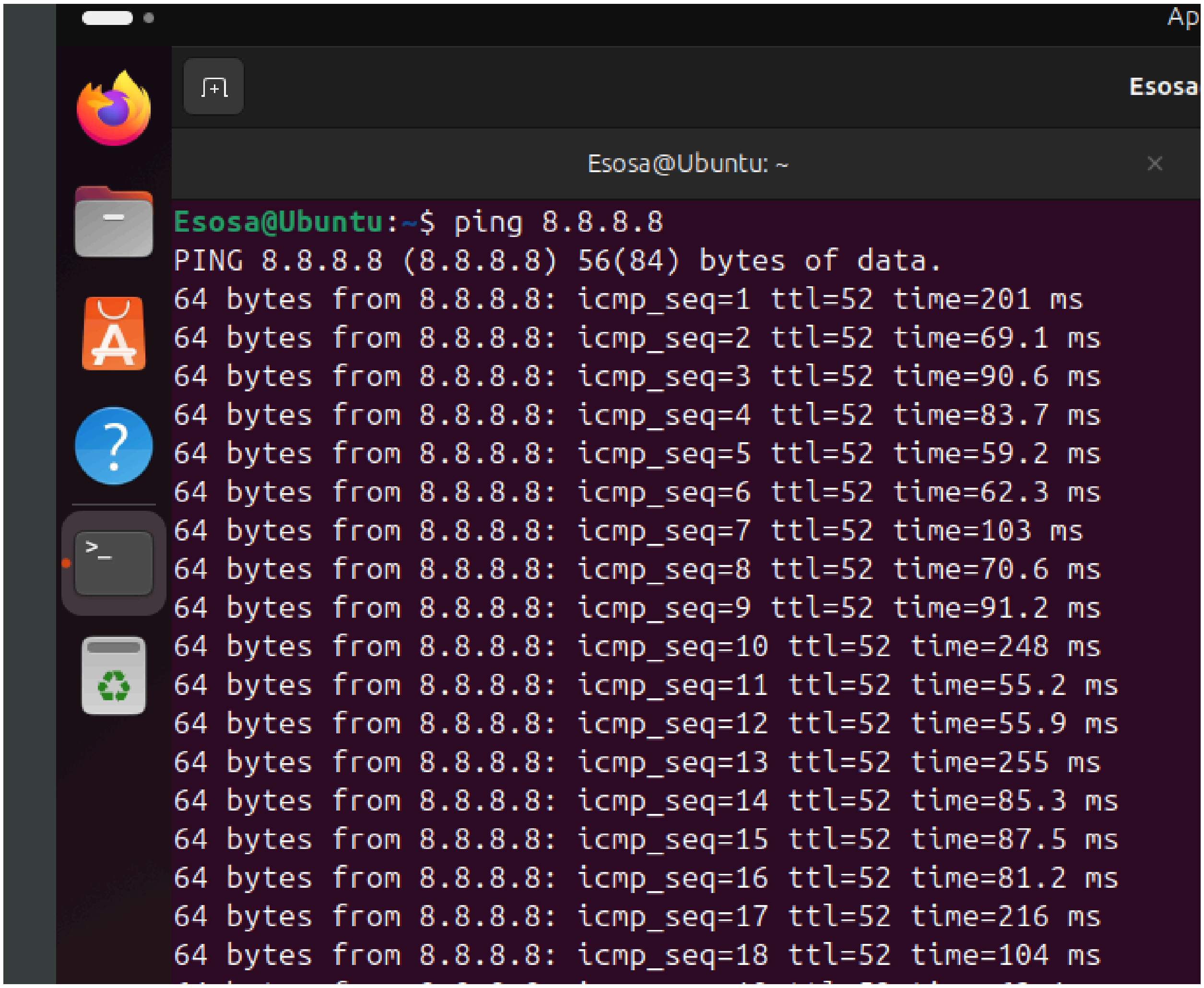
Now start Snort in IDS mode and observe alerts on the terminal:

```
sudo snort -A console -q -c /etc/snort/snort.conf -i enp0s3
```

Step 6: Generate ICMP Traffic:

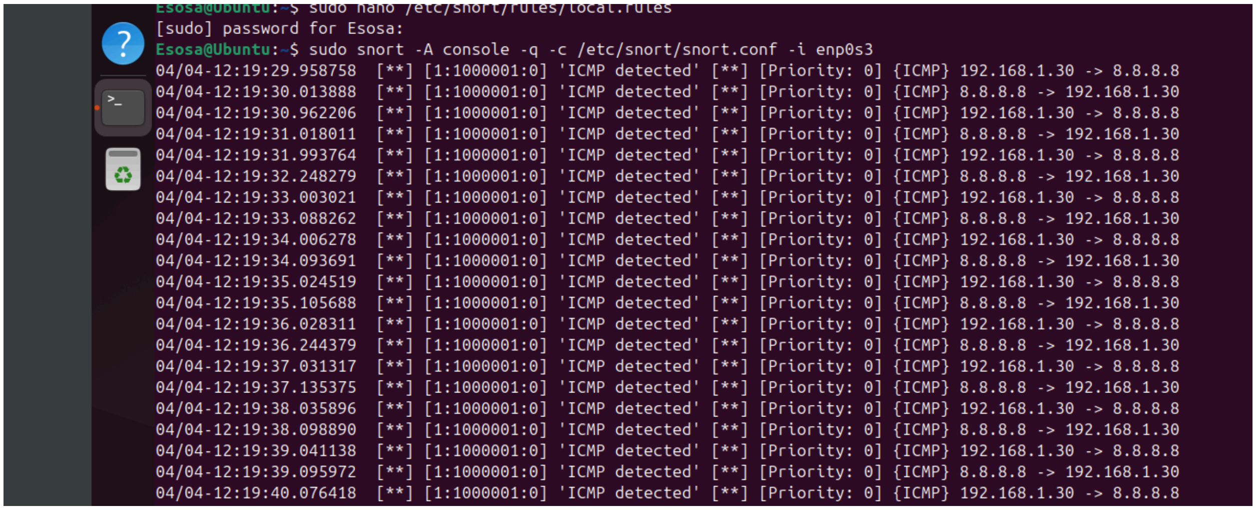
Use the ping command to generate ICMP packets:

```
ping 8.8.8.8
```



```
Esosa@Ubuntu:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=52 time=201 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=52 time=69.1 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=52 time=90.6 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=52 time=83.7 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=52 time=59.2 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=52 time=62.3 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=52 time=103 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=52 time=70.6 ms
64 bytes from 8.8.8.8: icmp_seq=9 ttl=52 time=91.2 ms
64 bytes from 8.8.8.8: icmp_seq=10 ttl=52 time=248 ms
64 bytes from 8.8.8.8: icmp_seq=11 ttl=52 time=55.2 ms
64 bytes from 8.8.8.8: icmp_seq=12 ttl=52 time=55.9 ms
64 bytes from 8.8.8.8: icmp_seq=13 ttl=52 time=255 ms
64 bytes from 8.8.8.8: icmp_seq=14 ttl=52 time=85.3 ms
64 bytes from 8.8.8.8: icmp_seq=15 ttl=52 time=87.5 ms
64 bytes from 8.8.8.8: icmp_seq=16 ttl=52 time=81.2 ms
64 bytes from 8.8.8.8: icmp_seq=17 ttl=52 time=216 ms
64 bytes from 8.8.8.8: icmp_seq=18 ttl=52 time=104 ms
```

You should see this in the Snort output:



```
Esosa@Ubuntu:~$ sudo nano /etc/snort/rules/local.rules
[sudo] password for Esosa:
Esosa@Ubuntu:~$ sudo snort -A console -q -c /etc/snort/snort.conf -i enp0s3
04/04-12:19:29.958758  [**] [1:1000001:0] 'ICMP detected' [**] [Priority: 0] {ICMP} 192.168.1.30 -> 8.8.8.8
04/04-12:19:30.013888  [**] [1:1000001:0] 'ICMP detected' [**] [Priority: 0] {ICMP} 8.8.8.8 -> 192.168.1.30
04/04-12:19:30.962206  [**] [1:1000001:0] 'ICMP detected' [**] [Priority: 0] {ICMP} 192.168.1.30 -> 8.8.8.8
04/04-12:19:31.018011  [**] [1:1000001:0] 'ICMP detected' [**] [Priority: 0] {ICMP} 8.8.8.8 -> 192.168.1.30
04/04-12:19:31.993764  [**] [1:1000001:0] 'ICMP detected' [**] [Priority: 0] {ICMP} 192.168.1.30 -> 8.8.8.8
04/04-12:19:32.248279  [**] [1:1000001:0] 'ICMP detected' [**] [Priority: 0] {ICMP} 8.8.8.8 -> 192.168.1.30
04/04-12:19:33.003021  [**] [1:1000001:0] 'ICMP detected' [**] [Priority: 0] {ICMP} 192.168.1.30 -> 8.8.8.8
04/04-12:19:33.088262  [**] [1:1000001:0] 'ICMP detected' [**] [Priority: 0] {ICMP} 8.8.8.8 -> 192.168.1.30
04/04-12:19:34.006278  [**] [1:1000001:0] 'ICMP detected' [**] [Priority: 0] {ICMP} 192.168.1.30 -> 8.8.8.8
04/04-12:19:34.093691  [**] [1:1000001:0] 'ICMP detected' [**] [Priority: 0] {ICMP} 8.8.8.8 -> 192.168.1.30
04/04-12:19:35.024519  [**] [1:1000001:0] 'ICMP detected' [**] [Priority: 0] {ICMP} 192.168.1.30 -> 8.8.8.8
04/04-12:19:35.105688  [**] [1:1000001:0] 'ICMP detected' [**] [Priority: 0] {ICMP} 8.8.8.8 -> 192.168.1.30
04/04-12:19:36.028311  [**] [1:1000001:0] 'ICMP detected' [**] [Priority: 0] {ICMP} 192.168.1.30 -> 8.8.8.8
04/04-12:19:36.244379  [**] [1:1000001:0] 'ICMP detected' [**] [Priority: 0] {ICMP} 8.8.8.8 -> 192.168.1.30
04/04-12:19:37.031317  [**] [1:1000001:0] 'ICMP detected' [**] [Priority: 0] {ICMP} 192.168.1.30 -> 8.8.8.8
04/04-12:19:37.135375  [**] [1:1000001:0] 'ICMP detected' [**] [Priority: 0] {ICMP} 8.8.8.8 -> 192.168.1.30
04/04-12:19:38.035896  [**] [1:1000001:0] 'ICMP detected' [**] [Priority: 0] {ICMP} 192.168.1.30 -> 8.8.8.8
04/04-12:19:38.098890  [**] [1:1000001:0] 'ICMP detected' [**] [Priority: 0] {ICMP} 8.8.8.8 -> 192.168.1.30
04/04-12:19:39.041138  [**] [1:1000001:0] 'ICMP detected' [**] [Priority: 0] {ICMP} 192.168.1.30 -> 8.8.8.8
04/04-12:19:39.095972  [**] [1:1000001:0] 'ICMP detected' [**] [Priority: 0] {ICMP} 8.8.8.8 -> 192.168.1.30
04/04-12:19:40.076418  [**] [1:1000001:0] 'ICMP detected' [**] [Priority: 0] {ICMP} 192.168.1.30 -> 8.8.8.8
```

Congratulations! Snort is working.

INSTALLATION AND CONFIGURATION OF SURICATA

Step 1: Add Suricata Repository and Install Suricata package:

Add the Open Information Security Foundation (OISF) repository to your system:

```
sudo add-apt-repository ppa:oisf/suricata-stable
```

Install Suricata:

```
sudo apt install -y suricata
```

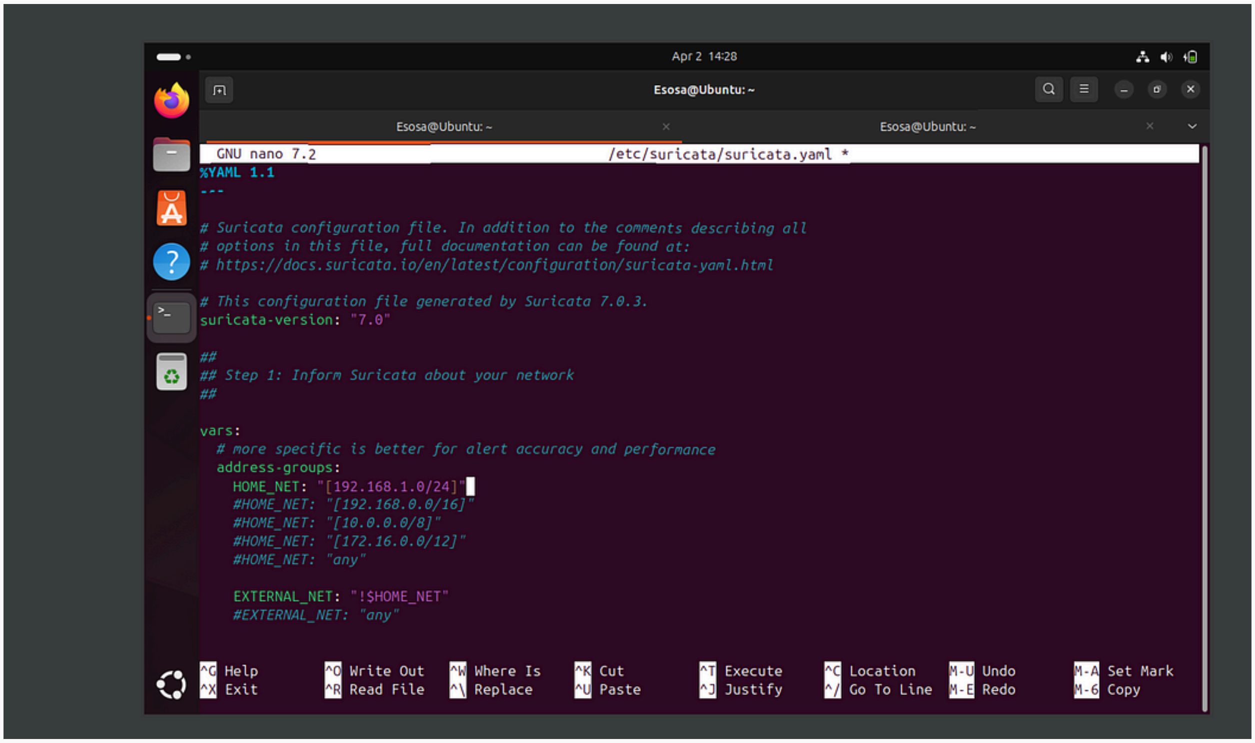
Step 2: Configure Suricata:

Open the main config file:

```
sudo nano /etc/suricata/suricata.yaml
```

Look for the HOME_NET variable and set it to your network:

```
home-net: "[192.168.1.0/24]"
```



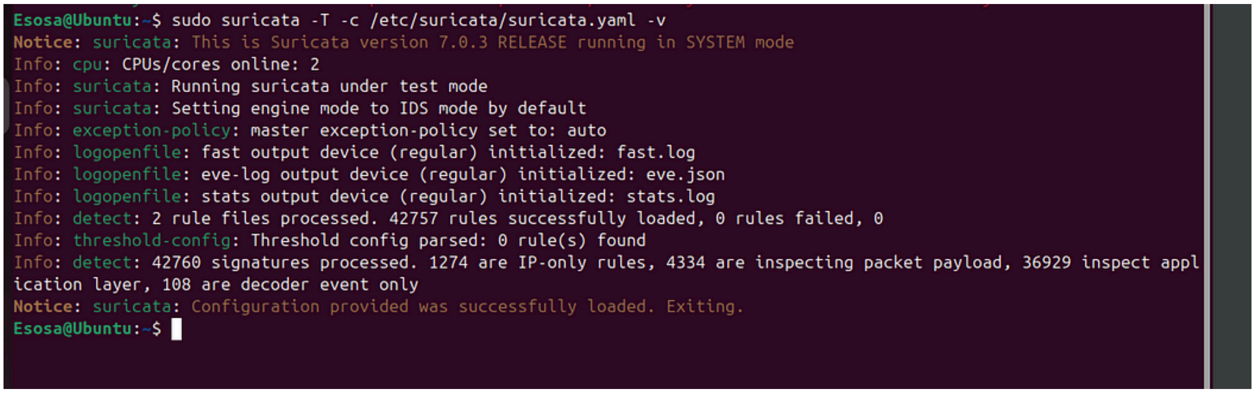
```
  GNU nano 7.2                    /etc/suricata/suricata.yaml *
%YAML 1.1
---

# Suricata configuration file. In addition to the comments describing all
# options in this file, full documentation can be found at:
# https://docs.suricata.io/en/latest/configuration/suricata-yaml.html

# This configuration file generated by Suricata 7.0.3.
suricata-version: "7.0"

##
## Step 1: Inform Suricata about your network
##

vars:
  # more specific is better for alert accuracy and performance
  address-groups:
    HOME_NET: "[192.168.1.0/24]"
    #HOME_NET: "[192.168.0.0/16]"
    #HOME_NET: "[10.0.0.0/8]"
    #HOME_NET: "[172.16.0.0/12]"
    #HOME_NET: "any"

    EXTERNAL_NET: "!$HOME_NET"
    #EXTERNAL_NET: "any"

^G Help        ^O Write Out   ^W Where Is    ^K Cut         ^T Execute     ^C Location    M-U Undo       M-A Set Mark
^X Exit        ^R Read File   ^\ Replace     ^U Paste       ^J Justify     ^/ Go To Line  M-E Redo       M-6 Copy
```

Also, confirm the interface to be used (you can pass it when running Suricata).

Step 3 : Test Suricata configuration:

```
sudo suricata -T -c /etc/suricata/suricata.yaml -v
```

If successful, you should see this:

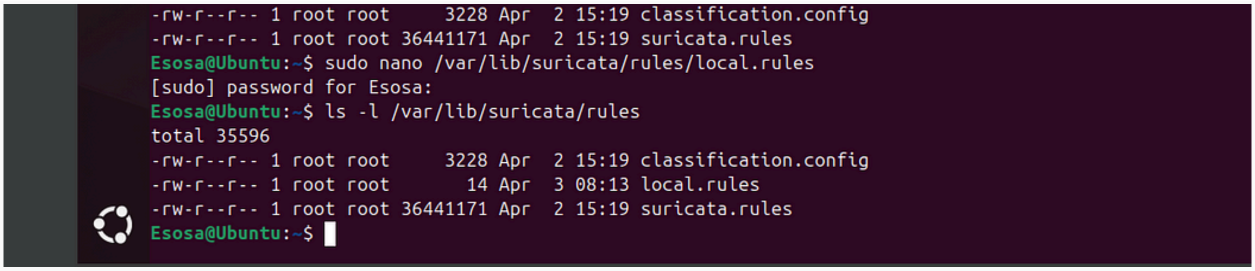


```
Esosa@Ubuntu:~$ sudo suricata -T -c /etc/suricata/suricata.yaml -v
Notice: suricata: This is Suricata version 7.0.3 RELEASE running in SYSTEM mode
Info: cpu: CPUs/cores online: 2
Info: suricata: Running suricata under test mode
Info: suricata: Setting engine mode to IDS mode by default
Info: exception-policy: master exception-policy set to: auto
Info: logopenfile: fast output device (regular) initialized: fast.log
Info: logopenfile: eve-log output device (regular) initialized: eve.json
Info: logopenfile: stats output device (regular) initialized: stats.log
Info: detect: 2 rule files processed. 42757 rules successfully loaded, 0 rules failed, 0
Info: threshold-config: Threshold config parsed: 0 rule(s) found
Info: detect: 42760 signatures processed. 1274 are IP-only rules, 4334 are inspecting packet payload, 36929 inspect appl
ication layer, 108 are decoder event only
Notice: suricata: Configuration provided was successfully loaded. Exiting.
Esosa@Ubuntu:~$ 
```

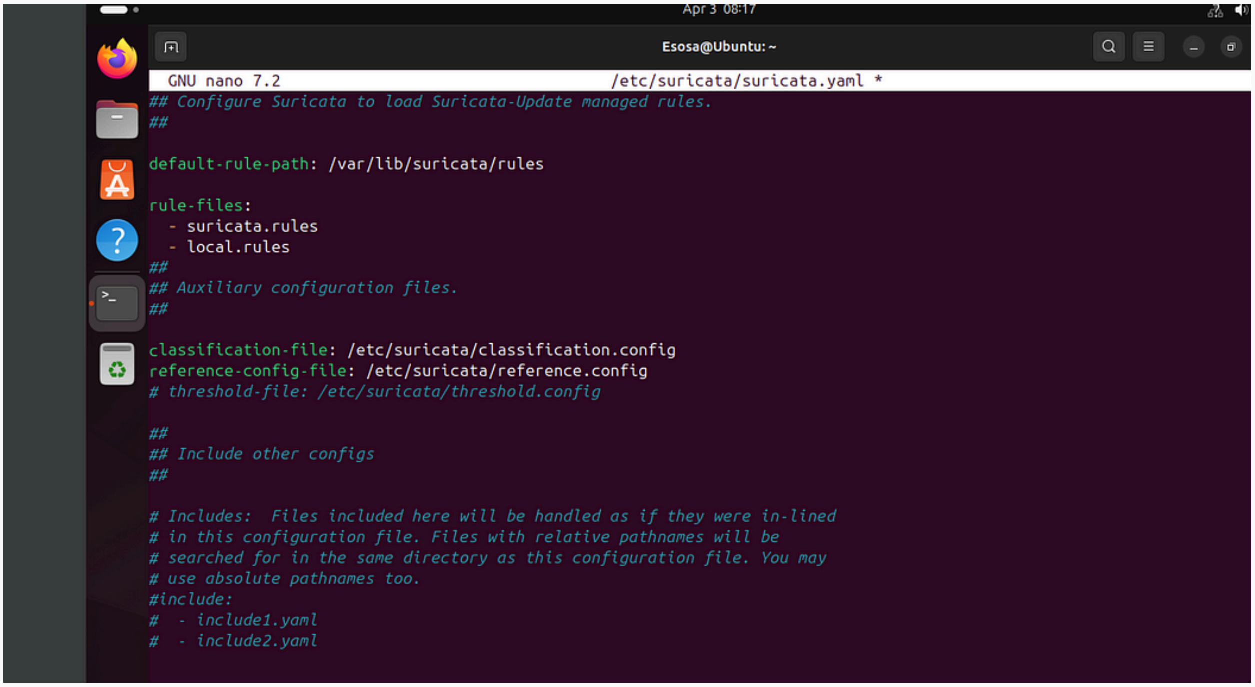
Step 4: Add Custom ICMP Rule:

Create a local rules file under the /Var/lib/suricata/rules directory and edit the file:

```
sudo nano /var/lib/suricata/rules/local.rules
```



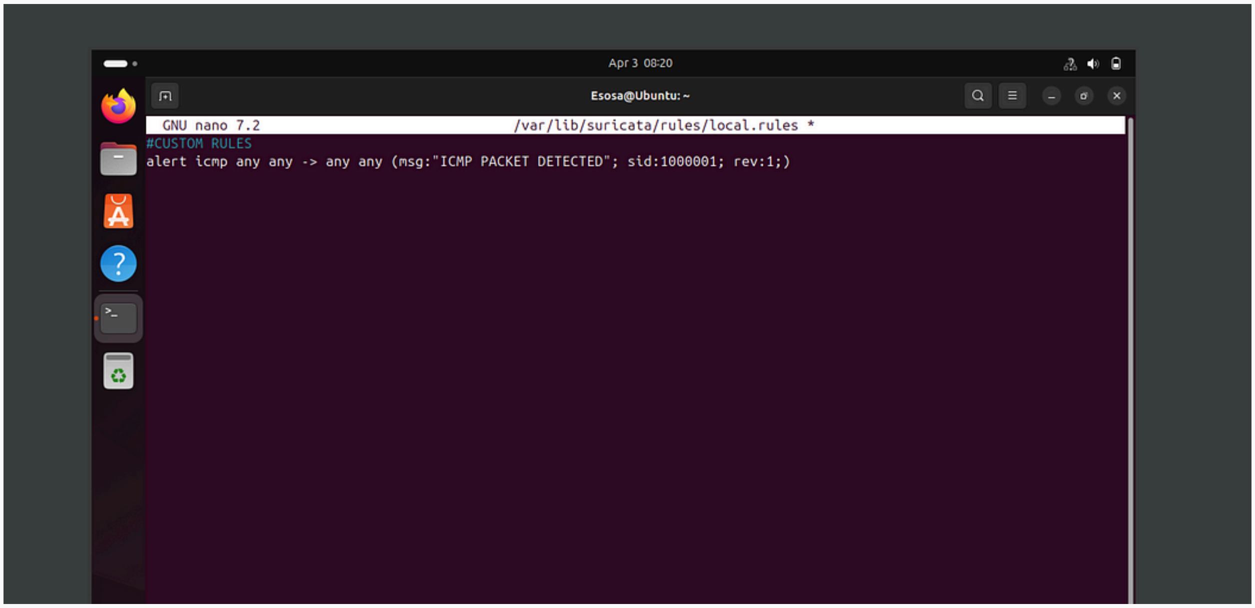
```
-rw-r--r-- 1 root root     3228 Apr  2 15:19 classification.config
-rw-r--r-- 1 root root 36441171 Apr  2 15:19 suricata.rules
Esosa@Ubuntu:~$ sudo nano /var/lib/suricata/rules/local.rules
[sudo] password for Esosa:
Esosa@Ubuntu:~$ ls -l /var/lib/suricata/rules
total 35596
-rw-r--r-- 1 root root     3228 Apr  2 15:19 classification.config
-rw-r--r-- 1 root root       14 Apr  3 08:13 local.rules
-rw-r--r-- 1 root root 36441171 Apr  2 15:19 suricata.rules
Esosa@Ubuntu:~$ 
```



```
  GNU nano 7.2                               /etc/suricata/suricata.yaml *
## Configure Suricata to load Suricata-Update managed rules.
##

default-rule-path: /var/lib/suricata/rules

rule-files:
  - suricata.rules
  - local.rules
##
## Auxiliary configuration files.
##

classification-file: /etc/suricata/classification.config
reference-config-file: /etc/suricata/reference.config
# threshold-file: /etc/suricata/threshold.config

##
## Include other configs
##

# Includes:  Files included here will be handled as if they were in-lined
# in this configuration file. Files with relative pathnames will be
# searched for in the same directory as this configuration file. You may
# use absolute pathnames too.
#include:
#  - include1.yaml
#  - include2.yaml
```

Add this rule:

```
alert icmp any any -> any any (msg:"ICMP Packet Detected "; sid:1000001; rev:1;)
```



```
  GNU nano 7.2                        /var/lib/suricata/rules/local.rules *
#CUSTOM RULES
alert icmp any any -> any any (msg:"ICMP PACKET DETECTED"; sid:1000001; rev:1;)
```

Save and Exit.

Run :

```
sudo suricata-update
```

This ensures suricata loads the new custom rule for detection.

Step 5: Start Suricata:

Since Suricata was installed using apt, it’s already configured as a systemd service.

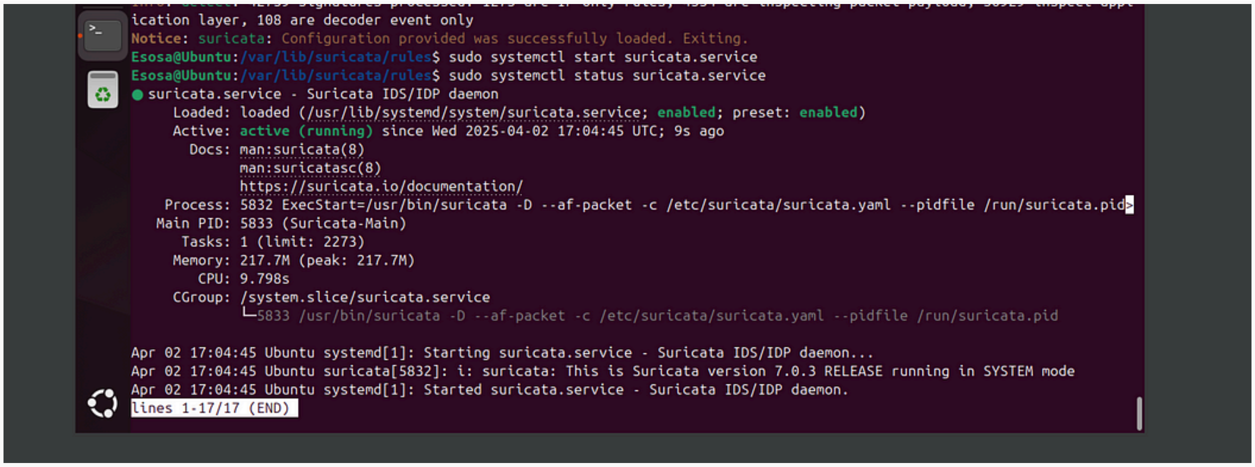
Run:

```
sudo systemctl enable suricata
```

This command makes Suricata start automatically at boot.

Confirm if it’s running :

```
sudo systemctl status suricata
```



```
ication layer, 108 are decoder event only
Notice: suricata: Configuration provided was successfully loaded. Exiting.
Esosa@Ubuntu:/var/lib/suricata/rules$ sudo systemctl start suricata.service
Esosa@Ubuntu:/var/lib/suricata/rules$ sudo systemctl status suricata.service
● suricata.service - Suricata IDS/IDP daemon
     Loaded: loaded (/usr/lib/systemd/system/suricata.service; enabled; preset: enabled)
     Active: active (running) since Wed 2025-04-02 17:04:45 UTC; 9s ago
       Docs: man:suricata(8)
             man:suricatasc(8)
             https://suricata.io/documentation/
    Process: 5832 ExecStart=/usr/bin/suricata -D --af-packet -c /etc/suricata/suricata.yaml --pidfile /run/suricata.pid>
   Main PID: 5833 (Suricata-Main)
      Tasks: 1 (limit: 2273)
     Memory: 217.7M (peak: 217.7M)
        CPU: 9.798s
     CGroup: /system.slice/suricata.service
             └─5833 /usr/bin/suricata -D --af-packet -c /etc/suricata/suricata.yaml --pidfile /run/suricata.pid

Apr 02 17:04:45 Ubuntu systemd[1]: Starting suricata.service - Suricata IDS/IDP daemon...
Apr 02 17:04:45 Ubuntu suricata[5832]: i: suricata: This is Suricata version 7.0.3 RELEASE running in SYSTEM mode
Apr 02 17:04:45 Ubuntu systemd[1]: Started suricata.service - Suricata IDS/IDP daemon.
lines 1-17/17 (END)
```

Step 6: Test with ping:

Now that Suricata is running,

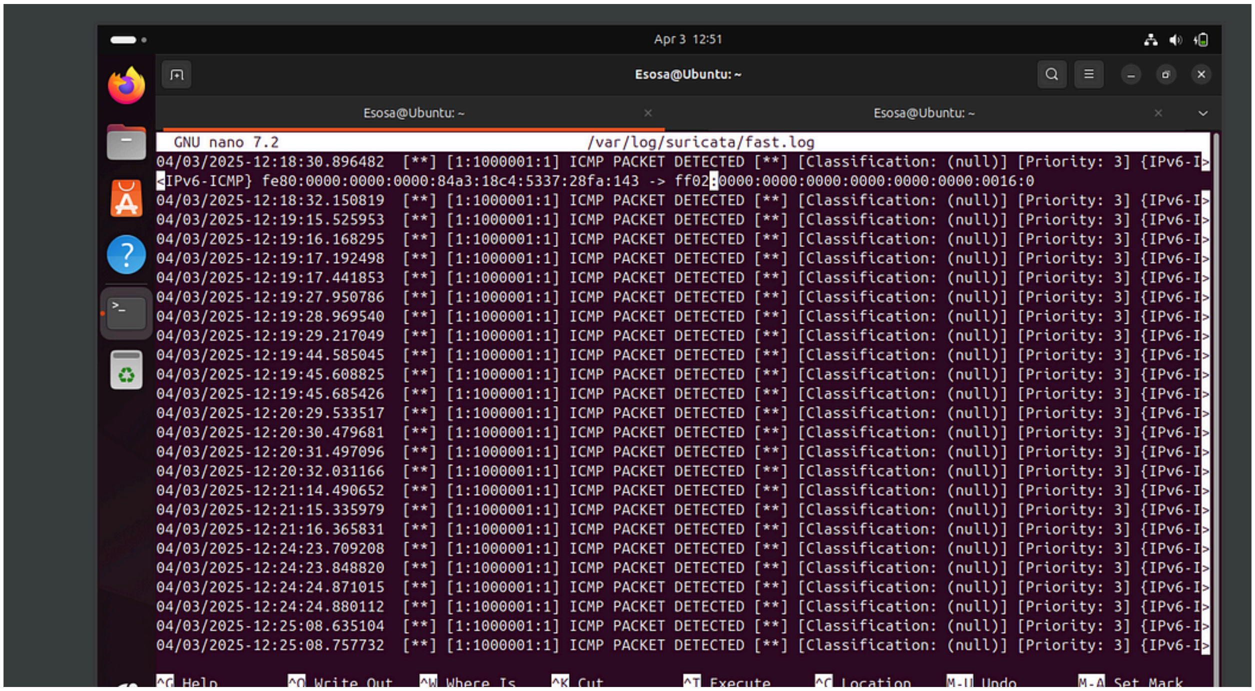
Run:

```
ping 8.8.8.8
```

Check alerts:

```
cat /var/log/suricata/fast.log
```

You should see:



```
  GNU nano 7.2                                /var/log/suricata/fast.log
04/03/2025-12:18:30.896482  [**] [1:1000001:1] ICMP PACKET DETECTED [**] [Classification: (null)] [Priority: 3] {IPv6-I>
<IPv6-ICMP} fe80:0000:0000:0000:84a3:18c4:5337:28fa:143 -> ff02:0000:0000:0000:0000:0000:0000:0016:0
04/03/2025-12:18:32.150819  [**] [1:1000001:1] ICMP PACKET DETECTED [**] [Classification: (null)] [Priority: 3] {IPv6-I>
04/03/2025-12:19:15.525953  [**] [1:1000001:1] ICMP PACKET DETECTED [**] [Classification: (null)] [Priority: 3] {IPv6-I>
04/03/2025-12:19:16.168295  [**] [1:1000001:1] ICMP PACKET DETECTED [**] [Classification: (null)] [Priority: 3] {IPv6-I>
04/03/2025-12:19:17.192498  [**] [1:1000001:1] ICMP PACKET DETECTED [**] [Classification: (null)] [Priority: 3] {IPv6-I>
04/03/2025-12:19:17.441853  [**] [1:1000001:1] ICMP PACKET DETECTED [**] [Classification: (null)] [Priority: 3] {IPv6-I>
04/03/2025-12:19:27.950786  [**] [1:1000001:1] ICMP PACKET DETECTED [**] [Classification: (null)] [Priority: 3] {IPv6-I>
04/03/2025-12:19:28.969540  [**] [1:1000001:1] ICMP PACKET DETECTED [**] [Classification: (null)] [Priority: 3] {IPv6-I>
04/03/2025-12:19:29.217049  [**] [1:1000001:1] ICMP PACKET DETECTED [**] [Classification: (null)] [Priority: 3] {IPv6-I>
04/03/2025-12:19:44.585045  [**] [1:1000001:1] ICMP PACKET DETECTED [**] [Classification: (null)] [Priority: 3] {IPv6-I>
04/03/2025-12:19:45.608825  [**] [1:1000001:1] ICMP PACKET DETECTED [**] [Classification: (null)] [Priority: 3] {IPv6-I>
04/03/2025-12:19:45.685426  [**] [1:1000001:1] ICMP PACKET DETECTED [**] [Classification: (null)] [Priority: 3] {IPv6-I>
04/03/2025-12:20:29.533517  [**] [1:1000001:1] ICMP PACKET DETECTED [**] [Classification: (null)] [Priority: 3] {IPv6-I>
04/03/2025-12:20:30.479681  [**] [1:1000001:1] ICMP PACKET DETECTED [**] [Classification: (null)] [Priority: 3] {IPv6-I>
04/03/2025-12:20:31.497096  [**] [1:1000001:1] ICMP PACKET DETECTED [**] [Classification: (null)] [Priority: 3] {IPv6-I>
04/03/2025-12:20:32.031166  [**] [1:1000001:1] ICMP PACKET DETECTED [**] [Classification: (null)] [Priority: 3] {IPv6-I>
04/03/2025-12:21:14.490652  [**] [1:1000001:1] ICMP PACKET DETECTED [**] [Classification: (null)] [Priority: 3] {IPv6-I>
04/03/2025-12:21:15.335979  [**] [1:1000001:1] ICMP PACKET DETECTED [**] [Classification: (null)] [Priority: 3] {IPv6-I>
04/03/2025-12:21:16.365831  [**] [1:1000001:1] ICMP PACKET DETECTED [**] [Classification: (null)] [Priority: 3] {IPv6-I>
04/03/2025-12:24:23.709208  [**] [1:1000001:1] ICMP PACKET DETECTED [**] [Classification: (null)] [Priority: 3] {IPv6-I>
04/03/2025-12:24:23.848820  [**] [1:1000001:1] ICMP PACKET DETECTED [**] [Classification: (null)] [Priority: 3] {IPv6-I>
04/03/2025-12:24:24.871015  [**] [1:1000001:1] ICMP PACKET DETECTED [**] [Classification: (null)] [Priority: 3] {IPv6-I>
04/03/2025-12:24:24.880112  [**] [1:1000001:1] ICMP PACKET DETECTED [**] [Classification: (null)] [Priority: 3] {IPv6-I>
04/03/2025-12:25:08.635104  [**] [1:1000001:1] ICMP PACKET DETECTED [**] [Classification: (null)] [Priority: 3] {IPv6-I>
04/03/2025-12:25:08.757732  [**] [1:1000001:1] ICMP PACKET DETECTED [**] [Classification: (null)] [Priority: 3] {IPv6-I>

^G Help        ^O Write Out   ^W Where Is    ^K Cut         ^T Execute     ^C Location    M-U Undo       M-A Set Mark
```

Congratulations! Suricata is working.

CONCLUSION

In this project, I demonstrated how to install, configure, and create custom rules for two powerful network intrusion detection systems: Snort and Suricata. By building and testing simple ICMP (ping) detection rules, I was able to simulate real-world packet monitoring scenarios and validate that both systems were functioning correctly. This hands-on exercise helped show important skills, including:

- Writing and implementing custom detection rules.
- Monitoring and analyzing network traffic.
- Understanding how IDS tools integrate into security operations.

This project lays a solid foundation for more advanced intrusion detection concepts, such as detecting TCP scans, malware communications, and building complex detection rules for real-world SOC environments.