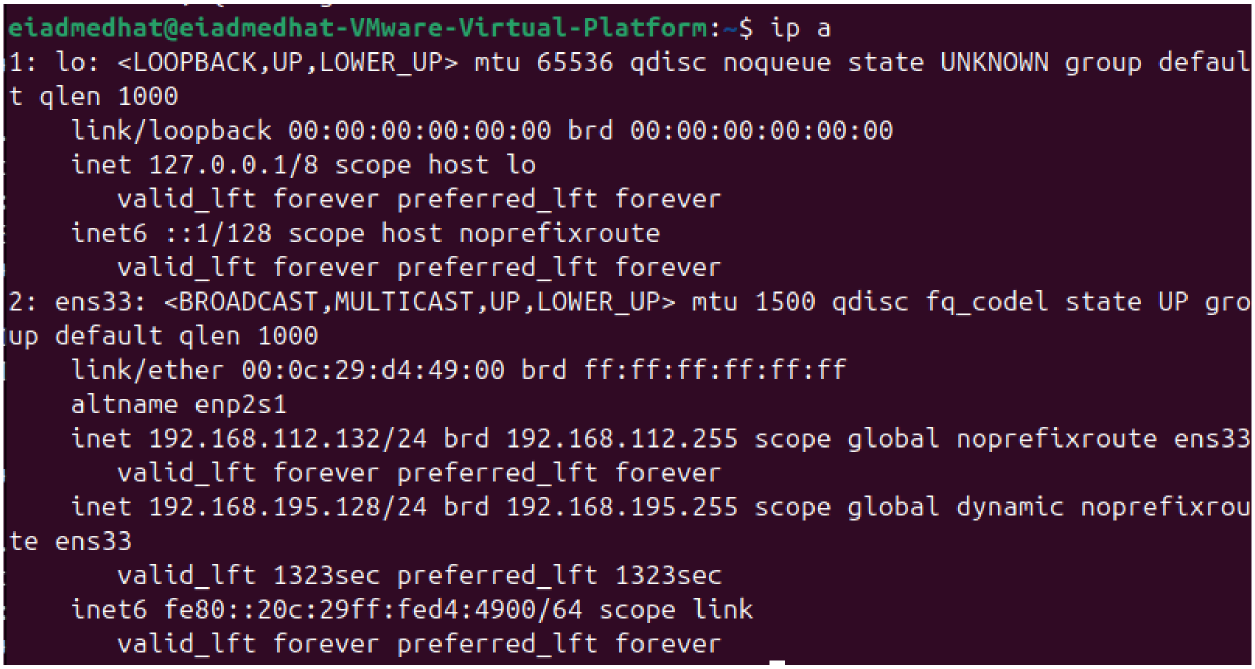
Step 1: Set Up the Environment

Objective: Prepare Ubuntu VM for Snort testing.

Commands:

- ip a
- ping 192.168.112.132



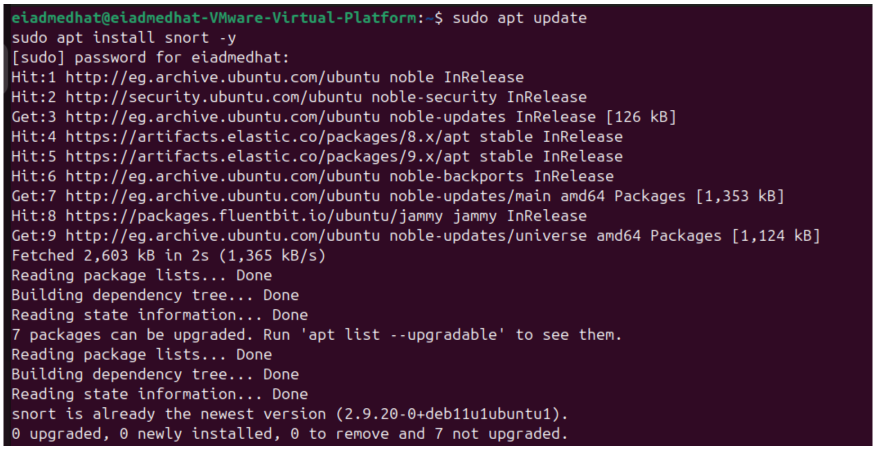
```
eiadmedhat@eiadmedhat-VMware-Virtual-Platform:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::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 gro
up default qlen 1000
    link/ether 00:0c:29:d4:49:00 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.112.132/24 brd 192.168.112.255 scope global noprefixroute ens33
       valid_lft forever preferred_lft forever
    inet 192.168.195.128/24 brd 192.168.195.255 scope global dynamic noprefixrou
te ens33
       valid_lft 1323sec preferred_lft 1323sec
    inet6 fe80::20c:29ff:fed4:4900/64 scope link
       valid_lft forever preferred_lft forever
```

Step 2: Install Snort

Objective: Ensure Snort is installed.

Commands:

- sudo apt update
- sudo apt install snort -y



```
eiadmedhat@eiadmedhat-VMware-Virtual-Platform:~$ sudo apt update
sudo apt install snort -y
[sudo] password for eiadmedhat:
Hit:1 http://eg.archive.ubuntu.com/ubuntu noble InRelease
Hit:2 http://security.ubuntu.com/ubuntu noble-security InRelease
Get:3 http://eg.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Hit:4 https://artifacts.elastic.co/packages/8.x/apt stable InRelease
Hit:5 https://artifacts.elastic.co/packages/9.x/apt stable InRelease
Hit:6 http://eg.archive.ubuntu.com/ubuntu noble-backports InRelease
Get:7 http://eg.archive.ubuntu.com/ubuntu noble-updates/main amd64 Packages [1,353 kB]
Hit:8 https://packages.fluentbit.io/ubuntu/jammy jammy InRelease
Get:9 http://eg.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Packages [1,124 kB]
Fetched 2,603 kB in 2s (1,365 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
7 packages can be upgraded. Run 'apt list --upgradable' to see them.
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 7 not upgraded.
```

Step 3: Configure Snort Variables

Objective: Set local network and rule paths.

File: /etc/snort/snort.conf

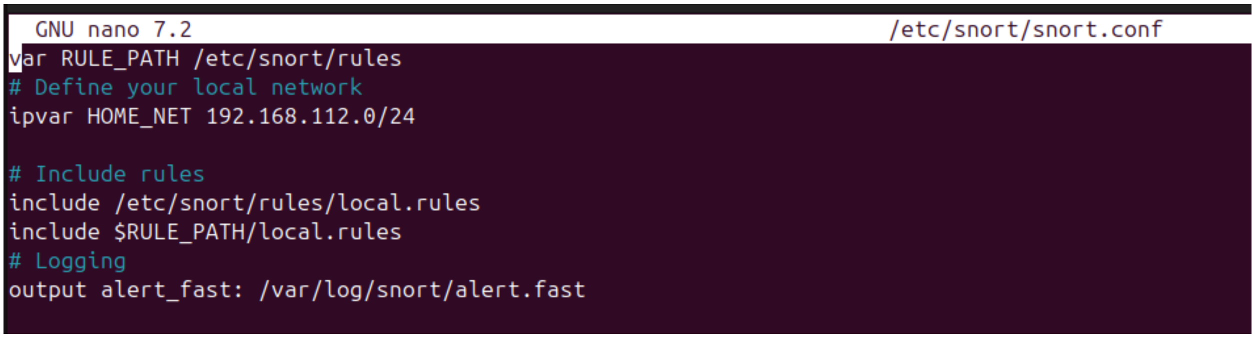
Content:

var RULE_PATH /etc/snort/rules

ipvar HOME_NET 192.168.112.0/24

include /etc/snort/rules/local.rules

output alert_fast: /var/log/snort/alert.fast



```
  GNU nano 7.2                                                          /etc/snort/snort.conf
var RULE_PATH /etc/snort/rules
# Define your local network
ipvar HOME_NET 192.168.112.0/24

# Include rules
include /etc/snort/rules/local.rules
include $RULE_PATH/local.rules
# Logging
output alert_fast: /var/log/snort/alert.fast
```

Step 4: Create Local Rules

Objective: Detect .exe downloads and ICMP pings.

File: /etc/snort/rules/local.rules

Content:

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

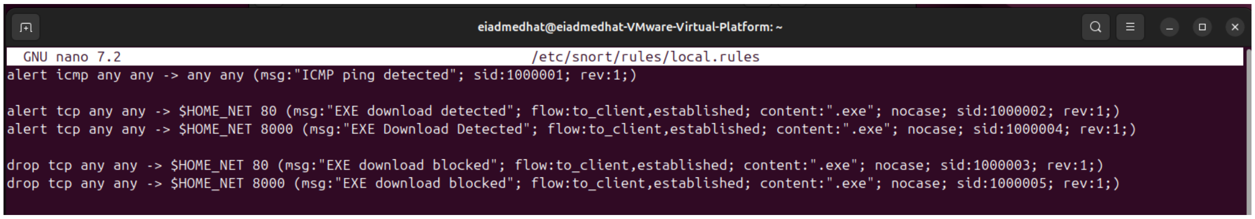
alert tcp any any -> $HOME_NET 80 (msg:"EXE download detected"; flow:to_client,established; content:".exe"; nocase; sid:1000002; rev:1;)

alert tcp any any -> $HOME_NET 8000 (msg:"EXE Download Detected"; flow:to_client,established; content:".exe"; nocase; sid:1000004; rev:1;)

alert tcp any any -> $HOME_NET any (msg:"EXE Download Detected"; content:".exe"; nocase; sid:1000010; rev:1;)

drop tcp any any -> $HOME_NET 80 (msg:"EXE download blocked"; flow:to_client,established; content:".exe"; nocase; sid:1000003; rev:1;)

drop tcp any any -> $HOME_NET 8000 (msg:"EXE download blocked"; flow:to_client,established; content:".exe"; nocase; sid:1000005; rev:1;)



```
eiadmedhat@eiadmedhat-VMware-Virtual-Platform: ~
  GNU nano 7.2                                   /etc/snort/rules/local.rules
alert icmp any any -> any any (msg:"ICMP ping detected"; sid:1000001; rev:1;)

alert tcp any any -> $HOME_NET 80 (msg:"EXE download detected"; flow:to_client,established; content:".exe"; nocase; sid:1000002; rev:1;)
alert tcp any any -> $HOME_NET 8000 (msg:"EXE Download Detected"; flow:to_client,established; content:".exe"; nocase; sid:1000004; rev:1;)

drop tcp any any -> $HOME_NET 80 (msg:"EXE download blocked"; flow:to_client,established; content:".exe"; nocase; sid:1000003; rev:1;)
drop tcp any any -> $HOME_NET 8000 (msg:"EXE download blocked"; flow:to_client,established; content:".exe"; nocase; sid:1000005; rev:1;)
```

Step 5: Test Snort Rules in IDS Mode

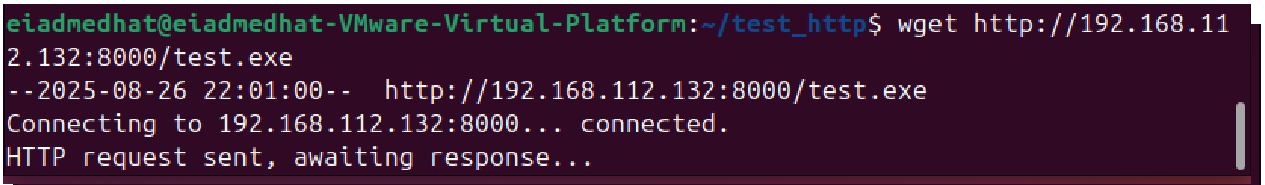
Objective: Verify Snort can detect .exe downloads.

Commands:

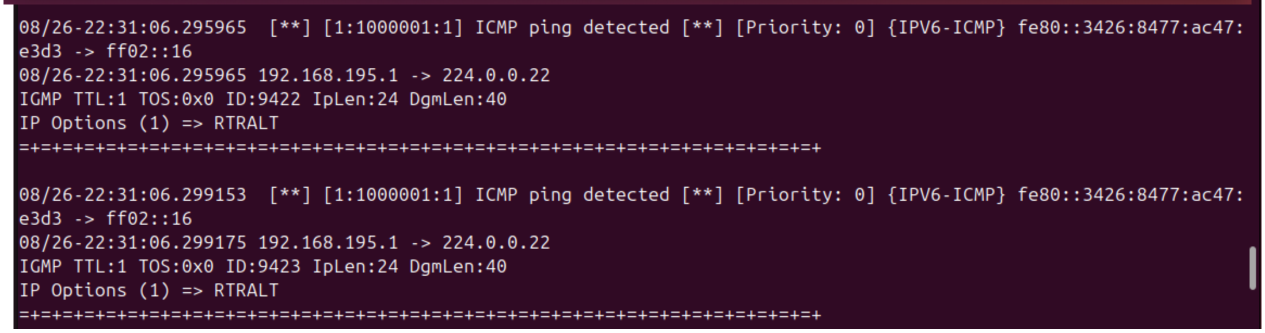
sudo snort -A console -q -c /etc/snort/snort.conf -i ens33 -K ascii -v

Test download:

wget http://192.168.112.132:8000/test.exe



```
eiadmedhat@eiadmedhat-VMware-Virtual-Platform:~/test_http$ wget http://192.168.11
2.132:8000/test.exe
--2025-08-26 22:01:00--  http://192.168.112.132:8000/test.exe
Connecting to 192.168.112.132:8000... connected.
HTTP request sent, awaiting response...
```



```
08/26-22:31:06.295965  [**] [1:1000001:1] ICMP ping detected [**] [Priority: 0] {IPV6-ICMP} fe80::3426:8477:ac47:
e3d3 -> ff02::16
08/26-22:31:06.295965 192.168.195.1 -> 224.0.0.22
IGMP TTL:1 TOS:0x0 ID:9422 IpLen:24 DgmLen:40
IP Options (1) => RTRALT
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

08/26-22:31:06.299153  [**] [1:1000001:1] ICMP ping detected [**] [Priority: 0] {IPV6-ICMP} fe80::3426:8477:ac47:
e3d3 -> ff02::16
08/26-22:31:06.299175 192.168.195.1 -> 224.0.0.22
IGMP TTL:1 TOS:0x0 ID:9423 IpLen:24 DgmLen:40
IP Options (1) => RTRALT
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

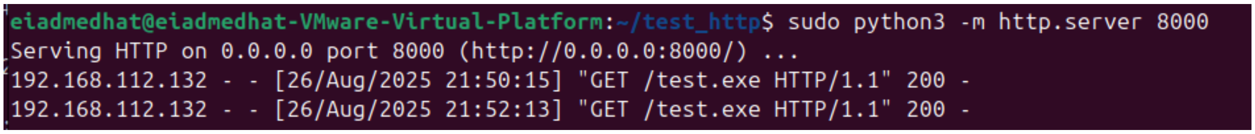
Step 6: Set Up a Python HTTP Server

Objective: Serve .exe files for testing.

Commands:

sudo python3 -m http.server 8000

touch test.exe



```
eiadmedhat@eiadmedhat-VMware-Virtual-Platform:~/test_http$ sudo python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
192.168.112.132 - - [26/Aug/2025 21:50:15] "GET /test.exe HTTP/1.1" 200 -
192.168.112.132 - - [26/Aug/2025 21:52:13] "GET /test.exe HTTP/1.1" 200 -
```

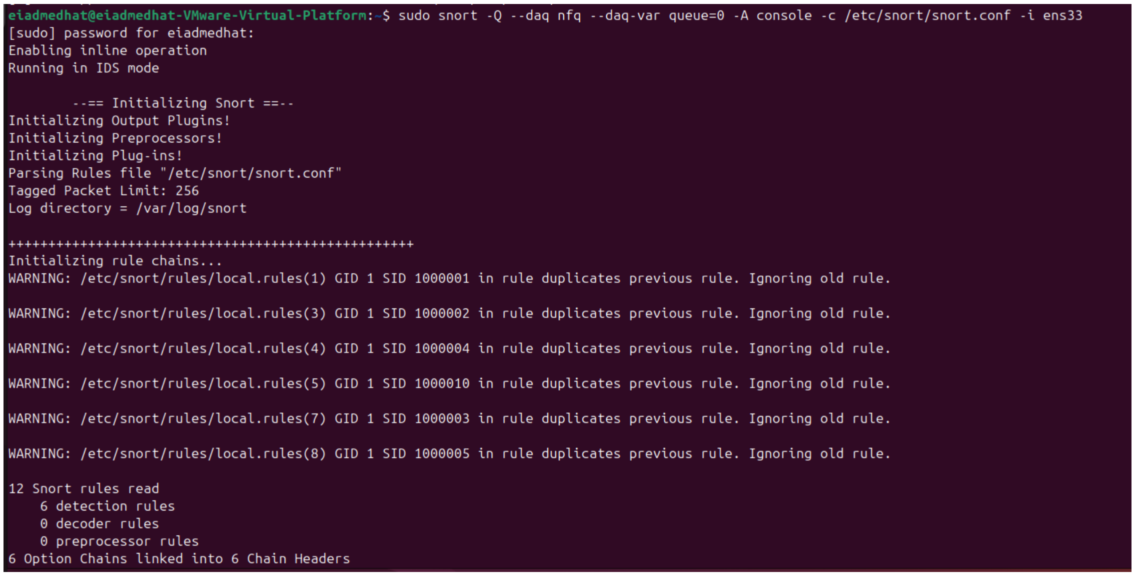
Step 7: Run Snort in IPS Mode (Block .exe)

Objective: Enable Snort to drop/block .exe downloads.

Commands:

sudo snort -Q --daq nfq --daq-var queue=0 -A console -c /etc/snort/snort.conf -i ens33

Test download: wget http://192.168.112.132:8000/test.exe

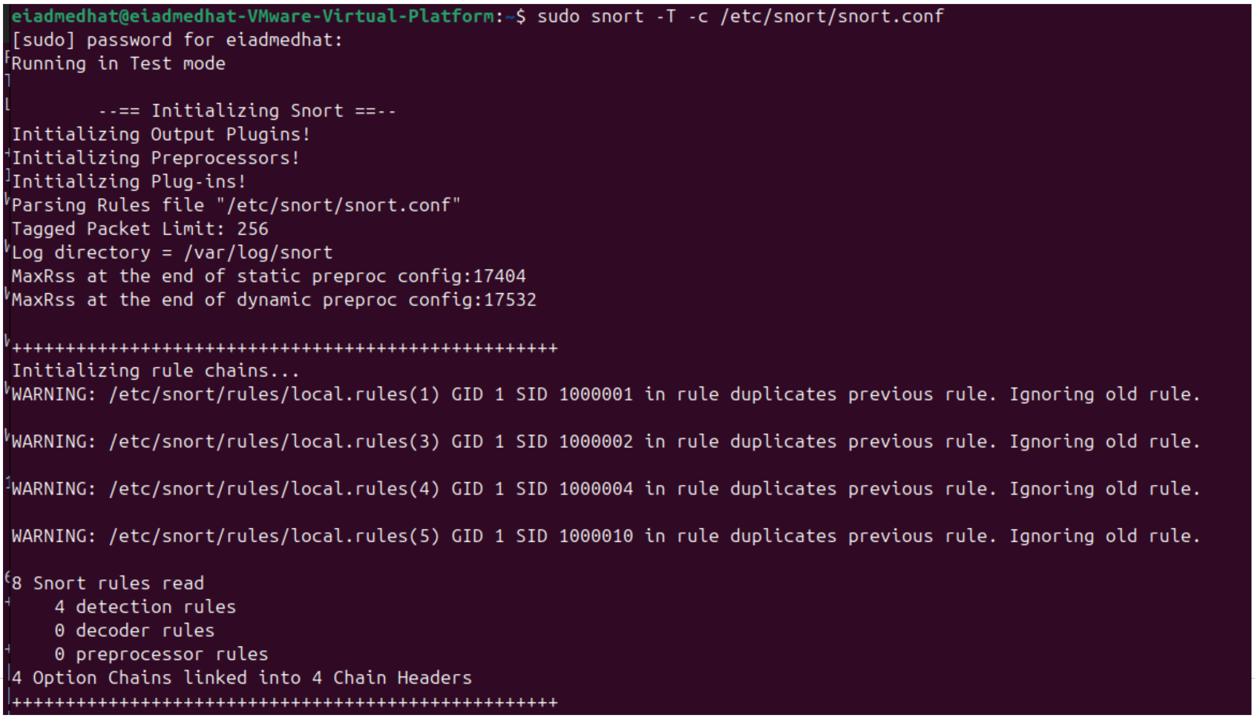


```
eiadmedhat@eiadmedhat-VMware-Virtual-Platform:~$ sudo snort -Q --daq nfq --daq-var queue=0 -A console -c /etc/snort/snort.conf -i ens33
[sudo] password for eiadmedhat:
Enabling inline operation
Running in IDS mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "/etc/snort/snort.conf"
Tagged Packet Limit: 256
Log directory = /var/log/snort

+++++++++++++++++++++++++++++++++++++++++++++++++++
Initializing rule chains...
WARNING: /etc/snort/rules/local.rules(1) GID 1 SID 1000001 in rule duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/local.rules(3) GID 1 SID 1000002 in rule duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/local.rules(4) GID 1 SID 1000004 in rule duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/local.rules(5) GID 1 SID 1000010 in rule duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/local.rules(7) GID 1 SID 1000003 in rule duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/local.rules(8) GID 1 SID 1000005 in rule duplicates previous rule. Ignoring old rule.

12 Snort rules read
    6 detection rules
    0 decoder rules
    0 preprocessor rules
6 Option Chains linked into 6 Chain Headers
```

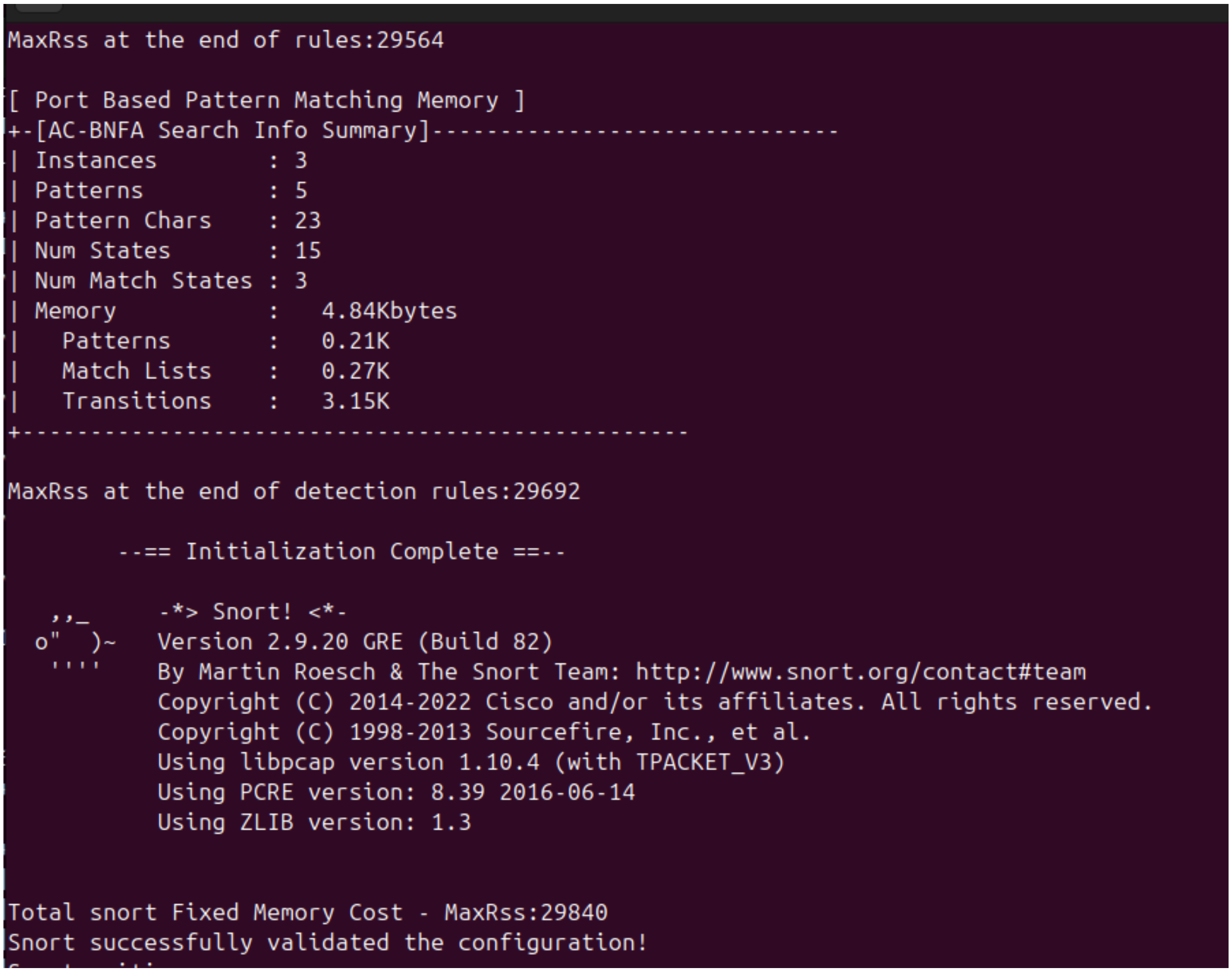
Step 8: Validate Configuration

Commands:

sudo snort -T -c /etc/snort/snort.conf



```
eiadmedhat@eiadmedhat-VMware-Virtual-Platform:~$ sudo snort -T -c /etc/snort/snort.conf
[sudo] password for eiadmedhat:
Running in Test mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "/etc/snort/snort.conf"
Tagged Packet Limit: 256
Log directory = /var/log/snort
MaxRss at the end of static preproc config:17404
MaxRss at the end of dynamic preproc config:17532

+++++++++++++++++++++++++++++++++++++++++++++++++++
Initializing rule chains...
WARNING: /etc/snort/rules/local.rules(1) GID 1 SID 1000001 in rule duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/local.rules(3) GID 1 SID 1000002 in rule duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/local.rules(4) GID 1 SID 1000004 in rule duplicates previous rule. Ignoring old rule.

WARNING: /etc/snort/rules/local.rules(5) GID 1 SID 1000010 in rule duplicates previous rule. Ignoring old rule.

8 Snort rules read
    4 detection rules
    0 decoder rules
    0 preprocessor rules
4 Option Chains linked into 4 Chain Headers
+++++++++++++++++++++++++++++++++++++++++++++++++++
```



```
MaxRss at the end of rules:29564

[ Port Based Pattern Matching Memory ]
+-[AC-BNFA Search Info Summary]------------------------------
| Instances        : 3
| Patterns         : 5
| Pattern Chars    : 23
| Num States       : 15
| Num Match States : 3
| Memory           :   4.84Kbytes
|   Patterns       :   0.21K
|   Match Lists    :   0.27K
|   Transitions    :   3.15K
+-------------------------------------------------

MaxRss at the end of detection rules:29692

        --== 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


Total snort Fixed Memory Cost - MaxRss:29840
Snort successfully validated the configuration!
```