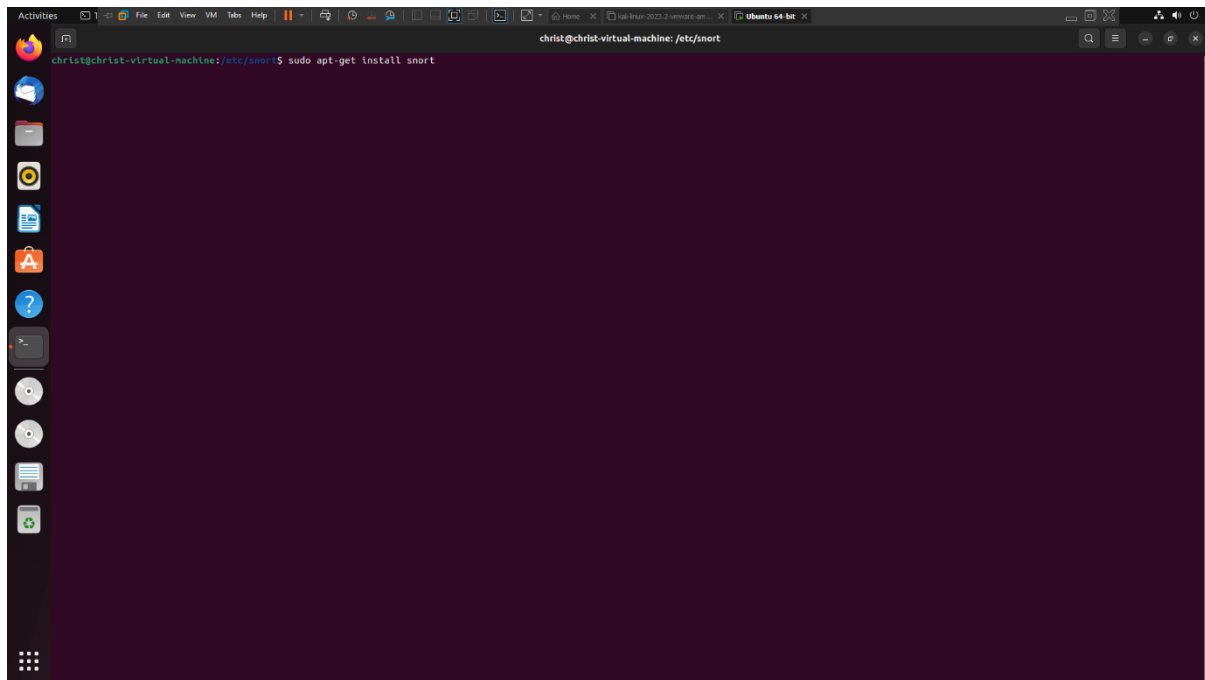


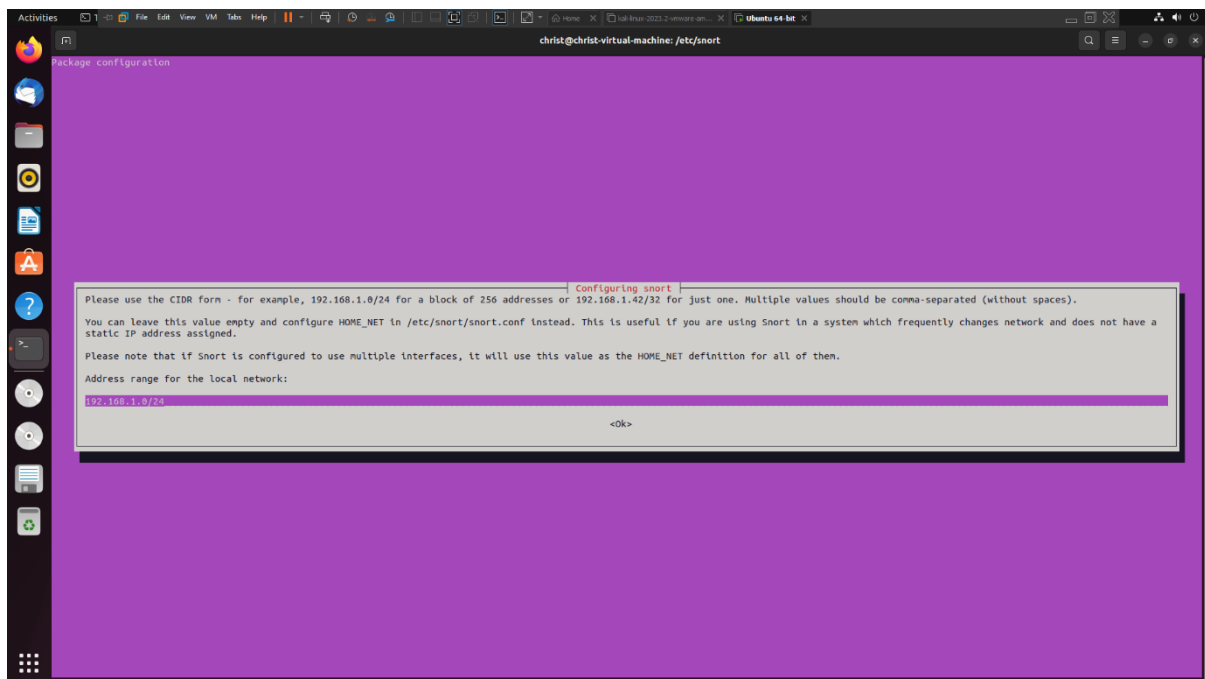
# SNORT DOCUMENTATION

Step 1: Install SNORT in your ubuntu

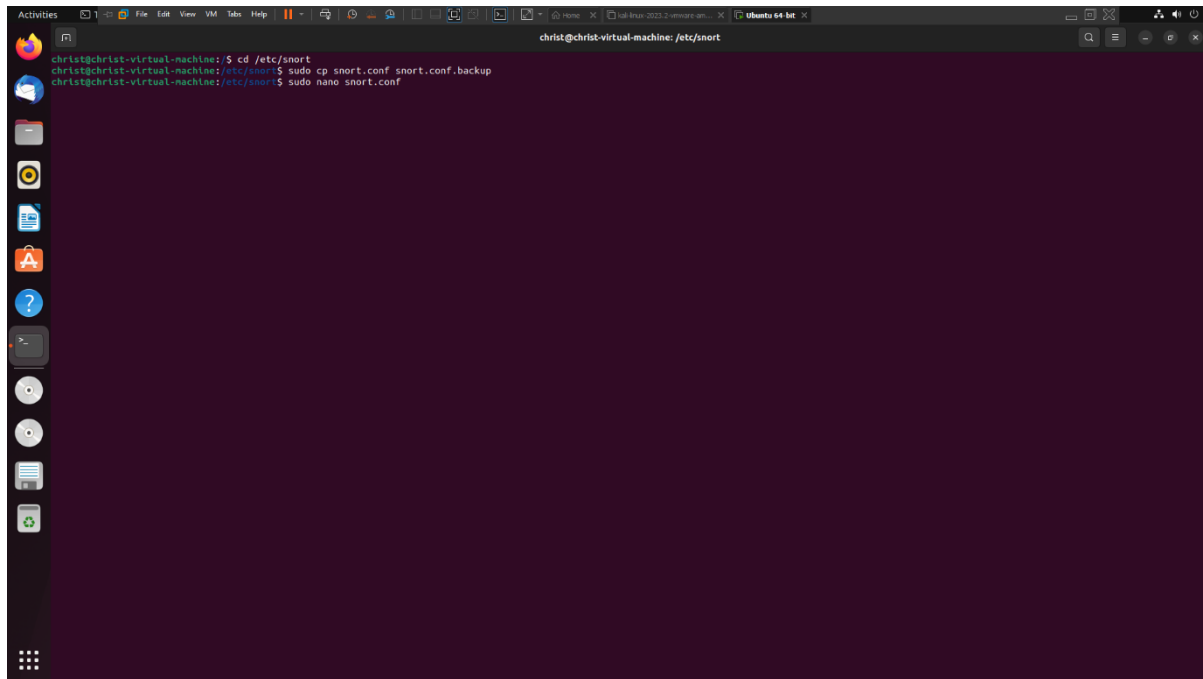


Step 2: Put the ip as I entered bellow

192.168.1.0/24

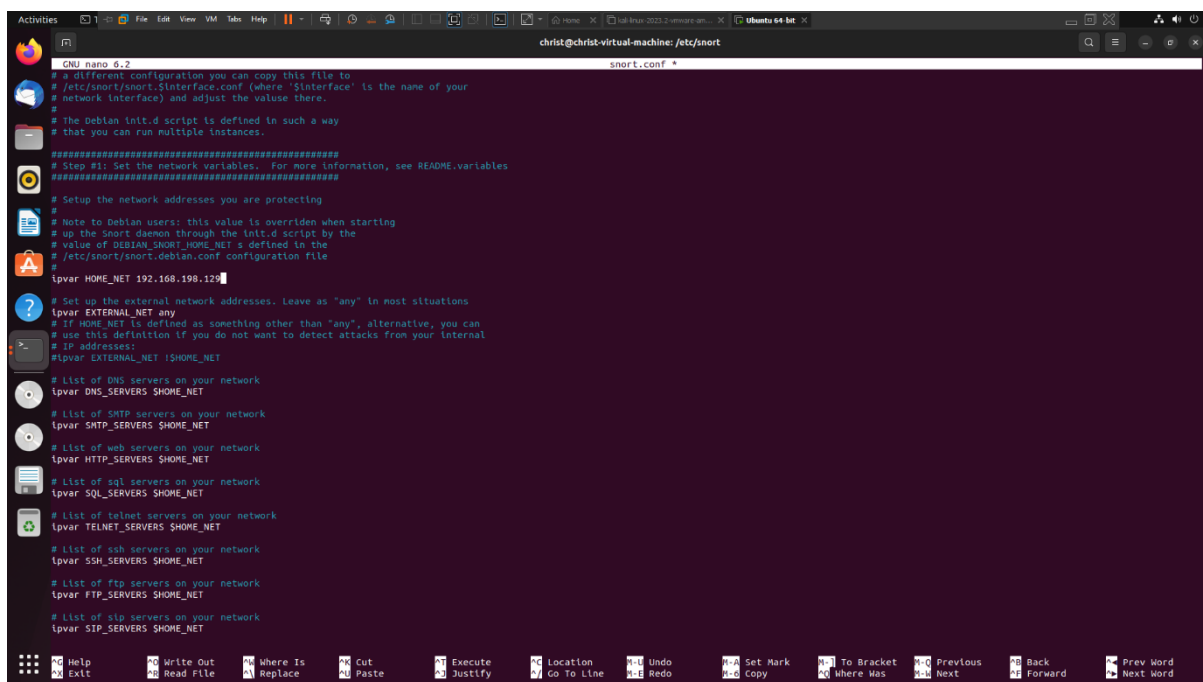


Step 3: Go to /etc/snort and cp the conf file and its backup file and open the snort.conf file using “sudo nano snort.conf”



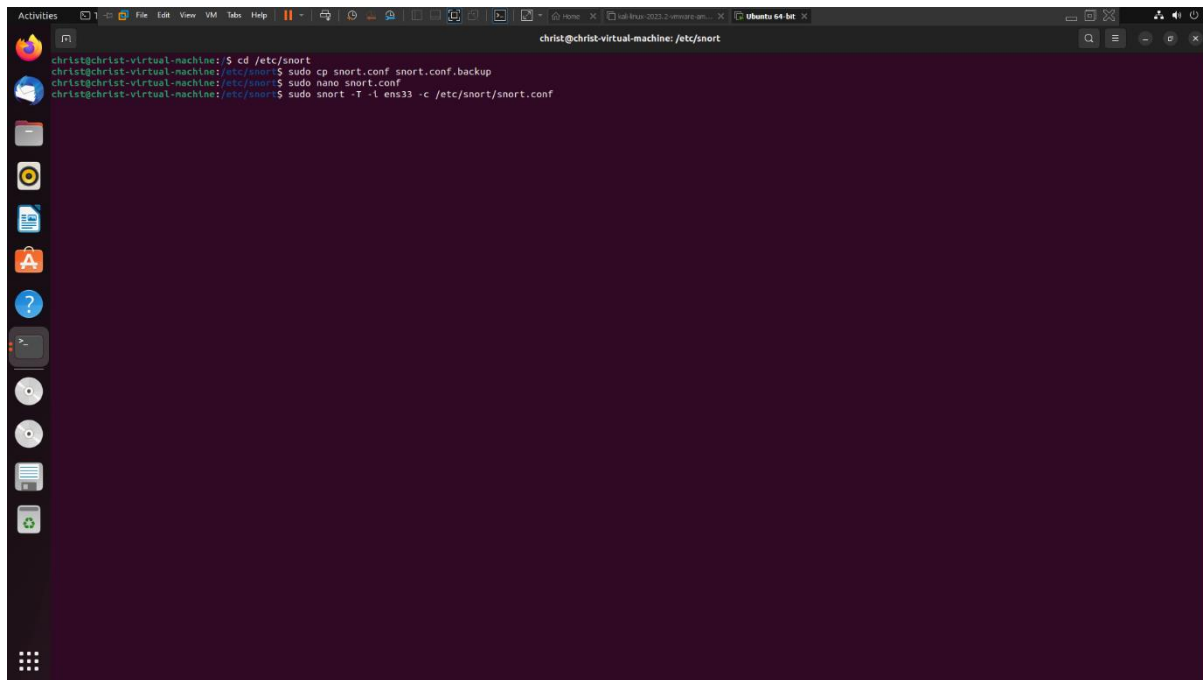
```
christ@christ-virtual-machine: /etc/snort
christ@christ-virtual-machine: /etc/snort$ cd /etc/snort
christ@christ-virtual-machine: /etc/snort$ sudo cp snort.conf snort.conf.backup
christ@christ-virtual-machine: /etc/snort$ sudo nano snort.conf
```

Step 4: After opening change the HOME\_NET ip as Ubuntu ip



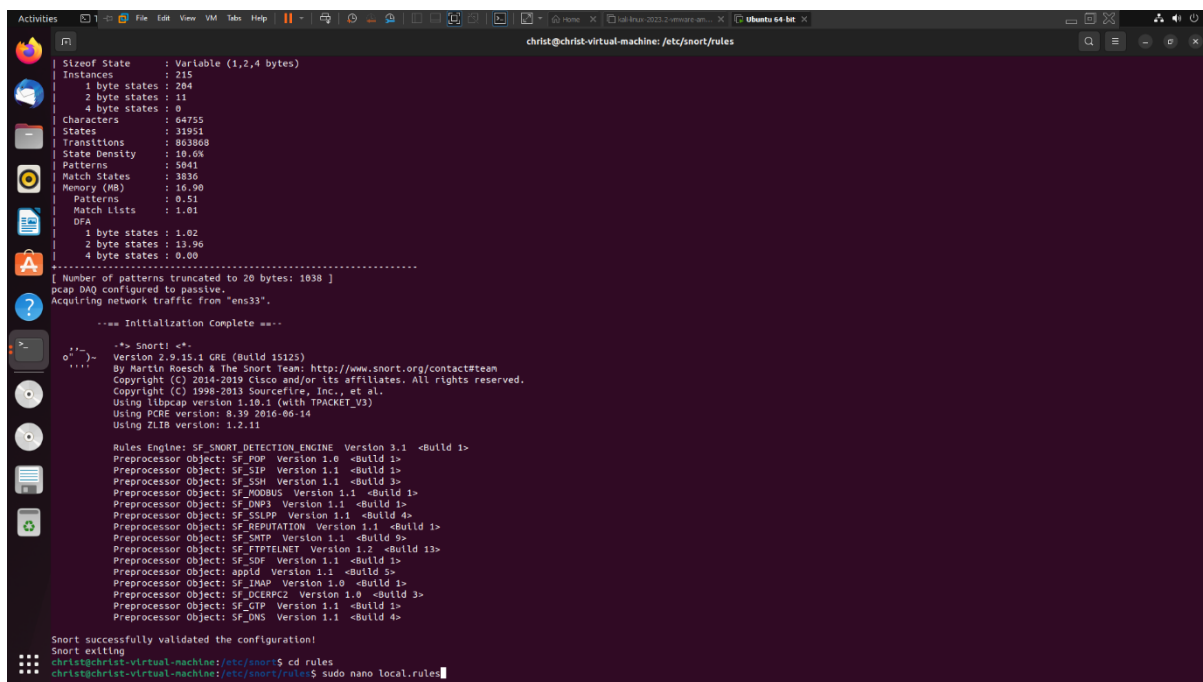
```
GNU nano 2.9.3 snort.conf
# a different configuration you can copy this file to
# /etc/snort/snort.Sinterface.conf (where 'Sinterface' is the name of your
# network interface) and adjust the value there.
#
# The Debian init.d script is defined in such a way
# that you can run multiple instances.
#####
# 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 overridden when starting
# up the Snort daemon through the init.d script by the
# value of DEBIAN_SNORT_HOME_NET defined in the
# /etc/snort/snort.debian.conf configuration file
#
ipvar HOME_NET 192.168.129
# 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 INTERNAL_NET !$HOME_NET
# List of DNS servers on your network
ipvar DNS_SERVERS $HOME_NET
# List of SMTP servers on your network
ipvar SMTP_SERVERS $HOME_NET
# List of web servers on your network
ipvar HTTP_SERVERS $HOME_NET
# List of sql servers on your network
ipvar SQL_SERVERS $HOME_NET
# List of telnet servers on your network
ipvar TELNET_SERVERS $HOME_NET
# List of ssh servers on your network
ipvar SSH_SERVERS $HOME_NET
# List of ftp servers on your network
ipvar FTP_SERVERS $HOME_NET
# List of sip servers on your network
ipvar SIP_SERVERS $HOME_NET
```

Step 5: Update the changes by this command “sudo nano -T -i <interface> -c snort.conf”.



```
christ@christ-virtual-machine: /etc/snort
christ@christ-virtual-machine: /etc/snort$ cd /etc/snort
christ@christ-virtual-machine: /etc/snort$ sudo cp snort.conf snort.conf.backup
christ@christ-virtual-machine: /etc/snort$ sudo nano snort.conf
christ@christ-virtual-machine: /etc/snort$ sudo snort -T -i ens33 -c /etc/snort/snort.conf
```

Step 6: Open the Local rules file by following “cd rules” “sudo nano local.rules”.



```
christ@christ-virtual-machine: /etc/snort/rules

Sizeof State      : Variable (1,2,4 bytes)
Instances         : 215
  1 byte states   : 204
  2 byte states   : 11
  4 byte states   : 0
Characters        : 64755
States           : 31951
Transitions       : 863868
State Density     : 10.0%
Patterns         : 5841
Match States     : 3836
Memory (MB)      : 16.90
  Patterns       : 0.51
  Match Lists    : 1.01
DFA
  1 byte states : 1.02
  2 byte states : 13.96
  4 byte states : 0.00
-----
[ Number of patterns truncated to 20 bytes: 1038 ]
pcap DAQ configured to passive.
Acquiring network traffic from "ens33".

--== Initialization Complete ==--

--* Snort! *--
Version 2.9.15.1 GRE (Build 15125)
By Martin Roesch & the Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.10.1 (with TPACKET_V3)
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.2.11

Rules Engine: SF_SNORT_DETECTION_ENGINE Version 3.1 <Build 1>
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
Preprocessor Object: SF_SOF Version 1.1 <Build 1>
Preprocessor Object: apdip Version 1.1 <Build 5>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>
Preprocessor Object: SF_CIP Version 1.1 <Build 1>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>

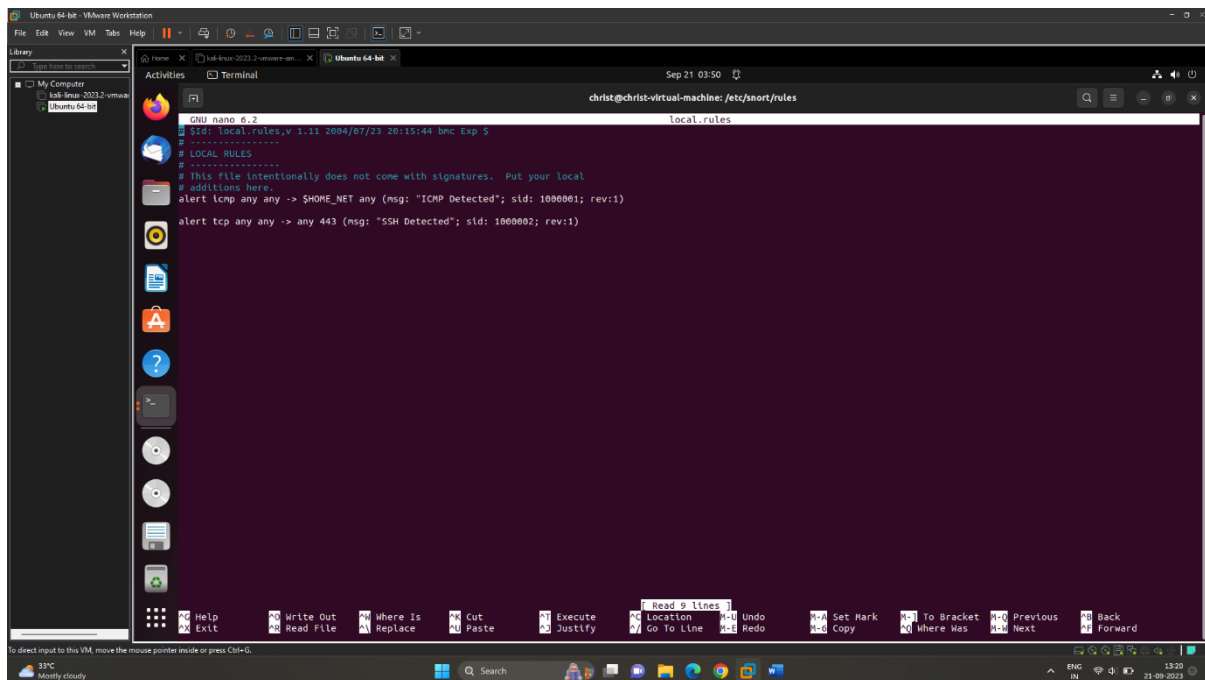
Snort successfully validated the configuration!
Snort exiting
christ@christ-virtual-machine: /etc/snort$ cd rules
christ@christ-virtual-machine: /etc/snort/rules$ sudo nano local.rules
```

Step 7: Add the given 2 rules

alert icmp any any -> \$HOME\_NET any (msg: "ICMP Detected"; sid: 1000001; rev:1)

alert tcp any any -> any 443 (msg: "SSH Detected"; sid: 1000002; rev:1)

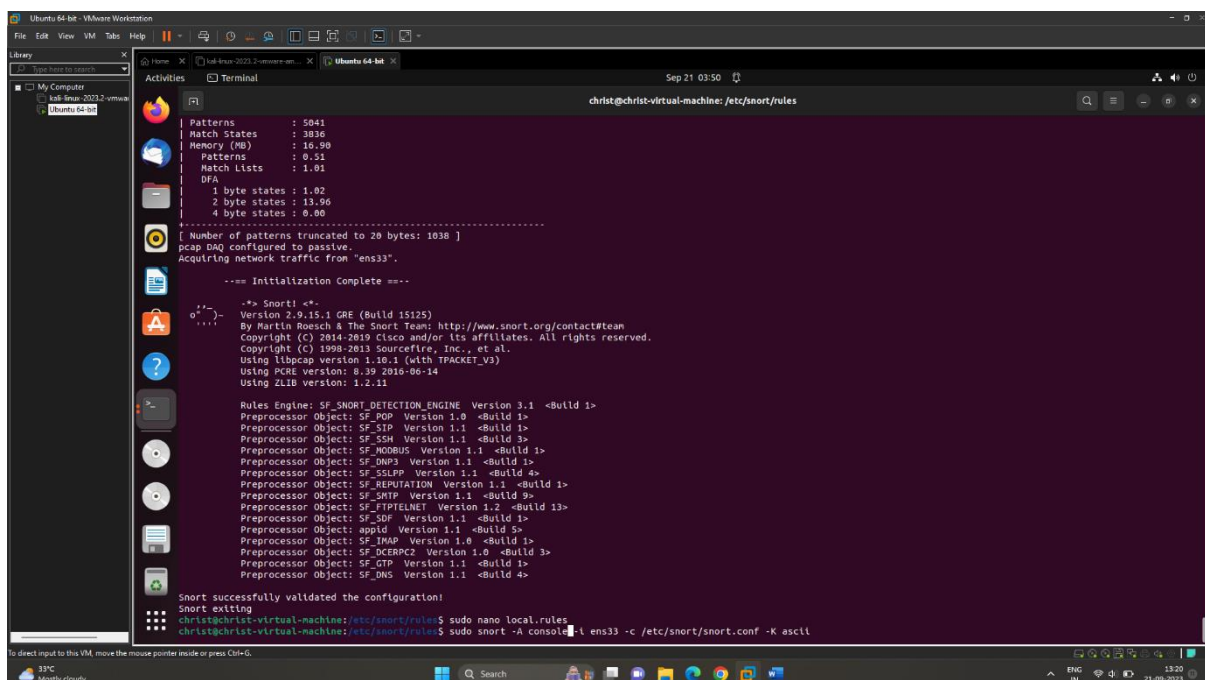
CTRL+X and Type YES and HIT ENTER to save



```
christ@christ-virtual-machine: /etc/snort/rules
GNU nano 6.2 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 -> $HOME_NET any (msg: "ICMP Detected"; sid: 1000001; rev:1)
alert tcp any any -> any 443 (msg: "SSH Detected"; sid: 1000002; rev:1)
```

Step 8: Run the bellow command to capture the traffic

sudo snort -A console -i ens33 -c snort.conf -K ascii



```
Patterns : 5041
Match States : 3836
Memory (MB) : 10.90
Patterns : 0.53
Match Lists : 1.01
DFA :
1 byte states : 1.02
2 byte states : 13.96
4 byte states : 0.00
-----
[ Number of patterns truncated to 20 bytes: 1038 ]
pcap DAQ configured to passive.
Acquiring network traffic from "ens33".

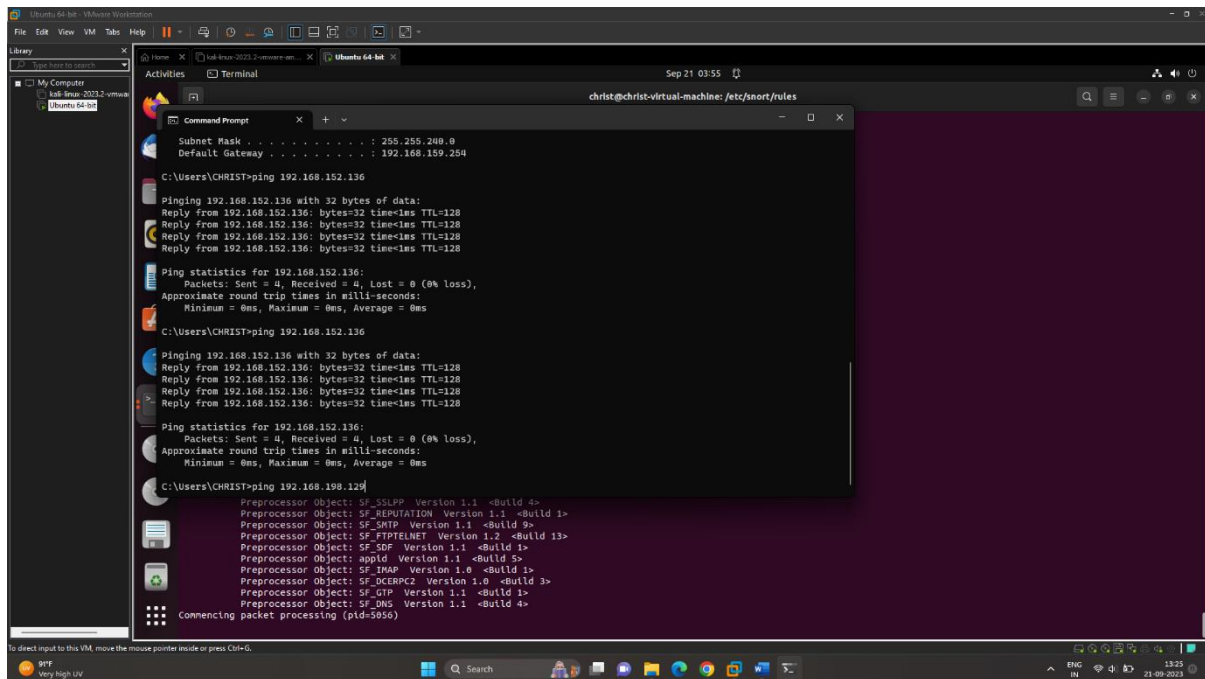
--- Initialization Complete ---

** Snort! **
Version 2.9.15.1 CRE (Build 15125)
By Martin Roesch & The Snort Team: http://www.snort.org/contact/team
Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.10.1 (with TPACKET_V3)
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.2.11

Rules Engine: SF_SNORT_DETECTION_ENGINE Version 3.1 <Build 1>
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Preprocessor Object: SF_MQDBUS Version 1.1 <Build 1>
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
Preprocessor Object: SF_FIPIELNET Version 1.2 <Build 13>
Preprocessor Object: SF_SDF Version 1.1 <Build 1>
Preprocessor Object: appid Version 1.1 <Build 5>
Preprocessor Object: SF_TMAP Version 1.0 <Build 1>
Preprocessor Object: SF_DCEPC2 Version 1.0 <Build 3>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>

Snort successfully validated the configuration!
Snort exiting
christ@christ-virtual-machine: /etc/snort/rules$ sudo nano local.rules
christ@christ-virtual-machine: /etc/snort/rules$ sudo snort -A console -i ens33 -c /etc/snort/snort.conf -K ascii
```

Step 9: Go to cmd in win and ping your ubuntu ip address



```
Subnet Mask . . . . . : 255.255.240.0
Default Gateway . . . . . : 192.168.159.254

C:\Users\CHRIST>ping 192.168.152.136

Pinging 192.168.152.136 with 32 bytes of data:
Reply from 192.168.152.136: bytes=32 time<1ms TTL=128
Reply from 192.168.152.136: bytes=32 time<1ms TTL=128
Reply from 192.168.152.136: bytes=32 time<1ms TTL=128
Reply from 192.168.152.136: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.152.136:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\CHRIST>ping 192.168.152.136

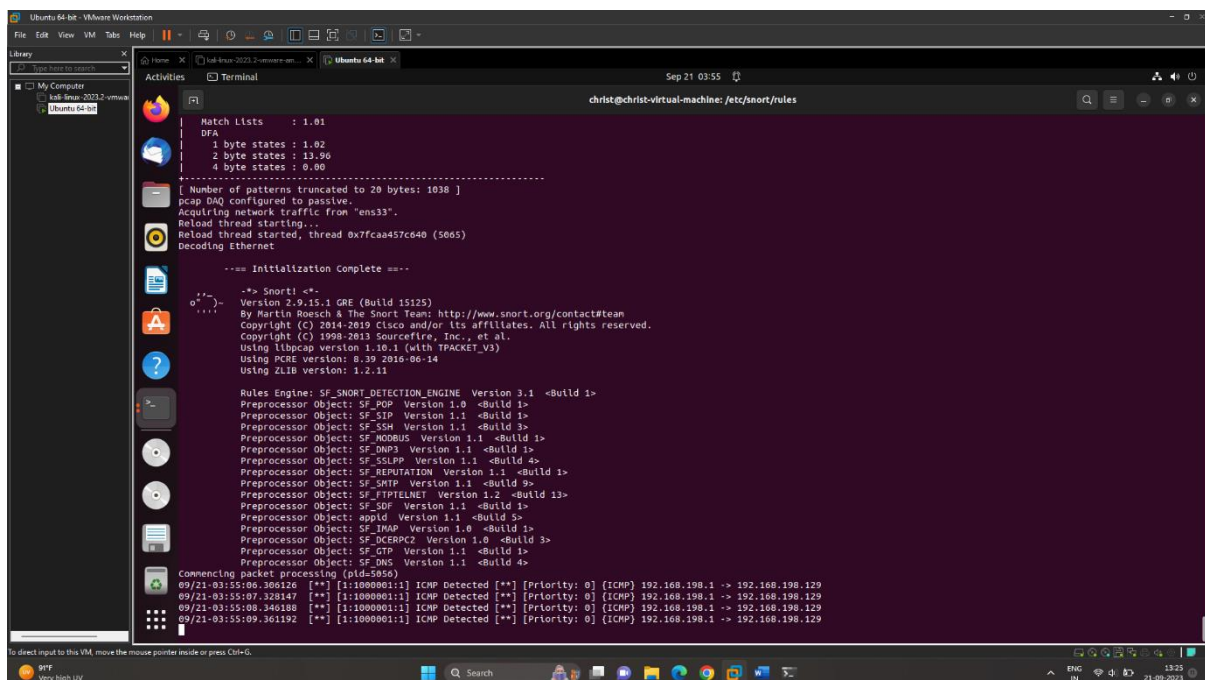
Pinging 192.168.152.136 with 32 bytes of data:
Reply from 192.168.152.136: bytes=32 time<1ms TTL=128
Reply from 192.168.152.136: bytes=32 time<1ms TTL=128
Reply from 192.168.152.136: bytes=32 time<1ms TTL=128
Reply from 192.168.152.136: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.152.136:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\CHRIST>ping 192.168.198.129

Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
Preprocessor Object: SF_SMP Version 1.1 <Build 9>
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
Preprocessor Object: SF_SDF Version 1.1 <Build 1>
Preprocessor Object: apd Version 1.1 <Build 5>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: SF_DCEPC2 Version 1.0 <Build 3>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Commencing packet processing (pid=5056)
```

## FINAL OUTPUT:



```
Match Lists : 1.01
DFA
1 byte states : 1.02
2 byte states : 13.90
4 byte states : 6.00
[ Number of patterns truncated to 20 bytes: 1038 ]
pcap DAQ configured to passive.
Acquiring network traffic from "ens33".
Reload thread starting...
Reload thread started, thread 0x7Fca457c640 (5065)
Decoding Ethernet

--- Initialization Complete ---

--> Snort! <--
Version 2.9.15.1 GRE (Build 15125)
By Martin Roesch & The Snort Team: http://www.snort.org/contact/team
Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.6.1 (with IPACKET_V3)
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.2.11

Rules Engine: SF_SNORT_DETECTION_ENGINE Version 3.1 <Build 1>
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
Preprocessor Object: SF_SMP Version 1.1 <Build 9>
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
Preprocessor Object: SF_SDF Version 1.1 <Build 1>
Preprocessor Object: apd Version 1.1 <Build 5>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: SF_DCEPC2 Version 1.0 <Build 3>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Commencing packet processing (pid=5056)
09/21-03:55:09.340126 *** [1:1000001:1] ICMP Detected *** [Priority: 0] [ICMP] 192.168.198.1 -> 192.168.198.129
09/21-03:55:07.328147 *** [1:1000001:1] ICMP Detected *** [Priority: 0] [ICMP] 192.168.198.1 -> 192.168.198.129
09/21-03:55:08.340188 *** [1:1000001:1] ICMP Detected *** [Priority: 0] [ICMP] 192.168.198.1 -> 192.168.198.129
09/21-03:55:09.361192 *** [1:1000001:1] ICMP Detected *** [Priority: 0] [ICMP] 192.168.198.1 -> 192.168.198.129
```