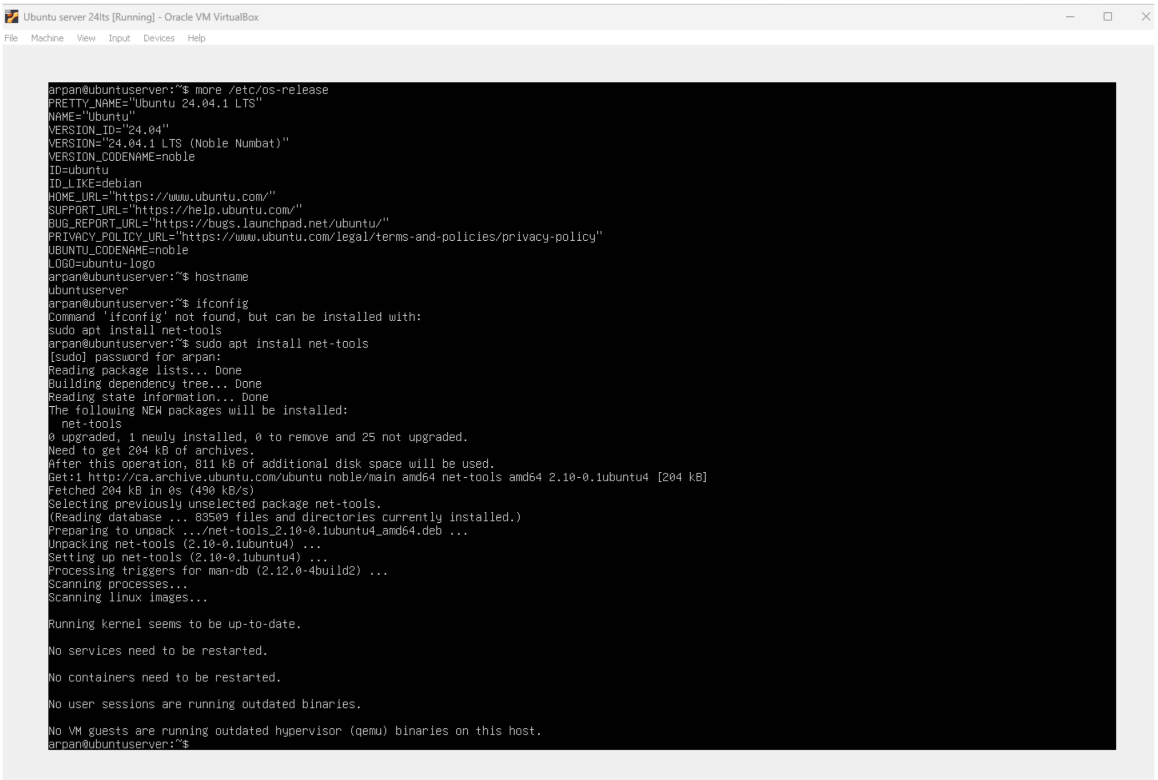
This project covers setting up **Snort IDS** on Ubuntu server and some use cases.

Installing Ubuntu Server on virtualbox:

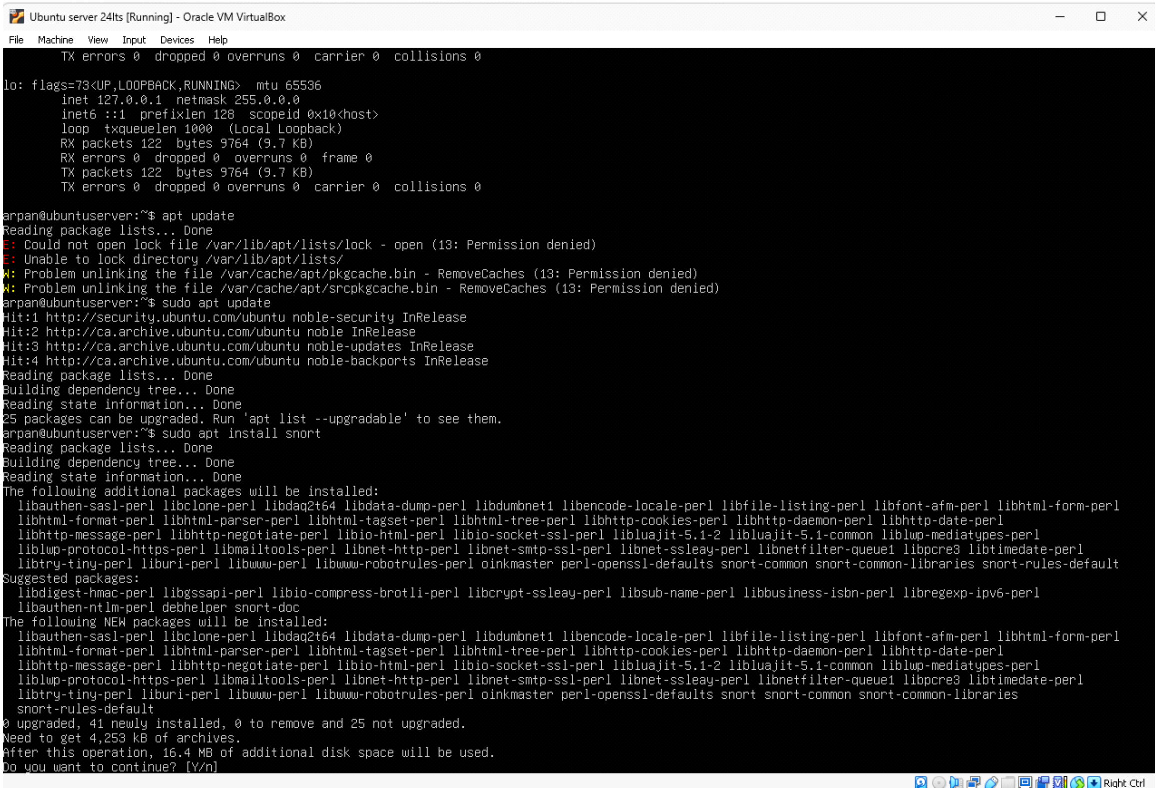


Ubuntu server 24lts [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

```
arpan@ubuntuserver:~$ more /etc/os-release
PRETTY_NAME="Ubuntu 24.04.1 LTS"
NAME="Ubuntu"
VERSION_ID="24.04"
VERSION="24.04.1 LTS (Noble Numbat)"
VERSION_CODENAME=noble
ID=ubuntu
ID_LIKE=debian
HOME_URL="https://www.ubuntu.com/"
SUPPORT_URL="https://help.ubuntu.com/"
BUG_REPORT_URL="https://bugs.launchpad.net/ubuntu/"
PRIVACY_POLICY_URL="https://www.ubuntu.com/legal/terms-and-policies/privacy-policy"
UBUNTU_CODENAME=noble
LOGO=ubuntu-logo
arpan@ubuntuserver:~$ hostname
ubuntuserver
arpan@ubuntuserver:~$ ifconfig
Command 'ifconfig' not found, but can be installed with:
sudo apt install net-tools
arpan@ubuntuserver:~$ sudo apt install net-tools
[sudo] password for arpan:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  net-tools
0 upgraded, 1 newly installed, 0 to remove and 25 not upgraded.
Need to get 204 kB of archives.
After this operation, 811 kB of additional disk space will be used.
Get:1 http://ca.archive.ubuntu.com/ubuntu noble/main amd64 net-tools amd64 2.10-0.1ubuntu4 [204 kB]
Fetched 204 kB in 0s (490 kB/s)
Selecting previously unselected package net-tools.
(Reading database ... 83509 files and directories currently installed.)
Preparing to unpack .../net-tools_2.10-0.1ubuntu4_amd64.deb ...
Unpacking net-tools (2.10-0.1ubuntu4) ...
Setting up net-tools (2.10-0.1ubuntu4) ...
Processing triggers for man-db (2.12.0-4build2) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
arpan@ubuntuserver:~$
```

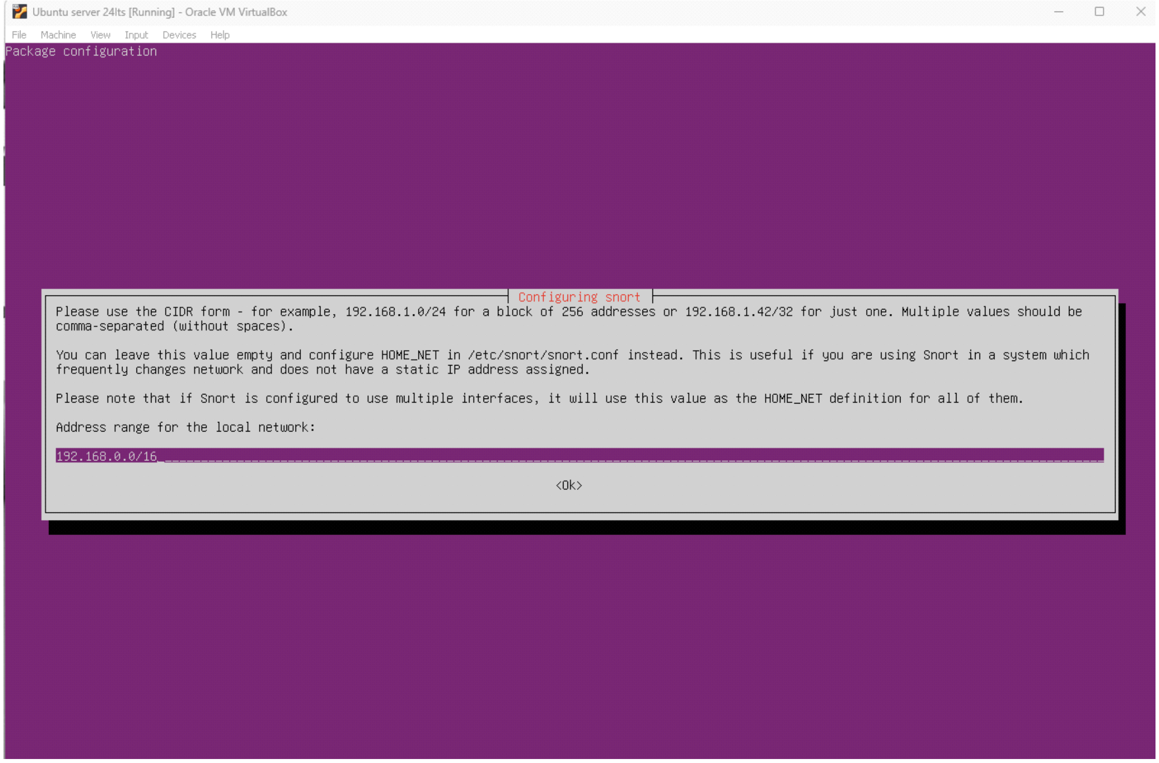
Install **snort** on ubuntu server using command:

sudo apt install snort


Ubuntu server 24lts [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Right Ctrl

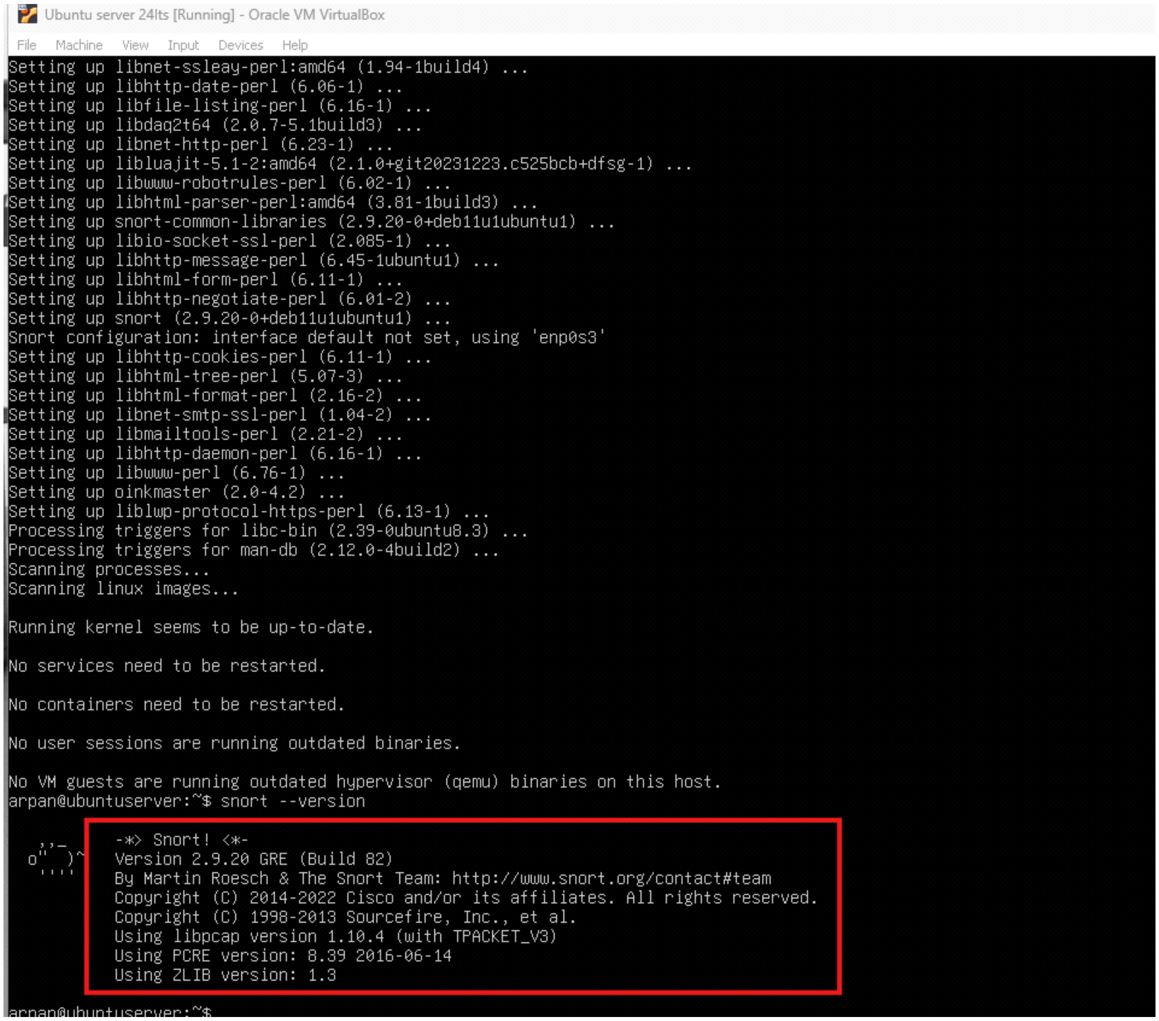
```
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 122  bytes 9764 (9.7 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 122  bytes 9764 (9.7 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

arpan@ubuntuserver:~$ apt update
Reading package lists... Done
E: Could not open lock file /var/lib/apt/lists/lock - open (13: Permission denied)
E: Unable to lock directory /var/lib/apt/lists/
W: Problem unlinking the file /var/cache/apt/pkgcache.bin - RemoveCaches (13: Permission denied)
W: Problem unlinking the file /var/cache/apt/srcpkgcache.bin - RemoveCaches (13: Permission denied)
arpan@ubuntuserver:~$ sudo apt update
Hit:1 http://security.ubuntu.com/ubuntu noble-security InRelease
Hit:2 http://ca.archive.ubuntu.com/ubuntu noble InRelease
Hit:3 http://ca.archive.ubuntu.com/ubuntu noble-updates InRelease
Hit:4 http://ca.archive.ubuntu.com/ubuntu noble-backports InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
25 packages can be upgraded. Run 'apt list --upgradable' to see them.
arpan@ubuntuserver:~$ sudo apt install snort
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libauthen-sasl-perl libclone-perl libdaq2t64 libdata-dump-perl libdumbnet1 libencode-locale-perl libfile-listing-perl libfont-afm-perl libhtml-form-perl
  libhtml-format-perl libhtml-parser-perl libhtml-tagset-perl libhtml-tree-perl libhttp-cookies-perl libhttp-daemon-perl libhttp-date-perl
  libhttp-message-perl libhttp-negotiate-perl libio-html-perl libio-socket-ssl-perl libluajit-5.1-2 libluajit-5.1-common liblwp-mediatypes-perl
  liblwp-protocol-https-perl libmailtools-perl libnet-http-perl libnet-smtp-ssl-perl libnet-ssleay-perl libnetfilter-queue1 libpcre3 libtimedate-perl
  libtry-tiny-perl liburi-perl libwww-perl libwww-robotrules-perl oinkmaster perl-openssl-defaults snort-common snort-common-libraries snort-rules-default
Suggested packages:
  libdigest-hmac-perl libgssapi-perl libio-compress-brotli-perl libcrypt-ssleay-perl libsub-name-perl libbusiness-isbn-perl libregexp-ipv6-perl
  libauthen-ntlm-perl debhelper snort-doc
The following NEW packages will be installed:
  libauthen-sasl-perl libclone-perl libdaq2t64 libdata-dump-perl libdumbnet1 libencode-locale-perl libfile-listing-perl libfont-afm-perl libhtml-form-perl
  libhtml-format-perl libhtml-parser-perl libhtml-tagset-perl libhtml-tree-perl libhttp-cookies-perl libhttp-daemon-perl libhttp-date-perl
  libhttp-message-perl libhttp-negotiate-perl libio-html-perl libio-socket-ssl-perl libluajit-5.1-2 libluajit-5.1-common liblwp-mediatypes-perl
  liblwp-protocol-https-perl libmailtools-perl libnet-http-perl libnet-smtp-ssl-perl libnet-ssleay-perl libnetfilter-queue1 libpcre3 libtimedate-perl
  libtry-tiny-perl liburi-perl libwww-perl libwww-robotrules-perl oinkmaster perl-openssl-defaults snort snort-common snort-common-libraries
  snort-rules-default
0 upgraded, 41 newly installed, 0 to remove and 25 not upgraded.
Need to get 4,253 kB of archives.
After this operation, 16.4 MB of additional disk space will be used.
Do you want to continue? [Y/n]
```

Set the ip address for the network.


Ubuntu server 24lts [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

```
Package configuration

                                         Configuring snort
 Please use the CIDR form - for example, 192.168.1.0/24 for a block of 256 addresses or 192.168.1.42/32 for just one. Multiple values should be
 comma-separated (without spaces).

 You can leave this value empty and configure HOME_NET in /etc/snort/snort.conf instead. This is useful if you are using Snort in a system which
 frequently changes network and does not have a static IP address assigned.

 Please note that if Snort is configured to use multiple interfaces, it will use this value as the HOME_NET definition for all of them.

 Address range for the local network:

 192.168.0.0/16_______________________________________________________________________________________________________________

                                                 <Ok>
```

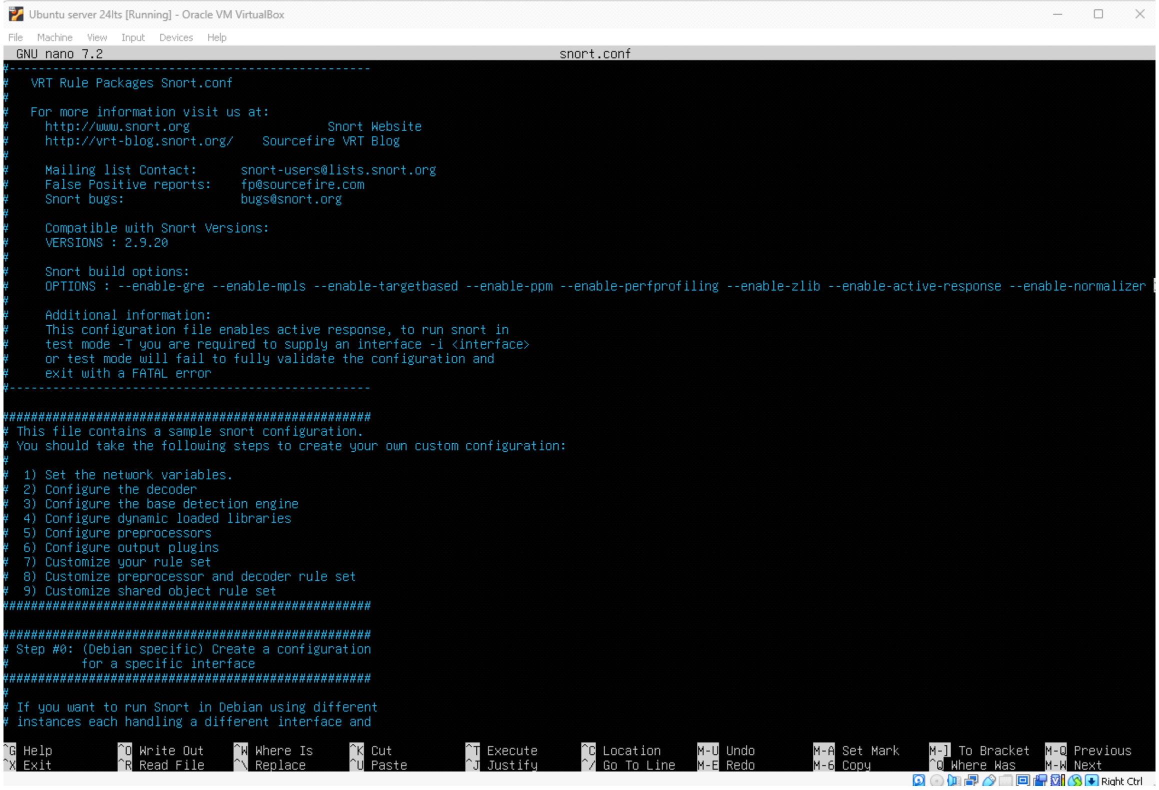
Check the version.



Ubuntu server 24lts [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

```
Setting up libnet-ssleay-perl:amd64 (1.94-1build4) ...
Setting up libhttp-date-perl (6.06-1) ...
Setting up libfile-listing-perl (6.16-1) ...
Setting up libdaq2t64 (2.0.7-5.1build3) ...
Setting up libnet-http-perl (6.23-1) ...
Setting up libluajit-5.1-2:amd64 (2.1.0+git20231223.c525bcb+dfsg-1) ...
Setting up libwww-robotrules-perl (6.02-1) ...
Setting up libhtml-parser-perl:amd64 (3.81-1build3) ...
Setting up snort-common-libraries (2.9.20-0+deb11u1ubuntu1) ...
Setting up libio-socket-ssl-perl (2.085-1) ...
Setting up libhttp-message-perl (6.45-1ubuntu1) ...
Setting up libhtml-form-perl (6.11-1) ...
Setting up libhttp-negotiate-perl (6.01-2) ...
Setting up snort (2.9.20-0+deb11u1ubuntu1) ...
Snort configuration: interface default not set, using 'enp0s3'
Setting up libhttp-cookies-perl (6.11-1) ...
Setting up libhtml-tree-perl (5.07-3) ...
Setting up libhtml-format-perl (2.16-2) ...
Setting up libnet-smtp-ssl-perl (1.04-2) ...
Setting up libmailtools-perl (2.21-2) ...
Setting up libhttp-daemon-perl (6.16-1) ...
Setting up libwww-perl (6.76-1) ...
Setting up oinkmaster (2.0-4.2) ...
Setting up liblwp-protocol-https-perl (6.13-1) ...
Processing triggers for libc-bin (2.39-0ubuntu8.3) ...
Processing triggers for man-db (2.12.0-4build2) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
arpan@ubuntuserver:~$ snort --version

   ,,_     -*> 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

arpan@ubuntuserver:~$
```

Navigate to **/etc/snort** and you can check the configurations in **snort.conf** file.

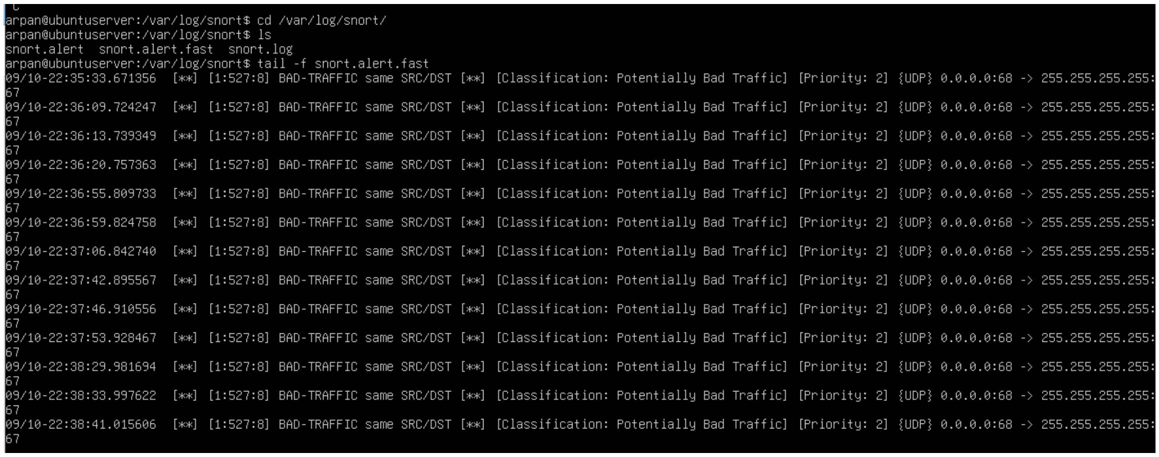

Ubuntu server 24lts [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Right Ctrl

```
  GNU nano 7.2                                                                snort.conf
#--------------------------------------------------
#   VRT Rule Packages Snort.conf
#
#   For more information visit us at:
#     http://www.snort.org                   Snort Website
#     http://vrt-blog.snort.org/    Sourcefire VRT Blog
#
#     Mailing list Contact:      snort-users@lists.snort.org
#     False Positive reports:    fp@sourcefire.com
#     Snort bugs:                bugs@snort.org
#
#     Compatible with Snort Versions:
#     VERSIONS : 2.9.20
#
#     Snort build options:
#     OPTIONS : --enable-gre --enable-mpls --enable-targetbased --enable-ppm --enable-perfprofiling --enable-zlib --enable-active-response --enable-normalizer
#
#     Additional information:
#     This configuration file enables active response, to run snort in
#     test mode -T you are required to supply an interface -i <interface>
#     or test mode will fail to fully validate the configuration and
#     exit with a FATAL error
#--------------------------------------------------

###################################################
# 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 #0: (Debian specific) Create a configuration
#          for a specific interface
###################################################
#
# If you want to run Snort in Debian using different
# instances each handling a different interface and
```

To view logs :

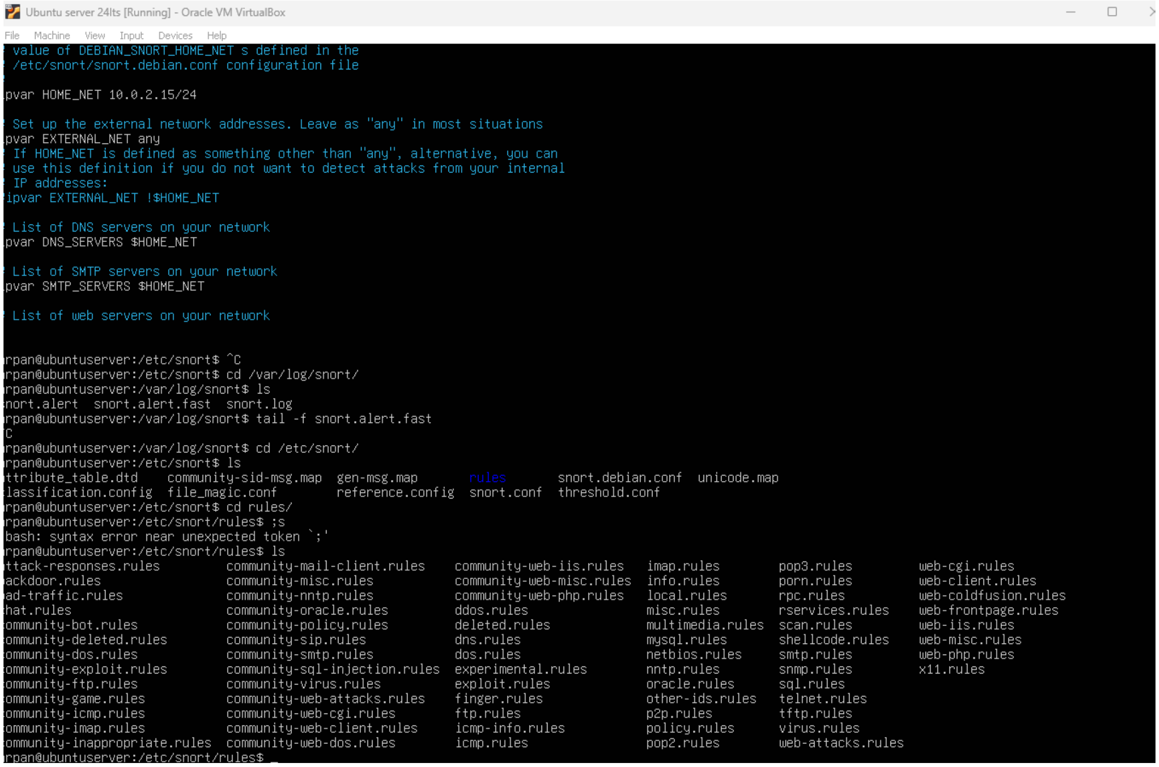
cd   /var/log/snort/

tail -f snort.alert.fast



```
^C
arpan@ubuntuserver:/var/log/snort$ cd /var/log/snort/
arpan@ubuntuserver:/var/log/snort$ ls
snort.alert  snort.alert.fast  snort.log
arpan@ubuntuserver:/var/log/snort$ tail -f snort.alert.fast
09/10-22:35:33.671356  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 -> 255.255.255.255:
67
09/10-22:36:09.724247  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 -> 255.255.255.255:
67
09/10-22:36:13.739349  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 -> 255.255.255.255:
67
09/10-22:36:20.757363  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 -> 255.255.255.255:
67
09/10-22:36:55.809733  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 -> 255.255.255.255:
67
09/10-22:36:59.824758  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 -> 255.255.255.255:
67
09/10-22:37:06.842740  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 -> 255.255.255.255:
67
09/10-22:37:42.895567  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 -> 255.255.255.255:
67
09/10-22:37:46.910556  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 -> 255.255.255.255:
67
09/10-22:37:53.928467  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 -> 255.255.255.255:
67
09/10-22:38:29.981694  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 -> 255.255.255.255:
67
09/10-22:38:33.997622  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 -> 255.255.255.255:
67
09/10-22:38:41.015606  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 -> 255.255.255.255:
67
```

We can view rules in **/etc/snort/rules**. The security policy or rules helps to detect the type of traffic coming in to our network. We can also customise the rules as deem fit.



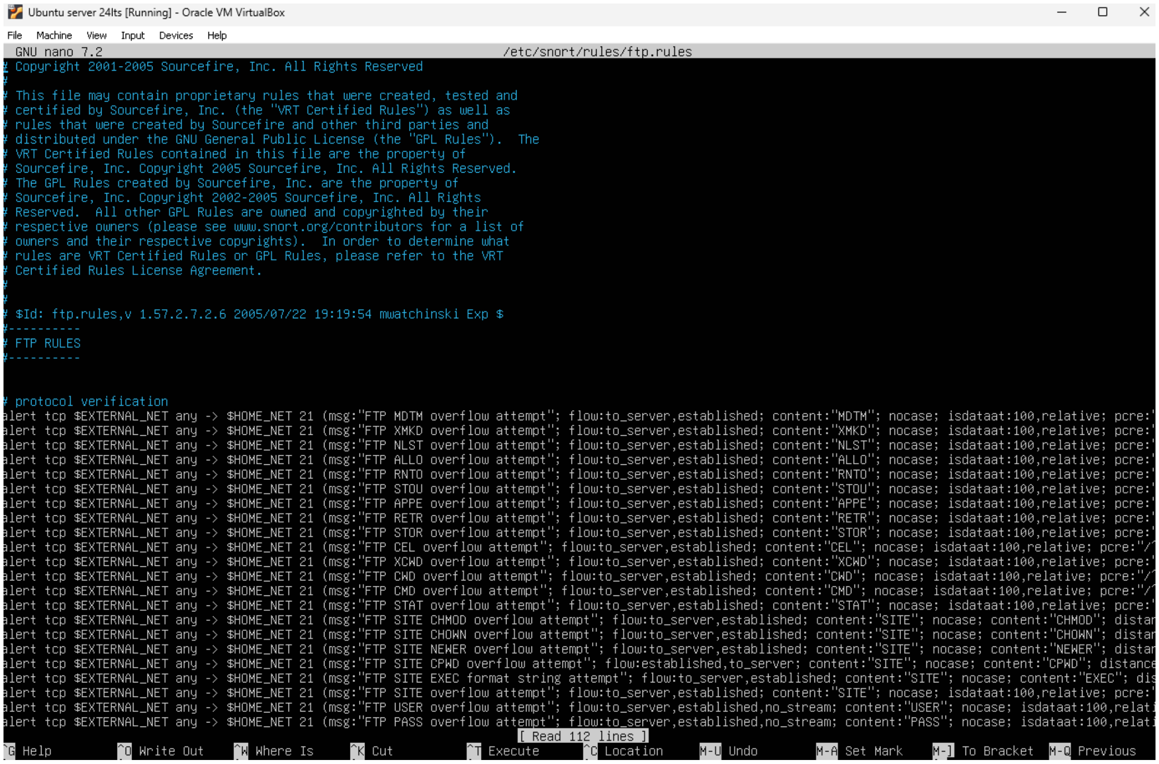
Ubuntu server 24lts [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

```
 value of DEBIAN_SNORT_HOME_NET s defined in the
 /etc/snort/snort.debian.conf configuration file

pvar HOME_NET 10.0.2.15/24

 Set up the external network addresses. Leave as "any" in most situations
pvar 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
pvar DNS_SERVERS $HOME_NET

 List of SMTP servers on your network
pvar SMTP_SERVERS $HOME_NET

 List of web servers on your network


rpan@ubuntuserver:/etc/snort$ ^C
rpan@ubuntuserver:/etc/snort$ cd /var/log/snort/
rpan@ubuntuserver:/var/log/snort$ ls
nort.alert  snort.alert.fast  snort.log
rpan@ubuntuserver:/var/log/snort$ tail -f snort.alert.fast
C
rpan@ubuntuserver:/var/log/snort$ cd /etc/snort/
rpan@ubuntuserver:/etc/snort$ ls
ttribute_table.dtd    community-sid-msg.map  gen-msg.map       rules       snort.debian.conf  unicode.map
lassification.config  file_magic.conf        reference.config  snort.conf  threshold.conf
rpan@ubuntuserver:/etc/snort$ cd rules/
rpan@ubuntuserver:/etc/snort/rules$ ;s
bash: syntax error near unexpected token `;'
rpan@ubuntuserver:/etc/snort/rules$ ls
ttack-responses.rules         community-mail-client.rules    community-web-iis.rules   imap.rules        pop3.rules         web-cgi.rules
ackdoor.rules                 community-misc.rules           community-web-misc.rules  info.rules        porn.rules         web-client.rules
ad-traffic.rules              community-nntp.rules           community-web-php.rules   local.rules       rpc.rules          web-coldfusion.rules
hat.rules                     community-oracle.rules         ddos.rules                misc.rules        rservices.rules    web-frontpage.rules
ommunity-bot.rules            community-policy.rules         deleted.rules             multimedia.rules  scan.rules         web-iis.rules
ommunity-deleted.rules        community-sip.rules            dns.rules                 mysql.rules       shellcode.rules    web-misc.rules
ommunity-dos.rules            community-smtp.rules           dos.rules                 netbios.rules     smtp.rules         web-php.rules
ommunity-exploit.rules        community-sql-injection.rules  experimental.rules        nntp.rules        snmp.rules         x11.rules
ommunity-ftp.rules            community-virus.rules          exploit.rules             oracle.rules      sql.rules
ommunity-game.rules           community-web-attacks.rules    finger.rules              other-ids.rules   telnet.rules
ommunity-icmp.rules           community-web-cgi.rules        ftp.rules                 p2p.rules         tftp.rules
ommunity-imap.rules           community-web-client.rules     icmp-info.rules           policy.rules      virus.rules
ommunity-inappropriate.rules  community-web-dos.rules        icmp.rules                pop2.rules        web-attacks.rules
rpan@ubuntuserver:/etc/snort/rules$ _
```

For example, open up a rule file:

sudo nano /etc/snort/rules/ftp.rules

We can see all the rules that are available as part of the verification. This helps in detecting cyber threats. In this case, we have an alert of **tcp** coming in from any network from any source/ destination to **home network, port 21** and we can flag it with a message **"FTP MDTM overflow attempt"**.



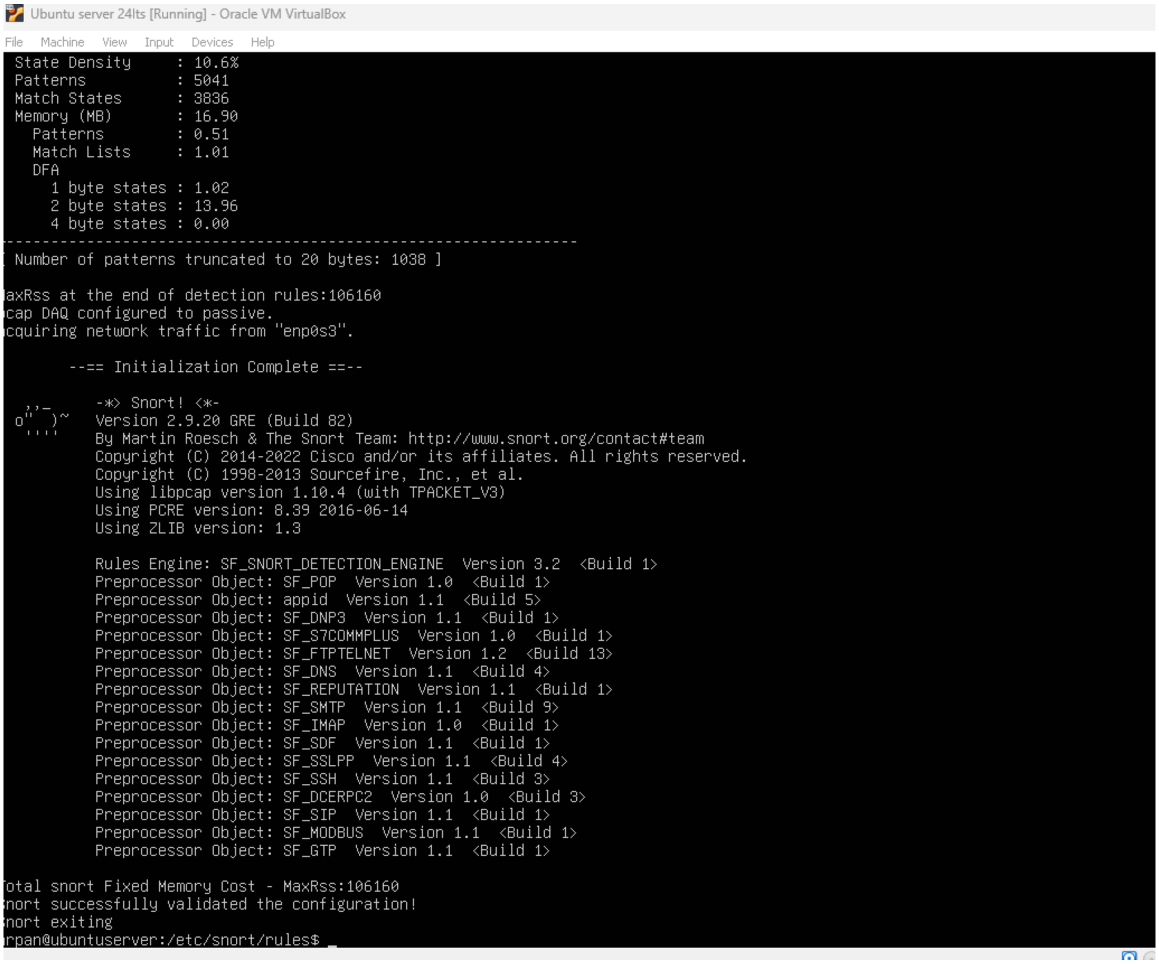
```
 GNU nano 7.2                                        /etc/snort/rules/ftp.rules
# Copyright 2001-2005 Sourcefire, Inc. All Rights Reserved
#
# This file may contain proprietary rules that were created, tested and
# certified by Sourcefire, Inc. (the "VRT Certified Rules") as well as
# rules that were created by Sourcefire and other third parties and
# distributed under the GNU General Public License (the "GPL Rules").  The
# VRT Certified Rules contained in this file are the property of
# Sourcefire, Inc. Copyright 2005 Sourcefire, Inc. All Rights Reserved.
# The GPL Rules created by Sourcefire, Inc. are the property of
# Sourcefire, Inc. Copyright 2002-2005 Sourcefire, Inc. All Rights
# Reserved.  All other GPL Rules are owned and copyrighted by their
# respective owners (please see www.snort.org/contributors for a list of
# owners and their respective copyrights).  In order to determine what
# rules are VRT Certified Rules or GPL Rules, please refer to the VRT
# Certified Rules License Agreement.
#
#
# $Id: ftp.rules,v 1.57.2.7.2.6 2005/07/22 19:19:54 mwatchinski Exp $
#----------
# FTP RULES
#----------


# protocol verification
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP MDTM overflow attempt"; flow:to_server,established; content:"MDTM"; nocase; isdataat:100,relative; pcre:'
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP XMKD overflow attempt"; flow:to_server,established; content:"XMKD"; nocase; isdataat:100,relative; pcre:'
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP NLST overflow attempt"; flow:to_server,established; content:"NLST"; nocase; isdataat:100,relative; pcre:'
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP ALLO overflow attempt"; flow:to_server,established; content:"ALLO"; nocase; isdataat:100,relative; pcre:'
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP RNTO overflow attempt"; flow:to_server,established; content:"RNTO"; nocase; isdataat:100,relative; pcre:'
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP STOU overflow attempt"; flow:to_server,established; content:"STOU"; nocase; isdataat:100,relative; pcre:'
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP APPE overflow attempt"; flow:to_server,established; content:"APPE"; nocase; isdataat:100,relative; pcre:'
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP RETR overflow attempt"; flow:to_server,established; content:"RETR"; nocase; isdataat:100,relative; pcre:'
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP STOR overflow attempt"; flow:to_server,established; content:"STOR"; nocase; isdataat:100,relative; pcre:'
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP CEL overflow attempt"; flow:to_server,established; content:"CEL"; nocase; isdataat:100,relative; pcre:"/^
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP XCWD overflow attempt"; flow:to_server,established; content:"XCWD"; nocase; isdataat:100,relative; pcre:'
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP CWD overflow attempt"; flow:to_server,established; content:"CWD"; nocase; isdataat:100,relative; pcre:"/^
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP CMD overflow attempt"; flow:to_server,established; content:"CMD"; nocase; isdataat:100,relative; pcre:"/^
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP STAT overflow attempt"; flow:to_server,established; content:"STAT"; nocase; isdataat:100,relative; pcre:'
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP SITE CHMOD overflow attempt"; flow:to_server,established; content:"SITE"; nocase; content:"CHMOD"; distan
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP SITE CHOWN overflow attempt"; flow:to_server,established; content:"SITE"; nocase; content:"CHOWN"; distan
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP SITE NEWER overflow attempt"; flow:to_server,established; content:"SITE"; nocase; content:"NEWER"; distan
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP SITE CPWD overflow attempt"; flow:established,to_server; content:"SITE"; nocase; content:"CPWD"; distance
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP SITE EXEC format string attempt"; flow:to_server,established; content:"SITE"; nocase; content:"EXEC"; dis
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP SITE overflow attempt"; flow:to_server,established; content:"SITE"; nocase; isdataat:100,relative; pcre:'
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP USER overflow attempt"; flow:to_server,established,no_stream; content:"USER"; nocase; isdataat:100,relati
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP PASS overflow attempt"; flow:to_server,established,no_stream; content:"PASS"; nocase; isdataat:100,relati
                                                                 [ Read 112 lines ]
^G Help        ^O Write Out    ^W Where Is     ^K Cut          ^T Execute      ^C Location     M-U Undo        M-A Set Mark    M-] To Bracket  M-Q Previous
```

Similarly, with all these rules/ signatures, we can identiy cyber threats.

Testing the rules:

Use command **sudo snort -T -c /etc/snort/snort.conf -i enp0s3**

This will help verify if the configurations are proper.

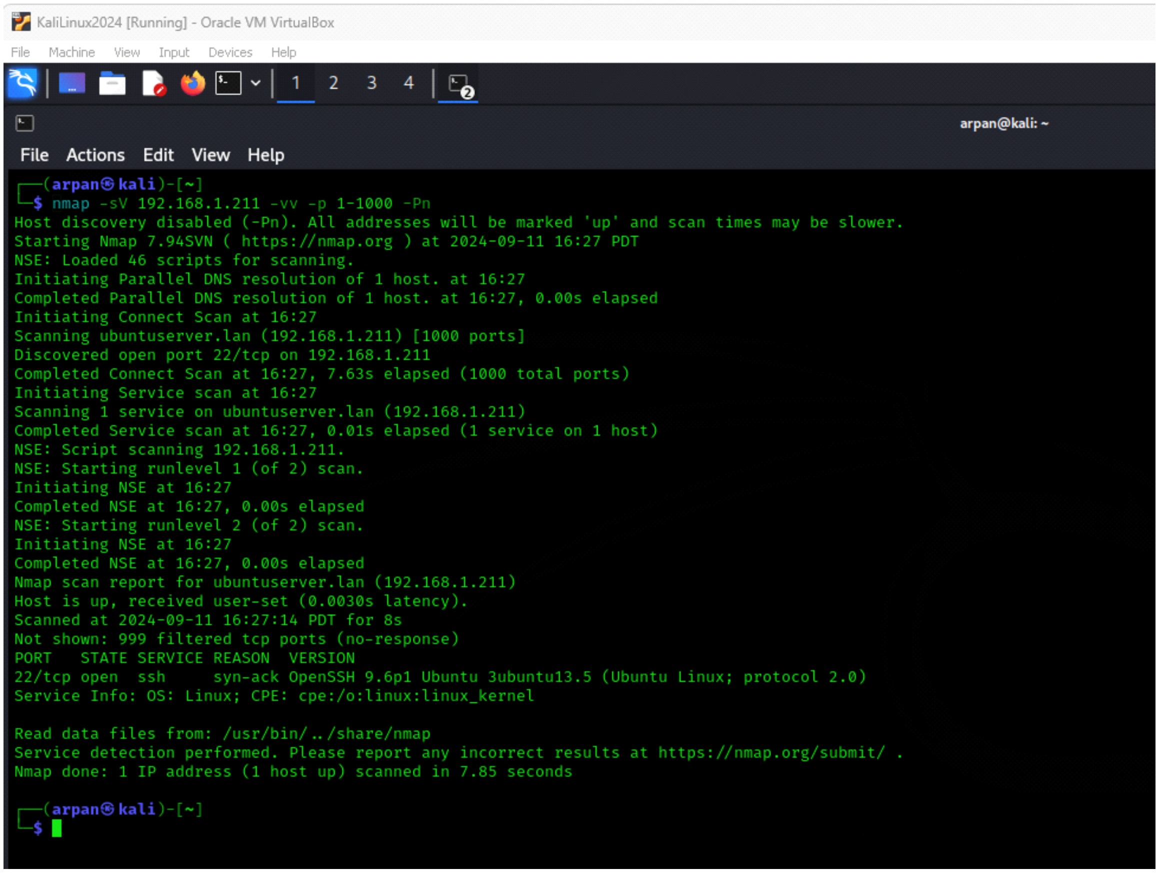


```
 State Density     : 10.6%
 Patterns          : 5041
 Match States      : 3836
 Memory (MB)       : 16.90
   Patterns        : 0.51
   Match Lists     : 1.01
   DFA
     1 byte states : 1.02
     2 byte states : 13.96
     4 byte states : 0.00
-----------------------------------------------------------------
[ Number of patterns truncated to 20 bytes: 1038 ]

axRss at the end of detection rules:106160
cap DAQ configured to passive.
cquiring network traffic from "enp0s3".

       --== 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_POP  Version 1.0  <Build 1>
           Preprocessor Object: appid  Version 1.1  <Build 5>
           Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
           Preprocessor Object: SF_S7COMMPLUS  Version 1.0  <Build 1>
           Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
           Preprocessor Object: SF_DNS  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_IMAP  Version 1.0  <Build 1>
           Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
           Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
           Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
           Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
           Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
           Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
           Preprocessor Object: SF_GTP  Version 1.1  <Build 1>

otal snort Fixed Memory Cost - MaxRss:106160
nort successfully validated the configuration!
nort exiting
rpan@ubuntuserver:/etc/snort/rules$ _
```

Monitoring real time traffic:

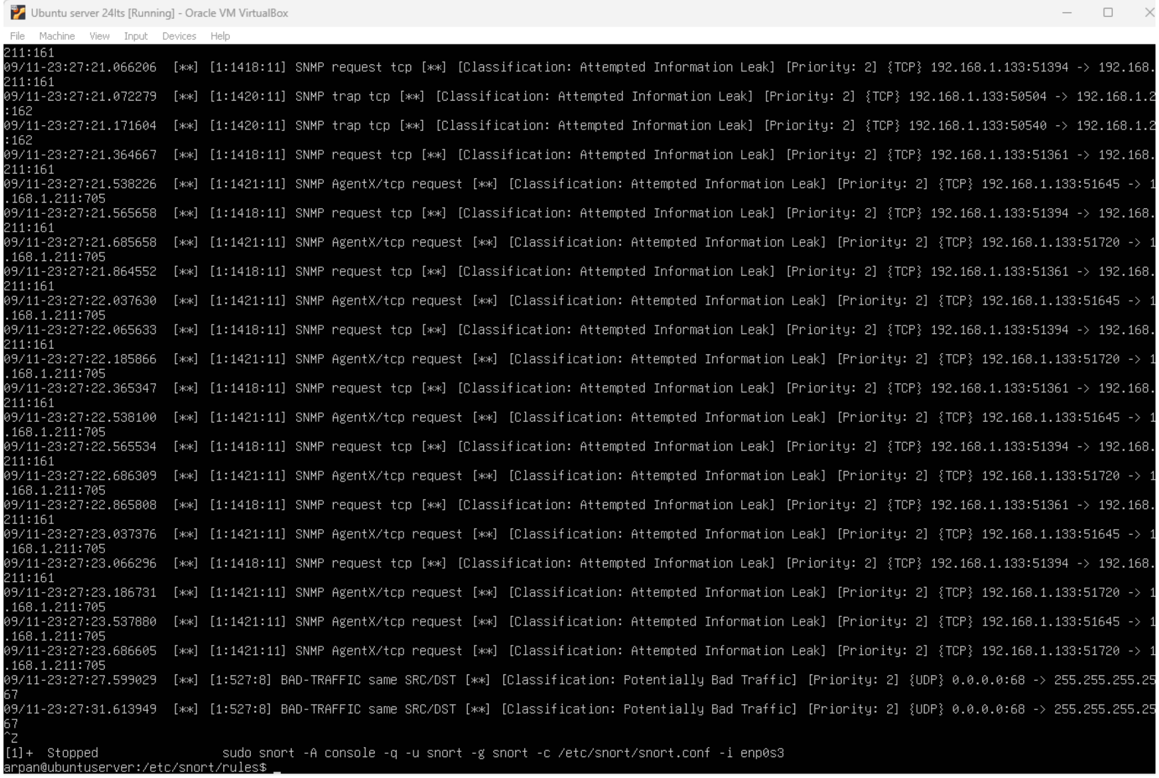
```
sudo snort - A console -q -u    snort -g snort -c /etc/snort/snort.conf -i enp0s3
```

Direct network scan/ NMAP scan from attacker (kali) machine:


KaliLinux2024 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
arpan@kali: ~
File Actions Edit View Help

```
┌──(arpan㉿kali)-[~]
└─$ nmap -sV 192.168.1.211 -vv -p 1-1000 -Pn
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-11 16:27 PDT
NSE: Loaded 46 scripts for scanning.
Initiating Parallel DNS resolution of 1 host. at 16:27
Completed Parallel DNS resolution of 1 host. at 16:27, 0.00s elapsed
Initiating Connect Scan at 16:27
Scanning ubuntuserver.lan (192.168.1.211) [1000 ports]
Discovered open port 22/tcp on 192.168.1.211
Completed Connect Scan at 16:27, 7.63s elapsed (1000 total ports)
Initiating Service scan at 16:27
Scanning 1 service on ubuntuserver.lan (192.168.1.211)
Completed Service scan at 16:27, 0.01s elapsed (1 service on 1 host)
NSE: Script scanning 192.168.1.211.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 16:27
Completed NSE at 16:27, 0.00s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 16:27
Completed NSE at 16:27, 0.00s elapsed
Nmap scan report for ubuntuserver.lan (192.168.1.211)
Host is up, received user-set (0.0030s latency).
Scanned at 2024-09-11 16:27:14 PDT for 8s
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE REASON  VERSION
22/tcp open  ssh     syn-ack OpenSSH 9.6p1 Ubuntu 3ubuntu13.5 (Ubuntu Linux; protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.85 seconds

┌──(arpan㉿kali)-[~]
└─$ 
```

We can see the alert detected as **SNMP request**, **Attempted Information Leak** against the operating system.


Ubuntu server 24lts [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

```
211:161
09/11-23:27:21.066206  [**] [1:1418:11] SNMP request tcp [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.1.133:51394 -> 192.168.
211:161
09/11-23:27:21.072279  [**] [1:1420:11] SNMP trap tcp [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.1.133:50504 -> 192.168.1.2
:162
09/11-23:27:21.171604  [**] [1:1420:11] SNMP trap tcp [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.1.133:50540 -> 192.168.1.2
:162
09/11-23:27:21.364667  [**] [1:1418:11] SNMP request tcp [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.1.133:51361 -> 192.168.
211:161
09/11-23:27:21.538226  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.1.133:51645 -> 1
.168.1.211:705
09/11-23:27:21.565658  [**] [1:1418:11] SNMP request tcp [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.1.133:51394 -> 192.168.
211:161
09/11-23:27:21.685658  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.1.133:51720 -> 1
.168.1.211:705
09/11-23:27:21.864552  [**] [1:1418:11] SNMP request tcp [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.1.133:51361 -> 192.168.
211:161
09/11-23:27:22.037630  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.1.133:51645 -> 1
.168.1.211:705
09/11-23:27:22.065633  [**] [1:1418:11] SNMP request tcp [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.1.133:51394 -> 192.168.
211:161
09/11-23:27:22.185866  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.1.133:51720 -> 1
.168.1.211:705
09/11-23:27:22.365347  [**] [1:1418:11] SNMP request tcp [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.1.133:51361 -> 192.168.
211:161
09/11-23:27:22.538100  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.1.133:51645 -> 1
.168.1.211:705
09/11-23:27:22.565534  [**] [1:1418:11] SNMP request tcp [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.1.133:51394 -> 192.168.
211:161
09/11-23:27:22.686309  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.1.133:51720 -> 1
.168.1.211:705
09/11-23:27:22.865808  [**] [1:1418:11] SNMP request tcp [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.1.133:51361 -> 192.168.
211:161
09/11-23:27:23.037376  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.1.133:51645 -> 1
.168.1.211:705
09/11-23:27:23.066296  [**] [1:1418:11] SNMP request tcp [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.1.133:51394 -> 192.168.
211:161
09/11-23:27:23.186731  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.1.133:51720 -> 1
.168.1.211:705
09/11-23:27:23.537880  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.1.133:51645 -> 1
.168.1.211:705
09/11-23:27:23.686605  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.1.133:51720 -> 1
.168.1.211:705
09/11-23:27:27.599029  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 -> 255.255.255.25
67
09/11-23:27:31.613949  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 -> 255.255.255.25
67
^Z
[1]+  Stopped                 sudo snort -A console -q -u snort -g snort -c /etc/snort/snort.conf -i enp0s3
arpan@ubuntuserver:/etc/snort/rules$ _
```

To conclude, **Snort** can be used in a variety of ways to protect networks from cyber attacks, be it as an IDS or a full-blown IPS.

This concludes the end of the project.