

SNORT DEMO

NAME: DHEVATHA S P
REG NO.: 22BCE0826

NAME OF FACULTY: DR. Satish C.J

COURSE TITLE : Penetration Testing and Vulnerability Analysis Lab

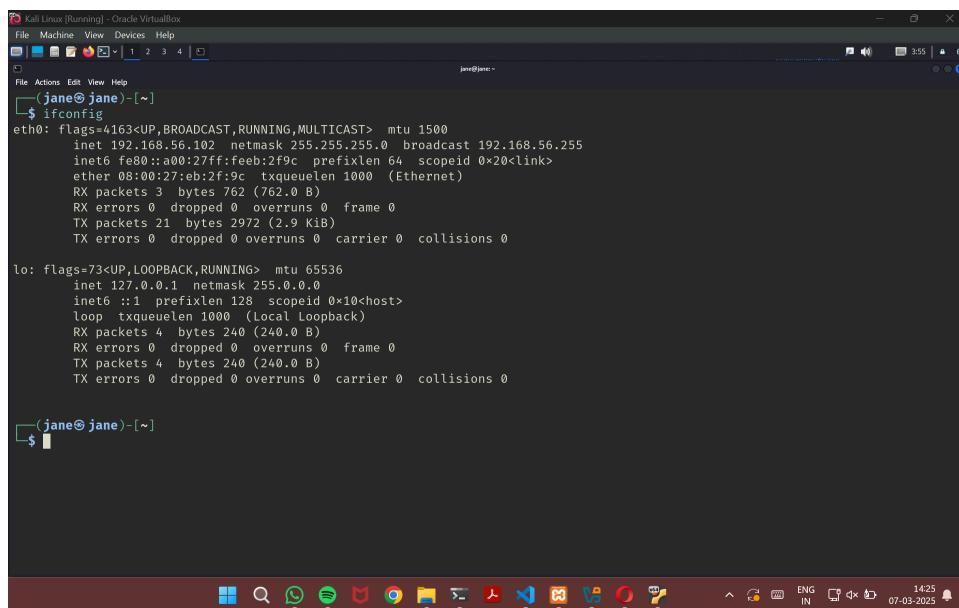
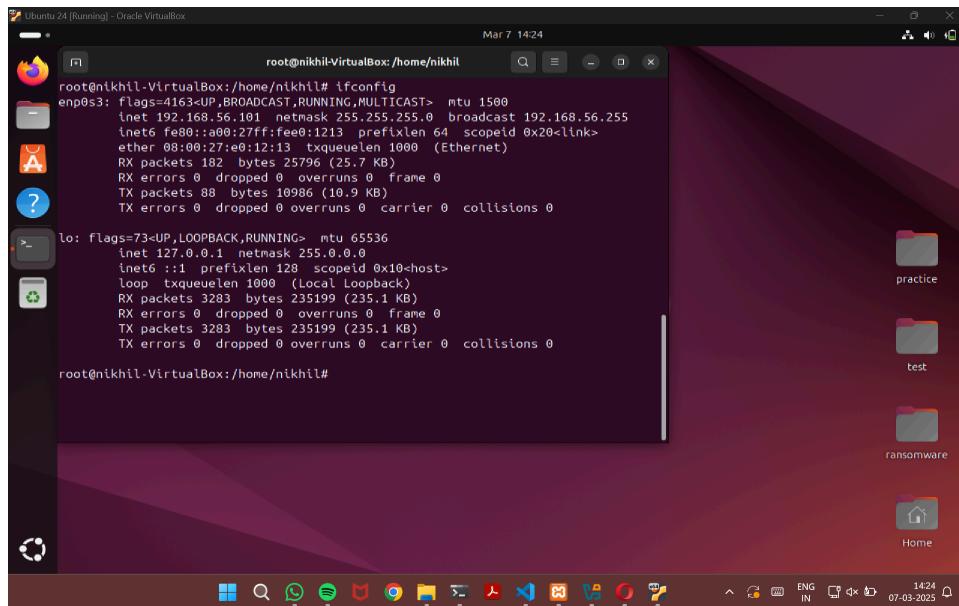
COURSE CODE: BCSE319P

LAB SLOT: L55+L56

SEMESTER: Winter Semester 2024-25

CLASS NO.: VL2024250505928

1. IP addresses of the Kali Linux and Ubuntu virtual machines



2. Installing SNORT in Ubuntu machine

```
nikhil@nikhil-VirtualBox: $ sudo apt-get install snort
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libdaq2t64 libdumbnet1 libluajit-5.1-2 libluajit-5.1-common libnetfilter-queue1 libpcre3 oinkmaster snort-common
  snort-common-libraries snort-rules-default
Suggested packages:
  snort-doc
The following NEW packages will be installed:
  libdaq2t64 libdumbnet1 libluajit-5.1-2 libluajit-5.1-common libnetfilter-queue1 libpcre3 oinkmaster snort
  snort-common snort-common-libraries snort-rules-default
0 upgraded, 11 newly installed, 0 to remove and 311 not upgraded.
Need to get 2,666 kB of archives.
After this operation, 11.4 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://in.archive.ubuntu.com/ubuntu noble/universe amd64 libluajit-5.1-common all 2.1.0+git20231223.c525bcb+dfsg-1 [49.2 kB]
Get:2 http://in.archive.ubuntu.com/ubuntu noble/universe amd64 libluajit-5.1-2 amd64 2.1.0+git20231223.c525bcb+dfsg-1 [275 kB]
Get:3 http://in.archive.ubuntu.com/ubuntu noble/universe amd64 libpcre3 amd64 2:8.39-15build1 [248 kB]
Get:4 http://in.archive.ubuntu.com/ubuntu noble/universe amd64 snort-common-libraries amd64 2.9.20-0+deb11u1ubunt1 [899 kB]
Get:5 http://in.archive.ubuntu.com/ubuntu noble/universe amd64 snort-rules-default all 2.9.20-0+deb11u1ubunt1 [144 kB]
Get:6 http://in.archive.ubuntu.com/ubuntu noble/universe amd64 snort-common all 2.9.20-0+deb11u1ubunt1 [47.7 kB]
Get:7 http://in.archive.ubuntu.com/ubuntu noble/universe amd64 libdumbnet1 amd64 1.17.0-1~ubunt2 [39.7 kB]
Get:8 http://in.archive.ubuntu.com/ubuntu noble/universe amd64 libnetfilter-queue1 amd64 1.0.5-4build1 [15.1 kB]
Get:9 http://in.archive.ubuntu.com/ubuntu noble/universe amd64 libdaq2t64 amd64 2.0.7-5.1build3 [92.9 kB]
Get:10 http://in.archive.ubuntu.com/ubuntu noble/universe amd64 snort amd64 2.9.20-0+deb11u1ubunt1 [791 kB]
Get:11 http://in.archive.ubuntu.com/ubuntu noble/universe amd64 oinkmaster all 2.0.4.2 [71.9 kB]
Fetched 2,666 kB in 11s (237 kB/s)
Preconfiguring packages ...
Snort configuration: interface default not set, using 'eno0$3'
Snort configuration: interface default not set, using 'eno0$3'
```

3. Locating the SNORT directory and the snort.conf file. And the rules directory.

```
root@nikhil-VirtualBox:~/home/nikhil# cd /etc/snort
root@nikhil-VirtualBox:/etc/snort# ls
attribute_table.dtd  community-sid-msg.map  gen-msg.map      rules      snort.debian.conf  unicode.map
classification.config  file_magic.conf    reference.config  snort.conf  threshold.conf
root@nikhil-VirtualBox:/etc/snort#
```

```
Ubuntu 24 [Running] - Oracle VM VirtualBox
Mar 9 19:10
root@nikhil-VirtualBox:/etc/snort#
root@nikhil-VirtualBox:/etc/snort# cd /etc/snort
root@nikhil-VirtualBox:/etc/snort# ls
attribute_table.dtd    community-sid-msg.map   gen-msg.map      rules      snort.debian.conf  unicode.map
classification.config  file_magic.conf        reference.config  snort.conf  threshold.conf
root@nikhil-VirtualBox:/etc/snort# nano snort.conf
root@nikhil-VirtualBox:/etc/snort# ls rules
attack-responses.rules    community-ntp.rules      deleted.rules      netbios.rules    sql.rules
backdoor.rules            community-oracle.rules   dns.rules        nntp.rules      telnet.rules
bad-traffic.rules         community-policy.rules  dos.rules       oracle.rules    tftp.rules
chat.rules                community-sip.rules     experimental.rules other-ids.rules virus.rules
community-bot.rules       community-smtp.rules   exploit.rules   p2p.rules      web-attacks.rules
community-deleted.rules   community-sql-injection.rules finger.rules   policy.rules   web-cgi.rules
community-dos.rules        community-virus.rules   ftp.rules      pop2.rules     web-client.rules
community-exploit.rules   community-web-attacks.rules icmp-info.rules  pop3.rules     web-coldfusion.rules
community-ftp.rules        community-web-cgi.rules  icmp.rules     porn.rules     web-frontpage.rules
community-game.rules      community-web-client.rules imap.rules    rpc.rules      web-iis.rules
community-icmp.rules       community-web-dos.rules  info.rules    rservices.rules  web-misc.rules
community-imap.rules       community-web-lts.rules  local.rules   scan.rules     web-php.rules
community-inappropriate.rules  community-web-misc.rules misc.rules    shellcode.rules xii.rules
community-mail-client.rules community-web-php.rules  multimedia.rules  smtp.rules
community-misc.rules       ddos.rules          mysql.rules    snmp.rules

root@nikhil-VirtualBox:/etc/snort#
```

4. Testing the snort.conf

5. Running the snort.conf with the cmd - snort -A console -c /etc/snort/snort.conf

Ubuntu 24 [Running] - Oracle VirtualBox

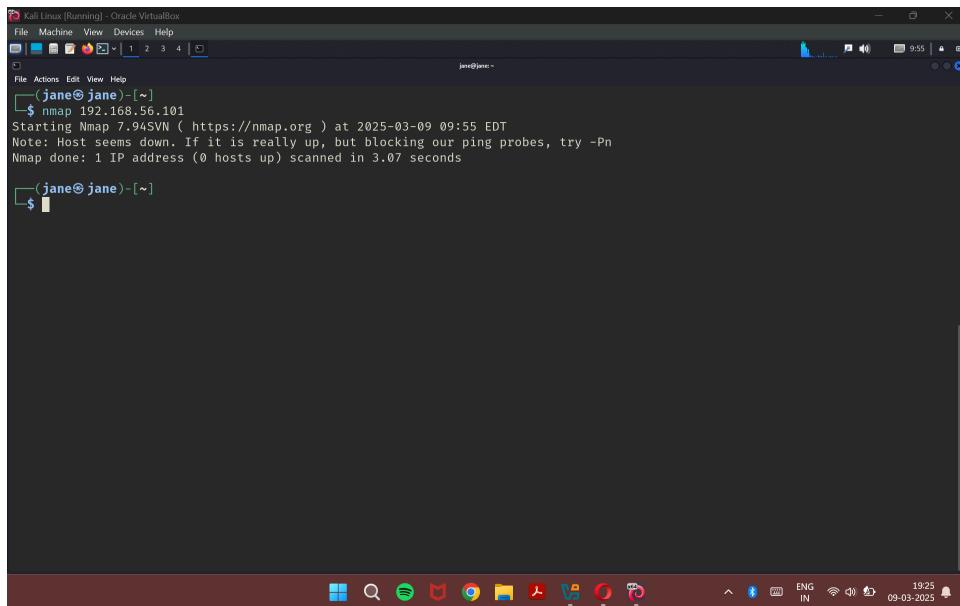
Mar 9 19:17

root@nikhil-VirtualBox:/etc/snort/rules

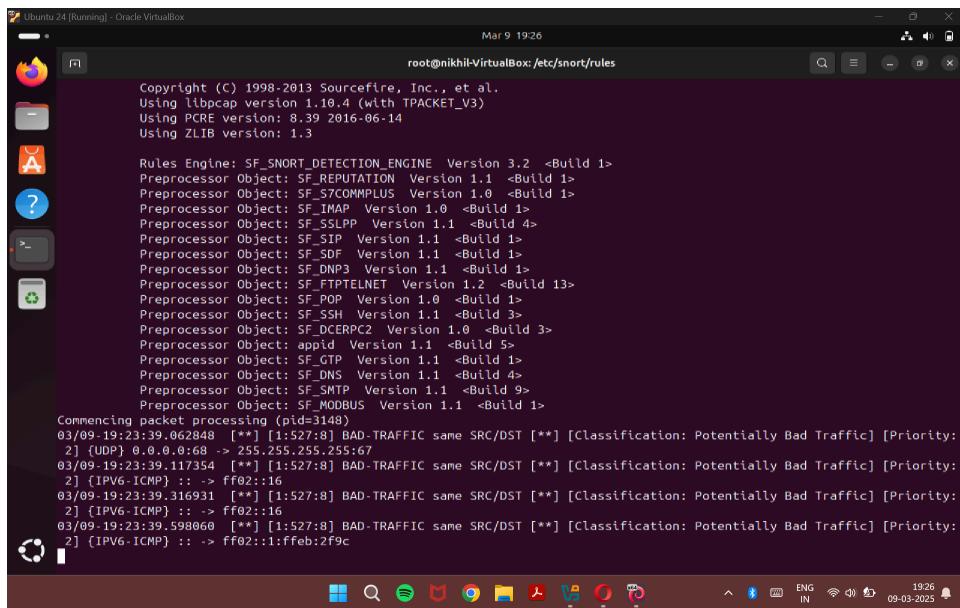
Decoding Ethernet

```
--> Snort! <--  
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 IPACKET_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_REPUTATION Version 1.1 <Build 1>  
Preprocessor Object: SF_S7COMPLUS Version 1.0 <Build 1>  
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>  
Preprocessor Object: SF_SSLLP Version 1.1 <Build 4>  
Preprocessor Object: SF_SIR Version 1.1 <Build 1>  
Preprocessor Object: SF_SDF Version 1.1 <Build 1>  
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>  
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>  
Preprocessor Object: SF_POP Version 1.0 <Build 1>  
Preprocessor Object: SF_SSH Version 1.1 <Build 3>  
Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>  
Preprocessor Object: appid Version 1.1 <Build 5>  
Preprocessor Object: SF_GTP Version 1.1 <Build 1>  
Preprocessor Object: SF_DNS Version 1.1 <Build 4>  
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>  
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>  
  
Commencing packet processing (pid=3148)
```

6. Performing NMAP scan from Kali Linux to Ubuntu while SNORT is still running



```
jane@jane:~$ nmap 192.168.56.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-09 09:55 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.07 seconds
```

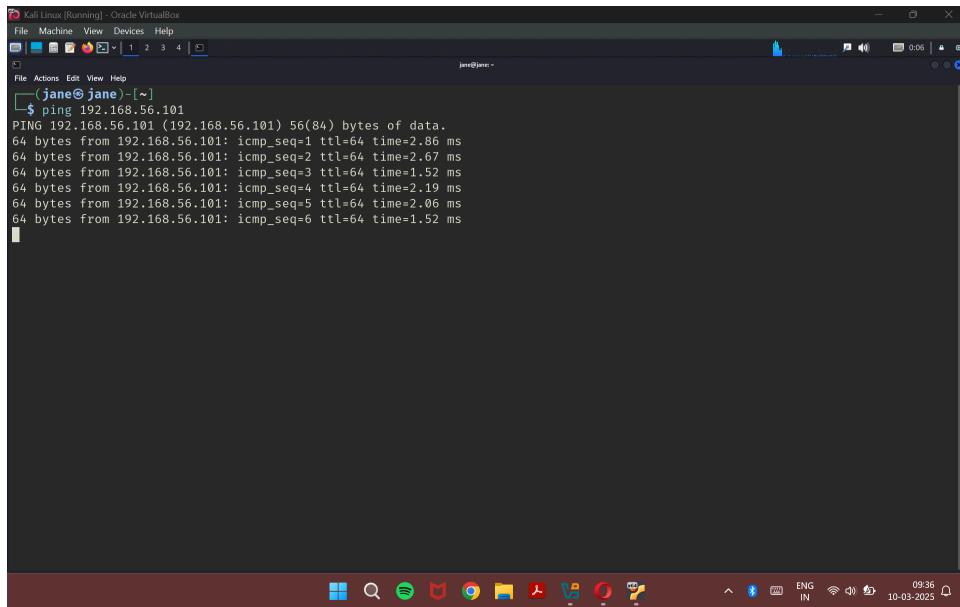


```
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.18.4 (with TPACKET_V3)
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.3

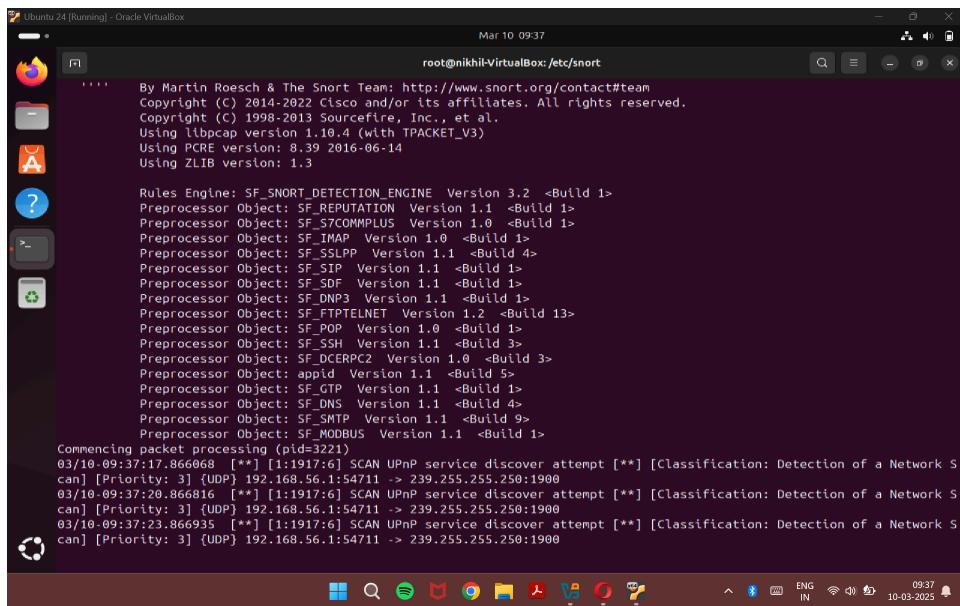
Rules Engine: SF_SNORT_DETECTION_ENGINE Version 3.2 <Build 1>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
Preprocessor Object: SF_S7COMPLUS Version 1.0 <Build 1>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Preprocessor Object: SF_SDF Version 1.1 <Build 1>
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>
Preprocessor Object: apid Version 1.1 <Build 5>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>

Commencing packet processing (pid=3148)
03/09-19:23:39.062848 [**] [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
03/09-19:23:39.117354 [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {IPV6-ICMP} :: -> ff02::16
03/09-19:23:39.316931 [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {IPV6-ICMP} :: -> ff02::1:ffeb:2f9c
```

7. Pinging Ubuntu from Kali Linux



```
(jane㉿jane) [~]
$ ping 192.168.56.101
PING 192.168.56.101 (192.168.56.101) 56(84) bytes of data.
64 bytes from 192.168.56.101: icmp_seq=1 ttl=64 time=2.86 ms
64 bytes from 192.168.56.101: icmp_seq=2 ttl=64 time=2.67 ms
64 bytes from 192.168.56.101: icmp_seq=3 ttl=64 time=1.52 ms
64 bytes from 192.168.56.101: icmp_seq=4 ttl=64 time=2.19 ms
64 bytes from 192.168.56.101: icmp_seq=5 ttl=64 time=2.06 ms
64 bytes from 192.168.56.101: icmp_seq=6 ttl=64 time=1.52 ms
```



```
root@nikhil-VirtualBox: /etc/snort
.....
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_REPUTATION Version 1.1 <Build 1>
Preprocessor Object: SF_S7COMMPLUS Version 1.0 <Build 1>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Preprocessor Object: SF_SDF Version 1.1 <Build 1>
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>
Preprocessor Object: apid Version 1.1 <Build 5>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>

Commencing packet processing (pid=3221)
03/10-09:37:17.866068 [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] {UDP} 192.168.56.1:54711 -> 239.255.255.250:1900
03/10-09:37:20.866816 [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] {UDP} 192.168.56.1:54711 -> 239.255.255.250:1900
03/10-09:37:23.866935 [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] {UDP} 192.168.56.1:54711 -> 239.255.255.250:1900
```

8. Adding rules to local.rules and testing validation

- a. Alert icmp \$EXTERNAL_NET any -> \$HOME_NET any (msg:"nik message"; sid:5889;rev:1;)

The screenshot shows the Ubuntu 24.04 LTS desktop environment running in Oracle VM VirtualBox. The terminal window is open to the directory `/etc/snort/rules` and displays the contents of the file `local.rules`. The terminal title is "GNU nano 7.2". The terminal window has a dark background with light-colored text. The desktop interface includes a dock at the bottom with icons for various applications like Dash, Help, Write Out, Read File, Where Is, Replace, Cut, Paste, Execute, Justify, Location, Go To Line, Undo, Redo, Set Mark, and Copy. The system tray at the bottom right shows the date as Mar 26 16:28, the time as 26-03-2025, and icons for network, battery, and volume.

```
nikhil@nikhil-VirtualBox: /etc/snort/rules
local.rules
GNU nano 7.2
# $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 $EXTERNAL_NET any -> $HOME_NET any (msg:"nik message"; sid:5889; rev:1);
```

Kali [Running] - Oracle VirtualBox

File Machine View Input Devices Help

File Actions Edit View Help

(jane㉿jane: ~)

```
$ ping 192.168.56.101
PING 192.168.56.101 (192.168.56.101) 56(84) bytes of data.
64 bytes from 192.168.56.101: icmp_seq=1 ttl=64 time=2.69 ms
64 bytes from 192.168.56.101: icmp_seq=2 ttl=64 time=1.21 ms
64 bytes from 192.168.56.101: icmp_seq=3 ttl=64 time=1.01 ms
64 bytes from 192.168.56.101: icmp_seq=4 ttl=64 time=1.37 ms
64 bytes from 192.168.56.101: icmp_seq=5 ttl=64 time=1.32 ms
64 bytes from 192.168.56.101: icmp_seq=6 ttl=64 time=1.60 ms
64 bytes from 192.168.56.101: icmp_seq=7 ttl=64 time=1.45 ms
64 bytes from 192.168.56.101: icmp_seq=8 ttl=64 time=1.38 ms
64 bytes from 192.168.56.101: icmp_seq=9 ttl=64 time=2.05 ms
```

```

03/27-14:32:49.998589 [**] [1:5889:1] ntk message [**] [Priority: 0] [ICMP] 192.168.56.101 -> 192.168.56.104
03/27-14:32:50.993392 [**] [1:5889:1] ntk message [**] [Priority: 0] [ICMP] 192.168.56.104 -> 192.168.56.101
03/27-14:32:50.993486 [**] [1:5889:1] ntk message [**] [Priority: 0] [ICMP] 192.168.56.101 -> 192.168.56.104
03/27-14:32:51.995695 [**] [1:5889:1] ntk message [**] [Priority: 0] [ICMP] 192.168.56.101 -> 192.168.56.101
03/27-14:32:51.995763 [**] [1:5889:1] ntk message [**] [Priority: 0] [ICMP] 192.168.56.101 -> 192.168.56.104
03/27-14:32:52.998845 [**] [1:5889:1] ntk message [**] [Priority: 0] [ICMP] 192.168.56.104 -> 192.168.56.101
03/27-14:32:52.998910 [**] [1:5889:1] ntk message [**] [Priority: 0] [ICMP] 192.168.56.101 -> 192.168.56.104
03/27-14:32:54.003241 [**] [1:5889:1] ntk message [**] [Priority: 0] [ICMP] 192.168.56.104 -> 192.168.56.101
03/27-14:32:54.003414 [**] [1:5889:1] ntk message [**] [Priority: 0] [ICMP] 192.168.56.101 -> 192.168.56.104
03/27-14:32:55.005857 [**] [1:5889:1] ntk message [**] [Priority: 0] [ICMP] 192.168.56.104 -> 192.168.56.101
03/27-14:32:55.005932 [**] [1:5889:1] ntk message [**] [Priority: 0] [ICMP] 192.168.56.101 -> 192.168.56.104
03/27-14:32:56.007801 [**] [1:5889:1] ntk message [**] [Priority: 0] [ICMP] 192.168.56.104 -> 192.168.56.101
03/27-14:32:56.007848 [**] [1:5889:1] ntk message [**] [Priority: 0] [ICMP] 192.168.56.101 -> 192.168.56.104
03/27-14:32:57.010797 [**] [1:5889:1] ntk message [**] [Priority: 0] [ICMP] 192.168.56.104 -> 192.168.56.101
03/27-14:32:58.037879 [**] [1:5889:1] ntk message [**] [Priority: 0] [ICMP] 192.168.56.104 -> 192.168.56.101
03/27-14:32:58.038865 [**] [1:5889:1] ntk message [**] [Priority: 0] [ICMP] 192.168.56.101 -> 192.168.56.104
03/27-14:32:59.043857 [**] [1:5889:1] ntk message [**] [Priority: 0] [ICMP] 192.168.56.104 -> 192.168.56.101
03/27-14:32:59.043919 [**] [1:5889:1] ntk message [**] [Priority: 0] [ICMP] 192.168.56.101 -> 192.168.56.104
03/27-14:33:00.043596 [**] [1:5889:1] ntk message [**] [Priority: 0] [ICMP] 192.168.56.104 -> 192.168.56.101
03/27-14:33:00.043650 [**] [1:5889:1] ntk message [**] [Priority: 0] [ICMP] 192.168.56.101 -> 192.168.56.104
03/27-14:33:01.046512 [**] [1:5889:1] ntk message [**] [Priority: 0] [ICMP] 192.168.56.104 -> 192.168.56.101
03/27-14:33:01.046565 [**] [1:5889:1] ntk message [**] [Priority: 0] [ICMP] 192.168.56.101 -> 192.168.56.104
03/27-14:33:02.047271 [**] [1:5889:1] ntk message [**] [Priority: 0] [ICMP] 192.168.56.104 -> 192.168.56.101
03/27-14:33:02.047333 [**] [1:5889:1] ntk message [**] [Priority: 0] [ICMP] 192.168.56.101 -> 192.168.56.104
03/27-14:33:03.049450 [**] [1:5889:1] ntk message [**] [Priority: 0] [ICMP] 192.168.56.104 -> 192.168.56.101
03/27-14:33:03.049501 [**] [1:5889:1] ntk message [**] [Priority: 0] [ICMP] 192.168.56.101 -> 192.168.56.104
03/27-14:33:04.060877 [**] [1:5889:1] ntk message [**] [Priority: 0] [ICMP] 192.168.56.104 -> 192.168.56.101
03/27-14:33:04.060146 [**] [1:5889:1] ntk message [**] [Priority: 0] [ICMP] 192.168.56.101 -> 192.168.56.104
03/27-14:33:05.061869 [**] [1:5889:1] ntk message [**] [Priority: 0] [ICMP] 192.168.56.104 -> 192.168.56.101
03/27-14:33:05.061921 [**] [1:5889:1] ntk message [**] [Priority: 0] [ICMP] 192.168.56.101 -> 192.168.56.104

```

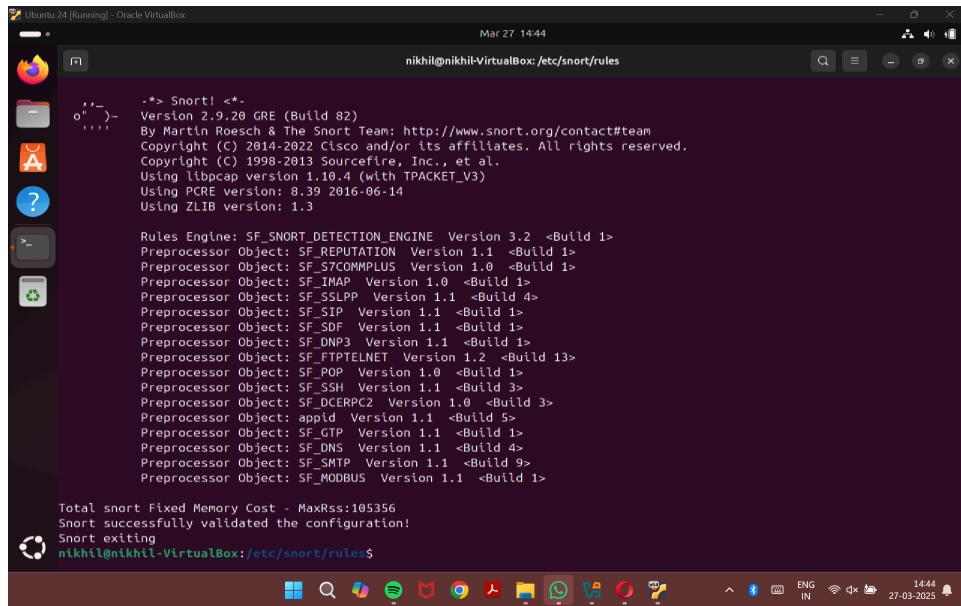
b. alert tcp any any -> \$HOME_NET 21 (msg:"FTP Attempted"; sid:60001;rev:1;)
 alert tcp any any -> \$HOME_NET 22 (msg:"SSH Attempted"; sid:60001;rev:1;)

```

GNU nano 7.2
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bnc Exp $           local.rules
# -----
# LOCAL RULES
# -----
# This file intentionally does not come with signatures. Put your local
# additions here.
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"nik message"; sid:5889; rev:1;)
alert tcp any any -> $HOME_NET 21 (msg:"FTP Attempted"; sid:60001; rev:1;)
alert tcp any any -> $HOME_NET 22 (msg:"SSH Attempted"; sid:60002; rev:1;)

Wrote 10 lines.

```



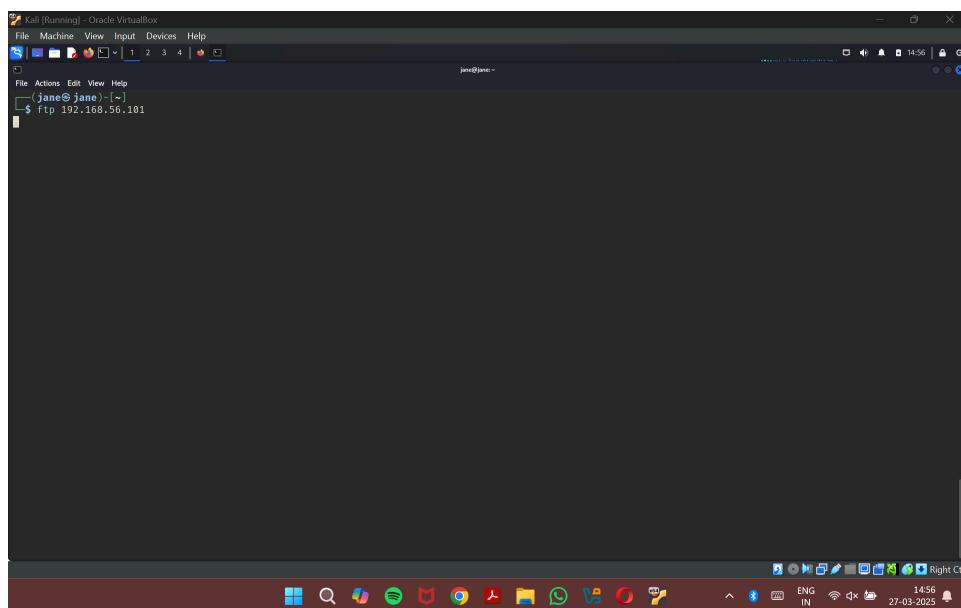
```

Ubuntu 24 [Running] - Oracle VirtualBox
Mar 27 14:44
nikhil@nikhil-VirtualBox:/etc/snort/rules

.*> Snort! <*.
Version 2.9.0 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_REPUTATION Version 1.1 <Build 1>
Preprocessor Object: SF_SF7COMMPLUS Version 1.0 <Build 1>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Preprocessor Object: SF_SDF Version 1.1 <Build 1>
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>
Preprocessor Object: apid Version 1.1 <Build 5>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>

Total snort Fixed Memory Cost - MaxRss:105356
Snort successfully validated the configuration!
Snort exiting
nikhil@nikhil-VirtualBox:/etc/snort/rules$
```



```

Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
(jane㉿jane):~$ ftp 192.168.56.101
jane@jane:~$
```

Ubuntu 24 [Running] - Oracle VirtualBox

Mar 27 14:56

nikhil@nikhil-VirtualBox: /etc/snort/rules

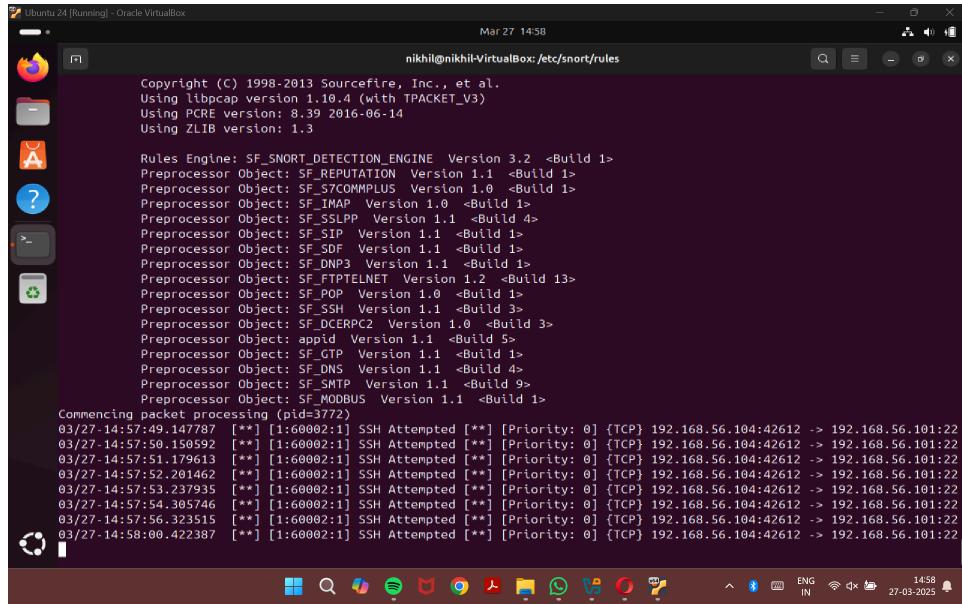
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.3

Rules Engine: SF_SNORT_DETECTION_ENGINE Version 3.2 <Build 1>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
Preprocessor Object: SF_S7COMPLUS Version 1.0 <Build 1>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Preprocessor Object: SF_SDF Version 1.1 <Build 1>
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Preprocessor Object: SF_DCEPFC2 Version 1.0 <Build 3>
Preprocessor Object: appid Version 1.1 <Build 5>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>

Commencing packet filtering (pid=3749)

03/27-14:56:29.501473 [**] [1:60001:1] FTP Attempted [**] [Priority: 0] {TCP} 192.168.56.104:52966 -> 192.168.56.101:21
03/27-14:56:30.510598 [**] [1:60001:1] FTP Attempted [**] [Priority: 0] {TCP} 192.168.56.104:52966 -> 192.168.56.101:21
03/27-14:56:31.533774 [**] [1:60001:1] FTP Attempted [**] [Priority: 0] {TCP} 192.168.56.104:52966 -> 192.168.56.101:21
03/27-14:56:32.558458 [**] [1:60001:1] FTP Attempted [**] [Priority: 0] {TCP} 192.168.56.104:52966 -> 192.168.56.101:21
03/27-14:56:33.582582 [**] [1:60001:1] FTP Attempted [**] [Priority: 0] {TCP} 192.168.56.104:52966 -> 192.168.56.101:21
03/27-14:56:34.451151 [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] [UDP] 192.168.56.1:60491 -> 239.255.255.250:1900
03/27-14:56:34.608048 [**] [1:60001:1] FTP Attempted [**] [Priority: 0] {TCP} 192.168.56.104:52966 -> 192.168.56.101:21
03/27-14:56:36.622883 [**] [1:60001:1] FTP Attempted [**] [Priority: 0] {TCP} 192.168.56.104:52966 -> 192.168.56.101:21
03/27-14:56:40.841312 [**] [1:60001:1] FTP Attempted [**] [Priority: 0] {TCP} 192.168.56.104:52966 -> 192.168.56.101:21

A screenshot of a Kali Linux desktop environment within Oracle VirtualBox. The terminal window in the foreground shows a root shell on a host named 'jane'. The command 'id' was run, displaying the user ID as 0. The command 'cat /etc/passwd' was run, showing the root password 'root'. The terminal window has a dark background with light-colored text. The desktop icons include a file manager, terminal, browser, and various system utilities. The taskbar at the bottom shows the Kali logo, a search icon, and several application icons. The system tray in the bottom right corner displays network status, battery level, and system information like 'ENG IN', '27-03-2025', and '14:57'.



Ubuntu 24 [Running] - Oracle VirtualBox
Mar 27 14:58
nikhil@nikhil-VirtualBox:/etc/snort/rules
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_REPUTATION Version 1.1 <Build 1>
Preprocessor Object: SF_S7COMMPLUS Version 1.0 <Build 1>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Preprocessor Object: SF_SD Version 1.1 <Build 1>
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>
Preprocessor Object: appid Version 1.1 <Build 5>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>
Commencing packet processing (pid=3772)
03/27-14:57:49.147787 [**] [1:60002:1] SSH Attempted [**] [Priority: 0] {TCP} 192.168.56.104:42612 -> 192.168.56.101:22
03/27-14:57:50.150592 [**] [1:60002:1] SSH Attempted [**] [Priority: 0] {TCP} 192.168.56.104:42612 -> 192.168.56.101:22
03/27-14:57:51.179613 [**] [1:60002:1] SSH Attempted [**] [Priority: 0] {TCP} 192.168.56.104:42612 -> 192.168.56.101:22
03/27-14:57:52.201462 [**] [1:60002:1] SSH Attempted [**] [Priority: 0] {TCP} 192.168.56.104:42612 -> 192.168.56.101:22
03/27-14:57:53.237935 [**] [1:60002:1] SSH Attempted [**] [Priority: 0] {TCP} 192.168.56.104:42612 -> 192.168.56.101:22
03/27-14:57:54.305746 [**] [1:60002:1] SSH Attempted [**] [Priority: 0] {TCP} 192.168.56.104:42612 -> 192.168.56.101:22
03/27-14:57:56.323515 [**] [1:60002:1] SSH Attempted [**] [Priority: 0] {TCP} 192.168.56.104:42612 -> 192.168.56.101:22
03/27-14:58:00.422387 [**] [1:60002:1] SSH Attempted [**] [Priority: 0] {TCP} 192.168.56.104:42612 -> 192.168.56.101:22