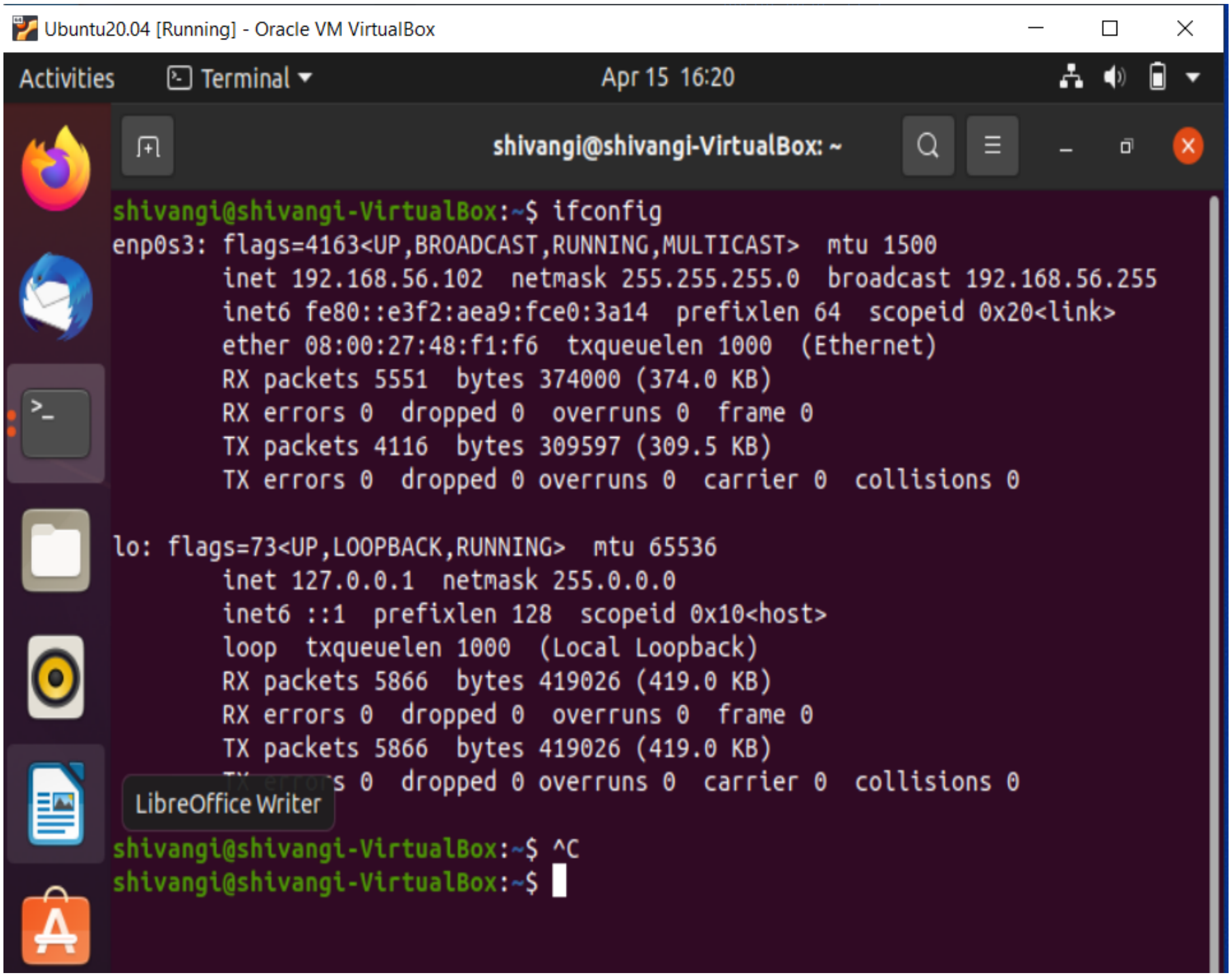
TOPIC: NETWORK INTRUSION DETECTION AND PREVENTION USING SNORT TOOL

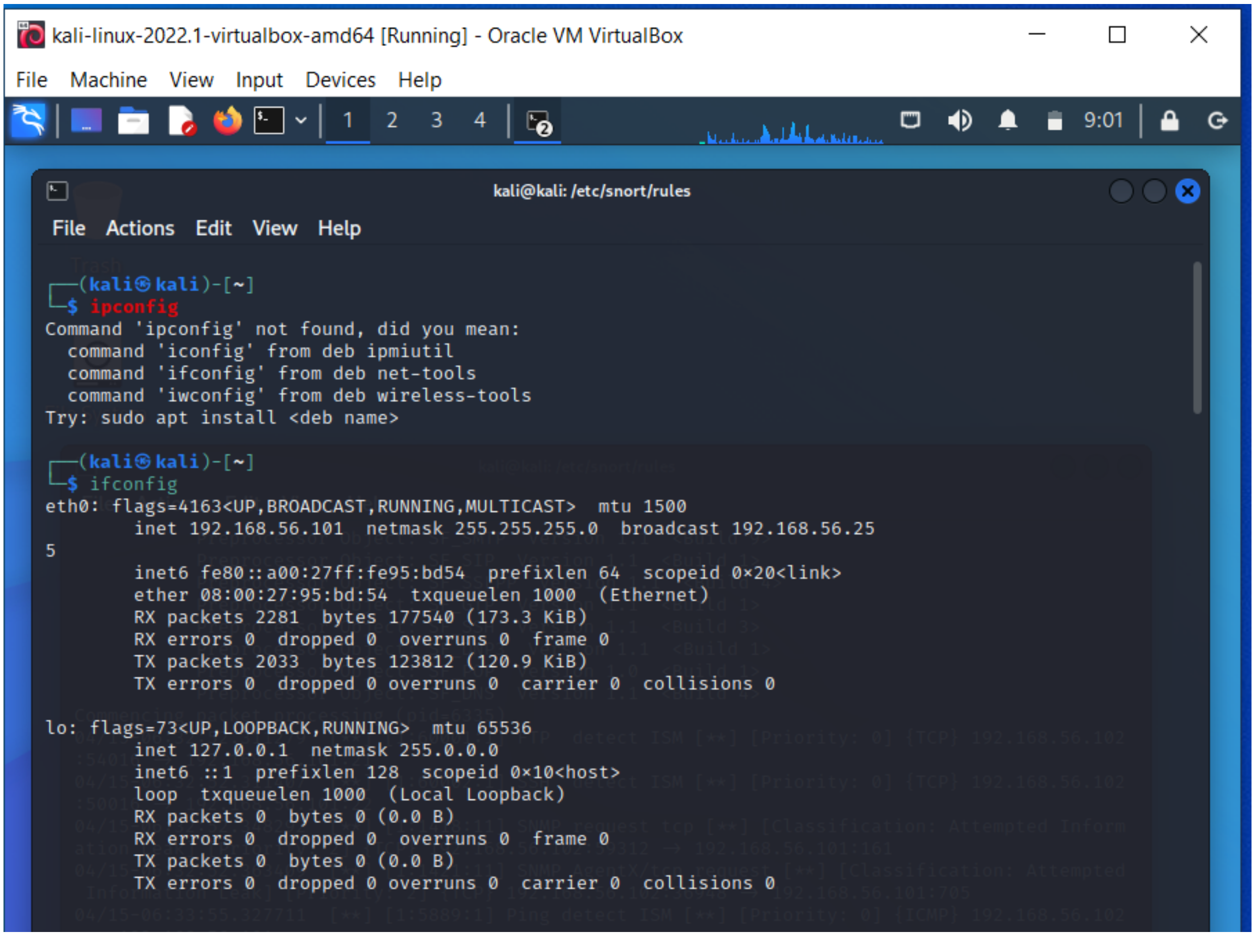
Concept - attack from ubuntu system to kali linux
Snort tool installed on kali linux

ifconfig command on ubuntu


Ubuntu20.04 [Running] - Oracle VM VirtualBox
Activities
Terminal
Apr 15 16:20
shivangi@shivangi-VirtualBox: ~
LibreOffice Writer

```
shivangi@shivangi-VirtualBox:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.56.102  netmask 255.255.255.0  broadcast 192.168.56.255
        inet6 fe80::e3f2:aea9:fce0:3a14  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:48:f1:f6  txqueuelen 1000  (Ethernet)
        RX packets 5551  bytes 374000 (374.0 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4116  bytes 309597 (309.5 KB)
        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 5866  bytes 419026 (419.0 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 5866  bytes 419026 (419.0 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

shivangi@shivangi-VirtualBox:~$ ^C
shivangi@shivangi-VirtualBox:~$
```

ifconfig command on kali linux


kali-linux-2022.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
9:01
kali@kali: /etc/snort/rules
File Actions Edit View Help

```
┌──(kali㉿kali)-[~]
└─$ ipconfig
Command 'ipconfig' not found, did you mean:
  command 'iconfig' from deb ipmiutil
  command 'ifconfig' from deb net-tools
  command 'iwconfig' from deb wireless-tools
Try: sudo apt install <deb name>

┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.56.101  netmask 255.255.255.0  broadcast 192.168.56.25
5
        inet6 fe80::a00:27ff:fe95:bd54  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:95:bd:54  txqueuelen 1000  (Ethernet)
        RX packets 2281  bytes 177540 (173.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2033  bytes 123812 (120.9 KiB)
        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 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

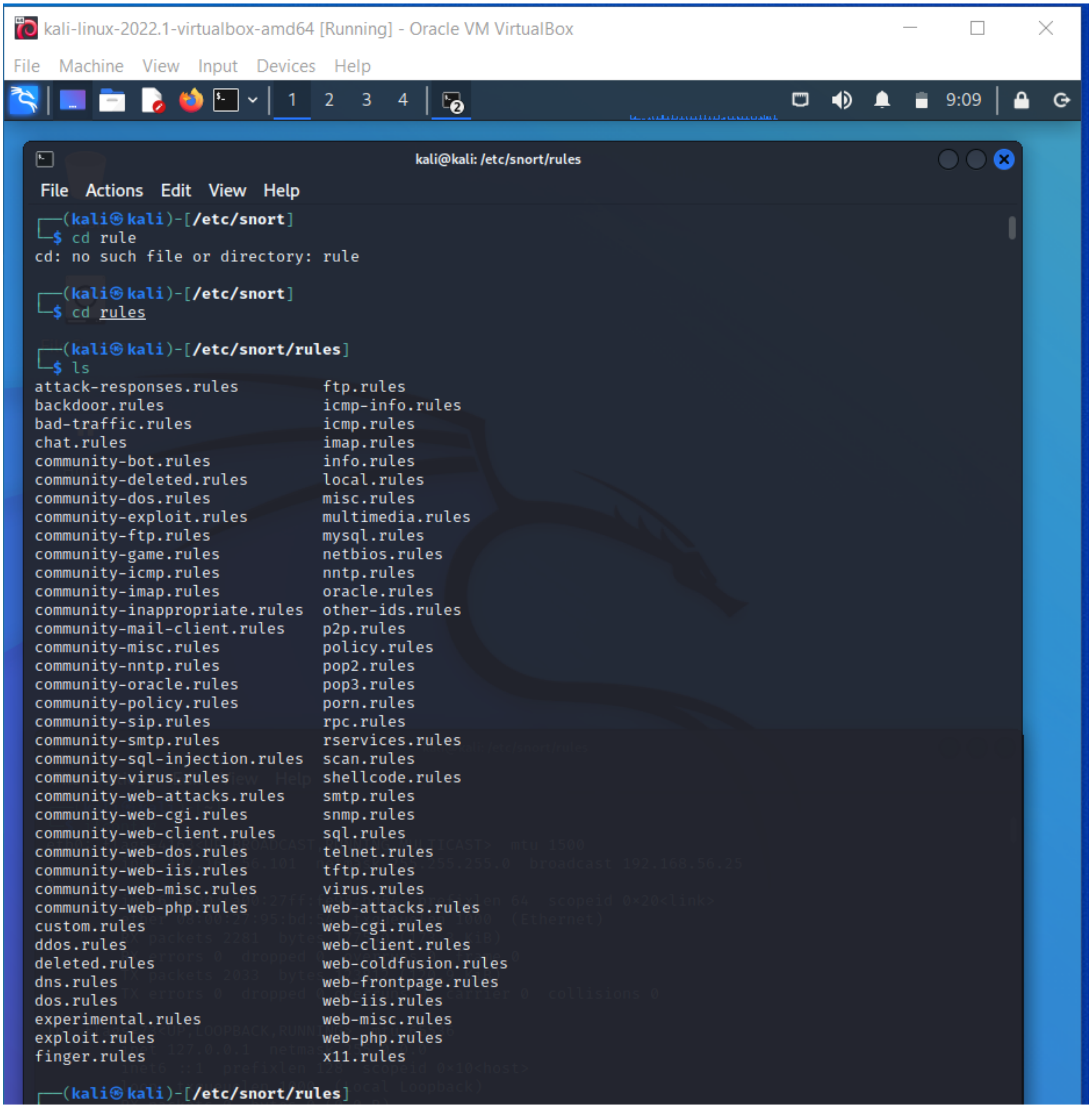
Setting up of snort tool on kali linux —------

Validating settings of snort

Your Snort should now be ready to run. Test the configuration using the parameter -T to enable test mode.

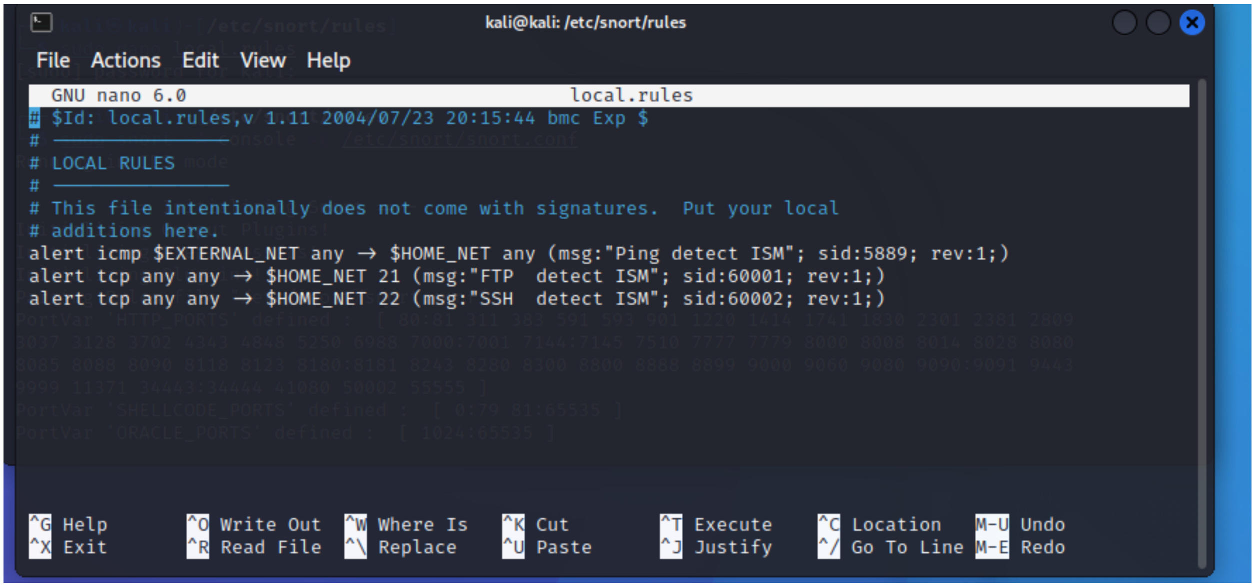
```
sudo snort -T -c /etc/snort/snort.conf
```

Rules files of snort-


kali-linux-2022.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
9:09
kali@kali: /etc/snort/rules
File Actions Edit View Help

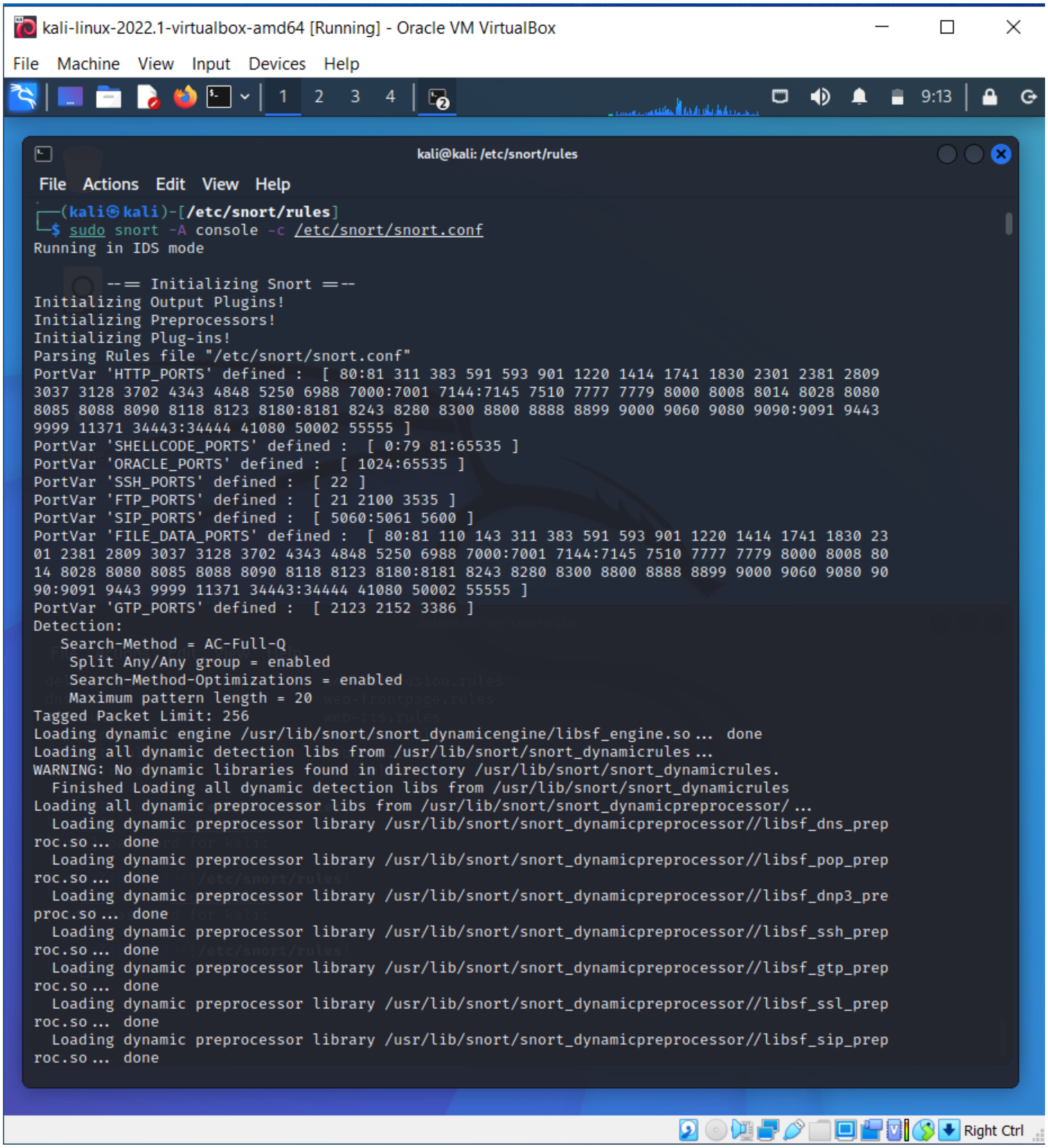
```
┌──(kali㉿kali)-[/etc/snort]
└─$ cd rule
cd: no such file or directory: rule

┌──(kali㉿kali)-[/etc/snort]
└─$ cd rules

┌──(kali㉿kali)-[/etc/snort/rules]
└─$ ls
attack-responses.rules          ftp.rules
backdoor.rules                  icmp-info.rules
bad-traffic.rules               icmp.rules
chat.rules                      imap.rules
community-bot.rules             info.rules
community-deleted.rules         local.rules
community-dos.rules             misc.rules
community-exploit.rules         multimedia.rules
community-ftp.rules             mysql.rules
community-game.rules            netbios.rules
community-icmp.rules            nntp.rules
community-imap.rules            oracle.rules
community-inappropriate.rules   other-ids.rules
community-mail-client.rules     p2p.rules
community-misc.rules            policy.rules
community-nntp.rules            pop2.rules
community-oracle.rules          pop3.rules
community-policy.rules          porn.rules
community-sip.rules             rpc.rules
community-smtp.rules            rservices.rules
community-sql-injection.rules   scan.rules
community-virus.rules           shellcode.rules
community-web-attacks.rules     smtp.rules
community-web-cgi.rules         snmp.rules
community-web-client.rules      sql.rules
community-web-dos.rules         telnet.rules
community-web-iis.rules         tftp.rules
community-web-misc.rules        virus.rules
community-web-php.rules         web-attacks.rules
custom.rules                    web-cgi.rules
ddos.rules                      web-client.rules
deleted.rules                   web-coldfusion.rules
dns.rules                       web-frontpage.rules
dos.rules                       web-iis.rules
experimental.rules              web-misc.rules
exploit.rules                   web-php.rules
finger.rules                    x11.rules

┌──(kali㉿kali)-[/etc/snort/rules]
```

Exploring the local.rules file and adding our custom rules to detect attack on kali



```
 GNU nano 6.0                                       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 $EXTERNAL_NET any → $HOME_NET any (msg:"Ping detect ISM"; sid:5889; rev:1;)
alert tcp any any → $HOME_NET 21 (msg:"FTP  detect ISM"; sid:60001; rev:1;)
alert tcp any any → $HOME_NET 22 (msg:"SSH  detect ISM"; sid:60002; rev:1;)




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

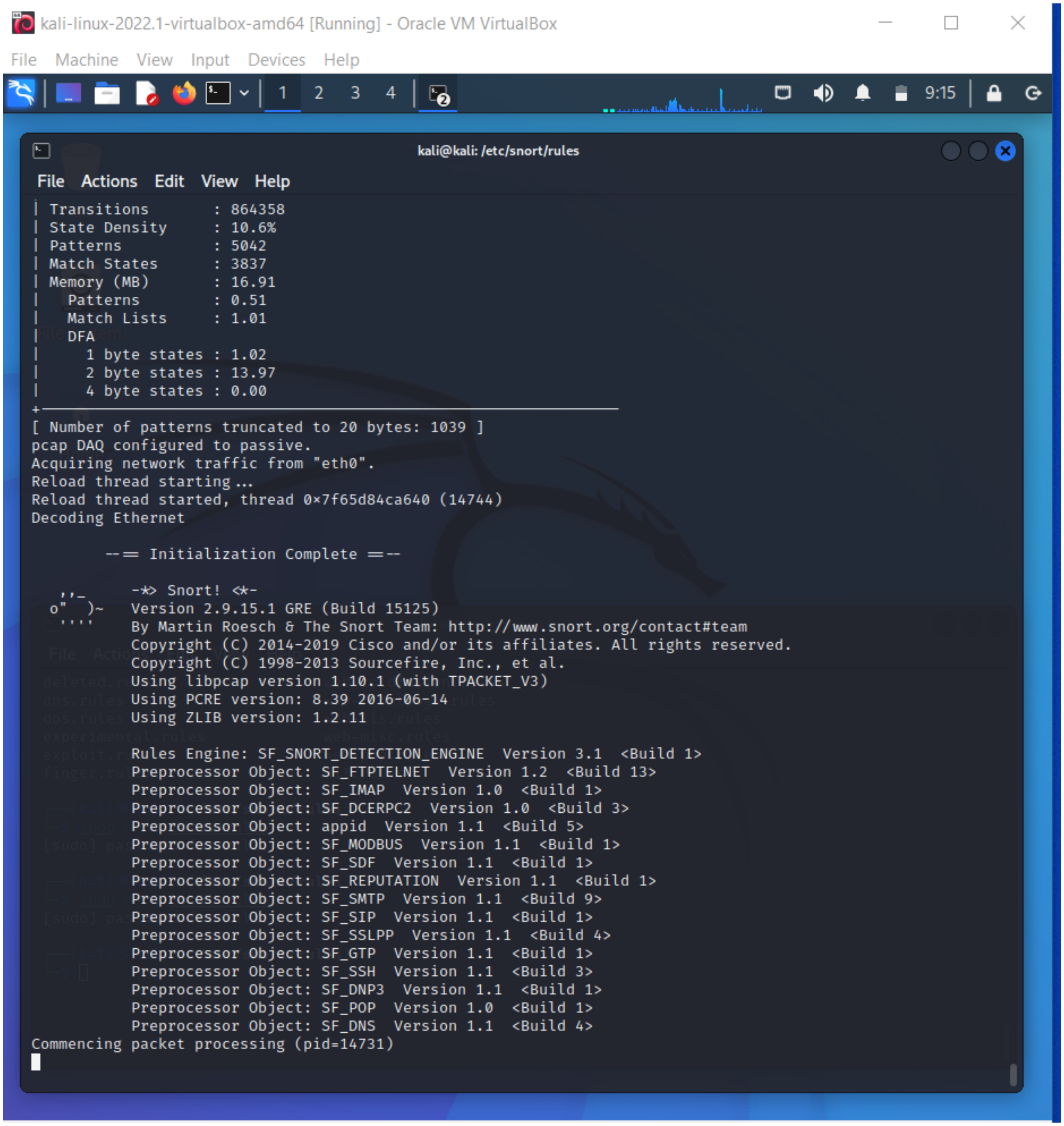
Running the snort in IDS mode



kali-linux-2022.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
9:13
kali@kali: /etc/snort/rules
File Actions Edit View Help
Right Ctrl

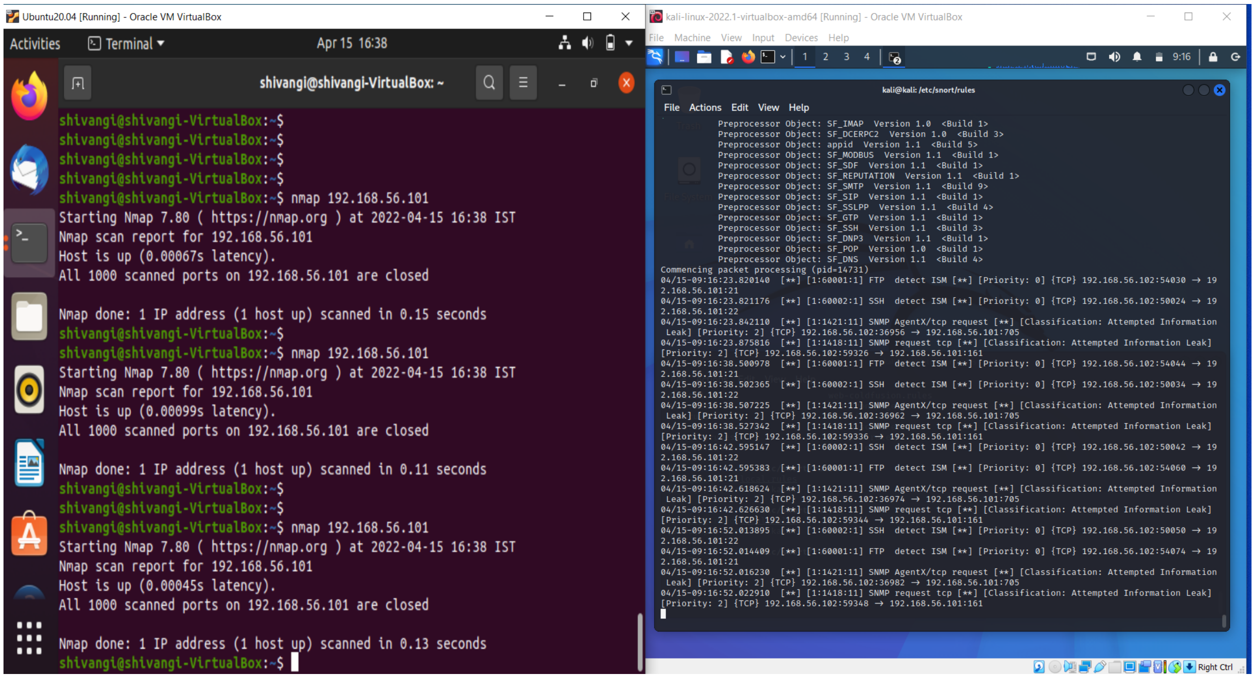
```
┌──(kali㉿kali)-[/etc/snort/rules]
└─$ sudo snort -A console -c /etc/snort/snort.conf
Running in IDS mode

        --== 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 23
01 2381 2809 3037 3128 3702 4343 4848 5250 6988 7000:7001 7144:7145 7510 7777 7779 8000 8008 80
14 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300 8800 8888 8899 9000 9060 9080 90
90:9091 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
Loading dynamic engine /usr/lib/snort/snort_dynamicengine/libsf_engine.so... done
Loading all dynamic detection libs from /usr/lib/snort/snort_dynamicrules...
WARNING: No dynamic libraries found in directory /usr/lib/snort/snort_dynamicrules.
  Finished Loading all dynamic detection libs from /usr/lib/snort/snort_dynamicrules
Loading all dynamic preprocessor libs from /usr/lib/snort/snort_dynamicpreprocessor/...
  Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_dns_prep
roc.so... done
  Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_pop_prep
roc.so... done
  Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_dnp3_pre
proc.so... done
  Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_ssh_prep
roc.so... done
  Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_gtp_prep
roc.so... done
  Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_ssl_prep
roc.so... done
  Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_sip_prep
roc.so... done
```

Before running of nmap attack from ubuntu side


kali-linux-2022.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
9:15
kali@kali: /etc/snort/rules
File Actions Edit View Help

```
| Transitions        : 864358
| State Density      : 10.6%
| Patterns           : 5042
| Match States       : 3837
| Memory (MB)        : 16.91
|   Patterns         : 0.51
|   Match Lists      : 1.01
|   DFA
|     1 byte states : 1.02
|     2 byte states : 13.97
|     4 byte states : 0.00
+----------------------------------------------------------------
[ Number of patterns truncated to 20 bytes: 1039 ]
pcap DAQ configured to passive.
Acquiring network traffic from "eth0".
Reload thread starting ...
Reload thread started, thread 0x7f65d84ca640 (14744)
Decoding Ethernet

        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   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_FTPTELNET  Version 1.2  <Build 13>
           Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
           Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
           Preprocessor Object: appid  Version 1.1  <Build 5>
           Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
           Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
           Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
           Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
           Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
           Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
           Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
           Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
           Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
           Preprocessor Object: SF_POP  Version 1.0  <Build 1>
           Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
Commencing packet processing (pid=14731)
```

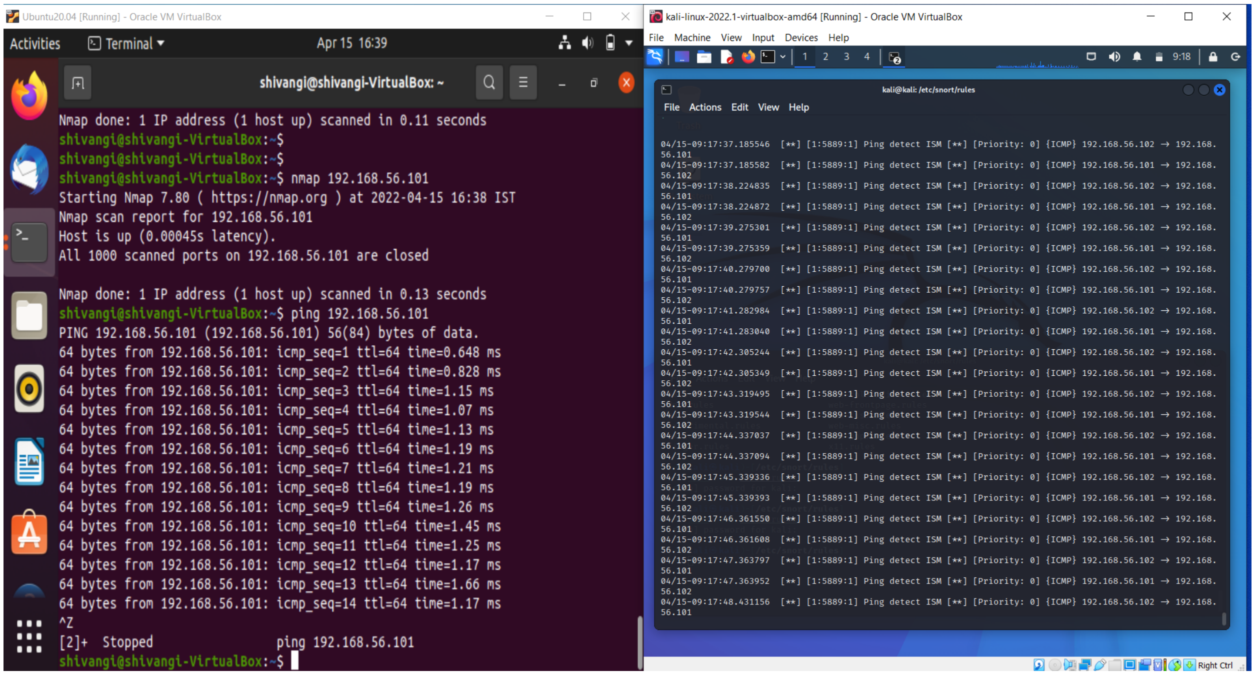
After nmap command


Ubuntu20.04 [Running] - Oracle VM VirtualBox
Activities
Terminal
Apr 15 16:38
shivangi@shivangi-VirtualBox: ~
kali-linux-2022.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
9:16
kali@kali: /etc/snort/rules
File Actions Edit View Help
Right Ctrl

```
shivangi@shivangi-VirtualBox:~$
shivangi@shivangi-VirtualBox:~$
shivangi@shivangi-VirtualBox:~$
shivangi@shivangi-VirtualBox:~$
shivangi@shivangi-VirtualBox:~$ nmap 192.168.56.101
Starting Nmap 7.80 ( https://nmap.org ) at 2022-04-15 16:38 IST
Nmap scan report for 192.168.56.101
Host is up (0.00067s latency).
All 1000 scanned ports on 192.168.56.101 are closed

Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds
shivangi@shivangi-VirtualBox:~$
shivangi@shivangi-VirtualBox:~$ nmap 192.168.56.101
Starting Nmap 7.80 ( https://nmap.org ) at 2022-04-15 16:38 IST
Nmap scan report for 192.168.56.101
Host is up (0.00099s latency).
All 1000 scanned ports on 192.168.56.101 are closed

Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
shivangi@shivangi-VirtualBox:~$
shivangi@shivangi-VirtualBox:~$
shivangi@shivangi-VirtualBox:~$ nmap 192.168.56.101
Starting Nmap 7.80 ( https://nmap.org ) at 2022-04-15 16:38 IST
Nmap scan report for 192.168.56.101
Host is up (0.00045s latency).
All 1000 scanned ports on 192.168.56.101 are closed

Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds
shivangi@shivangi-VirtualBox:~$
```

```
           Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
           Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
           Preprocessor Object: appid  Version 1.1  <Build 5>
           Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
           Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
           Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
           Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
           Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
           Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
           Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
           Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
           Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
           Preprocessor Object: SF_POP  Version 1.0  <Build 1>
           Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
Commencing packet processing (pid=14731)
04/15-09:16:23.820140  [**] [1:60001:1] FTP  detect ISM [**] [Priority: 0] {TCP} 192.168.56.102:54030 → 19
2.168.56.101:21
04/15-09:16:23.821176  [**] [1:60002:1] SSH  detect ISM [**] [Priority: 0] {TCP} 192.168.56.102:50024 → 19
2.168.56.101:22
04/15-09:16:23.842110  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attempted Information
 Leak] [Priority: 2] {TCP} 192.168.56.102:36956 → 192.168.56.101:705
04/15-09:16:23.875816  [**] [1:1418:11] SNMP request tcp [**] [Classification: Attempted Information Leak]
[Priority: 2] {TCP} 192.168.56.102:59326 → 192.168.56.101:161
04/15-09:16:38.500978  [**] [1:60001:1] FTP  detect ISM [**] [Priority: 0] {TCP} 192.168.56.102:54044 → 19
2.168.56.101:21
04/15-09:16:38.502365  [**] [1:60002:1] SSH  detect ISM [**] [Priority: 0] {TCP} 192.168.56.102:50034 → 19
2.168.56.101:22
04/15-09:16:38.507225  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attempted Information
 Leak] [Priority: 2] {TCP} 192.168.56.102:36962 → 192.168.56.101:705
04/15-09:16:38.527342  [**] [1:1418:11] SNMP request tcp [**] [Classification: Attempted Information Leak]
[Priority: 2] {TCP} 192.168.56.102:59336 → 192.168.56.101:161
04/15-09:16:42.595147  [**] [1:60002:1] SSH  detect ISM [**] [Priority: 0] {TCP} 192.168.56.102:50042 → 19
2.168.56.101:22
04/15-09:16:42.595383  [**] [1:60001:1] FTP  detect ISM [**] [Priority: 0] {TCP} 192.168.56.102:54060 → 19
2.168.56.101:21
04/15-09:16:42.618624  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attempted Information
 Leak] [Priority: 2] {TCP} 192.168.56.102:36974 → 192.168.56.101:705
04/15-09:16:42.626630  [**] [1:1418:11] SNMP request tcp [**] [Classification: Attempted Information Leak]
[Priority: 2] {TCP} 192.168.56.102:59344 → 192.168.56.101:161
04/15-09:16:52.013895  [**] [1:60002:1] SSH  detect ISM [**] [Priority: 0] {TCP} 192.168.56.102:50050 → 19
2.168.56.101:22
04/15-09:16:52.014409  [**] [1:60001:1] FTP  detect ISM [**] [Priority: 0] {TCP} 192.168.56.102:54074 → 19
2.168.56.101:21
04/15-09:16:52.016230  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attempted Information
 Leak] [Priority: 2] {TCP} 192.168.56.102:36982 → 192.168.56.101:705
04/15-09:16:52.022910  [**] [1:1418:11] SNMP request tcp [**] [Classification: Attempted Information Leak]
[Priority: 2] {TCP} 192.168.56.102:59348 → 192.168.56.101:161
```

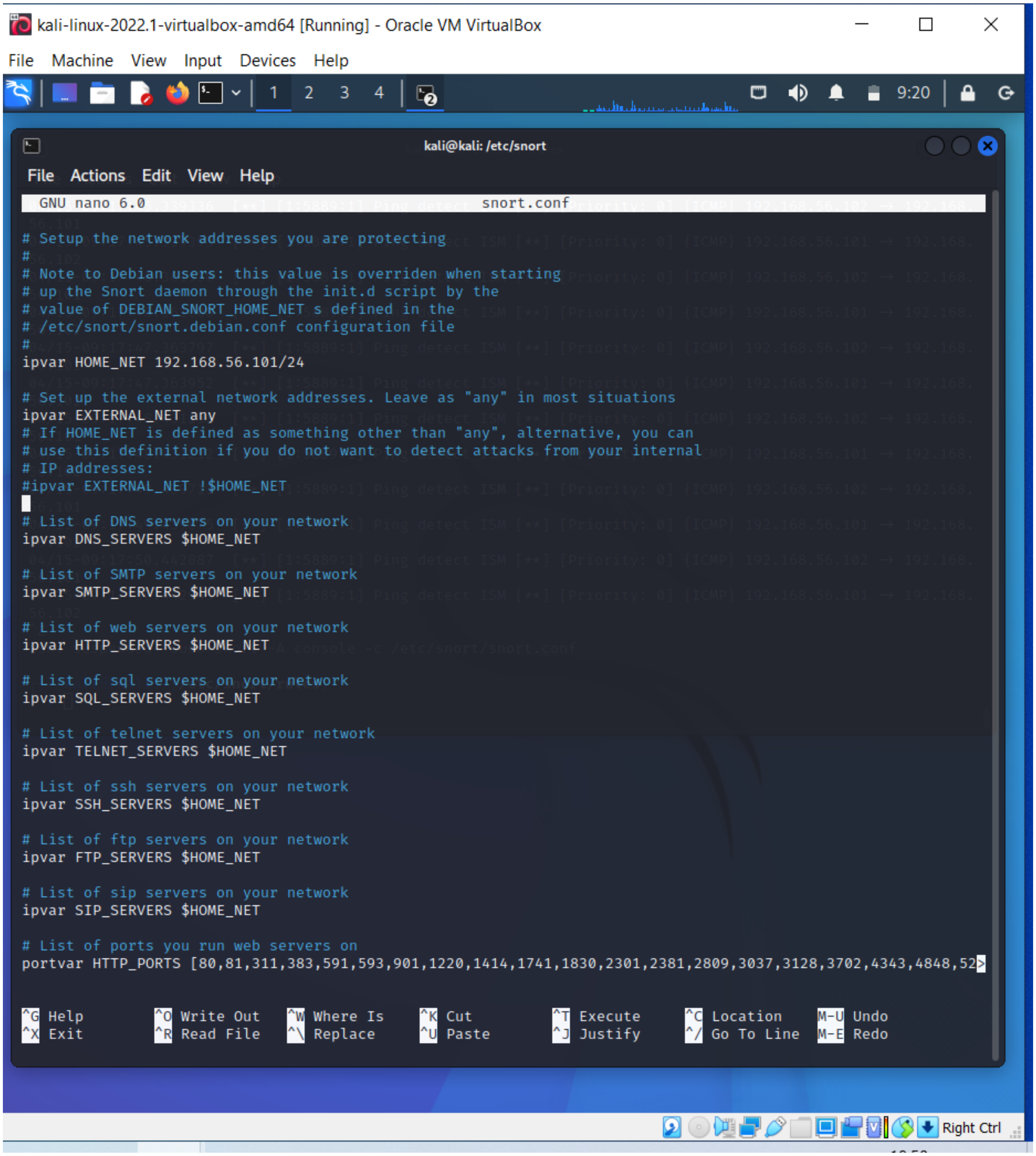
Pinging on kali system from ubuntu system


Ubuntu20.04 [Running] - Oracle VM VirtualBox
Activities
Terminal
Apr 15 16:39
shivangi@shivangi-VirtualBox: ~
kali-linux-2022.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
9:18
kali@kali: /etc/snort/rules
File Actions Edit View Help
Right Ctrl

```
Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
shivangi@shivangi-VirtualBox:~$
shivangi@shivangi-VirtualBox:~$
shivangi@shivangi-VirtualBox:~$ nmap 192.168.56.101
Starting Nmap 7.80 ( https://nmap.org ) at 2022-04-15 16:38 IST
Nmap scan report for 192.168.56.101
Host is up (0.00045s latency).
All 1000 scanned ports on 192.168.56.101 are closed

Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds
shivangi@shivangi-VirtualBox:~$ 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=0.648 ms
64 bytes from 192.168.56.101: icmp_seq=2 ttl=64 time=0.828 ms
64 bytes from 192.168.56.101: icmp_seq=3 ttl=64 time=1.15 ms
64 bytes from 192.168.56.101: icmp_seq=4 ttl=64 time=1.07 ms
64 bytes from 192.168.56.101: icmp_seq=5 ttl=64 time=1.13 ms
64 bytes from 192.168.56.101: icmp_seq=6 ttl=64 time=1.19 ms
64 bytes from 192.168.56.101: icmp_seq=7 ttl=64 time=1.21 ms
64 bytes from 192.168.56.101: icmp_seq=8 ttl=64 time=1.19 ms
64 bytes from 192.168.56.101: icmp_seq=9 ttl=64 time=1.26 ms
64 bytes from 192.168.56.101: icmp_seq=10 ttl=64 time=1.45 ms
64 bytes from 192.168.56.101: icmp_seq=11 ttl=64 time=1.25 ms
64 bytes from 192.168.56.101: icmp_seq=12 ttl=64 time=1.17 ms
64 bytes from 192.168.56.101: icmp_seq=13 ttl=64 time=1.66 ms
64 bytes from 192.168.56.101: icmp_seq=14 ttl=64 time=1.17 ms
^Z
[2]+  Stopped                 ping 192.168.56.101
shivangi@shivangi-VirtualBox:~$ 
```

```
04/15-09:17:37.185546  [**] [1:5889:1] Ping detect ISM [**] [Priority: 0] {ICMP} 192.168.56.102 → 192.168.
56.101
04/15-09:17:37.185582  [**] [1:5889:1] Ping detect ISM [**] [Priority: 0] {ICMP} 192.168.56.101 → 192.168.
56.102
04/15-09:17:38.224835  [**] [1:5889:1] Ping detect ISM [**] [Priority: 0] {ICMP} 192.168.56.102 → 192.168.
56.101
04/15-09:17:38.224872  [**] [1:5889:1] Ping detect ISM [**] [Priority: 0] {ICMP} 192.168.56.101 → 192.168.
56.102
04/15-09:17:39.275301  [**] [1:5889:1] Ping detect ISM [**] [Priority: 0] {ICMP} 192.168.56.102 → 192.168.
56.101
04/15-09:17:39.275359  [**] [1:5889:1] Ping detect ISM [**] [Priority: 0] {ICMP} 192.168.56.101 → 192.168.
56.102
04/15-09:17:40.279700  [**] [1:5889:1] Ping detect ISM [**] [Priority: 0] {ICMP} 192.168.56.102 → 192.168.
56.101
04/15-09:17:40.279757  [**] [1:5889:1] Ping detect ISM [**] [Priority: 0] {ICMP} 192.168.56.101 → 192.168.
56.102
04/15-09:17:41.282984  [**] [1:5889:1] Ping detect ISM [**] [Priority: 0] {ICMP} 192.168.56.102 → 192.168.
56.101
04/15-09:17:41.283040  [**] [1:5889:1] Ping detect ISM [**] [Priority: 0] {ICMP} 192.168.56.101 → 192.168.
56.102
04/15-09:17:42.305244  [**] [1:5889:1] Ping detect ISM [**] [Priority: 0] {ICMP} 192.168.56.102 → 192.168.
56.101
04/15-09:17:42.305349  [**] [1:5889:1] Ping detect ISM [**] [Priority: 0] {ICMP} 192.168.56.101 → 192.168.
56.102
04/15-09:17:43.319495  [**] [1:5889:1] Ping detect ISM [**] [Priority: 0] {ICMP} 192.168.56.102 → 192.168.
56.101
04/15-09:17:43.319544  [**] [1:5889:1] Ping detect ISM [**] [Priority: 0] {ICMP} 192.168.56.101 → 192.168.
56.102
04/15-09:17:44.337037  [**] [1:5889:1] Ping detect ISM [**] [Priority: 0] {ICMP} 192.168.56.102 → 192.168.
56.101
04/15-09:17:44.337094  [**] [1:5889:1] Ping detect ISM [**] [Priority: 0] {ICMP} 192.168.56.101 → 192.168.
56.102
04/15-09:17:45.339336  [**] [1:5889:1] Ping detect ISM [**] [Priority: 0] {ICMP} 192.168.56.102 → 192.168.
56.101
04/15-09:17:45.339393  [**] [1:5889:1] Ping detect ISM [**] [Priority: 0] {ICMP} 192.168.56.101 → 192.168.
56.102
04/15-09:17:46.361550  [**] [1:5889:1] Ping detect ISM [**] [Priority: 0] {ICMP} 192.168.56.102 → 192.168.
56.101
04/15-09:17:46.361608  [**] [1:5889:1] Ping detect ISM [**] [Priority: 0] {ICMP} 192.168.56.101 → 192.168.
56.102
04/15-09:17:47.363797  [**] [1:5889:1] Ping detect ISM [**] [Priority: 0] {ICMP} 192.168.56.102 → 192.168.
56.101
04/15-09:17:47.363952  [**] [1:5889:1] Ping detect ISM [**] [Priority: 0] {ICMP} 192.168.56.101 → 192.168.
56.102
04/15-09:17:48.431156  [**] [1:5889:1] Ping detect ISM [**] [Priority: 0] {ICMP} 192.168.56.102 → 192.168.
56.101
```

Making necessary HOME_NET changes in snort.conf file


kali-linux-2022.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
9:20
kali@kali: /etc/snort
File Actions Edit View Help
Right Ctrl

```
  GNU nano 6.0                                      snort.conf

# 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 192.168.56.101/24

# 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

# 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

# List of ports you run web servers on
portvar HTTP_PORTS [80,81,311,383,591,593,901,1220,1414,1741,1830,2301,2381,2809,3037,3128,3702,4343,4848,52>

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