CSCI 400 - Lab 5

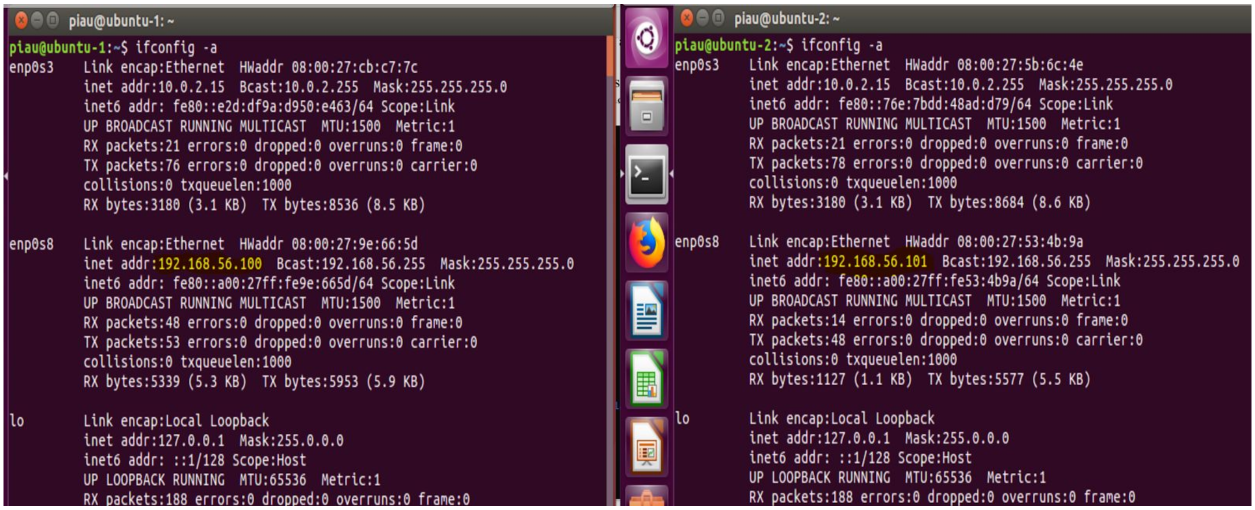
Prof. Faheem Abdur-Razzaaq

October 4, 2019

(Priya Thapa, Emranul Hakim, Lakpa S. Sherpa, Raul Nistor)

Intrusion Detection

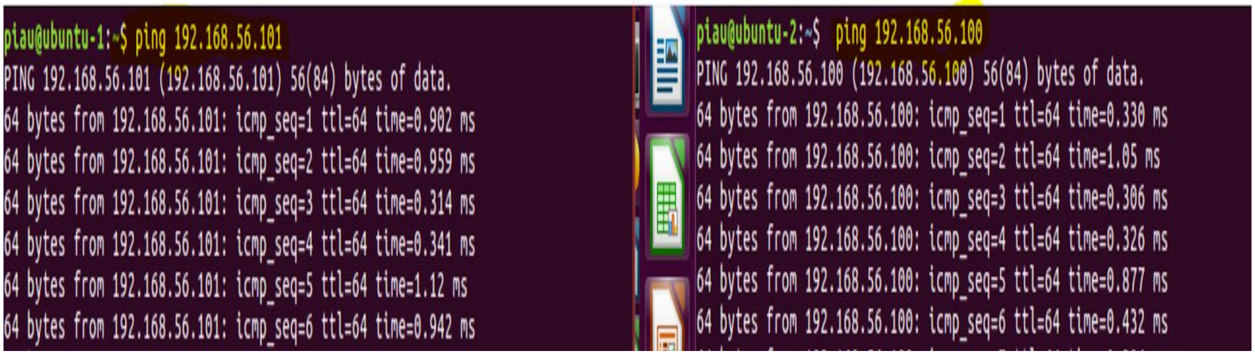
Setting up a Virtual Network



```
piau@ubuntu-1: ~
piau@ubuntu-1:~$ ifconfig -a
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:cb:c7:7c
          inet addr:10.0.2.15  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::e2d:df9a:d950:e463/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:21 errors:0 dropped:0 overruns:0 frame:0
          TX packets:76 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3180 (3.1 KB)  TX bytes:8536 (8.5 KB)

enp0s8    Link encap:Ethernet  HWaddr 08:00:27:9e:66:5d
          inet addr:192.168.56.100  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe9e:665d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:48 errors:0 dropped:0 overruns:0 frame:0
          TX packets:53 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5339 (5.3 KB)  TX bytes:5953 (5.9 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:188 errors:0 dropped:0 overruns:0 frame:0
```

```
piau@ubuntu-2: ~
piau@ubuntu-2:~$ ifconfig -a
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:5b:6c:4e
          inet addr:10.0.2.15  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::76e:7bdd:48ad:d79/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:21 errors:0 dropped:0 overruns:0 frame:0
          TX packets:78 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3180 (3.1 KB)  TX bytes:8684 (8.6 KB)

enp0s8    Link encap:Ethernet  HWaddr 08:00:27:53:4b:9a
          inet addr:192.168.56.101  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe53:4b9a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:14 errors:0 dropped:0 overruns:0 frame:0
          TX packets:48 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1127 (1.1 KB)  TX bytes:5577 (5.5 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:188 errors:0 dropped:0 overruns:0 frame:0
```

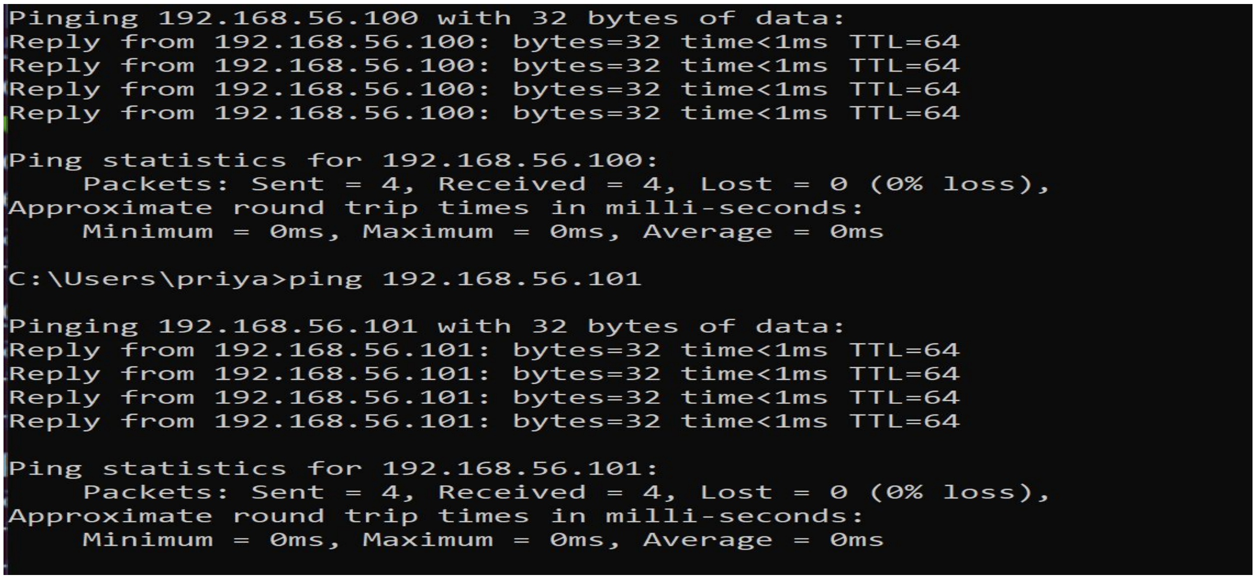
Internal Network Testing



```
piau@ubuntu-1:~$ 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=0.902 ms
64 bytes from 192.168.56.101: icmp_seq=2 ttl=64 time=0.959 ms
64 bytes from 192.168.56.101: icmp_seq=3 ttl=64 time=0.314 ms
64 bytes from 192.168.56.101: icmp_seq=4 ttl=64 time=0.341 ms
64 bytes from 192.168.56.101: icmp_seq=5 ttl=64 time=1.12 ms
64 bytes from 192.168.56.101: icmp_seq=6 ttl=64 time=0.942 ms
```

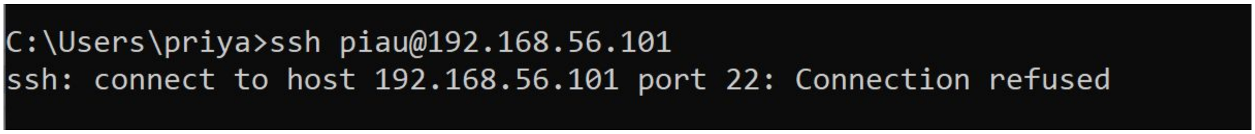
```
piau@ubuntu-2:~$ ping 192.168.56.100
PING 192.168.56.100 (192.168.56.100) 56(84) bytes of data.
64 bytes from 192.168.56.100: icmp_seq=1 ttl=64 time=0.330 ms
64 bytes from 192.168.56.100: icmp_seq=2 ttl=64 time=1.05 ms
64 bytes from 192.168.56.100: icmp_seq=3 ttl=64 time=0.306 ms
64 bytes from 192.168.56.100: icmp_seq=4 ttl=64 time=0.326 ms
64 bytes from 192.168.56.100: icmp_seq=5 ttl=64 time=0.877 ms
64 bytes from 192.168.56.100: icmp_seq=6 ttl=64 time=0.432 ms
```

Host connection with Virtual Network

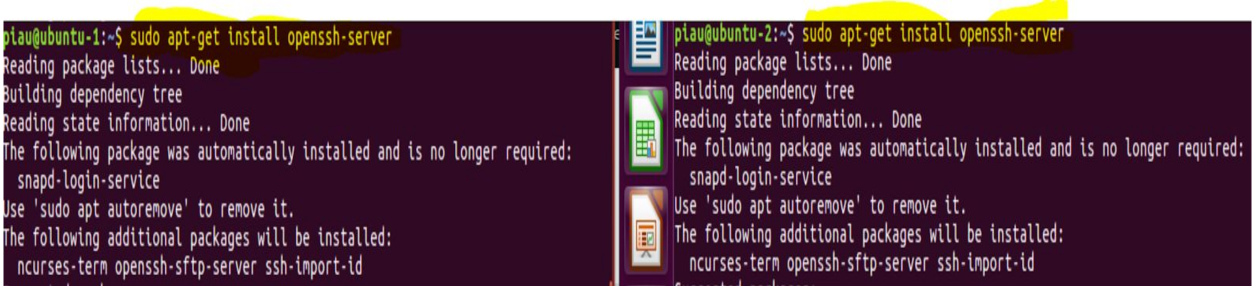


```
Pinging 192.168.56.100 with 32 bytes of data:
Reply from 192.168.56.100: bytes=32 time<1ms TTL=64
Reply from 192.168.56.100: bytes=32 time<1ms TTL=64
Reply from 192.168.56.100: bytes=32 time<1ms TTL=64
Reply from 192.168.56.100: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.56.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\priya>ping 192.168.56.101

Pinging 192.168.56.101 with 32 bytes of data:
Reply from 192.168.56.101: bytes=32 time<1ms TTL=64
Reply from 192.168.56.101: bytes=32 time<1ms TTL=64
Reply from 192.168.56.101: bytes=32 time<1ms TTL=64
Reply from 192.168.56.101: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.56.101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

We want to SSH into the virtual machines but it was not a success due to not installation of ssh in virtual machines.

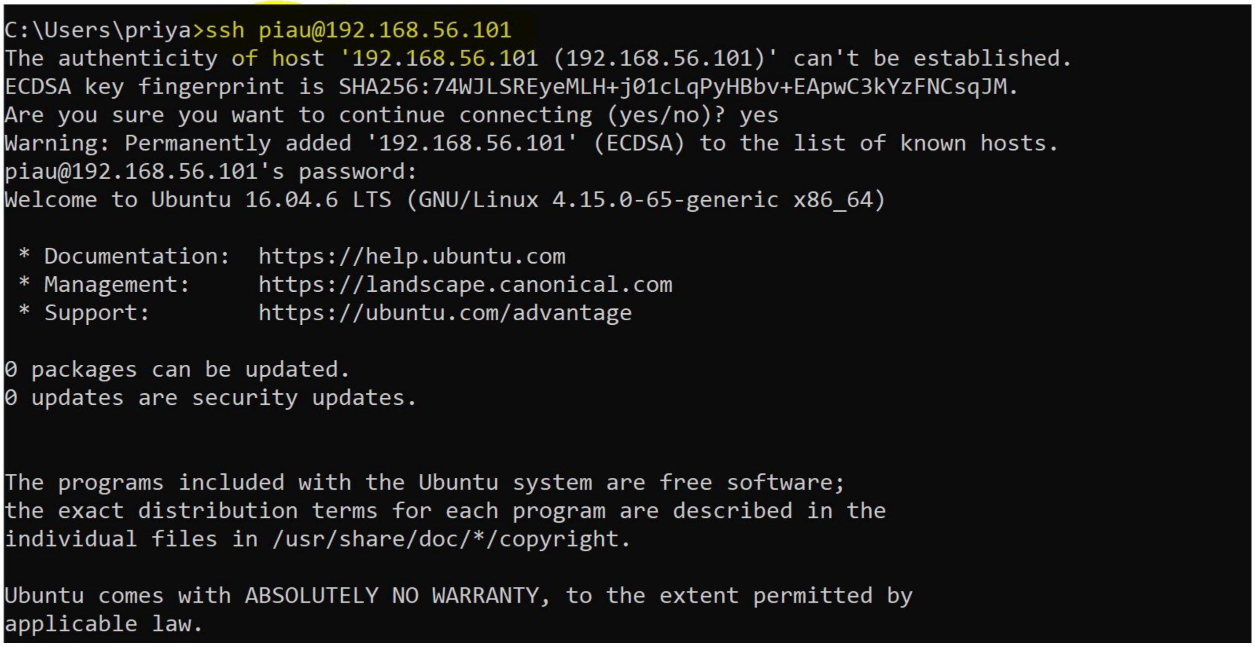


```
C:\Users\priya>ssh piau@192.168.56.101
ssh: connect to host 192.168.56.101 port 22: Connection refused
```



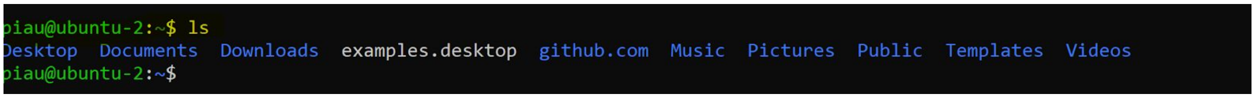
```
piau@ubuntu-1:~$ sudo apt-get install openssh-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required:
  snapd-login-service
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  ncurses-term openssh-sftp-server ssh-import-id
```

```
piau@ubuntu-2:~$ sudo apt-get install openssh-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required:
  snapd-login-service
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  ncurses-term openssh-sftp-server ssh-import-id
```



```
C:\Users\priya>ssh piau@192.168.56.101
The authenticity of host '192.168.56.101 (192.168.56.101)' can't be established.
ECDSA key fingerprint is SHA256:74WJLSREyeMLH+j01cLqPyHBbv+EApwC3kYzFNCsqJM.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.56.101' (ECDSA) to the list of known hosts.
piau@192.168.56.101's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.15.0-65-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

0 packages can be updated.
0 updates are security updates.


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
```

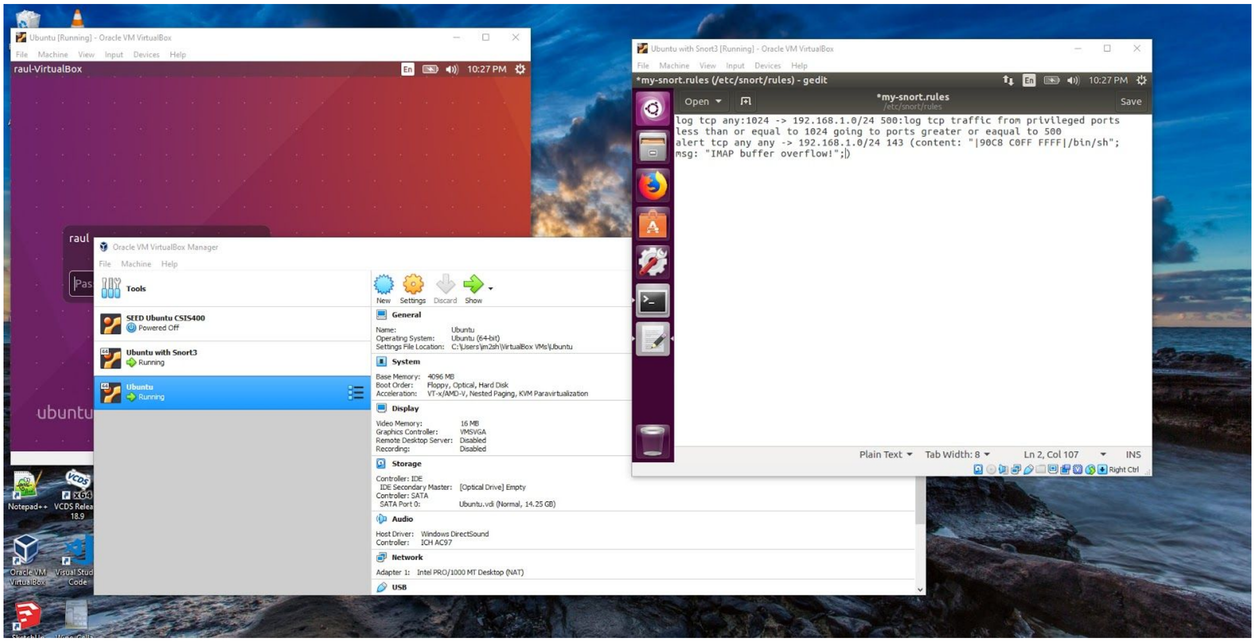
Host got access to virtual machine: (SSH)



```
piau@ubuntu-2:~$ ls
Desktop  Documents  Downloads  examples.desktop  github.com  Music  Pictures  Public  Templates  Videos
piau@ubuntu-2:~$
```

RAUL

This images show the implementation of custom set of rules



*my-snort.rules (/etc/snort/rules) - gedit

```
log tcp any:1024 -> 192.168.1.0/24 500:log tcp traffic from privileged ports
less than or equal to 1024 going to ports greater or eaqual to 500
alert tcp any any -> 192.168.1.0/24 143 (content: "|90C8 C0FF FFFF|/bin/sh";
msg: "IMAP buffer overflow!";)
```

Oracle VM VirtualBox Manager

SEED Ubuntu CSIS400 — Powered Off
Ubuntu with Snort3 — Running
Ubuntu — Running

General
Name: Ubuntu
Operating System: Ubuntu (64-bit)
Settings File Location: C:\Users\m2sh\VirtualBox VMs\Ubuntu

System
Base Memory: 4096 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging, KVM Paravirtualization

Display
Video Memory: 16 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled

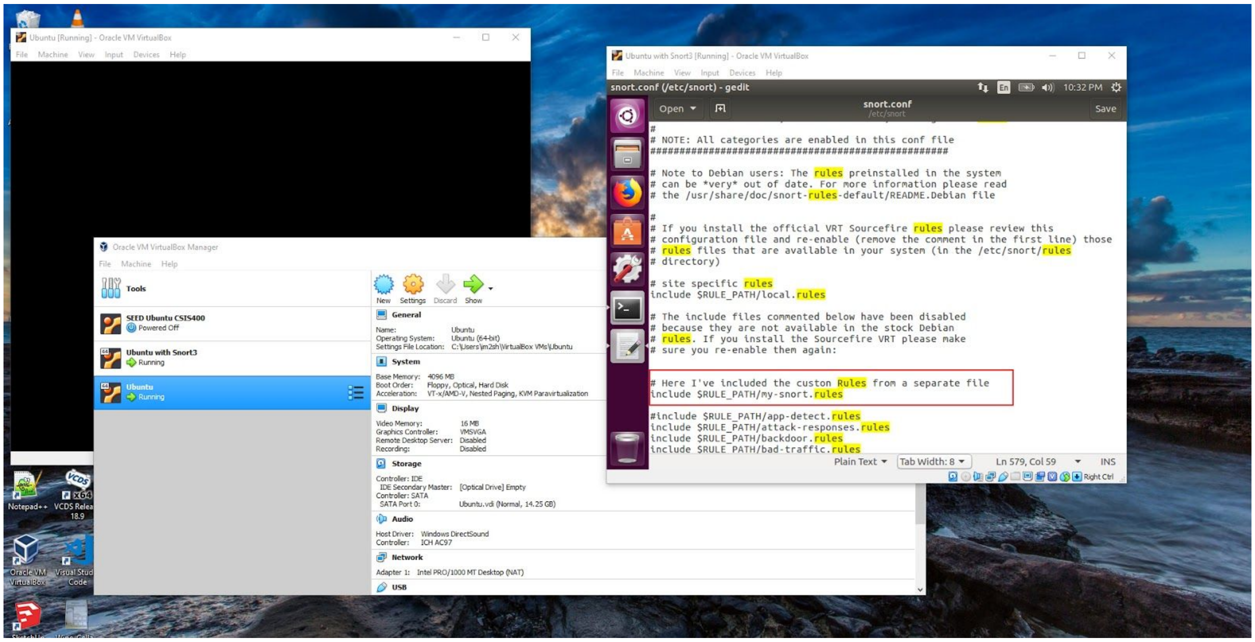
Storage
Controller: IDE
IDE Secondary Master: [Optical Drive] Empty
Controller: SATA
SATA Port 0: Ubuntu.vdi (Normal, 14.25 GB)

Audio
Host Driver: Windows DirectSound
Controller: ICH AC97

Network
Adapter 1: Intel PRO/1000 MT Desktop (NAT)

USB

Ubuntu [Running] - Oracle VM VirtualBox
Ubuntu with Snort3 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
raul-VirtualBox
10:27 PM
Open
Save
Plain Text
Tab Width: 8
Ln 2, Col 107
INS
Right Ctrl
Tools
New
Settings
Discard
Show



snort.conf (/etc/snort) - gedit

```
#
# NOTE: All categories are enabled in this conf file
###################################################

# Note to Debian users: The rules preinstalled in the system
# can be *very* out of date. For more information please read
# the /usr/share/doc/snort-rules-default/README.Debian file

#
# If you install the official VRT Sourcefire rules please review this
# configuration file and re-enable (remove the comment in the first line) those
# rules files that are available in your system (in the /etc/snort/rules
# directory)

# site specific rules
include $RULE_PATH/local.rules

# The include files commented below have been disabled
# because they are not available in the stock Debian
# rules. If you install the Sourcefire VRT please make
# sure you re-enable them again:

# Here I've included the custon Rules from a separate file
include $RULE_PATH/my-snort.rules

#include $RULE_PATH/app-detect.rules
include $RULE_PATH/attack-responses.rules
include $RULE_PATH/backdoor.rules
include $RULE_PATH/bad-traffic.rules
```

Oracle VM VirtualBox Manager

SEED Ubuntu CSIS400 — Powered Off
Ubuntu with Snort3 — Running
Ubuntu — Running

General
Name: Ubuntu
Operating System: Ubuntu (64-bit)
Settings File Location: C:\Users\m2sh\VirtualBox VMs\Ubuntu

System
Base Memory: 4096 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging, KVM Paravirtualization

Display
Video Memory: 16 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage
Controller: IDE
IDE Secondary Master: [Optical Drive] Empty
Controller: SATA
SATA Port 0: Ubuntu.vdi (Normal, 14.25 GB)

Audio
Host Driver: Windows DirectSound
Controller: ICH AC97

Network
Adapter 1: Intel PRO/1000 MT Desktop (NAT)

USB

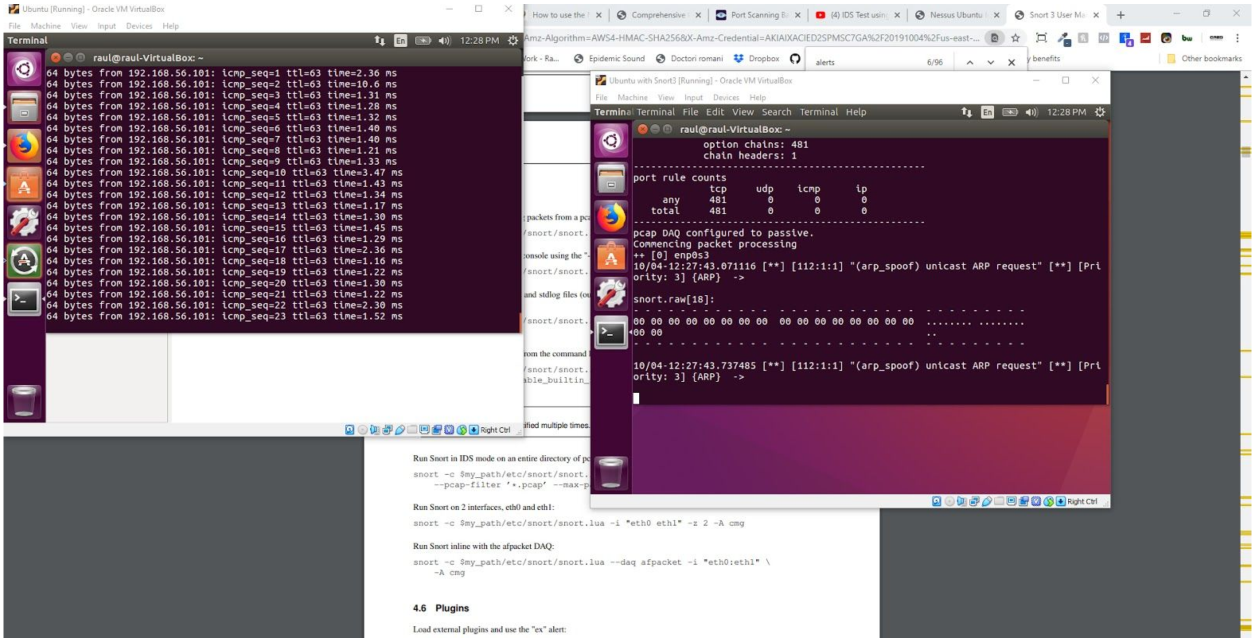
Ubuntu [Running] - Oracle VM VirtualBox
Ubuntu with Snort3 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
10:32 PM
Open
Save
Plain Text
Tab Width: 8
Ln 579, Col 59
INS
Right Ctrl

In the next set of images I ran the command:

sudo snort -c /usr/local/etc/snort/snort.lua -i enp0s3 -A cmg, on the Snort Environment to start detecting any incoming traffic, and

ping 192.168.56.101, on the Nmap Environment to start transmitting packets.

Snort was able to detect right away the packs coming through enp0s3 adapter.


Ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
12:28 PM
raul@raul-VirtualBox: ~
Ubuntu with Snort3 [Running] - Oracle VM VirtualBox
Terminal File Edit View Search Terminal Help
alerts 6/96
Right Ctrl

```
64 bytes from 192.168.56.101: icmp_seq=1 ttl=63 time=2.36 ms
64 bytes from 192.168.56.101: icmp_seq=2 ttl=63 time=10.6 ms
64 bytes from 192.168.56.101: icmp_seq=3 ttl=63 time=1.31 ms
64 bytes from 192.168.56.101: icmp_seq=4 ttl=63 time=1.28 ms
64 bytes from 192.168.56.101: icmp_seq=5 ttl=63 time=1.32 ms
64 bytes from 192.168.56.101: icmp_seq=6 ttl=63 time=1.40 ms
64 bytes from 192.168.56.101: icmp_seq=7 ttl=63 time=1.40 ms
64 bytes from 192.168.56.101: icmp_seq=8 ttl=63 time=1.21 ms
64 bytes from 192.168.56.101: icmp_seq=9 ttl=63 time=1.33 ms
64 bytes from 192.168.56.101: icmp_seq=10 ttl=63 time=3.47 ms
64 bytes from 192.168.56.101: icmp_seq=11 ttl=63 time=1.43 ms
64 bytes from 192.168.56.101: icmp_seq=12 ttl=63 time=1.34 ms
64 bytes from 192.168.56.101: icmp_seq=13 ttl=63 time=1.17 ms
64 bytes from 192.168.56.101: icmp_seq=14 ttl=63 time=1.30 ms
64 bytes from 192.168.56.101: icmp_seq=15 ttl=63 time=1.45 ms
64 bytes from 192.168.56.101: icmp_seq=16 ttl=63 time=1.29 ms
64 bytes from 192.168.56.101: icmp_seq=17 ttl=63 time=2.36 ms
64 bytes from 192.168.56.101: icmp_seq=18 ttl=63 time=1.16 ms
64 bytes from 192.168.56.101: icmp_seq=19 ttl=63 time=1.22 ms
64 bytes from 192.168.56.101: icmp_seq=20 ttl=63 time=1.30 ms
64 bytes from 192.168.56.101: icmp_seq=21 ttl=63 time=1.22 ms
64 bytes from 192.168.56.101: icmp_seq=22 ttl=63 time=2.30 ms
64 bytes from 192.168.56.101: icmp_seq=23 ttl=63 time=1.52 ms
```

```
            option chains: 481
            chain headers: 1
--------------------------------------------------
port rule counts
             tcp     udp    icmp      ip
     any     481       0       0       0
   total     481       0       0       0
--------------------------------------------------
pcap DAQ configured to passive.
Commencing packet processing
++ [0] enp0s3
10/04-12:27:43.071116 [**] [112:1:1] "(arp_spoof) unicast ARP request" [**] [Pri
ority: 3] {ARP}  ->

snort.raw[18]:
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ........ ........
00 00                                             ..
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

10/04-12:27:43.737485 [**] [112:1:1] "(arp_spoof) unicast ARP request" [**] [Pri
ority: 3] {ARP}  ->
```

Run Snort in IDS mode on an entire directory of pc

```
snort -c $my_path/etc/snort/snort.
    --pcap-filter '*.pcap' --max-p
```

Run Snort on 2 interfaces, eth0 and eth1:

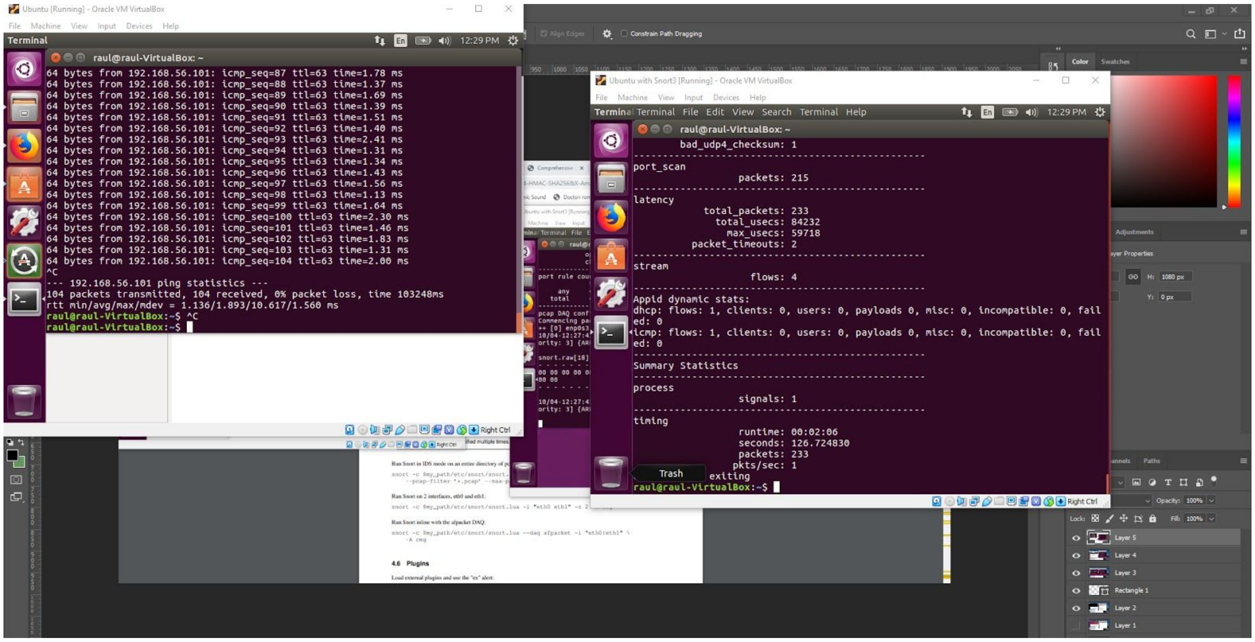
```
snort -c $my_path/etc/snort/snort.lua -i "eth0 eth1" -z 2 -A cmg
```

Run Snort inline with the afpacket DAQ:

```
snort -c $my_path/etc/snort/snort.lua --daq afpacket -i "eth0:eth1" \
    -A cmg
```

4.6 Plugins

Load external plugins and use the "ex" alert:


Ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
12:29 PM
raul@raul-VirtualBox: ~
Ubuntu with Snort3 [Running] - Oracle VM VirtualBox
Terminal File Edit View Search Terminal Help
Constrain Path Dragging
Color Swatches
Trash
Layer 5
Layer 4
Layer 3
Rectangle 1
Layer 2
Layer 1
Right Ctrl

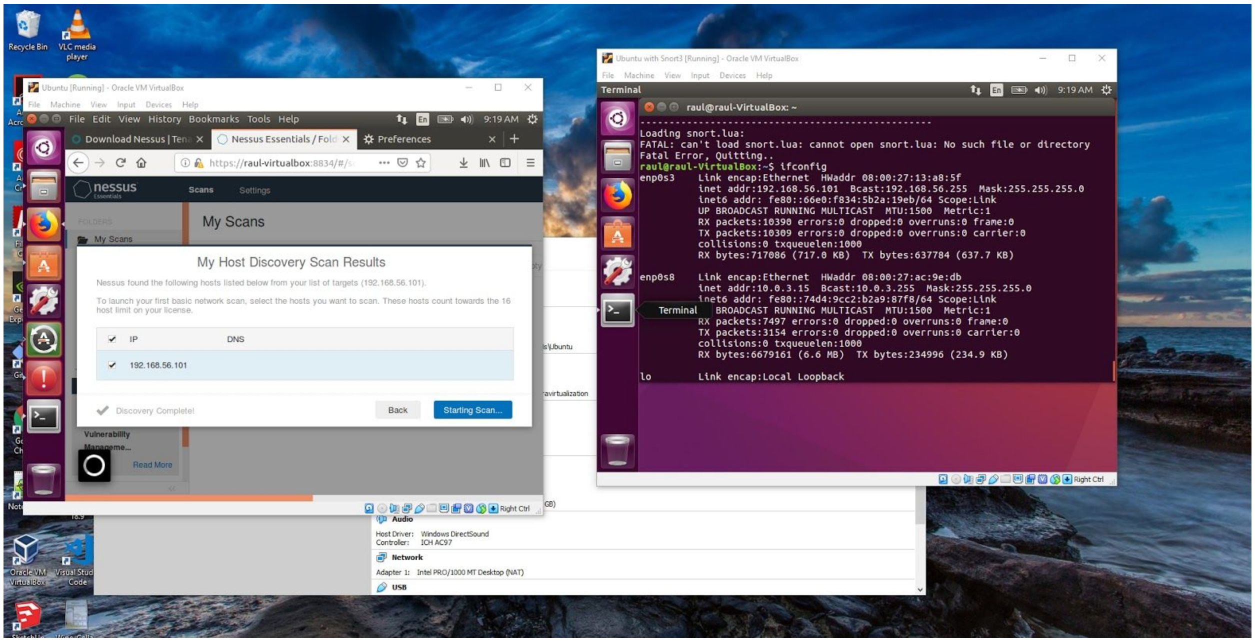
```
64 bytes from 192.168.56.101: icmp_seq=87 ttl=63 time=1.78 ms
64 bytes from 192.168.56.101: icmp_seq=88 ttl=63 time=1.37 ms
64 bytes from 192.168.56.101: icmp_seq=89 ttl=63 time=1.69 ms
64 bytes from 192.168.56.101: icmp_seq=90 ttl=63 time=1.39 ms
64 bytes from 192.168.56.101: icmp_seq=91 ttl=63 time=1.51 ms
64 bytes from 192.168.56.101: icmp_seq=92 ttl=63 time=1.40 ms
64 bytes from 192.168.56.101: icmp_seq=93 ttl=63 time=2.41 ms
64 bytes from 192.168.56.101: icmp_seq=94 ttl=63 time=1.31 ms
64 bytes from 192.168.56.101: icmp_seq=95 ttl=63 time=1.34 ms
64 bytes from 192.168.56.101: icmp_seq=96 ttl=63 time=1.43 ms
64 bytes from 192.168.56.101: icmp_seq=97 ttl=63 time=1.56 ms
64 bytes from 192.168.56.101: icmp_seq=98 ttl=63 time=1.13 ms
64 bytes from 192.168.56.101: icmp_seq=99 ttl=63 time=1.64 ms
64 bytes from 192.168.56.101: icmp_seq=100 ttl=63 time=2.30 ms
64 bytes from 192.168.56.101: icmp_seq=101 ttl=63 time=1.46 ms
64 bytes from 192.168.56.101: icmp_seq=102 ttl=63 time=1.83 ms
64 bytes from 192.168.56.101: icmp_seq=103 ttl=63 time=1.31 ms
64 bytes from 192.168.56.101: icmp_seq=104 ttl=63 time=2.00 ms
^C
--- 192.168.56.101 ping statistics ---
104 packets transmitted, 104 received, 0% packet loss, time 103248ms
rtt min/avg/max/mdev = 1.136/1.893/10.617/1.560 ms
raul@raul-VirtualBox:~$ ^C
raul@raul-VirtualBox:~$
```

```
        bad_udp4_checksum: 1
--------------------------------------------------
port_scan
                  packets: 215
--------------------------------------------------
latency
            total_packets: 233
              total_usecs: 84232
                max_usecs: 59718
          packet_timeouts: 2
--------------------------------------------------
stream
                    flows: 4
--------------------------------------------------
Appid dynamic stats:
dhcp: flows: 1, clients: 0, users: 0, payloads 0, misc: 0, incompatible: 0, fail
ed: 0
icmp: flows: 1, clients: 0, users: 0, payloads 0, misc: 0, incompatible: 0, fail
ed: 0
--------------------------------------------------
Summary Statistics
--------------------------------------------------
process
                  signals: 1
--------------------------------------------------
timing
                  runtime: 00:02:06
                  seconds: 126.724830
                  packets: 233
                 pkts/sec: 1
o")~ exiting
raul@raul-VirtualBox:~$
```

In the next set of images I ran the command:

sudo nmap -O --osscan-guess 192.168.56.101 which is the Snort Host Environment
sudo nmap -O --osscan-guess 10.0.2.15 which is the OSSEC HIDS Environment

On the OSSEC HIDS Environment it detected Linux as OS, but for the Snort Environment id did not detect the correct OS.


Ubuntu [Running] - Oracle VM VirtualBox
File Edit View History Bookmarks Tools Help
9:19 AM
Download Nessus | Tena
Nessus Essentials / Fold
Preferences
https://raul-virtualbox:8834/#/s
nessus Essentials
Scans
Settings
FOLDERS
My Scans
Vulnerability Manageme...
Read More
Ubuntu with Snort3 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
Right Ctrl
Audio
Network
USB

My Scans

My Host Discovery Scan Results

Nessus found the following hosts listed below from your list of targets (192.168.56.101).

To launch your first basic network scan, select the hosts you want to scan. These hosts count towards the 16 host limit on your license.

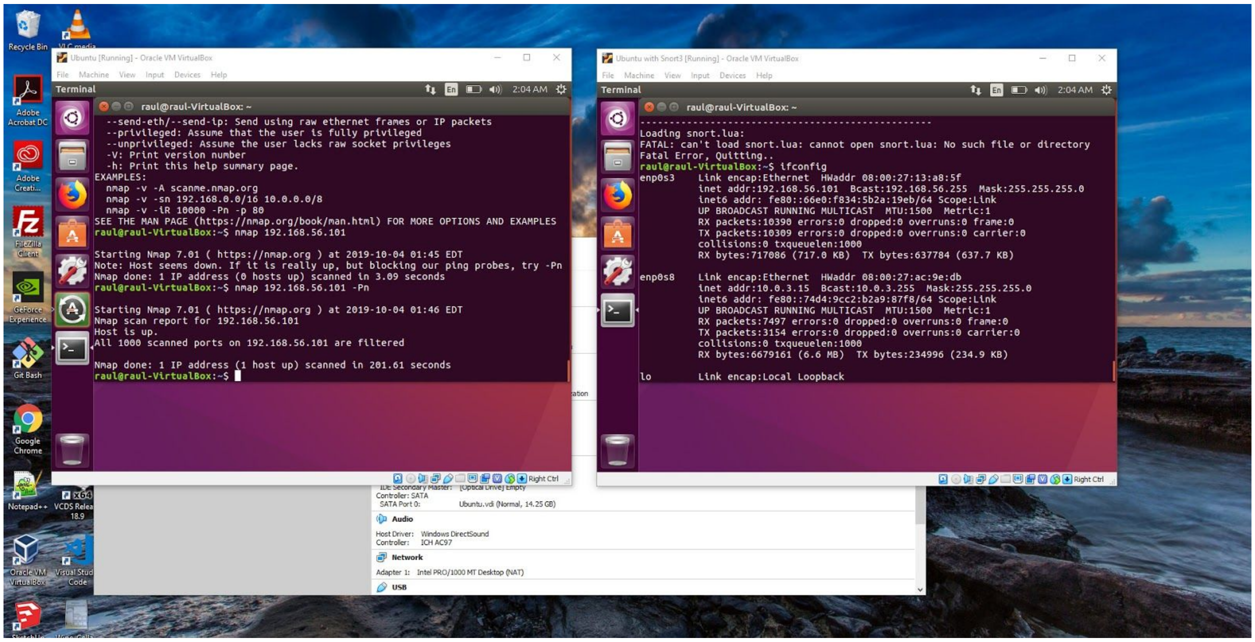
☑	IP	DNS
☑	192.168.56.101	

✓ Discovery Complete! Back Starting Scan...

Host Driver: Windows DirectSound
Controller: ICH AC97

Adapter 1: Intel PRO/1000 MT Desktop (NAT)

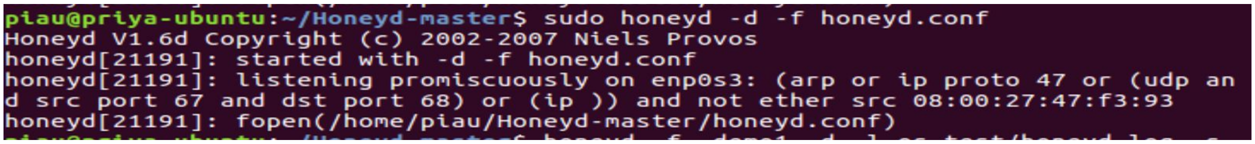
```
raul@raul-VirtualBox: ~
--------------------------------------------------
Loading snort.lua:
FATAL: can't load snort.lua: cannot open snort.lua: No such file or directory
Fatal Error, Quitting..
raul@raul-VirtualBox:~$ ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:13:a8:5f
          inet addr:192.168.56.101  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::66e0:f834:5b2a:19eb/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:10390 errors:0 dropped:0 overruns:0 frame:0
          TX packets:10309 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:717086 (717.0 KB)  TX bytes:637784 (637.7 KB)

enp0s8    Link encap:Ethernet  HWaddr 08:00:27:ac:9e:db
          inet addr:10.0.3.15  Bcast:10.0.3.255  Mask:255.255.255.0
          inet6 addr: fe80::74d4:9cc2:b2a9:87f8/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:7497 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3154 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:6679161 (6.6 MB)  TX bytes:234996 (234.9 KB)

lo        Link encap:Local Loopback
```


Ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
2:04 AM
Ubuntu with Snort3 [Running] - Oracle VM VirtualBox
Right Ctrl
Audio
Network
USB

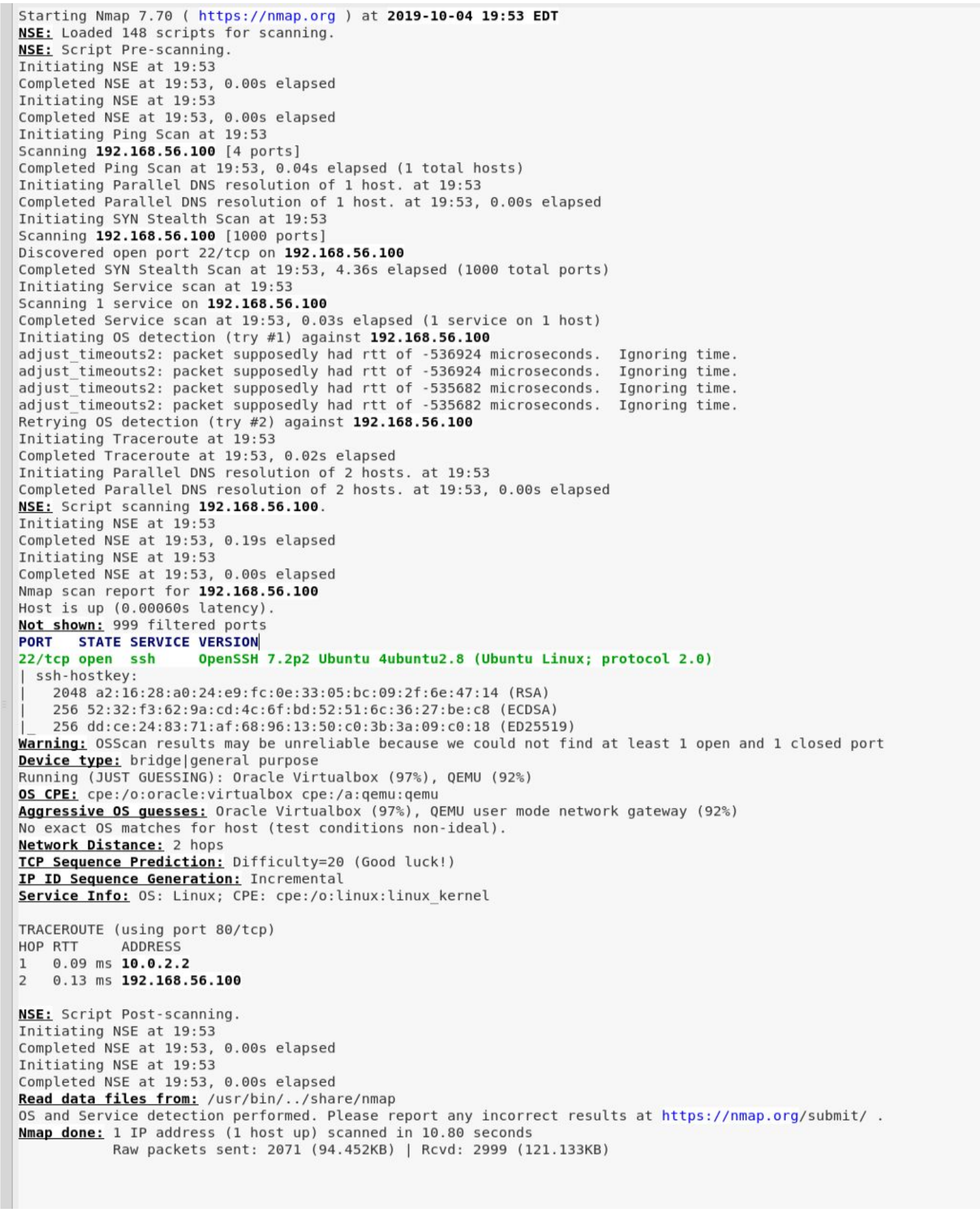
```
raul@raul-VirtualBox: ~
  --send-eth/--send-ip: Send using raw ethernet frames or IP packets
  --privileged: Assume that the user is fully privileged
  --unprivileged: Assume the user lacks raw socket privileges
  -V: Print version number
  -h: Print this help summary page.
EXAMPLES:
  nmap -v -A scanme.nmap.org
  nmap -v -sn 192.168.0.0/16 10.0.0.0/8
  nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
raul@raul-VirtualBox:~$ nmap 192.168.56.101

Starting Nmap 7.01 ( https://nmap.org ) at 2019-10-04 01:45 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 3.09 seconds
raul@raul-VirtualBox:~$ nmap 192.168.56.101 -Pn

Starting Nmap 7.01 ( https://nmap.org ) at 2019-10-04 01:46 EDT
Nmap scan report for 192.168.56.101
Host is up.
All 1000 scanned ports on 192.168.56.101 are filtered

Nmap done: 1 IP address (1 host up) scanned in 201.61 seconds
raul@raul-VirtualBox:~$
```

```
raul@raul-VirtualBox: ~
--------------------------------------------------
Loading snort.lua:
FATAL: can't load snort.lua: cannot open snort.lua: No such file or directory
Fatal Error, Quitting..
raul@raul-VirtualBox:~$ ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:13:a8:5f
          inet addr:192.168.56.101  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::66e0:f834:5b2a:19eb/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:10390 errors:0 dropped:0 overruns:0 frame:0
          TX packets:10309 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:717086 (717.0 KB)  TX bytes:637784 (637.7 KB)

enp0s8    Link encap:Ethernet  HWaddr 08:00:27:ac:9e:db
          inet addr:10.0.3.15  Bcast:10.0.3.255  Mask:255.255.255.0
          inet6 addr: fe80::74d4:9cc2:b2a9:87f8/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:7497 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3154 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:6679161 (6.6 MB)  TX bytes:234996 (234.9 KB)

lo        Link encap:Local Loopback
```

Honeyd:



```
piau@priya-ubuntu:~/Honeyd-master$ sudo honeyd -d -f honeyd.conf
Honeyd V1.6d Copyright (c) 2002-2007 Niels Provos
honeyd[21191]: started with -d -f honeyd.conf
honeyd[21191]: listening promiscuously on enp0s3: (arp or ip proto 47 or (udp an
d src port 67 and dst port 68) or (ip )) and not ether src 08:00:27:47:f3:93
honeyd[21191]: fopen(/home/piau/Honeyd-master/honeyd.conf)
```



```
Starting Nmap 7.70 ( https://nmap.org ) at 2019-10-04 19:53 EDT
NSE: Loaded 148 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 19:53
Completed NSE at 19:53, 0.00s elapsed
Initiating NSE at 19:53
Completed NSE at 19:53, 0.00s elapsed
Initiating Ping Scan at 19:53
Scanning 192.168.56.100 [4 ports]
Completed Ping Scan at 19:53, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:53
Completed Parallel DNS resolution of 1 host. at 19:53, 0.00s elapsed
Initiating SYN Stealth Scan at 19:53
Scanning 192.168.56.100 [1000 ports]
Discovered open port 22/tcp on 192.168.56.100
Completed SYN Stealth Scan at 19:53, 4.36s elapsed (1000 total ports)
Initiating Service scan at 19:53
Scanning 1 service on 192.168.56.100
Completed Service scan at 19:53, 0.03s elapsed (1 service on 1 host)
Initiating OS detection (try #1) against 192.168.56.100
adjust_timeouts2: packet supposedly had rtt of -536924 microseconds.  Ignoring time.
adjust_timeouts2: packet supposedly had rtt of -536924 microseconds.  Ignoring time.
adjust_timeouts2: packet supposedly had rtt of -535682 microseconds.  Ignoring time.
adjust_timeouts2: packet supposedly had rtt of -535682 microseconds.  Ignoring time.
Retrying OS detection (try #2) against 192.168.56.100
Initiating Traceroute at 19:53
Completed Traceroute at 19:53, 0.02s elapsed
Initiating Parallel DNS resolution of 2 hosts. at 19:53
Completed Parallel DNS resolution of 2 hosts. at 19:53, 0.00s elapsed
NSE: Script scanning 192.168.56.100.
Initiating NSE at 19:53
Completed NSE at 19:53, 0.19s elapsed
Initiating NSE at 19:53
Completed NSE at 19:53, 0.00s elapsed
Nmap scan report for 192.168.56.100
Host is up (0.00060s latency).
Not shown: 999 filtered ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 a2:16:28:a0:24:e9:fc:0e:33:05:bc:09:2f:6e:47:14 (RSA)
|   256 52:32:f3:62:9a:cd:4c:6f:bd:52:51:6c:36:27:be:c8 (ECDSA)
|_  256 dd:ce:24:83:71:af:68:96:13:50:c0:3b:3a:09:c0:18 (ED25519)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge|general purpose
Running (JUST GUESSING): Oracle Virtualbox (97%), QEMU (92%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox (97%), QEMU user mode network gateway (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=20 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   0.09 ms 10.0.2.2
2   0.13 ms 192.168.56.100

NSE: Script Post-scanning.
Initiating NSE at 19:53
Completed NSE at 19:53, 0.00s elapsed
Initiating NSE at 19:53
Completed NSE at 19:53, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.80 seconds
           Raw packets sent: 2071 (94.452KB) | Rcvd: 2999 (121.133KB)
```