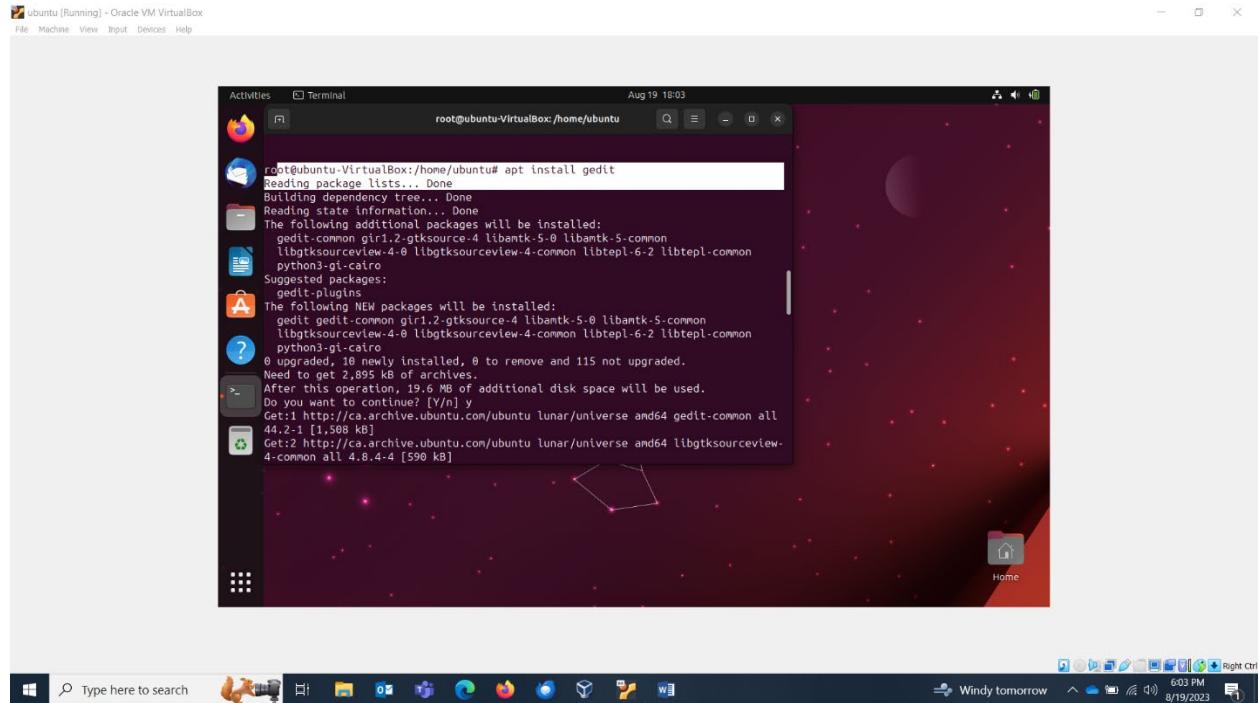


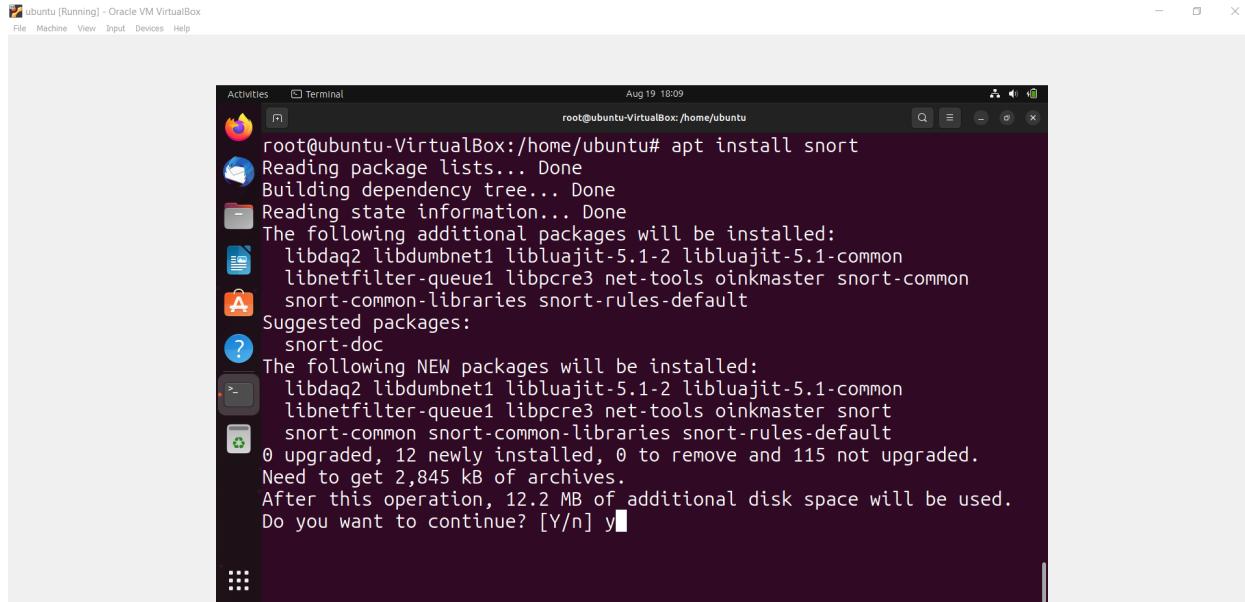
SNORT IN UBUNTU

I have installed ubuntu will full installation feature.

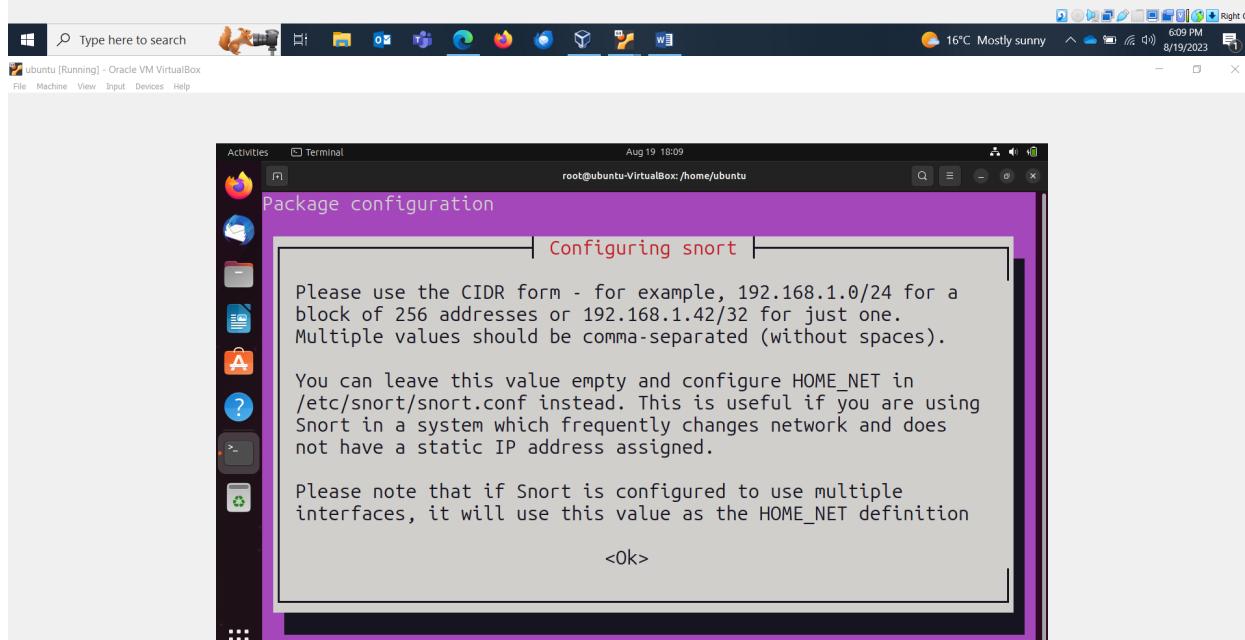
The adapter is enp0s3 & IP address is 192.168.1.78



INSTALLING SNORT:



```
Activities Terminal Aug 19 18:09
root@ubuntu-VirtualBox:/home/ubuntu# apt install snort
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libdaq2 libdumbnet1 libluajit-5.1-2 libluajit-5.1-common
  libnetfilter-queue1 libpcre3 net-tools oinkmaster snort-common
  snort-common-libraries snort-rules-default
Suggested packages:
  snort-doc
  The following NEW packages will be installed:
  libdaq2 libdumbnet1 libluajit-5.1-2 libluajit-5.1-common
  libnetfilter-queue1 libpcre3 net-tools oinkmaster snort
  snort-common snort-common-libraries snort-rules-default
0 upgraded, 12 newly installed, 0 to remove and 115 not upgraded.
Need to get 2,845 kB of archives.
After this operation, 12.2 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
```



Lets go to the configuration file in snort

Activities Terminal Aug 19 18:11 root@ubuntu-VirtualBox:/home/ubuntu# gedit /etc/snort/snort.conf

```
(gedit:3085): dconf-WARNING **: 18:11:18.671: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)
(gedit:3085): dconf-WARNING **: 18:11:18.671: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)
```

Type here to search 16°C Mostly sunny 6:11 PM 8/19/2023 Right Ctrl

Activities Gedit Aug 19 18:11 snort.conf /etc/snort.conf Save

```
1 #-----#
2 # VRT Rule Packages Snort.conf
3 #
4 # For more information visit us at:
5 # http://www.snort.org Snort Website
6 # http://vrt-blog.snort.org/ Sourcefire VRT Blog
7 #
8 # Mailing list Contact: snort-users@lists.snort.org
9 # False Positive reports: fp@sourcefire.com
10 # Snort bugs: bugs@snort.org
11 #
12 # Compatible with Snort Versions:
13 # VERSIONS : 2.9.15.1
14 #
15 # Snort build options:
16 # OPTIONS : --enable-gre --enable-mpls --enable-targetbased --enable-ppm --
17 # --enable-perfprofiling --enable-zlib --enable-active-response --enable-normalizer --
18 # --enable-reload --enable-react --enable-flexresp
19 #
20 # Additional information:
21 # This configuration file enables active response, to run snort in
22 # test mode -T you are required to supply an interface -i <interface>
23 # or test mode will fail to fully validate the configuration and
24 # exit with a FATAL error
25 ##### This file contains a sample snort configuration.
26 # You should take the following steps to create your own custom configuration:
27 #
28 # 1) Set the network variables.
```



Lets check the CIDR for home net.

The screenshot shows a Linux desktop environment with a terminal window open. The terminal window title is "snort.conf" and it shows the contents of the /etc/snort/snort.conf file. The file includes comments about the Debian init.d script and network variables. It defines HOME_NET as "any" and lists various DNS, SMTP, and HTTP servers. Two error messages are displayed on the right side of the terminal window: "commit changes (No such file)" repeated twice.

```
*snort.conf
/etc/snort
51 # The Debian init.d script is defined in such a way
52 # that you can run multiple instances.
53
54 ##### Step #1: Set the network variables. For more information, see README.variables
55 ##### If HOME_NET is defined as something other than "any", alternative, you can
56 # use this definition if you do not want to detect attacks from your internal
57 # IP addresses:
58 #ipvar HOME_NET !$HOME_NET
59 #
60 # Note to Debian users: this value is overridden when starting
61 # up the Snort daemon through the init.d script by the
62 # value of DEBIAN_SNORT_HOME_NET s defined in the
63 # /etc/snort/snort.debian.conf configuration file
64 #
65 #ipvar HOME_NET any
66
67 # Set up the external network addresses. Leave as "any" in most situations
68 #ipvar EXTERNAL_NET any
69 # If HOME_NET is defined as something other than "any", alternative, you can
70 # use this definition if you do not want to detect attacks from your internal
71 # IP addresses:
72 #ipvar EXTERNAL_NET !$HOME_NET
73
74 # List of DNS servers on your network
75 #ipvar DNS_SERVERS $HOME_NET
76
77 # List of SMTP servers on your network
78 #ipvar SMTP_SERVERS $HOME_NET
79
80 # List of web servers on your network
81 #ipvar HTTP_SERVERS $HOME_NET
82
83
84
85
86
87
```

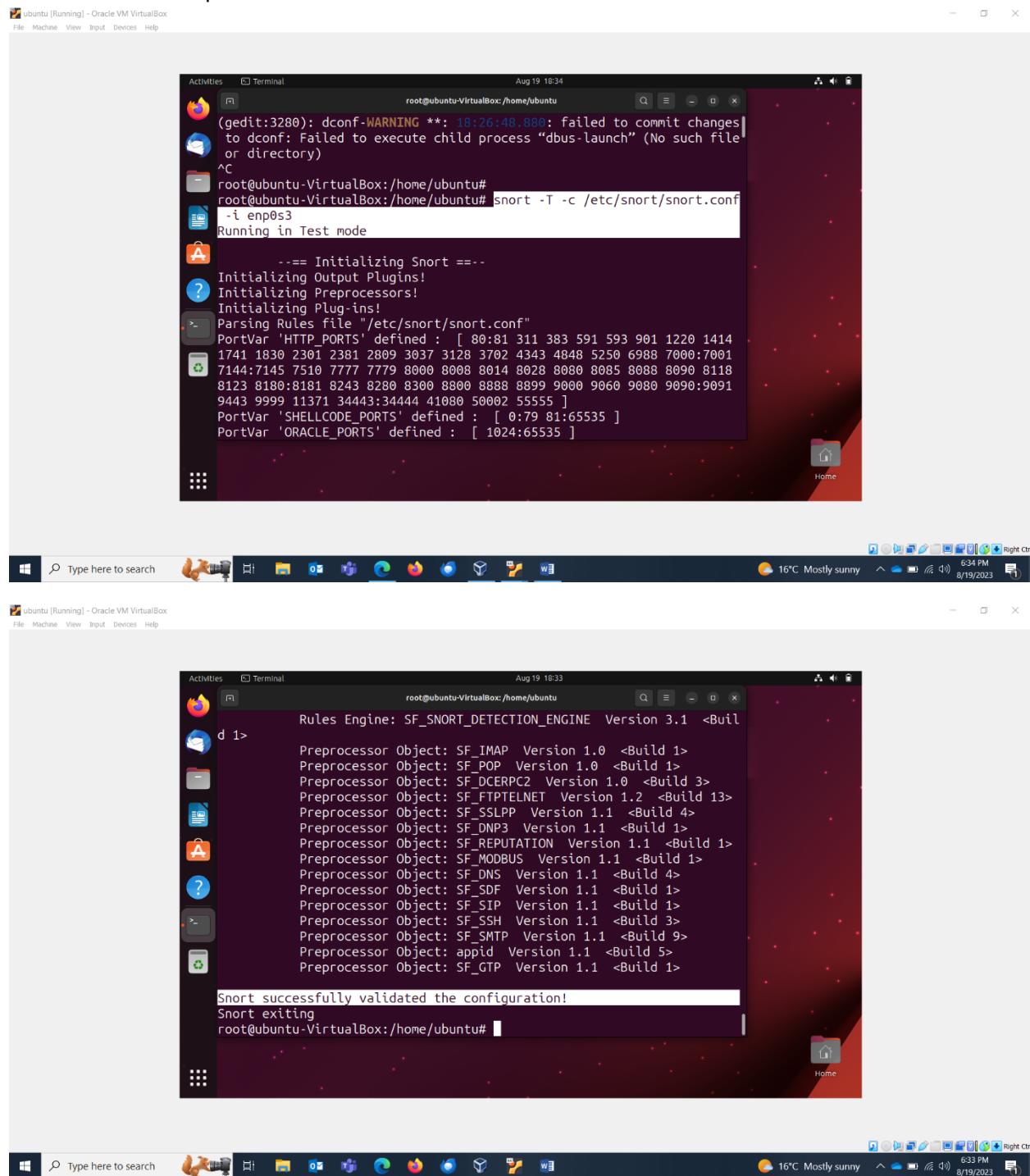
We'll now change it to 192.168.1.0/24

The screenshot shows the same Linux desktop environment and terminal window as the previous one, but with a change made to the configuration file. The "ipvar HOME_NET any" line has been replaced with "ipvar HOME_NET 192.168.1.0/24". The terminal window still displays the error messages "commit changes (No such file)" twice.

```
*snort.conf
/etc/snort
51 # The Debian init.d script is defined in such a way
52 # that you can run multiple instances.
53
54 ##### Step #1: Set the network variables. For more information, see README.variables
55 ##### If HOME_NET is defined as something other than "any", alternative, you can
56 # use this definition if you do not want to detect attacks from your internal
57 # IP addresses:
58 #ipvar HOME_NET !$HOME_NET
59 #
60 # Note to Debian users: this value is overridden when starting
61 # up the Snort daemon through the init.d script by the
62 # value of DEBIAN_SNORT_HOME_NET s defined in the
63 # /etc/snort/snort.debian.conf configuration file
64 #
65 #ipvar HOME_NET any
66
67 # Set up the external network addresses. Leave as "any" in most situations
68 #ipvar EXTERNAL_NET any
69 # If HOME_NET is defined as something other than "any", alternative, you can
70 # use this definition if you do not want to detect attacks from your internal
71 # IP addresses:
72 #ipvar EXTERNAL_NET !$HOME_NET
73
74 # List of DNS servers on your network
75 #ipvar DNS_SERVERS $HOME_NET
76
77 # List of SMTP servers on your network
78 #ipvar SMTP_SERVERS $HOME_NET
79
80 # List of web servers on your network
81 #ipvar HTTP_SERVERS $HOME_NET
82
83
84
85
86
87
```



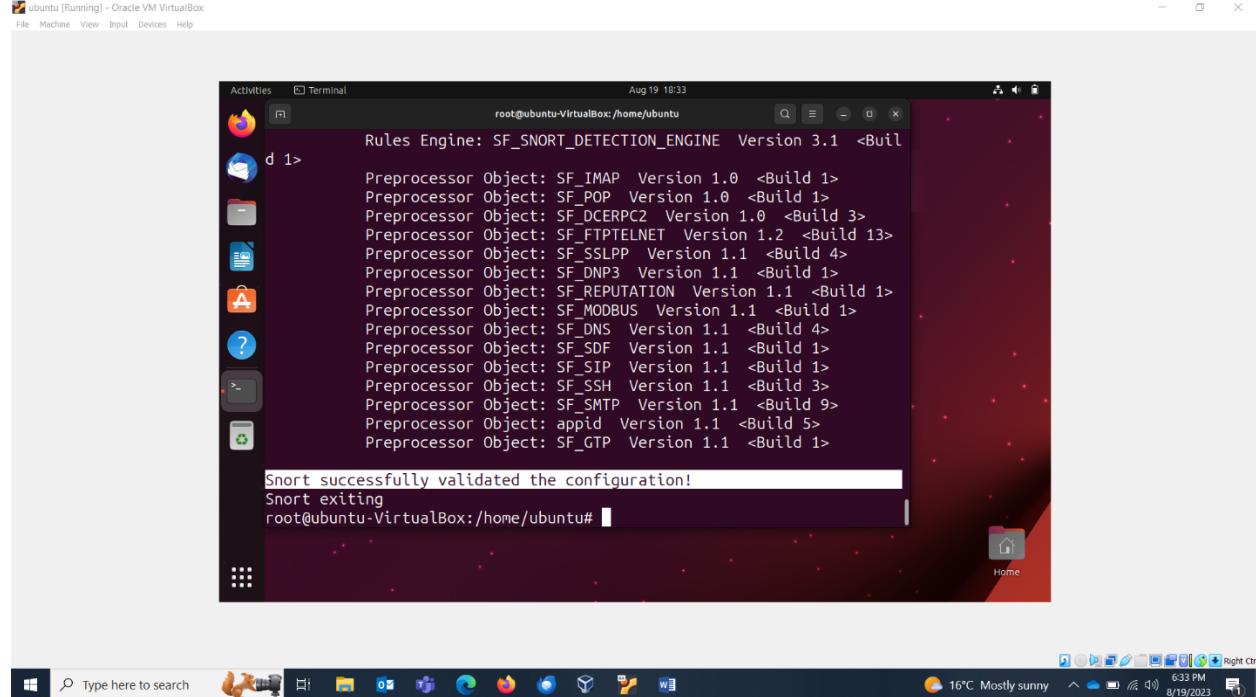
Rules verification exposure:



The screenshot shows a Linux desktop environment with a terminal window open. The terminal window title is "root@ubuntu-VirtualBox: /home/ubuntu". The terminal content shows the following steps:

```
(gedit:3280): dconf-WARNING **: 18:26:48.880: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)
^C
root@ubuntu-VirtualBox:/home/ubuntu# snort -T -c /etc/snort/snort.conf
-i enp0s3
Running in Test mode
A
==== 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 8300 8888 8899 9000 9060 9080 9090:9091
9443 9999 11371 34443:34444 41080 50000 55555 ]
PortVar 'SHELLCODE_PORTS' defined : [ 0:79 81:65535 ]
PortVar 'ORACLE_PORTS' defined : [ 1024:65535 ]
```

Below the terminal window, the desktop environment is visible, showing a dock with various icons and a system tray at the bottom.



The terminal window title is "root@ubuntu-VirtualBox: /home/ubuntu". The terminal content shows the following steps:

```
root@ubuntu-VirtualBox: /home/ubuntu
d 1>
Rules Engine: SF_SNORT_DETECTION_ENGINE Version 3.1 <Build 1>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_SDF Version 1.1 <Build 1>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
Preprocessor Object: appid Version 1.1 <Build 5>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>

Snort successfully validated the configuration!
Snort exiting
root@ubuntu-VirtualBox:/home/ubuntu#
```

Below the terminal window, the desktop environment is visible, showing a dock with various icons and a system tray at the bottom.



Lets start monitoring:

Fire up your kali/parrot machine & run nmap on the ubuntu machine.

My ip address of ubuntu is : 192.168.1.78 and parrot is 192.168.1.81

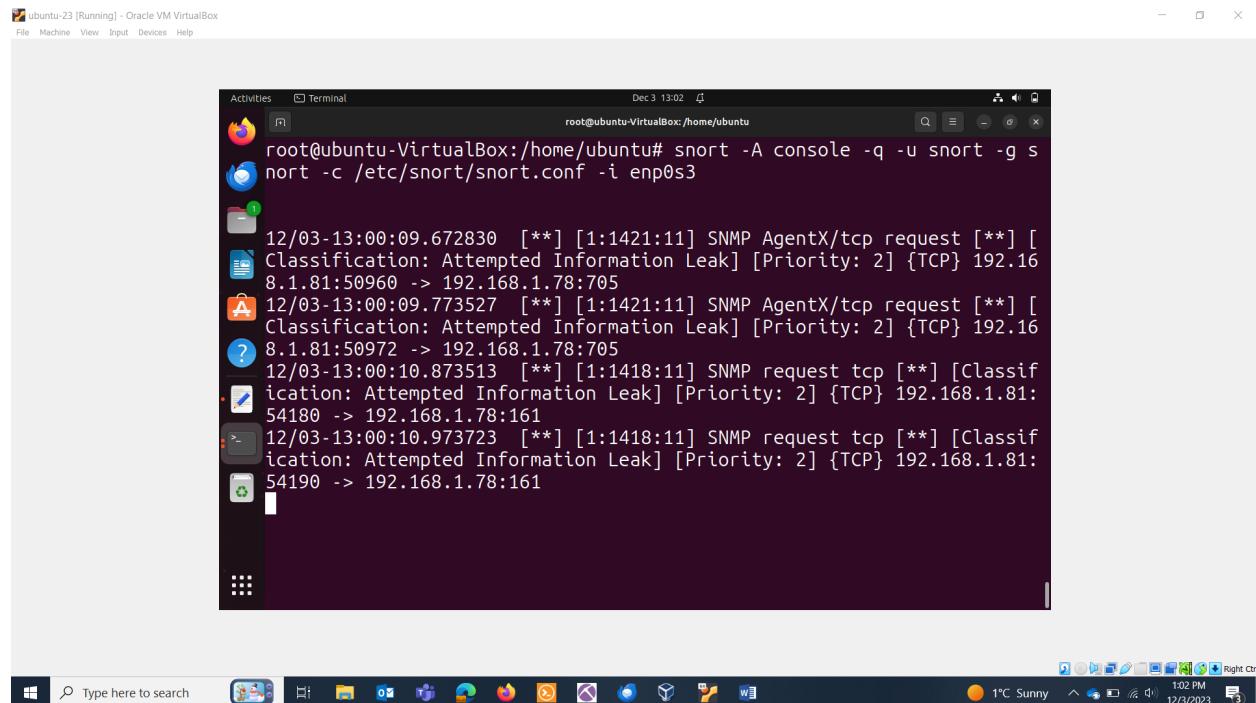
ATTACK 1: nmap scan:

```
[parrot@parrot:~]$ nmap 192.168.1.78 -Pn
Starting Nmap 7.93 ( https://nmap.org ) at 2023-12-03 15:00 EST
Nmap scan report for 192.168.1.78
Host is up (0.0017s latency).

PORT      STATE    SERVICE
20/tcp    closed   ftp-data
21/tcp    closed   ftp
22/tcp    open     ssh
445/tcp   closed   microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 4.76 seconds
```

Here is the trigger of Information leak which was attacked from 192.168.1.81:



ATTACK 2: DOS through hping3

Lets perform a dos attack from kali linux

```
#hping3 --flood 192.168.1.78
HPING 192.168.1.78 (enp0s3 192.168.1.78): NO FLAGS are set, 40 headers +
0 data bytes
hping in flood mode, no replies will be shown
```

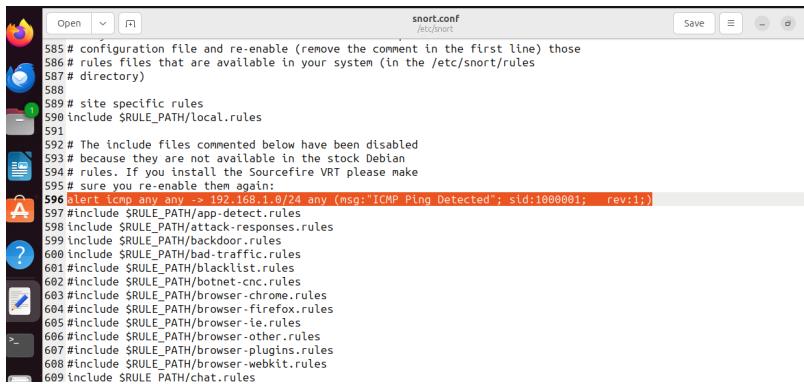
DIY: Analyze with wireshark.

Alerts in Snort console:

```
root@ubuntu-VirtualBox:/home/ubuntu
[**] [Priority: 3] [TCP] 192.168.1.81:5675 -> 192.168.1.78:0
12/03-13:05:31.911556 [**] [1:524:8] BAD-TRAFFIC tcp port 0 traffic [**] [Classification: Misc activity]
[**] [Priority: 3] [TCP] 192.168.1.81:5676 -> 192.168.1.78:0
12/03-13:05:31.912216 [**] [1:524:8] BAD-TRAFFIC tcp port 0 traffic [**] [Classification: Misc activity]
[**] [Priority: 3] [TCP] 192.168.1.81:5677 -> 192.168.1.78:0
12/03-13:05:31.912223 [**] [1:524:8] BAD-TRAFFIC tcp port 0 traffic [**] [Classification: Misc activity]
[**] [Priority: 3] [TCP] 192.168.1.81:5678 -> 192.168.1.78:0
12/03-13:05:31.912562 [**] [1:524:8] BAD-TRAFFIC tcp port 0 traffic [**] [Classification: Misc activity]
[**] [Priority: 3] [TCP] 192.168.1.81:5679 -> 192.168.1.78:0
12/03-13:05:31.912804 [**] [1:524:8] BAD-TRAFFIC tcp port 0 traffic [**] [Classification: Misc activity]
[**] [Priority: 3] [TCP] 192.168.1.81:5680 -> 192.168.1.78:0
12/03-13:05:31.913307 [**] [1:524:8] BAD-TRAFFIC tcp port 0 traffic [**] [Classification: Misc activity]
[**] [Priority: 3] [TCP] 192.168.1.81:5681 -> 192.168.1.78:0
12/03-13:05:31.913551 [**] [1:524:8] BAD-TRAFFIC tcp port 0 traffic [**] [Classification: Misc activity]
[**] [Priority: 3] [TCP] 192.168.1.81:5682 -> 192.168.1.78:0
12/03-13:05:31.913793 [**] [1:524:8] BAD-TRAFFIC tcp port 0 traffic [**] [Classification: Misc activity]
[**] [Priority: 3] [TCP] 192.168.1.81:5683 -> 192.168.1.78:0
12/03-13:05:31.913820 [**] [1:524:8] BAD-TRAFFIC tcp port 0 traffic [**] [Classification: Misc activity]
[**] [Priority: 3] [TCP] 192.168.1.81:5684 -> 192.168.1.78:0
12/03-13:05:31.914093 [**] [1:524:8] BAD-TRAFFIC tcp port 0 traffic [**] [Classification: Misc activity]
[**] [Priority: 3] [TCP] 192.168.1.81:5685 -> 192.168.1.78:0
12/03-13:05:31.914567 [**] [1:524:8] BAD-TRAFFIC tcp port 0 traffic [**] [Classification: Misc activity]
[**] [Priority: 3] [TCP] 192.168.1.81:5686 -> 192.168.1.78:0
12/03-13:05:31.914572 [**] [1:524:8] BAD-TRAFFIC tcp port 0 traffic [**] [Classification: Misc activity]
[**] [Priority: 3] [TCP] 192.168.1.81:5687 -> 192.168.1.78:0
12/03-13:05:31.915271 [**] [1:524:8] BAD-TRAFFIC tcp port 0 traffic [**] [Classification: Misc activity]
[**] [Priority: 3] [TCP] 192.168.1.81:5688 -> 192.168.1.78:0
12/03-13:05:31.922017 [**] [1:524:8] BAD-TRAFFIC tcp port 0 traffic [**] [Classification: Misc activity]
[**] [Priority: 3] [TCP] 192.168.1.81:5689 -> 192.168.1.78:0
12/03-13:05:31.922035 [**] [1:524:8] BAD-TRAFFIC tcp port 0 traffic [**] [Classification: Misc activity]
```

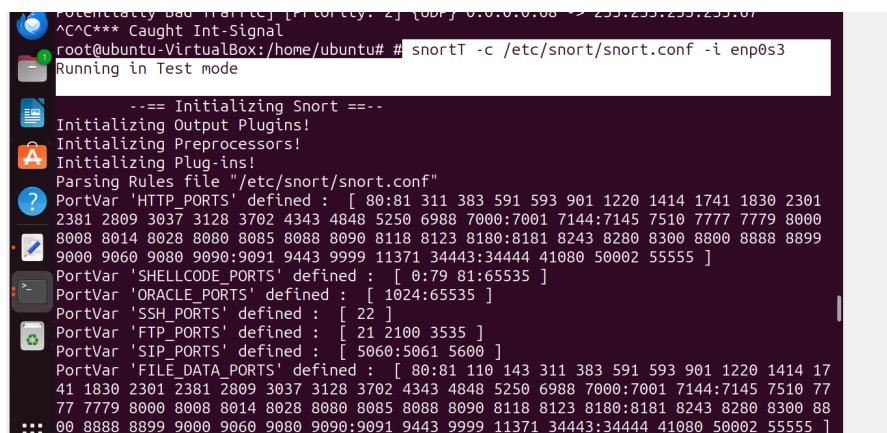
ATTACK 3: Rule for ping

Creating a rule:



```
snort.conf
585 # configuration file and re-enable (remove the comment in the first line) those
586 # rules files that are available in your system (in the /etc/snort/rules
587 # directory)
588
589 # site specific rules
590 include $RULE_PATH/local.rules
591
592 # The include files commented below have been disabled
593 # because they are not available in the stock Debian
594 # rules. If you install the Sourcefire VRT please make
595 # sure you re-enable them again:
596 alert icmp any any -> 192.168.1.0/24 any (msg:"ICMP Ping Detected"; sid:1000001; rev:1;)
597 #include $RULE_PATH/app-detect.rules
598 include $RULE_PATH/attack-responses.rules
599 include $RULE_PATH/backdoor.rules
600 include $RULE_PATH/bad-traffic.rules
601 #include $RULE_PATH/blacklist.rules
602 #include $RULE_PATH/botnet-cr.rules
603 #include $RULE_PATH/browser-chrome.rules
604 #include $RULE_PATH/browser-firefox.rules
605 #include $RULE_PATH/browser-ie.rules
606 #include $RULE_PATH/browser-other.rules
607 #include $RULE_PATH/browser-plugins.rules
608 #include $RULE_PATH/browser-webkit.rules
609 include $RULE_PATH/chat.rules
```

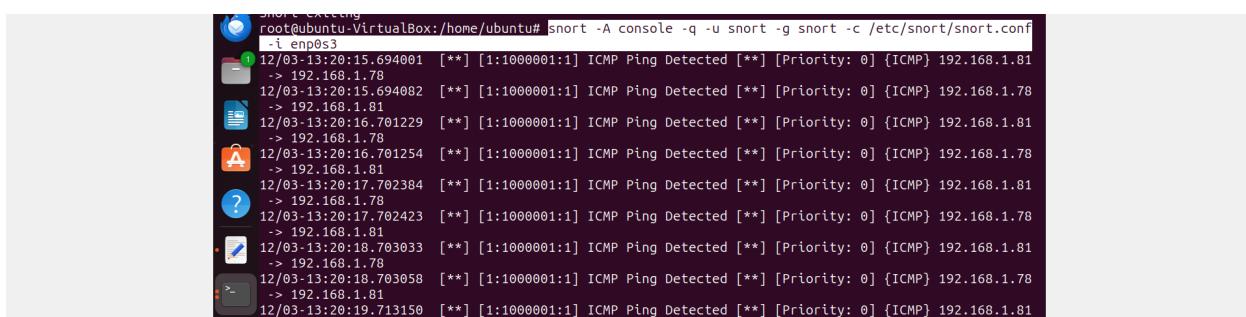
Verify the configurations



```
Potentially bad traffic [Priority: 2] (00f) 0.0.0.0.08 -> 255.255.255.255.07
^C<*** Caught Int-Signal
root@ubuntu-VirtualBox:/home/ubuntu# snortT -c /etc/snort/snort.conf -i enp0s3
Running in Test 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 'STP_PORTS' defined : [ 5060:5061 5600 ]
PortVar 'FILE_DATA_PORTS' defined : [ 80:81 110 143 311 383 591 593 901 1220 1414 17
41 1830 2301 2381 2809 3037 3128 3702 4343 4848 5250 6988 7000:7001 7144:7145 7510 77
77 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300 88
8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 50002 55555 ]
```

Ping from the other machine

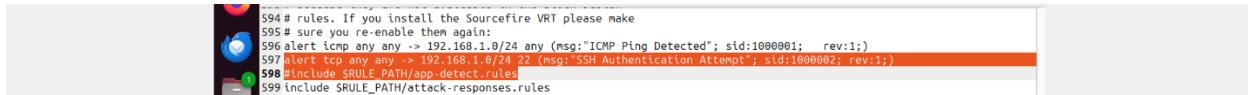
Fire up snort console



```
snort -A console -q -u snort -g snort -c /etc/snort/snort.conf
-> enp0s3
12/03/13:20:15.694001 [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 192.168.1.81
-> 192.168.1.78
12/03/13:20:15.694082 [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 192.168.1.78
-> 192.168.1.81
12/03/13:20:16.701229 [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 192.168.1.81
-> 192.168.1.78
12/03/13:20:16.701254 [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 192.168.1.78
-> 192.168.1.81
12/03/13:20:17.702384 [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 192.168.1.81
-> 192.168.1.78
12/03/13:20:17.702423 [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 192.168.1.78
-> 192.168.1.81
12/03/13:20:18.703033 [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 192.168.1.81
-> 192.168.1.78
12/03/13:20:18.703058 [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 192.168.1.78
-> 192.168.1.81
12/03/13:20:19.713150 [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 192.168.1.81
```

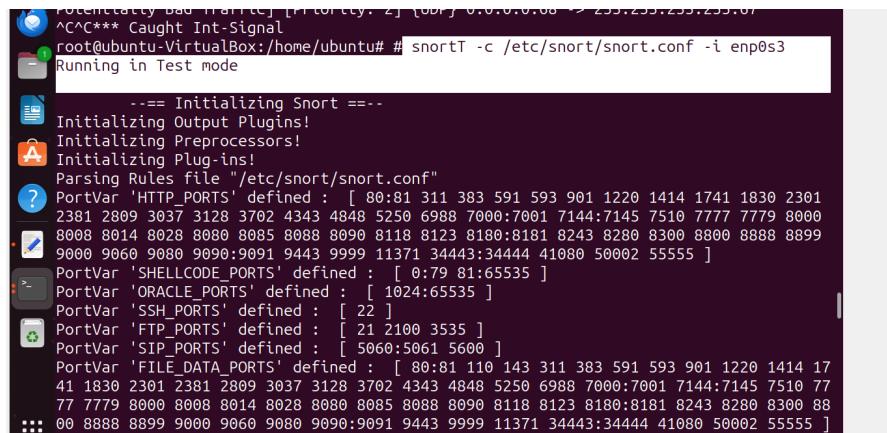
ATTACK 4: ssh

SSH rule



```
595# rules. If you install the Sourcefire VRT please make  
595# sure you re-enable them again:  
596alert icmp any any -> 192.168.1.0/24 any (msg:"ICMP Ping Detected"; sid:1000001; rev:1;)  
597alert tcp any any -> 192.168.1.0/24 22 (msg: "SSH Authentication Attempt"; sid:1000002; rev:1;)  
598# include $RULE_PATH/app-detect.rules  
599 include $RULE_PATH/attack-responses.rules
```

Verify conf.



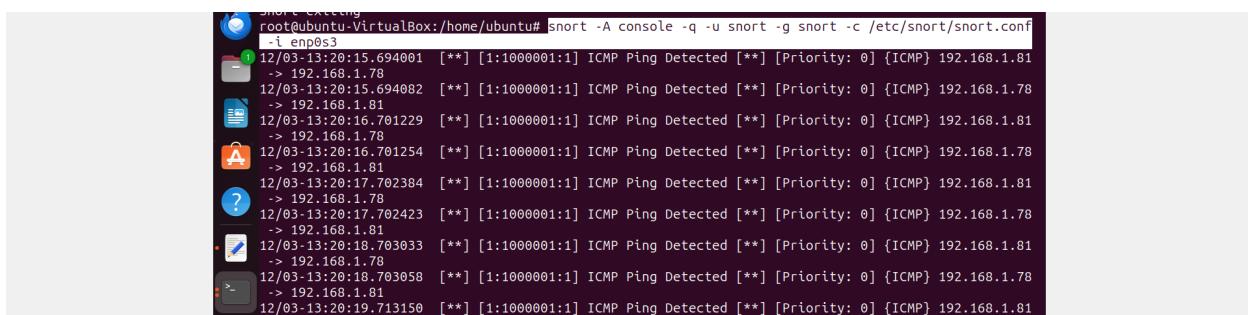
```
Potentially bad traffic [Priority: 2] {src} 0.0.0.0.08 -> 255.255.255.255.07  
^C*** Caught Int-Signal  
root@ubuntu-VirtualBox:/home/ubuntu# # snortT -c /etc/snort/snort.conf -i enp0s3  
Running in Test mode  
--= Initializing Snort --=  
Initializing Output Plugins!  
Initializing Preprocessors!  
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 17  
41 1830 2301 2381 2809 3037 3128 3702 4343 4848 5250 6988 7000:7001 7144:7145 7510 77  
77 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300 88  
00 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 50002 55555 ]
```

Try ssh



```
#ssh ubuntu@192.168.1.78  
The authenticity of host '192.168.1.78 (192.168.1.78)' can't be established.  
ECDSA key fingerprint is SHA256:2ziDovUyhxYhrBM+agkXqbaTkEswH7N8uB3dAwW6Ddk.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '192.168.1.78' (ECDSA) to the list of known hosts.  
ubuntu@192.168.1.78's password:  
Welcome to Ubuntu 23.04 (GNU/Linux 6.2.0-37-generic x86_64)  
  
 * Documentation: https://help.ubuntu.com  
 * Management: https://landscape.canonical.com  
 * Support: https://ubuntu.com/advantage  
  
0 updates can be applied immediately.  
ubuntu@ubuntu-VirtualBox:~$  
ubuntu@ubuntu-VirtualBox:~$
```

Look in console

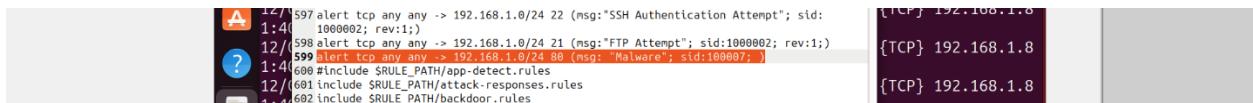


```
root@ubuntu-VirtualBox:/home/ubuntu# snort -A console -q -u snort -g snort -c /etc/snort/snort.conf  
-l enp0s3  
12/03/13:20:15.694001 [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 192.168.1.81  
-> 192.168.1.78  
12/03/13:20:15.694082 [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 192.168.1.78  
-> 192.168.1.81  
12/03/13:20:16.701229 [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 192.168.1.81  
-> 192.168.1.78  
12/03/13:20:16.701254 [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 192.168.1.78  
-> 192.168.1.81  
12/03/13:20:17.702384 [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 192.168.1.81  
-> 192.168.1.78  
12/03/13:20:17.702423 [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 192.168.1.78  
-> 192.168.1.81  
12/03/13:20:18.703033 [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 192.168.1.81  
-> 192.168.1.78  
12/03/13:20:18.703058 [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 192.168.1.78  
-> 192.168.1.81  
12/03/13:20:19.713150 [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 192.168.1.81
```

```
root@ubuntu:~/.VirtualBox/Homelab$ sudo netstat -an | grep 22
9.91.48:443 -> 192.168.1.78:36192
12/03/13:47:51.518461 [**] [1:1000002:1] SSH Authentication Attempt [**] [Priority: 0] {TCP} 91.18
9.91.48:443 -> 192.168.1.78:36192
12/03/13:47:51.518492 [**] [1:1000002:1] SSH Authentication Attempt [**] [Priority: 0] {TCP} 91.18
9.91.48:443 -> 192.168.1.78:36192
12/03/13:47:51.595329 [**] [1:1000002:1] SSH Authentication Attempt [**] [Priority: 0] {TCP} 91.18
9.91.48:443 -> 192.168.1.78:36192
12/03/13:47:59.111578 [**] [1:1000002:1] SSH Authentication Attempt [**] [Priority: 0] {TCP} 192.1
68.1.76:1514 -> 192.168.1.78:40550
12/03/13:48:00.638381 [**] [1:1000002:1] SSH Authentication Attempt [**] [Priority: 0] {TCP} 192.1
68.1.81:33360 -> 192.168.1.78:22
12/03/13:48:00.682511 [**] [1:1000002:1] SSH Authentication Attempt [**] [Priority: 0] {TCP} 192.1
68.1.81:33360 -> 192.168.1.78:22
12/03/13:48:00.804071 [**] [1:1000002:1] SSH Authentication Attempt [**] [Priority: 0] {TCP} 192.1
68.1.81:33360 -> 192.168.1.78:22
12/03/13:48:00.804828 [**] [1:1000002:1] SSH Authentication Attempt [**] [Priority: 0] {TCP} 192.1
68.1.81:33360 -> 192.168.1.78:22
12/03/13:48:00.972283 [**] [1:1000002:1] SSH Authentication Attempt [**] [Priority: 0] {TCP} 192.1
68.1.81:33360 -> 192.168.1.78:22
12/03/13:48:00.973056 [**] [1:1000002:1] SSH Authentication Attempt [**] [Priority: 0] {TCP} 192.1
68.1.81:33360 -> 192.168.1.78:22
12/03/13:48:02.964223 [**] [1:1000002:1] SSH Authentication Attempt [**] [Priority: 0] {TCP} 192.1
68.1.81:33360 -> 192.168.1.78:22
12/03/13:48:02.965093 [**] [1:1000002:1] SSH Authentication Attempt [**] [Priority: 0] {TCP} 192.1
68.1.81:33360 -> 192.168.1.78:22
12/03/13:48:09.340430 [**] [1:1000002:1] SSH Authentication Attempt [**] [Priority: 0] {TCP} 192.1
68.1.76:1514 -> 192.168.1.78:38242
12/03/13:48:09.683474 [**] [1:1000002:1] SSH Authentication Attempt [**] [Priority: 0] {TCP} 192.1
68.1.76:1515 -> 192.168.1.78:51308
```

ANALYZE WEB SERVER

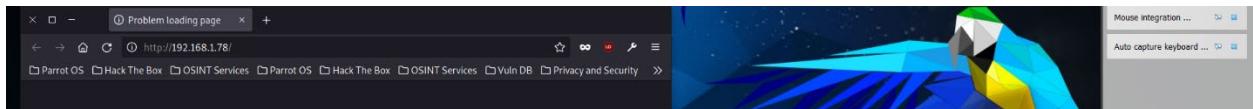
Adding rule:



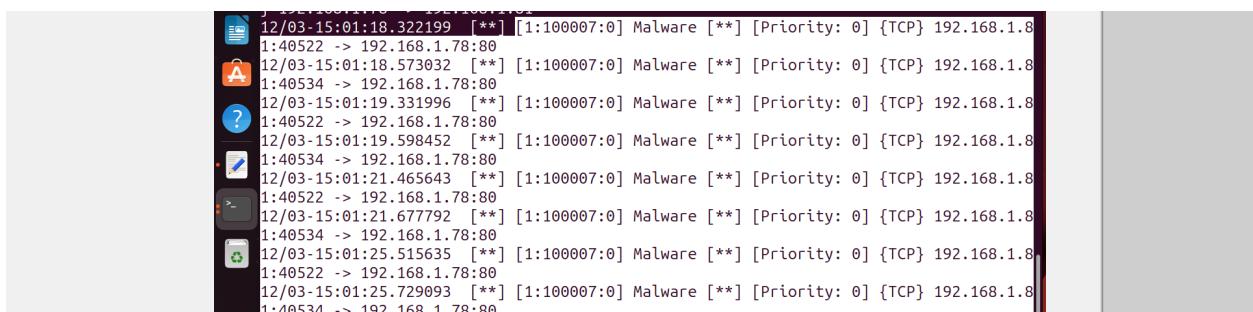
```
A 12/1:597 alert tcp any any -> 192.168.1.8/24 22 (msg:"SSH Authentication Attempt"; sid:1:400002; rev:1;)
12/1:598 alert tcp any any -> 192.168.1.8/24 21 (msg:"FTP Attempt"; sid:1000002; rev:1;)
12/1:599 alert tcp any any -> 192.168.1.8/24 80 (msg: "Malware"; sid:100007; )
12/1:600 #include $RULE_PATH/app-detect.rules
12/1:601 include $RULE_PATH/attack-responses.rules
12/1:602 include $RULE_PATH/backdoor.rules
```

Refresh your configurations: DIY

Access 192.168.1.78's webserver.



Capturing in console



```
12/03-15:01:18.322199 [*] [1:100007:0] Malware [**] [Priority: 0] {TCP} 192.168.1.8
1:40522 -> 192.168.1.78:80
12/03-15:01:18.573032 [*] [1:100007:0] Malware [**] [Priority: 0] {TCP} 192.168.1.8
1:40534 -> 192.168.1.78:80
12/03-15:01:19.331996 [*] [1:100007:0] Malware [**] [Priority: 0] {TCP} 192.168.1.8
1:40522 -> 192.168.1.78:80
12/03-15:01:19.598452 [*] [1:100007:0] Malware [**] [Priority: 0] {TCP} 192.168.1.8
1:40534 -> 192.168.1.78:80
12/03-15:01:21.465643 [*] [1:100007:0] Malware [**] [Priority: 0] {TCP} 192.168.1.8
1:40522 -> 192.168.1.78:80
12/03-15:01:21.677792 [*] [1:100007:0] Malware [**] [Priority: 0] {TCP} 192.168.1.8
1:40534 -> 192.168.1.78:80
12/03-15:01:25.515635 [*] [1:100007:0] Malware [**] [Priority: 0] {TCP} 192.168.1.8
1:40522 -> 192.168.1.78:80
12/03-15:01:25.729093 [*] [1:100007:0] Malware [**] [Priority: 0] {TCP} 192.168.1.8
1:40534 -> 192.168.1.78:80
```