



VIT[®]

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

Cyber Forensics and Investigation

Course Code: BCI4001

Slot: L55+L56

Faculty: Dr. AJU D

Assessment: 4

18BCI0247

Rohan Allen

Exercise 4: Snort

Aim: To download and install snort and to include and configure rulesets in order to implement an IDS solution which allows and omits certain traffic based on their protocol, port number etc.

After installing snort and doing all rule configuration

Snort testing: to check version

```
Microsoft Windows [Version 10.0.19041.1083]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>cd c:\Snort\bin

c:\Snort\bin>snort -V

-*> Snort! <*-
Version 2.9.18-WIN64 GRE (Build 169)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2021 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using PCRE version: 8.10 2010-06-25
Using ZLIB version: 1.2.11

c:\Snort\bin>
```

List of interfaces:

```
c:\Snort\bin>snort -W

-*> Snort! <*-
Version 2.9.18-WIN64 GRE (Build 169)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2021 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using PCRE version: 8.10 2010-06-25
Using ZLIB version: 1.2.11

Index  Physical Address      IP Address      Device Name      Description
-----
1      00:00:00:00:00:00      disabled       \Device\NPF_{46EAC3B7-0975-4393-8513-2D3A1FADA02B}  WAN Miniport (Network Monitor)
2      00:00:00:00:00:00      disabled       \Device\NPF_{F4CBD0C5-F687-4310-85BC-A29DB34C0916}  WAN Miniport (IPv6)
3      00:00:00:00:00:00      disabled       \Device\NPF_{76F3C4E6-6A82-41C8-A909-C331CBAEF855}  WAN Miniport (IP)
4      9C:DA:3E:AD:CA:95      169.254.171.188 \Device\NPF_{1591A01F-770D-4D27-B5F4-B52ACF7066A8}  Bluetooth Device (Personal Area Network)
5      9C:DA:3E:AD:CA:92      169.254.40.242  \Device\NPF_{E0E68657-24A4-47D0-A553-D21310199192}  Microsoft Wi-Fi Direct Virtual Adapter
6      9C:DA:3E:AD:CA:91      192.168.1.117   \Device\NPF_{D28E8B80-5950-40BF-B4F2-16D4D81236EF}  Intel(R) Dual Band Wireless-AC 7265 #2
7      9E:DA:3E:AD:CA:91      169.254.142.190 \Device\NPF_{093EC74F-1EC2-4A23-86C2-39CD44B7C395}  Microsoft Wi-Fi Direct Virtual Adapter #2
8      0A:00:27:00:00:09      192.168.56.1    \Device\NPF_{59E6C320-983F-41EC-9483-1F2D4140791D}  VirtualBox Host-Only Ethernet Adapter
9      00:00:00:00:00:00      disabled       \Device\NPF_{Loopback} Adapter for loopback traffic capture
10     00:00:00:00:00:00      169.254.237.172 \Device\NPF_{CEA811B7-2FC0-46A6-B703-B5F6BD157A2A}  ExpressVPN Wintun Driver

c:\Snort\bin>
```

```
snort -i 1 -c c:\Snort\etc\snort.conf -T
```

testing config file in 1st interface

```
Select Administrator: Command Prompt

c:\Snort\bin>snort -i 6 -c c:\Snort\etc\snort.conf -T
Running in Test mode

--== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "c:\Snort\etc\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 80
80 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 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 '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 c:\Snort\lib\snort_dynamicengine\sf_engine.dll... done
Loading all dynamic preprocessor libs from c:\Snort\lib\snort_dynamicpreprocessor...
Loading dynamic preprocessor library c:\Snort\lib\snort_dynamicpreprocessor\sf_dce2.dll... done
Loading dynamic preprocessor library c:\Snort\lib\snort_dynamicpreprocessor\sf_dnp3.dll... done
Loading dynamic preprocessor library c:\Snort\lib\snort_dynamicpreprocessor\sf_dns.dll... done
Loading dynamic preprocessor library c:\Snort\lib\snort_dynamicpreprocessor\sf_ftptelnet.dll... done
Loading dynamic preprocessor library c:\Snort\lib\snort_dynamicpreprocessor\sf_gtp.dll... done
Loading dynamic preprocessor library c:\Snort\lib\snort_dynamicpreprocessor\sf_imap.dll... done
Loading dynamic preprocessor library c:\Snort\lib\snort_dynamicpreprocessor\sf_modbus.dll... done
Loading dynamic preprocessor library c:\Snort\lib\snort_dynamicpreprocessor\sf_pop.dll... done
Loading dynamic preprocessor library c:\Snort\lib\snort_dynamicpreprocessor\sf_reputation.dll... done
Loading dynamic preprocessor library c:\Snort\lib\snort_dynamicpreprocessor\sf_sdf.dll... done
Loading dynamic preprocessor library c:\Snort\lib\snort_dynamicpreprocessor\sf_sip.dll... done
Loading dynamic preprocessor library c:\Snort\lib\snort_dynamicpreprocessor\sf_smtp.dll... done
Loading dynamic preprocessor library c:\Snort\lib\snort_dynamicpreprocessor\sf_ssh.dll... done
Loading dynamic preprocessor library c:\Snort\lib\snort_dynamicpreprocessor\sf_ssl.dll... done
Finished Loading all dynamic preprocessor libs from c:\Snort\lib\snort_dynamicpreprocessor
Log directory = c:\Snort\log
```

```
Select Administrator: Command Prompt

1 byte states : 1.06
2 byte states : 45.17
4 byte states : 65.19

-----
[ Number of patterns truncated to 20 bytes: 550 ]
pcap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "\Device\NPF_{D2BE8880-5950-40BF-B4F2-16D4DB1236EF}".

--== Initialization Complete ==--

--> Snort! <*-
o" )~
****
Version 2.9.18-WIN64 GRE (Build 169)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2021 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using PCRE version: 8.10 2010-06-25
Using ZLIB version: 1.2.11

Rules Engine: SF_SNORT_DETECTION_ENGINE Version 3.2 <Build 1>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Preprocessor Object: SF_SHTP Version 1.1 <Build 3>
Preprocessor Object: SF_SIP 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_POP Version 1.0 <Build 1>
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_FTPTNET Version 1.2 <Build 13>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>

Snort successfully validated the configuration!
Snort exiting

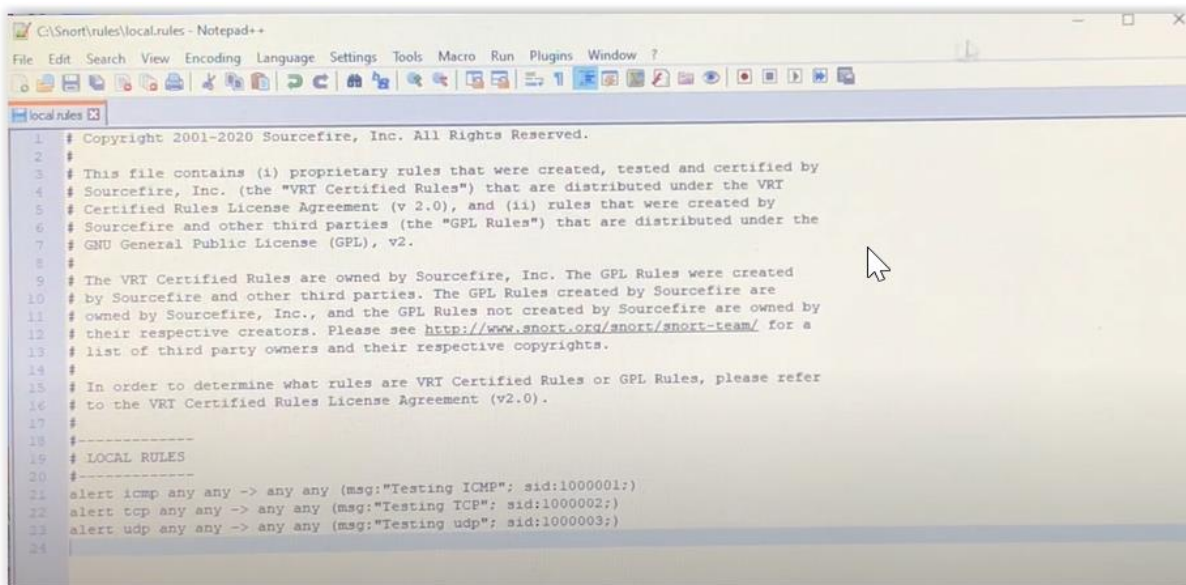
c:\Snort\bin>
```

alert icmp any any -> any any (msg:"Testing ICMP"; sid:1000001;)

alert tcp any any -> any any (msg:"Testing TCP"; sid:1000002;)

alert udp any any -> any any (msg:"Testing udp"; sid:1000003;)

put these in local.rules file



```
C:\Snort\rules\local.rules - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?

local.rules
1 # Copyright 2001-2020 Sourcefire, Inc. All Rights Reserved.
2 #
3 # This file contains (i) proprietary rules that were created, tested and certified by
4 # Sourcefire, Inc. (the "VRT Certified Rules") that are distributed under the VRT
5 # Certified Rules License Agreement (v 2.0), and (ii) rules that were created by
6 # Sourcefire and other third parties (the "GPL Rules") that are distributed under the
7 # GNU General Public License (GPL), v2.
8 #
9 # The VRT Certified Rules are owned by Sourcefire, Inc. The GPL Rules were created
10 # by Sourcefire and other third parties. The GPL Rules created by Sourcefire are
11 # owned by Sourcefire, Inc., and the GPL Rules not created by Sourcefire are owned by
12 # their respective creators. Please see http://www.snort.org/snort/snort-team/ for a
13 # list of third party owners and their respective copyrights.
14 #
15 # In order to determine what rules are VRT Certified Rules or GPL Rules, please refer
16 # to the VRT Certified Rules License Agreement (v2.0).
17 #
18 #-----
19 # LOCAL RULES
20 #-----
21 alert icmp any any -> any any (msg:"Testing ICMP"; sid:1000001;)
22 alert tcp any any -> any any (msg:"Testing TCP"; sid:1000002;)
23 alert udp any any -> any any (msg:"Testing udp"; sid:1000003;)
24
```

snort -i 6 -c c:\Snort\etc\snort.conf -A console

then testing these alert messages using 6th interface(Wifi) and printing results in console using above command.

Administrator: Command Prompt - snort -i 6 -c c:\snort\etc\snort.conf -A console

```
07/10-11:42:23.527337 00000000:0 Testing TCP 00000000:0 (TCP) 192.168.1.117:1051 -> 192.168.1.2:49154
07/10-11:42:23.528311 00000002:0 Testing TCP 00000000:0 (TCP) 192.168.1.2:49154 -> 192.168.1.117:1051
07/10-11:42:24.508203 00000003:0 Testing udp 00000000:0 (UDP) 192.168.1.2:36286 -> 192.168.1.117:56251
07/10-11:42:24.517166 00000003:0 Testing udp 00000000:0 (UDP) 192.168.1.2:36286 -> 192.168.1.117:56251
07/10-11:42:24.522253 00000003:0 Testing udp 00000000:0 (UDP) 192.168.1.2:36286 -> 192.168.1.117:56251
07/10-11:42:24.536770 00000003:0 Testing udp 00000000:0 (UDP) 192.168.1.2:36286 -> 192.168.1.117:56251
07/10-11:42:24.541656 00000003:0 Testing udp 00000000:0 (UDP) 192.168.1.2:36286 -> 192.168.1.117:56251
07/10-11:42:24.552283 00000003:0 Testing udp 00000000:0 (UDP) 192.168.1.2:36286 -> 192.168.1.117:56251
07/10-11:42:24.565643 00000003:0 Testing udp 00000000:0 (UDP) 192.168.1.2:36286 -> 192.168.1.117:56251
07/10-11:42:24.574152 00000003:0 Testing udp 00000000:0 (UDP) 192.168.1.2:36286 -> 192.168.1.117:56251
07/10-11:42:25.136773 00000002:0 Testing TCP 00000000:0 (TCP) 103.68.221.190:443 -> 192.168.1.117:1042
07/10-11:42:25.136960 00000002:0 Testing TCP 00000000:0 (TCP) 192.168.1.117:1042 -> 103.68.221.190:443
07/10-11:42:25.152932 00000002:0 Testing TCP 00000000:0 (TCP) 103.68.221.190:443 -> 192.168.1.117:1043
07/10-11:42:25.153102 00000002:0 Testing TCP 00000000:0 (TCP) 192.168.1.117:1043 -> 103.68.221.190:443
07/10-11:42:25.570887 00000003:0 Testing udp 00000000:0 (UDP) 192.168.1.117:60434 -> 192.168.1.2:53
07/10-11:42:25.574272 00000003:0 Testing udp 00000000:0 (UDP) 192.168.1.2:53 -> 192.168.1.117:60434
07/10-11:42:25.577953 00000002:0 Testing TCP 00000000:0 (TCP) 192.168.1.117:1052 -> 2.21.231.152:80
07/10-11:42:25.586201 00000002:0 Testing TCP 00000000:0 (TCP) 2.21.231.152:80 -> 192.168.1.117:1052
07/10-11:42:25.586390 00000002:0 Testing TCP 00000000:0 (TCP) 192.168.1.117:1052 -> 2.21.231.152:80
07/10-11:42:25.586630 00000002:0 Testing TCP 00000000:0 (TCP) 192.168.1.117:1052 -> 2.21.231.152:80
07/10-11:42:25.595105 00000002:0 Testing TCP 00000000:0 (TCP) 2.21.231.152:80 -> 192.168.1.117:1052
07/10-11:42:25.597887 00000002:0 Testing TCP 00000000:0 (TCP) 2.21.231.152:80 -> 192.168.1.117:1052
07/10-11:42:25.597887 00000002:0 Testing TCP 00000000:0 (TCP) 2.21.231.152:80 -> 192.168.1.117:1052
07/10-11:42:25.598027 00000002:0 Testing TCP 00000000:0 (TCP) 192.168.1.117:1052 -> 2.21.231.152:80
07/10-11:42:25.598147 00000002:0 Testing TCP 00000000:0 (TCP) 192.168.1.117:1052 -> 2.21.231.152:80
07/10-11:42:25.598167 00000002:0 Testing TCP 00000000:0 (TCP) 192.168.1.117:1052 -> 2.21.231.152:80
07/10-11:42:25.606804 00000002:0 Testing TCP 00000000:0 (TCP) 2.21.231.152:80 -> 192.168.1.117:1052
07/10-11:42:25.606804 00000002:0 Testing TCP 00000000:0 (TCP) 2.21.231.152:80 -> 192.168.1.117:1052
07/10-11:42:26.506126 00000003:0 Testing udp 00000000:0 (UDP) 192.168.1.117:56251 -> 229.255.255.250:1900
07/10-11:42:26.508651 00000003:0 Testing udp 00000000:0 (UDP) 192.168.1.2:36286 -> 192.168.1.117:56251
07/10-11:42:26.509419 00000003:0 Testing udp 00000000:0 (UDP) 192.168.1.2:58316 -> 192.168.1.117:56251
07/10-11:42:26.510590 00000003:0 Testing udp 00000000:0 (UDP) 192.168.1.2:36286 -> 192.168.1.117:56251
07/10-11:42:26.520807 00000003:0 Testing udp 00000000:0 (UDP) 192.168.1.2:36286 -> 192.168.1.117:56251
07/10-11:42:26.531121 00000003:0 Testing udp 00000000:0 (UDP) 192.168.1.2:36286 -> 192.168.1.117:56251
07/10-11:42:26.543258 00000003:0 Testing udp 00000000:0 (UDP) 192.168.1.2:36286 -> 192.168.1.117:56251
07/10-11:42:26.573921 00000003:0 Testing udp 00000000:0 (UDP) 192.168.1.2:36286 -> 192.168.1.117:56251
07/10-11:42:26.573921 00000003:0 Testing udp 00000000:0 (UDP) 192.168.1.2:36286 -> 192.168.1.117:56251
07/10-11:42:26.573921 00000003:0 Testing udp 00000000:0 (UDP) 192.168.1.2:36286 -> 192.168.1.117:56251
07/10-11:42:26.849709 00000002:0 Testing TCP 00000000:0 (TCP) 103.68.221.190:443 -> 192.168.1.117:3063
07/10-11:42:26.850201 00000002:0 Testing TCP 00000000:0 (TCP) 192.168.1.117:3063 -> 103.68.221.190:443
07/10-11:42:27.134095 00000002:0 Testing TCP 00000000:0 (TCP) 103.68.221.190:443 -> 192.168.1.117:1049
07/10-11:42:27.134286 00000002:0 Testing TCP 00000000:0 (TCP) 192.168.1.117:1049 -> 103.68.221.190:443
```

Administrator: Command Prompt

```
*** Caught Int-Signal
=====
Run time for packet processing was 72.573000 seconds
Snort processed 6791 packets.
Snort ran for 0 days 0 hours 1 minutes 12 seconds
  Pkts/min:      6791
  Pkts/sec:       94
=====
Packet I/O Totals:
  Received:      6795
  Analyzed:      6791 ( 99.941%)
  Dropped:        0 ( 0.000%)
  Filtered:        0 ( 0.000%)
  Outstanding:    4 ( 0.059%)
  Injected:        0
=====
Breakdown by protocol (includes rebuilt packets):
  Eth:           6800 (100.000%)
  VLAN:           0 ( 0.000%)
  IP4:           6799 ( 99.985%)
  Frag:           0 ( 0.000%)
  ICMP:           0 ( 0.000%)
  UDP:           2686 ( 39.500%)
  TCP:           4106 ( 60.500%)
  IP6:            0 ( 0.000%)
  IP6 Ext:        0 ( 0.000%)
  IP6 Opts:       0 ( 0.000%)
  Frag6:          0 ( 0.000%)
  ICMP6:          0 ( 0.000%)
  UDP6:           0 ( 0.000%)
  TCP6:           0 ( 0.000%)
  Teredo:         0 ( 0.000%)
  ICMP-IP:        0 ( 0.000%)
  EAPOL:          0 ( 0.000%)
  IP4/IP4:        0 ( 0.000%)
  IP4/IP6:        0 ( 0.000%)
  IP6/IP4:        0 ( 0.000%)
  IP6/IP6:        0 ( 0.000%)
  GRE:            0 ( 0.000%)
  GRE Eth:        0 ( 0.000%)
  GRE VLAN:       0 ( 0.000%)
  GRE IP4:        0 ( 0.000%)
  GRE IP6:        0 ( 0.000%)
```

