

# Practical -1

## 1. Configure the `snort.conf` file

- Go to `C:/Snort/etc` and open the `snort.conf` file.

```
79
80  # List of ports you might see oracle attacks on
81  portvar ORACLE_PORTS 1024:
82
83  # List of ports you want to look for SSH connections on:
84  portvar SSH_PORTS 22
85
86  # List of ports you run ftp servers on
87  portvar FTP_PORTS [21,2100,3535]
88
89  # List of ports you run SIP servers on
90  portvar SIP_PORTS [5060,5061,5600]
91
92  # List of file data ports for file inspection
93  portvar FILE_DATA_PORTS [$HTTP_PORTS,110,143]
94
95  # List of GTP ports for GTP preprocessor
96  portvar GTP_PORTS [2123,2152,3386]
97
98  # other variables, these should not be modified
99  var AIM_SERVERS [64.12.24.0/23,64.12.28.0/23,64.12.161.0/24,64.12.163.0/24,64.12.200.0/24,
100
101  # Path to your rules files (this can be a relative path)
102  # Note for Windows users: You are advised to make this an absolute path,
103  # such as: c:\snort\rules
104  var RULE_PATH C:\Snort\rules
105  #var SO_RULE_PATH ../so_rules
106  var SO_RULE_PATH C:\Snort\rules
107  #var PREPROC_RULE_PATH ../preproc rules
```

## 2. Set up Local Rules

- Navigate to `C:/Snort/bin` and open the `local.rules` file.
- Add the following rules to detect ICMP, HTTP, and DNS traffic:
  - ICMP Rule:**

```
alert icmp any any -> $HOME_NET any (msg:"ICMP traffic detected";
```

```
sid:1000001; rev:1;)
```

- **HTTP Rule:**

```
alert tcp any any -> $HOME_NET 80 (msg:"HTTP traffic detected";  
sid:1000002; rev:1;)
```

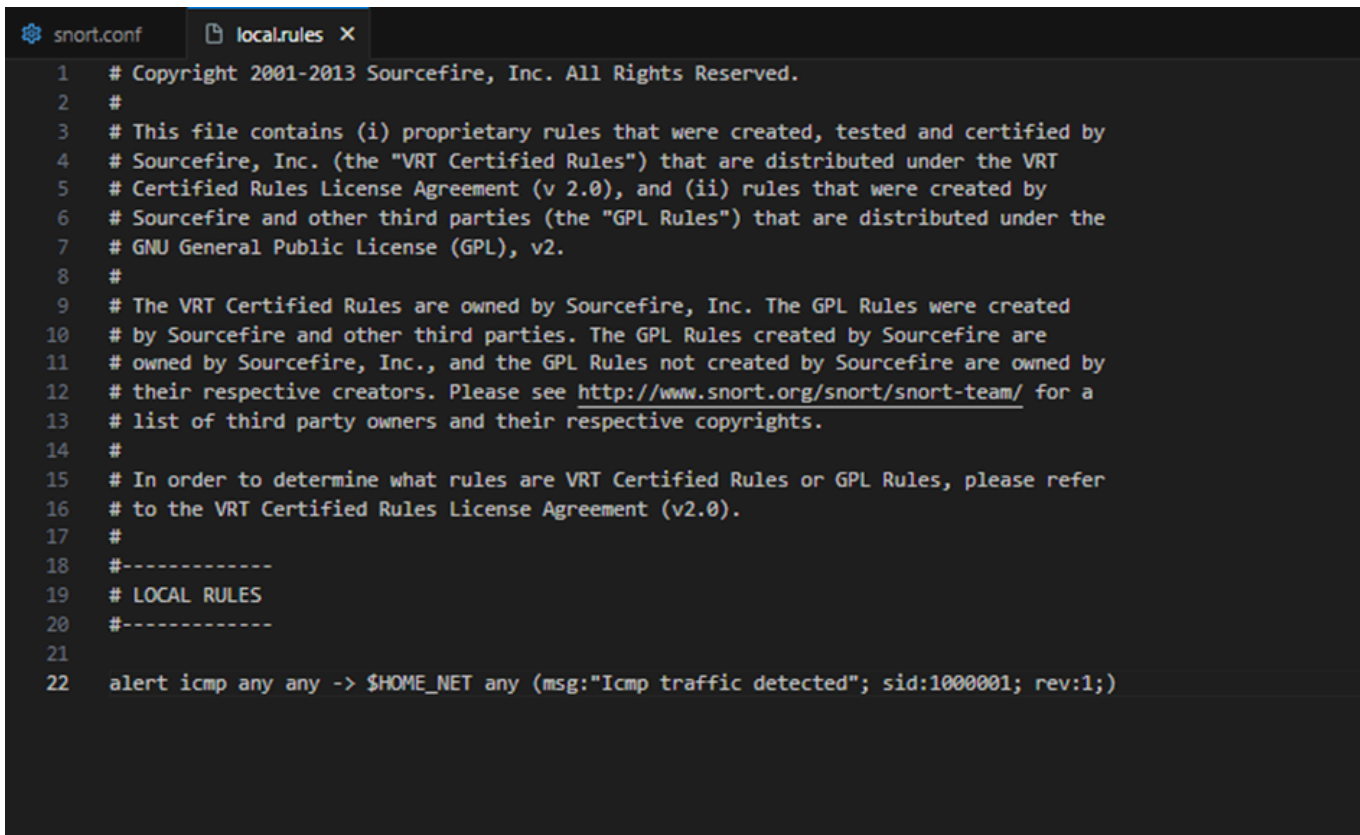
- **DNS Rules:**

- For **TCP**:

```
alert tcp any any -> $HOME_NET 53 (msg:"DNS traffic detected";  
sid:1000004; rev:1;)
```

- For **UDP**:

```
alert udp any any -> $HOME_NET 53 (msg:"DNS query traffic  
detected"; sid:1000003; rev:1;)
```



```
snort.conf  local.rules X  
1  # Copyright 2001-2013 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  
22 alert icmp any any -> $HOME_NET any (msg:"Icmp traffic detected"; sid:1000001; rev:1;)
```

### 3. Verify Network Interfaces

- Open Command Prompt as an administrator.

- Run:

```
snort -W
```

This command lists all available network interfaces. Note the interface number you'll use for running Snort.

```
C:\Snort\bin>Snort -W

--> Snort! <*-
o"  )~
....
Version 2.9.20-WIN64 GRE (Build 82)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using 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_{96907A2C-0F70-41DA-BC24-090C993F3900}  WAN Miniport (Network Monitor)
2  00:00:00:00:00:00      disabled      \Device\NPF_{481C5FF9-A01C-4DDA-B776-F3EAB9C74880}  WAN Miniport (IPv6)
3  00:00:00:00:00:00      disabled      \Device\NPF_{4EF4CBD5-9502-4BB4-A9D1-5828000352BA}  WAN Miniport (IP)
4  38:7A:0E:01:4E:8D      192.168.187.156 \Device\NPF_{1DB82A1C-8330-4F79-A6A7-E1A55692A3B4}  Intel(R) Wi-Fi 6E AX211 160MHz
5  3A:7A:0E:01:4E:8D      169.254.12.204 \Device\NPF_{D42B3C08-1D64-433D-853E-39DA0EF683A7}  Microsoft Wi-Fi Direct Virtual Adapter #2
6  38:7A:0E:01:4E:8E      169.254.22.108 \Device\NPF_{B880E500-E09E-4DB4-A8D7-387C38C27AE8}  Microsoft Wi-Fi Direct Virtual Adapter
7  0A:00:27:00:00:13      192.168.56.1   \Device\NPF_{D3EA9A98-5E67-40BB-AFE6-70D1919383BE}  VirtualBox Host-Only Ethernet Adapter
8  00:00:00:00:00:00      0000:0000:0000:0000:0000:0000 \Device\NPF_Loopback Adapter for loopback traffic capture
```

## 4. Test the Snort Configuration

- To test your configuration, run:

```
snort -c C:/Snort/etc/snort.conf -i <interface_number> -T
```

## 5. Start Snort in Console Mode

- Run Snort in live mode with:

```
snort -c C:/Snort/etc/snort.conf -i <interface_number> -A console
```

## 6. Testing the Rules

```
Administrator: Command Prompt - Snort -i 5 -c C:\Snort\etc\snort.conf -A console
Snort exiting

C:\Snort\bin>Snort -i 5 -c C:\Snort\etc\snort.conf -A console
Running in IDS 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 1
414 1741 1830 2301 2381 2809 3037 3128 3702 4343 4848 5250 6988 70
00:7001 7144:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 808
8 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 5
93 901 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 8
899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 500
02 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_dyna
micpreprocessor...
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamiccp
reprocessor\sf_dce2.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamiccp

Command Prompt
Microsoft Windows [Version 10.0.22631.4317]
(c) Microsoft Corporation. All rights reserved.

C:\Users\devam>ping google.com

Pinging google.com [142.250.71.110] with 32 bytes of data:
Reply from 142.250.71.110: bytes=32 time=43ms TTL=114
Reply from 142.250.71.110: bytes=32 time=45ms TTL=114
Reply from 142.250.71.110: bytes=32 time=47ms TTL=114
Reply from 142.250.71.110: bytes=32 time=47ms TTL=114

Ping statistics for 142.250.71.110:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 43ms, Maximum = 47ms, Average = 45ms

C:\Users\devam>
```

```
Administrator: Command Prompt - Snort -i 5 -c C:\Snort\etc\snort.conf -A console
Build 1> Rules Engine: SF_SNORT_DETECTION_ENGINE Version 3.2 <

Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
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>

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_FTPTELNET Version 1.2 <Build 1>

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>

Commencing packet processing (pid=29188)
10/14-15:19:00.950412  [*] [1:10000001:1] ICMP traffic detected [
**] [Priority: 0] {ICMP} 142.250.71.110 -> 10.7.88.252
10/14-15:19:01.964512  [*] [1:10000001:1] ICMP traffic detected [
**] [Priority: 0] {ICMP} 142.250.71.110 -> 10.7.88.252

Command Prompt
Microsoft Windows [Version 10.0.22631.4317]
(c) Microsoft Corporation. All rights reserved.

C:\Users\devam>ping google.com

Pinging google.com [142.250.71.110] with 32 bytes of data:
Reply from 142.250.71.110: bytes=32 time=43ms TTL=114
Reply from 142.250.71.110: bytes=32 time=45ms TTL=114
Reply from 142.250.71.110: bytes=32 time=47ms TTL=114
Reply from 142.250.71.110: bytes=32 time=47ms TTL=114

Ping statistics for 142.250.71.110:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 43ms, Maximum = 47ms, Average = 45ms

C:\Users\devam>
```