

<b>Ex. No : 9</b> <b>Date :</b>	<b>Demonstration of Intrusion Detection System(IDS)</b>
------------------------------------	---

**AIM:**

To demonstrate Intrusion Detection System (IDS) using Snort software tool.

**STEPS ON CONFIGURING AND INTRUSION DETECTION:**

1. Download Snort from the Snort.org website. (<http://www.snort.org/snort-downloads>)
2. Download Rules(<https://www.snort.org/snort-rules>). You must register to get the rules. (You should download these often)
3. Double click on the .exe to install snort. This will install snort in the “C:\Snort” folder. It is important to have WinPcap (<https://www.winpcap.org/install/>) installed
4. Extract the Rules file. You will need WinRAR for the .gz file.
5. Copy all files from the “rules” folder of the extracted folder. Now paste the rules into “C:\Snort\rules” folder.
6. Copy “snort.conf” file from the “etc” folder of the extracted folder. You must paste it into “C:\Snort\etc” folder. Overwrite any existing file. Remember if you modify your snort.conf file and download a new file, you must modify it for Snort to work.
7. Open a command prompt (cmd.exe) and navigate to folder “C:\Snort\bin” folder. ( at the Prompt, type cd\snort\bin)
8. To start (execute) snort in sniffer mode use following command:  
snort -dev -i 3  
-i indicates the interface number. You must pick the correct interface number. In my case, it is 3.  
-dev is used to run snort to capture packets on your network.

To check the interface list, use following command:

snort -W

```
Administrator: C:\Windows\system32\cmd.exe
Total Memory Allocated: 0
=====
Snort exiting
C:\Snort\bin>snort -W

o"~>~
) ) ) )

-*> Snort! <*-
Version 2.9.6.0-WIN32 GRE (Build 47)
By Martin Roesch & The Snort Team: http://www.snort.org/snort/snort-team

Copyright (C) 2014 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: 1.2.3

Index   Physical Address      IP Address      Device Name      Description
-----
1       00:00:00:00:00:00      0000:0000:fe80:0000:0000:0000:78d2:6299 \Device\
NPF_{45DAC1EF-70A2-4C33-B712-AE311620EB7A} VMware Virtual Ethernet Adapter
2       00:00:00:00:00:00      0000:0000:fe80:0000:0000:0000:bca3:2f56 \Device\
NPF_{C355D233-3D77-484F-A344-65626159980E} VMware Virtual Ethernet Adapter
3       00:00:00:00:00:00      0000:0000:fe80:0000:0000:0000:ada3:46c9 \Device\
NPF_{3264BC0F-4BF2-49C5-B5D9-A12EFE40F17C} Microsoft

C:\Snort\bin>
```

Finding an interface

You can tell which interface to use by looking at the Index number and finding Microsoft. As you can see in the above example, the other interfaces are for VMWare. My interface is 3.

- 9. To run snort in IDS mode, you will need to configure the file “snort.conf” according to your network environment.
- 10. To specify the network address that you want to protect in snort.conf file, look for the following line.  
var HOME\_NET 192.168.1.0/24 (You will normally see any here)
- 11. You may also want to set the addresses of DNS\_SERVERS, if you have some on your network.

Example:

example snort

- 12. Change the RULE\_PATH variable to the path of rules folder.  
var RULE\_PATH c:\snort\rules

path to rules

**13.** Change the path of all library files with the name and path on your system. and you must change the path of snort\_dynamicpreprocessorvariable.

C:\Snort\lib\snort\_dynamicccpreprocessor

You need to do this to all library files in the “C:\Snort\lib” folder. The old path might be: “/usr/local/lib/...”. you will need to replace that path with your system path. Using C:\Snort\lib

**14.** Change the path of the “dynamicengine” variable value in the “snort.conf” file..

Example:

dynamicengine C:\Snort\lib\snort\_dynamicengine\sf\_engine.dll

**15** Add the paths for “include classification.config” and “include reference.config” files.

include c:\snort\etc\classification.config

include c:\snort\etc\reference.config

**16.** Remove the comment (#) on the line to allow ICMP rules, if it is commented with a #.

include \$RULE\_PATH/icmp.rules

**17.** You can also remove the comment of ICMP-info rules comment, if it is commented.

include \$RULE\_PATH/icmp-info.rules

**18.** To add log files to store alerts generated by snort, search for the “output log” test in snort.conf and add the following line:

output alert\_fast: snort-alerts.ids

**19.** Comment (add a #) the whitelist \$WHITE\_LIST\_PATH/white\_list.rules and the blacklist

Change the nested\_ip inner , \ to nested\_ip inner #, \

**20.** Comment out (#) following lines:

#preprocessor normalize\_ip4

#preprocessor normalize\_tcp: ips ecn stream

#preprocessor normalize\_icmp4

#preprocessor normalize\_ip6

#preprocessor normalize\_icmp6

21. Save the “snort.conf” file.

22. To start snort in IDS mode, run the following command:

```
snort -c c:\snort\etc\snort.conf -l c:\snort\log -i 3
```

(Note: 3 is used for my interface card)

If a log is created, select the appropriate program to open it. You can use WordPad or NotePad++ to read the file.

To generate Log files in ASCII mode, you can use following command while running snort in IDS mode:

```
snort -A console -i3 -c c:\Snort\etc\snort.conf -l c:\Snort\log -K ascii
```

23. Scan the computer that is running snort from another computer by using PING or NMap (ZenMap).

After scanning or during the scan you can check the snort-alerts.ids file in the log folder to insure it is logging properly. You will see IP address folders appear.

Snort monitoring traffic –

```
Administrator: C:\Windows\system32\cmd.exe - snort -A console -i3 -c c:\Snort\etc\snort.conf -l c:\Snort\log
Rules Engine: SF_SNORT_DETECTION_ENGINE Version 2.1 <Build 1>
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>
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_GIP Version 1.1 <Build 1>
Preprocessor Object: SF_FIPIELNET Version 1.2 <Build 13>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_DMP3 Version 1.1 <Build 1>
Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>
Commencing packet processing (pid=2164)
03/29-23:53:16.033913 [**] [120:3:1] <http_inspect> NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE [**] [Classification: Unknown Traffic] [Priority: 3]
1 (TCP) 192.168.1.1:80 -> 192.168.1.20:56506
03/29-23:53:16.035372 [**] [120:3:1] <http_inspect> NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE [**] [Classification: Unknown Traffic] [Priority: 3]
1 (TCP) 192.168.1.1:80 -> 192.168.1.20:56507
03/29-23:53:16.036479 [**] [120:3:1] <http_inspect> NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE [**] [Classification: Unknown Traffic] [Priority: 3]
1 (TCP) 192.168.1.1:80 -> 192.168.1.20:56508
03/29-23:53:16.037093 [**] [120:3:1] <http_inspect> NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE [**] [Classification: Unknown Traffic] [Priority: 3]
1 (TCP) 192.168.1.1:80 -> 192.168.1.20:56509
03/29-23:53:16.142921 [**] [120:3:1] <http_inspect> NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE [**] [Classification: Unknown Traffic] [Priority: 3]
1 (TCP) 192.168.1.1:80 -> 192.168.1.20:302
03/29-23:53:16.194409 [**] [120:3:1] <http_inspect> NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE [**] [Classification: Unknown Traffic] [Priority: 3]
1 (TCP) 192.168.1.1:80 -> 192.168.1.20:56510
03/29-23:53:16.677078 [**] [120:3:1] <http_inspect> NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE [**] [Classification: Unknown Traffic] [Priority: 3]
1 (TCP) 192.168.1.1:80 -> 192.168.1.20:56512
03/29-23:53:16.808301 [**] [120:3:1] <http_inspect> NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE [**] [Classification: Unknown Traffic] [Priority: 3]
1 (TCP) 192.168.1.1:80 -> 192.168.1.20:56513
03/29-23:53:16.944237 [**] [120:3:1] <http_inspect> NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE [**] [Classification: Unknown Traffic] [Priority: 3]
1 (TCP) 192.168.1.1:80 -> 192.168.1.20:56514
03/29-23:53:16.948012 [**] [120:3:1] <http_inspect> NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE [**] [Classification: Unknown Traffic] [Priority: 3]
1 (TCP) 192.168.1.1:80 -> 192.168.1.20:56515
03/29-23:53:16.953992 [**] [120:3:1] <http_inspect> NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE [**] [Classification: Unknown Traffic] [Priority: 3]
1 (TCP) 192.168.1.1:80 -> 192.168.1.20:56516
03/29-23:53:16.967744 [**] [120:3:1] <http_inspect> NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE [**] [Classification: Unknown Traffic] [Priority: 3]
1 (TCP) 192.168.1.1:80 -> 192.168.1.20:56517
03/29-23:53:16.982649 [**] [120:3:1] <http_inspect> NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE [**] [Classification: Unknown Traffic] [Priority: 3]
1 (TCP) 192.168.1.1:80 -> 192.168.1.20:56518
```

## RESULT:

Thus the Intrusion Detection System(IDS) has been demonstrated by using the Open Source Snort Intrusion Detection Tool.