**EXPNO:- Date:**

**AIM:** To demonstrate intrusion detection system (ids) using the tool snort

**PROCEDURE:**

**1.Configure and Use Snort IDS on Windows**

Steps to configure Snort on Widnows machine and how to use it for detection of attacks.

**2. Steps:**

1. Download Snort from "http://www.snort.org/" website.

2. Also download Rules from the same website. You need to sign up to get rules for registered

Users.

3. Click on the Snort\_(version-number)\_Installer.exe file to install it. By-default it will

install snort in the "C:\Snort" directory.

4. Extract downloaded Rules file: snortrules-snapshot-(number).tar.gz

5. Copy all files from the "rules" directory of the extracted folder and paste them

into " C:\Snort\rules" directory.

6. Copy "snort.conf" file from the "etc" directory of the extracted folder and paste it

into "C:\Snort\etc" directory. Overwrite existing file if there is any.

7. Open command prompt (cmd.exe) and navigate to directory "C:\Snort\bin" directory.

8. To execute snort in sniffer mode use following command:

snort -dev -i 2

-i indicate interface number.

-dev is used to run snort to capture packets.

To check interface list use following command: snort -W

9. To execute snort in IDS mode, we need to configure a file "snort.conf" according to

our network environment.

10. Set up network address we want to protect in snort.conf file. To do that look for

"HOME\_NET" and add your IP address.

var HOME\_NET 10.1.1.17/8

11. You can also set addresses or DNS\_SERVERS, if you have any. otherwise go to the

next step.

12. Change RULE\_PATH variable with the path of rules directory.

var RULE\_PATH c:\snort\rules

13. Change the path of all libraries with the name and path on your system. or change path

of snort\_dynamicpreprocessorvariable.

sor file C:\Snort\lib\snort\_dynamiccpreprocessor\sf\_dcerpc.dll

You need to do this to all library files in the "C:\Snort\lib" directory. The old path might be

something like: "/usr/local/lib/...". you need to replace that path with you system path.

14. Change path of the "dynamicengine" variable value in the "snort.conf" file with the path

of your system. Such as: dynamicengine C:\Snort\lib\snort\_dynamicengine\sf\_engine.dll

15. Add complete path 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 alredy commented.

include $RULE\_PATH/icmp.rules

17. Similary, remove the comment of ICMP-info rules comment, if it is already commented.

include $RULE\_PATH/icmp-info.rules

18 To add log file to store alerts generated by snort, search for "output log" test and

add following line:

output alert\_fast: snort-alerts.ids

19. Comment whitelist $WHITE\_LIST\_PATH/white\_list.rules and blacklist

$BLACK\_LIST\_PATH/black\_list.rules lines. Also ensure that you add change the

line above $WHITE\_LIST\_PATH

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

20. Comment 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 and close it.

22. Go to the "C:\Snort\log" directory and create a file: snort-alerts.ids

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

snort -c c:\snort\etc\snort.conf -l c:\snort\log -i 2

Above command will generate log file that will not be readable without using a tool. To

read it use following command:

C:\Snort\Bin\> snort -r ..\log\log-filename

To generate Log files in ASCII mode use following command while running snort in IDS

mode:

snort -A console -i2 -c c:\Snort\etc\snort.conf -l c:\Snort\log -K ascii

24. Scan the computer running snort from another computer using PING or launch attack. Then

check snort-alerts.ids file the log folder.