INTRUSION DETECTION SYSTEM

AIM : To install, configure and test the Intrusion Detection System Snort.

STEPS :

1. Double-click the WinPcap_4_1_3.exe installer and the follow the on-screen prompts.
2. Double-click the Snort_2_9_8_2_Installer.exe and follow the on-screen prompts.
3. Create a sub-folder under c:\Snort called "rules" and another one called "preproc_rules".
4. Open the Snort rules package.
5. Extract the contents of the "rules" folder in the archive to c:\Snort\rules.
6. Extract the contents of the "preproc_rules" folder in the archive to c:\Snort\preproc_rules.
7. Ignore contents of so_rules folder and etc folder.
8. Change to Snort program directory : cd \snort\bin
9. Check the installed version for Snort : snort -V
10. Check network interfaces : snort -W
11. Open C:\Snort\etc\snort.conf and do the following

Step 1: Set the network variables

```
ipvar HOME_NET 10.0.0.0/8
ipvar EXTERNAL_NET !$HOME_NET
var RULE_PATH c:\Snort\rules
#var SO_RULE_PATH ../so_rules
(comment out)
var PREPROC_RULE_PATH c:\Snort\prepoc_rules
```

Step 2: Configure the decoder

```
config logdir: c:\Snort\log
(uncomment)
```

Step 3: Configure the base detection engine (NO CHANGES)

Step 4: Configure dynamic loaded libraries

```
dynamicpreprocessor directory c:\Snort\lib\snort_dynamicpreprocessor
dynamicengine c:\Snort\lib\snort_dynamicengine\sf_engine.dll
# dynamicdetection directory /usr/local/lib/snort_dynamicrules
(comment out)
```

Step 5: Configure preprocessors

Normalization Preprocessor (Comment out all lines)

```
#preprocessor normalize_ip4
#preprocessor normalize_tcp: ips ecn stream
#preprocessor normalize_icmp4
#preprocessor normalize_ip6
#preprocessor normalize_icmp6
```

Reputation Preprocessor (Comment out all lines)

```
#preprocessor reputation: \
#memcap 500, \
#priority whitelist, \
#nested_ip inner, \
#whitelist $WHITE_LIST_PATH/white_list.rules, \
#blacklist $BLACK_LIST_PATH/black_list.rules
```

If Reputation Preprocessor is not commented, then you will need to create blacklist and whitelist rules files.

Step 6: Configure output plugins (NO CHANGES)
Step 7: Customize your rule set (NO CHANGES)
Step 8: Customize preprocessor and decoder rule set

(Uncomment these lines and change / to \)

```
include $PREPROC_RULE_PATH\preprocessor.rules
include $PREPROC_RULE_PATH\decoder.rules
```

Step 9: Customize shared object rule set (NO CHANGES)

12. Open c:\Snort\rules\local.rules and add these rules.

```
alert icmp any any -> any any (msg:"ICMP Testing Rule"; sid:1000001; rev:1;)
alert tcp any any -> any 80 (msg:"TCP Testing Rule"; sid:1000002; rev:1;)
alert udp any any -> any any (msg:"UDP Testing Rule"; sid:1000003; rev:1;)
```

13. Run command prompt as administrator.
14. Start Snort using the -A option

```
cd \Snort\bin
snort -i 1 -c c:\Snort\etc\snort.conf -A console
```

14. Open another command prompt and send a ping to some host.

```
ping google.com
```

15. Open web browser and browse any page.
16. Check the alerts in the first command prompt.
17. To stop Snort, press Ctrl + C.
18. View the statistics that are displayed.