

INTRUSION DETECTION SYSTEM

Date:

AIM:

To demonstrate intrusion detection systems like snort.

PROCEDURE:

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.
3. Double click on the .exe to install snort. This will install snort in “C:\Snort” folder. Also install winpcap.
4. Extract the Rules file.
5. Copy all files from the “rules” folder of the extracted folder to “C:\Snort\rules” folder.
6. Copy the “snort.conf” file from the “etc” folder of the extracted folder and paste it in “C:\Snort\etc” folder. Overwrite Any existing file.
7. Open a command prompt (cmd.exe) and navigate to folder “C:\Snort\bin”.
8. Start snort in sniffer mode using the command “snort -dev -i3”. -i indicates the interface number. It’s to be selected carefully after inspection of the interfaces using the command “snort -w”.

OUTPUT:

```
C:\Windows\system32\cmd.exe
G:\Snort>snort -U

o's'~>
-==> Snort! <==
Version 2.9.20-UM64 GRE (Build 82)
19 Martin Roesch & The Snort Team: http://www.snort.org/contactteam
Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.

ved.
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_{DFA9D2C8-8742-4EB1-
9703-D09C4A13F232} WM Miniport (PTTP) disabled
2 00:00:00:00:00:00 disabled \Device\NPF_{E43D242B-7EAB-4626-
A952-46647FBB7393} WM Miniport (L2TP) disabled
3 00:00:00:00:00:00 disabled \Device\NPF_{71F897D7-EB7C-408D-
89DB-AC88D9D22270} WM Miniport (CSSTP) disabled
4 00:00:00:00:00:00 disabled \Device\NPF_{C83B1A52-AFF0-4F49-
B9CA-C798961A0563} WM Miniport (PPPOE) disabled
5 40:08:0F:05:6E:2B 10.10.46.47 \Device\NPF_{17FF0252-6062-428F-
B30F-D9FC735C7215} Realtek PCIe GBE Family Controller
6 00:00:00:00:00:00 disabled \Device\NPF_{0000:0000:0000:0000} \Device\
NPF_{loopback} loopback for local traffic capture
7 00:00:00:00:00:00 disabled \Device\NPF_{C29898C9D-B004-4FEF-
BDB6-57H562022CEE} WM Miniport <IRE02>

G:\Snort>bin
```

[illegible]

RESULT:

Thus the program to demonstrate IDS (snort) has been executed successfully and the output is verified.