

Aim: Set up, configuration and use of SNORT for Intrusion Detection

Theory:

Snort is an open source network intrusion prevention and detection system (IDS/IPS) developed by Sourcefire. Combining the benefits of signature, protocol, and anomaly-based inspection, Snort is the most widely deployed IDS/IPS technology worldwide. With millions of downloads and nearly 400,000 registered users, Snort has become the de facto standard for IPS.

Snort can be configured to run in three modes:

1. Sniffer mode : It simply reads the packets off of the network and displays them for you in a continuous stream on the console (screen)
2. Packet Logger mode : logs the packets to disk
3. Network Intrusion Detection System (NIDS) mode: it performs detection and analysis on network traffic. This is the most complex and configurable mode

Steps:

1. Get root access

```
$ sudo su root
```

2. Do updation

```
# apt-get update
```

3. Installation

```
# apt-get install snort
```

During installation:

- Put the name of network interface (by default it is eth0, change it to the interface name of your machine)
- Put the IP address of the machine followed by /24 (by default it is the network address. Replace it with your IP addr/24)

4. Configuration

```
# cd /etc
```

```
# ls
```

```
# cd /snort
```

```
# ls
```

```
# gedit snort.conf
```

Go to line no. 51

```
ipvar HOME_NET any
```

Replace “any” with your ip address i.e. ipvar HOME_NET 192.168.208.22

Save and close the file

5. Monitoring

snort -q -A console -i enp2s0

enp2s0 is the name of the interface

```
-----
[ Number of patterns truncated to 20 bytes: 1039 ]
pcap DAQ configured to passive.
Acquiring network traffic from "enp1s0".

--== Initialization Complete ==--

-*> Snort! <*-
0''')- Version 2.9.7.0 GRE (Build 149)
''')- By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
      Copyright (C) 2014 Cisco and/or its affiliates. All rights reserved.
      Copyright (C) 1998-2013 Sourcefire, Inc., et al.
      Using libpcap version 1.7.4
      Using PCRE version: 8.38 2015-11-23
      Using ZLIB version: 1.2.8

Rules Engine: SF_SNORT_DETECTION_ENGINE Version 2.4 <Build 1>
Preprocessor Object: SF_DCEP2C2 Version 1.0 <Build 3>
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Preprocessor Object: SF_SDF Version 1.1 <Build 1>
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>

Snort successfully validated the configuration!
Snort exiting
root@Admin:/etc/snort# █
```

6. Perform the following nmap command on neighbour's machine and observe the output in your machine

\$ nmap ip addr of your machine (This command is to be performed on neighbour's machine)

Output to be observed in SNORT terminal: IP address of the neighbour who is performing Intrusion i.e. Port Scanning

```
root@Admin:/etc/snort# snort -A console -q -c /etc/snort/snort.conf -i enp1s0
02/27-14:22:39.662751 00000000 [**] [1:1418:11] SNMP request tcp [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.0.106:41496 -> 192.168.0.107:161
02/27-14:22:39.705250 00000000 [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.0.106:41496 -> 192.168.0.107:705
02/27-14:23:17.962480 00000000 [**] [1:1418:11] SNMP request tcp [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.0.106:53600 -> 192.168.0.107:161
02/27-14:23:17.999881 00000000 [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.0.106:53600 -> 192.168.0.107:705
02/27-14:24:06.858571 00000000 [**] [1:1418:11] SNMP request tcp [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.0.133:36483 -> 192.168.0.107:161
02/27-14:24:06.879732 00000000 [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.0.133:36483 -> 192.168.0.107:705
```