# **SNORT IDS**

#### AIM:

To demonstrate Intrusion Detection System (IDS) using snort tool.

## ALGORITHM:

- 1. Download and extract the latest version of daq and snort
- 2. Install development packages libpcap and pcre.
- 3. Install daq and then followed by snort.
- 4. Verify the installation is correct.
- 5. Create the configuration file, rule file and log file directory
- 6. Create snort.conf and icmp.rules files
- 7. Execute snort from the command line
- 8. Ping to yahoo website from another terminal
- 9. Watch the alert messages in the log files

#### **OUTPUT:**

```
[root@localhost security lab]# cd /usr/src
```

[root@localhost security lab]# wget https://www.snort.org/downloads/snort/daq-2.0.7.tar.gz [root@localhost security lab]# wget https://www.snort.org/downloads/snort/snort-

## 2.9.16.1.tar.gz

```
[root@localhost security lab]# tar xvzf daq-2.0.7.tar.gz
```

[root@localhost security lab]# tar xvzf snort-2.9.16.1.tar.gz

[root@localhost security lab]# yum install libpcap\* pcre\* libdnet\* -y

[root@localhost security lab]# cd dag-2.0.7

[root@localhost security lab]#./configure

[root@localhost security lab]# make

[root@localhost security lab]# make install

[root@localhost security lab]# cd snort-2.9.16.1

[root@localhost security lab]#./configure

[root@localhost security lab]# make

[root@localhost security lab]# make install

[root@localhost security lab]# snort --version

,, -\*> Snort! <\*-

o" > Version 2.9.8.2 GRE (Build 335)

"" By Martin Roesch & The Snort Team: http://www.snort.org/contact#team Copyright (C) 2014-2015 Cisco and/or its affiliates. All rights reserved. Copyright (C) 1998-2013 Sourcefire, Inc., et al.

Using libpcap version 1.7.3

Using PCRE version: 8.38 2015-11-23 Using ZLIB version: 1.2.8

[root@localhost security lab]# mkdir /etc/snort [root@localhost security lab]# mkdir

## /etc/snort/rules

[root@localhost security lab]# mkdir /var/log/snort [root@localhost security lab]# vi /etc/snort/snort.conf

add this line- include /etc/snort/rules/icmp.rules

[root@localhost security lab]# vi /etc/snort/rules/icmp.rules

alert icmp any any -> any any (msg:"ICMP Packet"; sid:477; rev:3;)

[root@localhost security lab]# snort -i enp3s0 -c /etc/snort/snort.conf -l /var/log/snort/

## **Another terminal**

[root@localhost security lab]# ping www.yahoo.com Ctrl + C

[root@localhost security lab]# vi /var/log/snort/alert

[\*\*] [1:477:3] ICMP Packet [\*\*] [Priority: 0]

10/06-15:03:11.187877 192.168.43.148 -> 106.10.138.240

ICMP TTL:64 TOS:0x0 ID:45855 IpLen:20 DgmLen:84 DF Type:8 Code:0 ID:14680 Seq:64 ECHO

[\*\*] [1:477:3] ICMP Packet [\*\*] [Priority: 0]

10/06-15:03:11.341739 106.10.138.240 -> 192.168.43.148

ICMP TTL:52 TOS:0x38 ID:2493 IpLen:20 DgmLen:84 Type:0 Code:0 ID:14680 Seq:64 ECHO REPLY

[\*\*] [1:477:3] ICMP Packet [\*\*] [Priority: 0]

10/06-15:03:12.189727 192.168.43.148 -> 106.10.138.240

ICMP TTL:64 TOS:0x0 ID:46238 IpLen:20 DgmLen:84 DF Type:8 Code:0 ID:14680 Seq:65 ECHO

[\*\*] [1:477:3] ICMP Packet [\*\*] [Priority: 0]

10/06-15:03:12.340881 106.10.138.240 -> 192.168.43.148

ICMP TTL:52 TOS:0x38 ID:7545 IpLen:20 DgmLen:84 Type:0 Code:0 ID:14680 Seq:65 ECHO REPLY

## **RESULT:**

Thus, Intrusion Detection System (IDS) using snort tool has been demonstrated.