Exp. No.: 10 **Date:**

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 daq-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!

Result: