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

SNORTIDS

Aim:

TodemonstrateIntrusionDetectionSystem(IDS)usingsnorttool.

Algorithm:

1.Downloadandextractthelatestversionofdaqandsnort2.Install development packages - libpcap and pcre.

3. Installdaqandthenfollowedbysnort.
4. Verifytheinstallationiscorrect.
5. Createtheconfigurationfile,rulefileandlogfiledirectory
6. Createsnort.confandicmp.rulesfiles
7. Executesnortfromthecommand line
8. Pingtoyahoowebsitefromanotherterminal
9. Watchthealertmessagesinthelogfiles

Output:

[root@localhostsecuritylab]#cd/usr/src
[root@localhostsecuritylab]#wgethttps://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@localhostsecuritylab]#tarxvzfdaq-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@localhostsecurity lab]# cd daq-2.0.7
[root@localhostsecuritylab]#./configure[root@localhostsecuritylab]#make
[root@localhost security lab]# make install

[root@localhostsecuritylab]#cdsnort-2.9.16.1[root@localhostsecuritylab]#. /configure[root@localhostsecurity lab]#make [root@localhostsecuritylab]# makeinstall[root@localhostsecuritylab]#snort--version,,_-*>Snort!<*- o")~ Version 2.9.8.2 GRE (Build 335)

"" By Martin Roesch & The SnortTeam: http://www.snort.org/contact#team
Copyright(C)2014-2015Ciscoand/oritsaffiliates.Allrightsreserved.Copyright
(C)1998-2013Sourcefire,Inc.,etal. Using
libpcap version 1.7.3
UsingPCREversion:8.382015-11-23UsingZLIBversion:1.2.8 [root@localhost
security lab]# mkdir /etc/snort
[root@localhostsecuritylab]#mkdir/etc/snort/rules

[root@localhost security lab]# mkdir /var/log/snort
[root@localhostsecuritylab]#vi/etc/snort/snort.confadd
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@localhostsecuritylab]#snort-ienp3s0-c/etc/snort/snort.conf-l
/var/log/snort/Anotherterminal
[root@localhostsecuritylab]#pingwww.yahoo.comCtrl+C [root@localhost
security lab]# vi /var/log/snort/alert

[**][1:477:3]ICMPPacket[**][Priority:0]
10/06-15:03:11.187877192.168.43.148->106.10.138.240
ICMPTTL:64TOS:0x0ID:45855IpLen:20DgmLen:84DFType:8Code:0 ID:14680
Seq:64 ECHO

[**][1:477:3]ICMPPacket[**][Priority:0]
10/06-15:03:11.341739106.10.138.240->192.168.43.148
ICMPTTL:52TOS:0x38ID:2493IpLen:20DgmLen:84Type:0Code:0ID:14680 Seq:64
ECHO REPLY

[**][1:477:3]ICMPPacket[**][Priority:0]
10/06-15:03:12.189727192.168.43.148->106.10.138.240
ICMPTTL:64TOS:0x0ID:46238IpLen:20DgmLen:84DFType:8Code:0 ID:14680
Seq:65 ECHO

[**][1:477:3]ICMPPacket[**][Priority:0]

10/06-15:03:12.340881106.10.138.240->192.168.43.148
ICMPTTL:52TOS:0x38ID:7545IpLen:20DgmLen:84Type:0Code:0ID:14680 Seq:65
ECHO REPLY

Result: