Animesh Parab T2-T21 88

LAB ASSIGNMENT No. 11

Aim: Installing snort, configuring it in Intrusion Detection mode and writing rules for detecting pinging activity.

Lab Outcome Attained: LO6 **Theory:**

Steps to Install snort and configure it in Intrusion Detection Mode.

1. Check the name of the interface using command ifconfig.
2. Install snort in ubuntu machine using command *sudo apt-get install snort*
3. While installing the snort, name of the interface will be asked on which snort is supposed to listen. Enter the interface name observed in step 1.
4. Run the command *sudo gedit /etc/snort/snort.conf* . This opens snort configuration file.
5. Make following changes to configuration file.

   a. ipvar HOME_NET **192.168.0.0/24 (in section 1)**
6. Open new terminal. Open ftp.rule file in it by typing the command *sudo gedit /etc/snort/rules/ftp.rules (optional)*
7. Open new terminal and type the command *sudo snort -T -c /etc/snort/snort.conf -i* ***enp3s0*** to validate that all rules are there.

   We use the

   -T flag to test the configuration file,

   -c flag to tell Snort which configuration file to use, and -i to specify the interface that Snort will listen on.

8. Type the command *sudo snort -A console -q -u snort -g snort -c /etc/snort/snort.conf -i enp3s0* (to start snort in NIDS mode)

   We use the

   -A console The 'console' option prints fast mode alerts to stdout -q Quiet mode. Don't show banner and status report.

   -u snort Run Snort as the following user after startup

-g snort Run Snort as the following group after startup

-c /etc/snort/snort.conf The path to our snort.conf file

-i enp3s0 The interface to listen on (change to your interface if different)

9. Now go to kali linux machine.

10. Type command *nmap 192.168.0.107* on it to start port scanning of ubuntu machine and observe the output in terminal where snort is started in detection environment.

When you execute this command, you will not initially see any output. Snort is running, and is processing all packets that arrive on eth0 (or whichever interface you specified with the -i flag). Snort compares each packet to the rules it has loaded (in this case our single ICMP Ping rule), and will then print an alert to the console when a packet matches our rule.

11. Then try pinging ubuntu machine by typing the command *ping 192.168.0.107* and observe the output in terminal where snort is started in detection mode.

---

12. Adding rule for detecting ping activity performed by another machine:

---

a. In ubuntu machine, type the following command to create a file called local.rules : ***sudo gedit /etc/snort/rules/local.rules***

b. Write the following rule in it: ***alert icmp any any -> $HOME_NET any (msg:"ICMP test detected"; GID:1; sid:10000001; rev:001; classtype:icmp-event;)***

c. Save the local.rules file.

d. Comment the following lines in configuration file (snort.conf) of snort: icmp.rules and icmp-info.rules

e. Add the local.rules file in section 7 of configuration file of snort by writing: ***include $RULE_PATH local.rules***

f. Validate the changes made in snort.conf file by writing the command in terminal: ***sudo snort -T -c /etc/snort/snort.conf -i enp3s0***

g. Set the snort in Intrusion Detection Mode by typing the command: ***sudo snort -A console -q -u snort -g snort -c /etc/snort/snort.conf i enp3s0***

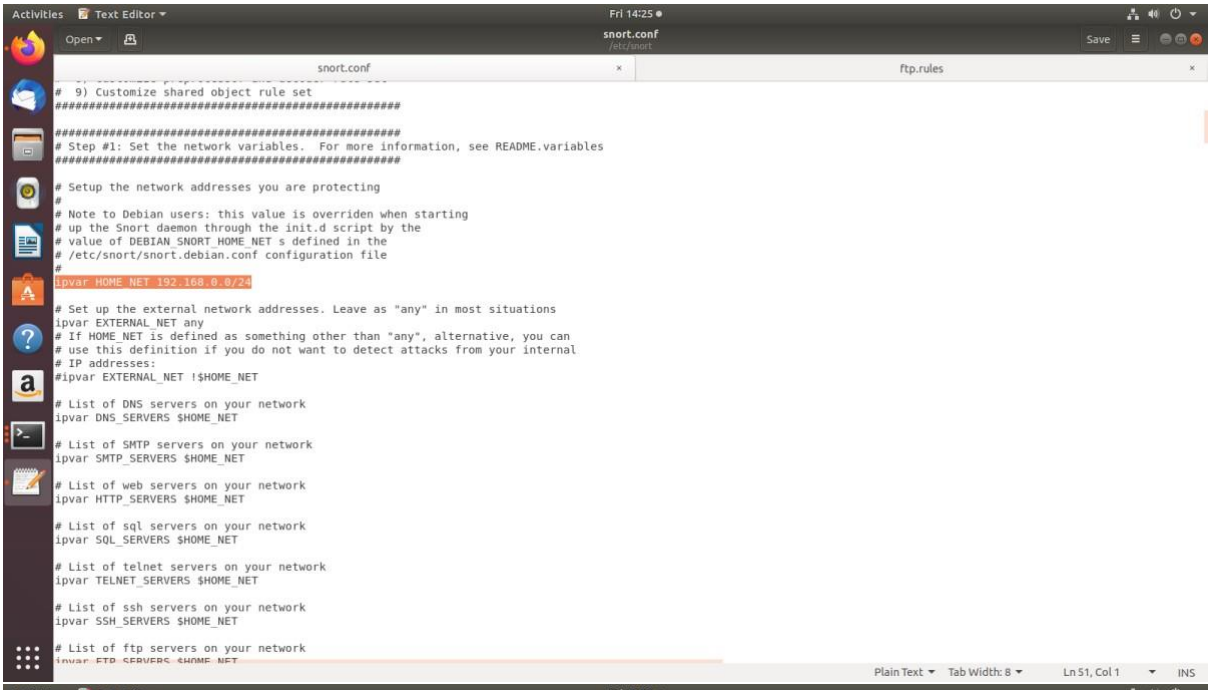
h. Now from kali machine ping the ubuntu machine and see the alert generated.

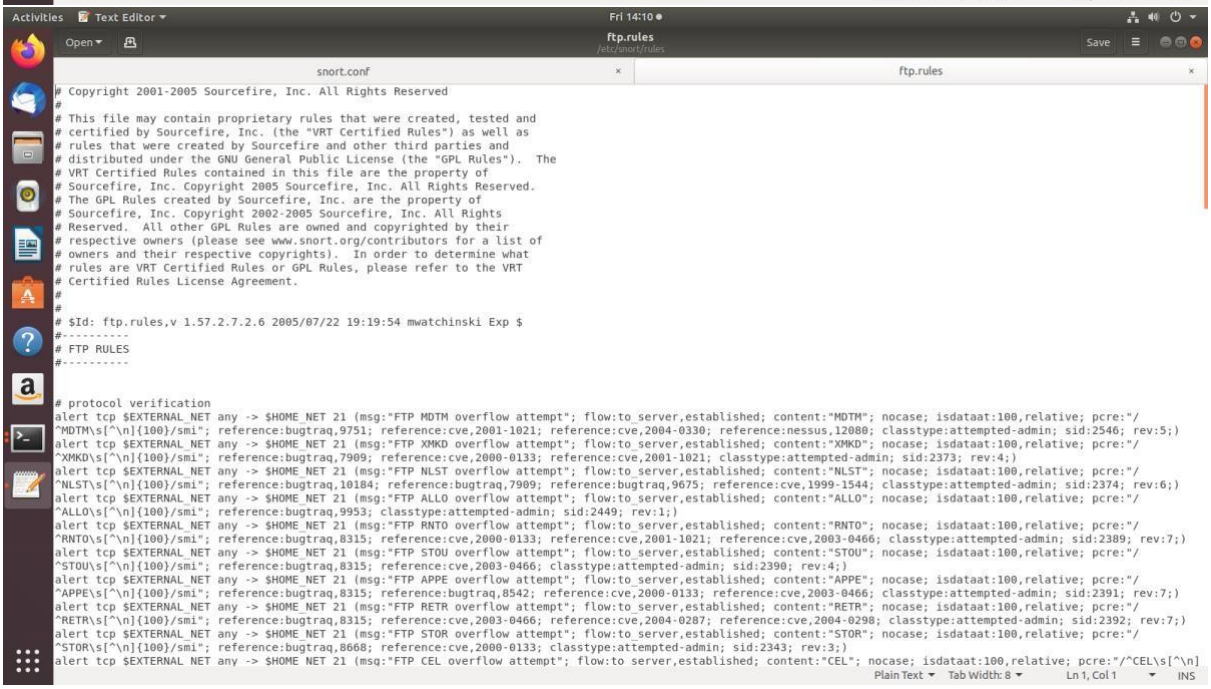
i. Observe the difference between the alerts generated when icmp.rules and icmp-info.rules are used and when local.rules is used to detect the ping activity.

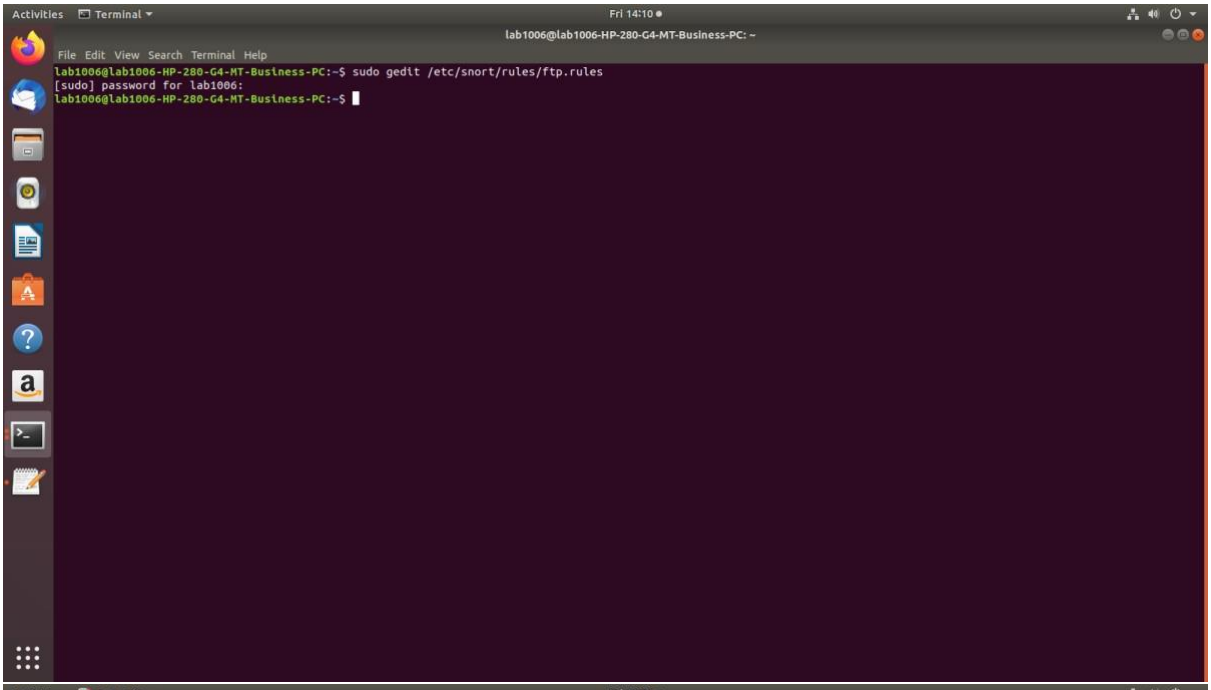
Reference Link for Demo: https://www.youtube.com/watch?v=iBsGSsbDMyw

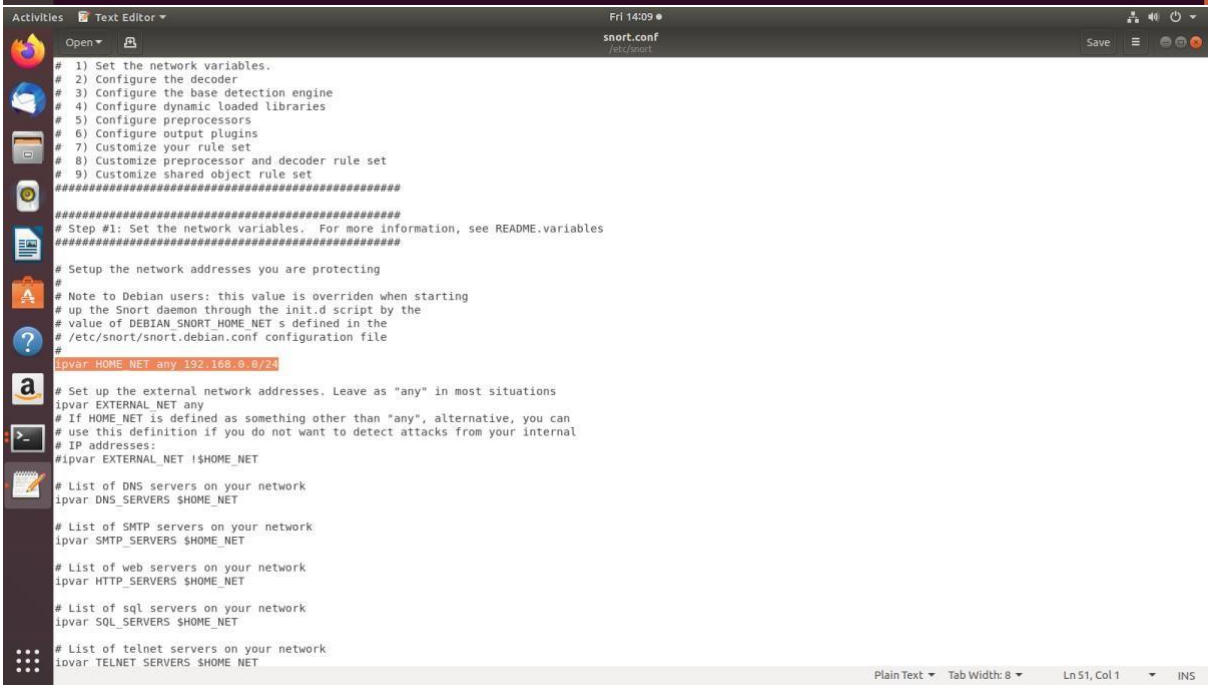
---

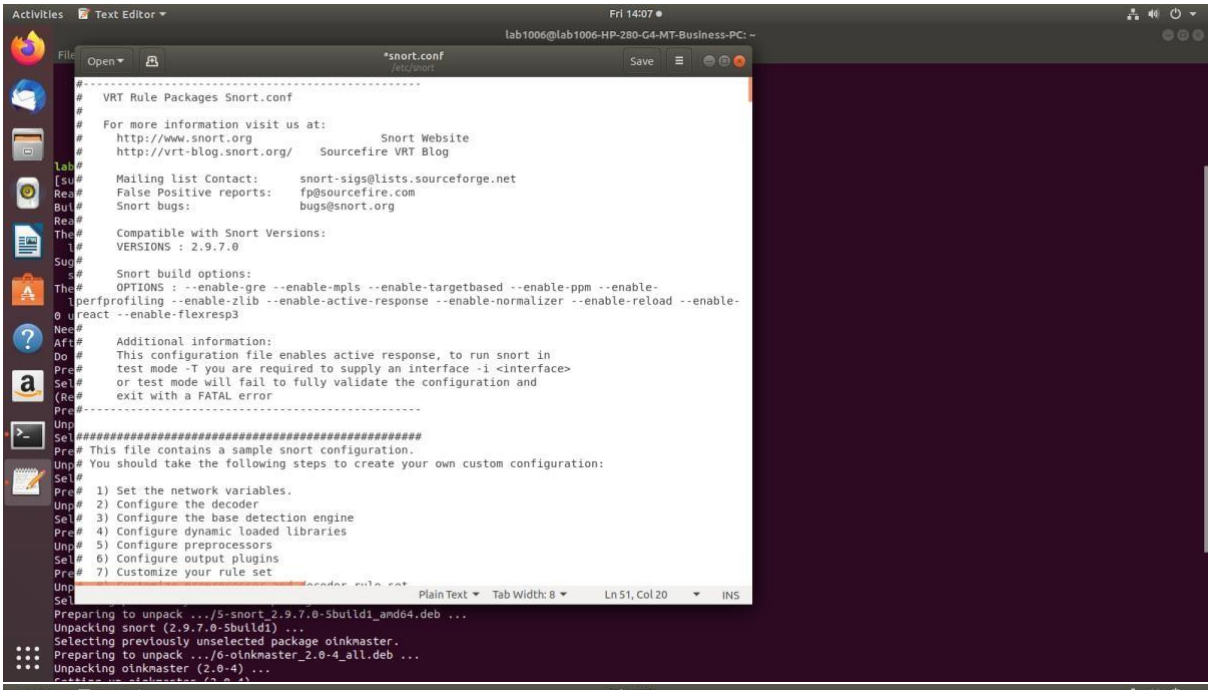
Output:

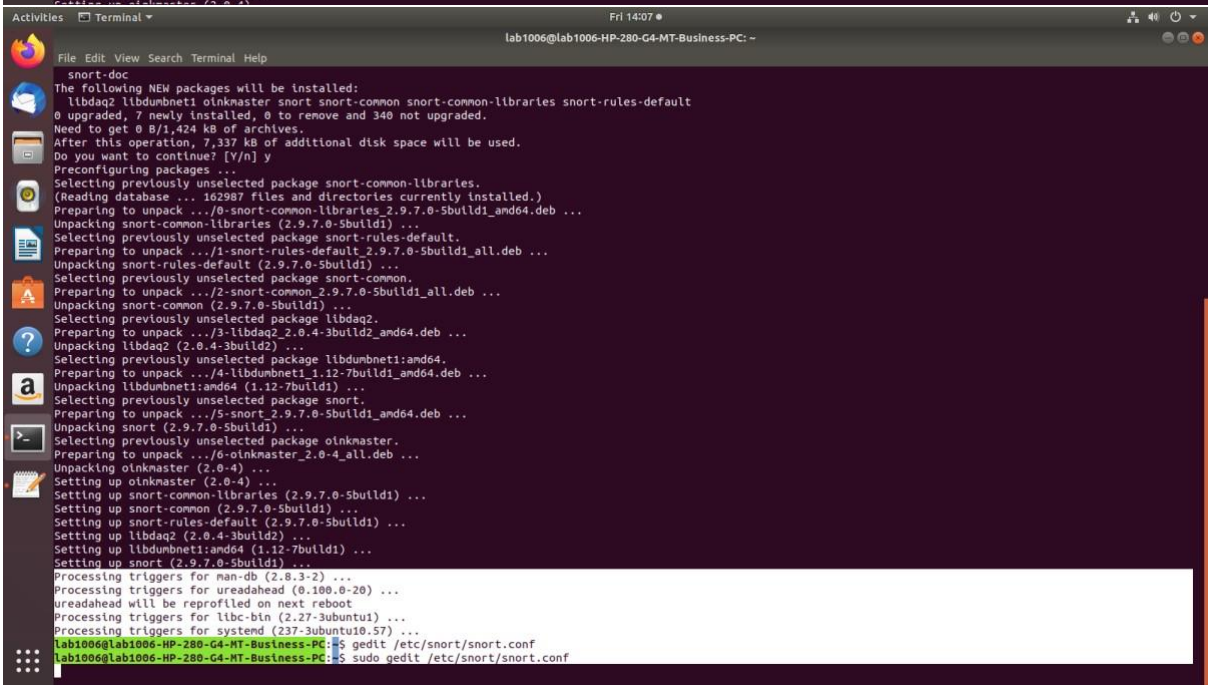

Activities
Text Editor
Fri 14:25
Open
snort.conf
/etc/snort
Save
snort.conf
ftp.rules
9) Customize shared object rule set
##
##
Step #1: Set the network variables. For more information, see README.variables
##
Setup the network addresses you are protecting
#
Note to Debian users: this value is overriden when starting
up the Snort daemon through the init.d script by the
value of DEBIAN_SNORT_HOME_NET s defined in the
/etc/snort/snort.debian.conf configuration file
#
ipvar HOME_NET 192.168.0.0/24
Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET any
If HOME_NET is defined as something other than "any", alternative, you can
use this definition if you do not want to detect attacks from your internal
IP addresses:
#ipvar EXTERNAL_NET !$HOME_NET
List of DNS servers on your network
ipvar DNS_SERVERS $HOME_NET
List of SMTP servers on your network
ipvar SMTP_SERVERS $HOME_NET
List of web servers on your network
ipvar HTTP_SERVERS $HOME_NET
List of sql servers on your network
ipvar SQL_SERVERS $HOME_NET
List of telnet servers on your network
ipvar TELNET_SERVERS $HOME_NET
List of ssh servers on your network
ipvar SSH_SERVERS $HOME_NET
List of ftp servers on your network
Plain Text
Tab Width: 8
Ln 51, Col 1
INS

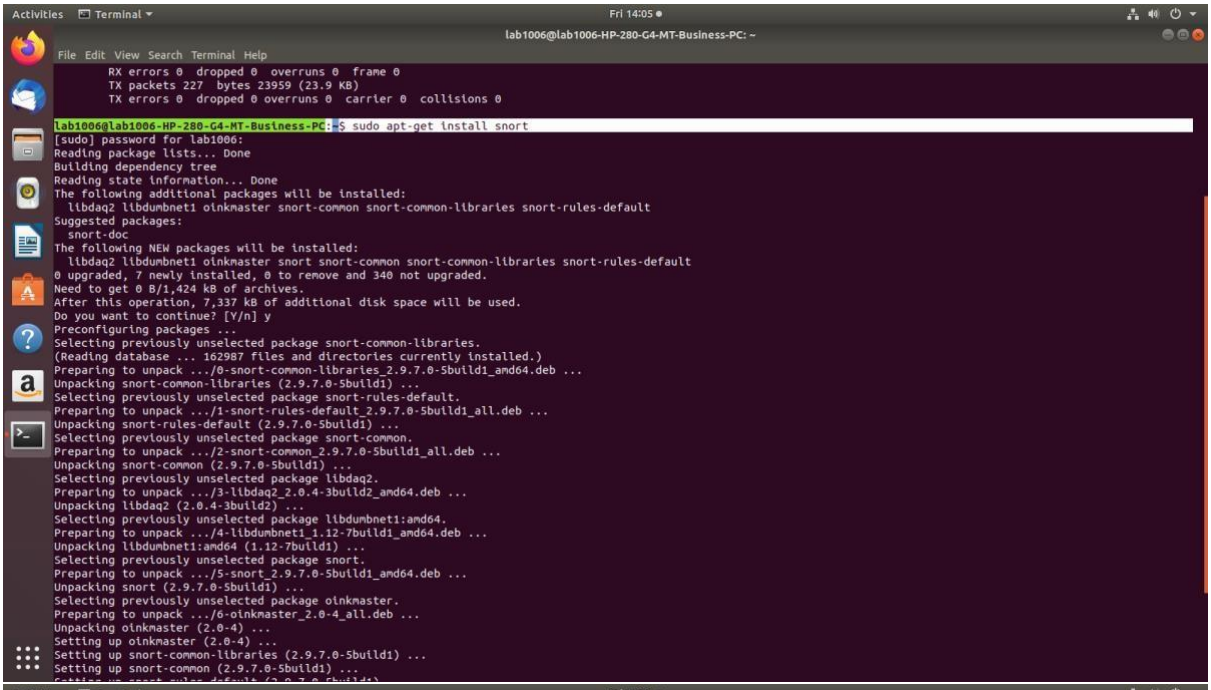

Activities
Text Editor
Fri 14:10
Open
ftp.rules
/etc/snort/rules
Save
snort.conf
ftp.rules
Copyright 2001-2005 Sourcefire, Inc. All Rights Reserved
#
This file may contain proprietary rules that were created, tested and
certified by Sourcefire, Inc. (the "VRT Certified Rules") as well as
rules that were created by Sourcefire and other third parties and
distributed under the GNU General Public License (the "GPL Rules"). The
VRT Certified Rules contained in this file are the property of
Sourcefire, Inc. Copyright 2005 Sourcefire, Inc. All Rights Reserved.
The GPL Rules created by Sourcefire, Inc. are the property of
Sourcefire, Inc. Copyright 2002-2005 Sourcefire, Inc. All Rights
Reserved. All other GPL Rules are owned and copyrighted by their
respective owners (please see www.snort.org/contributors for a list of
owners and their respective copyrights). In order to determine what
rules are VRT Certified Rules or GPL Rules, please refer to the VRT
Certified Rules License Agreement.
#
#
$Id: ftp.rules,v 1.57.2.7.2.6 2005/07/22 19:19:54 mwatchinski Exp $
#----------
FTP RULES
#----------
protocol verification
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP MDTM overflow attempt"; flow:to_server,established; content:"MDTM"; nocase; isdataat:100,relative; pcre:"/
^MDTM\s[^\n]{100}/smi"; reference:bugtraq,9751; reference:cve,2001-1021; reference:cve,2004-0330; reference:nessus,12080; classtype:attempted-admin; sid:2546; rev:5;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP XMKD overflow attempt"; flow:to_server,established; content:"XMKD"; nocase; isdataat:100,relative; pcre:"/
^XMKD\s[^\n]{100}/smi"; reference:bugtraq,7909; reference:cve,2000-0133; reference:cve,2001-1021; classtype:attempted-admin; sid:2373; rev:4;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP NLST overflow attempt"; flow:to_server,established; content:"NLST"; nocase; isdataat:100,relative; pcre:"/
^NLST\s[^\n]{100}/smi"; reference:bugtraq,10184; reference:bugtraq,7909; reference:bugtraq,9675; reference:cve,1999-1544; classtype:attempted-admin; sid:2374; rev:6;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP ALLO overflow attempt"; flow:to_server,established; content:"ALLO"; nocase; isdataat:100,relative; pcre:"/
^ALLO\s[^\n]{100}/smi"; reference:bugtraq,9953; classtype:attempted-admin; sid:2449; rev:1;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP RNTO overflow attempt"; flow:to_server,established; content:"RNTO"; nocase; isdataat:100,relative; pcre:"/
^RNTO\s[^\n]{100}/smi"; reference:bugtraq,8315; reference:cve,2000-0133; reference:cve,2001-1021; reference:cve,2003-0466; classtype:attempted-admin; sid:2389; rev:7;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP STOU overflow attempt"; flow:to_server,established; content:"STOU"; nocase; isdataat:100,relative; pcre:"/
^STOU\s[^\n]{100}/smi"; reference:bugtraq,8315; reference:cve,2003-0466; classtype:attempted-admin; sid:2390; rev:4;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP APPE overflow attempt"; flow:to_server,established; content:"APPE"; nocase; isdataat:100,relative; pcre:"/
^APPE\s[^\n]{100}/smi"; reference:bugtraq,8315; reference:bugtraq,8542; reference:cve,2000-0133; reference:cve,2003-0466; classtype:attempted-admin; sid:2391; rev:7;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP RETR overflow attempt"; flow:to_server,established; content:"RETR"; nocase; isdataat:100,relative; pcre:"/
^RETR\s[^\n]{100}/smi"; reference:bugtraq,8315; reference:cve,2003-0466; reference:cve,2004-0287; reference:cve,2004-0298; classtype:attempted-admin; sid:2392; rev:7;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP STOR overflow attempt"; flow:to_server,established; content:"STOR"; nocase; isdataat:100,relative; pcre:"/
^STOR\s[^\n]{100}/smi"; reference:bugtraq,8668; reference:cve,2000-0133; classtype:attempted-admin; sid:2343; rev:3;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP CEL overflow attempt"; flow:to server,established; content:"CEL"; nocase; isdataat:100,relative; pcre:"/^CEL\s[^\n]
Plain Text
Tab Width: 8
Ln 1, Col 1
INS

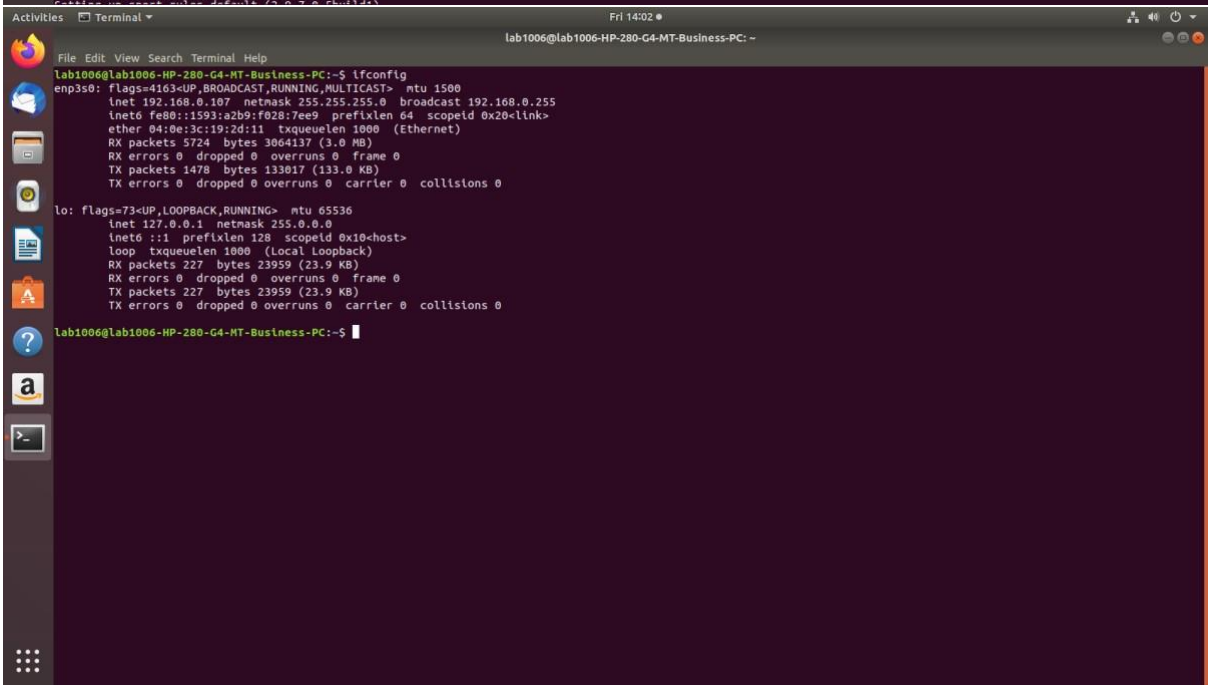

Activities
Terminal
Fri 14:10
lab1006@lab1006-HP-280-G4-MT-Business-PC: ~
File Edit View Search Terminal Help
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo gedit /etc/snort/rules/ftp.rules
[sudo] password for lab1006:
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$


Activities
Text Editor
Fri 14:09
Open
snort.conf
/etc/snort
Save
1) Set the network variables.
2) Configure the decoder
3) Configure the base detection engine
4) Configure dynamic loaded libraries
5) Configure preprocessors
6) Configure output plugins
7) Customize your rule set
8) Customize preprocessor and decoder rule set
9) Customize shared object rule set
Step #1: Set the network variables. For more information, see README.variables
Setup the network addresses you are protecting
Note to Debian users: this value is overriden when starting
up the Snort daemon through the init.d script by the
value of DEBIAN_SNORT_HOME_NET s defined in the
/etc/snort/snort.debian.conf configuration file
ipvar HOME_NET any 192.168.0.0/24
Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET any
If HOME_NET is defined as something other than "any", alternative, you can
use this definition if you do not want to detect attacks from your internal
IP addresses:
#ipvar EXTERNAL_NET !$HOME_NET
List of DNS servers on your network
ipvar DNS_SERVERS $HOME_NET
List of SMTP servers on your network
ipvar SMTP_SERVERS $HOME_NET
List of web servers on your network
ipvar HTTP_SERVERS $HOME_NET
List of sql servers on your network
ipvar SQL_SERVERS $HOME_NET
List of telnet servers on your network
ipvar TELNET_SERVERS $HOME_NET
Plain Text
Tab Width: 8
Ln 51, Col 1
INS


Activities
Text Editor
Fri 14:07
lab1006@lab1006-HP-280-G4-MT-Business-PC: ~
Open
*snort.conf
/etc/snort
Save
VRT Rule Packages Snort.conf
For more information visit us at:
http://www.snort.org Snort Website
http://vrt-blog.snort.org/ Sourcefire VRT Blog
Mailing list Contact: snort-sigs@lists.sourceforge.net
False Positive reports: fp@sourcefire.com
Snort bugs: bugs@snort.org
Compatible with Snort Versions:
VERSIONS : 2.9.7.0
Snort build options:
OPTIONS : --enable-gre --enable-mpls --enable-targetbased --enable-ppm --enable-perfprofiling --enable-zlib --enable-active-response --enable-normalizer --enable-reload --enable-react --enable-flexresp3
Additional information:
This configuration file enables active response, to run snort in
test mode -T you are required to supply an interface -i <interface>
or test mode will fail to fully validate the configuration and
exit with a FATAL error
This file contains a sample snort configuration.
You should take the following steps to create your own custom configuration:
1) Set the network variables.
2) Configure the decoder
3) Configure the base detection engine
4) Configure dynamic loaded libraries
5) Configure preprocessors
6) Configure output plugins
7) Customize your rule set
Plain Text
Tab Width: 8
Ln 51, Col 20
INS
Preparing to unpack .../5-snort_2.9.7.0-5build1_amd64.deb ...
Unpacking snort (2.9.7.0-5build1) ...
Selecting previously unselected package oinkmaster.
Preparing to unpack .../6-oinkmaster_2.0-4_all.deb ...
Unpacking oinkmaster (2.0-4) ...

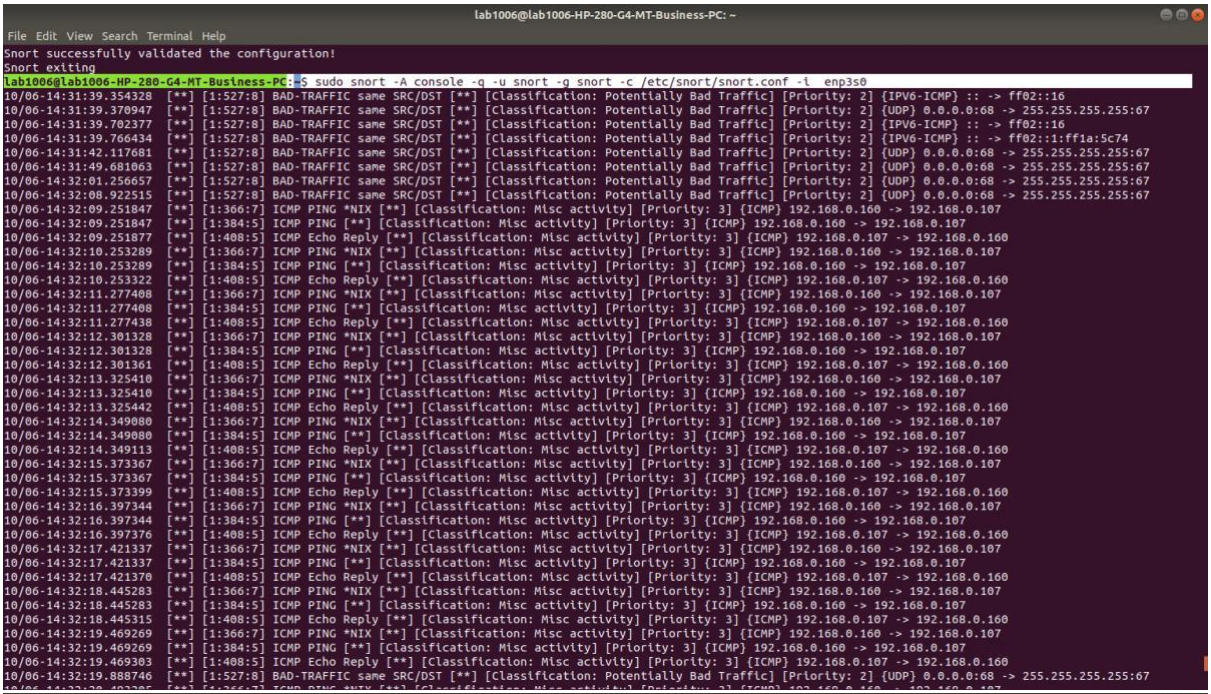

Activities
Terminal
Fri 14:07
lab1006@lab1006-HP-280-G4-MT-Business-PC: ~
File Edit View Search Terminal Help
snort-doc
The following NEW packages will be installed:
libdaq2 libdumbnet1 oinkmaster snort snort-common snort-common-libraries snort-rules-default
0 upgraded, 7 newly installed, 0 to remove and 340 not upgraded.
Need to get 0 B/1,424 kB of archives.
After this operation, 7,337 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Preconfiguring packages ...
Selecting previously unselected package snort-common-libraries.
(Reading database ... 162987 files and directories currently installed.)
Preparing to unpack .../0-snort-common-libraries_2.9.7.0-5build1_amd64.deb ...
Unpacking snort-common-libraries (2.9.7.0-5build1) ...
Selecting previously unselected package snort-rules-default.
Preparing to unpack .../1-snort-rules-default_2.9.7.0-5build1_all.deb ...
Unpacking snort-rules-default (2.9.7.0-5build1) ...
Selecting previously unselected package snort-common.
Preparing to unpack .../2-snort-common_2.9.7.0-5build1_all.deb ...
Unpacking snort-common (2.9.7.0-5build1) ...
Selecting previously unselected package libdaq2.
Preparing to unpack .../3-libdaq2_2.0.4-3build2_amd64.deb ...
Unpacking libdaq2 (2.0.4-3build2) ...
Selecting previously unselected package libdumbnet1:amd64.
Preparing to unpack .../4-libdumbnet1_1.12-7build1_amd64.deb ...
Unpacking libdumbnet1:amd64 (1.12-7build1) ...
Selecting previously unselected package snort.
Preparing to unpack .../5-snort_2.9.7.0-5build1_amd64.deb ...
Unpacking snort (2.9.7.0-5build1) ...
Selecting previously unselected package oinkmaster.
Preparing to unpack .../6-oinkmaster_2.0-4_all.deb ...
Unpacking oinkmaster (2.0-4) ...
Setting up oinkmaster (2.0-4) ...
Setting up snort-common-libraries (2.9.7.0-5build1) ...
Setting up snort-common (2.9.7.0-5build1) ...
Setting up snort-rules-default (2.9.7.0-5build1) ...
Setting up libdaq2 (2.0.4-3build2) ...
Setting up libdumbnet1:amd64 (1.12-7build1) ...
Setting up snort (2.9.7.0-5build1) ...
Processing triggers for man-db (2.8.3-2) ...
Processing triggers for ureadahead (0.100.0-20) ...
ureadahead will be reprofiled on next reboot
Processing triggers for libc-bin (2.27-3ubuntu1) ...
Processing triggers for systemd (237-3ubuntu10.57) ...
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ gedit /etc/snort/snort.conf
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo gedit /etc/snort/snort.conf

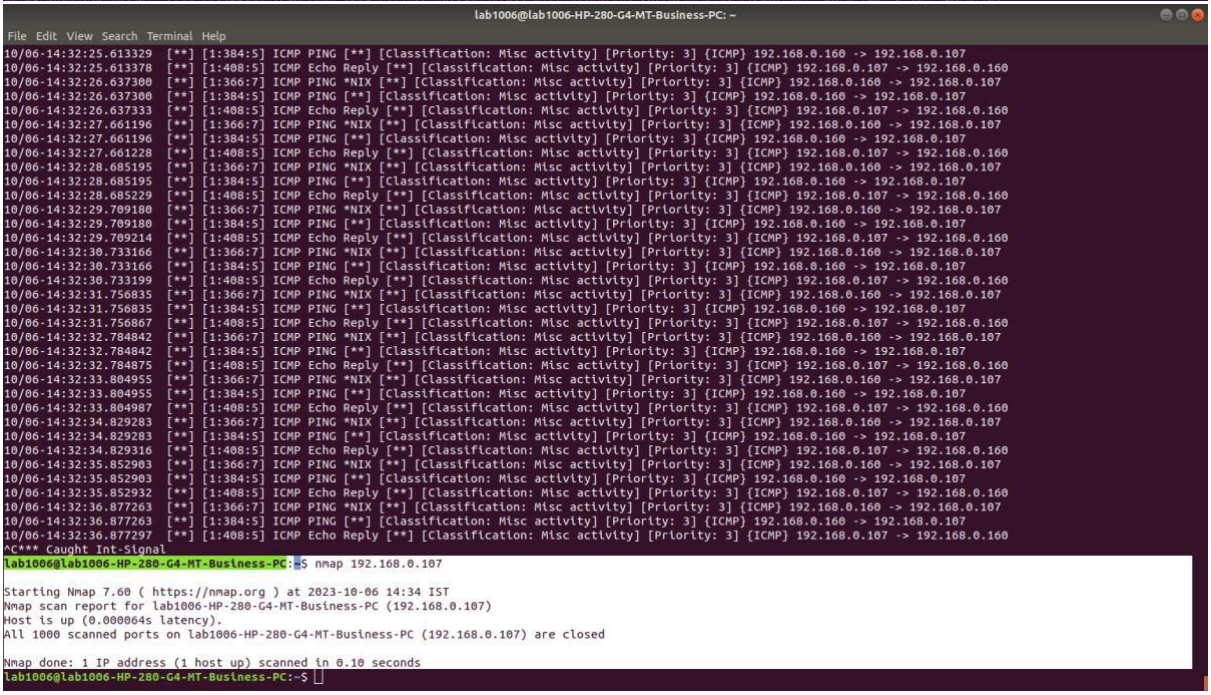

Activities
Terminal
Fri 14:05
lab1006@lab1006-HP-280-G4-MT-Business-PC: ~
File Edit View Search Terminal Help
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 227 bytes 23959 (23.9 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo apt-get install snort
[sudo] password for lab1006:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
libdaq2 libdumbnet1 oinkmaster snort-common snort-common-libraries snort-rules-default
Suggested packages:
snort-doc
The following NEW packages will be installed:
libdaq2 libdumbnet1 oinkmaster snort snort-common snort-common-libraries snort-rules-default
0 upgraded, 7 newly installed, 0 to remove and 340 not upgraded.
Need to get 0 B/1,424 kB of archives.
After this operation, 7,337 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Preconfiguring packages ...
Selecting previously unselected package snort-common-libraries.
(Reading database ... 162987 files and directories currently installed.)
Preparing to unpack .../0-snort-common-libraries_2.9.7.0-5build1_amd64.deb ...
Unpacking snort-common-libraries (2.9.7.0-5build1) ...
Selecting previously unselected package snort-rules-default.
Preparing to unpack .../1-snort-rules-default_2.9.7.0-5build1_all.deb ...
Unpacking snort-rules-default (2.9.7.0-5build1) ...
Selecting previously unselected package snort-common.
Preparing to unpack .../2-snort-common_2.9.7.0-5build1_all.deb ...
Unpacking snort-common (2.9.7.0-5build1) ...
Selecting previously unselected package libdaq2.
Preparing to unpack .../3-libdaq2_2.0.4-3build2_amd64.deb ...
Unpacking libdaq2 (2.0.4-3build2) ...
Selecting previously unselected package libdumbnet1:amd64.
Preparing to unpack .../4-libdumbnet1_1.12-7build1_amd64.deb ...
Unpacking libdumbnet1:amd64 (1.12-7build1) ...
Selecting previously unselected package snort.
Preparing to unpack .../5-snort_2.9.7.0-5build1_amd64.deb ...
Unpacking snort (2.9.7.0-5build1) ...
Selecting previously unselected package oinkmaster.
Preparing to unpack .../6-oinkmaster_2.0-4_all.deb ...
Unpacking oinkmaster (2.0-4) ...
Setting up oinkmaster (2.0-4) ...
Setting up snort-common-libraries (2.9.7.0-5build1) ...
Setting up snort-common (2.9.7.0-5build1) ...

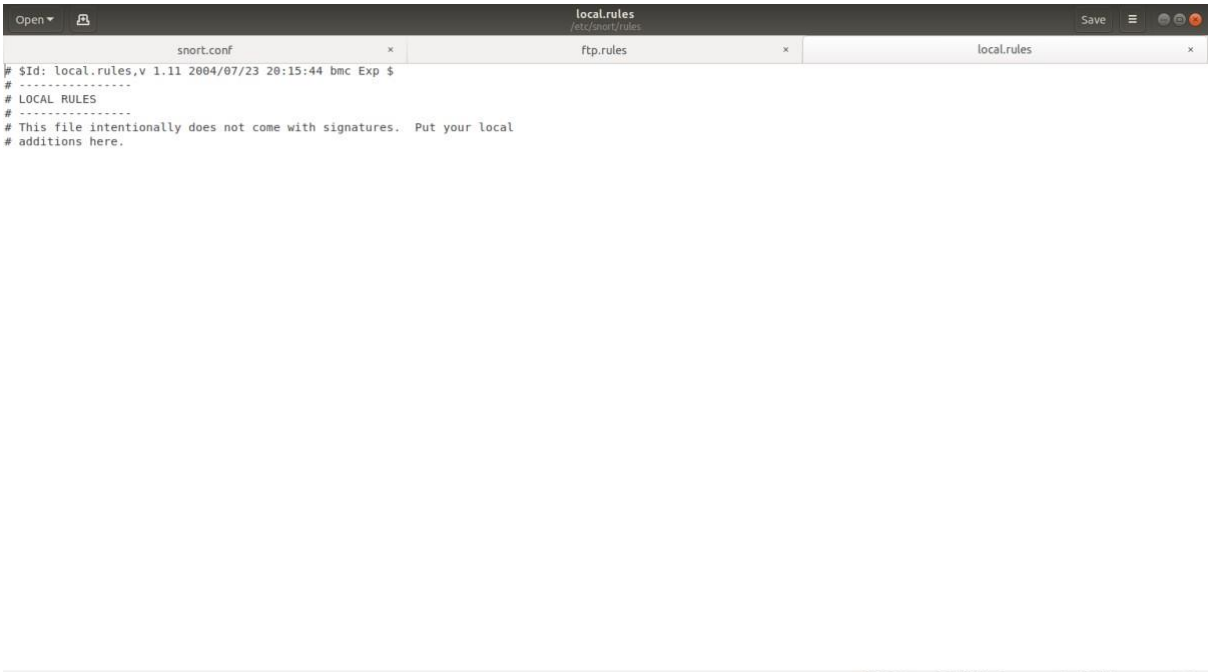

Activities
Terminal
Fri 14:02
lab1006@lab1006-HP-280-G4-MT-Business-PC: ~
File Edit View Search Terminal Help
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ ifconfig
enp3s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.0.107 netmask 255.255.255.0 broadcast 192.168.0.255
inet6 fe80::1593:a2b9:f028:7ee9 prefixlen 64 scopeid 0x20<link>
ether 04:0e:3c:19:2d:11 txqueuelen 1000 (Ethernet)
RX packets 5724 bytes 3064137 (3.0 MB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 1478 bytes 133017 (133.0 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 227 bytes 23959 (23.9 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 227 bytes 23959 (23.9 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$

```
lab1006@lab1006-HP-280-G4-MT-Business-PC: ~
File  Edit  View  Search  Terminal  Help
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo snort -T -c/etc/snort/snort.conf -i enp3s0
[sudo] password for lab1006:
Running in Test mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "/etc/snort/snort.conf"
ERROR: /etc/snort/snort.conf(51) Missing argument to HOME_NET
Fatal Error, Quitting..
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo snort -T -c/etc/snort/snort.conf -i enp3s0
Running in Test mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "/etc/snort/snort.conf"
PortVar 'HTTP_PORTS' defined :  [ 80:81 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 3702 4343 4848 5250 6988 7000:7001 7144:7145 7510 7777 7779 800
0 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 50002 55555 ]
PortVar 'SHELLCODE_PORTS' defined :  [ 0:79 81:65535 ]
PortVar 'ORACLE_PORTS' defined :  [ 1024:65535 ]
PortVar 'SSH_PORTS' defined :  [ 22 ]
PortVar 'FTP_PORTS' defined :  [ 21 2100 3535 ]
PortVar 'SIP_PORTS' defined :  [ 5060:5061 5600 ]
PortVar 'FILE_DATA_PORTS' defined :  [ 80:81 110 143 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 3702 4343 4848 5250 6988 7000:7001 7144:7145 7510
7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 50002 555
55 ]
PortVar 'GTP_PORTS' defined :  [ 2123 2152 3386 ]
Detection:
   Search-Method = AC-Full-Q
    Split Any/Any group = enabled
    Search-Method-Optimizations = enabled
```

```
lab1006@lab1006-HP-280-G4-MT-Business-PC: ~
File  Edit  View  Search  Terminal  Help
| State Density     : 10.6%
| Patterns          : 5055
| Match States      : 3855
| Memory (MB)       : 17.00
|   Patterns        : 0.51
|   Match Lists     : 1.02
|   DFA
|     1 byte states : 1.02
|     2 byte states : 14.05
|     4 byte states : 0.00
+----------------------------------------------------------------
[ Number of patterns truncated to 20 bytes: 1039 ]
pcap DAQ configured to passive.
Acquiring network traffic from "enp3s0".

        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   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 1.8.1
           Using PCRE version: 8.39 2016-06-14
           Using ZLIB version: 1.2.11

           Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 2.4  <Build 1>
           Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
           Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
           Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
           Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
           Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
           Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
           Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
           Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
           Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
           Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
           Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
           Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
           Preprocessor Object: SF_POP  Version 1.0  <Build 1>
           Preprocessor Object: SF_SDF  Version 1.1  <Build 1>

Snort successfully validated the configuration!
Snort exiting
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$
```

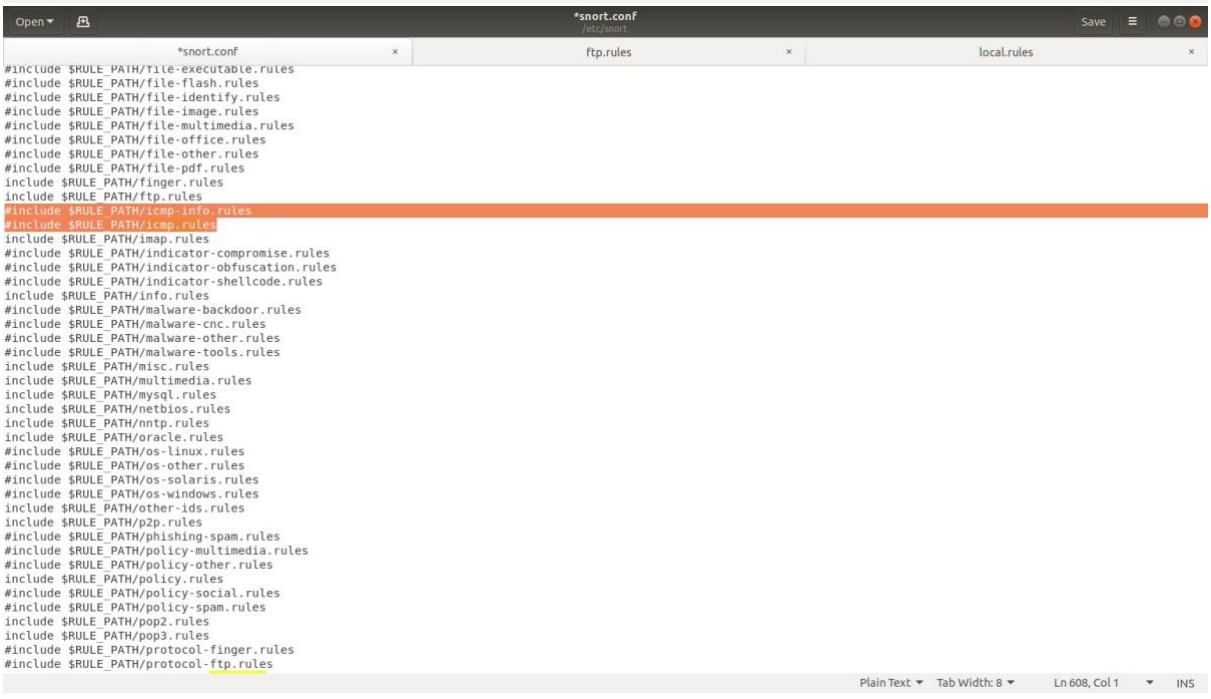

lab1006@lab1006-HP-280-G4-MT-Business-PC: ~
File Edit View Search Terminal Help
Snort successfully validated the configuration!
Snort exiting
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo snort -A console -q -u snort -g snort -c /etc/snort/snort.conf -i enp3s0
10/06-14:31:39.354328 [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {IPV6-ICMP} :: -> ff02::16
10/06-14:31:39.370947 [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 -> 255.255.255.255:67
10/06-14:31:39.702377 [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {IPV6-ICMP} :: -> ff02::16
10/06-14:31:39.766434 [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {IPV6-ICMP} :: -> ff02::1:ff1a:5c74
10/06-14:31:42.117681 [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 -> 255.255.255.255:67
10/06-14:31:49.681063 [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 -> 255.255.255.255:67
10/06-14:32:01.256657 [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 -> 255.255.255.255:67
10/06-14:32:08.922515 [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 -> 255.255.255.255:67
10/06-14:32:09.251847 [**] [1:366:7] ICMP PING *NIX [**] [Classification: Misc actlvity] [Priority: 3] {ICMP} 192.168.0.160 -> 192.168.0.107
10/06-14:32:09.251847 [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.0.160 -> 192.168.0.107
10/06-14:32:09.251877 [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.0.107 -> 192.168.0.160
10/06-14:32:10.253289 [**] [1:366:7] ICMP PING *NIX [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.0.160 -> 192.168.0.107
10/06-14:32:10.253289 [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.0.160 -> 192.168.0.107
10/06-14:32:10.253322 [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.0.107 -> 192.168.0.160
10/06-14:32:11.277408 [**] [1:366:7] ICMP PING *NIX [**] [Classification: Misc actlvity] [Priority: 3] {ICMP} 192.168.0.160 -> 192.168.0.107
10/06-14:32:11.277408 [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.0.160 -> 192.168.0.107
10/06-14:32:11.277438 [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.0.107 -> 192.168.0.160
10/06-14:32:12.301328 [**] [1:366:7] ICMP PING *NIX [**] [Classification: Misc actlvity] [Priority: 3] {ICMP} 192.168.0.160 -> 192.168.0.107
10/06-14:32:12.301328 [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.0.160 -> 192.168.0.107
10/06-14:32:12.301361 [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.0.107 -> 192.168.0.160
10/06-14:32:13.325410 [**] [1:366:7] ICMP PING *NIX [**] [Classification: Misc actlvity] [Priority: 3] {ICMP} 192.168.0.160 -> 192.168.0.107
10/06-14:32:13.325410 [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.0.160 -> 192.168.0.107
10/06-14:32:13.325442 [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.0.107 -> 192.168.0.160
10/06-14:32:14.349080 [**] [1:366:7] ICMP PING *NIX [**] [Classification: Misc actlvity] [Priority: 3] {ICMP} 192.168.0.160 -> 192.168.0.107
10/06-14:32:14.349080 [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.0.160 -> 192.168.0.107
10/06-14:32:14.349113 [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.0.107 -> 192.168.0.160
10/06-14:32:15.373367 [**] [1:366:7] ICMP PING *NIX [**] [Classification: Misc actlvity] [Priority: 3] {ICMP} 192.168.0.160 -> 192.168.0.107
10/06-14:32:15.373367 [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.0.160 -> 192.168.0.107
10/06-14:32:15.373399 [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.0.107 -> 192.168.0.160
10/06-14:32:16.397344 [**] [1:366:7] ICMP PING *NIX [**] [Classification: Misc actlvity] [Priority: 3] {ICMP} 192.168.0.160 -> 192.168.0.107
10/06-14:32:16.397344 [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.0.160 -> 192.168.0.107
10/06-14:32:16.397376 [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.0.107 -> 192.168.0.160
10/06-14:32:17.421337 [**] [1:366:7] ICMP PING *NIX [**] [Classification: Misc actlvity] [Priority: 3] {ICMP} 192.168.0.160 -> 192.168.0.107
10/06-14:32:17.421337 [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.0.160 -> 192.168.0.107
10/06-14:32:17.421370 [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.0.107 -> 192.168.0.160
10/06-14:32:18.445283 [**] [1:366:7] ICMP PING *NIX [**] [Classification: Misc actlvity] [Priority: 3] {ICMP} 192.168.0.160 -> 192.168.0.107
10/06-14:32:18.445283 [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.0.160 -> 192.168.0.107
10/06-14:32:18.445315 [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.0.107 -> 192.168.0.160
10/06-14:32:19.469269 [**] [1:366:7] ICMP PING *NIX [**] [Classification: Misc actlvity] [Priority: 3] {ICMP} 192.168.0.160 -> 192.168.0.107
10/06-14:32:19.469269 [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.0.160 -> 192.168.0.107
10/06-14:32:19.469303 [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.0.107 -> 192.168.0.160
10/06-14:32:19.888746 [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 -> 255.255.255.255:67

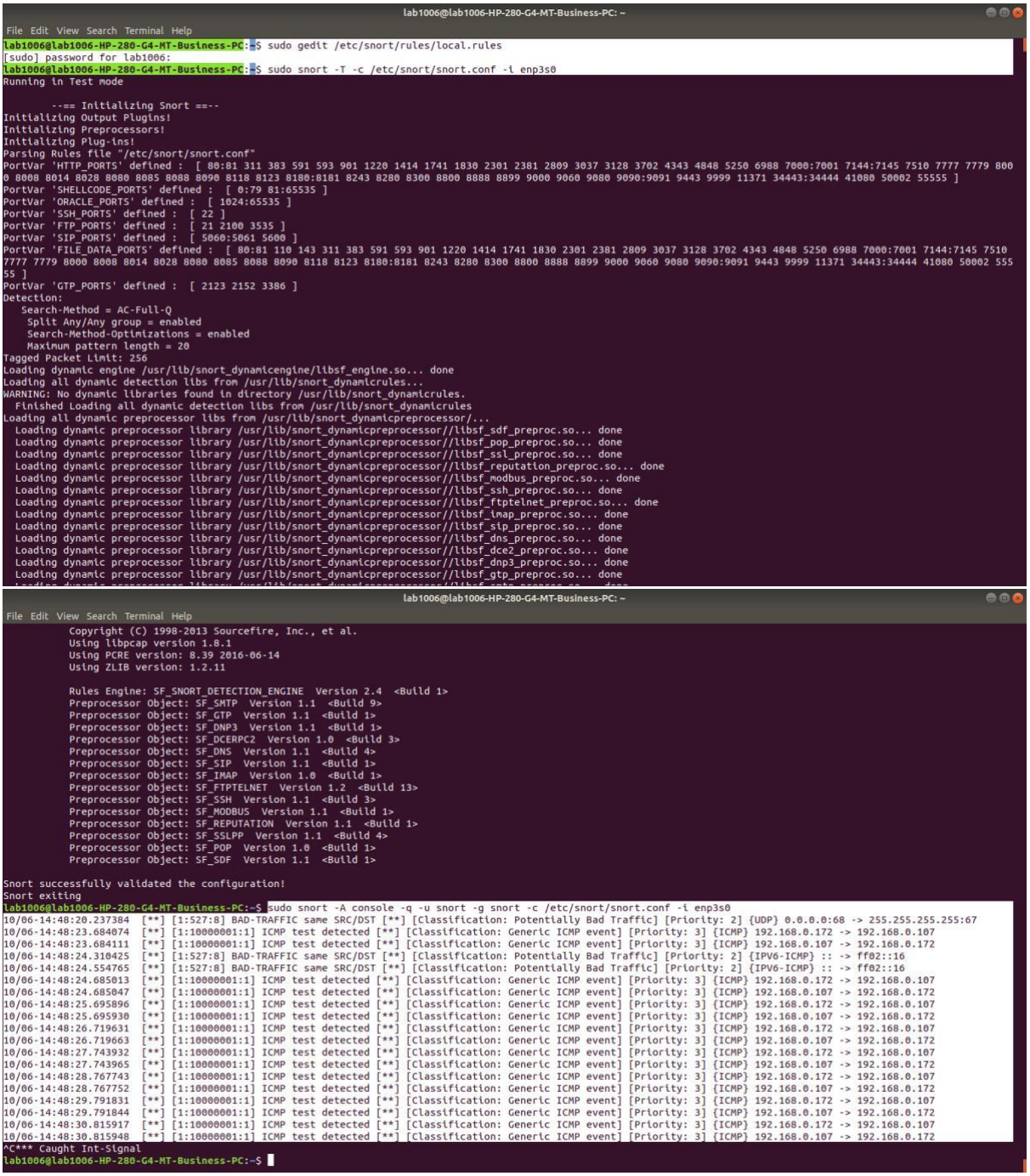

lab1006@lab1006-HP-280-G4-MT-Business-PC: ~
File Edit View Search Terminal Help
10/06-14:32:25.613329 [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.0.160 -> 192.168.0.107
10/06-14:32:25.613378 [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.0.107 -> 192.168.0.160
10/06-14:32:26.637300 [**] [1:366:7] ICMP PING *NIX [**] [Classification: Misc actlvity] [Priority: 3] {ICMP} 192.168.0.160 -> 192.168.0.107
10/06-14:32:26.637300 [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.0.160 -> 192.168.0.107
10/06-14:32:26.637333 [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.0.107 -> 192.168.0.160
10/06-14:32:27.661196 [**] [1:366:7] ICMP PING *NIX [**] [Classification: Misc actlvity] [Priority: 3] {ICMP} 192.168.0.160 -> 192.168.0.107
10/06-14:32:27.661196 [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.0.160 -> 192.168.0.107
10/06-14:32:27.661228 [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.0.107 -> 192.168.0.160
10/06-14:32:28.685195 [**] [1:366:7] ICMP PING *NIX [**] [Classification: Misc actlvity] [Priority: 3] {ICMP} 192.168.0.160 -> 192.168.0.107
10/06-14:32:28.685195 [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.0.160 -> 192.168.0.107
10/06-14:32:28.685229 [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.0.107 -> 192.168.0.160
10/06-14:32:29.709180 [**] [1:366:7] ICMP PING *NIX [**] [Classification: Misc actlvity] [Priority: 3] {ICMP} 192.168.0.160 -> 192.168.0.107
10/06-14:32:29.709180 [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.0.160 -> 192.168.0.107
10/06-14:32:29.709214 [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.0.107 -> 192.168.0.160
10/06-14:32:30.733166 [**] [1:366:7] ICMP PING *NIX [**] [Classification: Misc actlvity] [Priority: 3] {ICMP} 192.168.0.160 -> 192.168.0.107
10/06-14:32:30.733166 [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.0.160 -> 192.168.0.107
10/06-14:32:30.733199 [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.0.107 -> 192.168.0.160
10/06-14:32:31.756835 [**] [1:366:7] ICMP PING *NIX [**] [Classification: Misc actlvity] [Priority: 3] {ICMP} 192.168.0.160 -> 192.168.0.107
10/06-14:32:31.756835 [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.0.160 -> 192.168.0.107
10/06-14:32:31.756867 [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.0.107 -> 192.168.0.160
10/06-14:32:32.784842 [**] [1:366:7] ICMP PING *NIX [**] [Classification: Misc actlvity] [Priority: 3] {ICMP} 192.168.0.160 -> 192.168.0.107
10/06-14:32:32.784842 [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.0.160 -> 192.168.0.107
10/06-14:32:32.784875 [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.0.107 -> 192.168.0.160
10/06-14:32:33.804955 [**] [1:366:7] ICMP PING *NIX [**] [Classification: Misc actlvity] [Priority: 3] {ICMP} 192.168.0.160 -> 192.168.0.107
10/06-14:32:33.804955 [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.0.160 -> 192.168.0.107
10/06-14:32:33.804987 [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.0.107 -> 192.168.0.160
10/06-14:32:34.829283 [**] [1:366:7] ICMP PING *NIX [**] [Classification: Misc actlvity] [Priority: 3] {ICMP} 192.168.0.160 -> 192.168.0.107
10/06-14:32:34.829283 [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.0.160 -> 192.168.0.107
10/06-14:32:34.829316 [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.0.107 -> 192.168.0.160
10/06-14:32:35.852903 [**] [1:366:7] ICMP PING *NIX [**] [Classification: Misc actlvity] [Priority: 3] {ICMP} 192.168.0.160 -> 192.168.0.107
10/06-14:32:35.852903 [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.0.160 -> 192.168.0.107
10/06-14:32:35.852932 [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.0.107 -> 192.168.0.160
10/06-14:32:36.877263 [**] [1:366:7] ICMP PING *NIX [**] [Classification: Misc actlvity] [Priority: 3] {ICMP} 192.168.0.160 -> 192.168.0.107
10/06-14:32:36.877263 [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.0.160 -> 192.168.0.107
10/06-14:32:36.877297 [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.0.107 -> 192.168.0.160
^C*** Caught Int-Signal
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ nmap 192.168.0.107
Starting Nmap 7.60 (https://nmap.org) at 2023-10-06 14:34 IST
Nmap scan report for lab1006-HP-280-G4-MT-Business-PC (192.168.0.107)
Host is up (0.000064s latency).
All 1000 scanned ports on lab1006-HP-280-G4-MT-Business-PC (192.168.0.107) are closed
Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$


Open
local.rules
/etc/snort/rules
Save
snort.conf
ftp.rules
local.rules
$Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $

LOCAL RULES

This file intentionally does not come with signatures. Put your local
additions here.
Plain Text
Tab Width: 8
Ln 1, Col 1
INS


Open
*snort.conf
/etc/snort
Save
*snort.conf
ftp.rules
local.rules
#include $RULE_PATH/file-executable.rules
#include $RULE_PATH/file-flash.rules
#include $RULE_PATH/file-identify.rules
#include $RULE_PATH/file-image.rules
#include $RULE_PATH/file-multimedia.rules
#include $RULE_PATH/file-office.rules
#include $RULE_PATH/file-other.rules
#include $RULE_PATH/file-pdf.rules
include $RULE_PATH/finger.rules
include $RULE_PATH/ftp.rules
#include $RULE_PATH/icmp-info.rules
#include $RULE_PATH/icmp.rules
include $RULE_PATH/imap.rules
#include $RULE_PATH/indicator-compromise.rules
#include $RULE_PATH/indicator-obfuscation.rules
#include $RULE_PATH/indicator-shellcode.rules
include $RULE_PATH/info.rules
#include $RULE_PATH/malware-backdoor.rules
#include $RULE_PATH/malware-cnc.rules
#include $RULE_PATH/malware-other.rules
#include $RULE_PATH/malware-tools.rules
include $RULE_PATH/misc.rules
include $RULE_PATH/multimedia.rules
include $RULE_PATH/mysql.rules
include $RULE_PATH/netbios.rules
include $RULE_PATH/nntp.rules
include $RULE_PATH/oracle.rules
#include $RULE_PATH/os-linux.rules
#include $RULE_PATH/os-other.rules
#include $RULE_PATH/os-solaris.rules
#include $RULE_PATH/os-windows.rules
include $RULE_PATH/other-ids.rules
include $RULE_PATH/p2p.rules
#include $RULE_PATH/phishing-spam.rules
#include $RULE_PATH/policy-multimedia.rules
#include $RULE_PATH/policy-other.rules
include $RULE_PATH/policy.rules
#include $RULE_PATH/policy-social.rules
#include $RULE_PATH/policy-spam.rules
include $RULE_PATH/pop2.rules
include $RULE_PATH/pop3.rules
#include $RULE_PATH/protocol-finger.rules
#include $RULE_PATH/protocol-ftp.rules
Plain Text
Tab Width: 8
Ln 608, Col 1
INS



Conclusion: In conclusion, this assignment involved the installation and configuration of Snort, a powerful Intrusion Detection System. By following the step-by-step instructions, we successfully installed Snort, edited its configuration file, and executed rules to detect ICMP activities. This hands-on experience enhanced our understanding of network security and IDS functionality.