Objectives

In this lab students will explore the Snort Intrusion Detection Systems. The students will study Snort IDS, a signature based intrusion detection system used to detect network attacks. Snort can also be used as a simple packet logger. For the purpose of this lab the students will use snort as a packet sniffer and write their own IDS rules.

Software Reequirment

All required files are packed and configured in the provided virtual machine image.

-The VMWare Software - http://apps.eng.wayne.edu/MPStudents/Dreamspark.aspx

- The ubantu 14.04 or Ubantu Long Term Support (LTS) versionor Kali linux image
- The ubantu 14.04 or Ubuntu 14.04 Long Term Support (LTS) Version
- Snort: A signature-based Intrusion Detection System https://www.snort.org/#get-started

Implementation

Starting the Lab 1 Virtual Machine

In this lab, we use Ubuntu as our VM image.

Login the Ubuntu image with username and password

Installing Snort into the Operating System

To install the latest version of the snort, you can follow the installation instruction from the snort website. Note that installation instructions are vary from OSes. The instruction below shows how to install snort from its source code on Linux.

You can find more information here:

https://www.snort.org/#get-started

```
vishal@vishal-VirtualBox:~$ wget https://www.snort.org/downloads/snort/daq-2.0.7.tar.gz
--2021-03-08 20:04:42--  https://www.snort.org/downloads/snort/daq-2.0.7.tar.gz
Resolving www.snort.org (www.snort.org)... 104.18.138.9, 104.18.139.9, 2606:4700::6812:8a09, ...
Connecting to www.snort.org (www.snort.org)|104.18.138.9|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://snort-org-site.s3.amazonaws.com/production/release_files/files/000/015/642/original/daq-2.0.7.tar.gz?X-Amz-Algorithm=AWS4-HMAC-SHA25
6&X-Amz-Credential=AKIAIXACIED2SPMSC7GA%2F20210308%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20210308T143442Z&X-Amz-Expires=3600&X-Amz-SignedHeaders=
host&X-Amz-Signature=33550a826da86fbff4b50b24960ac27d4a8f6373fd2163569453ba70330c4062 [following]
--2021-03-08 20:04:42--  https://snort-org-site.s3.amazonaws.com/production/release_files/files/000/015/642/original/daq-2.0.7.tar.gz?X-Amz-Algorithm=
AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIXACIED2SPMSC7GA%2F20210308%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20210308T143442Z&X-Amz-Expires=3600&X-Amz
-SignedHeaders=host&X-Amz-Signature=33550a826da86fbff4b50b24960ac27d4a8f6373fd2163569453ba70330c4062
Resolving snort-org-site.s3.amazonaws.com (snort-org-site.s3.amazonaws.com)... 52.216.139.179
Connecting to snort-org-site.s3.amazonaws.com (snort-org-site.s3.amazonaws.com)|52.216.139.179|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 515126 (503K) [binary/octet-stream]
Saving to: 'daq-2.0.7.tar.gz'

daq-2.0.7.tar.gz                      74%[=================================================>                  ] 372.64K   114KB/s    eta 1s
daq-2.0.7.tar.gz                     100%[========================================================================>] 503.05K   116KB/s    in 4.6s

2021-03-08 20:04:48 (110 KB/s) - 'daq-2.0.7.tar.gz' saved [515126/515126]
```

```
vishal@vishal-VirtualBox:~$ wget https://www.snort.org/downloads/snort/snort-2.9.17.tar.gz
--2021-03-08 20:07:31--  https://www.snort.org/downloads/snort/snort-2.9.17.tar.gz
Resolving www.snort.org (www.snort.org)... 104.18.138.9, 104.18.139.9, 2606:4700::6812:8a09, ...
Connecting to www.snort.org (www.snort.org)|104.18.138.9|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://snort-org-site.s3.amazonaws.com/production/release_files/files/000/015/645/original/snort-2.9.17.tar.gz?X-Amz-Algorithm=AWS4-HMAC-SH
A256&X-Amz-Credential=AKIAIXACIED2SPMSC7GA%2F20210308%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20210308T143731Z&X-Amz-Expires=3600&X-Amz-SignedHeade
rs=host&X-Amz-Signature=08a48ae7439f05aca1e407604a2624a4db5bc1f4a0007dfb829e743965c819ea [following]
--2021-03-08 20:07:31--  https://snort-org-site.s3.amazonaws.com/production/release_files/files/000/015/645/original/snort-2.9.17.tar.gz?X-Amz-Algorit
hm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIXACIED2SPMSC7GA%2F20210308%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20210308T143731Z&X-Amz-Expires=3600&X-
Amz-SignedHeaders=host&X-Amz-Signature=08a48ae7439f05aca1e407604a2624a4db5bc1f4a0007dfb829e743965c819ea
Resolving snort-org-site.s3.amazonaws.com (snort-org-site.s3.amazonaws.com)... 52.216.106.43
Connecting to snort-org-site.s3.amazonaws.com (snort-org-site.s3.amazonaws.com)|52.216.106.43|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 6983018 (6.7M) [binary/octet-stream]
Saving to: 'snort-2.9.17.tar.gz'

snort-2.9.17.tar.gz                  100%[========================================================================>]   6.66M   127KB/s    in 65s

2021-03-08 20:08:38 (105 KB/s) - 'snort-2.9.17.tar.gz' saved [6983018/6983018]
```

```
vishal@vishal-VirtualBox:~$ tar xvzf daq-2.0.7.tar.gz
daq-2.0.7/
daq-2.0.7/config.h.in
daq-2.0.7/config.guess
daq-2.0.7/api/
daq-2.0.7/api/daq.h
daq-2.0.7/api/Makefile.am
daq-2.0.7/api/daq_common.h
daq-2.0.7/api/daq_base.c
daq-2.0.7/api/daq_api.h
daq-2.0.7/api/daq_mod_ops.c
daq-2.0.7/api/Makefile.in
daq-2.0.7/config.sub
daq-2.0.7/ltmain.sh
daq-2.0.7/os-daq-modules/
daq-2.0.7/os-daq-modules/daq-modules-config.in
daq-2.0.7/os-daq-modules/daq_ipfw.c
daq-2.0.7/os-daq-modules/Makefile.am
daq-2.0.7/os-daq-modules/daq_static_modules.h
daq-2.0.7/os-daq-modules/daq_dump.c
daq-2.0.7/os-daq-modules/daq_ipq.c
daq-2.0.7/os-daq-modules/daq_static_modules.c
daq-2.0.7/os-daq-modules/daq_pcap.c
daq-2.0.7/os-daq-modules/daq_nfq.c
daq-2.0.7/os-daq-modules/daq_netmap.c
daq-2.0.7/os-daq-modules/daq_afpacket.c
daq-2.0.7/os-daq-modules/Makefile.in
daq-2.0.7/compile
daq-2.0.7/install-sh
daq-2.0.7/missing
daq-2.0.7/Makefile.am
daq-2.0.7/aclocal.m4
daq-2.0.7/configure
daq-2.0.7/m4/
daq-2.0.7/m4/sf.m4
daq-2.0.7/m4/lt~obsolete.m4
daq-2.0.7/m4/ltoptions.m4
daq-2.0.7/m4/libtool.m4
daq-2.0.7/m4/ltsugar.m4
daq-2.0.7/m4/ax_cflags_gcc_option.m4
daq-2.0.7/m4/ltversion.m4
daq-2.0.7/daq.dsp
daq-2.0.7/COPYING
daq-2.0.7/sfbpf/
daq-2.0.7/sfbpf/sfbpf.h
```

```
vishal@vishal-VirtualBox:~$ ls
daq-2.0.7  daq-2.0.7.tar.gz  Desktop  Documents  Downloads  Music  Pictures  priv.pem  Public  snap  snort-2.9.17.tar.gz  Templates  Videos
vishal@vishal-VirtualBox:~$ cd daq-2.0.7
```

```
vishal@vishal-VirtualBox:~/daq-2.0.7$ ./configure && make && sudo make install
checking for a BSD-compatible install... /usr/bin/install -c
checking whether build environment is sane... yes
checking for a thread-safe mkdir -p... /usr/bin/mkdir -p
checking for gawk... no
checking for mawk... mawk
checking whether make sets $(MAKE)... yes
checking whether make supports nested variables... yes
checking for gcc... gcc
checking whether the C compiler works... yes
checking for C compiler default output file name... a.out
checking for suffix of executables...
checking whether we are cross compiling... no
checking for suffix of object files... o
checking whether we are using the GNU C compiler... yes
checking whether gcc accepts -g... yes
checking for gcc option to accept ISO C89... none needed
checking whether gcc understands -c and -o together... yes
checking for style of include used by make... GNU
checking dependency style of gcc... gcc3
checking build system type... x86_64-unknown-linux-gnu
checking host system type... x86_64-unknown-linux-gnu
checking how to print strings... printf
checking for a sed that does not truncate output... /usr/bin/sed
checking for grep that handles long lines and -e... /usr/bin/grep
checking for egrep... /usr/bin/grep -E
checking for fgrep... /usr/bin/grep -F
checking for ld used by gcc... /usr/bin/ld
checking if the linker (/usr/bin/ld) is GNU ld... yes
checking for BSD- or MS-compatible name lister (nm)... /usr/bin/nm -B
checking the name lister (/usr/bin/nm -B) interface... BSD nm
checking whether ln -s works... yes
checking the maximum length of command line arguments... 1572864
checking how to convert x86_64-unknown-linux-gnu file names to x86_64-unknown-linux-gnu format... func_convert_file_noop
checking how to convert x86_64-unknown-linux-gnu file names to toolchain format... func_convert_file_noop
checking for /usr/bin/ld option to reload object files... -r
checking for objdump... objdump
checking how to recognize dependent libraries... pass_all
checking for dlltool... no
checking how to associate runtime and link libraries... printf %s\n
checking for ar... ar
checking for archiver @FILE support... @
checking for strip... strip
checking for ranlib... ranlib
checking command to parse /usr/bin/nm -B output from gcc object... ok
checking for sysroot... no
```

```
checking for string.h... yes
checking for memory.h... yes
checking for strings.h... yes
checking for inttypes.h... yes
checking for stdint.h... yes
checking for unistd.h... yes
checking for dlfcn.h... yes
checking for objdir... .libs
checking if gcc supports -fno-rtti -fno-exceptions... no
checking for gcc option to produce PIC... -fPIC -DPIC
checking if gcc PIC flag -fPIC -DPIC works... yes
checking if gcc static flag -static works... yes
checking if gcc supports -c -o file.o... yes
checking if gcc supports -c -o file.o... (cached) yes
checking whether the gcc linker (/usr/bin/ld -m elf_x86_64) supports shared libraries... yes
checking whether -lc should be explicitly linked in... no
checking dynamic linker characteristics... GNU/Linux ld.so
checking how to hardcode library paths into programs... immediate
checking whether stripping libraries is possible... yes
checking if libtool supports shared libraries... yes
checking whether to build shared libraries... yes
checking whether to build static libraries... yes
checking for visibility support... yes
checking CFLAGS for gcc -Wall... -Wall
checking CFLAGS for gcc -Wwrite-strings... -Wwrite-strings
checking CFLAGS for gcc -Wsign-compare... -Wsign-compare
checking CFLAGS for gcc -Wcast-align... -Wcast-align
checking CFLAGS for gcc -Wextra... -Wextra
checking CFLAGS for gcc -Wformat... -Wformat
checking CFLAGS for gcc -Wformat-security... -Wformat-security
checking CFLAGS for gcc -Wno-unused-parameter... -Wno-unused-parameter
checking CFLAGS for gcc -fno-strict-aliasing... -fno-strict-aliasing
checking CFLAGS for gcc -fdiagnostics-show-option... -fdiagnostics-show-option
checking CFLAGS for gcc -pedantic -std=c99 -D_GNU_SOURCE... -pedantic -std=c99 -D_GNU_SOURCE
checking for getaddrinfo... yes
checking for flex... flex
checking for flex 2.4 or higher... yes
checking for bison... no
configure: WARNING: don't have both flex and bison; reverting to lex/yacc
checking for capable lex... insufficient
configure: error: Your operating system's lex is insufficient to compile
         libsfbpf. You should install both bison and flex.
         flex is a lex replacement that has many advantages,
         including being able to compile libsfbpf.  For more
         information, see http://www.gnu.org/software/flex/flex.html .
vishal@vishal-VirtualBox:~/daq-2.0.7$
```

```
vishal@vishal-VirtualBox:~/daq-2.0.7$ sudo apt-get install bison
[sudo] password for vishal:
Reading package lists... Done
Building dependency tree
Reading state information... Done
Suggested packages:
  bison-doc
The following NEW packages will be installed:
  bison
0 upgraded, 1 newly installed, 0 to remove and 246 not upgraded.
Need to get 657 kB of archives.
After this operation, 2,028 kB of additional disk space will be used.
Get:1 http://in.archive.ubuntu.com/ubuntu focal/main amd64 bison amd64 2:3.5.1+dfsg-1 [657 kB]
Fetched 657 kB in 7s (95.0 kB/s)
Selecting previously unselected package bison.
(Reading database ... 189119 files and directories currently installed.)
Preparing to unpack .../bison_2%3a3.5.1+dfsg-1_amd64.deb ...
Unpacking bison (2:3.5.1+dfsg-1) ...
Setting up bison (2:3.5.1+dfsg-1) ...
update-alternatives: using /usr/bin/bison.yacc to provide /usr/bin/yacc (yacc) in auto mode
Processing triggers for man-db (2.9.1-1) ...
```

```
vishal@vishal-VirtualBox:~/daq-2.0.7$ sudo apt-get install bison flex
Reading package lists... Done
Building dependency tree
Reading state information... Done
bison is already the newest version (2:3.5.1+dfsg-1).
flex is already the newest version (2.6.4-6.2).
0 upgraded, 0 newly installed, 0 to remove and 246 not upgraded.
```

```
vishal@vishal-VirtualBox:~/daq-2.0.7$ ./configure && make && sudo make install
checking for a BSD-compatible install... /usr/bin/install -c
checking whether build environment is sane... yes
checking for a thread-safe mkdir -p... /usr/bin/mkdir -p
checking for gawk... no
checking for mawk... mawk
checking whether make sets $(MAKE)... yes
checking whether make supports nested variables... yes
checking for gcc... gcc
checking whether the C compiler works... yes
checking for C compiler default output file name... a.out
checking for suffix of executables...
checking whether we are cross compiling... no
checking for suffix of object files... o
checking whether we are using the GNU C compiler... yes
checking whether gcc accepts -g... yes
checking for gcc option to accept ISO C89... none needed
checking whether gcc understands -c and -o together... yes
checking for style of include used by make... GNU
checking dependency style of gcc... gcc3
checking build system type... x86_64-unknown-linux-gnu
checking host system type... x86_64-unknown-linux-gnu
checking how to print strings... printf
checking for a sed that does not truncate output... /usr/bin/sed
checking for grep that handles long lines and -e... /usr/bin/grep
checking for egrep... /usr/bin/grep -E
checking for fgrep... /usr/bin/grep -F
checking for ld used by gcc... /usr/bin/ld
checking if the linker (/usr/bin/ld) is GNU ld... yes
checking for BSD- or MS-compatible name lister (nm)... /usr/bin/nm -B
checking the name lister (/usr/bin/nm -B) interface... BSD nm
checking whether ln -s works... yes
checking the maximum length of command line arguments... 1572864
checking how to convert x86_64-unknown-linux-gnu file names to x86_64-unknown-linux-gnu format... func_convert_file_noop
checking how to convert x86_64-unknown-linux-gnu file names to toolchain format... func_convert_file_noop
checking for /usr/bin/ld option to reload object files... -r
checking for objdump... objdump
checking how to recognize dependent libraries... pass_all
checking for dlltool... no
checking how to associate runtime and link libraries... printf %s\n
checking for ar... ar
checking for archiver @FILE support... @
checking for strip... strip
```

```
checking CFLAGS for gcc -Wextra... -Wextra
checking CFLAGS for gcc -Wformat... -Wformat
checking CFLAGS for gcc -Wformat-security... -Wformat-security
checking CFLAGS for gcc -Wno-unused-parameter... -Wno-unused-parameter
checking CFLAGS for gcc -fno-strict-aliasing... -fno-strict-aliasing
checking CFLAGS for gcc -fdiagnostics-show-option... -fdiagnostics-show-option
checking CFLAGS for gcc -pedantic -std=c99 -D_GNU_SOURCE... -pedantic -std=c99 -D_GNU_SOURCE
checking for getaddrinfo... yes
checking for flex... flex
checking for flex 2.4 or higher... yes
checking for bison... bison
checking linux/if_ether.h usability... yes
checking linux/if_ether.h presence... yes
checking for linux/if_ether.h... yes
checking linux/if_packet.h usability... yes
checking linux/if_packet.h presence... yes
checking for linux/if_packet.h... yes
checking whether TPACKET2_HDRLEN is declared... yes
checking whether PACKET_TX_RING is declared... yes
checking pcap.h usability... no
checking pcap.h presence... no
checking for pcap.h... no
checking for pcap_lib_version in -lpcap... no
checking netinet/in.h usability... yes
checking netinet/in.h presence... yes
checking for netinet/in.h... yes
checking libipq.h usability... no
checking libipq.h presence... no
checking for libipq.h... no
checking for linux/netfilter.h... yes
checking for netinet/in.h... (cached) yes
checking libnetfilter_queue/libnetfilter_queue.h usability... no
checking libnetfilter_queue/libnetfilter_queue.h presence... no
checking for libnetfilter_queue/libnetfilter_queue.h... no
checking for linux/netfilter.h... (cached) yes
checking for pcap.h... (cached) no
checking for pcap_lib_version... checking for pcap_lib_version in -lpcap... (cached) no

    ERROR!  Libpcap library version >= 1.0.0 not found.
    Get it from http://www.tcpdump.org
```

```
vishal@vishal-VirtualBox:~/daq-2.0.7$ sudo apt-get install tcpdump
Reading package lists... Done
Building dependency tree
Reading state information... Done
tcpdump is already the newest version (4.9.3-4).
tcpdump set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 246 not upgraded.
vishal@vishal-VirtualBox:~/daq-2.0.7$ tcpdump --v
tcpdump version 4.9.3
libpcap version 1.9.1 (with TPACKET_V3)
OpenSSL 1.1.1f  31 Mar 2020
vishal@vishal-VirtualBox:~/daq-2.0.7$ sudo apt-get install libpcap-dev
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libpcap0.8-dev
The following NEW packages will be installed:
  libpcap-dev libpcap0.8-dev
0 upgraded, 2 newly installed, 0 to remove and 246 not upgraded.
Need to get 248 kB of archives.
After this operation, 852 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://in.archive.ubuntu.com/ubuntu focal/main amd64 libpcap0.8-dev amd64 1.9.1-3 [244 kB]
Get:2 http://in.archive.ubuntu.com/ubuntu focal/main amd64 libpcap-dev amd64 1.9.1-3 [3,484 B]
Fetched 248 kB in 4s (60.8 kB/s)
Selecting previously unselected package libpcap0.8-dev:amd64.
(Reading database ... 189214 files and directories currently installed.)
Preparing to unpack .../libpcap0.8-dev_1.9.1-3_amd64.deb ...
Unpacking libpcap0.8-dev:amd64 (1.9.1-3) ...
Selecting previously unselected package libpcap-dev:amd64.
Preparing to unpack .../libpcap-dev_1.9.1-3_amd64.deb ...
Unpacking libpcap-dev:amd64 (1.9.1-3) ...
Setting up libpcap0.8-dev:amd64 (1.9.1-3) ...
Setting up libpcap-dev:amd64 (1.9.1-3) ...
Processing triggers for man-db (2.9.1-1) ...
```

```
vishal@vishal-VirtualBox:~/daq-2.0.7$ ./configure && make && sudo make install
checking for a BSD-compatible install... /usr/bin/install -c
checking whether build environment is sane... yes
checking for a thread-safe mkdir -p... /usr/bin/mkdir -p
checking for gawk... no
checking for mawk... mawk
checking whether make sets $(MAKE)... yes
checking whether make supports nested variables... yes
checking for gcc... gcc
checking whether the C compiler works... yes
checking for C compiler default output file name... a.out
checking for suffix of executables...
checking whether we are cross compiling... no
checking for suffix of object files... o
checking whether we are using the GNU C compiler... yes
checking whether gcc accepts -g... yes
checking for gcc option to accept ISO C89... none needed
checking whether gcc understands -c and -o together... yes
checking for style of include used by make... GNU
checking dependency style of gcc... gcc3
checking build system type... x86_64-unknown-linux-gnu
checking host system type... x86_64-unknown-linux-gnu
checking how to print strings... printf
checking for a sed that does not truncate output... /usr/bin/sed
checking for grep that handles long lines and -e... /usr/bin/grep
checking for egrep... /usr/bin/grep -E
checking for fgrep... /usr/bin/grep -F
checking for ld used by gcc... /usr/bin/ld
checking if the linker (/usr/bin/ld) is GNU ld... yes
checking for BSD- or MS-compatible name lister (nm)... /usr/bin/nm -B
checking the name lister (/usr/bin/nm -B) interface... BSD nm
checking whether ln -s works... yes
checking the maximum length of command line arguments... 1572864
checking how to convert x86_64-unknown-linux-gnu file names to x86_64-unknown-linux-gnu format... func_convert_file_noop
checking how to convert x86_64-unknown-linux-gnu file names to toolchain format... func_convert_file_noop
checking for /usr/bin/ld option to reload object files... -r
checking for objdump... objdump
checking how to recognize dependent libraries... pass_all
checking for dlltool... no
checking how to associate runtime and link libraries... printf %s\n
checking for ar... ar
checking for archiver @FILE support... @
checking for strip... strip
checking for ranlib... ranlib
```

```
See any operating system documentation about shared libraries for
more information, such as the ld(1) and ld.so(8) manual pages.
----------------------------------------------------------------------
make[2]: Nothing to be done for 'install-data-am'.
make[2]: Leaving directory '/home/vishal/daq-2.0.7/os-daq-modules'
make[1]: Leaving directory '/home/vishal/daq-2.0.7/os-daq-modules'
make[1]: Entering directory '/home/vishal/daq-2.0.7'
make[2]: Entering directory '/home/vishal/daq-2.0.7'
make[2]: Nothing to be done for 'install-exec-am'.
make[2]: Nothing to be done for 'install-data-am'.
make[2]: Leaving directory '/home/vishal/daq-2.0.7'
make[1]: Leaving directory '/home/vishal/daq-2.0.7'
vishal@vishal-VirtualBox:~/daq-2.0.7$ cd
vishal@vishal-VirtualBox:~$ tar xvzf snort-2.9.17.tar.gz
snort-2.9.17/
snort-2.9.17/snort.8
snort-2.9.17/install-sh
snort-2.9.17/snort.pc.in
snort-2.9.17/aclocal.m4
snort-2.9.17/config.guess
snort-2.9.17/compile
snort-2.9.17/config.h.in
snort-2.9.17/missing
snort-2.9.17/LICENSE
snort-2.9.17/config.sub
snort-2.9.17/COPYING
snort-2.9.17/templates/
snort-2.9.17/templates/sp_template.c
snort-2.9.17/templates/sp_template.h
snort-2.9.17/templates/spp_template.c
snort-2.9.17/templates/Makefile.in
snort-2.9.17/templates/Makefile.am
snort-2.9.17/templates/spp_template.h
snort-2.9.17/verstuff.pl
snort-2.9.17/Makefile.in
snort-2.9.17/etc/
snort-2.9.17/etc/file_magic.conf
snort-2.9.17/etc/unicode.map
snort-2.9.17/etc/gen-msg.map
snort-2.9.17/etc/attribute_table.dtd
snort-2.9.17/etc/Makefile.in
snort-2.9.17/etc/threshold.conf
```

```
vishal@vishal-VirtualBox:~$ cd snort-2.9.17
vishal@vishal-VirtualBox:~/snort-2.9.17$ ./configure --enable-sourcefire && make && sudo make install
checking for a BSD-compatible install... /usr/bin/install -c
checking whether build environment is sane... yes
checking for a thread-safe mkdir -p... /usr/bin/mkdir -p
checking for gawk... no
checking for mawk... mawk
checking whether make sets $(MAKE)... yes
checking whether make supports nested variables... yes
checking whether make supports the include directive... yes (GNU style)
checking for gcc... gcc
checking whether the C compiler works... yes
checking for C compiler default output file name... a.out
checking for suffix of executables...
checking whether we are cross compiling... no
checking for suffix of object files... o
checking whether we are using the GNU C compiler... yes
checking whether gcc accepts -g... yes
checking for gcc option to accept ISO C89... none needed
checking whether gcc understands -c and -o together... yes
checking dependency style of gcc... gcc3
checking for gcc option to accept ISO C99... none needed
checking for gcc option to accept ISO Standard C... (cached) none needed
checking for gcc... (cached) gcc
checking whether we are using the GNU C compiler... (cached) yes
checking whether gcc accepts -g... (cached) yes
checking for gcc option to accept ISO C89... (cached) none needed
checking whether gcc understands -c and -o together... (cached) yes
checking dependency style of gcc... (cached) gcc3
checking build system type... x86_64-pc-linux-gnu
checking host system type... x86_64-pc-linux-gnu
checking how to print strings... printf
checking for a sed that does not truncate output... /usr/bin/sed
checking for grep that handles long lines and -e... /usr/bin/grep
checking for egrep... /usr/bin/grep -E
checking for fgrep... /usr/bin/grep -F
checking for ld used by gcc... /usr/bin/ld
checking if the linker (/usr/bin/ld) is GNU ld... yes
checking for BSD- or MS-compatible name lister (nm)... /usr/bin/nm -B
checking the name lister (/usr/bin/nm -B) interface... BSD nm
checking whether ln -s works... yes
checking the maximum length of command line arguments... 1572864
checking how to convert x86_64-pc-linux-gnu file names to x86_64-pc-linux-gnu format... func_convert_file_noop
checking how to convert x86_64-pc-linux-gnu file names to toolchain format... func_convert_file_noop
```

```
   ERROR!  Libpcre header not found.
   Get it from http://www.pcre.org
vishal@vishal-VirtualBox:~/snort-2.9.17$ sudo apt-get install libpcre3.dev
Reading package lists... Done
Building dependency tree
Reading state information... Done
Note, selecting 'libpcre3-dev' for regex 'libpcre3.dev'
The following additional packages will be installed:
  libpcre16-3 libpcre32-3 libpcrecpp0v5
The following NEW packages will be installed:
  libpcre16-3 libpcre3-dev libpcre32-3 libpcrecpp0v5
0 upgraded, 4 newly installed, 0 to remove and 246 not upgraded.
Need to get 846 kB of archives.
After this operation, 3,586 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://in.archive.ubuntu.com/ubuntu focal/main amd64 libpcre16-3 amd64 2:8.39-12build1 [150 kB]
Get:2 http://in.archive.ubuntu.com/ubuntu focal/main amd64 libpcre32-3 amd64 2:8.39-12build1 [140 kB]
Get:3 http://in.archive.ubuntu.com/ubuntu focal/main amd64 libpcrecpp0v5 amd64 2:8.39-12build1 [15.5 kB]
Get:4 http://in.archive.ubuntu.com/ubuntu focal/main amd64 libpcre3-dev amd64 2:8.39-12build1 [540 kB]
Fetched 846 kB in 8s (109 kB/s)
Selecting previously unselected package libpcre16-3:amd64.
(Reading database ... 189321 files and directories currently installed.)
Preparing to unpack .../libpcre16-3_2%3a8.39-12build1_amd64.deb ...
Unpacking libpcre16-3:amd64 (2:8.39-12build1) ...
Selecting previously unselected package libpcre32-3:amd64.
Preparing to unpack .../libpcre32-3_2%3a8.39-12build1_amd64.deb ...
Unpacking libpcre32-3:amd64 (2:8.39-12build1) ...
Selecting previously unselected package libpcrecpp0v5:amd64.
Preparing to unpack .../libpcrecpp0v5_2%3a8.39-12build1_amd64.deb ...
Unpacking libpcrecpp0v5:amd64 (2:8.39-12build1) ...
Selecting previously unselected package libpcre3-dev:amd64.
Preparing to unpack .../libpcre3-dev_2%3a8.39-12build1_amd64.deb ...
Unpacking libpcre3-dev:amd64 (2:8.39-12build1) ...
Setting up libpcrecpp0v5:amd64 (2:8.39-12build1) ...
Setting up libpcre16-3:amd64 (2:8.39-12build1) ...
Setting up libpcre32-3:amd64 (2:8.39-12build1) ...
Setting up libpcre3-dev:amd64 (2:8.39-12build1) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for libc-bin (2.31-0ubuntu9) ...
```

```
vishal@vishal-VirtualBox:~/snort-2.9.17$ ./configure --enable-sourcefire && make && sudo make install
checking for a BSD-compatible install... /usr/bin/install -c
checking whether build environment is sane... yes
checking for a thread-safe mkdir -p... /usr/bin/mkdir -p
checking for gawk... no
checking for mawk... mawk
checking whether make sets $(MAKE)... yes
checking whether make supports nested variables... yes
checking whether make supports the include directive... yes (GNU style)
checking for gcc... gcc
checking whether the C compiler works... yes
checking for C compiler default output file name... a.out
checking for suffix of executables...
checking whether we are cross compiling... no
checking for suffix of object files... o
checking whether we are using the GNU C compiler... yes
checking whether gcc accepts -g... yes
checking for gcc option to accept ISO C89... none needed
checking whether gcc understands -c and -o together... yes
checking dependency style of gcc... gcc3
checking for gcc option to accept ISO C99... none needed
checking for gcc option to accept ISO Standard C... (cached) none needed
checking for gcc... (cached) gcc
checking whether we are using the GNU C compiler... (cached) yes
checking whether gcc accepts -g... (cached) yes
checking for gcc option to accept ISO C89... (cached) none needed
checking whether gcc understands -c and -o together... (cached) yes
checking dependency style of gcc... (cached) gcc3
checking build system type... x86_64-pc-linux-gnu
checking host system type... x86_64-pc-linux-gnu
checking how to print strings... printf
checking for a sed that does not truncate output... /usr/bin/sed
checking for grep that handles long lines and -e... /usr/bin/grep
checking for egrep... /usr/bin/grep -E
checking for fgrep... /usr/bin/grep -F
checking for ld used by gcc... /usr/bin/ld
checking if the linker (/usr/bin/ld) is GNU ld... yes
checking for BSD- or MS-compatible name lister (nm)... /usr/bin/nm -B
checking the name lister (/usr/bin/nm -B) interface... BSD nm
checking whether ln -s works... yes
checking the maximum length of command line arguments... 1572864
checking how to convert x86_64-pc-linux-gnu file names to x86_64-pc-linux-gnu format... func_convert_file_noop
checking how to convert x86_64-pc-linux-gnu file names to toolchain format... func_convert_file_noop
checking for /usr/bin/ld option to reload object files... -r
checking for objdump... objdump
```

```
   ERROR!  dnet header not found, go get it from
   http://code.google.com/p/libdnet/ or use the --with-dnet-*
   options, if you have it installed in an unusual place
make: *** No targets specified and no makefile found.  Stop.
vishal@vishal-VirtualBox:~/snort-2.9.17$ sudo apt-get install libdumbnet-dev
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libdumbnet1
The following NEW packages will be installed:
  libdumbnet-dev libdumbnet1
0 upgraded, 2 newly installed, 0 to remove and 246 not upgraded.
Need to get 81.8 kB of archives.
After this operation, 329 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://in.archive.ubuntu.com/ubuntu focal/universe amd64 libdumbnet1 amd64 1.12-9build1 [25.4 kB]
Get:2 http://in.archive.ubuntu.com/ubuntu focal/universe amd64 libdumbnet-dev amd64 1.12-9build1 [56.4 kB]
Fetched 81.8 kB in 2s (46.8 kB/s)
Selecting previously unselected package libdumbnet1:amd64.
(Reading database ... 189466 files and directories currently installed.)
Preparing to unpack .../libdumbnet1_1.12-9build1_amd64.deb ...
Unpacking libdumbnet1:amd64 (1.12-9build1) ...
Selecting previously unselected package libdumbnet-dev.
Preparing to unpack .../libdumbnet-dev_1.12-9build1_amd64.deb ...
Unpacking libdumbnet-dev (1.12-9build1) ...
Setting up libdumbnet1:amd64 (1.12-9build1) ...
Setting up libdumbnet-dev (1.12-9build1) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for libc-bin (2.31-0ubuntu9) ...
```

```
vishal@vishal-VirtualBox:~/snort-2.9.17$ ./configure --enable-sourcefire && make && sudo make install
checking for a BSD-compatible install... /usr/bin/install -c
checking whether build environment is sane... yes
checking for a thread-safe mkdir -p... /usr/bin/mkdir -p
checking for gawk... no
checking for mawk... mawk
checking whether make sets $(MAKE)... yes
checking whether make supports nested variables... yes
checking whether make supports the include directive... yes (GNU style)
checking for gcc... gcc
checking whether the C compiler works... yes
checking for C compiler default output file name... a.out
checking for suffix of executables...
checking whether we are cross compiling... no
checking for suffix of object files... o
checking whether we are using the GNU C compiler... yes
checking whether gcc accepts -g... yes
checking for gcc option to accept ISO C89... none needed
checking whether gcc understands -c and -o together... yes
checking dependency style of gcc... gcc3
checking for gcc option to accept ISO C99... none needed
checking for gcc option to accept ISO Standard C... (cached) none needed
checking for gcc... (cached) gcc
checking whether we are using the GNU C compiler... (cached) yes
checking whether gcc accepts -g... (cached) yes
checking for gcc option to accept ISO C89... (cached) none needed
checking whether gcc understands -c and -o together... (cached) yes
checking dependency style of gcc... (cached) gcc3
checking build system type... x86_64-pc-linux-gnu
checking host system type... x86_64-pc-linux-gnu
checking how to print strings... printf
checking for a sed that does not truncate output... /usr/bin/sed
checking for grep that handles long lines and -e... /usr/bin/grep
checking for egrep... /usr/bin/grep -E
checking for fgrep... /usr/bin/grep -F
checking for ld used by gcc... /usr/bin/ld
checking if the linker (/usr/bin/ld) is GNU ld... yes
checking for BSD- or MS-compatible name lister (nm)... /usr/bin/nm -B
checking the name lister (/usr/bin/nm -B) interface... BSD nm
checking whether ln -s works... yes
checking the maximum length of command line arguments... 1572864
checking how to convert x86_64-pc-linux-gnu file names to x86_64-pc-linux-gnu format... func_convert_file_noop
checking how to convert x86_64-pc-linux-gnu file names to toolchain format... func_convert_file_noop
```

```
Package configuration

                    Configuring snort
 This value is usually "eth0", but this may be inappropriate in some network environments; for a dialup connection "ppp0" might be more
 appropriate (see the output of "/sbin/ifconfig").

 Typically, this is the same interface as the "default route" is on. You can determine which interface is used for this by running "/sbin/route
 -n" (look for "0.0.0.0").

 It is also not uncommon to use an interface with no IP address configured in promiscuous mode. For such cases, select the interface in this
 system that is physically connected to the network that should be inspected, enable promiscuous mode later on and make sure that the network
 traffic is sent to this interface (either connected to a "port mirroring/spanning" port in a switch, to a hub, or to a tap).

 You can configure multiple interfaces, just by adding more than one interface name separated by spaces. Each interface can have its own
 specific configuration.

 Interface(s) which Snort should listen on:

 eth0

                                                  <Ok>
```

```
vishal@vishal-VirtualBox:~$ sudo tar -xvzf snortrules-snapshot-2983.tar.gz -C /etc/snort/rules
rules/
rules/VRT-License.txt
rules/os-linux.rules
rules/file-flash.rules
rules/exploit.rules
rules/protocol-icmp.rules
rules/protocol-voip.rules
rules/local.rules
rules/browser-ie.rules
rules/pua-other.rules
rules/protocol-imap.rules
rules/tftp.rules
rules/file-executable.rules
rules/chat.rules
rules/policy-social.rules
rules/web-php.rules
rules/specific-threats.rules
rules/browser-chrome.rules
rules/ddos.rules
rules/malware-backdoor.rules
rules/server-iis.rules
rules/malware-tools.rules
rules/protocol-ftp.rules
rules/icmp-info.rules
rules/protocol-pop.rules
rules/backdoor.rules
rules/spyware-put.rules
rules/netbios.rules
rules/file-office.rules
rules/botnet-cnc.rules
rules/malware-cnc.rules
rules/policy-spam.rules
rules/os-other.rules
rules/server-mssql.rules
rules/browser-firefox.rules
rules/finger.rules
rules/pop3.rules
rules/policy-multimedia.rules
rules/file-pdf.rules
rules/other-ids.rules
```

```
vishal@vishal-VirtualBox:~$ cd /etc/snort/rules
vishal@vishal-VirtualBox:/etc/snort/rules$ ls
attack-responses.rules          community-mail-client.rules    community-web-iis.rules    icmp.rules        pop2.rules       telnet.rules
backdoor.rules                  community-misc.rules           community-web-misc.rules   imap.rules        pop3.rules       tftp.rules
bad-traffic.rules               community-nntp.rules           community-web-php.rules    info.rules        porn.rules       virus.rules
chat.rules                      community-oracle.rules         ddos.rules                 local.rules       preproc_rules    web-attacks.rules
community-bot.rules             community-policy.rules         deleted.rules              misc.rules        rpc.rules        web-cgi.rules
community-deleted.rules         community-sip.rules            dns.rules                  multimedia.rules  rservices.rules  web-client.rules
community-dos.rules             community-smtp.rules           dos.rules                  mysql.rules       rules            web-coldfusion.rules
community-exploit.rules         community-sql-injection.rules  etc                        netbios.rules     scan.rules       web-frontpage.rules
community-ftp.rules             community-virus.rules          experimental.rules         nntp.rules        shellcode.rules  web-iis.rules
community-game.rules            community-web-attacks.rules    exploit.rules              oracle.rules      smtp.rules       web-misc.rules
community-icmp.rules            community-web-cgi.rules        finger.rules               other-ids.rules   snmp.rules       web-php.rules
community-imap.rules            community-web-client.rules     ftp.rules                  p2p.rules         so_rules         x11.rules
community-inappropriate.rules   community-web-dos.rules        icmp-info.rules            policy.rules      sql.rules
vishal@vishal-VirtualBox:/etc/snort/rules$ cd
vishal@vishal-VirtualBox:~$ snort --version

   ,,_     -*> 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 1.9.1 (with TPACKET_V3)
           Using PCRE version: 8.39 2016-06-14
           Using ZLIB version: 1.2.11
```

```
vishal@vishal-VirtualBox:~$ snort --version

   ,,_     -*> 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 1.9.1 (with TPACKET_V3)
           Using PCRE version: 8.39 2016-06-14
           Using ZLIB version: 1.2.11
```

```
vishal@vishal-VirtualBox:~$ snort -h
snort: option requires an argument -- 'h'

   ,,_     -*> 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 1.9.1 (with TPACKET_V3)
           Using PCRE version: 8.39 2016-06-14
           Using ZLIB version: 1.2.11

USAGE: snort [-options] <filter options>
Options:
        -A         Set alert mode: fast, full, console, test or none  (alert file alerts only)
                   "unsock" enables UNIX socket logging (experimental).
        -b         Log packets in tcpdump format (much faster!)
        -B <mask>  Obfuscated IP addresses in alerts and packet dumps using CIDR mask
        -c <rules> Use Rules File <rules>
        -C         Print out payloads with character data only (no hex)
        -d         Dump the Application Layer
        -D         Run Snort in background (daemon) mode
        -e         Display the second layer header info
        -f         Turn off fflush() calls after binary log writes
        -F <bpf>   Read BPF filters from file <bpf>
        -g <gname> Run snort gid as <gname> group (or gid) after initialization
        -G <0xid>  Log Identifier (to uniquely id events for multiple snorts)
        -h <hn>    Set home network = <hn>
                   (for use with -l or -B, does NOT change $HOME_NET in IDS mode)
        -H         Make hash tables deterministic.
        -i <if>    Listen on interface <if>
        -I         Add Interface name to alert output
        -k <mode>  Checksum mode (all,noip,notcp,noudp,noicmp,none)
        -K <mode>  Logging mode (pcap[default],ascii,none)
        -l <ld>    Log to directory <ld>
        -L <file>  Log to this tcpdump file
        -M         Log messages to syslog (not alerts)
        -m <umask> Set umask = <umask>
        -n <cnt>   Exit after receiving <cnt> packets
        -N         Turn off logging (alerts still work)
        -O         Obfuscate the logged IP addresses
        -p         Disable promiscuous mode sniffing
        -P <snap>  Set explicit snaplen of packet (default: 1514)
        -q         Quiet. Don't show banner and status report
        -Q         Enable inline mode operation.
```

While you install the snort, you system may miss some libraries. You need to install the required libraries, too.

Snort is software created by Martin Roesch, which is widely used as Intrusion Prevention System [IPS] and Intrusion Detection System [IDS] in the network. It is separated into the five most important mechanisms for instance: Detection engine, Logging, and alerting system, a Packet decoder, Preprocessor, and Output modules.

The program is quite famous to carry out real-time traffic analysis, also used to detect query or attacks, packet logging on Internet Protocol networks, to detect malicious activity, denial of service attacks and port scans by monitoring network traffic, buffer overflows, server message block probes, and stealth port scans.

Snort can be configured in three main modes:

Sniffer mode: it will observe network packets and present them on the console.

Packet logger mode: it will record packets to the disk.

Intrusion detection mode: the program will monitor network traffic and analyze it against a rule set defined by the user.

After that, the application will execute a precise action depend upon what has been identified.

Configuring and Starting the Snort IDS

After installing the Snort, we need to configure it. The configuration file of snort is stored at /etc/snort/snort.conf. The screenshot below shows the commands to configure the Snort. You need to switch to root to gain the permission to read the snort configurations file.

After configuring the Snort, you need to start the Snort. You can simply type the following command to start the service.

```
vishal@vishal-VirtualBox:~$ sudo su
root@vishal-VirtualBox:/home/vishal# vim /etc/snortsnort.conf

[1]+  Stopped                 vim /etc/snortsnort.conf
root@vishal-VirtualBox:/home/vishal# service snort start
root@vishal-VirtualBox:/home/vishal# /etc/init.d/snort start
Starting snort (via systemctl): snort.service.
root@vishal-VirtualBox:/home/vishal#
```

```
#--------------------------------------------------
#   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-no
rmalizer --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
#  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
"/etc/snort/snort.conf" 735L, 28880C                                                                  1,1           Top
```


```
root@vishal-VirtualBox:/home/vishal# vi /etc/snort/snort.conf

[1]+  Stopped                 vi /etc/snort/snort.conf
root@vishal-VirtualBox:/home/vishal# mkdir log
root@vishal-VirtualBox:/home/vishal# snort -l./log -b -c /etc/snort/snort.conf
Running in IDS 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 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 3444
3:34444 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 7000:70
01 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 99
99 11371 34443:34444 41080 50002 55555 ]
PortVar 'GTP_PORTS' defined :  [ 2123 2152 3386 ]
Detection:
   Search-Method = AC-Full-Q
    Split Any/Any group = enabled
    Search-Method-Optimizations = enabled
    Maximum pattern length = 20
Tagged Packet Limit: 256
Loading dynamic engine /usr/lib/snort_dynamicengine/libsf_engine.so... done
Loading all dynamic detection libs from /usr/lib/snort_dynamicrules...
WARNING: No dynamic libraries found in directory /usr/lib/snort_dynamicrules.
  Finished Loading all dynamic detection libs from /usr/lib/snort_dynamicrules
Loading all dynamic preprocessor libs from /usr/lib/snort_dynamicpreprocessor/...
  Loading dynamic preprocessor library /usr/lib/snort_dynamicpreprocessor//libsf_ftptelnet_preproc.so... done
  Loading dynamic preprocessor library /usr/lib/snort_dynamicpreprocessor//libsf_reputation_preproc.so... done
  Loading dynamic preprocessor library /usr/lib/snort_dynamicpreprocessor//libsf_sdf_preproc.so... done
  Loading dynamic preprocessor library /usr/lib/snort_dynamicpreprocessor//libsf_dnp3_preproc.so... done
  Loading dynamic preprocessor library /usr/lib/snort_dynamicpreprocessor//libsf_pop_preproc.so... done
  Loading dynamic preprocessor library /usr/lib/snort_dynamicpreprocessor//libsf_dce2_preproc.so... done
  Loading dynamic preprocessor library /usr/lib/snort_dynamicpreprocessor//libsf_smtp_preproc.so... done
```

```
Frag3 global config:
    Max frags: 65536
    Fragment memory cap: 4194304 bytes
Frag3 engine config:
    Bound Address: default
    Target-based policy: WINDOWS
    Fragment timeout: 180 seconds
    Fragment min_ttl:   1
    Fragment Anomalies: Alert
    Overlap Limit:     10
    Min fragment Length:     100
      Max Expected Streams: 768
Stream global config:
    Track TCP sessions: ACTIVE
    Max TCP sessions: 262144
    TCP cache pruning timeout: 30 seconds
    TCP cache nominal timeout: 3600 seconds
    Memcap (for reassembly packet storage): 8388608
    Track UDP sessions: ACTIVE
    Max UDP sessions: 131072
    UDP cache pruning timeout: 30 seconds
    UDP cache nominal timeout: 180 seconds
    Track ICMP sessions: INACTIVE
    Track IP sessions: INACTIVE
    Log info if session memory consumption exceeds 1048576
    Send up to 2 active responses
    Wait at least 5 seconds between responses
    Protocol Aware Flushing: ACTIVE
        Maximum Flush Point: 16000
Stream TCP Policy config:
    Bound Address: default
    Reassembly Policy: WINDOWS
    Timeout: 180 seconds
    Limit on TCP Overlaps: 10
    Maximum number of bytes to queue per session: 1048576
    Maximum number of segs to queue per session: 2621
    Options:
        Require 3-Way Handshake: YES
        3-Way Handshake Timeout: 180
        Detect Anomalies: YES
    Reassembly Ports:
```

```
    Maximum number of segs to queue per session: 2621
    Options:
        Require 3-Way Handshake: YES
        3-Way Handshake Timeout: 180
        Detect Anomalies: YES
    Reassembly Ports:
      21 client (Footprint)
      22 client (Footprint)
      23 client (Footprint)
      25 client (Footprint)
      42 client (Footprint)
      53 client (Footprint)
      79 client (Footprint)
      80 client (Footprint) server (Footprint)
      81 client (Footprint) server (Footprint)
      109 client (Footprint)
      110 client (Footprint)
      111 client (Footprint)
      113 client (Footprint)
      119 client (Footprint)
      135 client (Footprint)
      136 client (Footprint)
      137 client (Footprint)
      139 client (Footprint)
      143 client (Footprint)
      161 client (Footprint)
      additional ports configured but not printed.
Stream UDP Policy config:
    Timeout: 180 seconds
HttpInspect Config:
    GLOBAL CONFIG
      Detect Proxy Usage:       NO
      IIS Unicode Map Filename: /etc/snort/unicode.map
      IIS Unicode Map Codepage: 1252
      Memcap used for logging URI and Hostname: 150994944
      Max Gzip Memory: 104857600
      Max Gzip Sessions: 201649
      Gzip Compress Depth: 65535
      Gzip Decompress Depth: 65535
    DEFAULT SERVER CONFIG:
      Server profile: All
      Ports (PAF): 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
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 5
0002 55555
      Server Flow Depth: 0
      Client Flow Depth: 0
```

```
      Client Flow Depth: 0
      Max Chunk Length: 500000
      Small Chunk Length Evasion: chunk size <= 10, threshold >= 5 times
      Max Header Field Length: 750
      Max Number Header Fields: 100
      Max Number of WhiteSpaces allowed with header folding: 200
      Inspect Pipeline Requests: YES
      URI Discovery Strict Mode: NO
      Allow Proxy Usage: NO
      Disable Alerting: NO
      Oversize Dir Length: 500
      Only inspect URI: NO
      Normalize HTTP Headers: NO
      Inspect HTTP Cookies: YES
      Inspect HTTP Responses: YES
      Extract Gzip from responses: YES
      Decompress response files:
      Unlimited decompression of gzip data from responses: YES
      Normalize Javascripts in HTTP Responses: YES
      Max Number of WhiteSpaces allowed with Javascript Obfuscation in HTTP responses: 200
      Normalize HTTP Cookies: NO
      Enable XFF and True Client IP: NO
      Log HTTP URI data: NO
      Log HTTP Hostname data: NO
      Extended ASCII code support in URI: NO
      Ascii: YES alert: NO
      Double Decoding: YES alert: NO
      %U Encoding: YES alert: YES
      Bare Byte: YES alert: NO
      UTF 8: YES alert: NO
      IIS Unicode: YES alert: NO
      Multiple Slash: YES alert: NO
      IIS Backslash: YES alert: NO
      Directory Traversal: YES alert: NO
      Web Root Traversal: YES alert: NO
      Apache WhiteSpace: YES alert: NO
      IIS Delimiter: YES alert: NO
      IIS Unicode Map: GLOBAL IIS UNICODE MAP CONFIG
      Non-RFC Compliant Characters: 0x00 0x01 0x02 0x03 0x04 0x05 0x06 0x07
      Whitespace Characters: 0x09 0x0b 0x0c 0x0d
```

```
4150 Snort rules read
    3476 detection rules
    0 decoder rules
    0 preprocessor rules
3476 Option Chains linked into 271 Chain Headers
0 Dynamic rules
+++++++++++++++++++++++++++++++++++++++++++++++++

+-------------------[Rule Port Counts]---------------------------------------
|             tcp     udp    icmp      ip
|     src     151      18       0       0
|     dst    3306     126       0       0
|     any     383      48     145      22
|      nc      27       8      94      20
|     s+d      12       5       0       0
+------------------------------------------------------------------------------

+-----------------------[detection-filter-config]--------------------------------
| memory-cap : 1048576 bytes
+-----------------------[detection-filter-rules]---------------------------------
| none
-------------------------------------------------------------------------------

+-----------------------[rate-filter-config]-----------------------------------
| memory-cap : 1048576 bytes
+-----------------------[rate-filter-rules]------------------------------------
| none
-------------------------------------------------------------------------------
```

```
+-----------------------[event-filter-config]---------------------------------
| memory-cap : 1048576 bytes
+-----------------------[event-filter-global]---------------------------------
| none
+-----------------------[event-filter-local]----------------------------------
| gen-id=1      sig-id=3152       type=Threshold tracking=src count=5   seconds=2
| gen-id=1      sig-id=2275       type=Threshold tracking=dst count=5   seconds=60
| gen-id=1      sig-id=2495       type=Both      tracking=dst count=20  seconds=60
| gen-id=1      sig-id=1991       type=Limit     tracking=src count=1   seconds=60
| gen-id=1      sig-id=2923       type=Threshold tracking=dst count=10  seconds=60
| gen-id=1      sig-id=2924       type=Threshold tracking=dst count=10  seconds=60
| gen-id=1      sig-id=2496       type=Both      tracking=dst count=20  seconds=60
| gen-id=1      sig-id=2523       type=Both      tracking=dst count=10  seconds=10
| gen-id=1      sig-id=2494       type=Both      tracking=dst count=20  seconds=60
| gen-id=1      sig-id=3273       type=Threshold tracking=src count=5   seconds=2
+----------------------[suppression]-----------------------------------------
| none
-------------------------------------------------------------------------------
Rule application order: activation->dynamic->pass->drop->sdrop->reject->alert->log
Verifying Preprocessor Configurations!
WARNING: flowbits key 'smb.tree.create.llsrpc' is set but not ever checked.
WARNING: flowbits key 'ms_sql_seen_dns' is checked but not ever set.
33 out of 1024 flowbits in use.
```

```
[ Port Based Pattern Matching Memory ]
+- [ Aho-Corasick Summary ] ------------------------------------
| Storage Format    : Full-Q
| Finite Automaton  : DFA
| Alphabet Size     : 256 Chars
| Sizeof State      : Variable (1,2,4 bytes)
| Instances         : 215
|     1 byte states : 204
|     2 byte states : 11
|     4 byte states : 0
| Characters        : 64982
| States            : 32135
| Transitions       : 872051
| 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 "enp0s3".
Reload thread starting...
Reload thread started, thread 0x7f6ab6eb5700 (4654)
Decoding Ethernet
```

```
        --== 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 1.9.1 (with TPACKET_V3)
           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_SIP  Version 1.1  <Build 1>
           Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
           Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
           Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
           Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
           Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
           Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
           Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
           Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
           Preprocessor Object: SF_POP  Version 1.0  <Build 1>
           Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
           Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
           Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
           Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
Commencing packet processing (pid=4649)
```

```
root@vishal-VirtualBox:/home/vishal# cd log
root@vishal-VirtualBox:/home/vishal/log# ls
alert  snort.log.1615833585
root@vishal-VirtualBox:/home/vishal/log#
```

$ service snort start

or

$ /etc/init.d/

snort start

```
root@vishal-VirtualBox:/home/vishal# /etc/init.d/snort start
Starting snort (via systemctl): snort.service.
root@vishal-VirtualBox:/home/vishal# service snort start
root@vishal-VirtualBox:/home/vishal#
```

Snort Rules

Snort is a signature-based IDS, and it defines rules to detect the intrusions. All rules of Snort are stored under /etc/snort/rules directory. The screenshot below shows the files that contain rules of Snort.

$ ls /etc/snort/rules

```
root@vishal-VirtualBox:/home/vishal# ls /etc/snort/rules/
attack-responses.rules          community-mail-client.rules    community-web-iis.rules    icmp.rules        pop2.rules        telnet.rules
backdoor.rules                  community-misc.rules           community-web-misc.rules   imap.rules        pop3.rules        tftp.rules
bad-traffic.rules               community-nntp.rules           community-web-php.rules    info.rules        porn.rules        virus.rules
chat.rules                      community-oracle.rules         ddos.rules                 local.rules       preproc_rules     web-attacks.rules
community-bot.rules             community-policy.rules         deleted.rules              misc.rules        rpc.rules         web-cgi.rules
community-deleted.rules         community-sip.rules            dns.rules                  multimedia.rules  rservices.rules   web-client.rules
community-dos.rules             community-smtp.rules           dos.rules                  mysql.rules       rules             web-coldfusion.rules
community-exploit.rules         community-sql-injection.rules  etc                        netbios.rules     scan.rules        web-frontpage.rules
community-ftp.rules             community-virus.rules          experimental.rules         nntp.rules        shellcode.rules   web-iis.rules
community-game.rules            community-web-attacks.rules    exploit.rules              oracle.rules      smtp.rules        web-misc.rules
community-icmp.rules            community-web-cgi.rules        finger.rules               other-ids.rules   snmp.rules        web-php.rules
community-imap.rules            community-web-client.rules     ftp.rules                  p2p.rules         so_rules          x11.rules
community-inappropriate.rules   community-web-dos.rules        icmp-info.rules            policy.rules      sql.rules
root@vishal-VirtualBox:/home/vishal#
```

```
root@vishal-VirtualBox:/home/vishal# vim /etc/snort/rules/web-misc.rules

[3]+  Stopped                 vim /etc/snort/rules/web-misc.rules
root@vishal-VirtualBox:/home/vishal#
```

```
# 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: web-misc.rules,v 1.118.2.8.2.6 2005/07/22 19:19:54 mwatchinski Exp $
#---------------
# WEB-MISC RULES
#---------------

alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS 443 (msg:"WEB-MISC SSLv2 Client_Hello with pad Challenge Length overflow attempt"; flow:to_server,establi
shed; flowbits:isnotset,sslv2.client_hello.request; flowbits:isnotset,sslv3.client_hello.request; flowbits:isnotset,tlsv1.client_hello.request; byte_t
est:1,<,128,0; content:"|01|"; depth:1; offset:3; byte_test:2,<,768,4; flowbits:set,sslv2.client_hello.request; byte_test:2,>,32,10; classtype:attempt
ed-admin; sid:2657; rev:8;)
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS 443 (msg:"WEB-MISC SSLv2 Client_Hello Challenge Length overflow attempt"; flow:to_server,established; flo
wbits:isnotset,sslv2.client_hello.request; flowbits:isnotset,sslv3.client_hello.request; flowbits:isnotset,tlsv1.client_hello.request; byte_test:1,>,1
27,0; content:"|01|"; depth:1; offset:2; byte_test:2,<,768,3; flowbits:set,sslv2.client_hello.request; byte_test:2,>,32,9; classtype:attempted-admin;
sid:2656; rev:7;)
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC cross site scripting attempt"; flow:to_server,established; content:"<SCRIPT>";
 nocase; classtype:web-application-attack; sid:1497; rev:6;)
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC cross site scripting HTML Image tag set to javascript attempt"; flow:to_server
,established; content:"img src=javascript"; nocase; reference:bugtraq,4858; reference:cve,2002-0902; classtype:web-application-attack; sid:1667; rev:7
;)
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC Cisco IOS HTTP configuration attempt"; flow:to_server,established; uricontent:
"/level/"; uricontent:"/exec/"; reference:bugtraq,2936; reference:cve,2001-0537; classtype:web-application-attack; sid:1250; rev:11;)
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC Netscape Enterprise DOS"; flow:to_server,established; content:"REVLOG / "; dep
th:9; reference:bugtraq,2294; reference:cve,2001-0251; classtype:web-application-attack; sid:1047; rev:9;)
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC Netscape Enterprise directory listing attempt"; flow:to_server,established; co
ntent:"INDEX "; depth:6; reference:bugtraq,2285; reference:cve,2001-0250; classtype:web-application-attack; sid:1048; rev:9;)
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC iPlanet GETPROPERTIES attempt"; flow:to_server,established; content:"GETPROPER
TIES"; depth:13; reference:bugtraq,2732; reference:cve,2001-0746; classtype:web-application-attack; sid:1050; rev:11;)
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC Tomcat view source attempt"; flow:to_server,established; uricontent:"%252ejsp"
; reference:bugtraq,2527; reference:cve,2001-0590; classtype:web-application-attack; sid:1056; rev:8;)
"/etc/snort/rules/web-misc.rules" 443L, 97307C                                                                  6,1           Top
```

Writing and Adding a Snort Rule

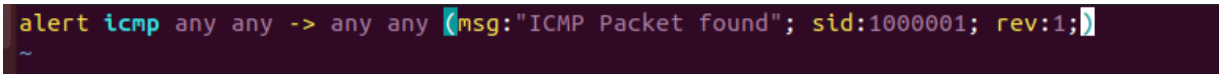
Next, we are going to add a simple snort rule. You should add your own rules at /etc/snort/rules/local.rules. Add the following line into the local.rules file

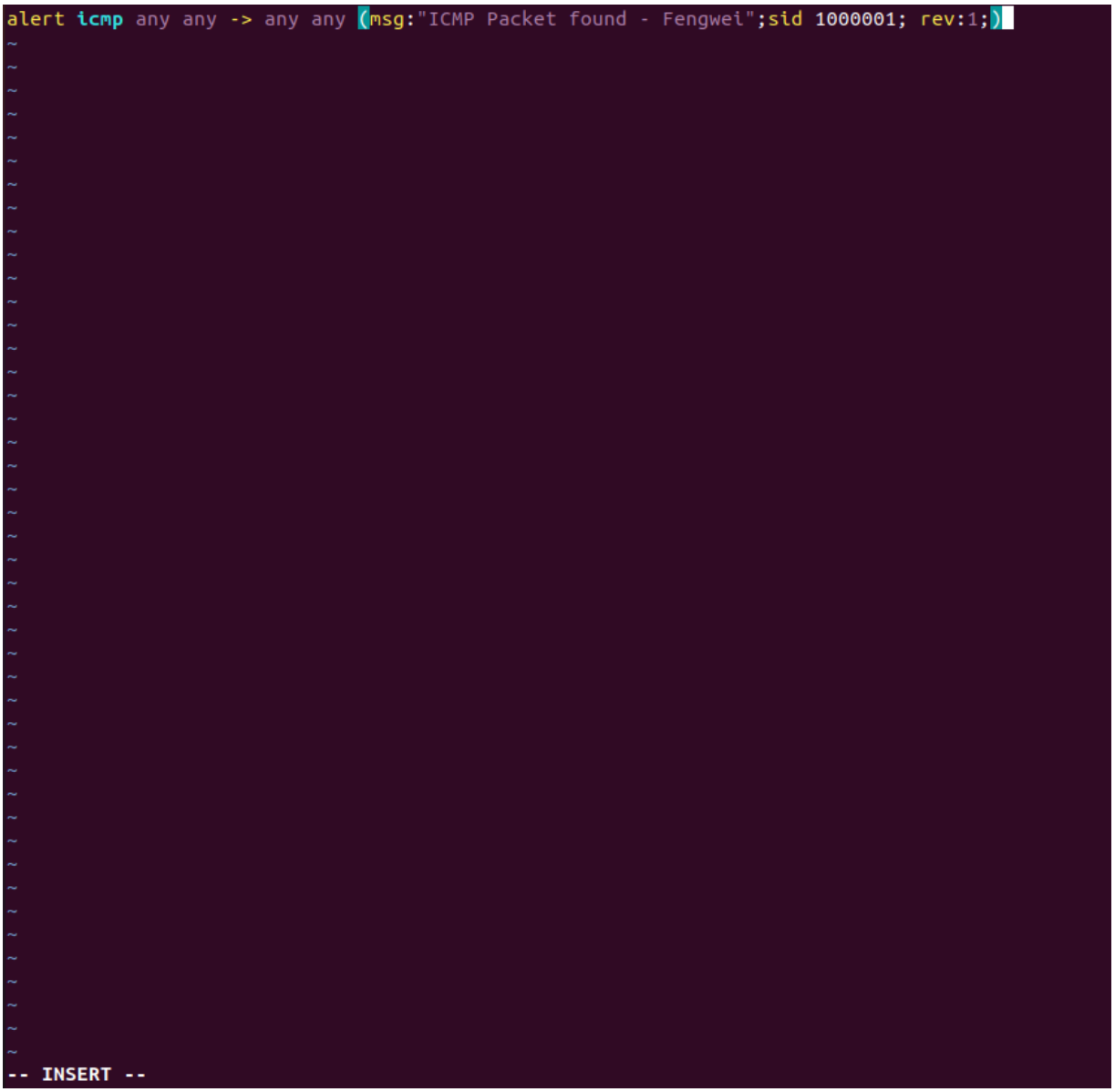
alert icmp any any -> any any (msg:"ICMP Packet found"; sid:1000001; rev:1;)

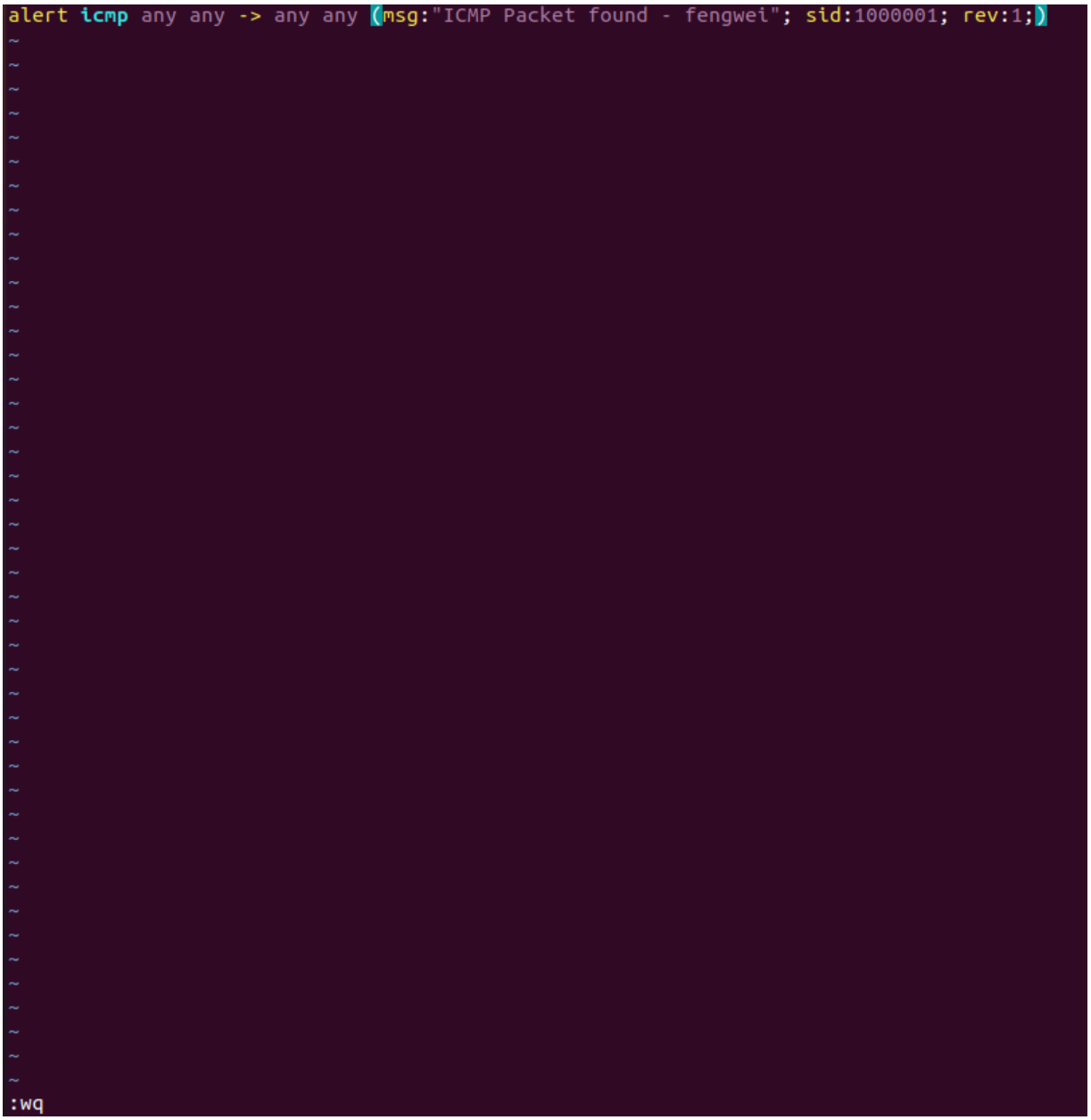
Basically, this rule defines that an alert will be logged if an ICMP packet is found. The ICMP packet could be from any IP address and the rule ID is 1000001. e.g. Make sure to pick a SID greater 1000000 for your own rules.

```
root@vishal-VirtualBox:/home/vishal# ls /etc/snort/rules/
attack-responses.rules          community-mail-client.rules    community-web-iis.rules    icmp.rules          pop2.rules          telnet.rules
backdoor.rules                  community-misc.rules           community-web-misc.rules   imap.rules          pop3.rules          tftp.rules
bad-traffic.rules               community-nntp.rules           community-web-php.rules    info.rules          porn.rules          virus.rules
chat.rules                      community-oracle.rules         ddos.rules                 local.rules         preproc_rules       web-attacks.rules
community-bot.rules             community-policy.rules         deleted.rules              misc.rules          rpc.rules           web-cgi.rules
community-deleted.rules         community-sip.rules            dns.rules                  multimedia.rules    rservices.rules     web-client.rules
community-dos.rules             community-smtp.rules           dos.rules                  mysql.rules         rules               web-coldfusion.rules
community-exploit.rules         community-sql-injection.rules  etc                        netbios.rules       scan.rules          web-frontpage.rules
community-ftp.rules             community-virus.rules          experimental.rules         nntp.rules          shellcode.rules     web-iis.rules
community-game.rules            community-web-attacks.rules    exploit.rules              oracle.rules        smtp.rules          web-misc.rules
community-icmp.rules            community-web-cgi.rules        finger.rules               other-ids.rules     snmp.rules          web-php.rules
community-imap.rules            community-web-client.rules     ftp.rules                  p2p.rules           so_rules            x11.rules
community-inappropriate.rules   community-web-dos.rules        icmp-info.rules            policy.rules        sql.rules
root@vishal-VirtualBox:/home/vishal# vim /etc/local.rules
```


"/etc/local.rules" [New File]
0,0-1
All


alert icmp any any -> any any (msg:"ICMP Packet found"; sid:1000001; rev:1;)
~


alert icmp any any -> any any (msg:"ICMP Packet found - Fengwei";sid 1000001; rev:1;)
-- INSERT --

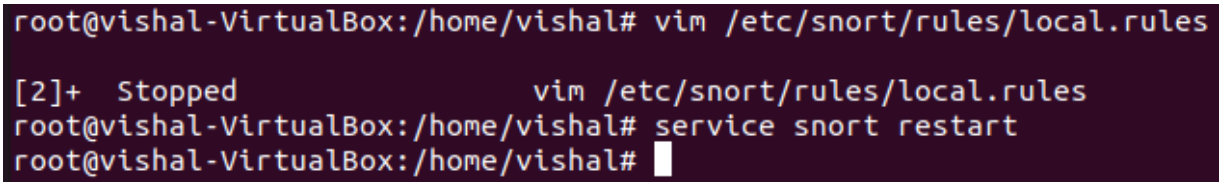


To make the rule become effective, you need to restart the snort service by typing the following command.

$ service snort restart

or

$ /etc/init.d/snort restart



```
# $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.
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"/etc/snort/rules/local.rules" 6L, 199C
```

```
# $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
alert icmp any any -> $HOME_Net any (msg:"ICMP Packet found"; sid :1000001; rev:1;)
~
~
~
~
~
```

```
root@vishal-VirtualBox:/home/vishal# service snort restart
```

Triggering an Alert for the New Rule

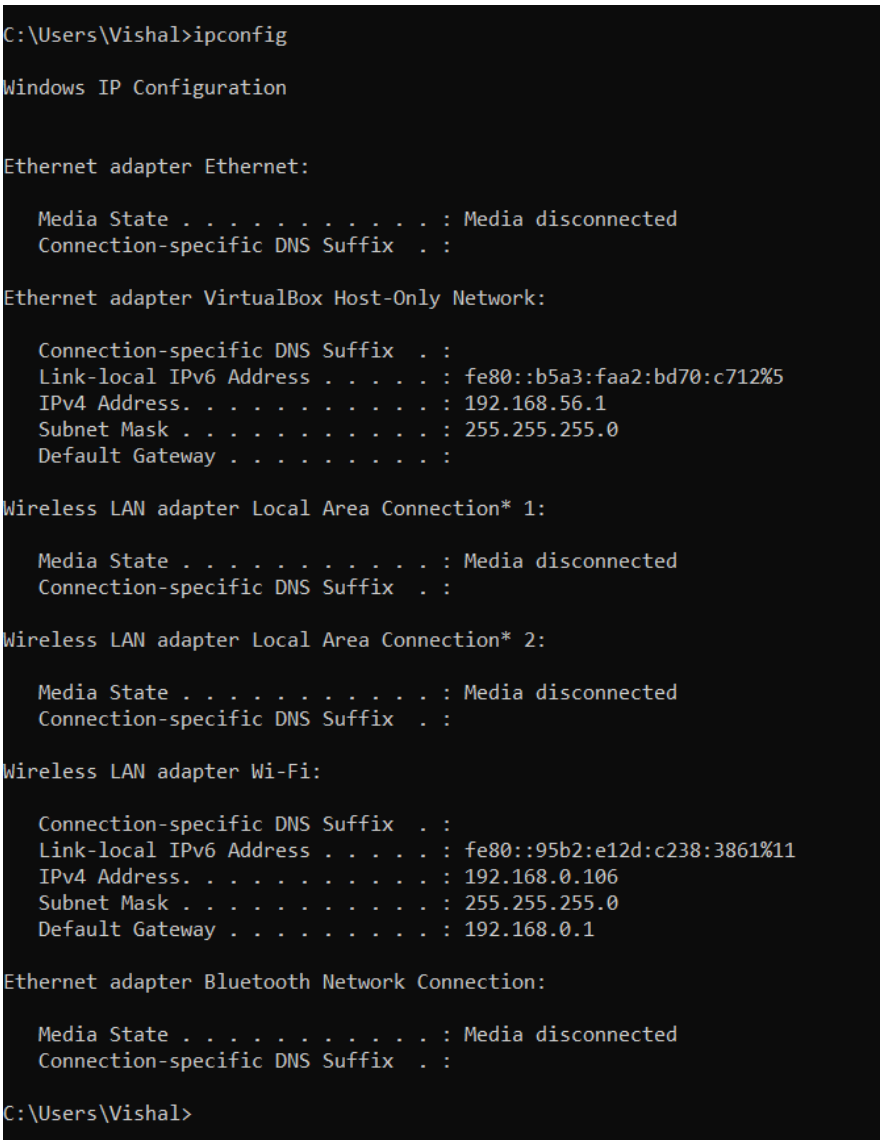
To trigger an alert for the new rule, you only need to send an ICMP message to the VM image where snort runs. First, you need to find the IP address of the VM by typing the following command.

$ ifconfig

```
vishal@vishal-VirtualBox:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.56.101  netmask 255.255.255.0  broadcast 192.168.56.255
        inet6 fe80::f0c2:3a24:f3c4:4331  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:f0:a8:07  txqueuelen 1000  (Ethernet)
        RX packets 1152  bytes 1046879 (1.0 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 735  bytes 85090 (85.0 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 393  bytes 33077 (33.0 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 393  bytes 33077 (33.0 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

vishal@vishal-VirtualBox:~$
```



For instance, the screenshot shows the execution result on my VM image, and the IP address is e.g. 172.16.108.242

After you have a terminal, you can just type the following command to send ping messages to the VM.

$ ping 172.16.108.242

After you send the ping messages, the alerts should be triggered and you can find the log messages in /var/log/snort/snort.log. However, the snort.log file will be binary format. You need to use a tool, called u2spewfoo, to read it. Observer terminal on screen with log where you can see that the SID is 1000001, and the alerts are generated by the ICMP messages.

```
C:\Users\Vishal>ping 192.168.56.101

Pinging 192.168.56.101 with 32 bytes of data:
Reply from 192.168.56.101: bytes=32 time<1ms TTL=64
Reply from 192.168.56.101: bytes=32 time<1ms TTL=64
Reply from 192.168.56.101: bytes=32 time<1ms TTL=64
Reply from 192.168.56.101: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.56.101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```
vishal@vishal-VirtualBox:~$ sudo su
root@vishal-VirtualBox:/home/vishal# sudo snort -A console -q -c /etc/snort/snort.conf -i enp0s3
03/16-13:14:32.821293  [**] [1:382:7] ICMP PING Windows [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.56.1 -> 192.168.56.101
03/16-13:14:32.821293  [**] [1:1000001:1] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.56.1 -> 192.168.56.101
03/16-13:14:32.821293  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.56.1 -> 192.168.56.101
03/16-13:14:32.821317  [**] [1:1000001:1] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.56.101 -> 192.168.56.1
03/16-13:14:32.821317  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.56.101 -> 192.168.56.1
03/16-13:14:33.824587  [**] [1:382:7] ICMP PING Windows [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.56.1 -> 192.168.56.101
03/16-13:14:33.824587  [**] [1:1000001:1] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.56.1 -> 192.168.56.101
03/16-13:14:33.824587  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.56.1 -> 192.168.56.101
03/16-13:14:33.824615  [**] [1:1000001:1] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.56.101 -> 192.168.56.1
03/16-13:14:33.824615  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.56.101 -> 192.168.56.1
03/16-13:14:34.829665  [**] [1:382:7] ICMP PING Windows [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.56.1 -> 192.168.56.101
03/16-13:14:34.829665  [**] [1:1000001:1] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.56.1 -> 192.168.56.101
03/16-13:14:34.829665  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.56.1 -> 192.168.56.101
03/16-13:14:34.829690  [**] [1:1000001:1] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.56.101 -> 192.168.56.1
03/16-13:14:34.829690  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.56.101 -> 192.168.56.1
03/16-13:14:35.834316  [**] [1:382:7] ICMP PING Windows [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.56.1 -> 192.168.56.101
03/16-13:14:35.834316  [**] [1:1000001:1] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.56.1 -> 192.168.56.101
03/16-13:14:35.834316  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.56.1 -> 192.168.56.101
03/16-13:14:35.834340  [**] [1:1000001:1] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.56.101 -> 192.168.56.1
03/16-13:14:35.834340  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.56.101 -> 192.168.56.1
```

```
root@vishal-VirtualBox:/home/vishal# sudo snort -A console -q -c /etc/snort/snort.conf -i enp0s3
03/16-13:21:48.916591  [**] [1:382:7] ICMP PING Windows [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.56.1 -> 192.168.56.101
03/16-13:21:48.916591  [**] [1:1000001:1] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.56.1 -> 192.168.56.101
03/16-13:21:48.916591  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.56.1 -> 192.168.56.101
03/16-13:21:48.916615  [**] [1:1000001:1] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.56.101 -> 192.168.56.1
03/16-13:21:48.916615  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.56.101 -> 192.168.56.1
03/16-13:21:49.919490  [**] [1:382:7] ICMP PING Windows [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.56.1 -> 192.168.56.101
03/16-13:21:49.919490  [**] [1:1000001:1] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.56.1 -> 192.168.56.101
03/16-13:21:49.919490  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.56.1 -> 192.168.56.101
03/16-13:21:49.919526  [**] [1:1000001:1] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.56.101 -> 192.168.56.1
03/16-13:21:49.919526  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.56.101 -> 192.168.56.1
03/16-13:21:50.925607  [**] [1:382:7] ICMP PING Windows [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.56.1 -> 192.168.56.101
03/16-13:21:50.925607  [**] [1:1000001:1] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.56.1 -> 192.168.56.101
03/16-13:21:50.925607  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.56.1 -> 192.168.56.101
03/16-13:21:50.925633  [**] [1:1000001:1] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.56.101 -> 192.168.56.1
03/16-13:21:50.925633  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.56.101 -> 192.168.56.1
03/16-13:21:51.931081  [**] [1:382:7] ICMP PING Windows [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.56.1 -> 192.168.56.101
03/16-13:21:51.931081  [**] [1:1000001:1] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.56.1 -> 192.168.56.101
03/16-13:21:51.931081  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.56.1 -> 192.168.56.101
03/16-13:21:51.931098  [**] [1:1000001:1] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.56.101 -> 192.168.56.1
03/16-13:21:51.931098  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.56.101 -> 192.168.56.1
03/16-13:21:51.996333  [**] [1:382:7] ICMP PING Windows [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.56.1 -> 192.168.56.101
03/16-13:21:51.996333  [**] [1:1000001:1] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.56.1 -> 192.168.56.101
03/16-13:21:51.996333  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.56.1 -> 192.168.56.101
03/16-13:21:51.996386  [**] [1:1000001:1] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.56.101 -> 192.168.56.1
03/16-13:21:51.996386  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.56.101 -> 192.168.56.1
03/16-13:21:53.002643  [**] [1:382:7] ICMP PING Windows [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.56.1 -> 192.168.56.101
03/16-13:21:53.002643  [**] [1:1000001:1] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.56.1 -> 192.168.56.101
03/16-13:21:53.002643  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.56.1 -> 192.168.56.101
03/16-13:21:53.002675  [**] [1:1000001:1] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.56.101 -> 192.168.56.1
03/16-13:21:53.002675  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.56.101 -> 192.168.56.1
03/16-13:21:54.008856  [**] [1:382:7] ICMP PING Windows [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.56.1 -> 192.168.56.101
03/16-13:21:54.008856  [**] [1:1000001:1] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.56.1 -> 192.168.56.101
03/16-13:21:54.008856  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.56.1 -> 192.168.56.101
03/16-13:21:54.008886  [**] [1:1000001:1] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.56.101 -> 192.168.56.1
03/16-13:21:54.008886  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.56.101 -> 192.168.56.1
03/16-13:21:55.016492  [**] [1:382:7] ICMP PING Windows [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.56.1 -> 192.168.56.101
03/16-13:21:55.016492  [**] [1:1000001:1] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.56.1 -> 192.168.56.101
03/16-13:21:55.016492  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.56.1 -> 192.168.56.101
03/16-13:21:55.016518  [**] [1:1000001:1] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.56.101 -> 192.168.56.1
03/16-13:21:55.016518  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.56.101 -> 192.168.56.1
```

Assignments for Lab 1

1.Read the lab instructions above and finish all the tasks.

2.Answer the questions and justify your answers. Simple yes or no answer will not get any credits.

a. What is a zero-day attack?

A zero-day vulnerability refers to a software vulnerability unknown to the manufacturer which if it comes to the notice of hackers can be successfully exploited by them. In other words, it is a security hole in a software which is discovered and exploited by the hacking community even before the developers (or the vendors) of the software become aware of it.

This type of security threat can prove extremely fatal since the software developers themselves are not aware of the security vulnerability being exploited and therefore it could be weeks or months before the appropriate patch or fix is released to remedy the security vulnerability. Enough time for the hacking community to wreak havoc.

It gets its name as '**zero-day**' vulnerability because the security vulnerability is 'yet-to-be-discovered' by the software manufacturer or vendor. (To be more precise, it's been 'zero days' since the security vulnerability was discovered. Therefore 'zero-day vulnerability!').

How to recognize it

Unfortunately recognizing zero-day exploits is not an easy task. But with the right kind of security software, you'll be better equipped to handle such attacks. Therefore, let's take a look at the factors you should focus on in order to successfully counter these zero-day exploits.

Here's a typical lifecycle of an attack utilizing zero days to compromise devices:

1. A vulnerability or new attack vector is discovered by a malware author.
2. The capability is weaponized and proven to work
3. The zero day is kept secret and utilized by cyber criminals.
4. The vulnerability is discovered by defenders.
5. The OS vendor or application vendor deliver a patch.
6. The zero day is no longer a zero day.

b. Can Snort catch zero-day network attacks? If not, why not? If yes, how?

No, snort cannot catch zero-day attack. As snort checks with the predefined rules for prevention of attacks and zero-day attacks are unknown to the developers, so without the rules it cannot be prevented.

c. Given a network that has 1 million connections daily where 0.1% (not 10%) are attacks. If the IDS has a true positive rate of 95%,and the probability thatan alarm is an attack is 95%. What is the false alarm rate?

No of attacks = 0.1% of 1000000 = 1000 attacks

No of benign events = 99.9% of 1000000 = 999000 events

IDS has a true positive rate of 95% means that out of 1000 attacks, only 950 will set of alarms.

Therefore, Number of true alarms = 950 alarms

Since 95% of the total alarms are attacks,

No of total alarms = (100 * 950) / 95 = 1000 alarms

No of false alarms = 1000 – 950 = 50 alarms.

Therefore, False Alarm Rate

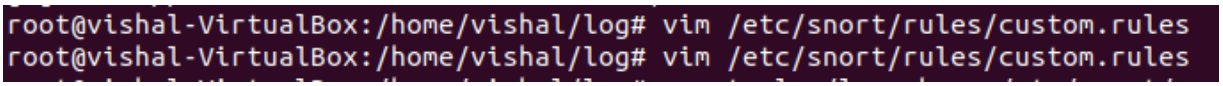
= (Number of false alarms / Total Benign Events) * 100

= (50 / 999000) * 100

= 0.005 %

3.Write and add another snort rule and show me you trigger it.

a. The rule you added (from the rules file)



```
alert tcp any any -> any any (msg:"Possible Neutrino exploit kit infection."; content:"vclphjybj.ioxbpjgtqvwqfzmwhn.ga"; classtype:trojan-activity; si
d:999995; rev:1)

-- INSERT --                                                                                      1,166          All
```

```
alert tcp any any -> any any (msg:"Possible Neutrino exploit kit infection."; content:"vclphjybj.ioxbpjgtqvwqfzmwhn.ga"; classtype:trojan-activity; si
d:999995; rev:1)

:wq
```

```
# $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
alert icmp any any -> $HOME_Net any (msg:"ICMP Packet found"; sid :1000001; rev:1;)
```

b. A description of how you triggered the alertc.The alert itself from the log file (after converting it to readable text)

Extra Credit (10pt):Write a rule that will fire when you browse to any site from the machine Snort is running on; it should look for any outbound TCP request to the site you have considered and alert on it.

```
vishal@vishal-VirtualBox:~$ sudo su
root@vishal-VirtualBox:/home/vishal# sudo snort -A console -q -c /etc/snort/snort.conf -i enp0s3
03/16-13:14:32.821293  [**] [1:382:7] ICMP PING Windows [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.56.1 -> 192.168.56.101
03/16-13:14:32.821293  [**] [1:1000001:1] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.56.1 -> 192.168.56.101
03/16-13:14:32.821293  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.56.1 -> 192.168.56.101
03/16-13:14:32.821317  [**] [1:1000001:1] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.56.101 -> 192.168.56.1
03/16-13:14:32.821317  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.56.101 -> 192.168.56.1
03/16-13:14:33.824587  [**] [1:382:7] ICMP PING Windows [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.56.1 -> 192.168.56.101
03/16-13:14:33.824587  [**] [1:1000001:1] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.56.1 -> 192.168.56.101
03/16-13:14:33.824587  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.56.1 -> 192.168.56.101
03/16-13:14:33.824615  [**] [1:1000001:1] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.56.101 -> 192.168.56.1
03/16-13:14:33.824615  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.56.101 -> 192.168.56.1
03/16-13:14:34.829665  [**] [1:382:7] ICMP PING Windows [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.56.1 -> 192.168.56.101
03/16-13:14:34.829665  [**] [1:1000001:1] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.56.1 -> 192.168.56.101
03/16-13:14:34.829665  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.56.1 -> 192.168.56.101
03/16-13:14:34.829690  [**] [1:1000001:1] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.56.101 -> 192.168.56.1
03/16-13:14:34.829690  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.56.101 -> 192.168.56.1
03/16-13:14:35.834316  [**] [1:382:7] ICMP PING Windows [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.56.1 -> 192.168.56.101
03/16-13:14:35.834316  [**] [1:1000001:1] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.56.1 -> 192.168.56.101
03/16-13:14:35.834316  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.56.1 -> 192.168.56.101
03/16-13:14:35.834340  [**] [1:1000001:1] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.56.101 -> 192.168.56.1
03/16-13:14:35.834340  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.56.101 -> 192.168.56.1
```

```
root@vishal-VirtualBox:/home/vishal# sudo snort -A console -q -c /etc/snort/snort.conf -i enp0s3
03/16-13:21:48.916591  [**] [1:382:7] ICMP PING Windows [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.56.1 -> 192.168.56.101
03/16-13:21:48.916591  [**] [1:1000001:1] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.56.1 -> 192.168.56.101
03/16-13:21:48.916591  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.56.1 -> 192.168.56.101
03/16-13:21:48.916615  [**] [1:1000001:1] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.56.101 -> 192.168.56.1
03/16-13:21:48.916615  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.56.101 -> 192.168.56.1
03/16-13:21:49.919490  [**] [1:382:7] ICMP PING Windows [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.56.1 -> 192.168.56.101
03/16-13:21:49.919490  [**] [1:1000001:1] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.56.1 -> 192.168.56.101
03/16-13:21:49.919490  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.56.1 -> 192.168.56.101
03/16-13:21:49.919526  [**] [1:1000001:1] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.56.101 -> 192.168.56.1
03/16-13:21:49.919526  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.56.101 -> 192.168.56.1
03/16-13:21:50.925607  [**] [1:382:7] ICMP PING Windows [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.56.1 -> 192.168.56.101
03/16-13:21:50.925607  [**] [1:1000001:1] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.56.1 -> 192.168.56.101
03/16-13:21:50.925607  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.56.1 -> 192.168.56.101
03/16-13:21:50.925633  [**] [1:1000001:1] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.56.101 -> 192.168.56.1
03/16-13:21:50.925633  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.56.101 -> 192.168.56.1
03/16-13:21:51.931081  [**] [1:382:7] ICMP PING Windows [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.56.1 -> 192.168.56.101
03/16-13:21:51.931081  [**] [1:1000001:1] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.56.1 -> 192.168.56.101
03/16-13:21:51.931081  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.56.1 -> 192.168.56.101
03/16-13:21:51.931098  [**] [1:1000001:1] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.56.101 -> 192.168.56.1
03/16-13:21:51.931098  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.56.101 -> 192.168.56.1
03/16-13:21:51.996333  [**] [1:382:7] ICMP PING Windows [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.56.1 -> 192.168.56.101
03/16-13:21:51.996333  [**] [1:1000001:1] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.56.1 -> 192.168.56.101
03/16-13:21:51.996333  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.56.1 -> 192.168.56.101
03/16-13:21:51.996386  [**] [1:1000001:1] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.56.101 -> 192.168.56.1
03/16-13:21:51.996386  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.56.101 -> 192.168.56.1
03/16-13:21:53.002643  [**] [1:382:7] ICMP PING Windows [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.56.1 -> 192.168.56.101
03/16-13:21:53.002643  [**] [1:1000001:1] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.56.1 -> 192.168.56.101
03/16-13:21:53.002643  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.56.1 -> 192.168.56.101
03/16-13:21:53.002675  [**] [1:1000001:1] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.56.101 -> 192.168.56.1
03/16-13:21:53.002675  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.56.101 -> 192.168.56.1
03/16-13:21:54.008856  [**] [1:382:7] ICMP PING Windows [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.56.1 -> 192.168.56.101
03/16-13:21:54.008856  [**] [1:1000001:1] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.56.1 -> 192.168.56.101
03/16-13:21:54.008856  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.56.1 -> 192.168.56.101
03/16-13:21:54.008886  [**] [1:1000001:1] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.56.101 -> 192.168.56.1
03/16-13:21:54.008886  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.56.101 -> 192.168.56.1
03/16-13:21:55.016492  [**] [1:382:7] ICMP PING Windows [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.56.1 -> 192.168.56.101
03/16-13:21:55.016492  [**] [1:1000001:1] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.56.1 -> 192.168.56.101
03/16-13:21:55.016492  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.56.1 -> 192.168.56.101
03/16-13:21:55.016518  [**] [1:1000001:1] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.56.101 -> 192.168.56.1
03/16-13:21:55.016518  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.56.101 -> 192.168.56.1
```

Conclusion:

1. Snort has the capability to detect unusual incoming packet traffic in a network. To analyze intruder or malicious activity, it is foremost in understanding the malicious pattern. The malicious pattern is a basic information to generate Snort rules.
2. Snort detection is based on the Snort rules, which matched with the Snort rules in the database. Snort rules is a simple rule and easy to understand because most of Snort rules write on single line and describes about basic structure of rule.