Name: Aartee chimate
UID:2018140012
Branch:IT
Sub:CSS

Experiment-6

```
aartee@aartee: ~
aartee@aartee:~$ apt show snort
Package: snort
Version: 2.9.7.0-5build1
Priority: optional
Section: universe/net
Origin: Ubuntu
Maintainer: Ubuntu Developers <ubuntu-devel-discuss@lists.ubuntu.com>
Original-Maintainer: Javier Fernández-Sanguino Peña <jfs@debian.org>
Bugs: https://bugs.launchpad.net/ubuntu/+filebug
Installed-Size: 1,987 kB
Pre-Depends: adduser (>= 3.11)
Depends: snort-common-libraries (>= 2.9.7.0-5build1), snort-rules-default (>= 2.
9.7.0-5build1), snort-common (>= 2.9.7.0-5build1), debconf (>= 0.5) | debconf-2.
0, rsyslog | system-log-daemon, logrotate, net-tools, libc6 (>= 2.16), libdaq2,
libdumbnet1 (>= 1.8), liblzma5 (>= 5.1.1alpha+20120614), libpcap0.8 (>= 1.0.0),
libpcre3, zlib1g (>= 1:1.1.4)
Recommends: iproute2
Suggests: snort-doc
Conflicts: snort-mysql, snort-pgsql
Replaces: snort-common (<< 2.0.2-3)
Homepage: http://www.snort.org/
Download-Size: 656 kB
APT-Manual-Installed: yes
APT-Sources: http://in.archive.ubuntu.com/ubuntu focal/universe amd64 Packages
```

```
aartee@aartee: ~
APT-Sources: http://in.archive.ubuntu.com/ubuntu focal/universe amd64 Packages
Description: flexible Network Intrusion Detection System
 Snort is a libpcap-based packet sniffer/logger which can be used as a
 lightweight network intrusion detection system. It features rules-based
 logging and can perform content searching/matching in addition to
 detecting a variety of other attacks and probes, such as buffer
 overflows, stealth port scans, CGI attacks, SMB probes, and much more.
 Snort has a real-time alerting capability, with alerts being sent to
 syslog, a separate "alert" file, or even to a Windows computer via Samba.
 .
 This package provides the plain-vanilla version of Snort.

aartee@aartee:~$ Sudo apt update

Command 'Sudo' not found, did you mean:

  command 'ludo' from snap ludo (0.15.5)
  command 'udo' from deb udo (6.4.1-5)
  command 'sudo' from deb sudo (1.8.31-1ubuntu1.2)
  command 'sudo' from deb sudo-ldap (1.8.31-1ubuntu1.2)

See 'snap info <snapname>' for additional versions.

aartee@aartee:~$
```

aartee@aartee: ~

```
See 'snap info <snapname>' for additional versions.

aartee@aartee:~$ sudo apt update
[sudo] password for aartee:
Hit:1 http://in.archive.ubuntu.com/ubuntu focal InRelease
Get:2 http://in.archive.ubuntu.com/ubuntu focal-updates InRelease [114 kB]
Get:3 http://in.archive.ubuntu.com/ubuntu focal-backports InRelease [108 kB]
Hit:4 http://ppa.launchpad.net/stefansundin/truecrypt/ubuntu focal InRelease
Get:5 http://security.ubuntu.com/ubuntu focal-security InRelease [114 kB]
Get:6 http://in.archive.ubuntu.com/ubuntu focal-updates/main i386 Packages [571
kB]
Get:7 http://in.archive.ubuntu.com/ubuntu focal-updates/main amd64 Packages [1,3
88 kB]
Get:8 http://in.archive.ubuntu.com/ubuntu focal-updates/main Translation-en [281
 kB]
Get:9 http://in.archive.ubuntu.com/ubuntu focal-updates/main amd64 DEP-11 Metada
ta [278 kB]
Get:10 http://in.archive.ubuntu.com/ubuntu focal-updates/universe amd64 DEP-11 M
etadata [361 kB]
Get:11 http://in.archive.ubuntu.com/ubuntu focal-updates/universe DEP-11 64x64 I
cons [389 kB]
Get:12 http://in.archive.ubuntu.com/ubuntu focal-updates/multiverse amd64 DEP-11
 Metadata [940 B]
Get:13 http://in.archive.ubuntu.com/ubuntu focal-backports/main amd64 DEP-11 Met
```

aartee@aartee: ~/snort-source-files/gperftools-2.8

```
aartee@aartee:~/snort-source-files/libdaq$ ./bootstrap
+ autoreconf -ivf --warnings=all
autoreconf: Entering directory `.'
autoreconf: configure.ac: not using Gettext
autoreconf: running: aclocal -I m4 --output=aclocal.m4t
Can't exec "aclocal": No such file or directory at /usr/share/autoconf/Autom4te/
FileUtils.pm line 326.
autoreconf: failed to run aclocal: No such file or directory
aartee@aartee:~/snort-source-files/libdaq$ ./configure
bash: ./configure: No such file or directory
aartee@aartee:~/snort-source-files/libdaq$ make
make: *** No targets specified and no makefile found.  Stop.
aartee@aartee:~/snort-source-files/libdaq$ sudo make install
[sudo] password for aartee:
make: *** No rule to make target 'install'.  Stop.
aartee@aartee:~/snort-source-files/libdaq$ cd ../
aartee@aartee:~/snort-source-files$ wget https://github.com/gperftools/gperftool
s/releases/download/gperftools-2.8/gperftools-2.8.tar.gz
--2021-12-06 19:54:32--  https://github.com/gperftools/gperftools/releases/downl
oad/gperftools-2.8/gperftools-2.8.tar.gz
Resolving github.com (github.com)... 13.234.210.38
Connecting to github.com (github.com)|13.234.210.38|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://objects.githubusercontent.com/github-production-release-asset-
```

aartee@aartee: ~/snort-source-files/gperftools-2.8

```
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 libr
aries... 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 how to run the C++ preprocessor... g++ -std=gnu++11 -E
checking for ld used by g++ -std=gnu++11... /usr/bin/ld -m elf_x86_64
checking if the linker (/usr/bin/ld -m elf_x86_64) is GNU ld... yes
checking whether the g++ -std=gnu++11 linker (/usr/bin/ld -m elf_x86_64) support
s shared libraries... yes
checking for g++ -std=gnu++11 option to produce PIC... -fPIC -DPIC
checking if g++ -std=gnu++11 PIC flag -fPIC -DPIC works... yes
checking if g++ -std=gnu++11 static flag -static works... yes
checking if g++ -std=gnu++11 supports -c -o file.o... yes
checking if g++ -std=gnu++11 supports -c -o file.o... (cached) yes
checking whether the g++ -std=gnu++11 linker (/usr/bin/ld -m elf_x86_64) support
s shared libraries... yes
checking dynamic linker characteristics... (cached) GNU/Linux ld.so
```

aartee@aartee: ~/snort-source-files/gperftools-2.8

```
checking execinfo.h usability... yes
checking execinfo.h presence... yes
checking for execinfo.h... yes
checking unwind.h usability... yes
checking unwind.h presence... yes
checking for unwind.h... yes
checking sched.h usability... yes
checking sched.h presence... yes
checking for sched.h... yes
checking conflict-signal.h usability... no
checking conflict-signal.h presence... no
checking for conflict-signal.h... no
checking sys/prctl.h usability... yes
checking sys/prctl.h presence... yes
checking for sys/prctl.h... yes
checking linux/ptrace.h usability... yes
checking linux/ptrace.h presence... yes
checking for linux/ptrace.h... yes
checking sys/syscall.h usability... yes
checking sys/syscall.h presence... yes
checking for sys/syscall.h... yes
checking sys/socket.h usability... yes
checking sys/socket.h presence... yes
checking for sys/socket.h... yes
```

aartee@aartee: ~/snort-source-files/gperftools-2.8

```
ibtcmalloc_internal_la-system-alloc.lo -MD -MP -MF src/.deps/libtcmalloc_interna
l_la-system-alloc.Tpo -c src/system-alloc.cc  -fPIC -DPIC -o src/.libs/libtcmall
oc_internal_la-system-alloc.o
libtool: compile:  g++ -std=gnu++11 -DHAVE_CONFIG_H -I. -I./src -I./src -pthread
 -DNDEBUG -Wall -Wwrite-strings -Woverloaded-virtual -Wno-sign-compare -Wno-unus
ed-result -fsized-deallocation -faligned-new -DNO_FRAME_POINTER -g -O2 -MT src/l
ibtcmalloc_internal_la-system-alloc.lo -MD -MP -MF src/.deps/libtcmalloc_interna
l_la-system-alloc.Tpo -c src/system-alloc.cc -o src/libtcmalloc_internal_la-syst
em-alloc.o >/dev/null 2>&1
mv -f src/.deps/libtcmalloc_internal_la-system-alloc.Tpo src/.deps/libtcmalloc_i
nternal_la-system-alloc.Plo
/bin/bash ./libtool  --tag=CXX   --mode=compile g++ -std=gnu++11 -DHAVE_CONFIG_H
 -I. -I./src  -I./src   -pthread -DNDEBUG -Wall -Wwrite-strings -Woverloaded-vir
tual -Wno-sign-compare  -Wno-unused-result -fsized-deallocation -faligned-new  -
DNO_FRAME_POINTER   -g -O2 -MT src/libtcmalloc_internal_la-memfs_malloc.lo -MD -
MP -MF src/.deps/libtcmalloc_internal_la-memfs_malloc.Tpo -c -o src/libtcmalloc_
internal_la-memfs_malloc.lo `test -f 'src/memfs_malloc.cc' || echo './'`src/memf
s_malloc.cc
libtool: compile:  g++ -std=gnu++11 -DHAVE_CONFIG_H -I. -I./src -I./src -pthread
 -DNDEBUG -Wall -Wwrite-strings -Woverloaded-virtual -Wno-sign-compare -Wno-unus
ed-result -fsized-deallocation -faligned-new -DNO_FRAME_POINTER -g -O2 -MT src/l
ibtcmalloc_internal_la-memfs_malloc.lo -MD -MP -MF src/.deps/libtcmalloc_interna
l_la-memfs_malloc.Tpo -c src/memfs_malloc.cc  -fPIC -DPIC -o src/.libs/libtcmall
oc_internal_la-memfs_malloc.o
```

aartee@aartee: ~/snort-source-files/gperftools-2.8

```
a-page_heap.Tpo -c src/page_heap.cc  -fPIC -DPIC -o src/.libs/libtcmalloc_intern
al_la-page_heap.o
libtool: compile:  g++ -std=gnu++11 -DHAVE_CONFIG_H -I. -I./src -I./src -pthread
 -DNDEBUG -Wall -Wwrite-strings -Woverloaded-virtual -Wno-sign-compare -Wno-unus
ed-result -fsized-deallocation -faligned-new -DNO_FRAME_POINTER -g -O2 -MT src/l
ibtcmalloc_internal_la-page_heap.lo -MD -MP -MF src/.deps/libtcmalloc_internal_l
a-page_heap.Tpo -c src/page_heap.cc -o src/libtcmalloc_internal_la-page_heap.o >
/dev/null 2>&1
mv -f src/.deps/libtcmalloc_internal_la-page_heap.Tpo src/.deps/libtcmalloc_inte
rnal_la-page_heap.Plo
/bin/bash ./libtool  --tag=CXX   --mode=compile g++ -std=gnu++11 -DHAVE_CONFIG_H
 -I. -I./src  -I./src   -pthread -DNDEBUG -Wall -Wwrite-strings -Woverloaded-vir
tual -Wno-sign-compare  -Wno-unused-result -fsized-deallocation -faligned-new  -
DNO_FRAME_POINTER   -g -O2 -MT src/libtcmalloc_internal_la-sampler.lo -MD -MP -M
F src/.deps/libtcmalloc_internal_la-sampler.Tpo -c -o src/libtcmalloc_internal_l
a-sampler.lo `test -f 'src/sampler.cc' || echo './'`src/sampler.cc
libtool: compile:  g++ -std=gnu++11 -DHAVE_CONFIG_H -I. -I./src -I./src -pthread
 -DNDEBUG -Wall -Wwrite-strings -Woverloaded-virtual -Wno-sign-compare -Wno-unus
ed-result -fsized-deallocation -faligned-new -DNO_FRAME_POINTER -g -O2 -MT src/l
ibtcmalloc_internal_la-sampler.lo -MD -MP -MF src/.deps/libtcmalloc_internal_la-
sampler.Tpo -c src/sampler.cc  -fPIC -DPIC -o src/.libs/libtcmalloc_internal_la-
sampler.o
libtool: compile:  g++ -std=gnu++11 -DHAVE_CONFIG_H -I. -I./src -I./src -pthread
 -DNDEBUG -Wall -Wwrite-strings -Woverloaded-virtual -Wno-sign-compare -Wno-unus
```

aartee@aartee: ~/snort-source-files/gperftools-2.8

```
tcmalloc_debug.la libtcmalloc_and_profiler.la; do lib=".libs/`basename $la .la`.
a"; [ ! -f "$lib" ] || : "$lib"; done
aartee@aartee:~/snort-source-files/gperftools-2.8$ sudo make install
rm -f debugallocation_test.sh
cp -p ./src/tests/debugallocation_test.sh debugallocation_test.sh
rm -f tcmalloc_unittest.sh
cp -p ./src/tests/tcmalloc_unittest.sh tcmalloc_unittest.sh
rm -f sampling_test.sh
cp -p ./src/tests/sampling_test.sh sampling_test.sh
rm -f heap-profiler_unittest.sh
cp -p ./src/tests/heap-profiler_unittest.sh heap-profiler_unittest.sh
rm -f heap-checker_unittest.sh
cp -p ./src/tests/heap-checker_unittest.sh heap-checker_unittest.sh
rm -f heap-checker-death_unittest.sh
cp -p ./src/tests/heap-checker-death_unittest.sh heap-checker-death_unittest.sh
rm -f sampling_debug_test.sh
cp -p ./src/tests/sampling_test.sh sampling_debug_test.sh
rm -f heap-profiler_debug_unittest.sh
cp -p ./src/tests/heap-profiler_unittest.sh heap-profiler_debug_unittest.sh
rm -f heap-checker_debug_unittest.sh
cp -p ./src/tests/heap-checker_unittest.sh heap-checker_debug_unittest.sh
rm -f profiler_unittest.sh
cp -p ./src/tests/profiler_unittest.sh profiler_unittest.sh
for la in libtcmalloc_minimal.la libtcmalloc_minimal_debug.la libtcmalloc.la lib
```

```
aartee@aartee: ~/snort-source-files/gperftools-2.8
rofile.html docs/cpuprofile-fileformat.html docs/pprof-test-big.gif docs/pprof-t
est.gif docs/pprof-vsnprintf-big.gif docs/pprof-vsnprintf.gif '/usr/local/share/
doc/gperftools'
 /usr/bin/mkdir -p '/usr/local/include/google'
 /usr/bin/install -c -m 644 src/google/heap-checker.h src/google/heap-profiler.h
 src/google/malloc_extension.h src/google/malloc_extension_c.h src/google/malloc
_hook.h src/google/malloc_hook_c.h src/google/profiler.h src/google/stacktrace.h
 src/google/tcmalloc.h '/usr/local/include/google'
 /usr/bin/mkdir -p '/usr/local/share/man/man1'
 /usr/bin/install -c -m 644 docs/pprof.1 '/usr/local/share/man/man1'
 /usr/bin/mkdir -p '/usr/local/include/gperftools'
 /usr/bin/install -c -m 644 src/gperftools/tcmalloc.h '/usr/local/include/gperft
ools'
 /usr/bin/mkdir -p '/usr/local/include/gperftools'
 /usr/bin/install -c -m 644 src/gperftools/stacktrace.h src/gperftools/malloc_ho
ok.h src/gperftools/malloc_hook_c.h src/gperftools/malloc_extension.h src/gperft
ools/malloc_extension_c.h src/gperftools/nallocx.h src/gperftools/heap-profiler.
h src/gperftools/heap-checker.h src/gperftools/profiler.h '/usr/local/include/gp
erftools'
 /usr/bin/mkdir -p '/usr/local/lib/pkgconfig'
 /usr/bin/install -c -m 644 libtcmalloc.pc libtcmalloc_minimal.pc libtcmalloc_de
bug.pc libtcmalloc_minimal_debug.pc libprofiler.pc '/usr/local/lib/pkgconfig'
make[1]: Leaving directory '/home/aartee/snort-source-files/gperftools-2.8'
aartee@aartee:~/snort-source-files/gperftools-2.8$
```

```
aartee@aartee: ~/snort-source-files/snort3
aartee@aartee:~/snort-source-files/snort3$ sudo install CMake
install: missing destination file operand after 'CMake'
Try 'install --help' for more information.
aartee@aartee:~/snort-source-files/snort3$  cmake .

Command 'cmake' not found, but can be installed with:

sudo snap install cmake  # version 3.22.0, or
sudo apt  install cmake  # version 3.16.3-1ubuntu1

See 'snap info cmake' for additional versions.

aartee@aartee:~/snort-source-files/snort3$ sudo apt  install cmake
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  chromium-codecs-ffmpeg-extra gstreamer1.0-vaapi
  libgstreamer-plugins-bad1.0-0 libva-wayland2
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  cmake-data libjsoncpp1 librhash0
Suggested packages:
  cmake-doc ninja-build
```

```
aartee@aartee: ~/snort-source-files/snort3
aartee@aartee:~/snort-source-files/snort3$ sudo idconfig
[sudo] password for aartee:
sudo: idconfig: command not found
aartee@aartee:~/snort-source-files/snort3$ sudo ldconfig
aartee@aartee:~/snort-source-files/snort3$ snort -V

   ,,_     -*> 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

aartee@aartee:~/snort-source-files/snort3$ ip address show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gr
```

```
aartee@aartee: ~/snort-source-files/snort3
  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

aartee@aartee:~/snort-source-files/snort3$ ip address show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gr
oup default qlen 1000
    link/ether 08:00:27:c3:cd:ee brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
       valid_lft 81265sec preferred_lft 81265sec
    inet6 fe80::5a0a:4be5:bd8d:5075/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
aartee@aartee:~/snort-source-files/snort3$ ip link set dev ens33 promisc on
```

```
aartee@aartee: ~/snort-source-files/snort3
  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

aartee@aartee:~/snort-source-files/snort3$ ip address show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gr
oup default qlen 1000
    link/ether 08:00:27:c3:cd:ee brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
       valid_lft 81265sec preferred_lft 81265sec
    inet6 fe80::5a0a:4be5:bd8d:5075/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
aartee@aartee:~/snort-source-files/snort3$ ip link set dev ens33 promisc on
```

```
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required:
  libfprint-2-tod1
Use 'sudo apt autoremove' to remove it.
The following NEW packages will be installed:
  ethtool
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 134 kB of archives.
After this operation, 461 kB of additional disk space will be used.
Get:1 http://us.archive.ubuntu.com/ubuntu focal/main amd64 ethtool amd64 1:5.4-1 [134 kB]
Fetched 134 kB in 2s (82.5 kB/s)
Selecting previously unselected package ethtool.
(Reading database ... 190939 files and directories currently installed.)
Preparing to unpack .../ethtool_1%3a5.4-1_amd64.deb ...
Unpacking ethtool (1:5.4-1) ...
Setting up ethtool (1:5.4-1) ...
Processing triggers for man-db (2.9.1-1) ...
```

```
nort3-community-rules.tar.gz
--2020-09-02 07:04:05--  https://www.snort.org/downloads/community/snort3-community-rules.tar.gz
Resolving www.snort.org (www.snort.org)... 104.18.139.9, 104.18.138.9, 2606:4700::6812:8a09, ...
Connecting to www.snort.org (www.snort.org)|104.18.139.9|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://snort-org-site.s3.amazonaws.com/production/release_files/files/000/014/845/ori
ginal/snort3-community-rules.tar.gz?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIXACIE
D2SPMSC7GA%2F20200902%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20200902T140406Z&X-Amz-Expires=
3600&X-Amz-SignedHeaders=host&X-Amz-Signature=ddf485fad50f8d318f622ede1042e2f0893bd14852db20a9dd
5cca01cbba910f [following]
--2020-09-02 07:04:07--  https://snort-org-site.s3.amazonaws.com/production/release_files/files/
000/014/845/original/snort3-community-rules.tar.gz?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Creden
tial=AKIAIXACIED2SPMSC7GA%2F20200902%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20200902T140406Z
&X-Amz-Expires=3600&X-Amz-SignedHeaders=host&X-Amz-Signature=ddf485fad50f8d318f622ede1042e2f0893
bd14852db20a9dd5cca01cbba910f
Resolving snort-org-site.s3.amazonaws.com (snort-org-site.s3.amazonaws.com)... 52.217.37.156
Connecting to snort-org-site.s3.amazonaws.com (snort-org-site.s3.amazonaws.com)|52.217.37.156|:4
43... connected.
HTTP request sent, awaiting response... 200 OK
Length: 277050 (271K) [application/gzip]
Saving to: ‘snort3-community-rules.tar.gz’

snort3-community-rules. 100%[===============================>] 270.56K   274KB/s    in 1.0s

2020-09-02 07:04:09 (274 KB/s) - ‘snort3-community-rules.tar.gz’ saved [277050/277050]
```

```
-- 4. configure performance
-- 5. configure detection
-- 6. configure filters
-- 7. configure outputs
-- 8. configure tweaks

------------------------------------------------------------------------------
-- 1. configure defaults
------------------------------------------------------------------------------

-- HOME_NET and EXTERNAL_NET must be set now
-- setup the network addresses you are protecting
HOME_NET = '10.0.2.15/24'

-- set up the external network addresses.
-- (leave as "any" in most situations)
EXTERNAL_NET = 'any'
EXTERNAL_NET = '!$HOME_NET'

include 'snort_defaults.lua'
include 'file_magic.lua'

------------------------------------------------------------------------------
:x
```

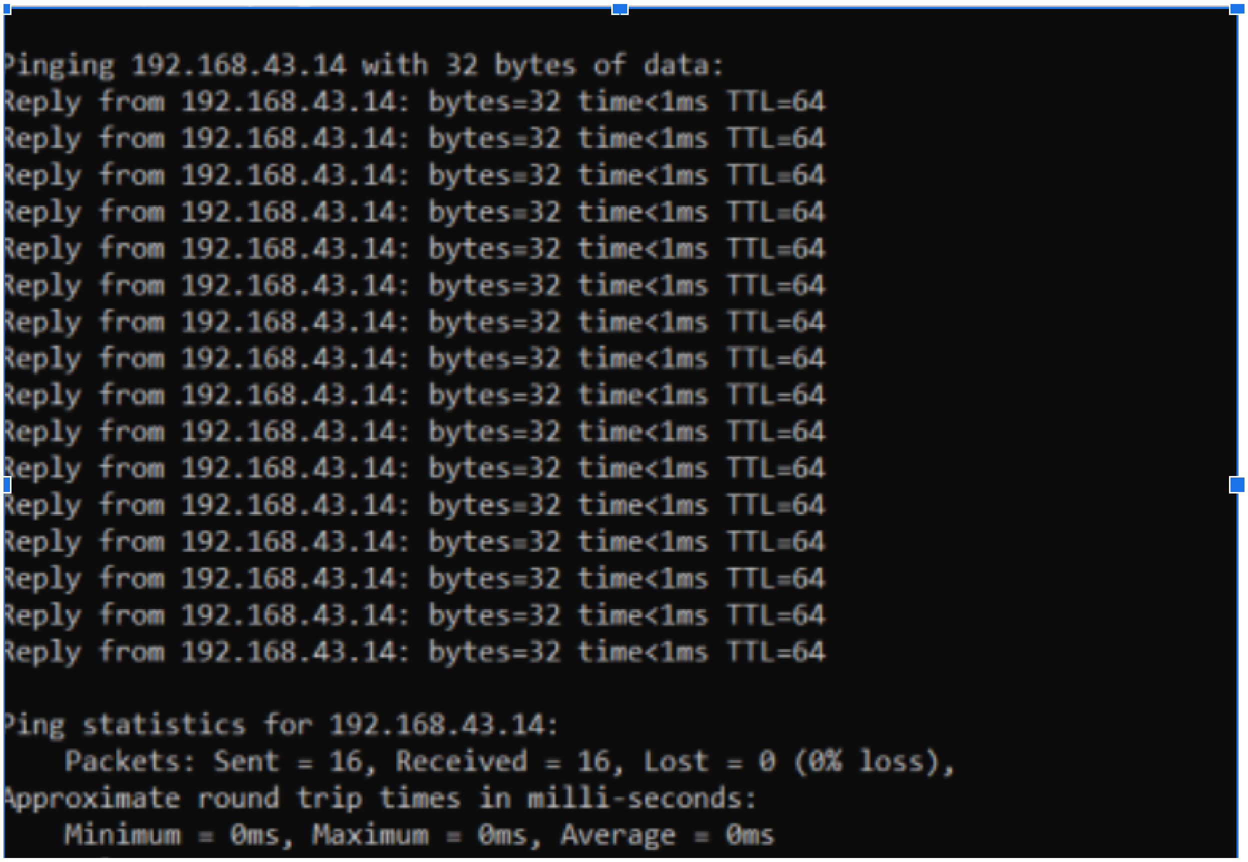
```
default_gtp =
{
    { version = 0, messages = gtp_v0_msg, infos = gtp_v0_info },
    { version = 1, messages = gtp_v1_msg, infos = gtp_v1_info },
    { version = 2, messages = gtp_v2_msg, infos = gtp_v2_info },
}


ips =
{
    -- use this to enable decoder and inspector alerts
    --enable_builtin_rules = true,

    -- use include for rules files; be sure to set your path
    -- note that rules files can include other rules files
    include = '/usr/local/etc/rules/snort3-community-rules/snort3-community.rules'
}

--------------------------------------------------------------------------------
```

```
rt/snort.lua
--------------------------------------------------
o")~   Snort++ 3.1.17.0
--------------------------------------------------
Loading /usr/local/etc/snort/snort.lua:
Loading snort_defaults.lua:
Finished snort_defaults.lua:
Loading file_magic.lua:
Finished file_magic.lua:
        ips
        ssh
        hosts
        host_cache
        pop
        so_proxy
        stream_tcp
        smtp
        gtp_inspect
        packets
        dce_http_proxy
        stream_icmp
        stream_file
Finished /usr/local/etc/snort/snort.lua:
--------------------------------------------------
pcap DAQ configured to passive.

Snort successfully validated the configuration (with 0 warnings).
o")~   Snort exiting
```

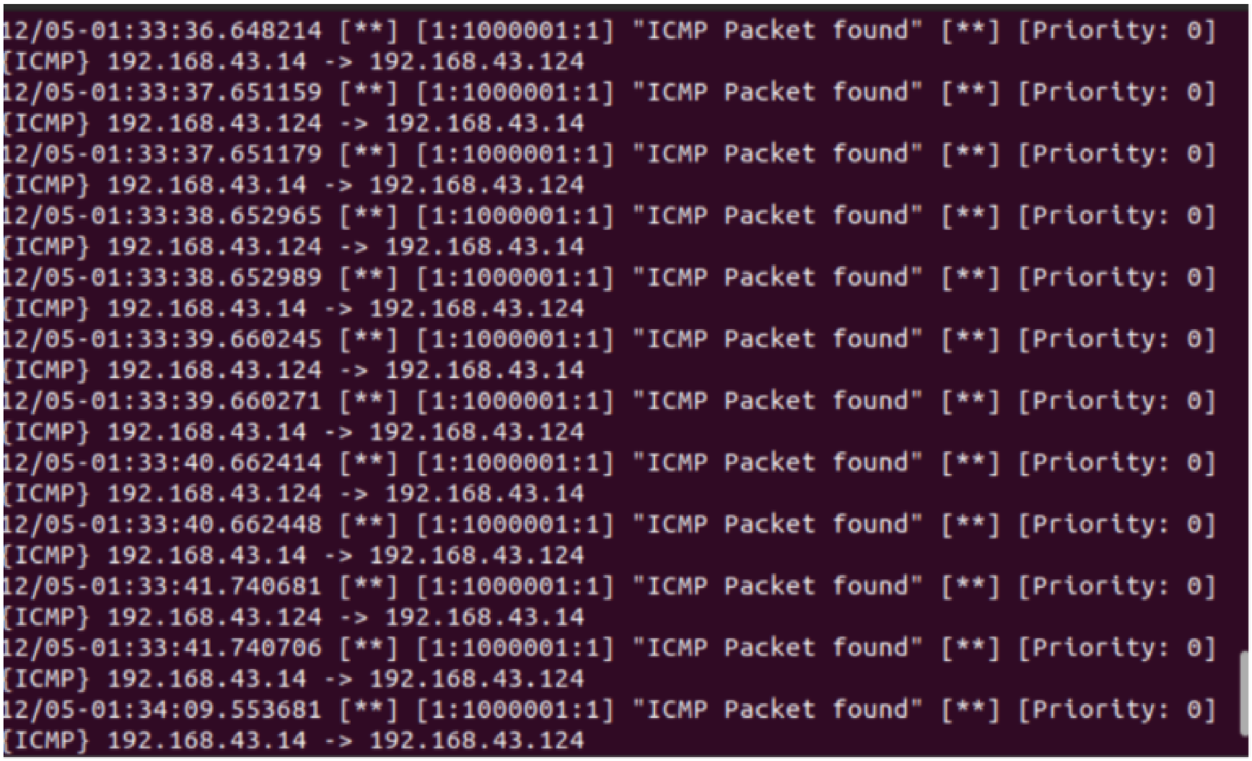
```
alert icmp any any -> $HOME_NET any (msg:"ICMP Packet found"; sid:1000001; rev:1;)
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
:x
```

```
Loading /usr/local/etc/rules/local.rules:
Finished /usr/local/etc/rules/local.rules:
Finished rule args:
--------------------------------------------------
rule counts
       total rules loaded: 1
               text rules: 1
            option chains: 1
            chain headers: 1
--------------------------------------------------
port rule counts
             tcp     udp    icmp      ip
     any       0       0       1       0
   total       0       0       1       0
--------------------------------------------------
ips policies rule stats
              id  loaded  shared enabled    file
               0       1       0       1    /usr/local/etc/snort/snort.lua
--------------------------------------------------
pcap DAQ configured to passive.

Snort successfully validated the configuration (with 0 warnings).
o")~   Snort exiting
```

```
Loading rule args:
Loading /usr/local/etc/rules/local.rules:
Finished /usr/local/etc/rules/local.rules:
Finished rule args:
--------------------------------------------------
rule counts
       total rules loaded: 1
               text rules: 1
            option chains: 1
            chain headers: 1
--------------------------------------------------
port rule counts
             tcp     udp    icmp      ip
     any       0       0       1       0
   total       0       0       1       0
--------------------------------------------------
ips policies rule stats
               id  loaded  shared enabled    file
                0       1       0       1    /usr/local/etc/snort/snort.lua
--------------------------------------------------
pcap DAQ configured to passive.
Commencing packet processing
++ [0] enp0s3
```



```
Pinging 192.168.43.14 with 32 bytes of data:
Reply from 192.168.43.14: bytes=32 time<1ms TTL=64
Reply from 192.168.43.14: bytes=32 time<1ms TTL=64
Reply from 192.168.43.14: bytes=32 time<1ms TTL=64
Reply from 192.168.43.14: bytes=32 time<1ms TTL=64
Reply from 192.168.43.14: bytes=32 time<1ms TTL=64
Reply from 192.168.43.14: bytes=32 time<1ms TTL=64
Reply from 192.168.43.14: bytes=32 time<1ms TTL=64
Reply from 192.168.43.14: bytes=32 time<1ms TTL=64
Reply from 192.168.43.14: bytes=32 time<1ms TTL=64
Reply from 192.168.43.14: bytes=32 time<1ms TTL=64
Reply from 192.168.43.14: bytes=32 time<1ms TTL=64
Reply from 192.168.43.14: bytes=32 time<1ms TTL=64
Reply from 192.168.43.14: bytes=32 time<1ms TTL=64
Reply from 192.168.43.14: bytes=32 time<1ms TTL=64
Reply from 192.168.43.14: bytes=32 time<1ms TTL=64
Reply from 192.168.43.14: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.43.14:
    Packets: Sent = 16, Received = 16, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```



```
12/05-01:33:36.648214 [**] [1:1000001:1] "ICMP Packet found" [**] [Priority: 0]
{ICMP} 192.168.43.14 -> 192.168.43.124
12/05-01:33:37.651159 [**] [1:1000001:1] "ICMP Packet found" [**] [Priority: 0]
{ICMP} 192.168.43.124 -> 192.168.43.14
12/05-01:33:37.651179 [**] [1:1000001:1] "ICMP Packet found" [**] [Priority: 0]
{ICMP} 192.168.43.14 -> 192.168.43.124
12/05-01:33:38.652965 [**] [1:1000001:1] "ICMP Packet found" [**] [Priority: 0]
{ICMP} 192.168.43.124 -> 192.168.43.14
12/05-01:33:38.652989 [**] [1:1000001:1] "ICMP Packet found" [**] [Priority: 0]
{ICMP} 192.168.43.14 -> 192.168.43.124
12/05-01:33:39.660245 [**] [1:1000001:1] "ICMP Packet found" [**] [Priority: 0]
{ICMP} 192.168.43.124 -> 192.168.43.14
12/05-01:33:39.660271 [**] [1:1000001:1] "ICMP Packet found" [**] [Priority: 0]
{ICMP} 192.168.43.14 -> 192.168.43.124
12/05-01:33:40.662414 [**] [1:1000001:1] "ICMP Packet found" [**] [Priority: 0]
{ICMP} 192.168.43.124 -> 192.168.43.14
12/05-01:33:40.662448 [**] [1:1000001:1] "ICMP Packet found" [**] [Priority: 0]
{ICMP} 192.168.43.14 -> 192.168.43.124
12/05-01:33:41.740681 [**] [1:1000001:1] "ICMP Packet found" [**] [Priority: 0]
{ICMP} 192.168.43.124 -> 192.168.43.14
12/05-01:33:41.740706 [**] [1:1000001:1] "ICMP Packet found" [**] [Priority: 0]
{ICMP} 192.168.43.14 -> 192.168.43.124
12/05-01:34:09.553681 [**] [1:1000001:1] "ICMP Packet found" [**] [Priority: 0]
{ICMP} 192.168.43.14 -> 192.168.43.124
```

1. What is a zero-day attack?

Zero day attack is the term used to describe the threat of an unknown security vulnerability in a computer software or application for which either the patch has not been released or the application developers were unaware of or did not have sufficient time to address.

Zero-day attack can be perceived in two ways: The first one is where these attacks are said to be attacks that target the back door or vulnerabilities of any software that has been patched or declared publicly, on the other hand, the second one states that these attacks take advantage of a vulnerability or bug in the software on the day it was released itself hence the name Zero-day.

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

Snort clearly is able to detect zero-days' (a mean of 17% detection). The detection rate is however on overall greater for theoretically known attacks (a mean of 54% detection). As a basis for analysis, the detected attacks are categorized according to the vulnerabilities they exploit. (Buffer Error, command injection, PHP file inclusion, etc) A theoretical estimate of Snort's potency at detecting attacks can be gained by observing the vulnerability coverage of its ruleset. There were 9128 signatures in the tested Snort ruleset. At the time of the release of this ruleset, there were 21166 vulnerabilities disclosed in the US National Vulnerability Database (NVD). Of these vulnerabilities, 9104 were of high severity as defined by the Common Vulnerability Scoring System [20]. A high severity vulnerability can loosely be seen as a vulnerability that can be remotely exploited to gain privileges of a host (e.g., user or admin). Metasploit exploits typically cohere to such vulnerabilities. These are also a focus area of the Snort ruleset due to

their severity. The ratio between Snort signatures, disclosed vulnerabilities, and disclosed vulnerabilities of high severity seems to be rather consistent over time: the number of Snort alarms in the official ruleset is about as large as the number of disclosed high vulnerabilities, and a bit less than half of the total number of disclosed vulnerabilities.

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

```
alert icmp any any -> $HOME_NET any (msg:"ICMP Packet found"; sid:1000001; rev:1
;)
alert tcp any any -> $HOME_NET 21 (msg:"FTP incoming"; sid:100006927; rev:1;)
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"/usr/local/etc/rules/local.rules" 2L, 161C                    2,54          All
```

```
port rule counts
             tcp     udp    icmp      ip
     any       0       0       1       0
     dst       1       0       0       0
   total       1       0       1       0
-------------------------------------------------
ips policies rule stats
               id  loaded  shared enabled    file
                0       2       0       2    /usr/local/etc/snort/snort.lua
-------------------------------------------------
pcap DAQ configured to passive.
Commencing packet processing
++ [0] enp0s3
12/05-11:02:48.886643 [**] [1:100006927:1] "FTP incoming" [**] [Priority: 0] {TC
P} 192.168.43.124:58976 -> 192.168.43.14:21
12/05-11:02:49.387785 [**] [1:100006927:1] "FTP incoming" [**] [Priority: 0] {TC
P} 192.168.43.124:58976 -> 192.168.43.14:21
12/05-11:02:49.889653 [**] [1:100006927:1] "FTP incoming" [**] [Priority: 0] {TC
P} 192.168.43.124:58976 -> 192.168.43.14:21
12/05-11:02:50.390409 [**] [1:100006927:1] "FTP incoming" [**] [Priority: 0] {TC
P} 192.168.43.124:58976 -> 192.168.43.14:21
12/05-11:02:50.890591 [**] [1:100006927:1] "FTP incoming" [**] [Priority: 0] {TC
P} 192.168.43.124:58976 -> 192.168.43.14:21
```

EXTRA:

```
alert icmp any any -> $HOME_NET any (msg:"ICMP Packet found"; sid:1000001; rev:1
;)
alert tcp any any -> $HOME_NET 21 (msg:"FTP incoming"; sid:100006927; rev:1;)
alert tcp any any -> any any (content:"www.facebook.com"; msg:"someone visiting
facebook!"; sid:10000009; rev:1;)
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"/usr/local/etc/rules/local.rules" 3L, 275C                    3,39          All
```

```
               0       3       0       3    /usr/local/etc/snort/snort.lua
--------------------------------------------------
fast pattern port groups        src     dst     any
                   packet:        0       0       1
--------------------------------------------------
search engine
                instances: 1
                 patterns: 1
            pattern chars: 17
               num states: 17
         num match states: 1
             memory scale: KB
             total memory: 1.53516
           pattern memory: 0.0546875
        match list memory: 0.164062
        transition memory: 1.19141
--------------------------------------------------
pcap DAQ configured to passive.
Commencing packet processing
++ [0] enp0s3
12/05-12:19:32.075334 [**] [1:10000009:1] "someone visiting facebook!" [**] [Pri
ority: 0] {TCP} 192.168.43.14:34824 -> 31.13.79.35:443
```