

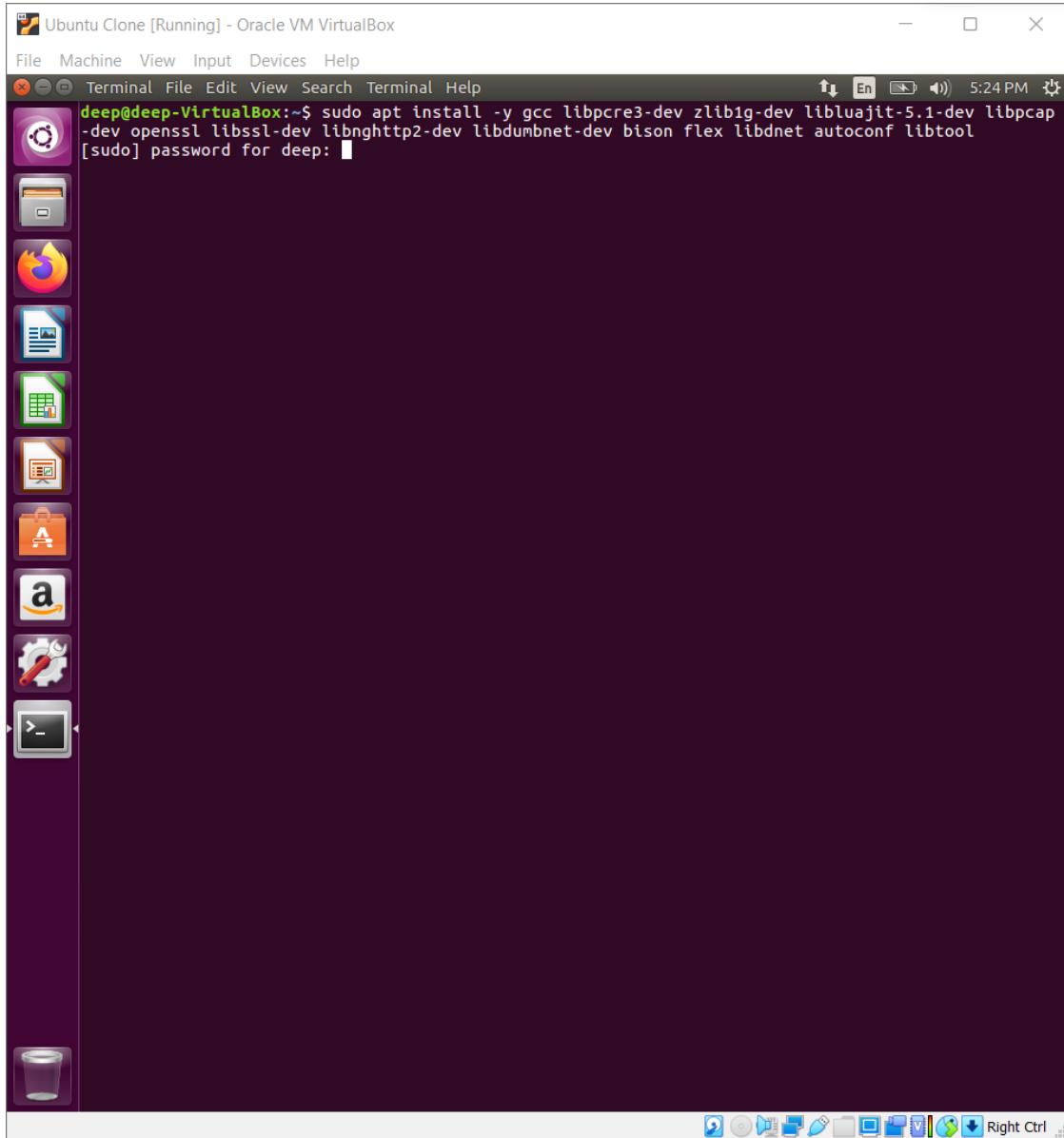
## **Experiment 6: Firewall and Intrusion Detection System**

Name: Deep Nayak UID: 2019130045 TE COMPS

**AIM :** To explore the Snort Intrusion Detection Systems and study Snort IDS, a signature-based intrusion detection system used to detect network attacks. Snort can also be used as a simple packet logger. Use snort as a packet sniffer and write my own IDS rules.

## **OUTPUT :**

- Installing Snort and various other dependencies it requires.



Ubuntu Clone [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

deep@deep-VirtualBox: ~

```
Selecting previously unselected package zlib1g-dev:amd64.
Preparing to unpack .../zlib1g-dev_1%3a1.2.8.dfsg-2ubuntu4.3_amd64.deb ...
Unpacking zlib1g-dev:amd64 (1:1.2.8.dfsg-2ubuntu4.3) ...
Selecting previously unselected package libssl-dev:amd64.
Preparing to unpack .../libssl-dev_1.0.2g-1ubuntu4.20_amd64.deb ...
Unpacking libssl-dev:amd64 (1.0.2g-1ubuntu4.20) ...
Selecting previously unselected package libssl-doc.
Preparing to unpack .../libssl-doc_1.0.2g-1ubuntu4.20_all.deb ...
Unpacking libssl-doc (1.0.2g-1ubuntu4.20) ...
Selecting previously unselected package libtool.
Preparing to unpack .../libtool_2.4.6-0.1_all.deb ...
Unpacking libtool (2.4.6-0.1) ...
Selecting previously unselected package libdnet:amd64.
Preparing to unpack .../libdnet_2.64build2_amd64.deb ...
Unpacking libdnet:amd64 (2.64build2) ...
Processing triggers for install-info (6.1.0.dfsg.1-5) ...
Processing triggers for man-db (2.7.5-1) ...
Processing triggers for libc-bin (2.23-0ubuntu11.3) ...
Processing triggers for doc-base (0.10.7) ...
Processing 2 added doc-base files...
Setting up libsigsegv2:amd64 (2.10-4) ...
Setting up m4 (1.4.17-5) ...
Setting up libfl-dev:amd64 (2.6.0-11) ...
Setting up flex (2.6.0-11) ...
Setting up libdumbnet1:amd64 (1.12-7) ...
Setting up libdumbnet-dev (1.12-7) ...
Setting up libpcrccpp0v5:amd64 (2:8.38-3.1) ...
Setting up autoconf (2.69-9) ...
Setting up autotools-dev (20150820.1) ...
Setting up automake (1:1.15-4ubuntu1) ...
update-alternatives: using /usr/bin/automake-1.15 to provide /usr/bin/automake (automake) in auto mode
Setting up libbison-dev:amd64 (2:3.0.4.dfsg-1) ...
Setting up bison (2:3.0.4.dfsg-1) ...
update-alternatives: using /usr/bin/bison.yacc to provide /usr/bin/yacc (yacc) in auto mode
Setting up libltdl-dev:amd64 (2.4.6-0.1) ...
Setting up libluajit-5.1-common (2.0.4+dfsg-1+deb9u1build0.16.04.1) ...
Setting up libluajit-5.1-2:amd64 (2.0.4+dfsg-1+deb9u1build0.16.04.1) ...
Setting up libluajit-5.1-dev:amd64 (2.0.4+dfsg-1+deb9u1build0.16.04.1) ...
Setting up libnghhttp2-14:amd64 (1.7.1-1) ...
Setting up libnghhttp2-dev (1.7.1-1) ...
Setting up libpcap0.8-dev (1.7.4-2ubuntu0.1) ...
Setting up libpcap-dev (1.7.4-2ubuntu0.1) ...
Setting up libpcre32-3:amd64 (2:8.38-3.1) ...
Setting up libpcre3-dev:amd64 (2:8.38-3.1) ...
Setting up zlib1g-dev:amd64 (1:1.2.8.dfsg-2ubuntu4.3) ...
Setting up libssl-dev:amd64 (1.0.2g-1ubuntu4.20) ...
Setting up libssl-doc (1.0.2g-1ubuntu4.20) ...
Setting up libtool (2.4.6-0.1) ...
Setting up libdnet:amd64 (2.64build2) ...
Processing triggers for libc-bin (2.23-0ubuntu11.3) ...
deep@deep-VirtualBox:~$
```

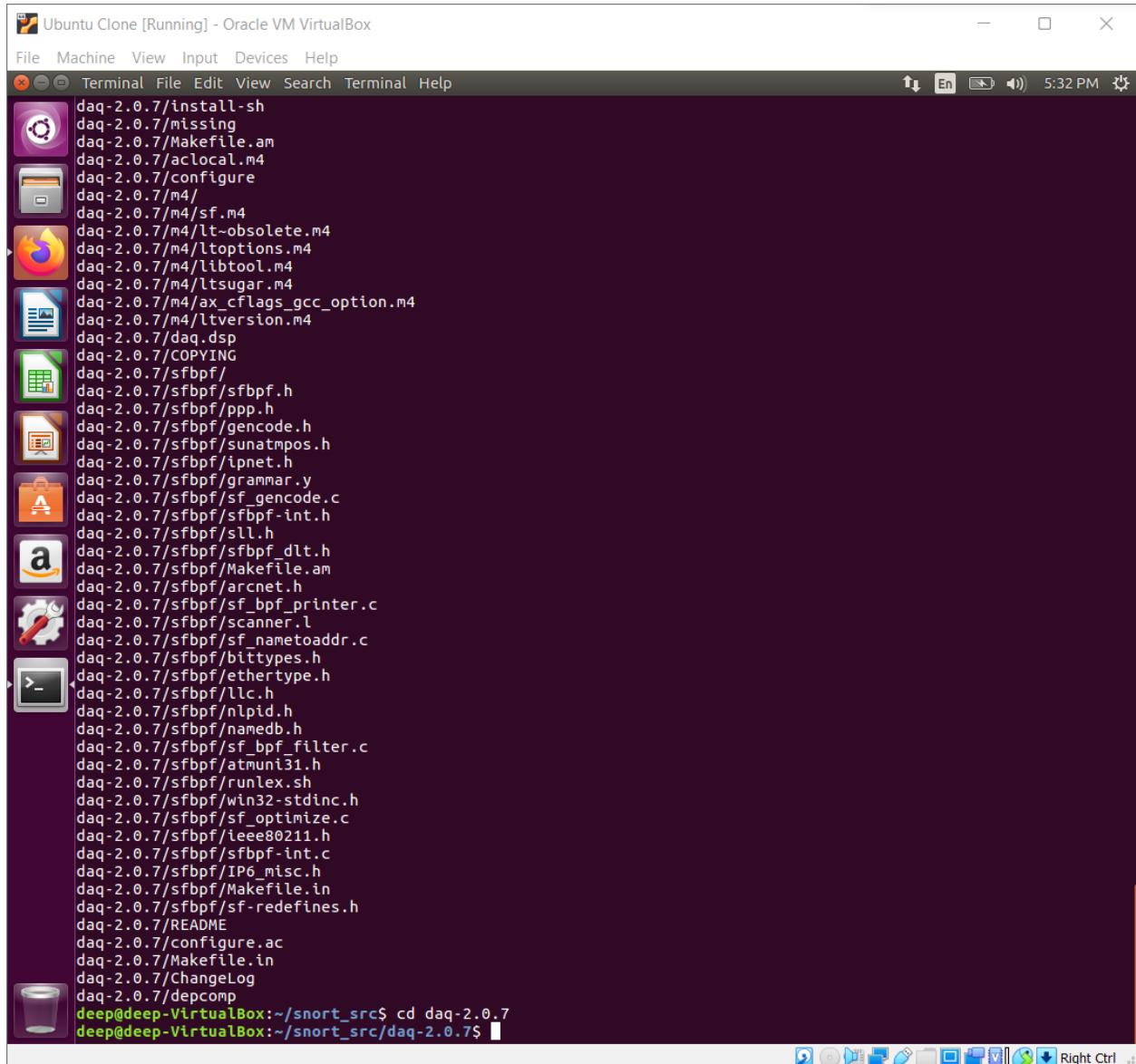
## Downloading and installing prerequisites for Snort

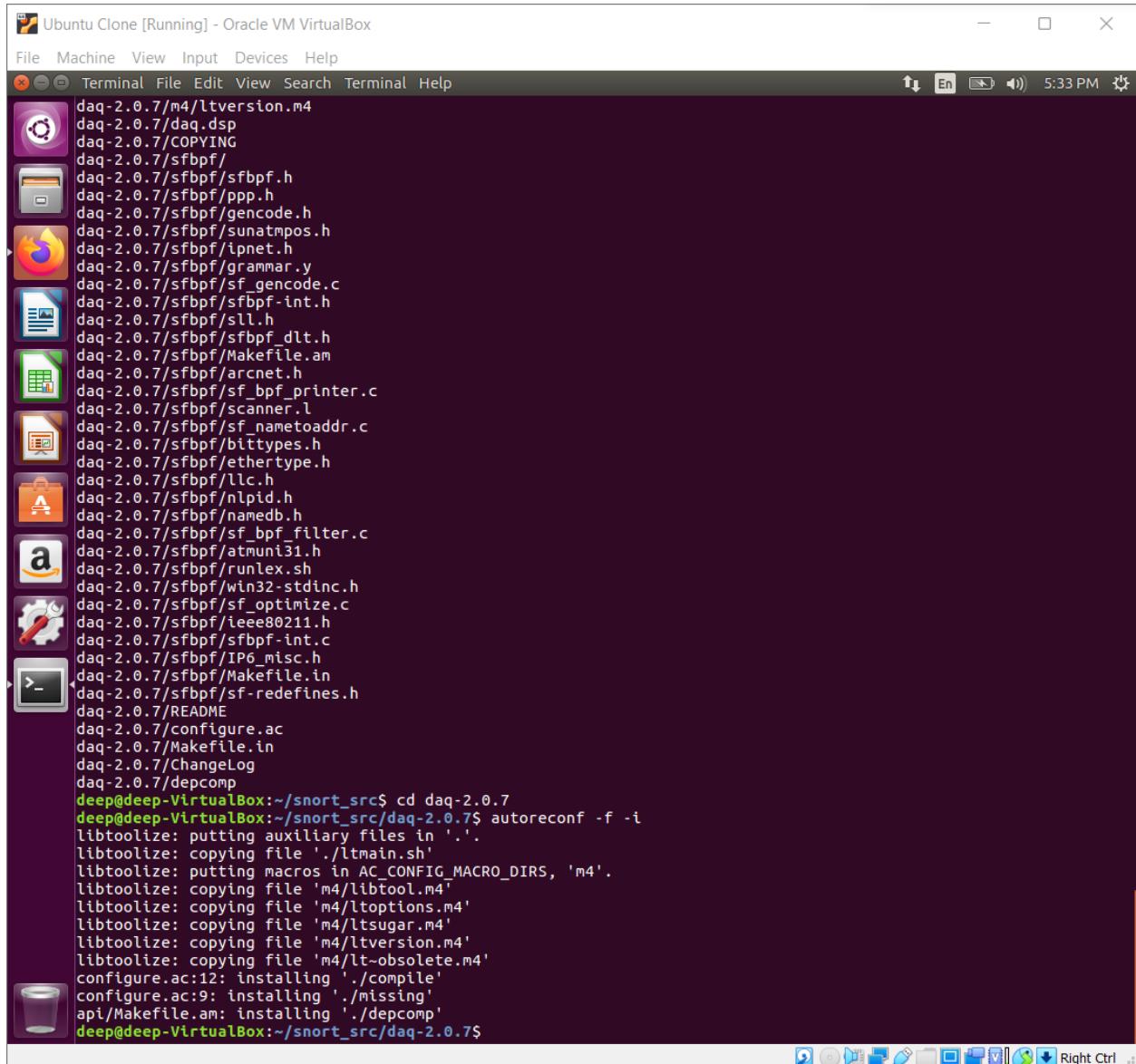
The screenshot shows a terminal window titled "Ubuntu Clone [Running] - Oracle VM VirtualBox". The terminal is displaying a series of package installations and a wget command to download the Snort source code.

```
Setting up libdumbnet-dev (1.12-7) ...
Setting up libpcrecpp0v5:amd64 (2:8.38-3.1) ...
Setting up autoconf (2.69-9) ...
Setting up autotools-dev (20150820.1) ...
Setting up automake (1:1.15-4ubuntu1) ...
update-alternatives: using /usr/bin/automake-1.15 to provide /usr/bin/automake (automake) in auto mode
Setting up libbison-dev:amd64 (2:3.0.4.dfsg-1) ...
Setting up bison (2:3.0.4.dfsg-1) ...
update-alternatives: using /usr/bin/bison.yacc to provide /usr/bin/yacc (yacc) in auto mode
Setting up libltdl-dev:amd64 (2.4.6-0.1) ...
Setting up libluajit-5.1-common (2.0.4+dfsg-1+deb9u1build0.16.04.1) ...
Setting up libluajit-5.1-2:amd64 (2.0.4+dfsg-1+deb9u1build0.16.04.1) ...
Setting up libluajit-5.1-dev:amd64 (2.0.4+dfsg-1+deb9u1build0.16.04.1) ...
Setting up libnnghttp2-14:amd64 (1.7.1-1) ...
Setting up libnnghttp2-dev (1.7.1-1) ...
Setting up libpcap0.8-dev (1.7.4-2ubuntu0.1) ...
Setting up libpcap-dev (1.7.4-2ubuntu0.1) ...
Setting up libpcre3-3:amd64 (2:8.38-3.1) ...
Setting up libpcre3-dev:amd64 (2:8.38-3.1) ...
Setting up zlibg-dev:amd64 (1:1.2.8.dfsg-2ubuntu4.3) ...
Setting up libssl-dev:amd64 (1.0.2g-1ubuntu4.20) ...
Setting up libssl-doc (1.0.2g-1ubuntu4.20) ...
Setting up libttool (2.4.6-0.1) ...
Setting up libdnet:amd64 (2.64build2) ...
Processing triggers for libc-bin (2.23-0ubuntu11.3) ...
deep@deep-VirtualBox:~$ ls
Desktop  Downloads      Music  osc  Pictures  prog1.c  prog2.c  prog3.c  Templates
Documents examples.desktop  osc  osc2  prog1  prog2  prog3  Public  Videos
deep@deep-VirtualBox:~/snort_src$ wget https://www.snort.org/downloads/snort/daq-2.0.7.tar.gz
--2021-12-09 17:31:45-- https://www.snort.org/downloads/snort/daq-2.0.7.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/000/021/683/original/daq-2.0.7.tar.gz?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAU7AK51TMGOEV4EFM%2F20211209%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20211209T120146Z&X-Amz-Expires=3600&X-Amz-SignedHeaders=host&X-Amz-Signature=522d81541082eaa4870962bd67ac33e71b4341b272b63cabb76d98831aeb9079 [following]
--2021-12-09 17:31:46-- https://snort-org-site.s3.amazonaws.com/production/release_files/files/000/021/683/original/daq-2.0.7.tar.gz?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAU7AK51TMGOEV4EFM%2F20211209%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20211209T120146Z&X-Amz-Expires=3600&X-Amz-SignedHeaders=host&X-Amz-Signature=522d81541082eaa4870962bd67ac33e71b4341b272b63cabb76d98831aeb9079
Resolving snort-org-site.s3.amazonaws.com (snort-org-site.s3.amazonaws.com)... 52.217.8.44
Connecting to snort-org-site.s3.amazonaws.com (snort-org-site.s3.amazonaws.com)|52.217.8.44|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 515154 (503K) [binary/octet-stream]
Saving to: 'daq-2.0.7.tar.gz'

daq-2.0.7.tar.gz          100%[=====] 503.08K   437KB/s    in 1.2s

2021-12-09 17:31:49 (437 KB/s) - 'daq-2.0.7.tar.gz' saved [515154/515154]
deep@deep-VirtualBox:~/snort_src$
```





Ubuntu Clone [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

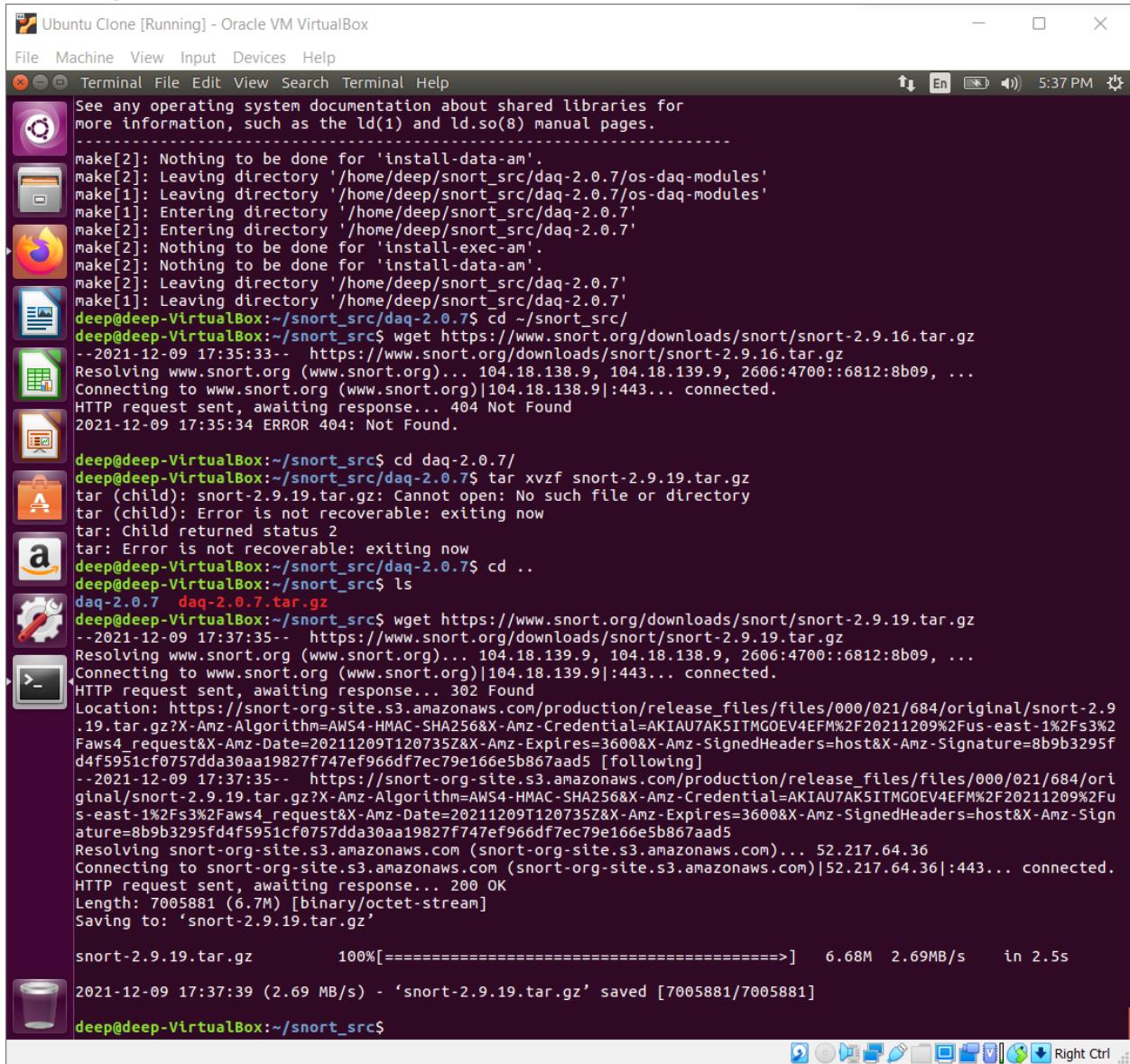
Terminal File Edit View Search Terminal Help

```
libtool: install: (cd /home/deep/snort_src/daq-2.0.7/os-daq-modules; /bin/bash "/home/deep/snort_src/daq-2.0.7/libtool" --tag CC --mode=relink gcc -DBUILDING_SO -g -O2 -fvisibility=hidden -Wall -Wwrite-strings -Wsign-compare -Wcast-align -Wextra -Wformat -Wformat-security -Wno-unused-parameter -fno-strict-aliasing -fdiagnostics-show-option -pedantic -std=c99 -D_GNU_SOURCE -module -export-dynamic -avoid-version -shared -o daq_afpacket.la -rpath /usr/local/lib/daq daq_afpacket_la-daq_afpacket.lo ../../sfbpf/libsfbpf.la )
libtool: relink: gcc -shared -fPIC -DPIC .libs/daq_afpacket_la-daq_afpacket.o -L/usr/local/lib -lsfbpf -g -O2 -Wl,-soname -Wl,daq_afpacket.so -o .libs/daq_afpacket.so
libtool: install: /usr/bin/install -c .libs/daq_afpacket.soT /usr/local/lib/daq/daq_afpacket.so
libtool: install: /usr/bin/install -c .libs/daq_afpacket.lai /usr/local/lib/daq/daq_afpacket.la
libtool: install: /usr/bin/install -c .libs/daq_pcaps.so /usr/local/lib/daq/daq_pcaps.so
libtool: install: /usr/bin/install -c .libs/daq_pcaps.lai /usr/local/lib/daq/daq_pcaps.la
libtool: install: /usr/bin/install -c .libs/daq_dump.so /usr/local/lib/daq/daq_dump.so
libtool: install: /usr/bin/install -c .libs/daq_dump.lai /usr/local/lib/daq/daq_dump.la
libtool: warning: relinking 'daq_ipfw.la'
libtool: install: (cd /home/deep/snort_src/daq-2.0.7/os-daq-modules; /bin/bash "/home/deep/snort_src/daq-2.0.7/libtool" --tag CC --mode=relink gcc -DBUILDING_SO -g -O2 -fvisibility=hidden -Wall -Wwrite-strings -Wsign-compare -Wcast-align -Wextra -Wformat -Wformat-security -Wno-unused-parameter -fno-strict-aliasing -fdiagnostics-show-option -pedantic -std=c99 -D_GNU_SOURCE -module -export-dynamic -avoid-version -shared -o daq_ipfw.la -rpath /usr/local/lib/daq daq_ipfw_la-daq_ipfw.lo ../../sfbpf/libsfbpf.la )
libtool: relink: gcc -shared -fPIC -DPIC .libs/daq_ipfw_la-daq_ipfw.o -L/usr/local/lib -lsfbpf -g -O2 -Wl,-soname -Wl,daq_ipfw.so -o .libs/daq_ipfw.so
libtool: install: /usr/bin/install -c .libs/daq_ipfw.soT /usr/local/lib/daq/daq_ipfw.so
libtool: install: /usr/bin/install -c .libs/daq_ipfw.lai /usr/local/lib/daq/daq_ipfw.la
libtool: finish: PATH="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/snap/bin:/sbin" ldconfig -n /usr/local/lib/daq
-----
Libraries have been installed in:
  /usr/local/lib/daq

If you ever happen to want to link against installed libraries
in a given directory, LIBDIR, you must either use libtool, and
specify the full pathname of the library, or use the '-LLIBDIR'
flag during linking and do at least one of the following:
  - add LIBDIR to the 'LD_LIBRARY_PATH' environment variable
    during execution
  - add LIBDIR to the 'LD_RUN_PATH' environment variable
    during linking
  - use the '-Wl,-rpath -Wl,LIBDIR' linker flag
  - have your system administrator add LIBDIR to '/etc/ld.so.conf'

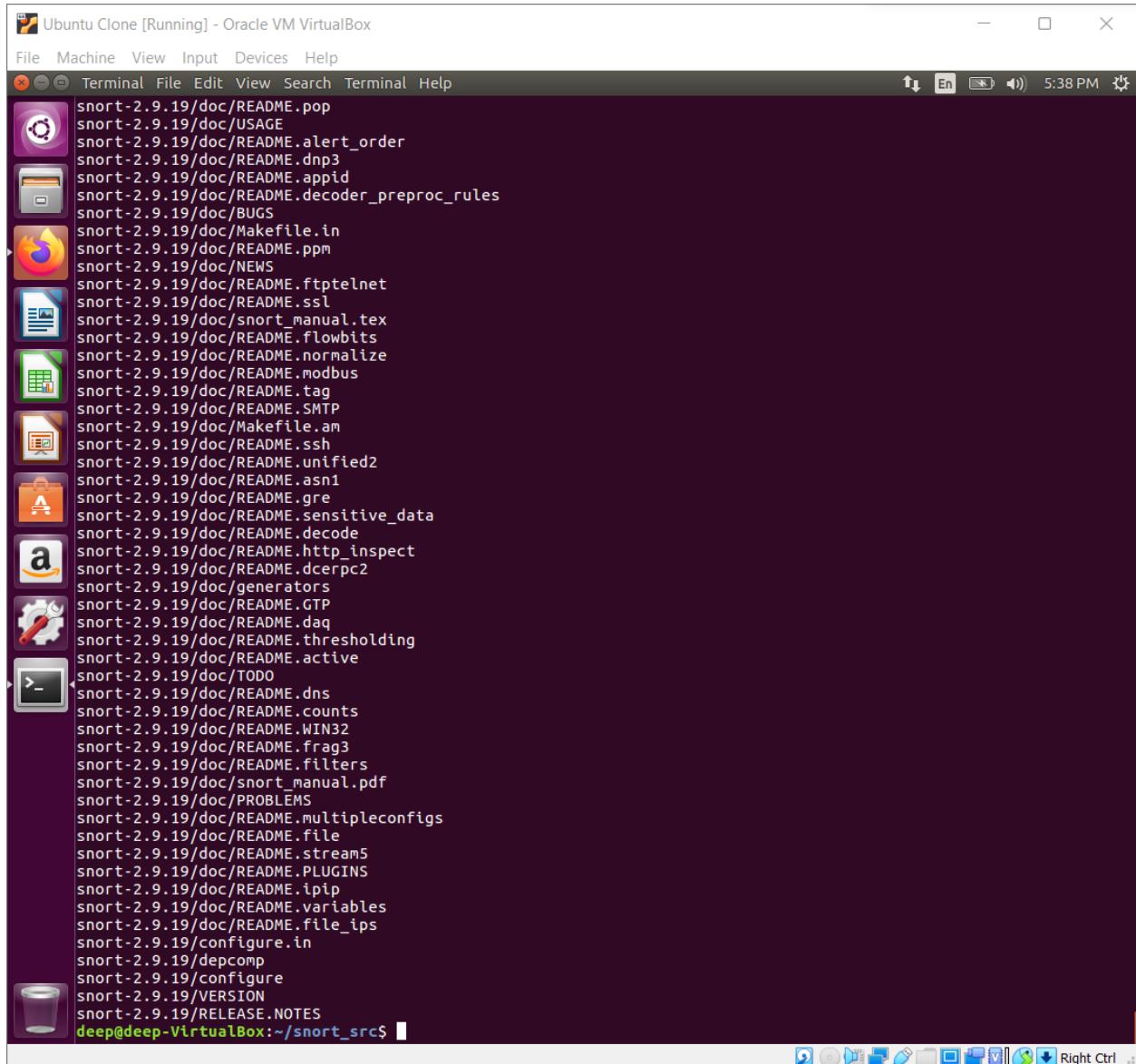
See any operating system documentation about shared libraries for
more information, such as the ld(1) and ld.so(8) manual pages.
-----
make[2]: Nothing to be done for 'install-data-am'.
make[2]: Leaving directory '/home/deep/snort_src/daq-2.0.7/os-daq-modules'
make[1]: Leaving directory '/home/deep/snort_src/daq-2.0.7/os-daq-modules'
make[1]: Entering directory '/home/deep/snort_src/daq-2.0.7'
make[2]: Entering directory '/home/deep/snort_src/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/deep/snort_src/daq-2.0.7'
make[1]: Leaving directory '/home/deep/snort_src/daq-2.0.7'
deep@deep-VirtualBox:~/snort_src/daq-2.0.7$
```

## Building Snort from its source



The screenshot shows a terminal window titled "Ubuntu Clone [Running] - Oracle VM VirtualBox". The terminal is displaying a series of commands and their outputs related to building Snort from source and downloading the Snort 2.9.19 tarball.

```
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/deep/snort_src/daq-2.0.7/os-daq-modules'  
make[1]: Leaving directory '/home/deep/snort_src/daq-2.0.7/os-daq-modules'  
make[1]: Entering directory '/home/deep/snort_src/daq-2.0.7'  
make[2]: Entering directory '/home/deep/snort_src/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/deep/snort_src/daq-2.0.7'  
make[1]: Leaving directory '/home/deep/snort_src/daq-2.0.7'  
deep@deep-VirtualBox:~/snort_src/daq-2.0.7$ cd ~/snort_src/  
deep@deep-VirtualBox:~/snort_src$ wget https://www.snort.org/downloads/snort/snort-2.9.16.tar.gz  
--2021-12-09 17:35:33-- https://www.snort.org/downloads/snort/snort-2.9.16.tar.gz  
Resolving www.snort.org (www.snort.org)... 104.18.138.9, 104.18.139.9, 2606:4700::6812:8b09, ...  
Connecting to www.snort.org (www.snort.org)|104.18.138.9|:443... connected.  
HTTP request sent, awaiting response... 404 Not Found  
2021-12-09 17:35:34 ERROR 404: Not Found.  
  
deep@deep-VirtualBox:~/snort_src$ cd daq-2.0.7/  
deep@deep-VirtualBox:~/snort_src/daq-2.0.7$ tar xvzf snort-2.9.19.tar.gz  
tar (child): snort-2.9.19.tar.gz: Cannot open: No such file or directory  
tar (child): Error is not recoverable: exiting now  
tar: Child returned status 2  
tar: Error is not recoverable: exiting now  
deep@deep-VirtualBox:~/snort_src/daq-2.0.7$ cd ..  
deep@deep-VirtualBox:~/snort_src$ ls  
daq-2.0.7 daq-2.0.7.tar.gz  
deep@deep-VirtualBox:~/snort_src$ wget https://www.snort.org/downloads/snort/snort-2.9.19.tar.gz  
--2021-12-09 17:37:35-- https://www.snort.org/downloads/snort/snort-2.9.19.tar.gz  
Resolving www.snort.org (www.snort.org)... 104.18.139.9, 104.18.138.9, 2606:4700::6812:8b09, ...  
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/000/021/684/original/snort-2.9.19.tar.gz?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAU7AK5ITMG0EV4EFM%2F20211209%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20211209T120735Z&X-Amz-Expires=3600&X-Amz-SignedHeaders=host&X-Amz-Signature=8b9b3295fd4f5951cf0757dda30aa19827f747ef966df7ec79e166e5b867aad5 [following]  
--2021-12-09 17:37:35-- https://snort-org-site.s3.amazonaws.com/production/release_files/files/000/021/684/original/snort-2.9.19.tar.gz?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAU7AK5ITMG0EV4EFM%2F20211209%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20211209T120735Z&X-Amz-Expires=3600&X-Amz-SignedHeaders=host&X-Amz-Signature=8b9b3295fd4f5951cf0757dda30aa19827f747ef966df7ec79e166e5b867aad5  
Resolving snort-org-site.s3.amazonaws.com (snort-org-site.s3.amazonaws.com)... 52.217.64.36  
Connecting to snort-org-site.s3.amazonaws.com (snort-org-site.s3.amazonaws.com)|52.217.64.36|:443... connected.  
HTTP request sent, awaiting response... 200 OK  
Length: 7005881 (6.7M) [binary/octet-stream]  
Saving to: 'snort-2.9.19.tar.gz'  
  
snort-2.9.19.tar.gz      100%[=====] 6.68M 2.69MB/s    in 2.5s  
2021-12-09 17:37:39 (2.69 MB/s) - 'snort-2.9.19.tar.gz' saved [7005881/7005881]  
deep@deep-VirtualBox:~/snort_src$
```



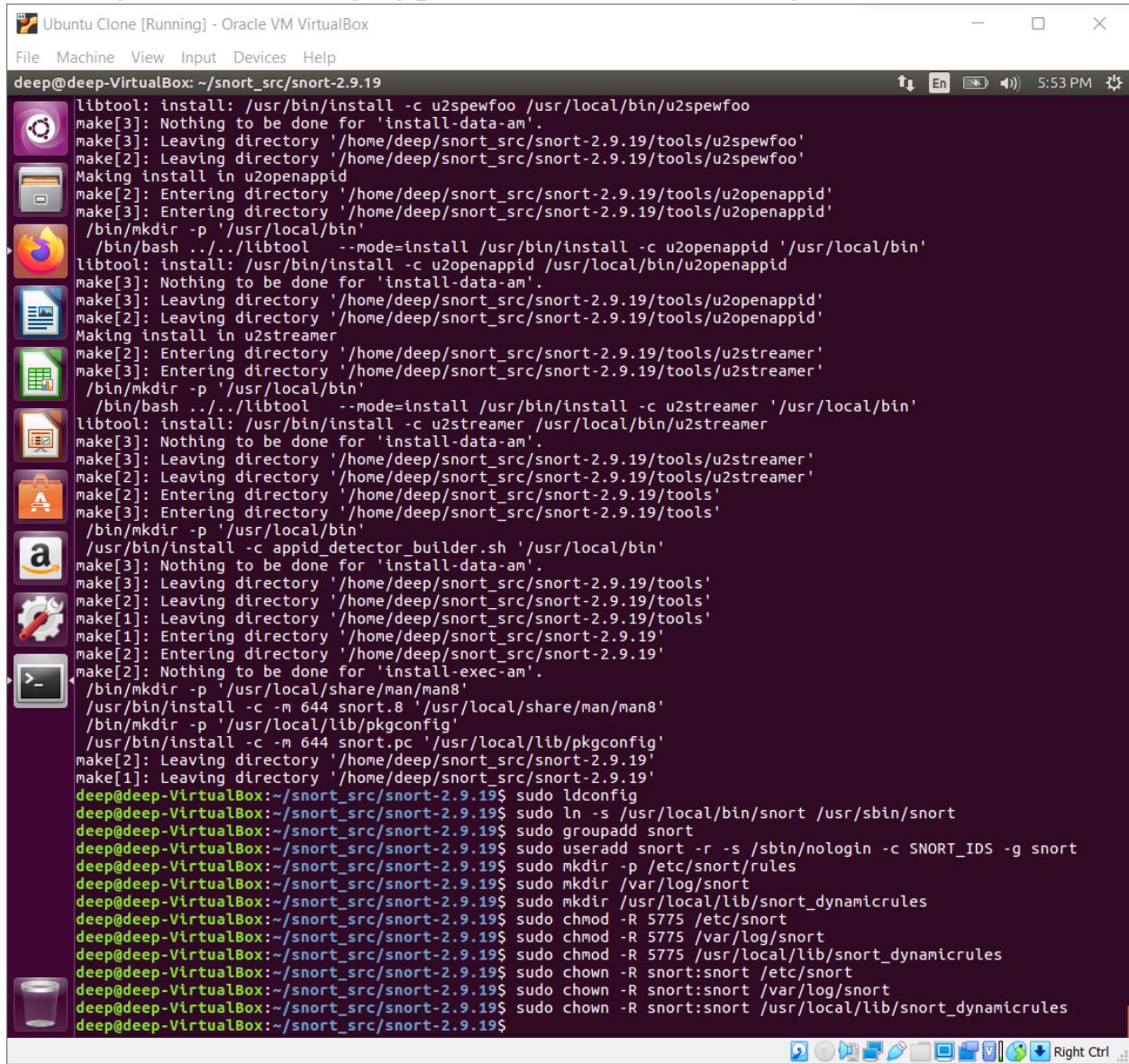
Ubuntu Clone [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Terminal File Edit View Search Terminal Help

```
make[3]: Entering directory '/home/deep/snort_src/snort-2.9.19/tools/u2boat'
/bin/mkdir -p '/usr/local/bin'
/bin/bash ../../libtool --mode=install /usr/bin/install -c u2boat '/usr/local/bin'
libtool: install: /usr/bin/install -c u2boat /usr/local/bin/u2boat
/bin/mkdir -p '/usr/local/share/doc/snort'
/usr/bin/install -c -m 644 README.u2boat '/usr/local/share/doc/snort'
make[3]: Leaving directory '/home/deep/snort_src/snort-2.9.19/tools/u2boat'
make[2]: Leaving directory '/home/deep/snort_src/snort-2.9.19/tools/u2boat'
Making install in u2spewfoo
make[2]: Entering directory '/home/deep/snort_src/snort-2.9.19/tools/u2spewfoo'
make[3]: Entering directory '/home/deep/snort_src/snort-2.9.19/tools/u2spewfoo'
/bin/mkdir -p '/usr/local/bin'
/bin/bash ../../libtool --mode=install /usr/bin/install -c u2spewfoo '/usr/local/bin'
libtool: install: /usr/bin/install -c u2spewfoo /usr/local/bin/u2spewfoo
make[3]: Nothing to be done for 'install-data-am'.
make[3]: Leaving directory '/home/deep/snort_src/snort-2.9.19/tools/u2spewfoo'
make[2]: Leaving directory '/home/deep/snort_src/snort-2.9.19/tools/u2spewfoo'
Making install in u2openappid
make[2]: Entering directory '/home/deep/snort_src/snort-2.9.19/tools/u2openappid'
make[3]: Entering directory '/home/deep/snort_src/snort-2.9.19/tools/u2openappid'
/bin/mkdir -p '/usr/local/bin'
/bin/bash ../../libtool --mode=install /usr/bin/install -c u2openappid '/usr/local/bin'
libtool: install: /usr/bin/install -c u2openappid /usr/local/bin/u2openappid
make[3]: Nothing to be done for 'install-data-am'.
make[3]: Leaving directory '/home/deep/snort_src/snort-2.9.19/tools/u2openappid'
make[2]: Leaving directory '/home/deep/snort_src/snort-2.9.19/tools/u2openappid'
Making install in u2streamer
make[2]: Entering directory '/home/deep/snort_src/snort-2.9.19/tools/u2streamer'
make[3]: Entering directory '/home/deep/snort_src/snort-2.9.19/tools/u2streamer'
/bin/mkdir -p '/usr/local/bin'
/bin/bash ../../libtool --mode=install /usr/bin/install -c u2streamer '/usr/local/bin'
libtool: install: /usr/bin/install -c u2streamer /usr/local/bin/u2streamer
make[3]: Nothing to be done for 'install-data-am'.
make[3]: Leaving directory '/home/deep/snort_src/snort-2.9.19/tools/u2streamer'
make[2]: Leaving directory '/home/deep/snort_src/snort-2.9.19/tools/u2streamer'
make[2]: Entering directory '/home/deep/snort_src/snort-2.9.19/tools'
make[3]: Entering directory '/home/deep/snort_src/snort-2.9.19/tools'
/bin/mkdir -p '/usr/local/bin'
/usr/bin/install -c appid_detector_builder.sh '/usr/local/bin'
make[3]: Nothing to be done for 'install-data-am'.
make[3]: Leaving directory '/home/deep/snort_src/snort-2.9.19/tools'
make[2]: Leaving directory '/home/deep/snort_src/snort-2.9.19/tools'
make[1]: Leaving directory '/home/deep/snort_src/snort-2.9.19/tools'
make[1]: Entering directory '/home/deep/snort_src/snort-2.9.19'
make[2]: Entering directory '/home/deep/snort_src/snort-2.9.19'
make[2]: Nothing to be done for 'install-exec-am'.
/bin/mkdir -p '/usr/local/share/man/man8'
/usr/bin/install -c -m 644 snort.8 '/usr/local/share/man/man8'
/bin/mkdir -p '/usr/local/lib/pkgconfig'
/usr/bin/install -c -m 644 snort.pc '/usr/local/lib/pkgconfig'
make[2]: Leaving directory '/home/deep/snort_src/snort-2.9.19'
make[1]: Leaving directory '/home/deep/snort_src/snort-2.9.19'
deep@deep-VirtualBox:~/snort_src/snort-2.9.19$
```

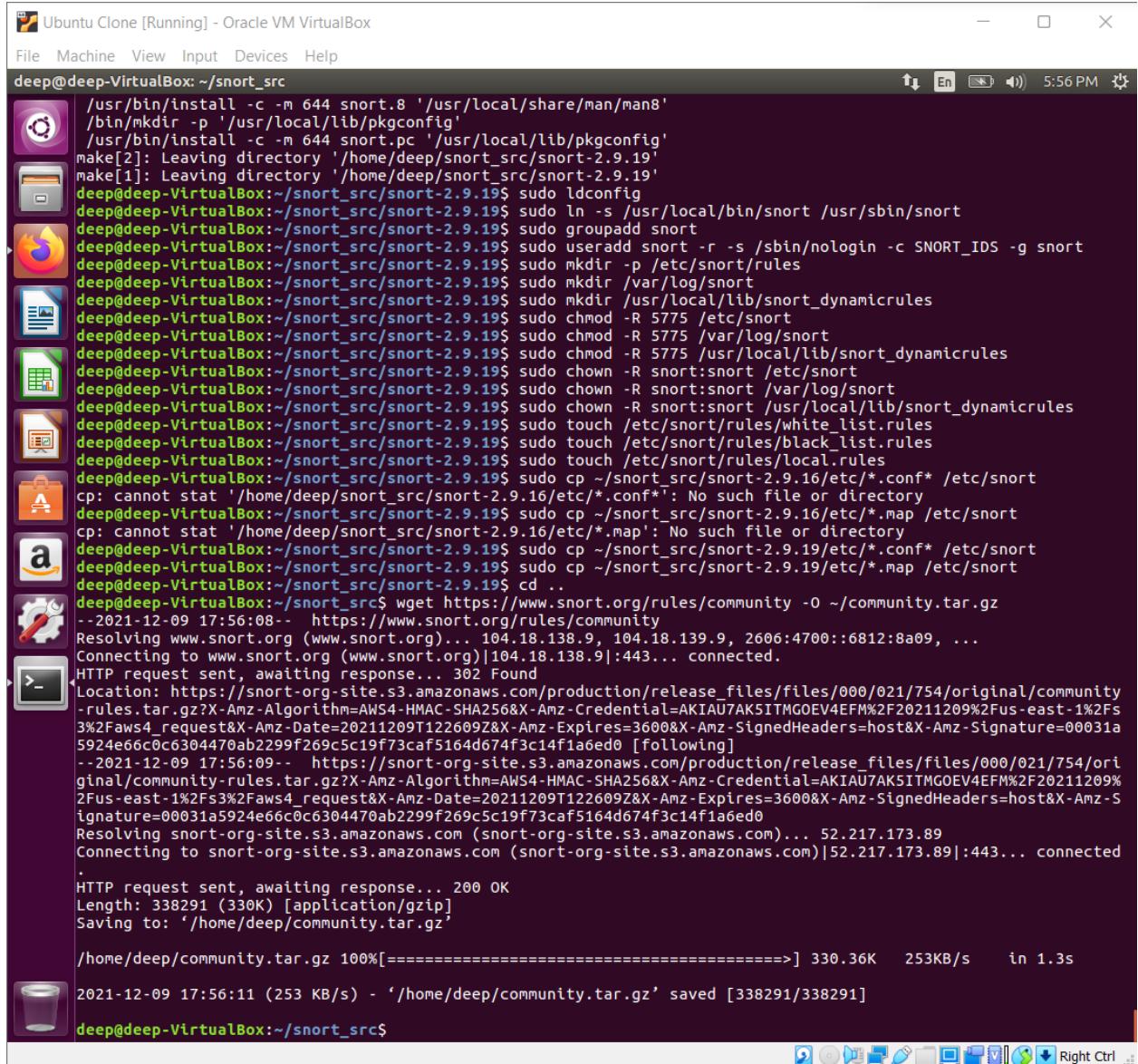
## Creating links and changing permissions of snort configuration files



The screenshot shows a terminal window titled "Ubuntu Clone [Running] - Oracle VM VirtualBox". The terminal session is running on a virtual machine with the command "deep@deep-VirtualBox: ~/snort\_src/snort-2.9.19\$". The user is executing a series of commands to install and configure Snort. The commands include:

```
libtool: install: /usr/bin/install -c u2spewfoo /usr/local/bin/u2spewfoo
make[3]: Nothing to be done for 'install-data-am'.
make[2]: Leaving directory '/home/deep/snort_src/snort-2.9.19/tools/u2spewfoo'
make[1]: Leaving directory '/home/deep/snort_src/snort-2.9.19/tools/u2spewfoo'
Making install in u2openappid
make[2]: Entering directory '/home/deep/snort_src/snort-2.9.19/tools/u2openappid'
make[3]: Entering directory '/home/deep/snort_src/snort-2.9.19/tools/u2openappid'
/bin/mkdir -p '/usr/local/bin'
/bin/bash ../../libtool --mode=install /usr/bin/install -c u2openappid '/usr/local/bin/u2openappid'
libtool: install: /usr/bin/install -c u2openappid /usr/local/bin/u2openappid
make[3]: Nothing to be done for 'install-data-am'.
make[2]: Leaving directory '/home/deep/snort_src/snort-2.9.19/tools/u2openappid'
make[1]: Leaving directory '/home/deep/snort_src/snort-2.9.19/tools/u2openappid'
Making install in u2streamer
make[2]: Entering directory '/home/deep/snort_src/snort-2.9.19/tools/u2streamer'
make[3]: Entering directory '/home/deep/snort_src/snort-2.9.19/tools/u2streamer'
/bin/mkdir -p '/usr/local/bin'
/bin/bash ../../libtool --mode=install /usr/bin/install -c u2streamer '/usr/local/bin/u2streamer'
libtool: install: /usr/bin/install -c u2streamer /usr/local/bin/u2streamer
make[3]: Nothing to be done for 'install-data-am'.
make[2]: Leaving directory '/home/deep/snort_src/snort-2.9.19/tools/u2streamer'
make[1]: Leaving directory '/home/deep/snort_src/snort-2.9.19/tools/u2streamer'
make[2]: Entering directory '/home/deep/snort_src/snort-2.9.19/tools'
make[3]: Entering directory '/home/deep/snort_src/snort-2.9.19/tools'
/bin/mkdir -p '/usr/local/bin'
/usr/bin/install -c appid_detector_builder.sh '/usr/local/bin/appid_detector_builder.sh'
make[3]: Nothing to be done for 'install-data-am'.
make[2]: Leaving directory '/home/deep/snort_src/snort-2.9.19/tools'
make[1]: Leaving directory '/home/deep/snort_src/snort-2.9.19/tools'
make[1]: Entering directory '/home/deep/snort_src/snort-2.9.19'
make[2]: Entering directory '/home/deep/snort_src/snort-2.9.19'
make[2]: Nothing to be done for 'install-exec-am'.
/bin/mkdir -p '/usr/local/share/man/man8'
/usr/bin/install -c -m 644 snort.8 '/usr/local/share/man/man8'
/bin/mkdir -p '/usr/local/lib/pkgconfig'
/usr/bin/install -c -m 644 snort.pc '/usr/local/lib/pkgconfig'
make[2]: Leaving directory '/home/deep/snort_src/snort-2.9.19'
make[1]: Leaving directory '/home/deep/snort_src/snort-2.9.19'
deep@deep-VirtualBox:~/snort_src/snort-2.9.19$ sudo ldconfig
deep@deep-VirtualBox:~/snort_src/snort-2.9.19$ sudo ln -s /usr/local/bin/snort /usr/sbin/snort
deep@deep-VirtualBox:~/snort_src/snort-2.9.19$ sudo groupadd snort
deep@deep-VirtualBox:~/snort_src/snort-2.9.19$ sudo useradd snort -r -s /sbin/nologin -c SNORT_IDS -g snort
deep@deep-VirtualBox:~/snort_src/snort-2.9.19$ sudo mkdir -p /etc/snort/rules
deep@deep-VirtualBox:~/snort_src/snort-2.9.19$ sudo mkdir /var/log/snort
deep@deep-VirtualBox:~/snort_src/snort-2.9.19$ sudo mkdir /usr/local/lib/snort_dynamicrules
deep@deep-VirtualBox:~/snort_src/snort-2.9.19$ sudo chmod -R 5775 /etc/snort
deep@deep-VirtualBox:~/snort_src/snort-2.9.19$ sudo chmod -R 5775 /var/log/snort
deep@deep-VirtualBox:~/snort_src/snort-2.9.19$ sudo chmod -R 5775 /usr/local/lib/snort_dynamicrules
deep@deep-VirtualBox:~/snort_src/snort-2.9.19$ sudo chown -R snort:snort /etc/snort
deep@deep-VirtualBox:~/snort_src/snort-2.9.19$ sudo chown -R snort:snort /var/log/snort
deep@deep-VirtualBox:~/snort_src/snort-2.9.19$ sudo chown -R snort:snort /usr/local/lib/snort_dynamicrules
deep@deep-VirtualBox:~/snort_src/snort-2.9.19$
```

## Downloading Community rules and using them as a base for local rules



The screenshot shows a terminal window titled "Ubuntu Clone [Running] - Oracle VM VirtualBox". The terminal session is running on a virtual machine named "deep@deep-VirtualBox". The user is in the directory `~/snort\_src` and is executing commands to build Snort and download community rules.

```
/usr/bin/install -c -m 644 snort.8 '/usr/local/share/man/man8'  
/bin/mkdir -p '/usr/local/lib/pkgconfig'  
/usr/bin/install -c -m 644 snort.pc '/usr/local/lib/pkgconfig'  
make[2]: Leaving directory '/home/deep/snort_src/snort-2.9.19'  
make[1]: Leaving directory '/home/deep/snort_src/snort-2.9.19'  
deep@deep-VirtualBox:~/snort_src/snort-2.9.19$ sudo ldconfig  
deep@deep-VirtualBox:~/snort_src/snort-2.9.19$ sudo ln -s /usr/local/bin/snort /usr/sbin/snort  
deep@deep-VirtualBox:~/snort_src/snort-2.9.19$ sudo groupadd snort  
deep@deep-VirtualBox:~/snort_src/snort-2.9.19$ sudo useradd snort -r -s /sbin/nologin -c SNORT_IDS -g snort  
deep@deep-VirtualBox:~/snort_src/snort-2.9.19$ sudo mkdir -p /etc/snort/rules  
deep@deep-VirtualBox:~/snort_src/snort-2.9.19$ sudo mkdir /var/log/snort  
deep@deep-VirtualBox:~/snort_src/snort-2.9.19$ sudo mkdir /usr/local/lib/snort_dynamicrules  
deep@deep-VirtualBox:~/snort_src/snort-2.9.19$ sudo chmod -R 5775 /etc/snort  
deep@deep-VirtualBox:~/snort_src/snort-2.9.19$ sudo chmod -R 5775 /var/log/snort  
deep@deep-VirtualBox:~/snort_src/snort-2.9.19$ sudo chmod -R 5775 /usr/local/lib/snort_dynamicrules  
deep@deep-VirtualBox:~/snort_src/snort-2.9.19$ sudo chown -R snort:snort /etc/snort  
deep@deep-VirtualBox:~/snort_src/snort-2.9.19$ sudo chown -R snort:snort /var/log/snort  
deep@deep-VirtualBox:~/snort_src/snort-2.9.19$ sudo chown -R snort:snort /usr/local/lib/snort_dynamicrules  
deep@deep-VirtualBox:~/snort_src/snort-2.9.19$ sudo touch /etc/snort/rules/white_list.rules  
deep@deep-VirtualBox:~/snort_src/snort-2.9.19$ sudo touch /etc/snort/rules/black_list.rules  
deep@deep-VirtualBox:~/snort_src/snort-2.9.19$ sudo touch /etc/snort/rules/local.rules  
deep@deep-VirtualBox:~/snort_src/snort-2.9.19$ sudo cp ~/snort_src/snort-2.9.16/etc/*.conf* /etc/snort  
cp: cannot stat '/home/deep/snort_src/snort-2.9.16/etc/*.conf*': No such file or directory  
deep@deep-VirtualBox:~/snort_src/snort-2.9.19$ sudo cp ~/snort_src/snort-2.9.16/etc/*.map /etc/snort  
cp: cannot stat '/home/deep/snort_src/snort-2.9.16/etc/*.map': No such file or directory  
deep@deep-VirtualBox:~/snort_src/snort-2.9.19$ sudo cp ~/snort_src/snort-2.9.19/etc/*.conf* /etc/snort  
deep@deep-VirtualBox:~/snort_src/snort-2.9.19$ sudo cp ~/snort_src/snort-2.9.19/etc/*.map /etc/snort  
deep@deep-VirtualBox:~/snort_src/snort-2.9.19$ cd ..  
deep@deep-VirtualBox:~/snort_src$ wget https://www.snort.org/rules/community -O ~/community.tar.gz  
--2021-12-09 17:56:08-- https://www.snort.org/rules/community  
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/000/021/754/original/community-rules.tar.gz?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAU7AK5ITMG0EV4EFM%2F20211209%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20211209T122609Z&X-Amz-Expires=3600&X-Amz-SignedHeaders=host&X-Amz-Signature=00031a5924e66c0c6304470ab2299f269c5c19f73caf5164d674f3c14f1a6ed0 [following]  
--2021-12-09 17:56:09-- https://snort-org-site.s3.amazonaws.com/production/release_files/files/000/021/754/original/community-rules.tar.gz?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAU7AK5ITMG0EV4EFM%2F20211209%2Fus-east-1%2Fs3%2Faws4 request&X-Amz-Date=20211209T122609Z&X-Amz-Expires=3600&X-Amz-SignedHeaders=host&X-Amz-Signature=00031a5924e66c0c6304470ab2299f269c5c19f73caf5164d674f3c14f1a6ed0  
Resolving snort-org-site.s3.amazonaws.com (snort-org-site.s3.amazonaws.com)... 52.217.173.89  
Connecting to snort-org-site.s3.amazonaws.com (snort-org-site.s3.amazonaws.com)|52.217.173.89|:443... connected  
. HTTP request sent, awaiting response... 200 OK  
Length: 338291 (330K) [application/gzip]  
Saving to: '/home/deep/community.tar.gz'  
  
/home/deep/community.tar.gz 100%[=====] 330.36K 253KB/s in 1.3s  
2021-12-09 17:56:11 (253 KB/s) - '/home/deep/community.tar.gz' saved [338291/338291]  
deep@deep-VirtualBox:~/snort_src$
```

Ubuntu Clone [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

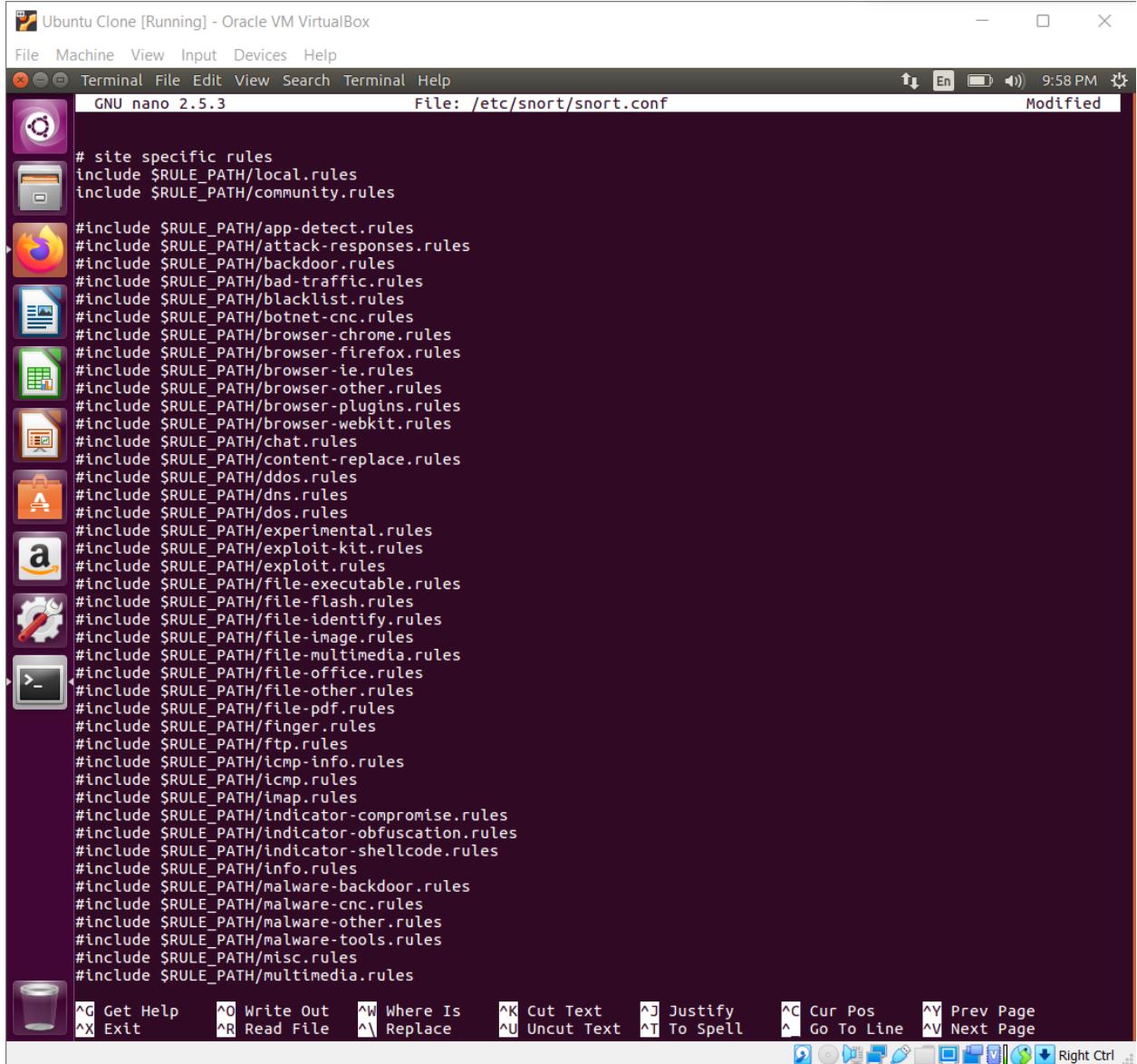
Terminal File Edit View Search Terminal Help

```
deep@deep-VirtualBox:~/snort_src/snort-2.9.19$ sudo mkdir /usr/local/lib/snort_dynamicrules
deep@deep-VirtualBox:~/snort_src/snort-2.9.19$ sudo chmod -R 5775 /etc/snort
deep@deep-VirtualBox:~/snort_src/snort-2.9.19$ sudo chmod -R 5775 /var/log/snort
deep@deep-VirtualBox:~/snort_src/snort-2.9.19$ sudo chmod -R 5775 /usr/local/lib/snort_dynamicrules
deep@deep-VirtualBox:~/snort_src/snort-2.9.19$ sudo chown -R snort:snort /etc/snort
deep@deep-VirtualBox:~/snort_src/snort-2.9.19$ sudo chown -R snort:snort /var/log/snort
deep@deep-VirtualBox:~/snort_src/snort-2.9.19$ sudo chown -R snort:snort /usr/local/lib/snort_dynamicrules
deep@deep-VirtualBox:~/snort_src/snort-2.9.19$ sudo touch /etc/snort/rules/white_list.rules
deep@deep-VirtualBox:~/snort_src/snort-2.9.19$ sudo touch /etc/snort/rules/black_list.rules
deep@deep-VirtualBox:~/snort_src/snort-2.9.19$ sudo cp ~/snort_src/snort-2.9.16/etc/*.conf* /etc/snort
cp: cannot stat '/home/deep/snort_src/snort-2.9.16/etc/*.*': No such file or directory
deep@deep-VirtualBox:~/snort_src/snort-2.9.19$ sudo cp ~/snort_src/snort-2.9.16/etc/*.map /etc/snort
cp: cannot stat '/home/deep/snort_src/snort-2.9.16/etc/*.*': No such file or directory
deep@deep-VirtualBox:~/snort_src/snort-2.9.19$ sudo cp ~/snort_src/snort-2.9.19/etc/*.conf* /etc/snort
deep@deep-VirtualBox:~/snort_src/snort-2.9.19$ sudo cp ~/snort_src/snort-2.9.19/etc/*.map /etc/snort
deep@deep-VirtualBox:~/snort_src/snort-2.9.19$ cd ..
deep@deep-VirtualBox:~/snort_src$ wget https://www.snort.org/rules/community -O ~/community.tar.gz
--2021-12-09 17:56:08-- https://www.snort.org/rules/community
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/000/021/754/original/community
-rules.tar.gz?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAU7AK5ITMGOEV4EFM%2F20211209%2Fus-east-1%2Fs
3%2Faws4_request&X-Amz-Date=20211209T122609Z&X-Amz-Expires=3600&X-Amz-SignedHeaders=host&X-Amz-Signature=00031a
5924e66c0c6304470ab2299f269c5c19f73caf5164d674f3c14f1a6ed0 [following]
--2021-12-09 17:56:09-- https://snort.org-site.s3.amazonaws.com/production/release_files/files/000/021/754/ori
ginal/community-rules.tar.gz?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAU7AK5ITMGOEV4EFM%2F20211209%
2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20211209T122609Z&X-Amz-Expires=3600&X-Amz-SignedHeaders=host&X-Amz-S
ignature=00031a5924e66c0c6304470ab2299f269c5c19f73caf5164d674f3c14f1a6ed0
Resolving snort.org-site.s3.amazonaws.com (snort.org-site.s3.amazonaws.com)... 52.217.173.89
Connecting to snort.org-site.s3.amazonaws.com (snort.org-site.s3.amazonaws.com)|52.217.173.89|:443... connected
.
HTTP request sent, awaiting response... 200 OK
Length: 338291 (330K) [application/gzip]
Saving to: '/home/deep/community.tar.gz'

/home/deep/community.tar.gz 100%[=====] 330.36K 253KB/s in 1.3s
2021-12-09 17:56:11 (253 KB/s) - '/home/deep/community.tar.gz' saved [338291/338291]

deep@deep-VirtualBox:~/snort_src$ sudo tar -xvf ~/community.tar.gz -C ~/
community-rules/
community-rules/community.rules
community-rules/VRT-License.txt
community-rules/LICENSE
community-rules/AUTHORS
community-rules/snort.conf
community-rules/sid-msg.map
deep@deep-VirtualBox:~/snort_src$ sudo cp ~/community-rules/* /etc/snort/rules
deep@deep-VirtualBox:~/snort_src$ sudo sed -i 's/include \$RULE\_PATH/#include \$RULE\_PATH/' /etc/snort/snort.
conf
deep@deep-VirtualBox:~/snort_src$
```

## Configuring Snort to look for whitelisted and blacklisted URLs and also listen to rules mentioned in community rules and local rules

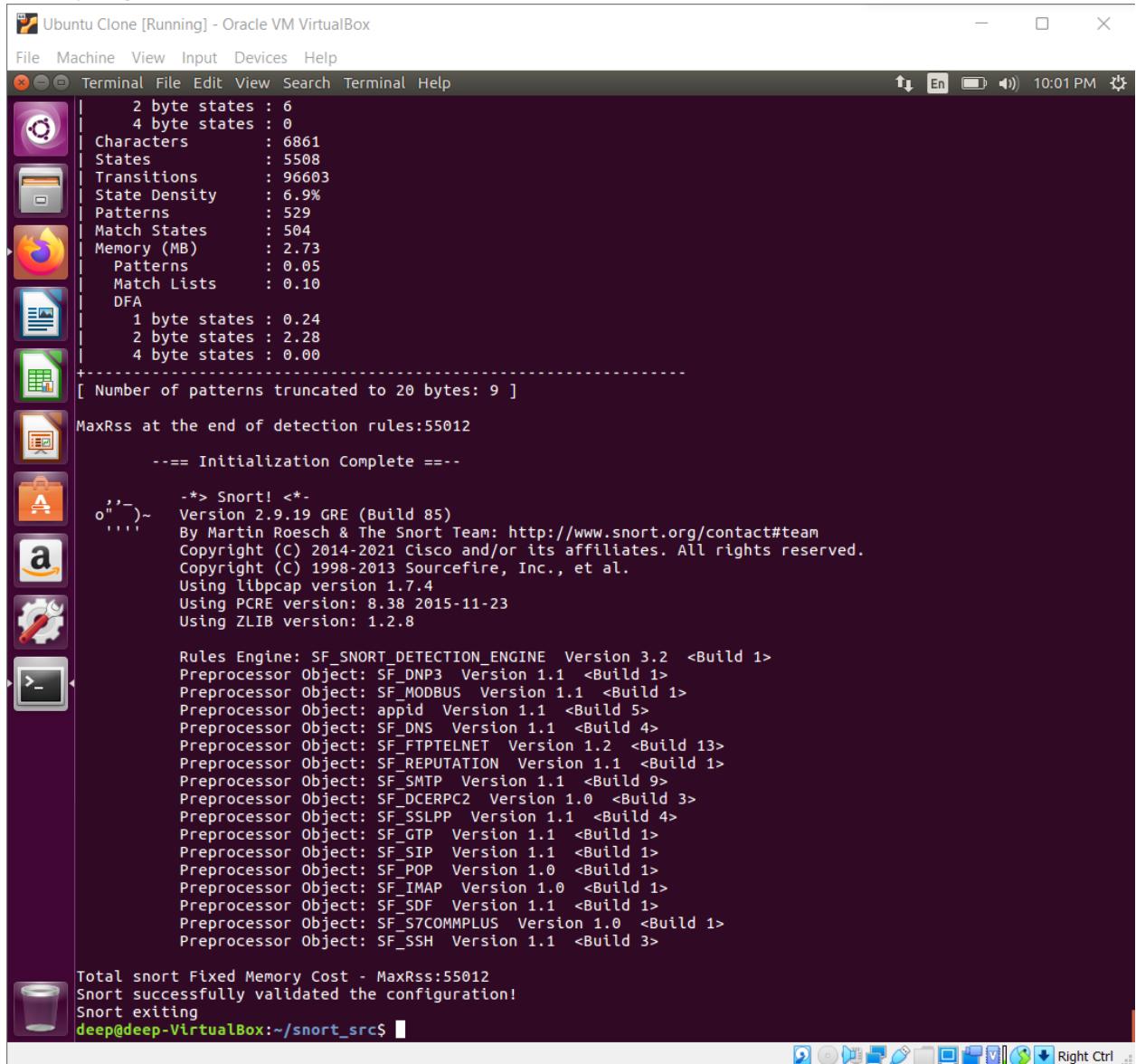


The screenshot shows a terminal window titled "Ubuntu Clone [Running] - Oracle VM VirtualBox". The window title bar includes standard icons for minimize, maximize, and close. The menu bar contains "File", "Machine", "View", "Input", "Devices", and "Help". The top right corner shows the system tray with icons for battery, signal strength, and volume, along with the time "9:58 PM". The main area of the terminal is a text editor titled "GNU nano 2.5.3" with the file path "File: /etc/snort/snort.conf". The text in the editor is a configuration file for Snort, specifically the "snort.conf" file. It contains numerous "#include \$RULE\_PATH/...rules" statements, which are used to include various rule sets such as app-detect.rules, attack-responses.rules, backdoor.rules, bad-traffic.rules, blacklist.rules, botnet-cnc.rules, browser-chrome.rules, browser-firefox.rules, browser-ie.rules, browser-other.rules, browser-plugins.rules, browser-webkit.rules, chat.rules, content-replace.rules, ddos.rules, dns.rules, dos.rules, experimental.rules, exploit-kit.rules, exploit.rules, file-executable.rules, file-flash.rules, file-identify.rules, file-image.rules, file-multimedia.rules, file-office.rules, file-other.rules, file-pdf.rules, finger.rules, ftp.rules, icmp-info.rules, icmp.rules, imap.rules, indicator-compromise.rules, indicator-obfuscation.rules, indicator-shellcode.rules, info.rules, malware-backdoor.rules, malware-cnc.rules, malware-other.rules, malware-tools.rules, misc.rules, and multimedia.rules. The bottom of the terminal window shows a series of keyboard shortcuts and icons for file operations like Get Help, Write Out, Where Is, Cut Text, Justify, Cur Pos, Prev Page, Exit, Read File, Replace, Uncut Text, To Spell, Go To Line, Next Page, and Right Ctrl.

```
# site specific rules
#include $RULE_PATH/local.rules
#include $RULE_PATH/community.rules

#include $RULE_PATH/app-detect.rules
#include $RULE_PATH/attack-responses.rules
#include $RULE_PATH/backdoor.rules
#include $RULE_PATH/bad-traffic.rules
#include $RULE_PATH/blacklist.rules
#include $RULE_PATH/botnet-cnc.rules
#include $RULE_PATH/browser-chrome.rules
#include $RULE_PATH/browser-firefox.rules
#include $RULE_PATH/browser-ie.rules
#include $RULE_PATH/browser-other.rules
#include $RULE_PATH/browser-plugins.rules
#include $RULE_PATH/browser-webkit.rules
#include $RULE_PATH/chat.rules
#include $RULE_PATH/content-replace.rules
#include $RULE_PATH/ddos.rules
#include $RULE_PATH/dns.rules
#include $RULE_PATH/dos.rules
#include $RULE_PATH/experimental.rules
#include $RULE_PATH/exploit-kit.rules
#include $RULE_PATH/exploit.rules
#include $RULE_PATH/file-executable.rules
#include $RULE_PATH/file-flash.rules
#include $RULE_PATH/file-identify.rules
#include $RULE_PATH/file-image.rules
#include $RULE_PATH/file-multimedia.rules
#include $RULE_PATH/file-office.rules
#include $RULE_PATH/file-other.rules
#include $RULE_PATH/file-pdf.rules
#include $RULE_PATH/finger.rules
#include $RULE_PATH/ftp.rules
#include $RULE_PATH/icmp-info.rules
#include $RULE_PATH/icmp.rules
#include $RULE_PATH/imap.rules
#include $RULE_PATH/indicator-compromise.rules
#include $RULE_PATH/indicator-obfuscation.rules
#include $RULE_PATH/indicator-shellcode.rules
#include $RULE_PATH/info.rules
#include $RULE_PATH/malware-backdoor.rules
#include $RULE_PATH/malware-cnc.rules
#include $RULE_PATH/malware-other.rules
#include $RULE_PATH/malware-tools.rules
#include $RULE_PATH/misc.rules
#include $RULE_PATH/multimedia.rules
```

## Verifying Snort Installation



The screenshot shows a terminal window titled "Ubuntu Clone [Running] - Oracle VM VirtualBox". The terminal displays the output of a Snort configuration validation command. The output includes statistics about byte states, character counts, transition counts, state density, and DFA metrics. It also shows the number of patterns truncated to 20 bytes (9). The Snort version information is displayed, including the build number (85), copyright details from 1998-2021, and the versions of libpcap, PCRE, and ZLIB used. The rules engine version is listed as 3.2. The terminal concludes with a message indicating successful validation and exiting.

```
2 byte states : 6
4 byte states : 0
Characters      : 6861
States          : 5508
Transitions     : 96603
State Density   : 6.9%
Patterns        : 529
Match States    : 504
Memory (MB)     : 2.73
  Patterns      : 0.05
  Match Lists   : 0.10
DFA
  1 byte states : 0.24
  2 byte states : 2.28
  4 byte states : 0.00
+-----[ Number of patterns truncated to 20 bytes: 9 ]
MaxRSS at the end of detection rules:55012
==== Initialization Complete ====
o'')~- -*> Snort! <*- Version 2.9.19 GRE (Build 85)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2021 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.7.4
Using PCRE version: 8.38 2015-11-23
Using ZLIB version: 1.2.8

Rules Engine: SF_SNORT_DETECTION_ENGINE Version 3.2 <Build 1>
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>
Preprocessor Object: appid Version 1.1 <Build 5>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
Preprocessor Object: SF_REPUTATION 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_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: SF_SDF Version 1.1 <Build 1>
Preprocessor Object: SF_S7COMMPLUS Version 1.0 <Build 1>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>

Total snort Fixed Memory Cost - MaxRSS:55012
Snort successfully validated the configuration!
Snort exiting
deep@deep-VirtualBox:~/snort_src$
```

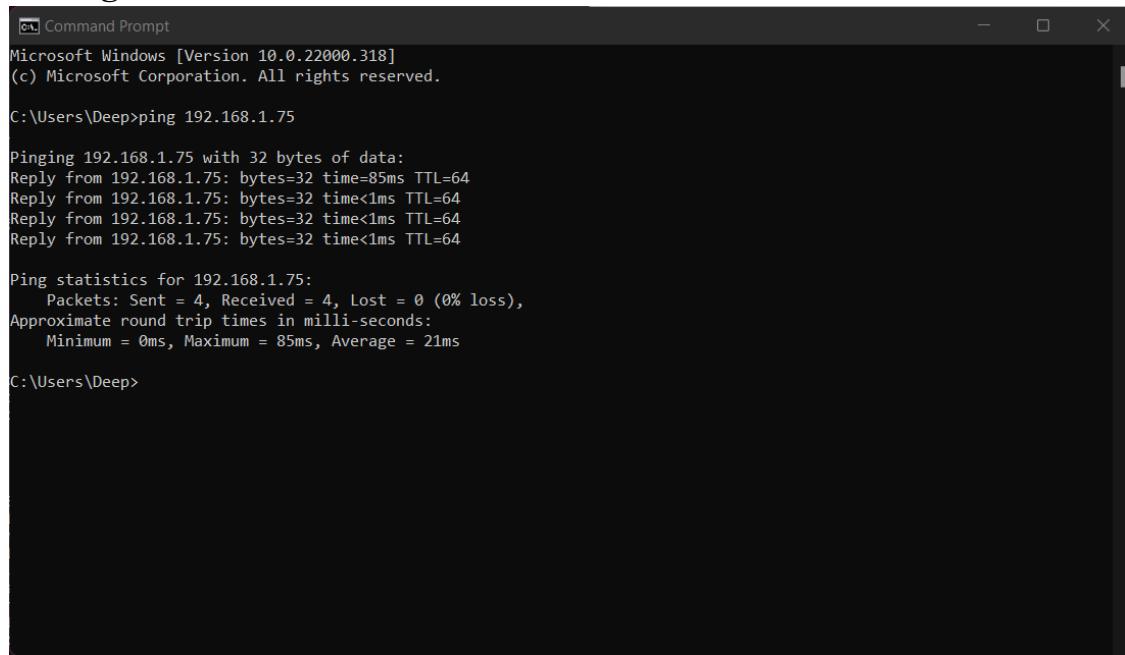
## Writing custom rule to check for any incoming ICMP Packet

The screenshot shows a Linux desktop environment with a terminal window open in the foreground. The terminal window is titled "deep@deep-VirtualBox: ~/snort\_src" and displays the command "GNU nano 2.5.3" followed by the file path "File: /etc/snort/rules/local.rules". Inside the terminal, there is a single line of text:

```
alert icmp any any -> $HOME_NET any (msg:"ICMP Packet found"; sid:10000001; rev:001;)
```

The terminal window has a dark background and a light-colored text area. At the bottom, there is a menu bar with various options like File, Machine, View, Input, Devices, Help, and a system tray with icons for battery, signal, and time (10:13 PM). Below the terminal window, the desktop environment is visible, featuring a vertical dock on the left containing icons for various applications such as a terminal, file manager, browser, and system tools. The desktop background is a dark purple color.

## Hitting IP Address of the Virtual Machine from the host machine



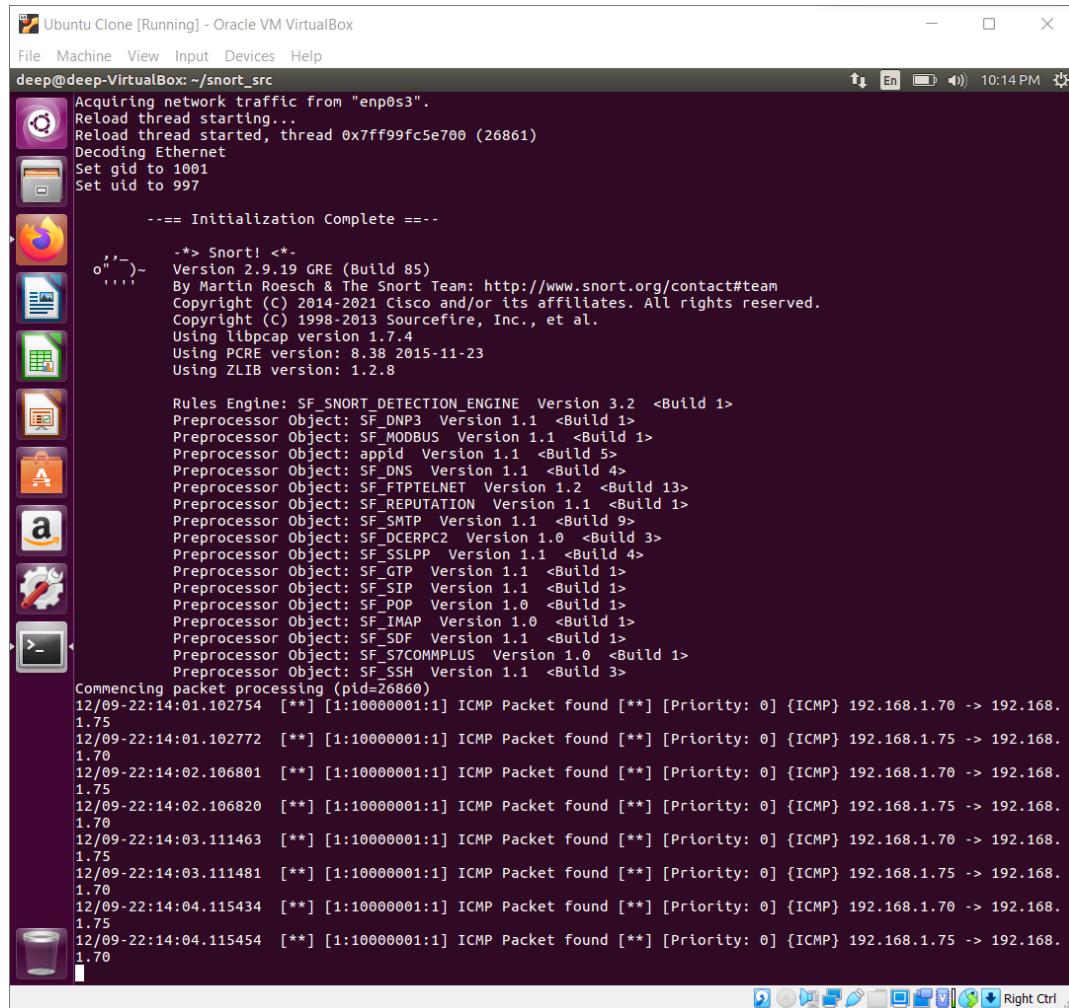
```
Command Prompt
Microsoft Windows [Version 10.0.22000.318]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Deep>ping 192.168.1.75

Pinging 192.168.1.75 with 32 bytes of data:
Reply from 192.168.1.75: bytes=32 time=85ms TTL=64
Reply from 192.168.1.75: bytes=32 time<1ms TTL=64
Reply from 192.168.1.75: bytes=32 time<1ms TTL=64
Reply from 192.168.1.75: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.75:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 85ms, Average = 21ms

C:\Users\Deep>
```



```
Ubuntu Clone [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
deep@deep-VirtualBox: ~/snort_src

Acquiring network traffic from "enp0s3".
Reload thread starting...
Reload thread started, thread 0x7ff99fc5e700 (26861)
Decoding Ethernet
Set gid to 1001
Set uid to 997

==== Initialization Complete ===

-> Snort! <*-
Version 2.9.19 GRE (Build 85)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2021 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.7.4
Using PCRE version: 8.38 2015-11-23
Using ZLIB version: 1.2.8

Rules Engine: SF_SNORT_DETECTION_ENGINE Version 3.2 <Build 1>
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>
Preprocessor Object: apid Version 1.1 <Build 5>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
Preprocessor Object: SF_REPUTATION 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_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: SF_SDF Version 1.1 <Build 1>
Preprocessor Object: SF_STCOMMPLUS Version 1.0 <Build 1>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>

Commencing packet processing (pid=26860)
12/09-22:14:01.102754 [**] [1:10000001:1] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.1.70 -> 192.168.1.75
12/09-22:14:01.102772 [**] [1:10000001:1] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.1.75 -> 192.168.1.70
12/09-22:14:02.106801 [**] [1:10000001:1] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.1.70 -> 192.168.1.75
12/09-22:14:02.106820 [**] [1:10000001:1] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.1.75 -> 192.168.1.70
12/09-22:14:03.111463 [**] [1:10000001:1] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.1.70 -> 192.168.1.75
12/09-22:14:03.111481 [**] [1:10000001:1] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.1.75 -> 192.168.1.70
12/09-22:14:04.115434 [**] [1:10000001:1] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.1.70 -> 192.168.1.75
12/09-22:14:04.115454 [**] [1:10000001:1] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.1.75 -> 192.168.1.70
```

## **1. What is a zero-day attack?**

- A zero-day assault occurs when a weakness, or software/hardware vulnerability, is exploited and attackers distribute malware before a patch can be created to correct the hole—hence the term "zero-day."
- In 2021, Google's Chrome suffered a series of zero-day threats, causing Chrome to issue updates. The vulnerability stemmed from a bug in the V8 JavaScript engine used in the web browser.
- Apple's iOS is often described as the most secure of the major smartphone platforms. However, in 2020, it fell victim to at least two sets of iOS zero-day vulnerabilities, including a zero-day bug that allowed attackers to compromise iPhones remotely.

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

- Snort works only on certain rule sets defined by the users.
- If a particular error is not bound by any rule set then any hacker can utilize it to perform a zero day attack on newly launched applications.
- However, snort is also very widely used and has multiple community rule sets that define most of the common vulnerabilities that an application might encounter.
- The results from a study show that 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).
- This proves that even though Snort is not fully capable of catching zero day attacks, it can be used to catch attacks of low level that can rule out basic bugs in a new application.

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

Number of attacks on the network = 0.1% of 1000000 = 1000 attacks

Number 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 off alarms.

Therefore, Number of true alarms = 950 alarms

Since 95% of the total alarms are attacks, Number of total alarms =  $(100 * 950) / 95 = 1000$  alarms

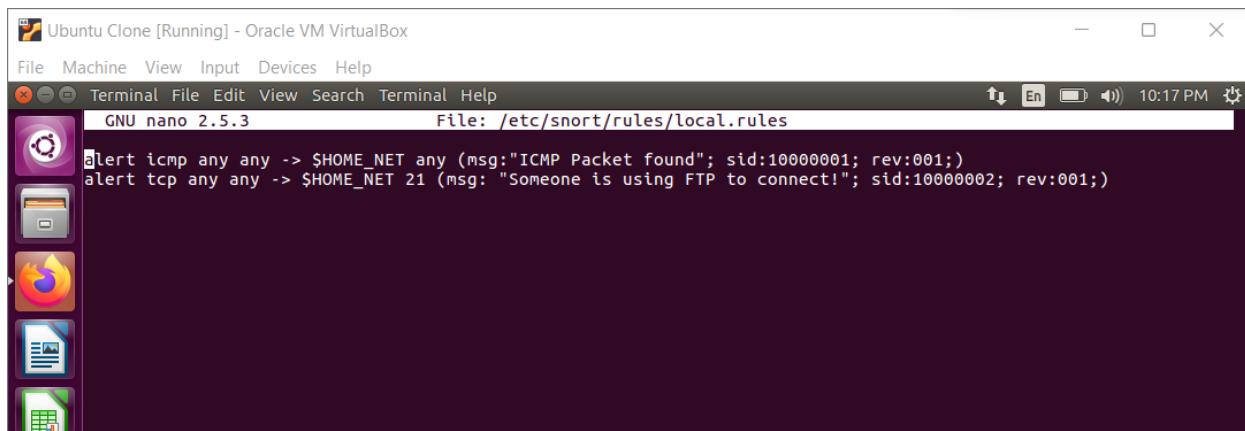
Therefore, Number of false alarms =  $1000 - 950 = 50$  alarms.

Therefore, False Alarm Rate =  $(\text{Number of false alarms} / \text{Total Benign Events}) * 100$

$= (50 / 999000) * 100 = 0.005\%$

- 4. Write and add another snort rule and trigger it**

### Writing custom Snort Rule to trigger whenever an incoming FTP connection is detected



The screenshot shows a terminal window titled "Ubuntu Clone [Running] - Oracle VM VirtualBox". The window contains a terminal session with the command "nano /etc/snort/rules/local.rules". The file is open in the nano editor, showing the following content:

```
alert icmp any any -> $HOME_NET any (msg:"ICMP Packet found"; sid:10000001; rev:001;)
alert tcp any any -> $HOME_NET 21 (msg: "Someone is using FTP to connect!"; sid:10000002; rev:001;)
```

The terminal window also displays a docked menu bar with icons for Home, File, Terminal, View, Search, and Help. The status bar at the bottom right shows the time as 10:17 PM.

## Trying to connect Host Machine to Virtual Machine using FTP

```
Command Prompt

C:\Users\Deep>ping 192.168.1.75

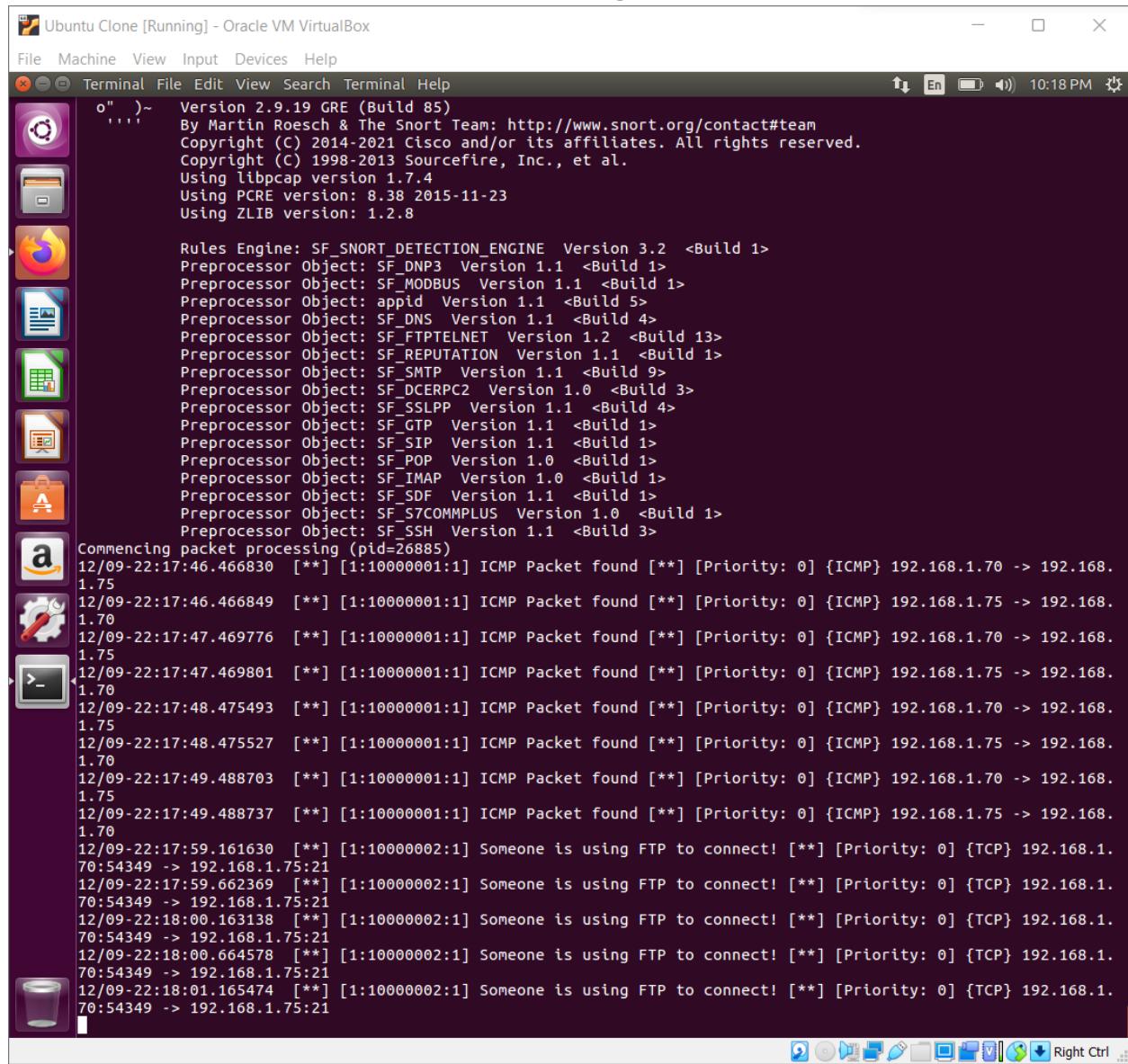
Pinging 192.168.1.75 with 32 bytes of data:
Reply from 192.168.1.75: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.75:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Deep>ftp 192.168.1.75
> ftp: connect :Connection refused
ftp> exit
Invalid command.
ftp> quit

C:\Users\Deep>
```

## Snort is able to detect all the incoming FTP connections

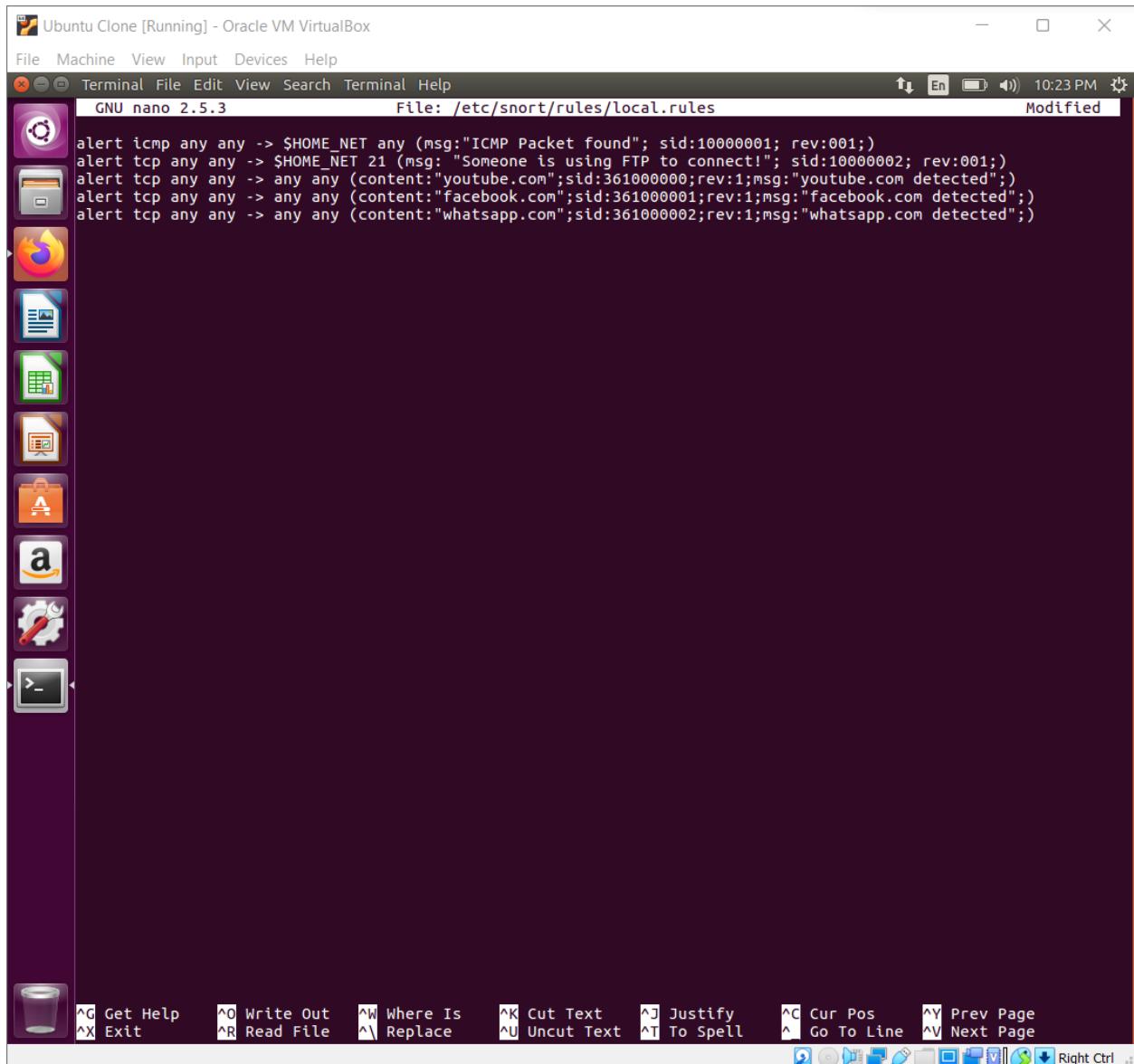


The screenshot shows a terminal window titled "Ubuntu Clone [Running] - Oracle VM VirtualBox". The terminal displays the Snort configuration and log output. The configuration includes details about the version (2.9.19 GRE (Build 85)), copyright information (by Martin Roesch & The Snort Team, 1998-2013 Sourcefire, Inc.), and various preprocessor objects. The log output shows multiple ICMP packets being processed, followed by several entries indicating incoming FTP connections from IP address 192.168.1.75 to 192.168.1.70.

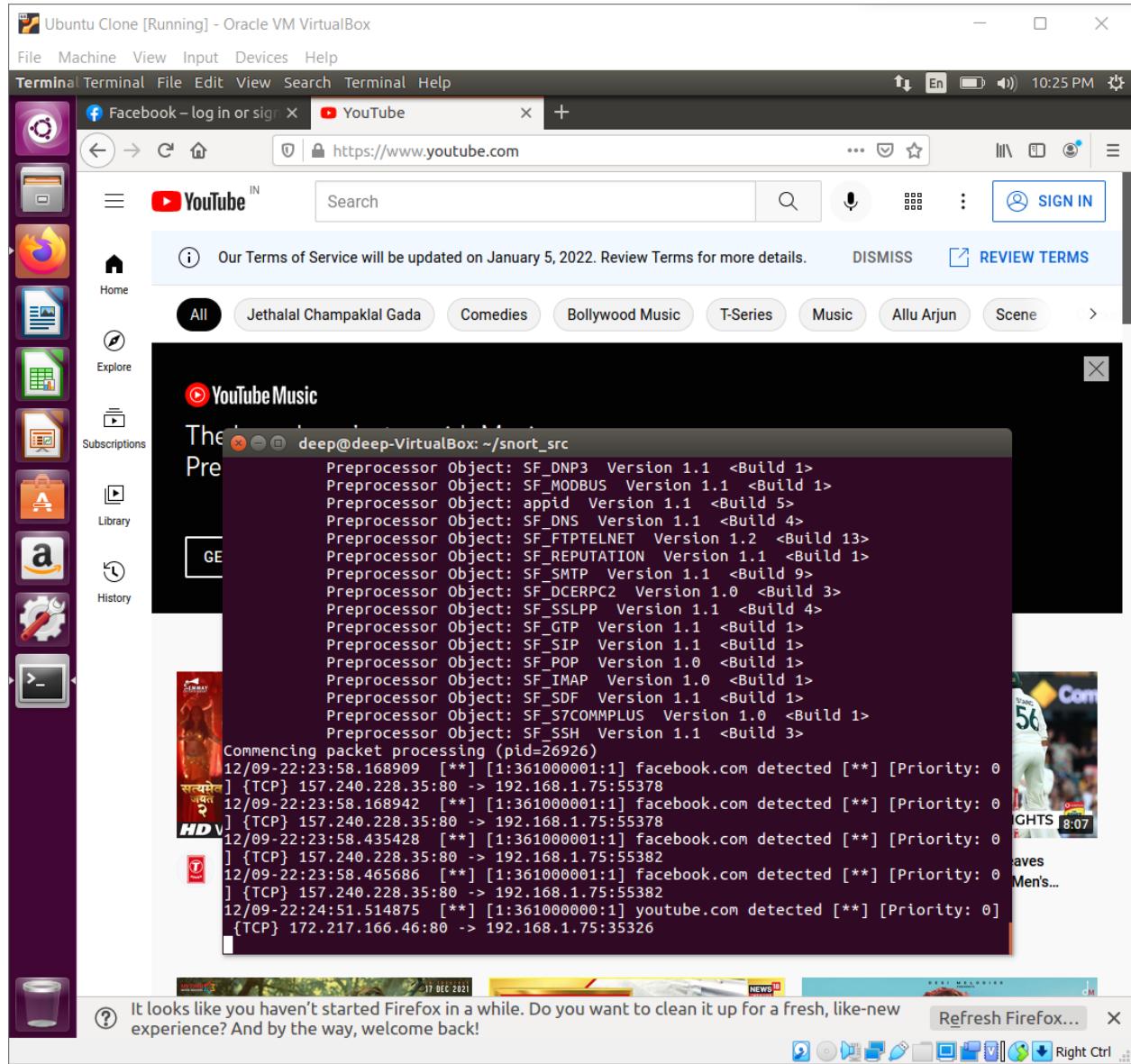
```
o" .~- Version 2.9.19 GRE (Build 85)
    ... By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
    Copyright (C) 2014-2021 Cisco and/or its affiliates. All rights reserved.
    Copyright (C) 1998-2013 Sourcefire, Inc., et al.
    Using libpcap version 1.7.4
    Using PCRE version: 8.38 2015-11-23
    Using ZLIB version: 1.2.8

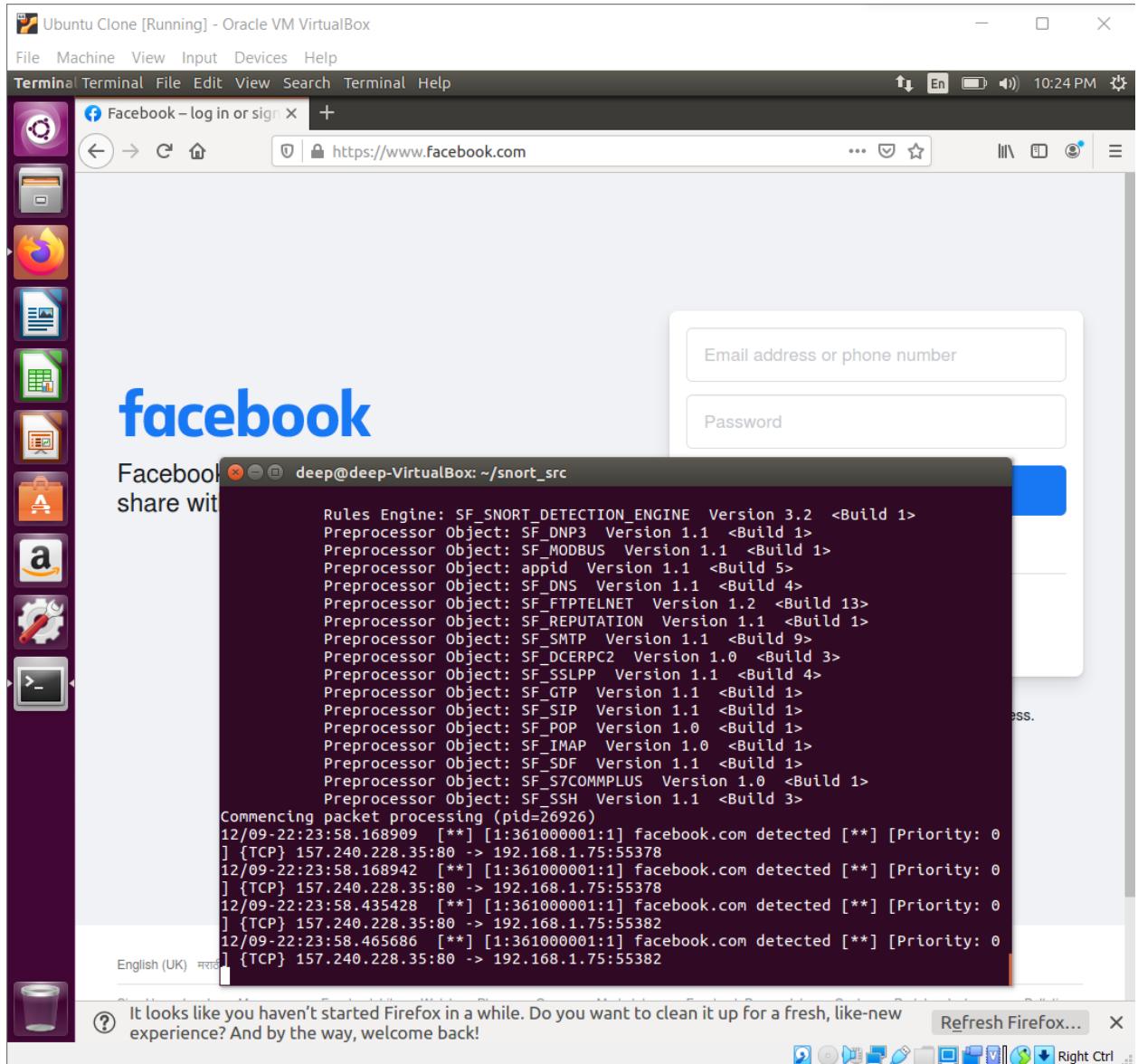
    Rules Engine: SF_SNORT_DETECTION_ENGINE Version 3.2 <Build 1>
    Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
    Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>
    Preprocessor Object: appid Version 1.1 <Build 5>
    Preprocessor Object: SF_DNS Version 1.1 <Build 4>
    Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
    Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
    Preprocessor Object: SF_SMB Version 1.1 <Build 9>
    Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>
    Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
    Preprocessor Object: SF_GTP Version 1.1 <Build 1>
    Preprocessor Object: SF_SIP Version 1.1 <Build 1>
    Preprocessor Object: SF_POP Version 1.0 <Build 1>
    Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
    Preprocessor Object: SF_SDF Version 1.1 <Build 1>
    Preprocessor Object: SF_S7COMMPLUS Version 1.0 <Build 1>
    Preprocessor Object: SF_SSH Version 1.1 <Build 3>

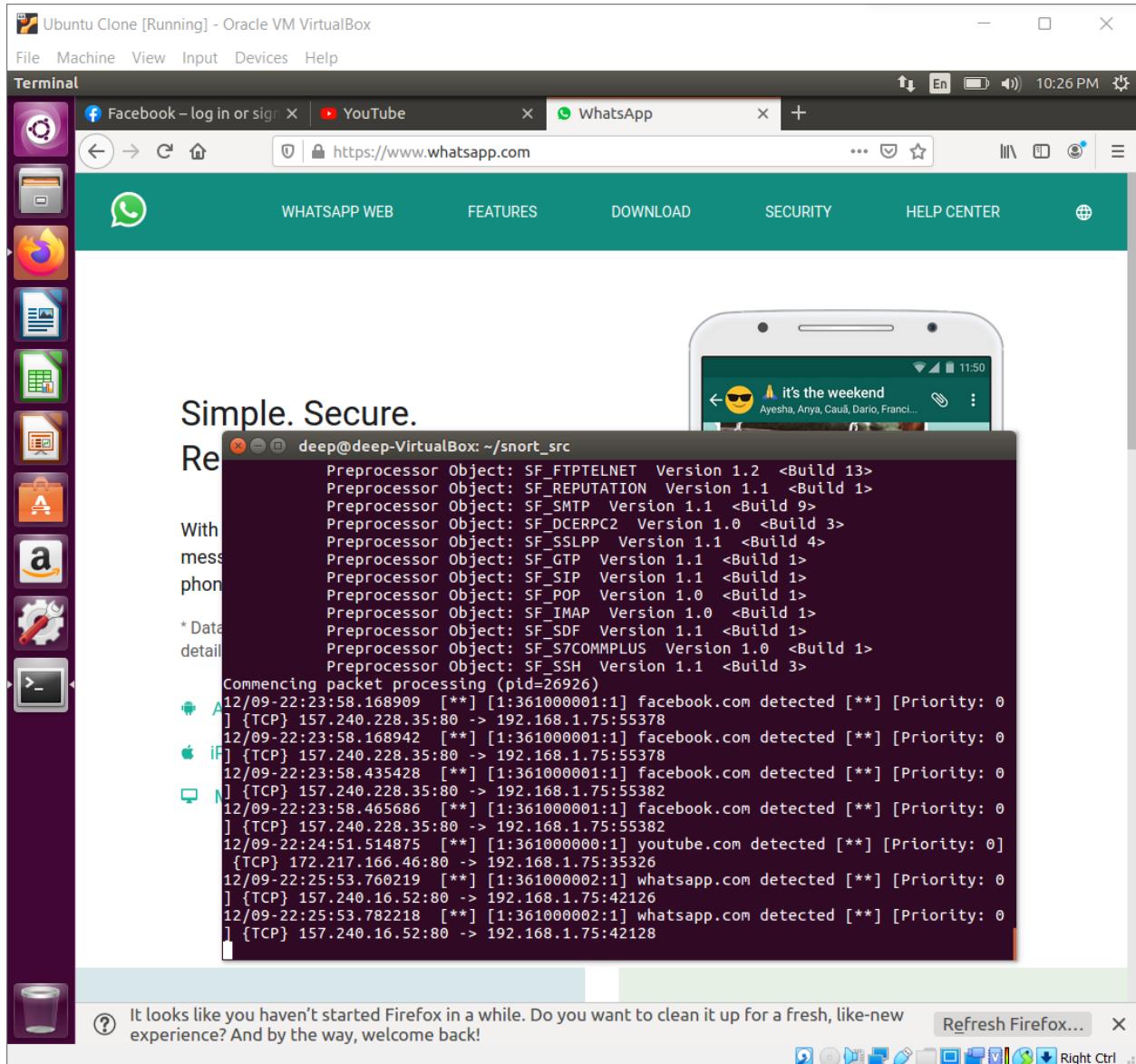
Commencing packet processing (pid=26885)
12/09-22:17:46.466830  [**] [1:10000001:1] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.1.70 -> 192.168.1.75
12/09-22:17:46.466849  [**] [1:10000001:1] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.1.75 -> 192.168.1.70
12/09-22:17:47.469776  [**] [1:10000001:1] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.1.70 -> 192.168.1.75
12/09-22:17:47.469801  [**] [1:10000001:1] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.1.75 -> 192.168.1.70
12/09-22:17:48.475493  [**] [1:10000001:1] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.1.70 -> 192.168.1.75
12/09-22:17:48.475527  [**] [1:10000001:1] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.1.75 -> 192.168.1.70
12/09-22:17:49.488703  [**] [1:10000001:1] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.1.70 -> 192.168.1.75
12/09-22:17:49.488737  [**] [1:10000001:1] ICMP Packet found [**] [Priority: 0] {ICMP} 192.168.1.75 -> 192.168.1.70
12/09-22:17:59.161630  [**] [1:10000002:1] Someone is using FTP to connect! [**] [Priority: 0] {TCP} 192.168.1.70:54349 -> 192.168.1.75:21
12/09-22:17:59.662369  [**] [1:10000002:1] Someone is using FTP to connect! [**] [Priority: 0] {TCP} 192.168.1.70:54349 -> 192.168.1.75:21
12/09-22:18:00.163138  [**] [1:10000002:1] Someone is using FTP to connect! [**] [Priority: 0] {TCP} 192.168.1.70:54349 -> 192.168.1.75:21
12/09-22:18:00.664578  [**] [1:10000002:1] Someone is using FTP to connect! [**] [Priority: 0] {TCP} 192.168.1.70:54349 -> 192.168.1.75:21
12/09-22:18:01.165474  [**] [1:10000002:1] Someone is using FTP to connect! [**] [Priority: 0] {TCP} 192.168.1.70:54349 -> 192.168.1.75:21
```



## Detecting if any custom website is being accessed by any user







## Conclusion:

1. Snort IDS is a robust and convenient application that can be easily configured to monitor any network traffic on a particular device and prevent basic attacks from happening.
2. Although Snort is not fully equipped to detect zero day attacks, thanks to the community rule sets, many of the basic vulnerabilities of basic applications are ruled out providing help to some extent.

3. Through this experiment I learnt to install and configure Snort to analyze incoming ICMP packets, TCP Packets and filter them based on the URL, Port Number as well as IP Address.

**Github Link:**

<https://github.com/deepnayak/CSS-Lab-Deep-Nayak/tree/master/Experiment%206>