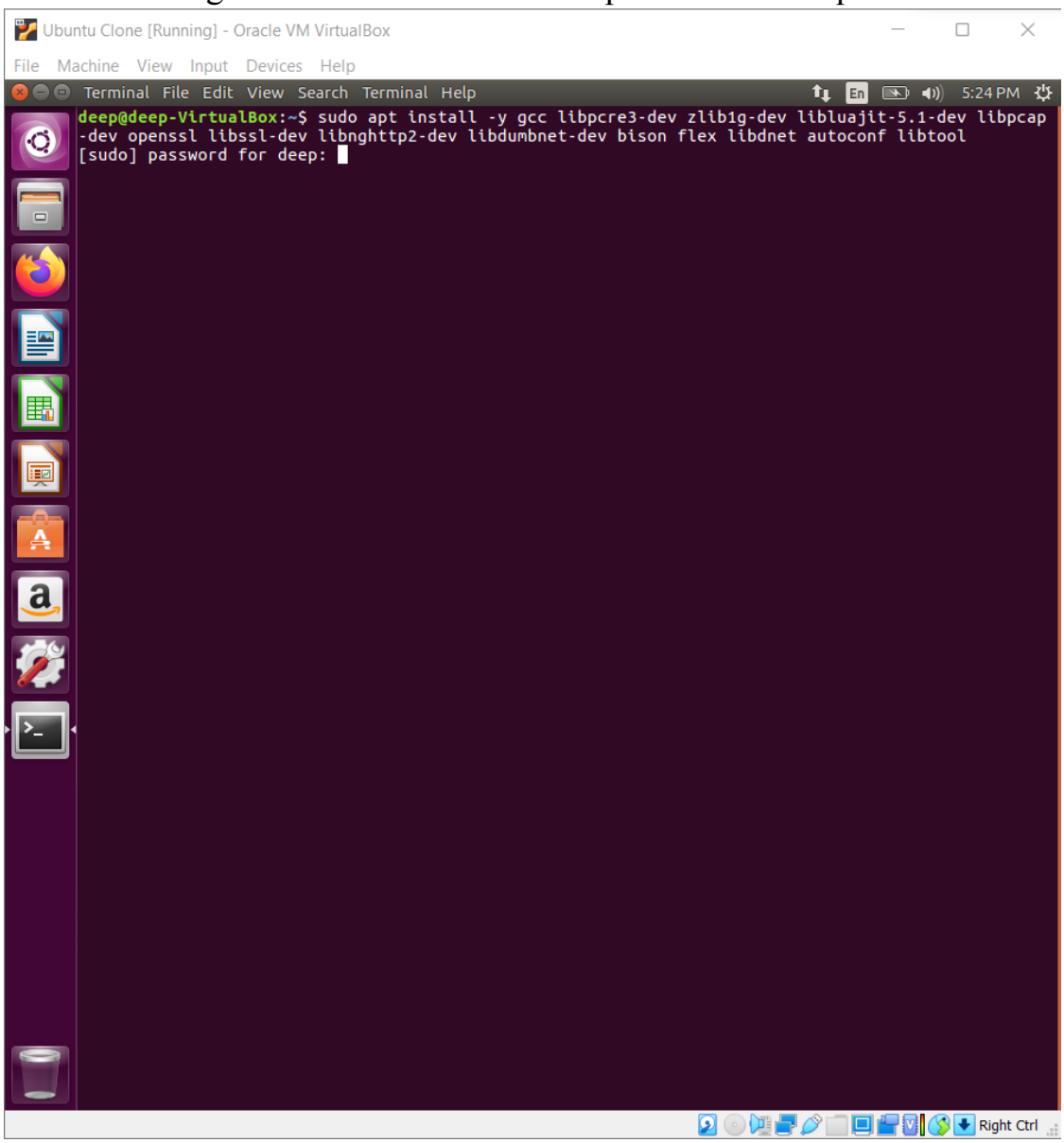
Experiment 6: Firewall and Intrusion Detection System

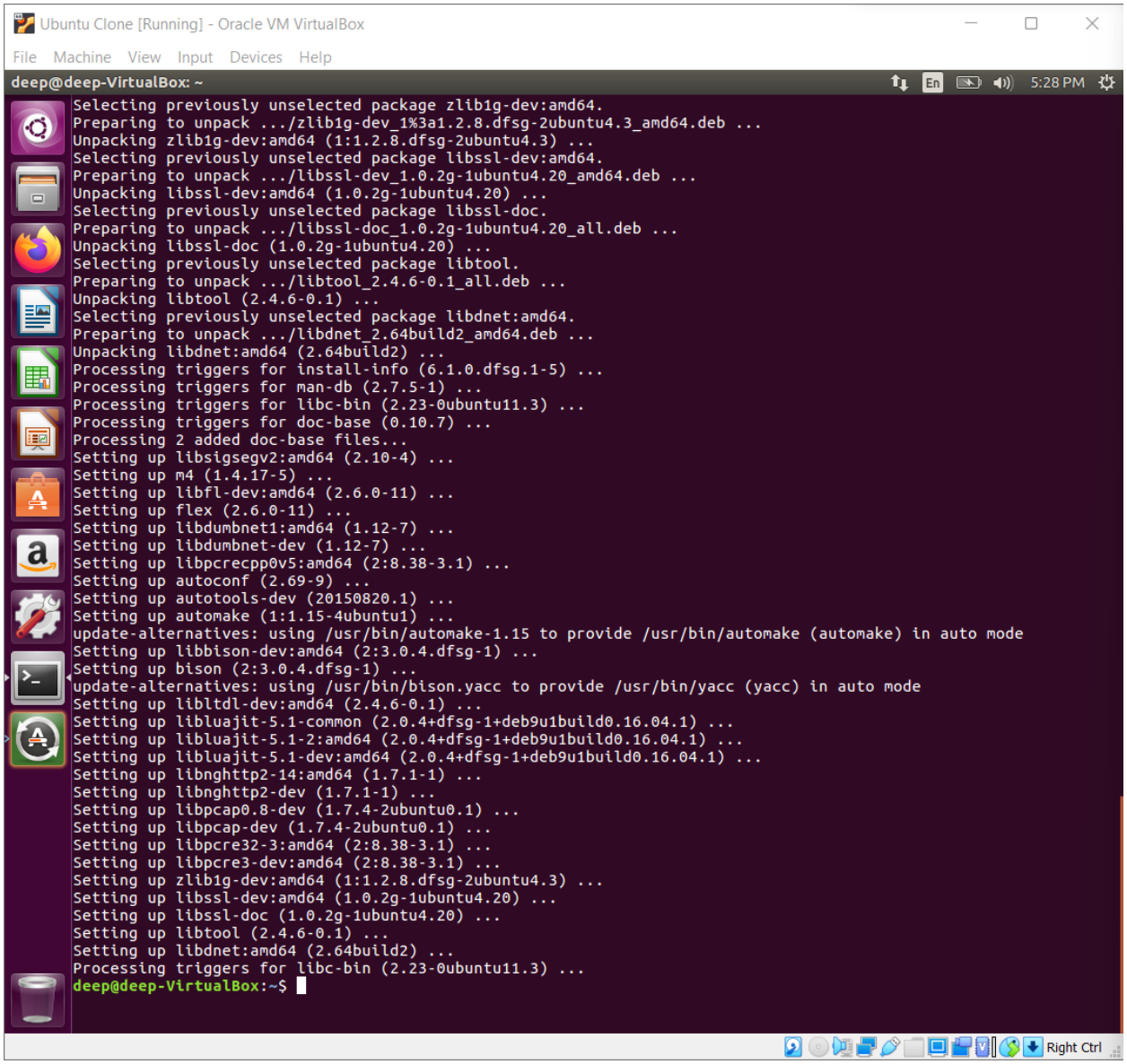
Name: Deep Nayak **UID**: 2019130045 TE COMPS

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.

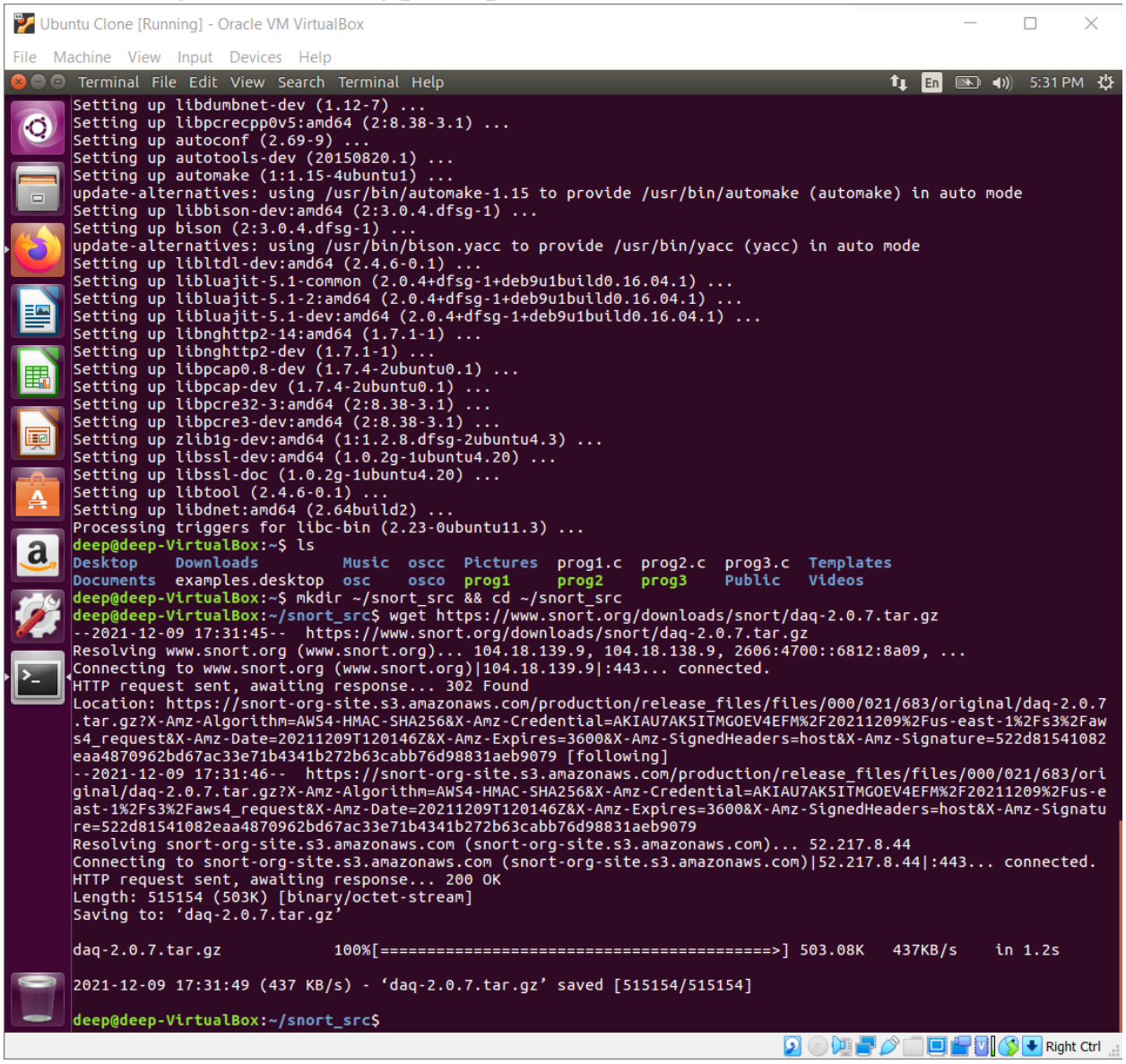
OUTPUT :

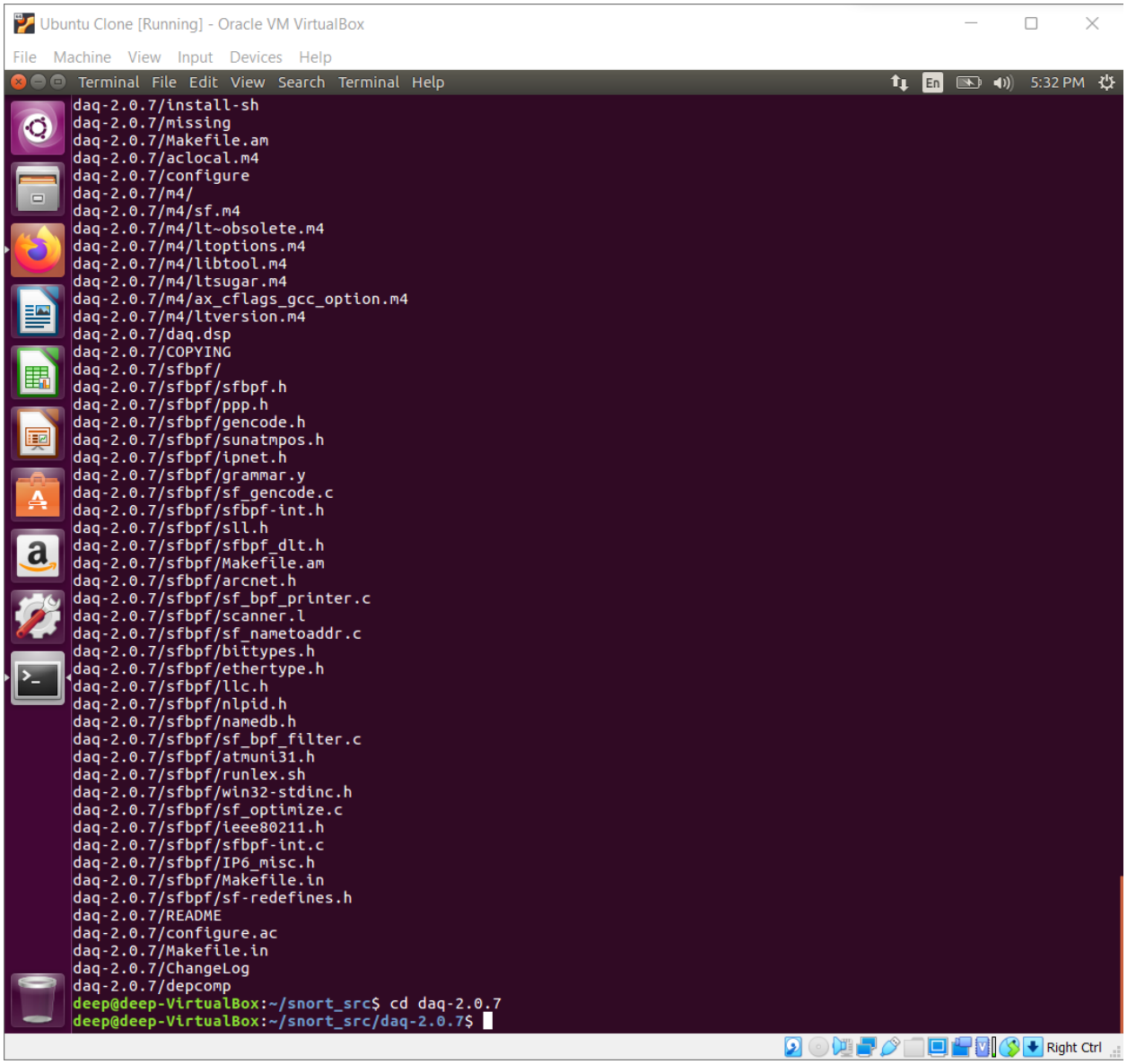
- Installing Snort and various other dependencies it requires.

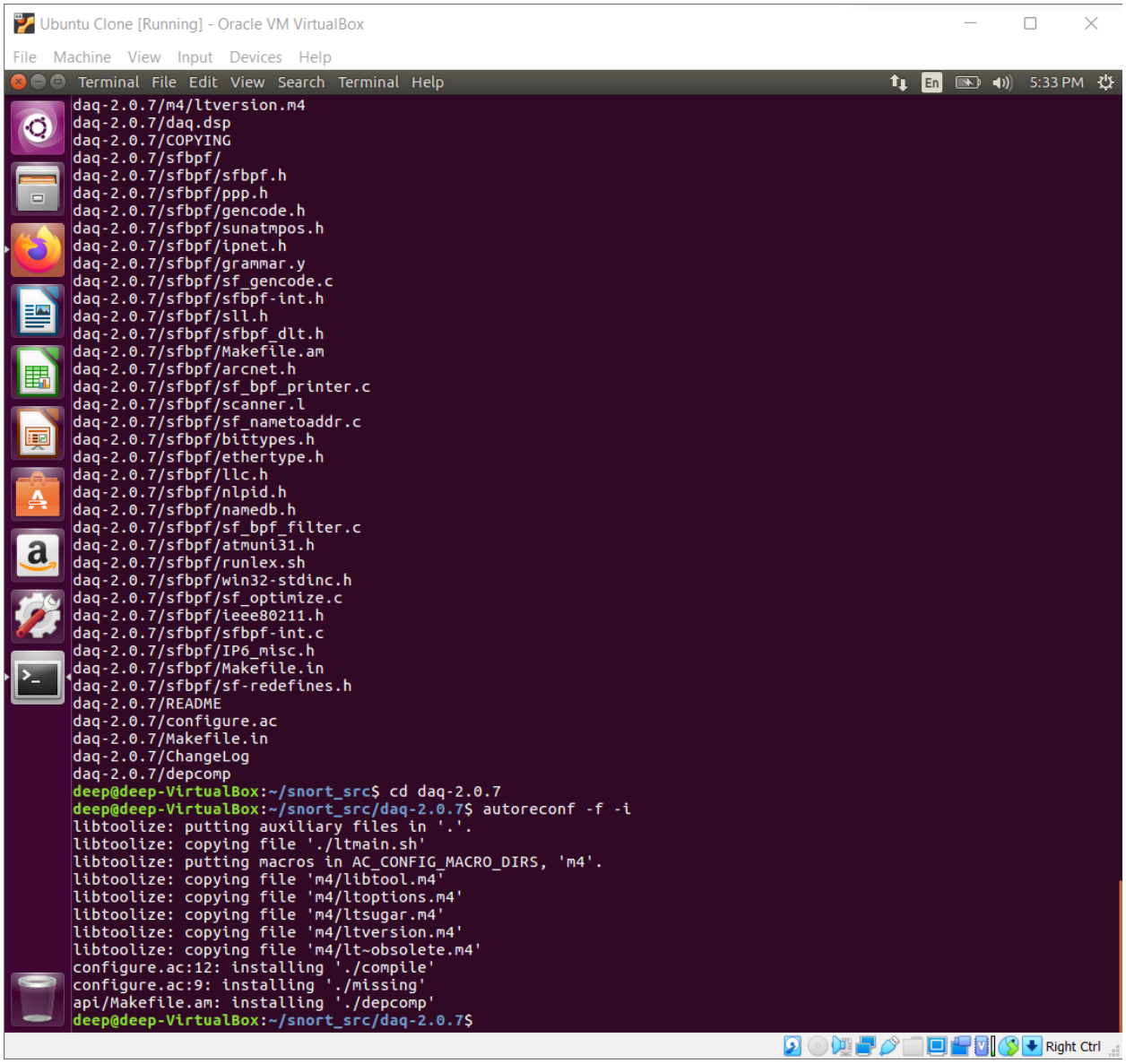


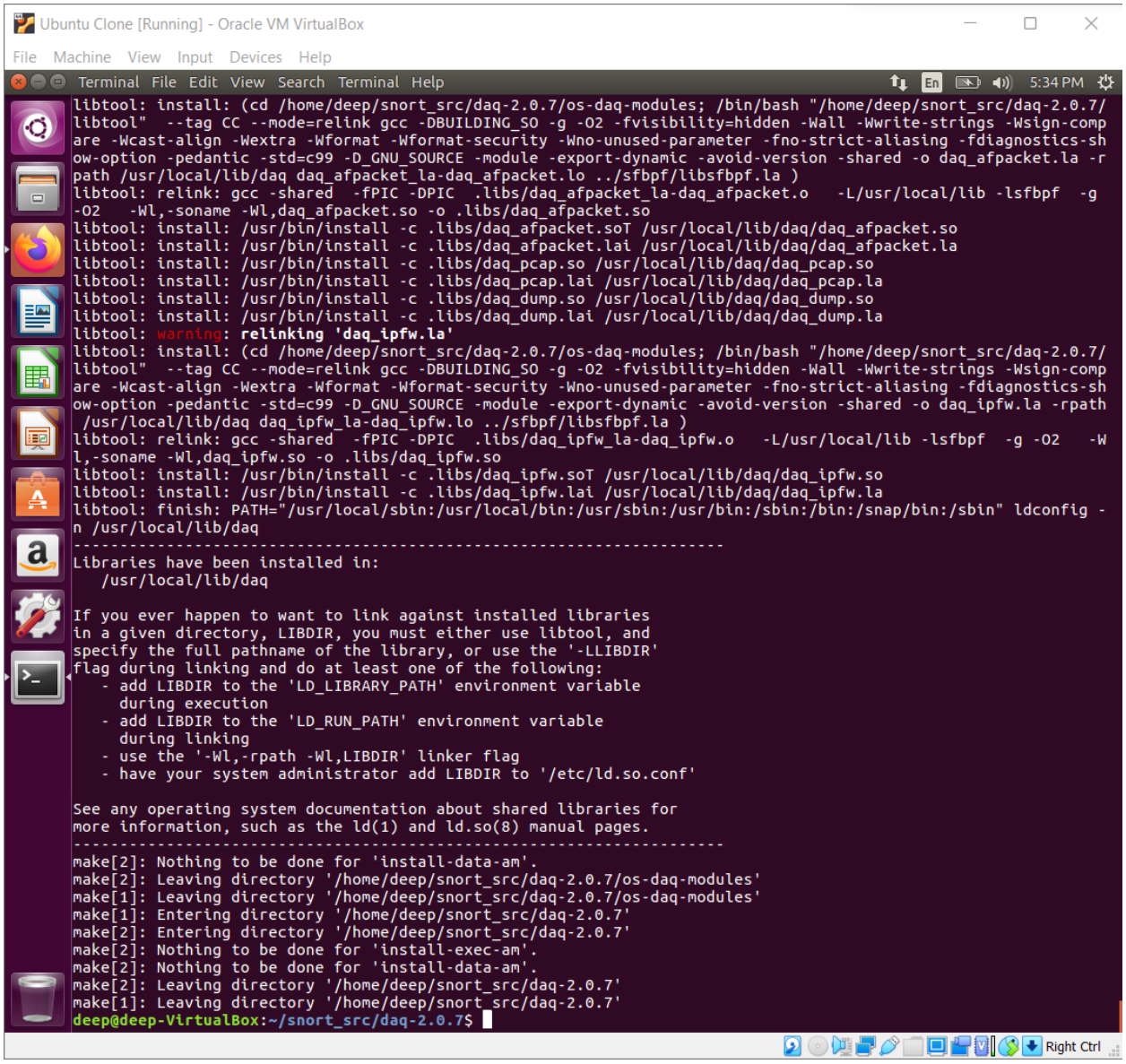

Ubuntu Clone [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
deep@deep-VirtualBox: ~
5:28 PM
Selecting previously unselected package zlib1g-dev:amd64.
Preparing to unpack .../zlib1g-dev_1%3a1.2.8.dfsg-2ubuntu4.3_amd64.deb ...
Unpacking zlib1g-dev:amd64 (1:1.2.8.dfsg-2ubuntu4.3) ...
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 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 libnghttp2-14:amd64 (1.7.1-1) ...
Setting up libnghttp2-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:~$
Right Ctrl

Downloading and installing prerequisites for Snort

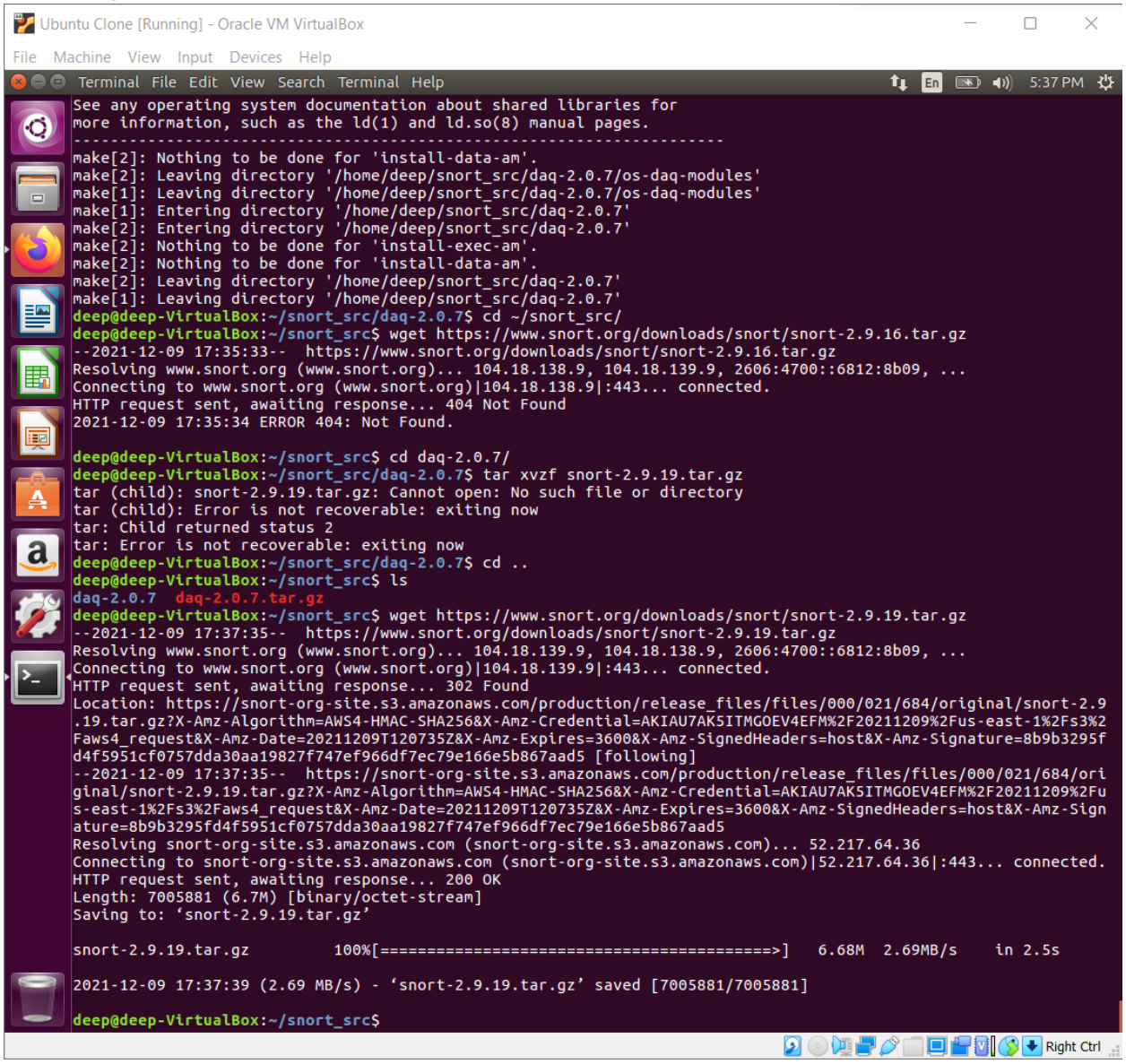


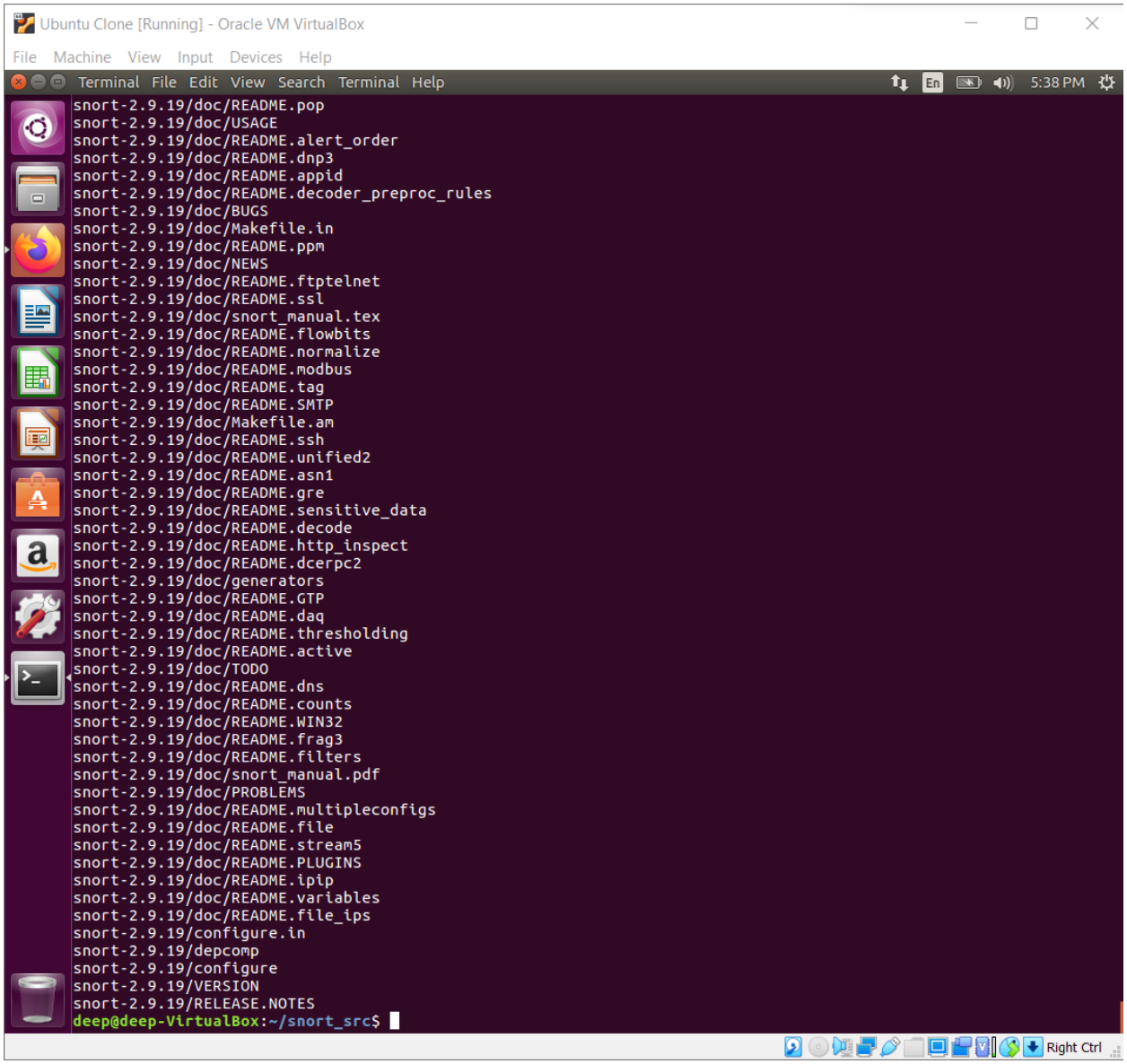

Ubuntu Clone [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal File Edit View Search Terminal Help
5:32 PM
daq-2.0.7/install-sh
daq-2.0.7/missing
daq-2.0.7/Makefile.am
daq-2.0.7/aclocal.m4
daq-2.0.7/configure
daq-2.0.7/m4/
daq-2.0.7/m4/sf.m4
daq-2.0.7/m4/lt~obsolete.m4
daq-2.0.7/m4/ltoptions.m4
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
daq-2.0.7/sfbpf/ppp.h
daq-2.0.7/sfbpf/gencode.h
daq-2.0.7/sfbpf/sunatmpos.h
daq-2.0.7/sfbpf/ipnet.h
daq-2.0.7/sfbpf/grammar.y
daq-2.0.7/sfbpf/sf_gencode.c
daq-2.0.7/sfbpf/sfbpf-int.h
daq-2.0.7/sfbpf/sll.h
daq-2.0.7/sfbpf/sfbpf_dlt.h
daq-2.0.7/sfbpf/Makefile.am
daq-2.0.7/sfbpf/arcnet.h
daq-2.0.7/sfbpf/sf_bpf_printer.c
daq-2.0.7/sfbpf/scanner.l
daq-2.0.7/sfbpf/sf_nametoaddr.c
daq-2.0.7/sfbpf/bittypes.h
daq-2.0.7/sfbpf/ethertype.h
daq-2.0.7/sfbpf/llc.h
daq-2.0.7/sfbpf/nlpid.h
daq-2.0.7/sfbpf/namedb.h
daq-2.0.7/sfbpf/sf_bpf_filter.c
daq-2.0.7/sfbpf/atmuni31.h
daq-2.0.7/sfbpf/runlex.sh
daq-2.0.7/sfbpf/win32-stdinc.h
daq-2.0.7/sfbpf/sf_optimize.c
daq-2.0.7/sfbpf/ieee80211.h
daq-2.0.7/sfbpf/sfbpf-int.c
daq-2.0.7/sfbpf/IP6_misc.h
daq-2.0.7/sfbpf/Makefile.in
daq-2.0.7/sfbpf/sf-redefines.h
daq-2.0.7/README
daq-2.0.7/configure.ac
daq-2.0.7/Makefile.in
daq-2.0.7/ChangeLog
daq-2.0.7/depcomp
deep@deep-VirtualBox:~/snort_src$ cd daq-2.0.7
deep@deep-VirtualBox:~/snort_src/daq-2.0.7$
Right Ctrl

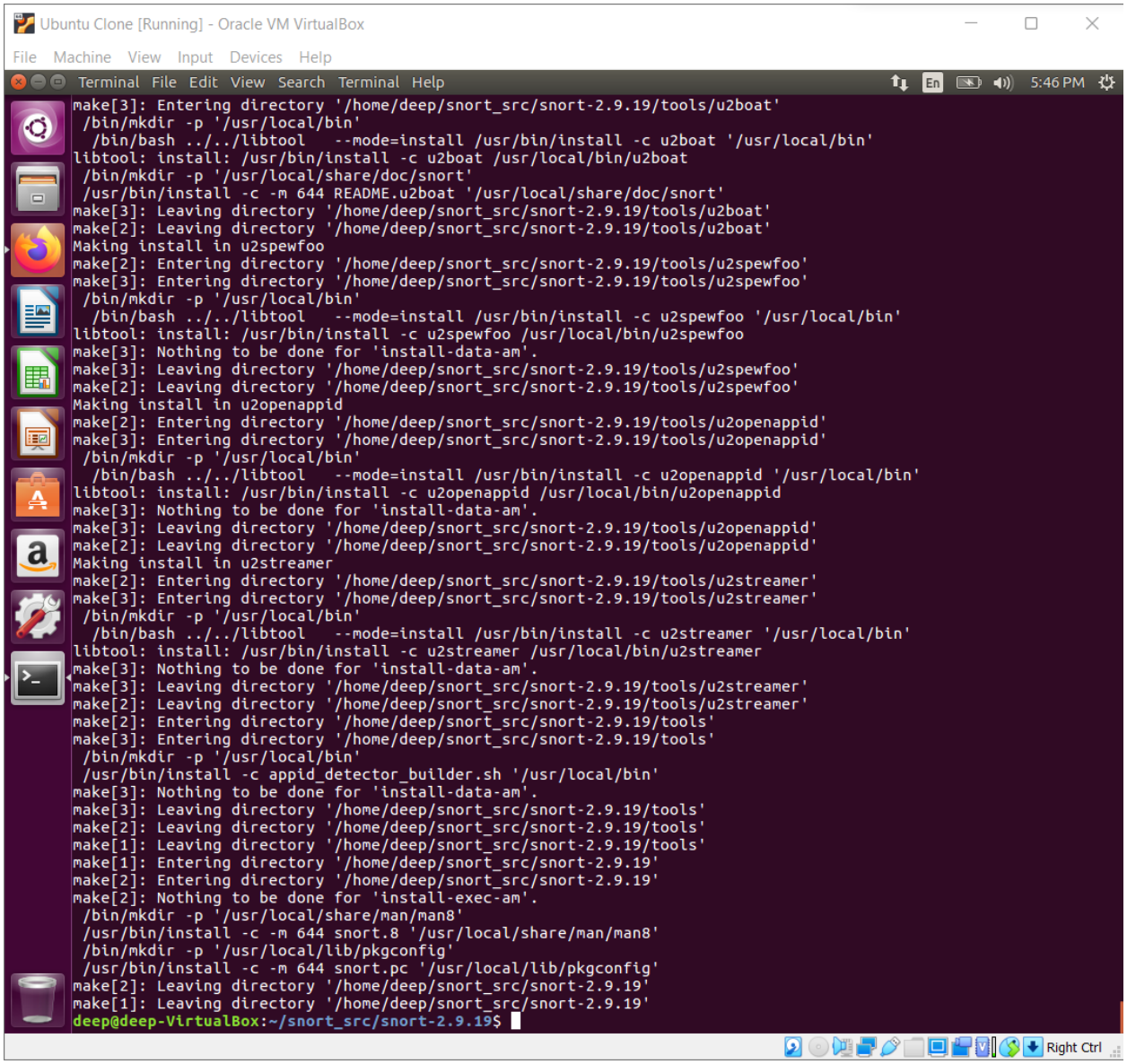

Ubuntu Clone [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal File Edit View Search Terminal Help
5:33 PM
daq-2.0.7/m4/ltversion.m4
daq-2.0.7/daq.dsp
daq-2.0.7/COPYING
daq-2.0.7/sfbpf/
daq-2.0.7/sfbpf/sfbpf.h
daq-2.0.7/sfbpf/ppp.h
daq-2.0.7/sfbpf/gencode.h
daq-2.0.7/sfbpf/sunatmpos.h
daq-2.0.7/sfbpf/ipnet.h
daq-2.0.7/sfbpf/grammar.y
daq-2.0.7/sfbpf/sf_gencode.c
daq-2.0.7/sfbpf/sfbpf-int.h
daq-2.0.7/sfbpf/sll.h
daq-2.0.7/sfbpf/sfbpf_dlt.h
daq-2.0.7/sfbpf/Makefile.am
daq-2.0.7/sfbpf/arcnet.h
daq-2.0.7/sfbpf/sf_bpf_printer.c
daq-2.0.7/sfbpf/scanner.l
daq-2.0.7/sfbpf/sf_nametoaddr.c
daq-2.0.7/sfbpf/bittypes.h
daq-2.0.7/sfbpf/ethertype.h
daq-2.0.7/sfbpf/llc.h
daq-2.0.7/sfbpf/nlpid.h
daq-2.0.7/sfbpf/namedb.h
daq-2.0.7/sfbpf/sf_bpf_filter.c
daq-2.0.7/sfbpf/atmuni31.h
daq-2.0.7/sfbpf/runlex.sh
daq-2.0.7/sfbpf/win32-stdinc.h
daq-2.0.7/sfbpf/sf_optimize.c
daq-2.0.7/sfbpf/ieee80211.h
daq-2.0.7/sfbpf/sfbpf-int.c
daq-2.0.7/sfbpf/IP6_misc.h
daq-2.0.7/sfbpf/Makefile.in
daq-2.0.7/sfbpf/sf-redefines.h
daq-2.0.7/README
daq-2.0.7/configure.ac
daq-2.0.7/Makefile.in
daq-2.0.7/ChangeLog
daq-2.0.7/depcomp
deep@deep-VirtualBox:~/snort_src$ cd daq-2.0.7
deep@deep-VirtualBox:~/snort_src/daq-2.0.7$ autoreconf -f -i
libtoolize: putting auxiliary files in '.'.
libtoolize: copying file './ltmain.sh'
libtoolize: putting macros in AC_CONFIG_MACRO_DIRS, 'm4'.
libtoolize: copying file 'm4/libtool.m4'
libtoolize: copying file 'm4/ltoptions.m4'
libtoolize: copying file 'm4/ltsugar.m4'
libtoolize: copying file 'm4/ltversion.m4'
libtoolize: copying file 'm4/lt~obsolete.m4'
configure.ac:12: installing './compile'
configure.ac:9: installing './missing'
api/Makefile.am: installing './depcomp'
deep@deep-VirtualBox:~/snort_src/daq-2.0.7$
Right Ctrl


Ubuntu Clone [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal File Edit View Search Terminal Help
5:34 PM
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_pcap.so /usr/local/lib/daq/daq_pcap.so
libtool: install: /usr/bin/install -c .libs/daq_pcap.lai /usr/local/lib/daq/daq_pcap.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:/sbin:/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$
Right Ctrl

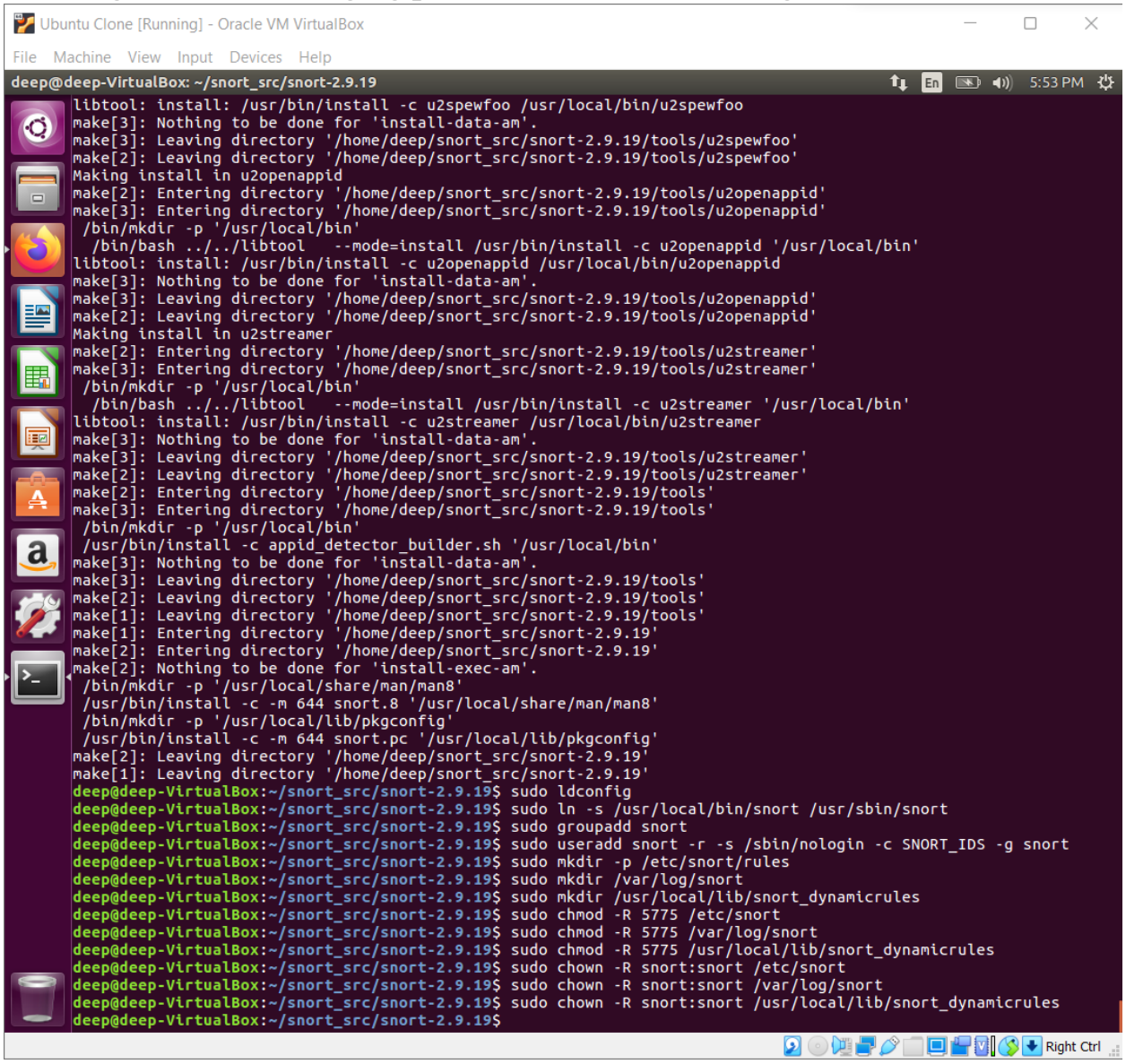
Building Snort from its source



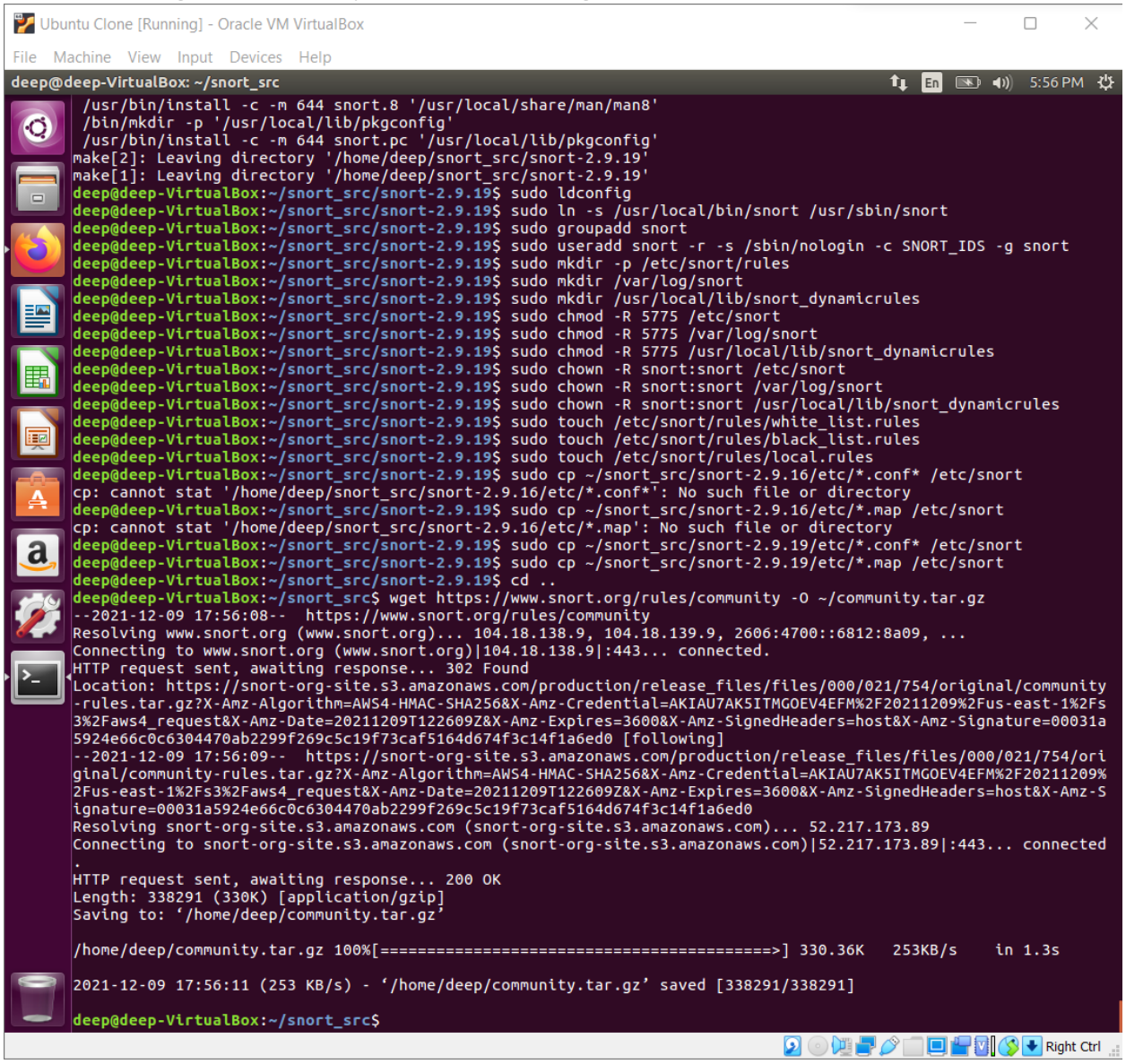

Ubuntu Clone [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal File Edit View Search Terminal Help
5:38 PM
snort-2.9.19/doc/README.pop
snort-2.9.19/doc/USAGE
snort-2.9.19/doc/README.alert_order
snort-2.9.19/doc/README.dnp3
snort-2.9.19/doc/README.appid
snort-2.9.19/doc/README.decoder_preproc_rules
snort-2.9.19/doc/BUGS
snort-2.9.19/doc/Makefile.in
snort-2.9.19/doc/README.ppm
snort-2.9.19/doc/NEWS
snort-2.9.19/doc/README.ftptelnet
snort-2.9.19/doc/README.ssl
snort-2.9.19/doc/snort_manual.tex
snort-2.9.19/doc/README.flowbits
snort-2.9.19/doc/README.normalize
snort-2.9.19/doc/README.modbus
snort-2.9.19/doc/README.tag
snort-2.9.19/doc/README.SMTP
snort-2.9.19/doc/Makefile.am
snort-2.9.19/doc/README.ssh
snort-2.9.19/doc/README.unified2
snort-2.9.19/doc/README.asn1
snort-2.9.19/doc/README.gre
snort-2.9.19/doc/README.sensitive_data
snort-2.9.19/doc/README.decode
snort-2.9.19/doc/README.http_inspect
snort-2.9.19/doc/README.dcerpc2
snort-2.9.19/doc/generators
snort-2.9.19/doc/README.GTP
snort-2.9.19/doc/README.daq
snort-2.9.19/doc/README.thresholding
snort-2.9.19/doc/README.active
snort-2.9.19/doc/TODO
snort-2.9.19/doc/README.dns
snort-2.9.19/doc/README.counts
snort-2.9.19/doc/README.WIN32
snort-2.9.19/doc/README.frag3
snort-2.9.19/doc/README.filters
snort-2.9.19/doc/snort_manual.pdf
snort-2.9.19/doc/PROBLEMS
snort-2.9.19/doc/README.multipleconfigs
snort-2.9.19/doc/README.file
snort-2.9.19/doc/README.stream5
snort-2.9.19/doc/README.PLUGINS
snort-2.9.19/doc/README.ipip
snort-2.9.19/doc/README.variables
snort-2.9.19/doc/README.file_ips
snort-2.9.19/configure.in
snort-2.9.19/depcomp
snort-2.9.19/configure
snort-2.9.19/VERSION
snort-2.9.19/RELEASE.NOTES
deep@deep-VirtualBox:~/snort_src$
Right Ctrl

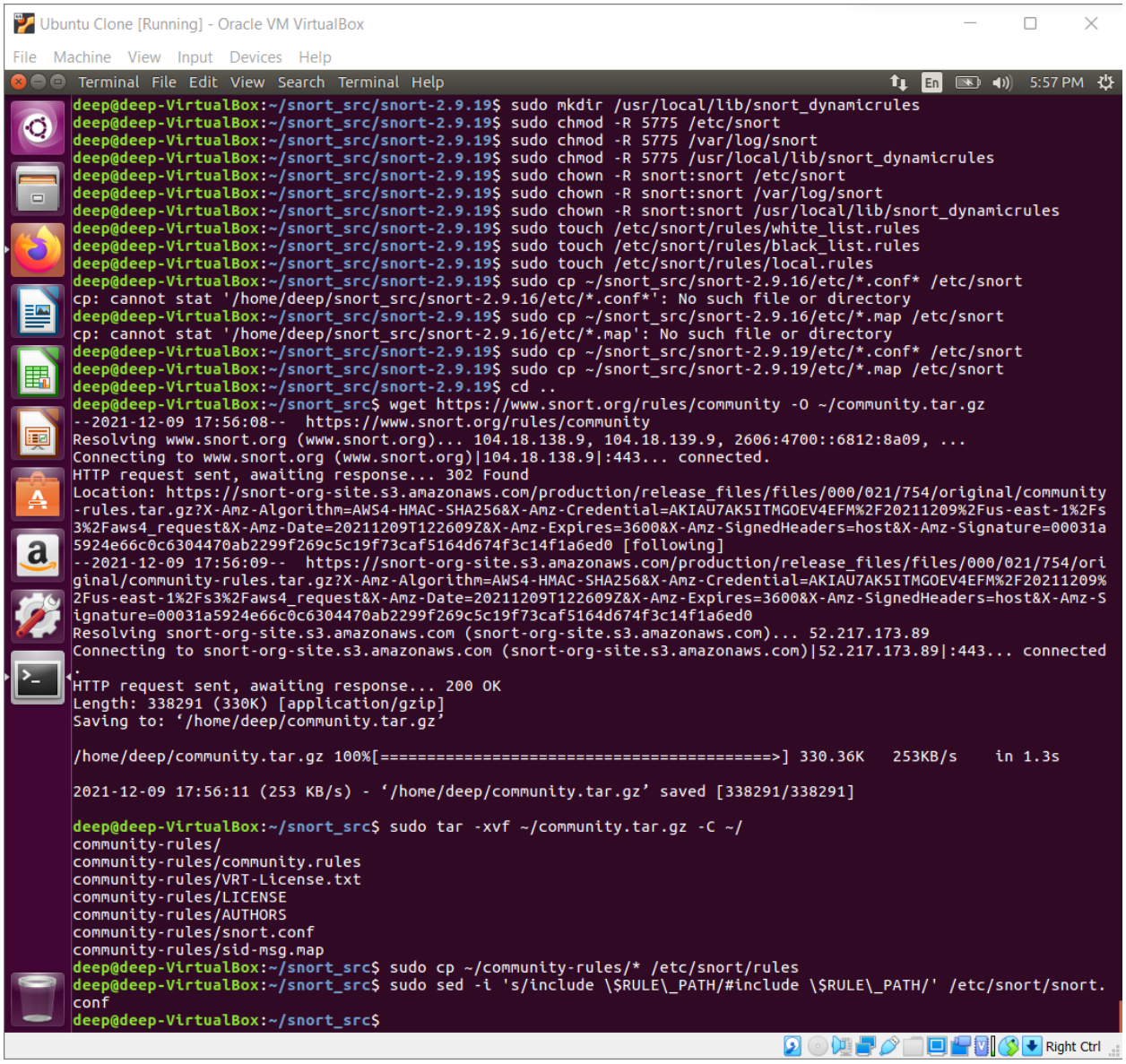

Ubuntu Clone [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal File Edit View Search Terminal Help
5:46 PM
make[3]: Entering directory '/home/deep/snort_src/snort-2.9.19/tools/u2boat'
/bin/mkdir -p '/usr/local/bin'
/bin/bash ../../libtool --mode=install /usr/bin/install -c 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$
Right Ctrl

Creating links and changing permissions of snort configuration files

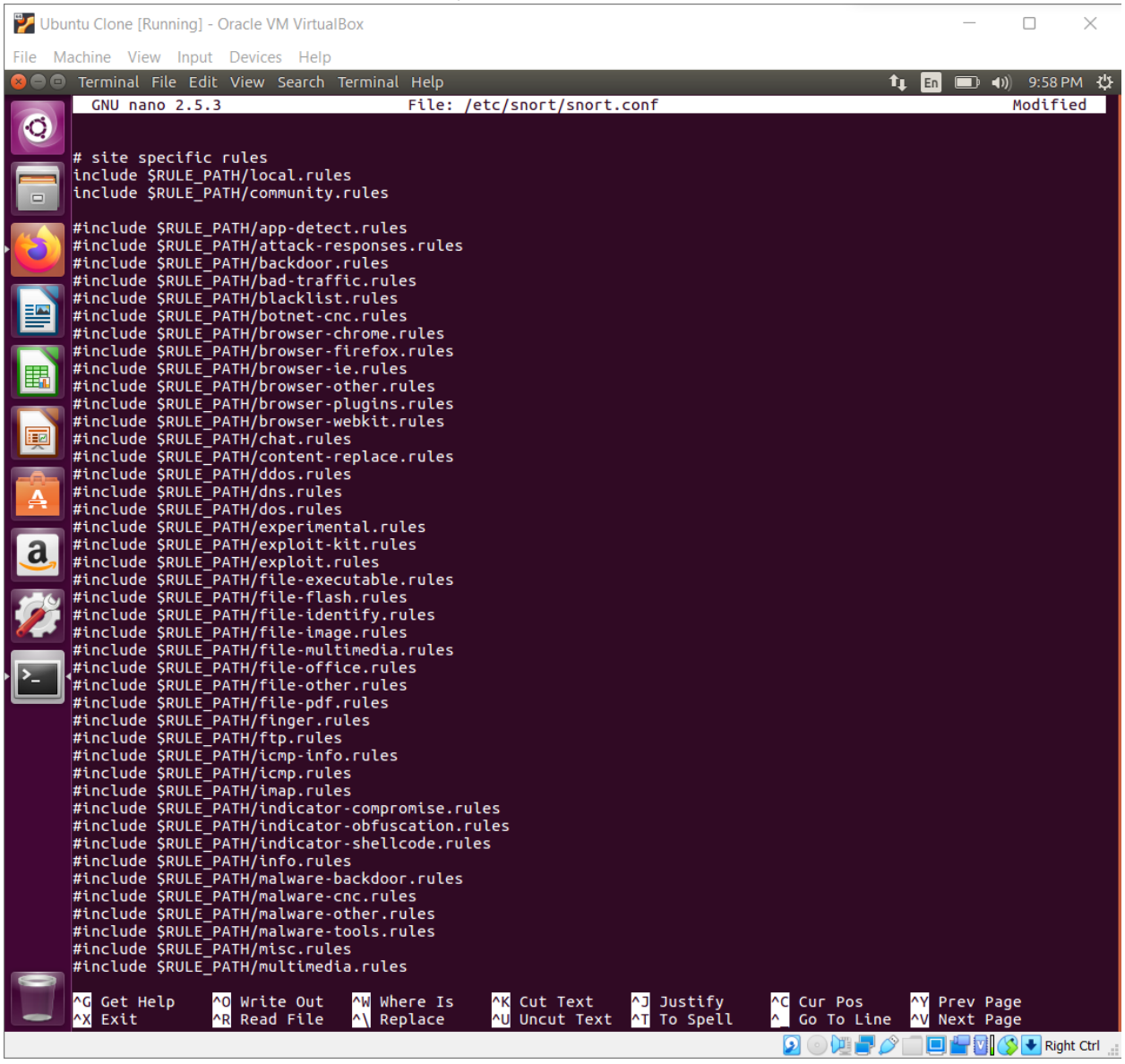


Downloading Community rules and using them as a base for local rules

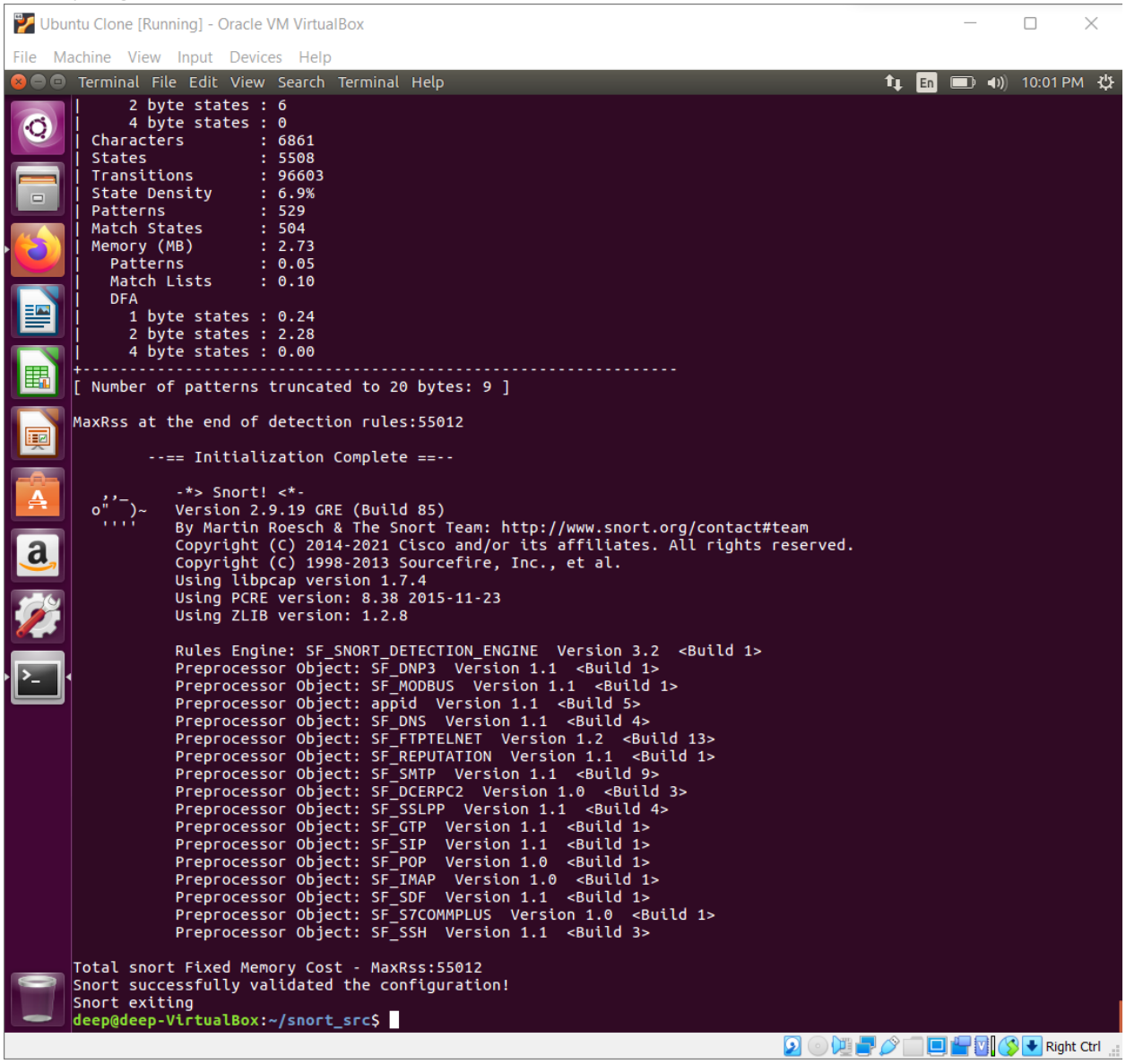



Ubuntu Clone [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal File Edit View Search Terminal Help
5:57 PM
deep@deep-VirtualBox:~/snort_src/snort-2.9.19$ sudo mkdir /usr/local/lib/snort_dynamicrules
deep@deep-VirtualBox:~/snort_src/snort-2.9.19$ sudo chmod -R 5775 /etc/snort
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=AKIAU7AK5ITMGOEV4EFM%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=AKIAU7AK5ITMGOEV4EFM%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$ 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$
Right Ctrl

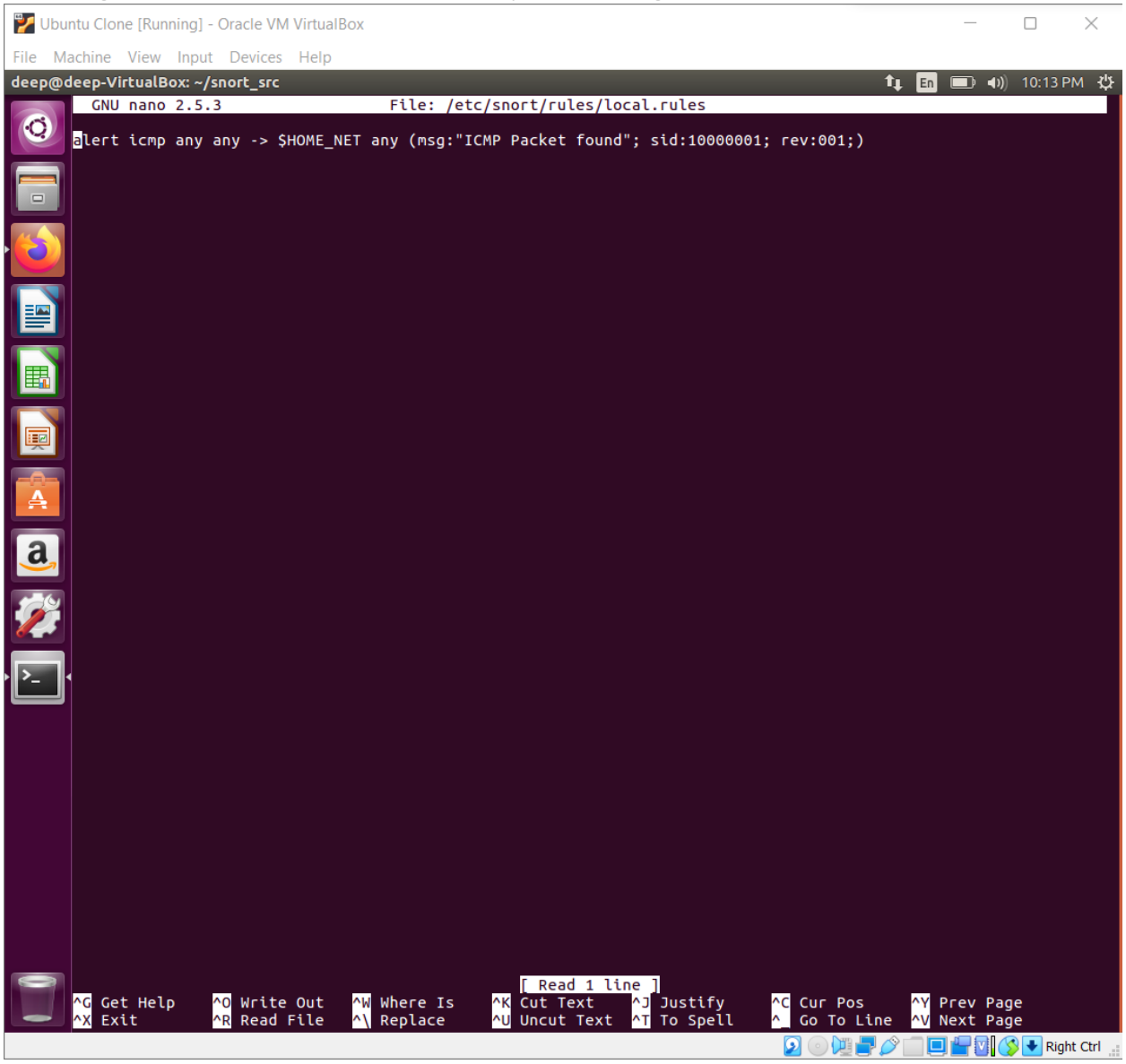
Configuring Snort to look for whitelisted and blacklisted URLs and also listen to rules mentioned in community rules and local rules



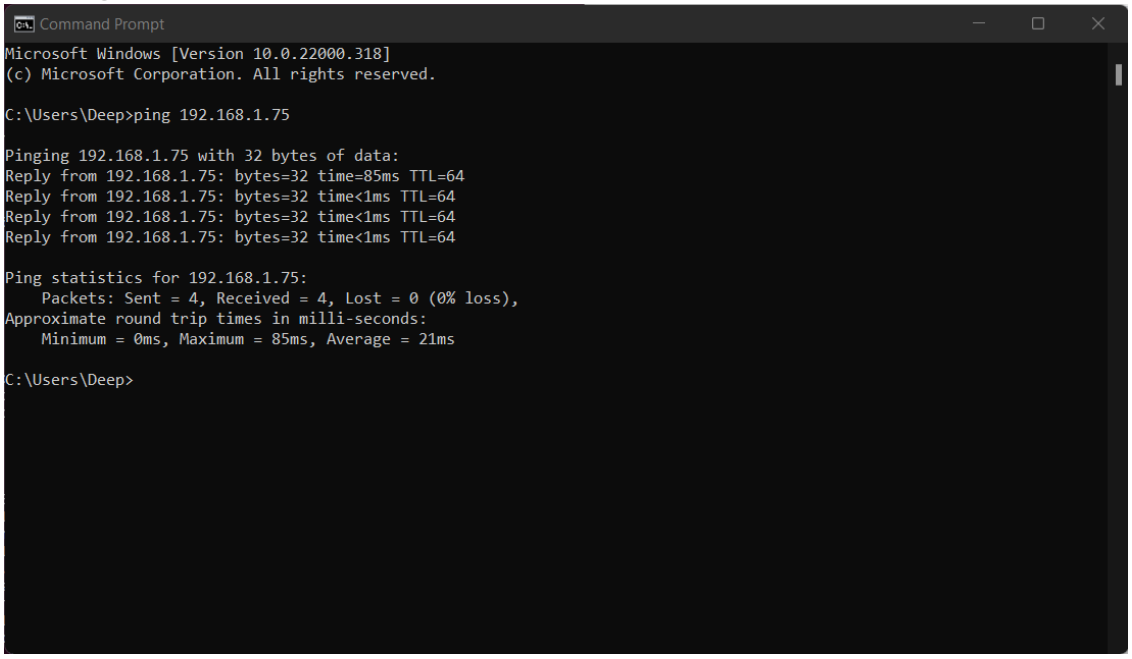
Verifying Snort Installation

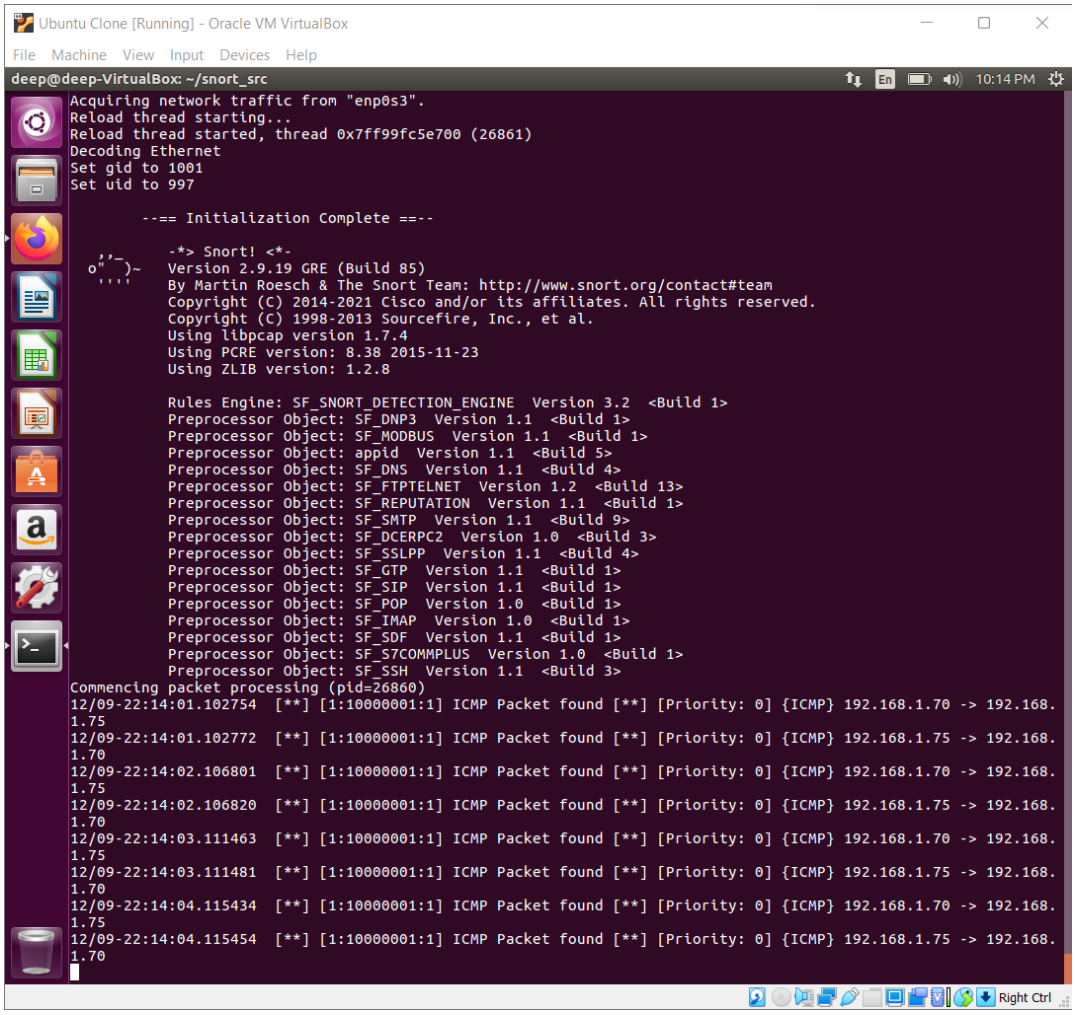


Writing custom rule to check for any incoming ICMP Packet



Hitting IP Address of the Virtual Machine from the host machine





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?

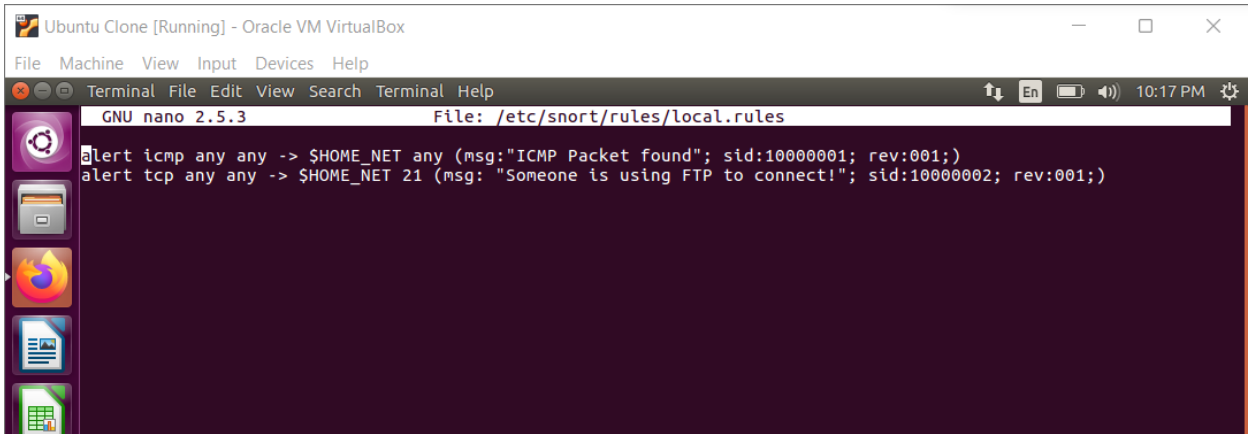
- Snort works only on certain rule sets defined by the users.
- If a particular error is not bound by any rule set then any hacker can utilize it to perform a zero day attack on newly launched applications.
- However, snort is also very widely used and has multiple community rule sets that define most 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?**

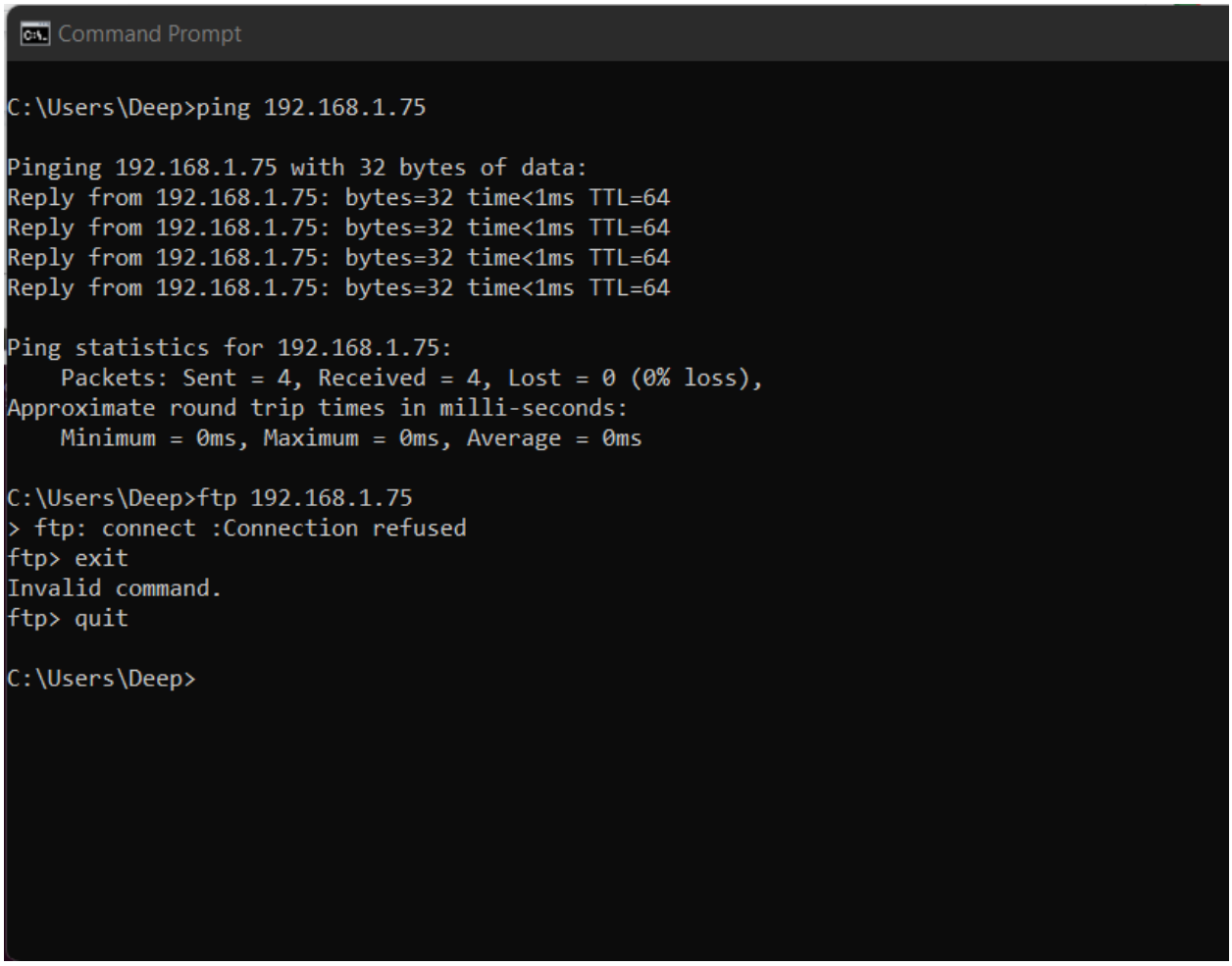
   Number of attacks on the network = 0.1% of 1000000 = 1000 attacks
   Number of benign events = 99.9% of 1000000 = 999000 events
   IDS has a true positive rate of 95% means that out of 1000 attacks, only 950 will set off alarms.
   Therefore, Number of true alarms = 950 alarms
   Since 95% of the total 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 = (Number of false alarms / Total Benign Events) * 100
   = (50 / 999000) * 100 = 0.005%

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

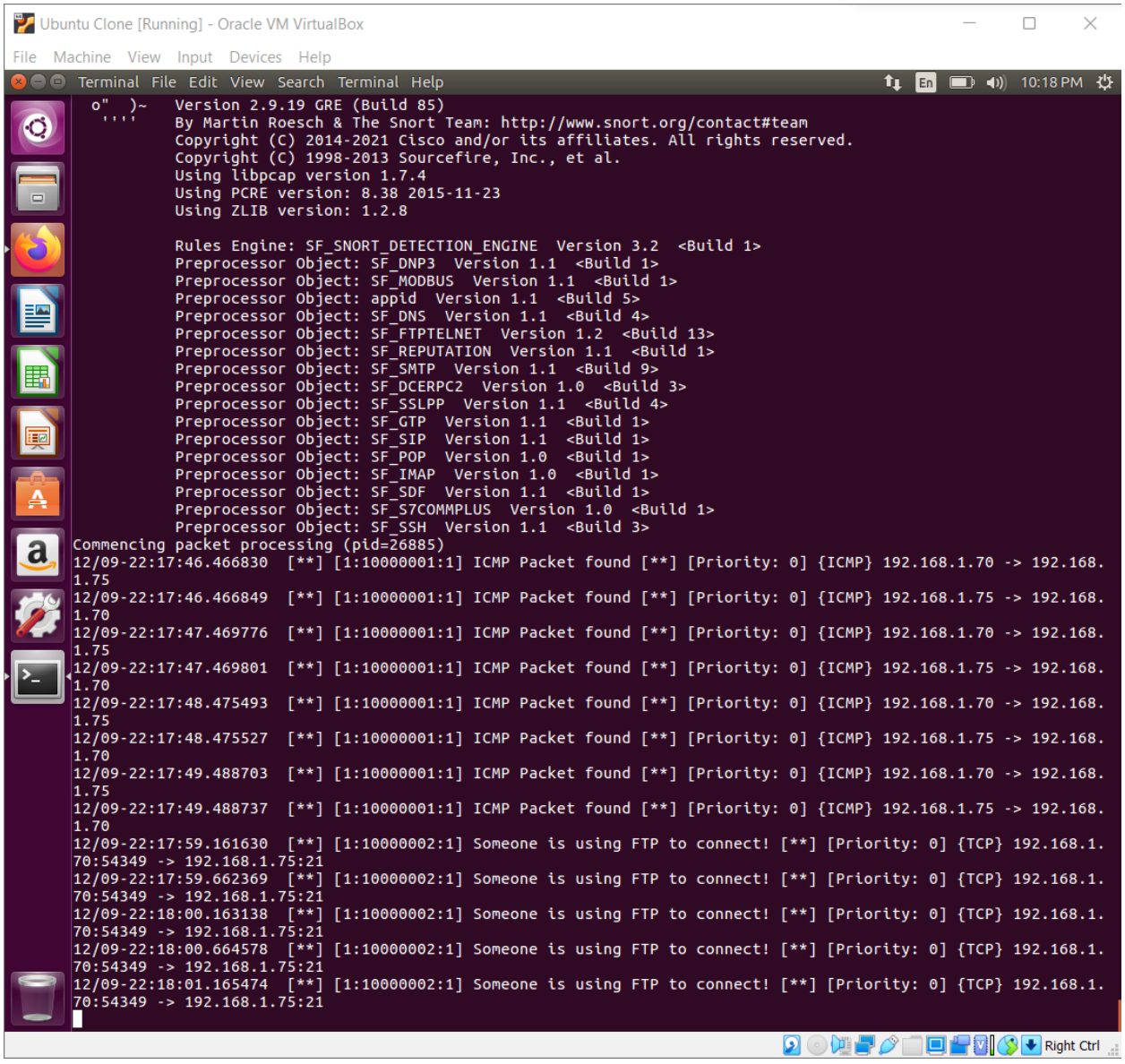
Writing custom Snort Rule to trigger whenever an incoming FTP connection is detected

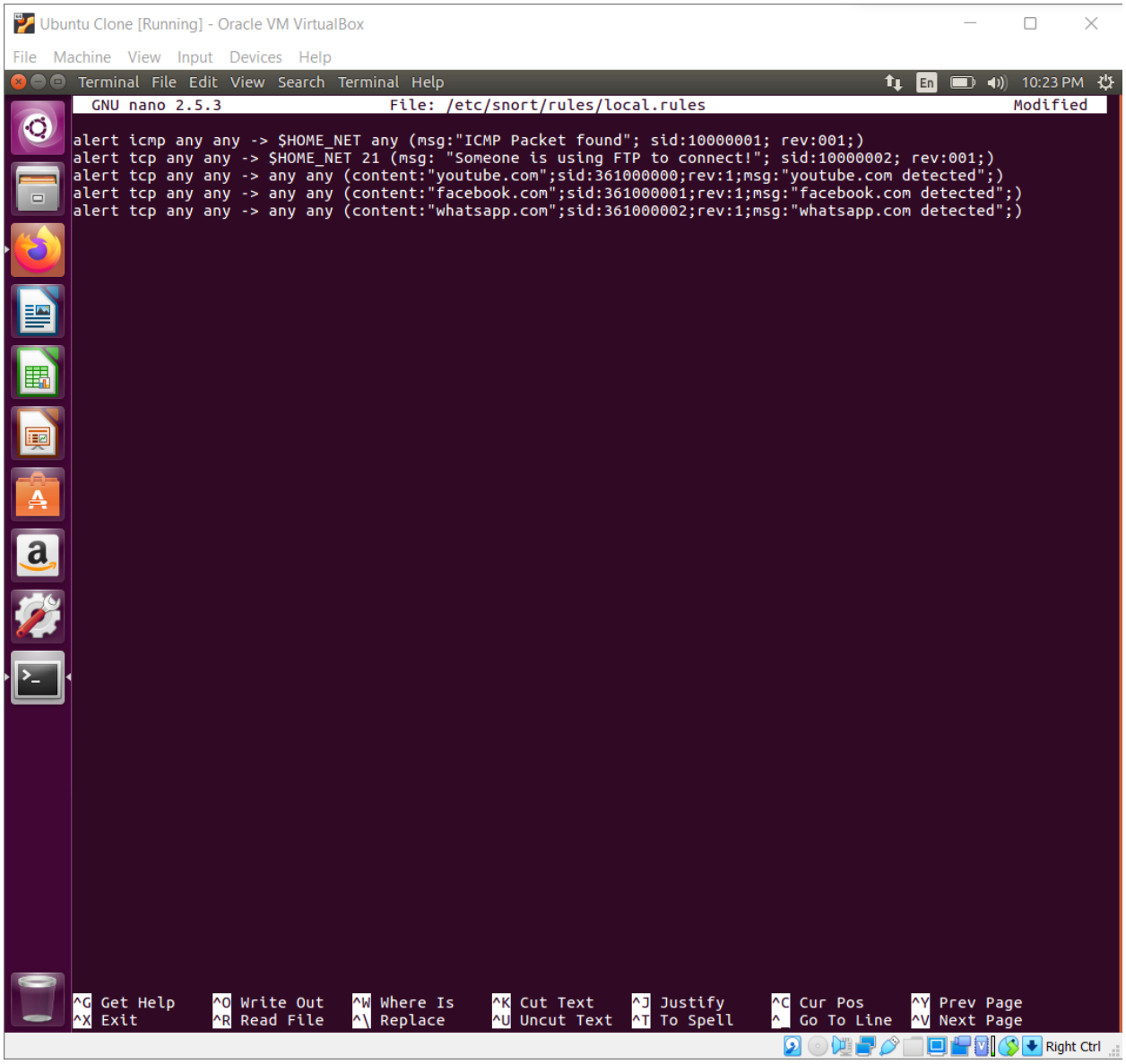


Trying to connect Host Machine to Virtual Machine using FTP

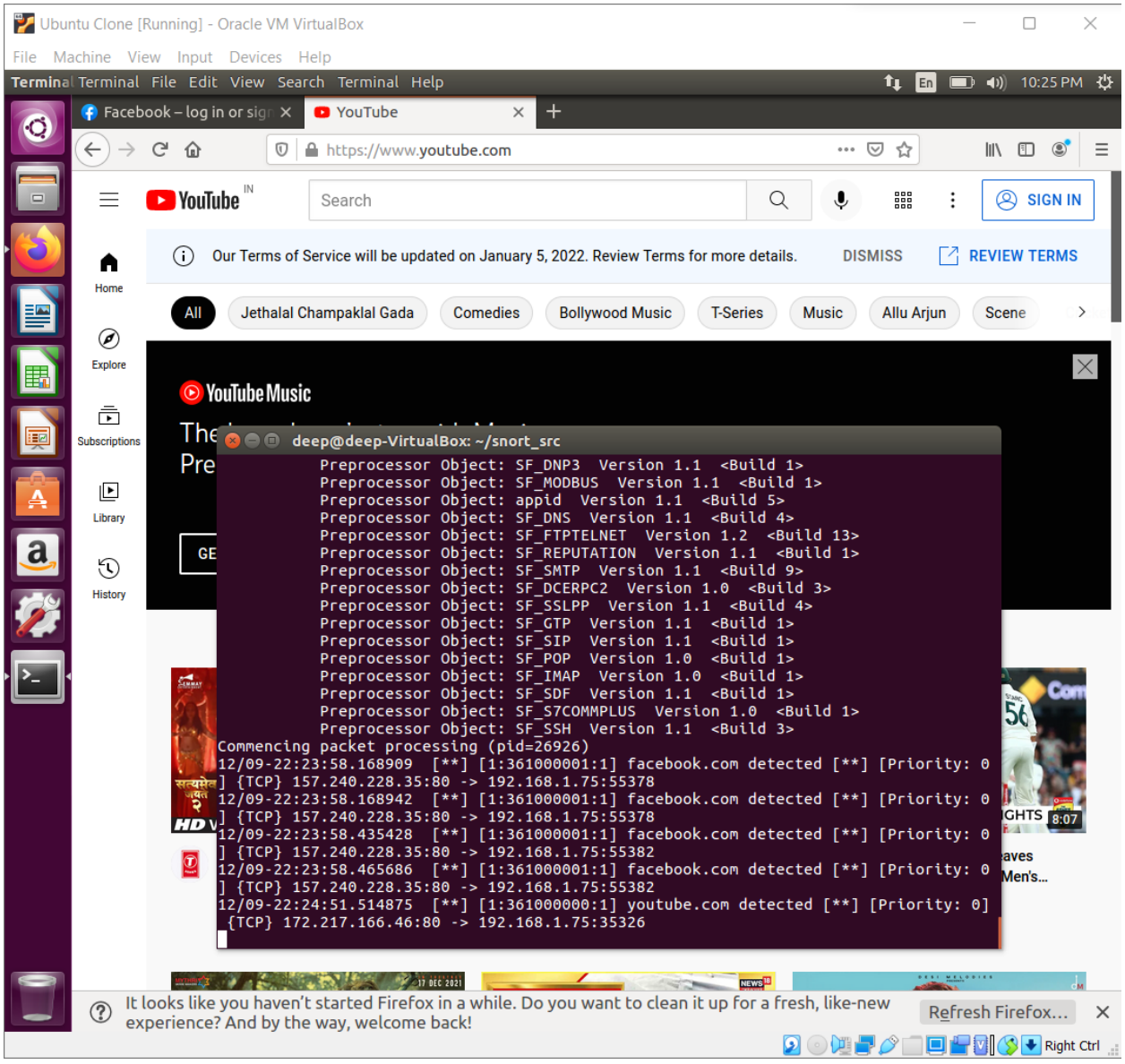


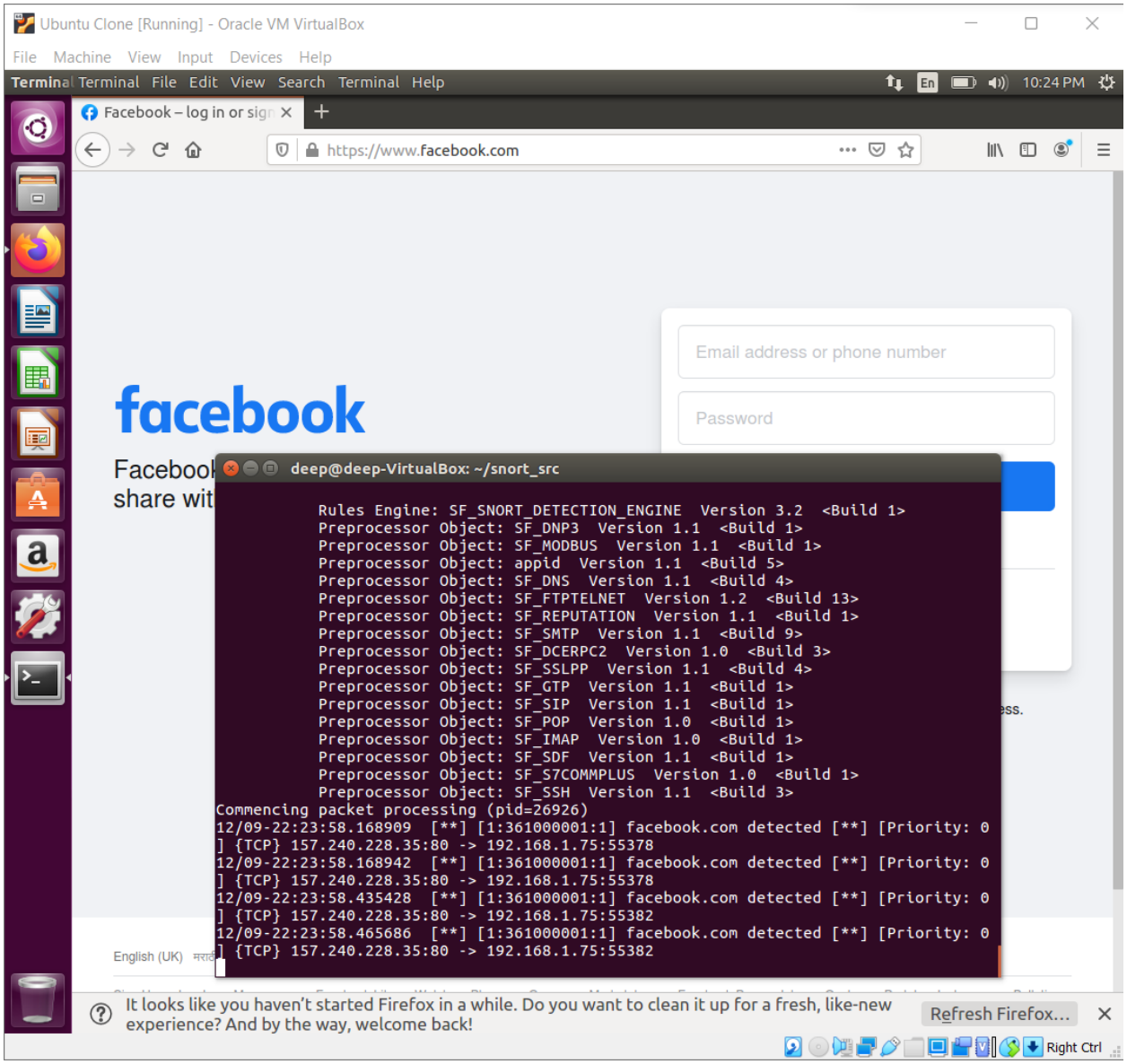
Snort is able to detect all the incoming FTP connections

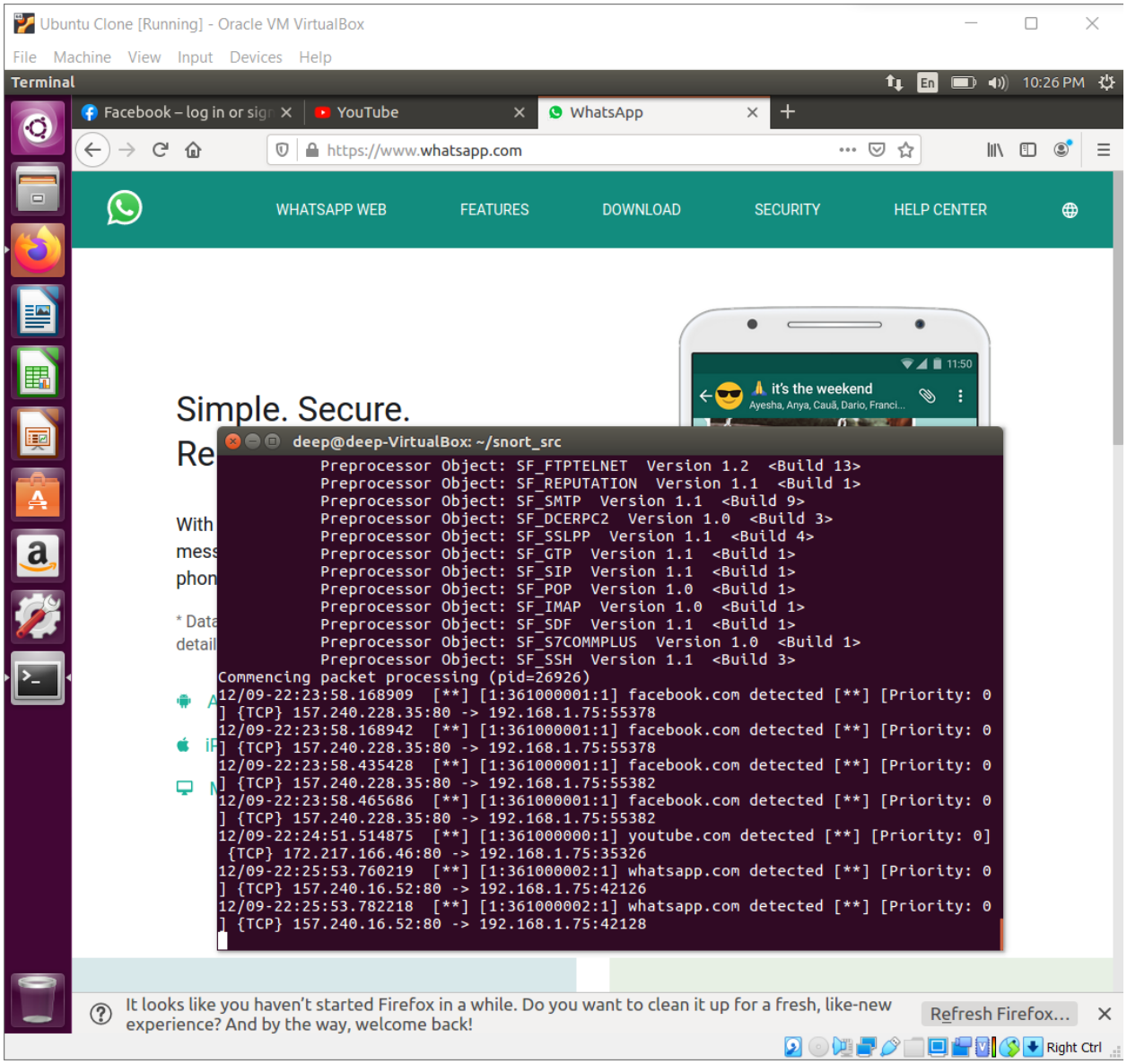



Ubuntu Clone [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal File Edit View Search Terminal Help
10:23 PM
GNU nano 2.5.3 File: /etc/snort/rules/local.rules Modified
alert icmp any any -> $HOME_NET any (msg:"ICMP Packet found"; sid:10000001; rev:001;)
alert tcp any any -> $HOME_NET 21 (msg: "Someone is using FTP to connect!"; sid:10000002; rev:001;)
alert tcp any any -> any any (content:"youtube.com";sid:361000000;rev:1;msg:"youtube.com detected";)
alert tcp any any -> any any (content:"facebook.com";sid:361000001;rev:1;msg:"facebook.com detected";)
alert tcp any any -> any any (content:"whatsapp.com";sid:361000002;rev:1;msg:"whatsapp.com detected";)
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos ^Y Prev Page
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Spell ^_ Go To Line ^V Next Page
Right Ctrl

Detecting if any custom website is being accessed by any user




Ubuntu Clone [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal File Edit View Search Terminal Help
10:24 PM
Facebook – log in or sign
https://www.facebook.com
facebook
Email address or phone number
Password
deep@deep-VirtualBox: ~/snort_src
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>
Commencing packet processing (pid=26926)
12/09-22:23:58.168909 [**] [1:361000001:1] facebook.com detected [**] [Priority: 0
] {TCP} 157.240.228.35:80 -> 192.168.1.75:55378
12/09-22:23:58.168942 [**] [1:361000001:1] facebook.com detected [**] [Priority: 0
] {TCP} 157.240.228.35:80 -> 192.168.1.75:55378
12/09-22:23:58.435428 [**] [1:361000001:1] facebook.com detected [**] [Priority: 0
] {TCP} 157.240.228.35:80 -> 192.168.1.75:55382
12/09-22:23:58.465686 [**] [1:361000001:1] facebook.com detected [**] [Priority: 0
] {TCP} 157.240.228.35:80 -> 192.168.1.75:55382
English (UK)
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...
Right Ctrl



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