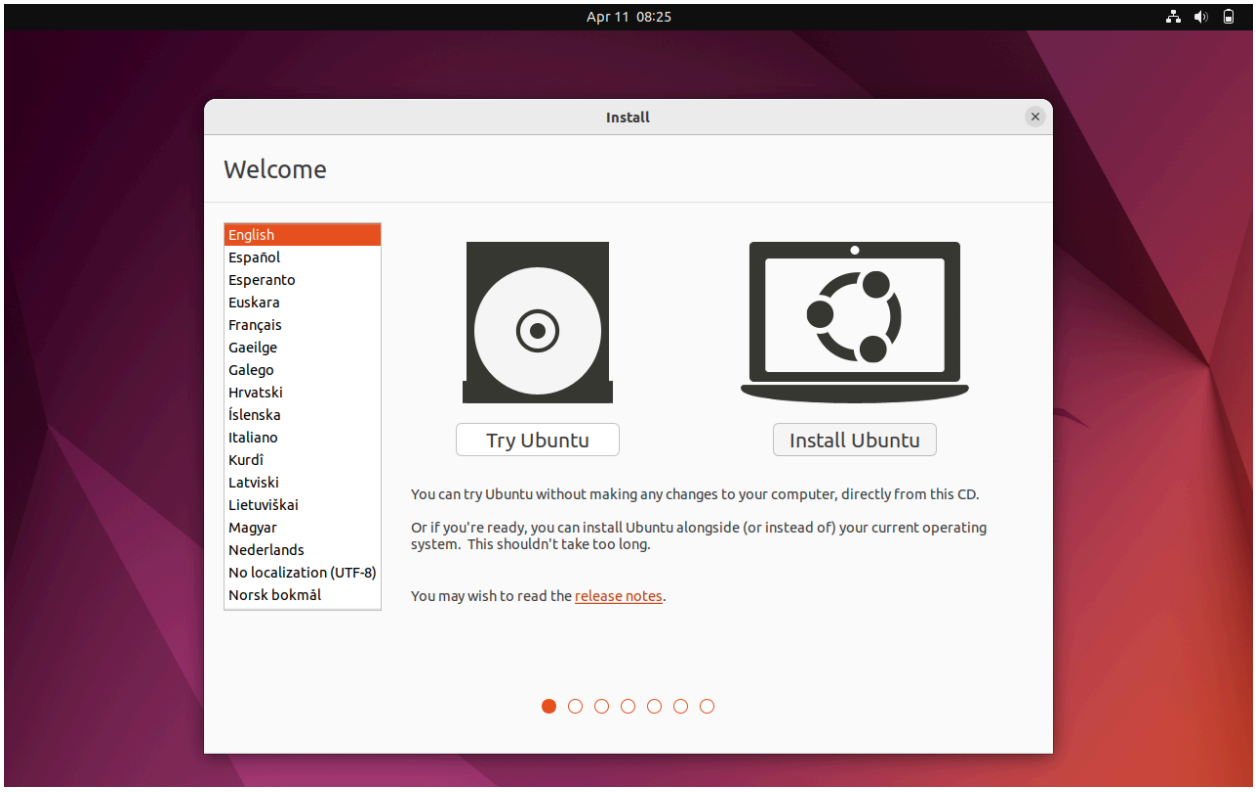
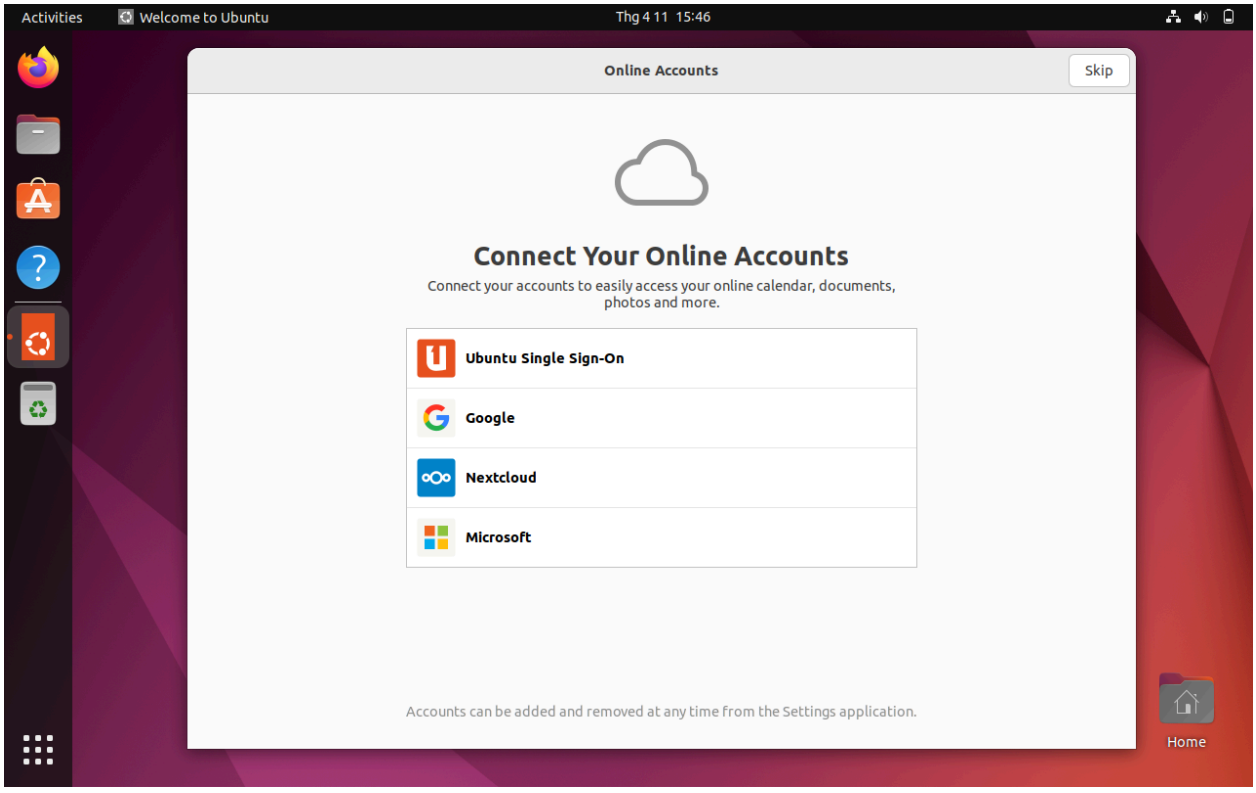
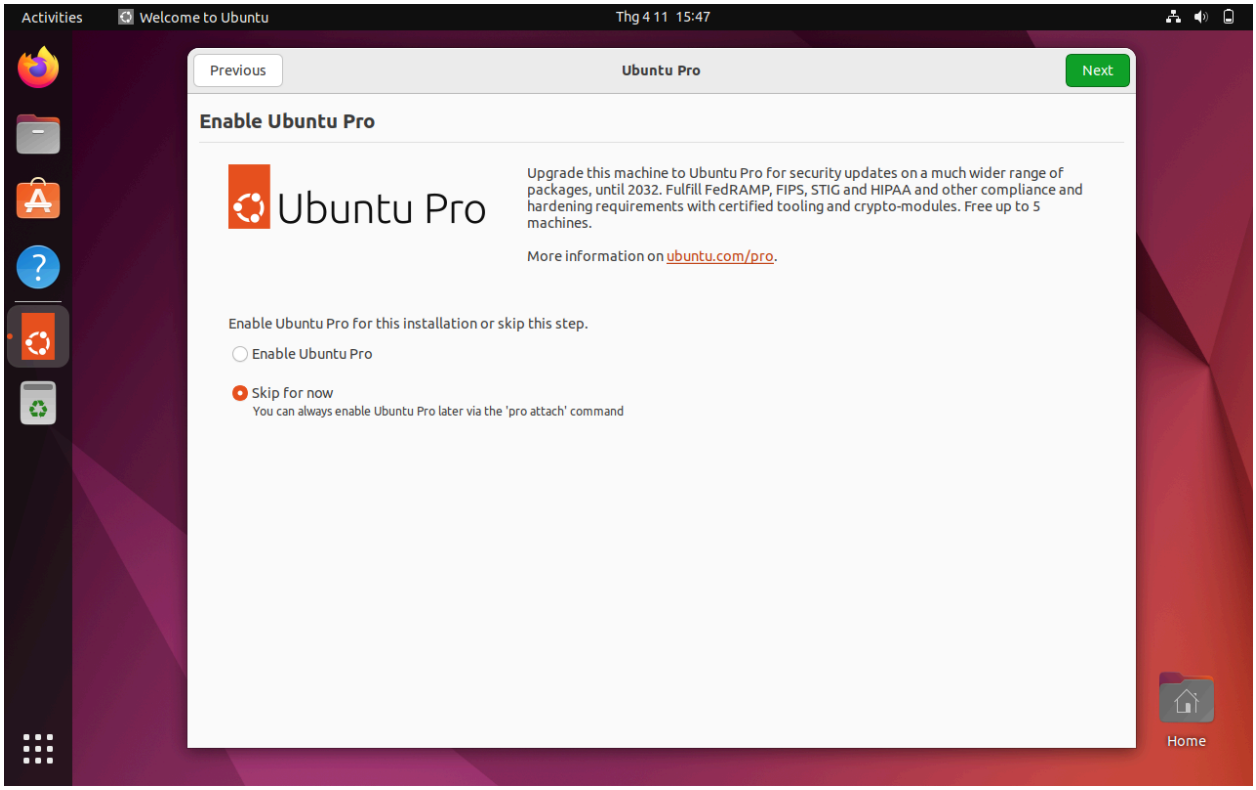
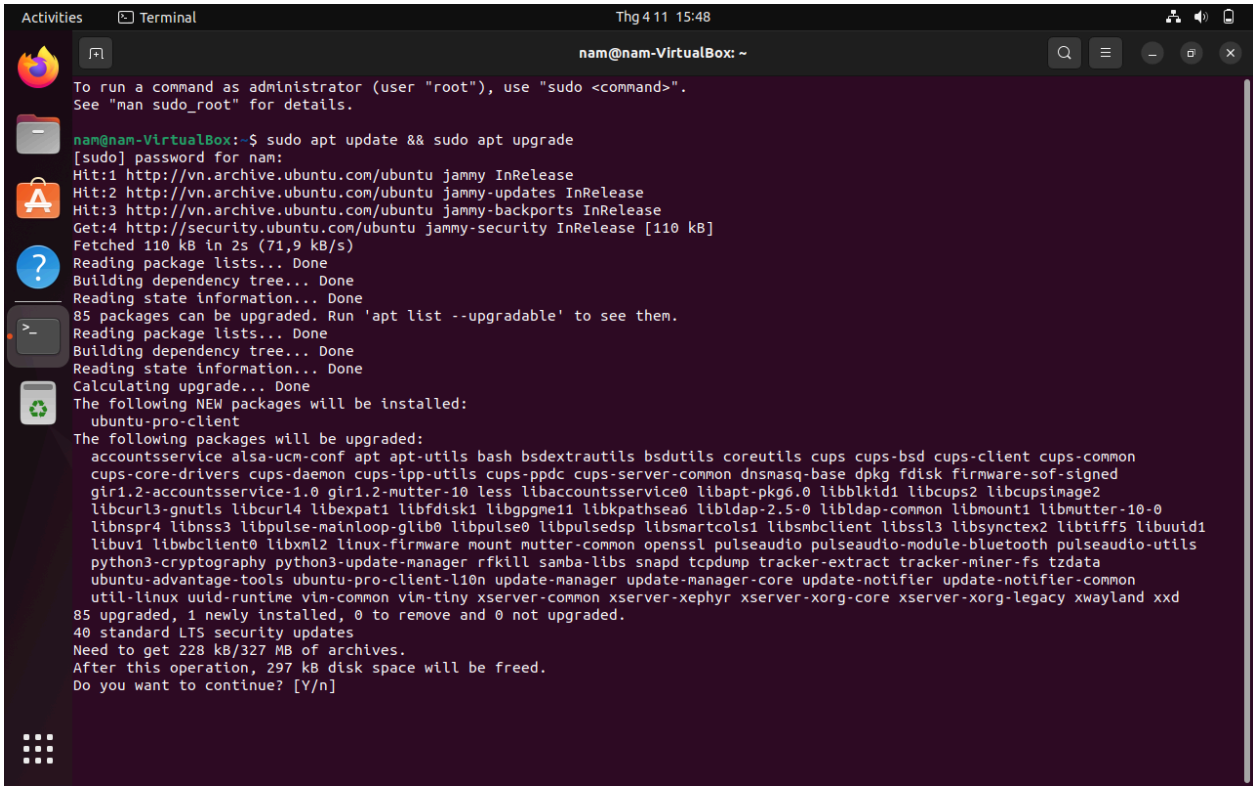
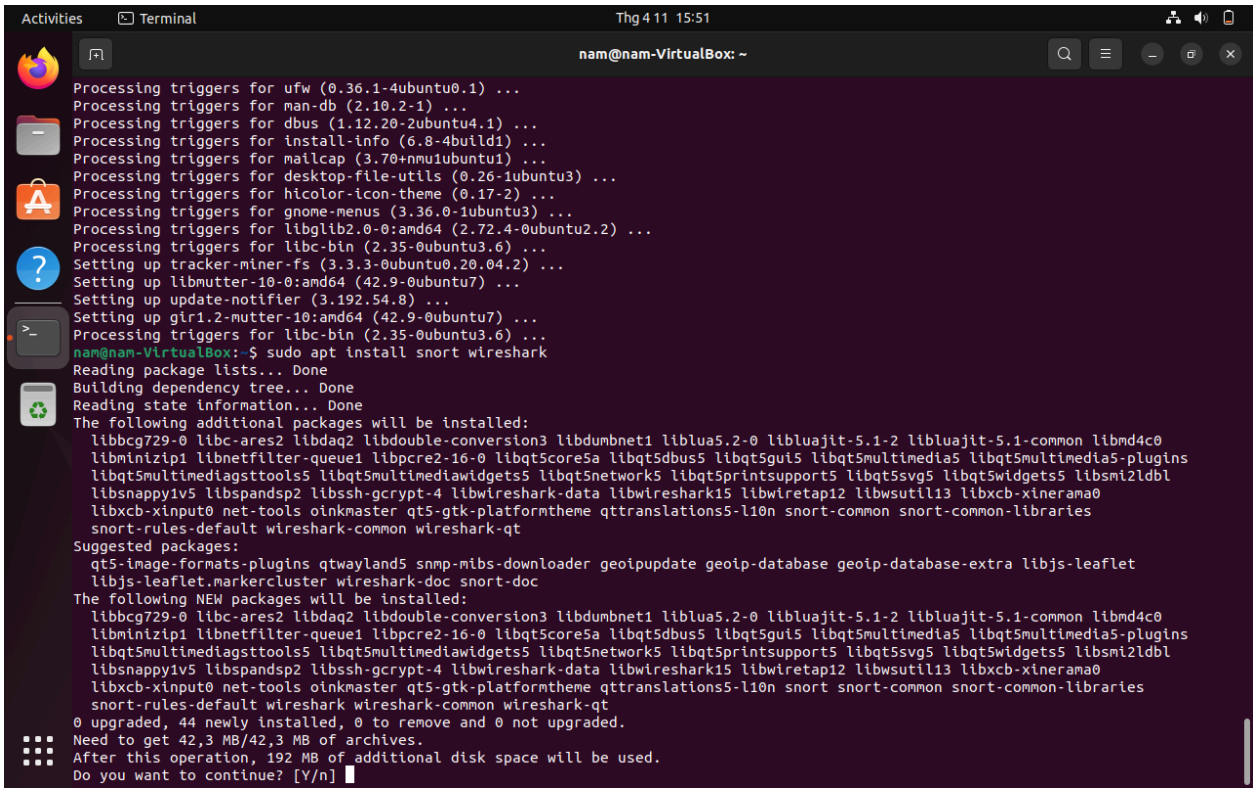
Lab 13.01


Apr 11 08:25
Install
Welcome
English
Español
Esperanto
Euskara
Français
Gaeilge
Galego
Hrvatski
Íslenska
Italiano
Kurdî
Latviski
Lietuviškai
Magyar
Nederlands
No localization (UTF-8)
Norsk bokmål
Try Ubuntu
Install Ubuntu
You can try Ubuntu without making any changes to your computer, directly from this CD.
Or if you're ready, you can install Ubuntu alongside (or instead of) your current operating system. This shouldn't take too long.
You may wish to read the release notes.

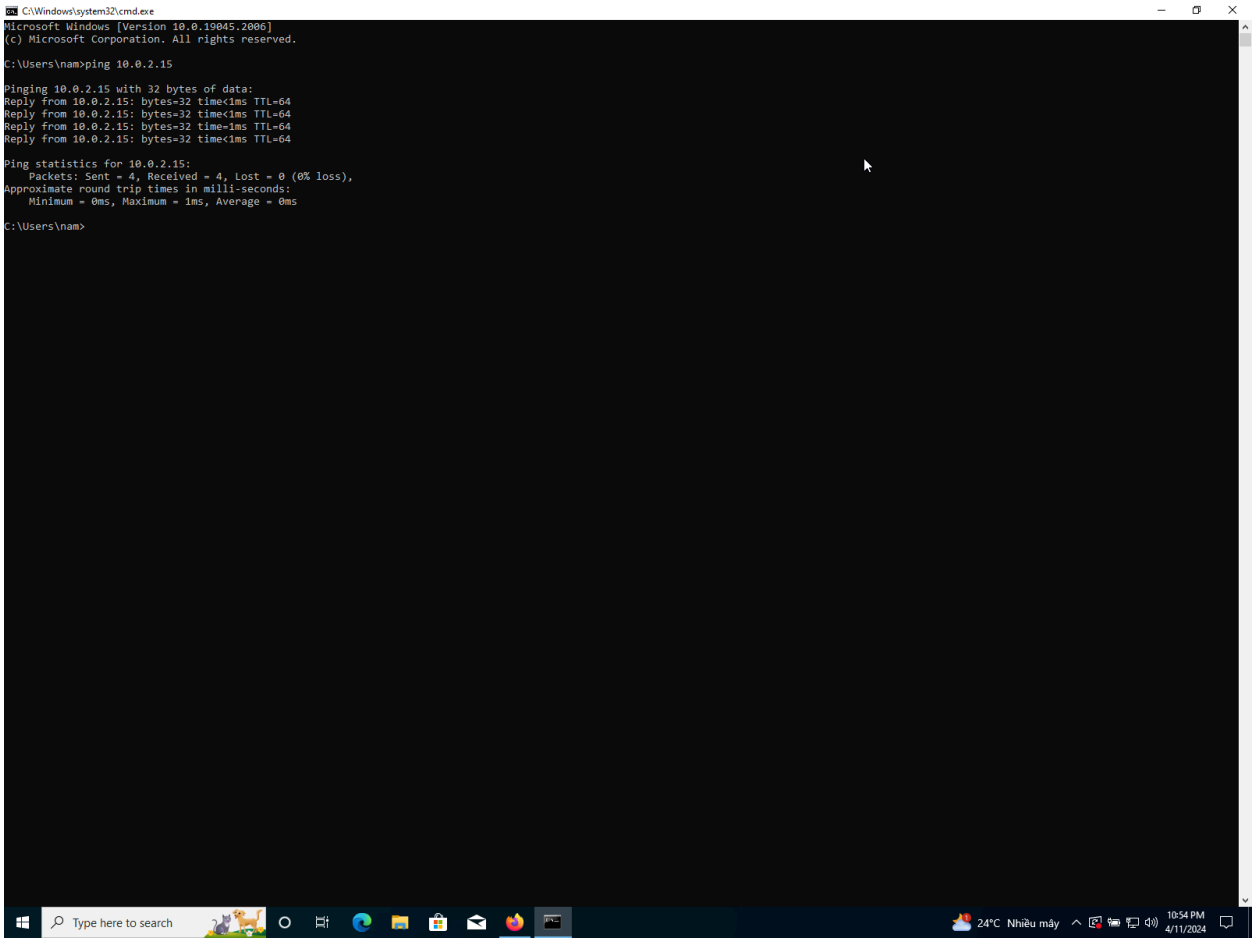

Activities
Welcome to Ubuntu
Thg 4 11 15:46
Online Accounts
Skip
Connect Your Online Accounts
Connect your accounts to easily access your online calendar, documents, photos and more.
Ubuntu Single Sign-On
Google
Nextcloud
Microsoft
Accounts can be added and removed at any time from the Settings application.
Home

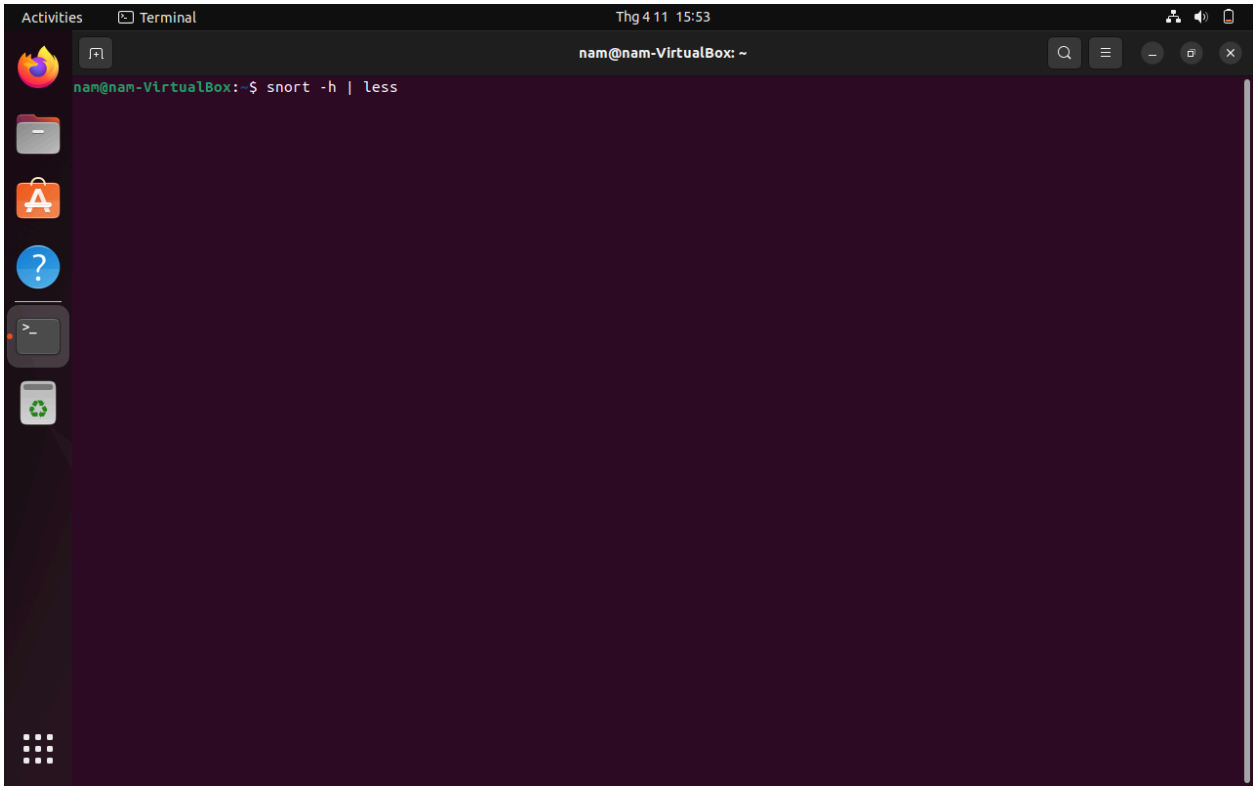

Activities
Welcome to Ubuntu
Thg 4 11 15:47
Previous
Ubuntu Pro
Next
Enable Ubuntu Pro
Ubuntu Pro
Upgrade this machine to Ubuntu Pro for security updates on a much wider range of packages, until 2032. Fulfill FedRAMP, FIPS, STIG and HIPAA and other compliance and hardening requirements with certified tooling and crypto-modules. Free up to 5 machines.
More information on ubuntu.com/pro.
Enable Ubuntu Pro for this installation or skip this step.
Enable Ubuntu Pro
Skip for now
You can always enable Ubuntu Pro later via the 'pro attach' command
Home

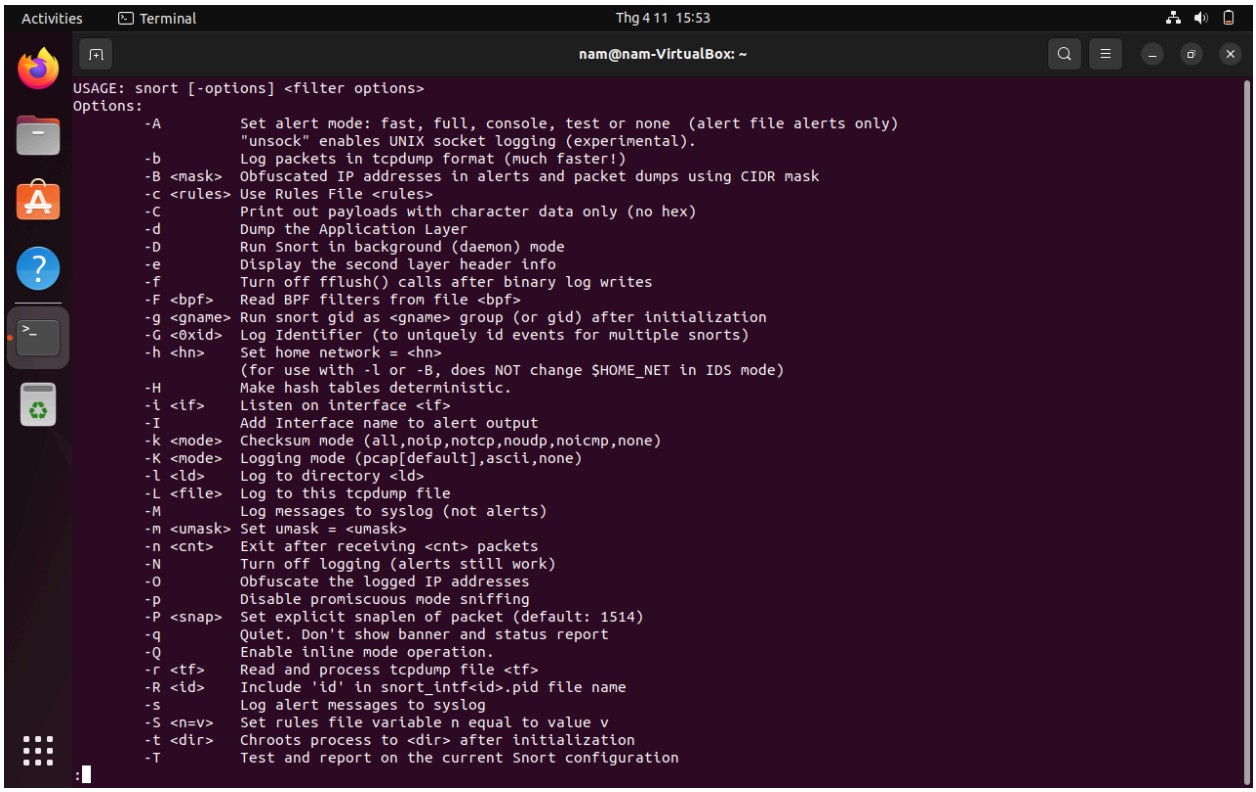

Activities
Terminal
Thg 4 11 15:48
nam@nam-VirtualBox: ~
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
nam@nam-VirtualBox:~$ sudo apt update && sudo apt upgrade
[sudo] password for nam:
Hit:1 http://vn.archive.ubuntu.com/ubuntu jammy InRelease
Hit:2 http://vn.archive.ubuntu.com/ubuntu jammy-updates InRelease
Hit:3 http://vn.archive.ubuntu.com/ubuntu jammy-backports InRelease
Get:4 http://security.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
Fetched 110 kB in 2s (71,9 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
85 packages can be upgraded. Run 'apt list --upgradable' to see them.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
The following NEW packages will be installed:
ubuntu-pro-client
The following packages will be upgraded:
accountsservice alsa-ucm-conf apt apt-utils bash bsdextrautils bsdutils coreutils cups cups-bsd cups-client cups-common
cups-core-drivers cups-daemon cups-ipp-utils cups-ppdc cups-server-common dnsmasq-base dpkg fdisk firmware-sof-signed
gir1.2-accountsservice-1.0 gir1.2-mutter-10 less libaccountsservice0 libapt-pkg6.0 libblkid1 libcups2 libcupsimage2
libcurl3-gnutls libcurl4 libexpat1 libfdisk1 libgpgme11 libkpathsea6 libldap-2.5-0 libldap-common libmount1 libmutter-10-0
libnspr4 libnss3 libpulse-mainloop-glib0 libpulse0 libpulsedsp libsmartcols1 libsmbclient libssl3 libsynctex2 libtiff5 libuuid1
libuv1 libwbclient0 libxml2 linux-firmware mount mutter-common openssl pulseaudio pulseaudio-module-bluetooth pulseaudio-utils
python3-cryptography python3-update-manager rfkill samba-libs snapd tcpdump tracker-extract tracker-miner-fs tzdata
ubuntu-advantage-tools ubuntu-pro-client-l10n update-manager update-manager-core update-notifier update-notifier-common
util-linux uuid-runtime vim-common vim-tiny xserver-common xserver-xephyr xserver-xorg-core xserver-xorg-legacy xwayland xxd
85 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
40 standard LTS security updates
Need to get 228 kB/327 MB of archives.
After this operation, 297 kB disk space will be freed.
Do you want to continue? [Y/n]

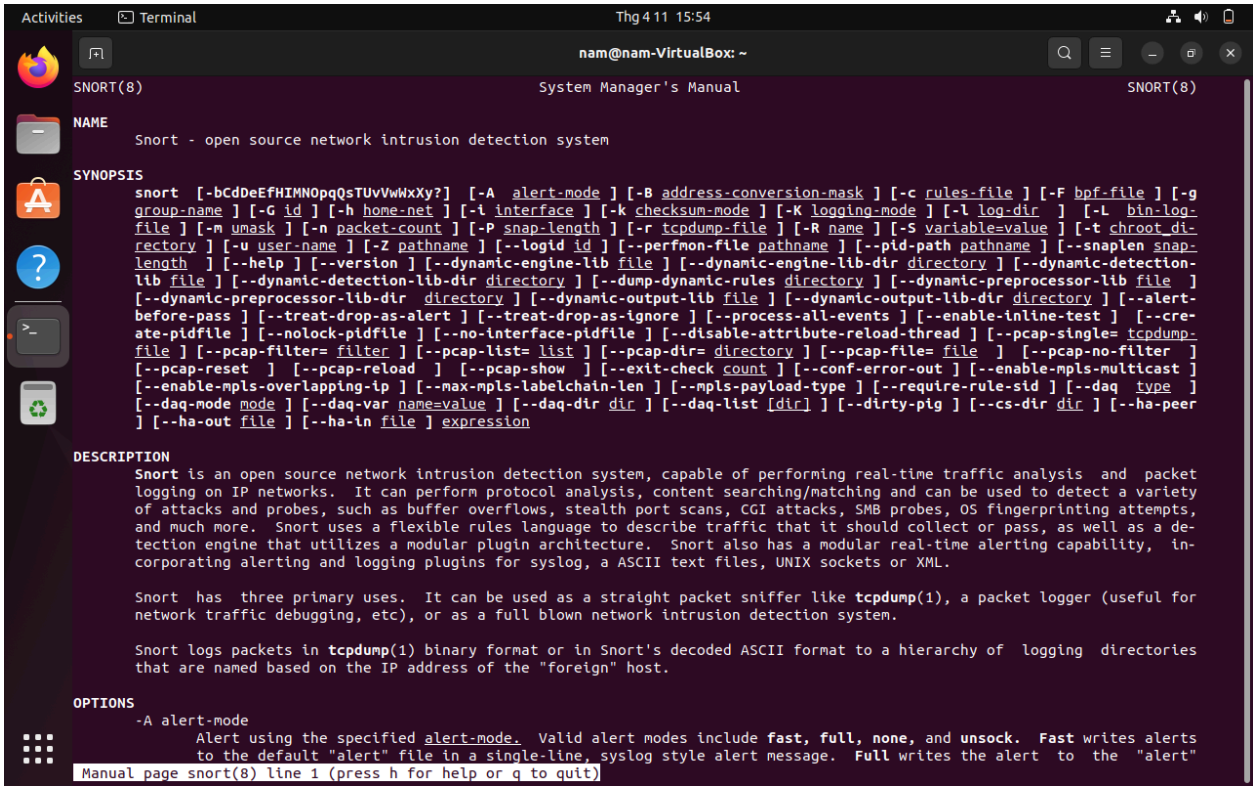

Activities
Terminal
Thg 4 11 15:51
nam@nam-VirtualBox: ~
Processing triggers for ufw (0.36.1-4ubuntu0.1) ...
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for dbus (1.12.20-2ubuntu4.1) ...
Processing triggers for install-info (6.8-4build1) ...
Processing triggers for mailcap (3.70+nmu1ubuntu1) ...
Processing triggers for desktop-file-utils (0.26-1ubuntu3) ...
Processing triggers for hicolor-icon-theme (0.17-2) ...
Processing triggers for gnome-menus (3.36.0-1ubuntu3) ...
Processing triggers for libglib2.0-0:amd64 (2.72.4-0ubuntu2.2) ...
Processing triggers for libc-bin (2.35-0ubuntu3.6) ...
Setting up tracker-miner-fs (3.3.3-0ubuntu0.20.04.2) ...
Setting up libmutter-10-0:amd64 (42.9-0ubuntu7) ...
Setting up update-notifier (3.192.54.8) ...
Setting up gir1.2-mutter-10:amd64 (42.9-0ubuntu7) ...
Processing triggers for libc-bin (2.35-0ubuntu3.6) ...
nam@nam-VirtualBox:~$ sudo apt install snort wireshark
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
libbcg729-0 libc-ares2 libdaq2 libdouble-conversion3 libdumbnet1 liblua5.2-0 libluajit-5.1-2 libluajit-5.1-common libmd4c0
libminizip1 libnetfilter-queue1 libpcre2-16-0 libqt5core5a libqt5dbus5 libqt5gui5 libqt5multimedia5 libqt5multimedia5-plugins
libqt5multimediagsttools5 libqt5multimediawidgets5 libqt5network5 libqt5printsupport5 libqt5svg5 libqt5widgets5 libsmi2ldbl
libsnappy1v5 libspandsp2 libssh-gcrypt-4 libwireshark-data libwireshark15 libwiretap12 libwsutil13 libxcb-xinerama0
libxcb-xinput0 net-tools oinkmaster qt5-gtk-platformtheme qttranslations5-l10n snort-common snort-common-libraries
snort-rules-default wireshark-common wireshark-qt
Suggested packages:
qt5-image-formats-plugins qtwayland5 snmp-mibs-downloader geoipupdate geoip-database geoip-database-extra libjs-leaflet
libjs-leaflet.markercluster wireshark-doc snort-doc
The following NEW packages will be installed:
libbcg729-0 libc-ares2 libdaq2 libdouble-conversion3 libdumbnet1 liblua5.2-0 libluajit-5.1-2 libluajit-5.1-common libmd4c0
libminizip1 libnetfilter-queue1 libpcre2-16-0 libqt5core5a libqt5dbus5 libqt5gui5 libqt5multimedia5 libqt5multimedia5-plugins
libqt5multimediagsttools5 libqt5multimediawidgets5 libqt5network5 libqt5printsupport5 libqt5svg5 libqt5widgets5 libsmi2ldbl
libsnappy1v5 libspandsp2 libssh-gcrypt-4 libwireshark-data libwireshark15 libwiretap12 libwsutil13 libxcb-xinerama0
libxcb-xinput0 net-tools oinkmaster qt5-gtk-platformtheme qttranslations5-l10n snort snort-common snort-common-libraries
snort-rules-default wireshark wireshark-common wireshark-qt
0 upgraded, 44 newly installed, 0 to remove and 0 not upgraded.
Need to get 42,3 MB/42,3 MB of archives.
After this operation, 192 MB of additional disk space will be used.
Do you want to continue? [Y/n]

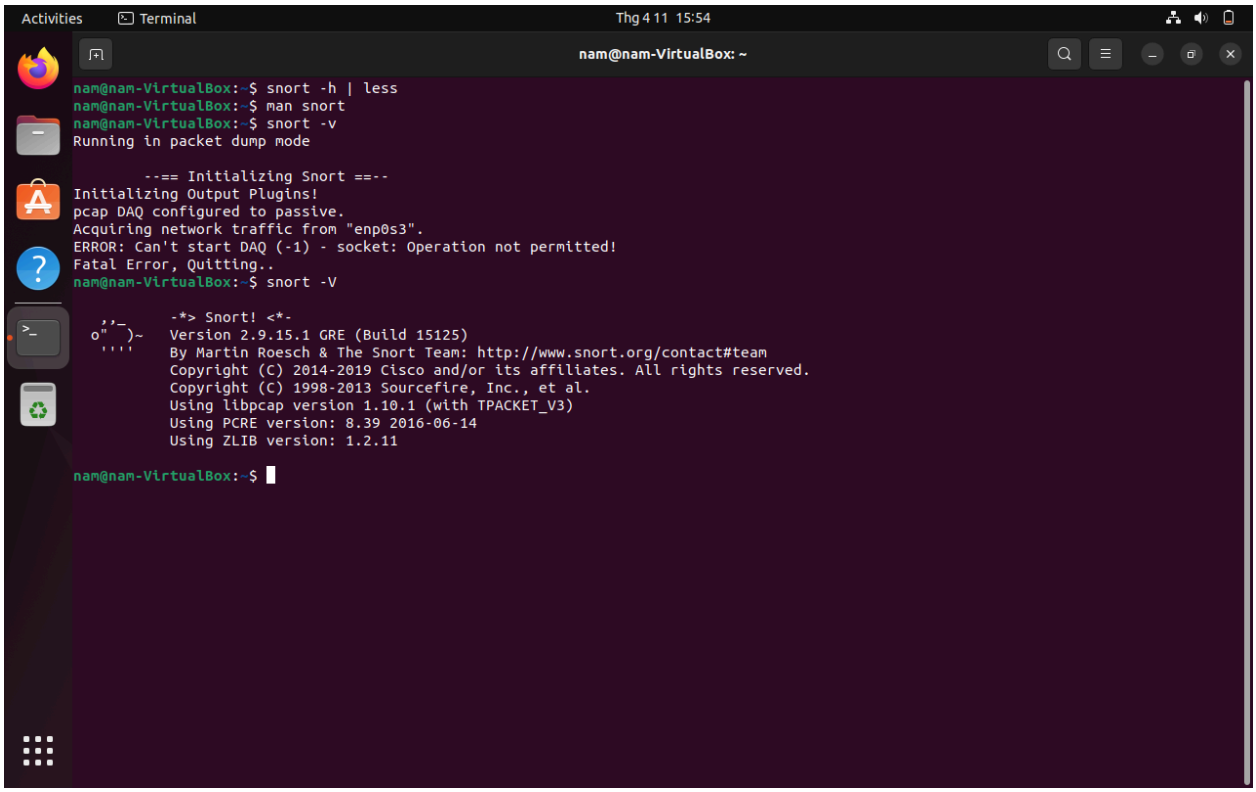
Lab 13.02

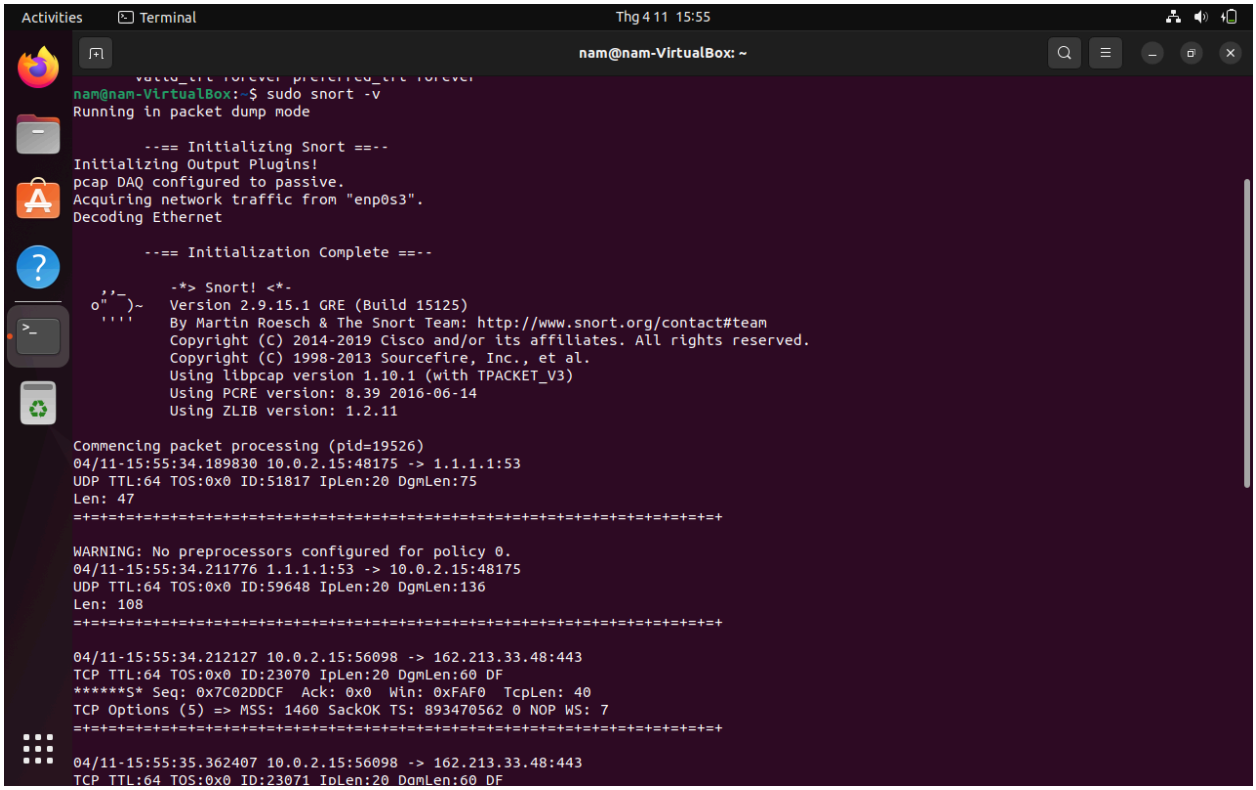

C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.19045.2006]
(c) Microsoft Corporation. All rights reserved.
C:\Users\nam>ping 10.0.2.15
Pinging 10.0.2.15 with 32 bytes of data:
Reply from 10.0.2.15: bytes=32 time<1ms TTL=64
Reply from 10.0.2.15: bytes=32 time<1ms TTL=64
Reply from 10.0.2.15: bytes=32 time<1ms TTL=64
Reply from 10.0.2.15: bytes=32 time<1ms TTL=64
Ping statistics for 10.0.2.15:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\Users\nam>
Type here to search
24°C Nhiều mây
10:54 PM
4/11/2024

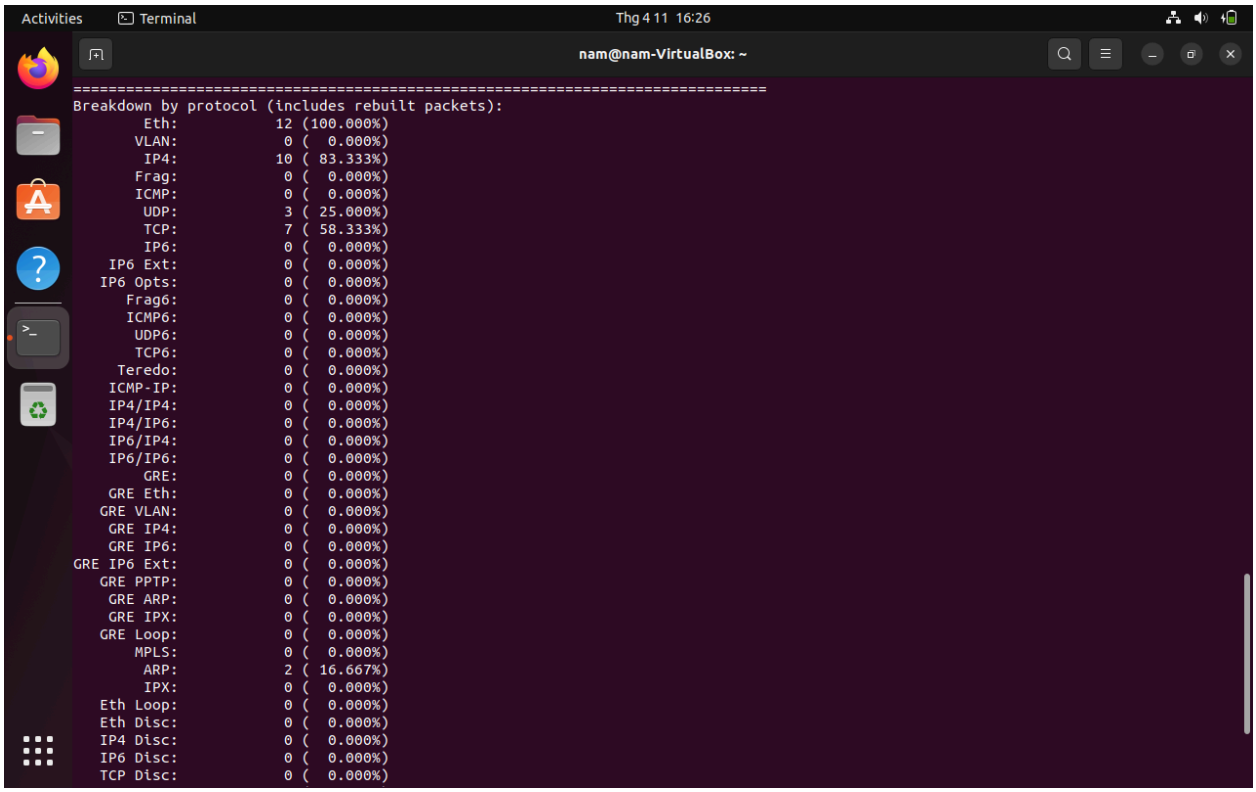

Activities
Terminal
Thg 4 11 15:53
nam@nam-VirtualBox: ~
nam@nam-VirtualBox:~$ snort -h | less

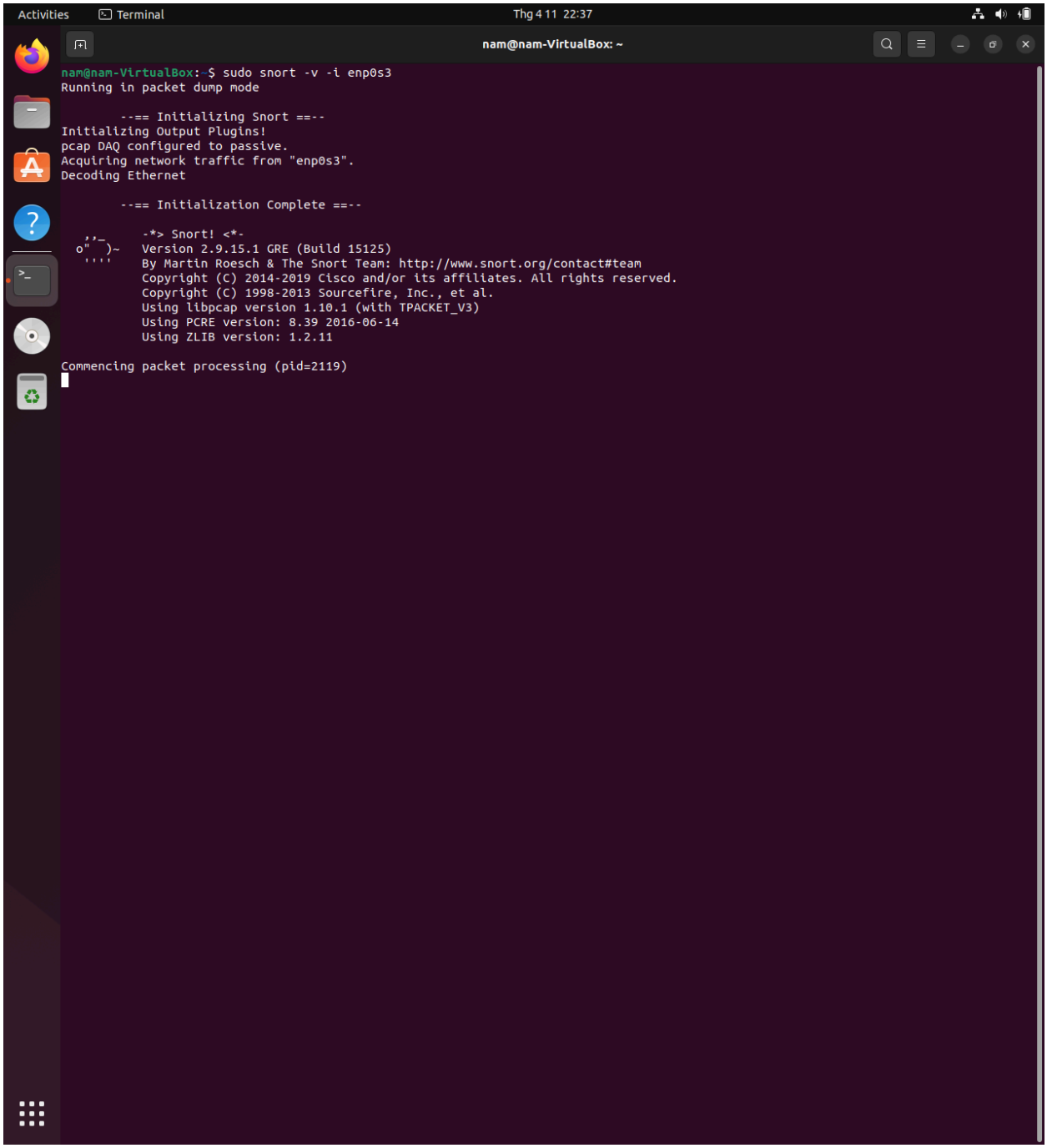

Activities
Terminal
Thg 4 11 15:53
nam@nam-VirtualBox: ~
USAGE: snort [-options] <filter options>
Options:
-A Set alert mode: fast, full, console, test or none (alert file alerts only)
"unsock" enables UNIX socket logging (experimental).
-b Log packets in tcpdump format (much faster!)
-B <mask> Obfuscated IP addresses in alerts and packet dumps using CIDR mask
-c <rules> Use Rules File <rules>
-C Print out payloads with character data only (no hex)
-d Dump the Application Layer
-D Run Snort in background (daemon) mode
-e Display the second layer header info
-f Turn off fflush() calls after binary log writes
-F <bpf> Read BPF filters from file <bpf>
-g <gname> Run snort gid as <gname> group (or gid) after initialization
-G <0xid> Log Identifier (to uniquely id events for multiple snorts)
-h <hn> Set home network = <hn>
(for use with -l or -B, does NOT change $HOME_NET in IDS mode)
-H Make hash tables deterministic.
-i <if> Listen on interface <if>
-I Add Interface name to alert output
-k <mode> Checksum mode (all,noip,notcp,noudp,noicmp,none)
-K <mode> Logging mode (pcap[default],ascii,none)
-l <ld> Log to directory <ld>
-L <file> Log to this tcpdump file
-M Log messages to syslog (not alerts)
-m <umask> Set umask = <umask>
-n <cnt> Exit after receiving <cnt> packets
-N Turn off logging (alerts still work)
-O Obfuscate the logged IP addresses
-p Disable promiscuous mode sniffing
-P <snap> Set explicit snaplen of packet (default: 1514)
-q Quiet. Don't show banner and status report
-Q Enable inline mode operation.
-r <tf> Read and process tcpdump file <tf>
-R <id> Include 'id' in snort_intf<id>.pid file name
-s Log alert messages to syslog
-S <n=v> Set rules file variable n equal to value v
-t <dir> Chroots process to <dir> after initialization
-T Test and report on the current Snort configuration
:

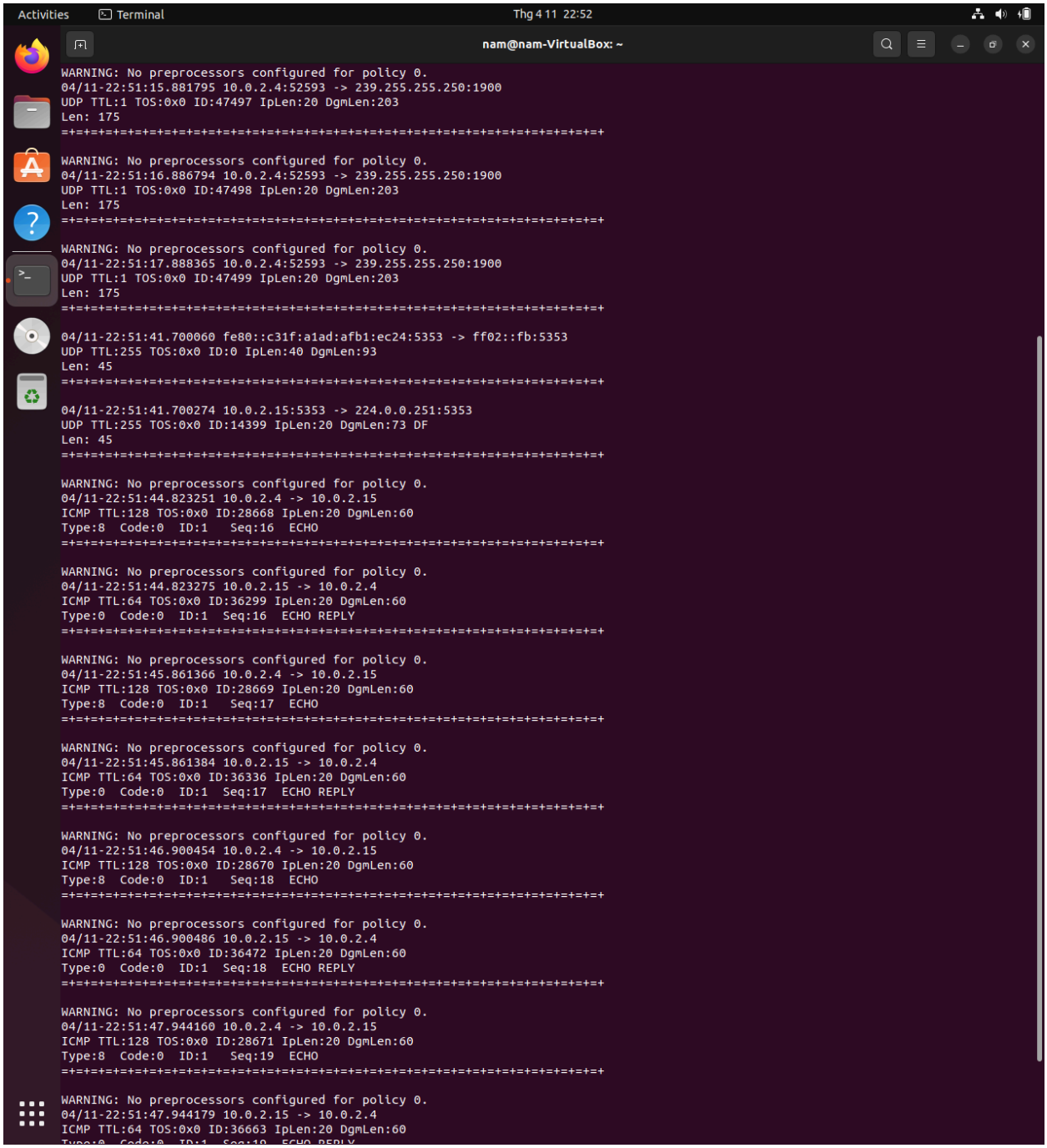

Activities
Terminal
Thg 4 11 15:54
nam@nam-VirtualBox: ~
SNORT(8) System Manager's Manual SNORT(8)
NAME
Snort - open source network intrusion detection system
SYNOPSIS
snort [-bCdDeEfHIMNOpqQsTUvVwWxXy?] [-A alert-mode] [-B address-conversion-mask] [-c rules-file] [-F bpf-file] [-g group-name] [-G id] [-h home-net] [-i interface] [-k checksum-mode] [-K logging-mode] [-l log-dir] [-L bin-log-file] [-m umask] [-n packet-count] [-P snap-length] [-r tcpdump-file] [-R name] [-S variable=value] [-t chroot_directory] [-u user-name] [-Z pathname] [--logid id] [--perfmon-file pathname] [--pid-path pathname] [--snaplen snap-length] [--help] [--version] [--dynamic-engine-lib file] [--dynamic-engine-lib-dir directory] [--dynamic-detection-lib file] [--dynamic-detection-lib-dir directory] [--dump-dynamic-rules directory] [--dynamic-preprocessor-lib file] [--dynamic-preprocessor-lib-dir directory] [--dynamic-output-lib file] [--dynamic-output-lib-dir directory] [--alert-before-pass] [--treat-drop-as-alert] [--treat-drop-as-ignore] [--process-all-events] [--enable-inline-test] [--create-pidfile] [--nolock-pidfile] [--no-interface-pidfile] [--disable-attribute-reload-thread] [--pcap-single= tcpdump-file] [--pcap-filter= filter] [--pcap-list= list] [--pcap-dir= directory] [--pcap-file= file] [--pcap-no-filter] [--pcap-reset] [--pcap-reload] [--pcap-show] [--exit-check count] [--conf-error-out] [--enable-mpls-multicast] [--enable-mpls-overlapping-ip] [--max-mpls-labelchain-len] [--mpls-payload-type] [--require-rule-sid] [--daq type] [--daq-mode mode] [--daq-var name=value] [--daq-dir dir] [--daq-list [dir]] [--dirty-pig] [--cs-dir dir] [--ha-peer] [--ha-out file] [--ha-in file] expression
DESCRIPTION
Snort is an open source network intrusion detection system, capable of performing real-time traffic analysis and packet logging on IP networks. It can perform protocol analysis, content searching/matching and can be used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, OS fingerprinting attempts, and much more. Snort uses a flexible rules language to describe traffic that it should collect or pass, as well as a detection engine that utilizes a modular plugin architecture. Snort also has a modular real-time alerting capability, incorporating alerting and logging plugins for syslog, a ASCII text files, UNIX sockets or XML.
Snort has three primary uses. It can be used as a straight packet sniffer like tcpdump(1), a packet logger (useful for network traffic debugging, etc), or as a full blown network intrusion detection system.
Snort logs packets in tcpdump(1) binary format or in Snort's decoded ASCII format to a hierarchy of logging directories that are named based on the IP address of the "foreign" host.
OPTIONS
-A alert-mode
Alert using the specified alert-mode. Valid alert modes include fast, full, none, and unsock. Fast writes alerts to the default "alert" file in a single-line, syslog style alert message. Full writes the alert to the "alert"
Manual page snort(8) line 1 (press h for help or q to quit)

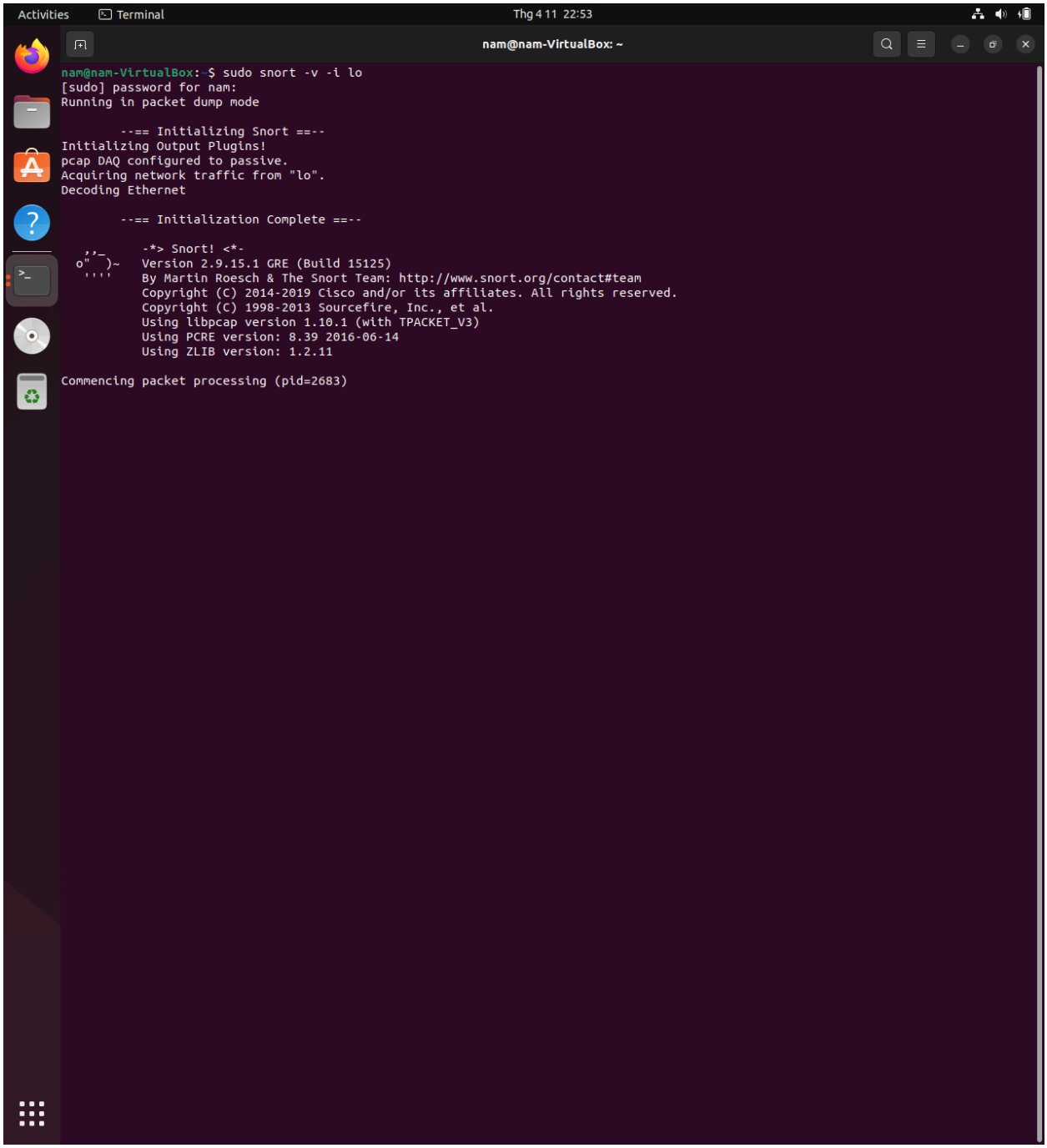

Activities
Terminal
Thg 4 11 15:54
nam@nam-VirtualBox: ~
nam@nam-VirtualBox:~$ snort -h | less
nam@nam-VirtualBox:~$ man snort
nam@nam-VirtualBox:~$ snort -v
Running in packet dump mode
--== Initializing Snort ==--
Initializing Output Plugins!
pcap DAQ configured to passive.
Acquiring network traffic from "enp0s3".
ERROR: Can't start DAQ (-1) - socket: Operation not permitted!
Fatal Error, Quitting..
nam@nam-VirtualBox:~$ snort -V
-*> Snort! <*-
Version 2.9.15.1 GRE (Build 15125)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.10.1 (with TPACKET_V3)
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.2.11
nam@nam-VirtualBox:~$

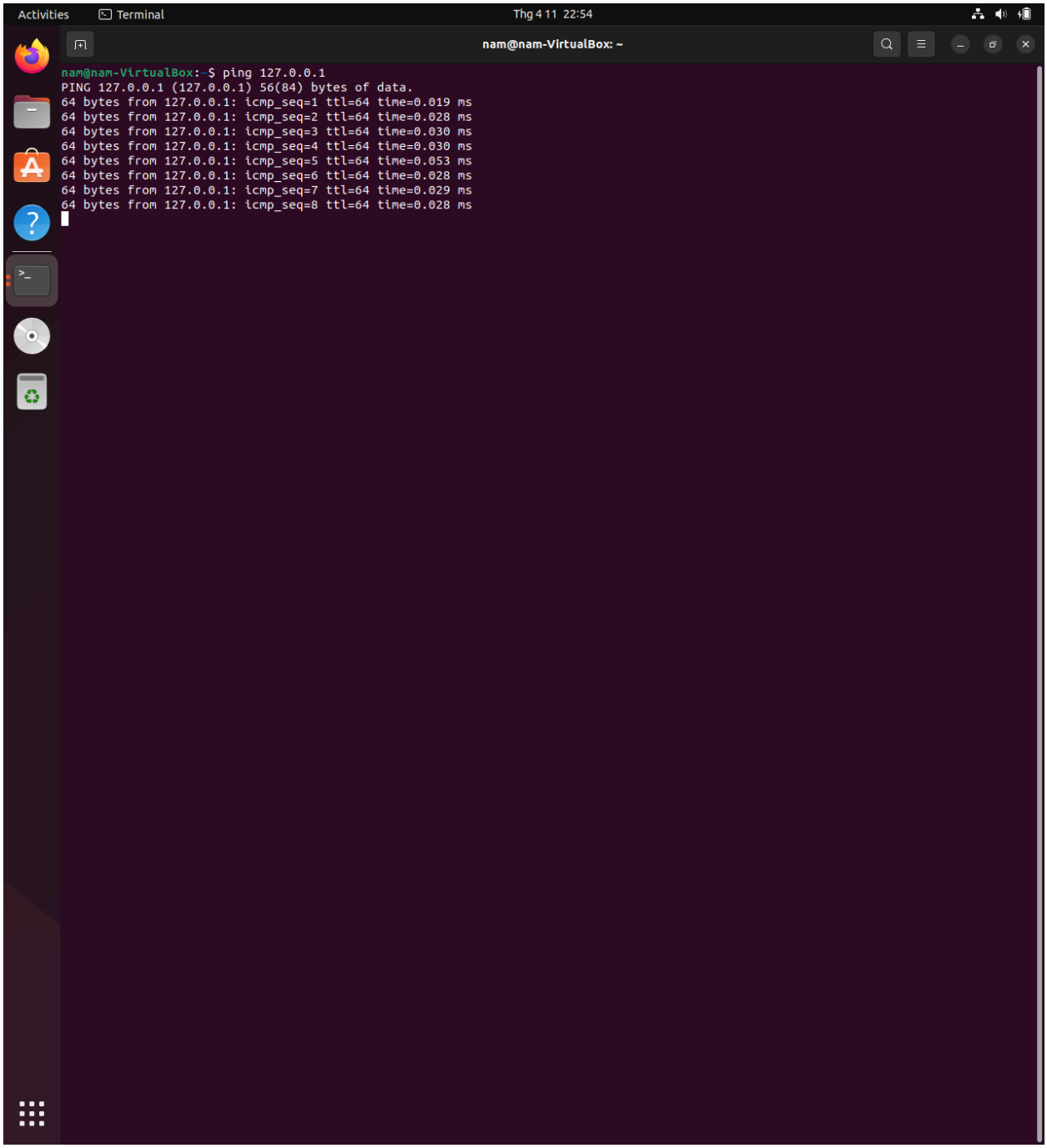

Activities
Terminal
Thg 4 11 15:55
nam@nam-VirtualBox: ~
nam@nam-VirtualBox:~$ sudo snort -v
Running in packet dump mode
--== Initializing Snort ==--
Initializing Output Plugins!
pcap DAQ configured to passive.
Acquiring network traffic from "enp0s3".
Decoding Ethernet
--== Initialization Complete ==--
-*> Snort! <*-
Version 2.9.15.1 GRE (Build 15125)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.10.1 (with TPACKET_V3)
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.2.11
Commencing packet processing (pid=19526)
04/11-15:55:34.189830 10.0.2.15:48175 -> 1.1.1.1:53
UDP TTL:64 TOS:0x0 ID:51817 IpLen:20 DgmLen:75
Len: 47
WARNING: No preprocessors configured for policy 0.
04/11-15:55:34.211776 1.1.1.1:53 -> 10.0.2.15:48175
UDP TTL:64 TOS:0x0 ID:59648 IpLen:20 DgmLen:136
Len: 108
04/11-15:55:34.212127 10.0.2.15:56098 -> 162.213.33.48:443
TCP TTL:64 TOS:0x0 ID:23070 IpLen:20 DgmLen:60 DF
******S* Seq: 0x7C02DDCF Ack: 0x0 Win: 0xFAF0 TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 893470562 0 NOP WS: 7
04/11-15:55:35.362407 10.0.2.15:56098 -> 162.213.33.48:443

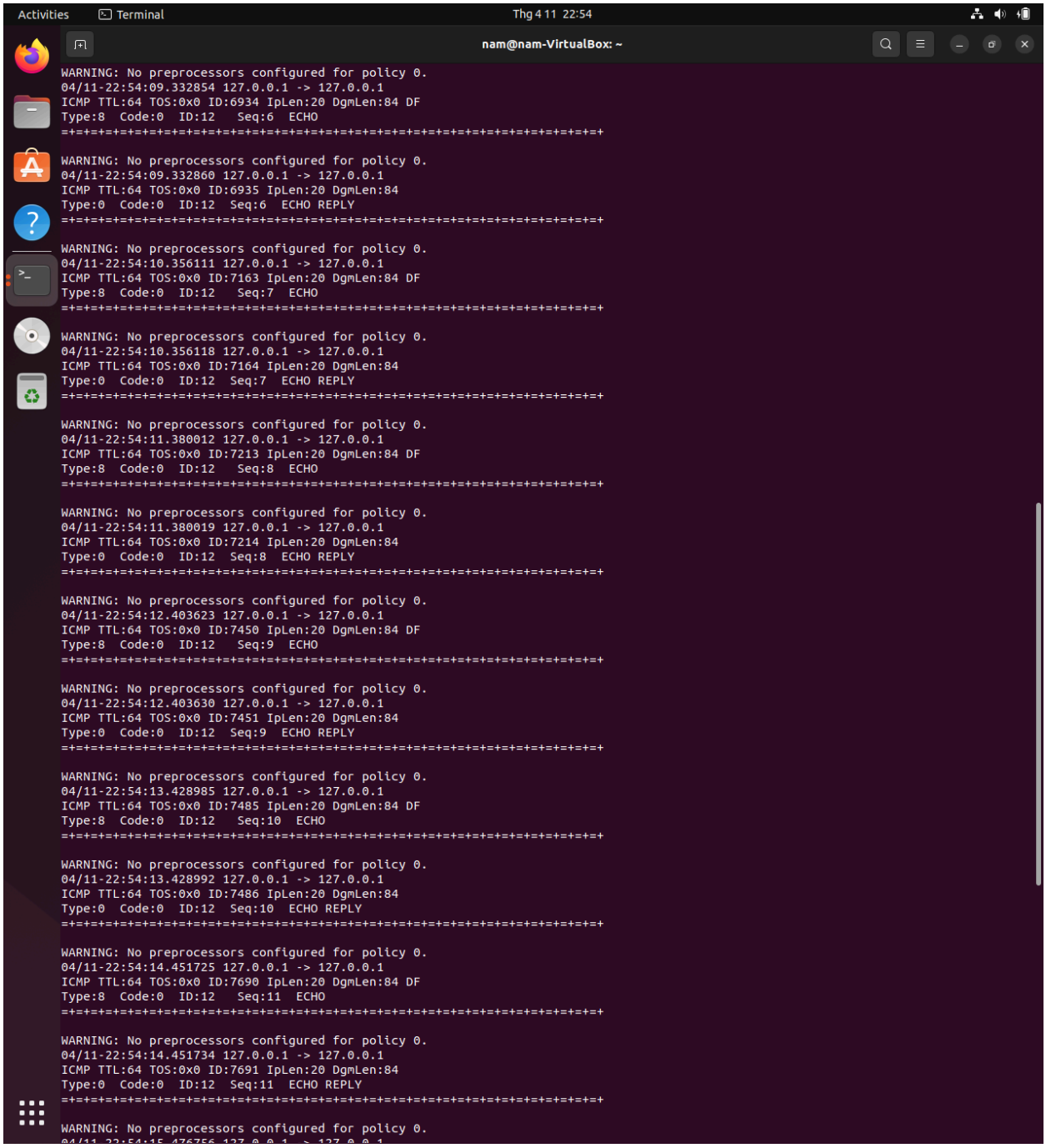

Activities
Terminal
Thg 4 11 16:26
nam@nam-VirtualBox: ~
Breakdown by protocol (includes rebuilt packets):
Eth: 12 (100.000%)
VLAN: 0 (0.000%)
IP4: 10 (83.333%)
Frag: 0 (0.000%)
ICMP: 0 (0.000%)
UDP: 3 (25.000%)
TCP: 7 (58.333%)
IP6: 0 (0.000%)
IP6 Ext: 0 (0.000%)
IP6 Opts: 0 (0.000%)
Frag6: 0 (0.000%)
ICMP6: 0 (0.000%)
UDP6: 0 (0.000%)
TCP6: 0 (0.000%)
Teredo: 0 (0.000%)
ICMP-IP: 0 (0.000%)
IP4/IP4: 0 (0.000%)
IP4/IP6: 0 (0.000%)
IP6/IP4: 0 (0.000%)
IP6/IP6: 0 (0.000%)
GRE: 0 (0.000%)
GRE Eth: 0 (0.000%)
GRE VLAN: 0 (0.000%)
GRE IP4: 0 (0.000%)
GRE IP6: 0 (0.000%)
GRE IP6 Ext: 0 (0.000%)
GRE PPTP: 0 (0.000%)
GRE ARP: 0 (0.000%)
GRE IPX: 0 (0.000%)
GRE Loop: 0 (0.000%)
MPLS: 0 (0.000%)
ARP: 2 (16.667%)
IPX: 0 (0.000%)
Eth Loop: 0 (0.000%)
Eth Disc: 0 (0.000%)
IP4 Disc: 0 (0.000%)
IP6 Disc: 0 (0.000%)
TCP Disc: 0 (0.000%)

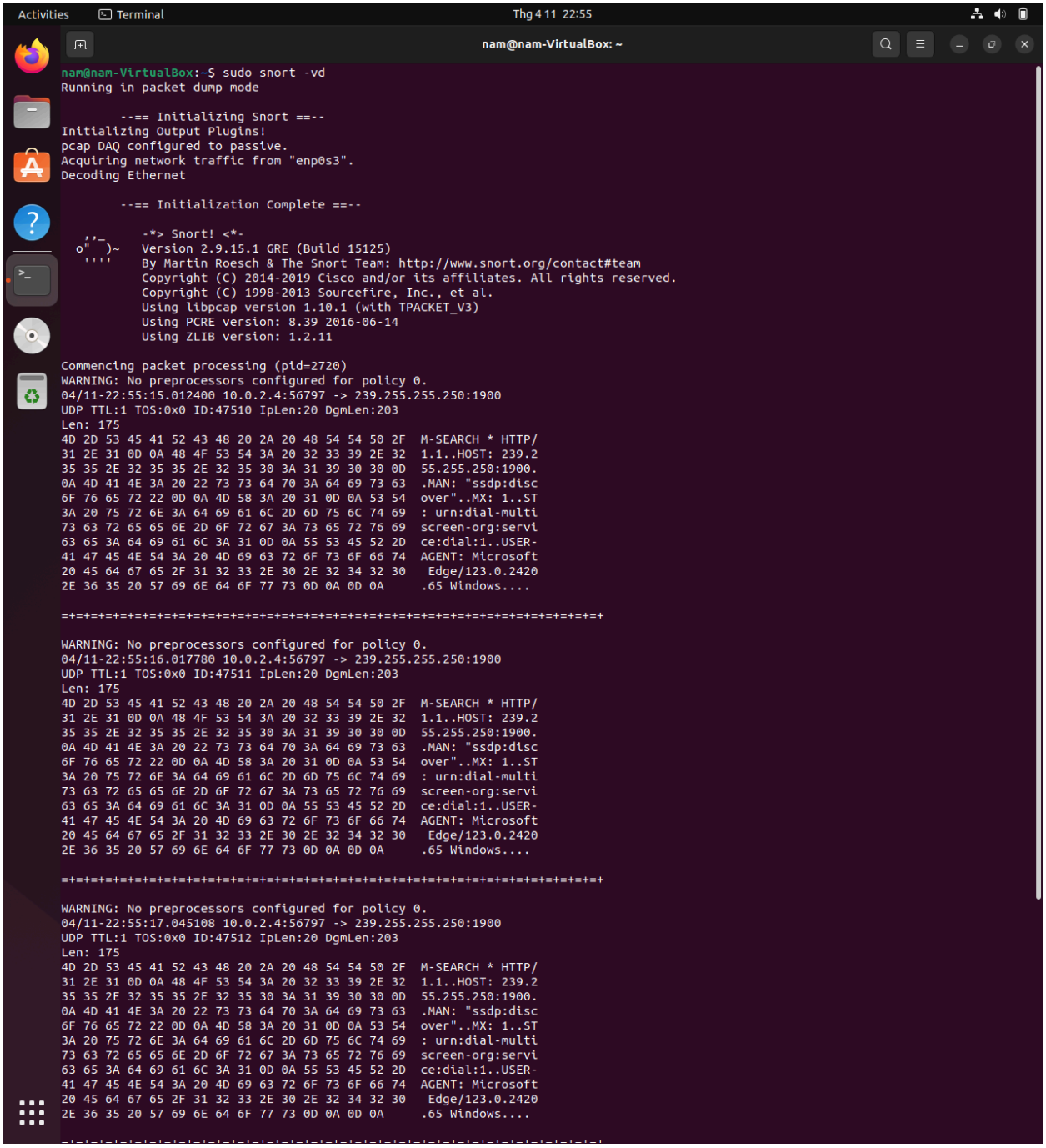

Activities
Terminal
Thg 4 11 22:37
nam@nam-VirtualBox: ~
nam@nam-VirtualBox:~$ sudo snort -v -i enp0s3
Running in packet dump mode
--== Initializing Snort ==--
Initializing Output Plugins!
pcap DAQ configured to passive.
Acquiring network traffic from "enp0s3".
Decoding Ethernet
--== Initialization Complete ==--
-*> Snort! <*-
Version 2.9.15.1 GRE (Build 15125)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.10.1 (with TPACKET_V3)
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.2.11
Commencing packet processing (pid=2119)

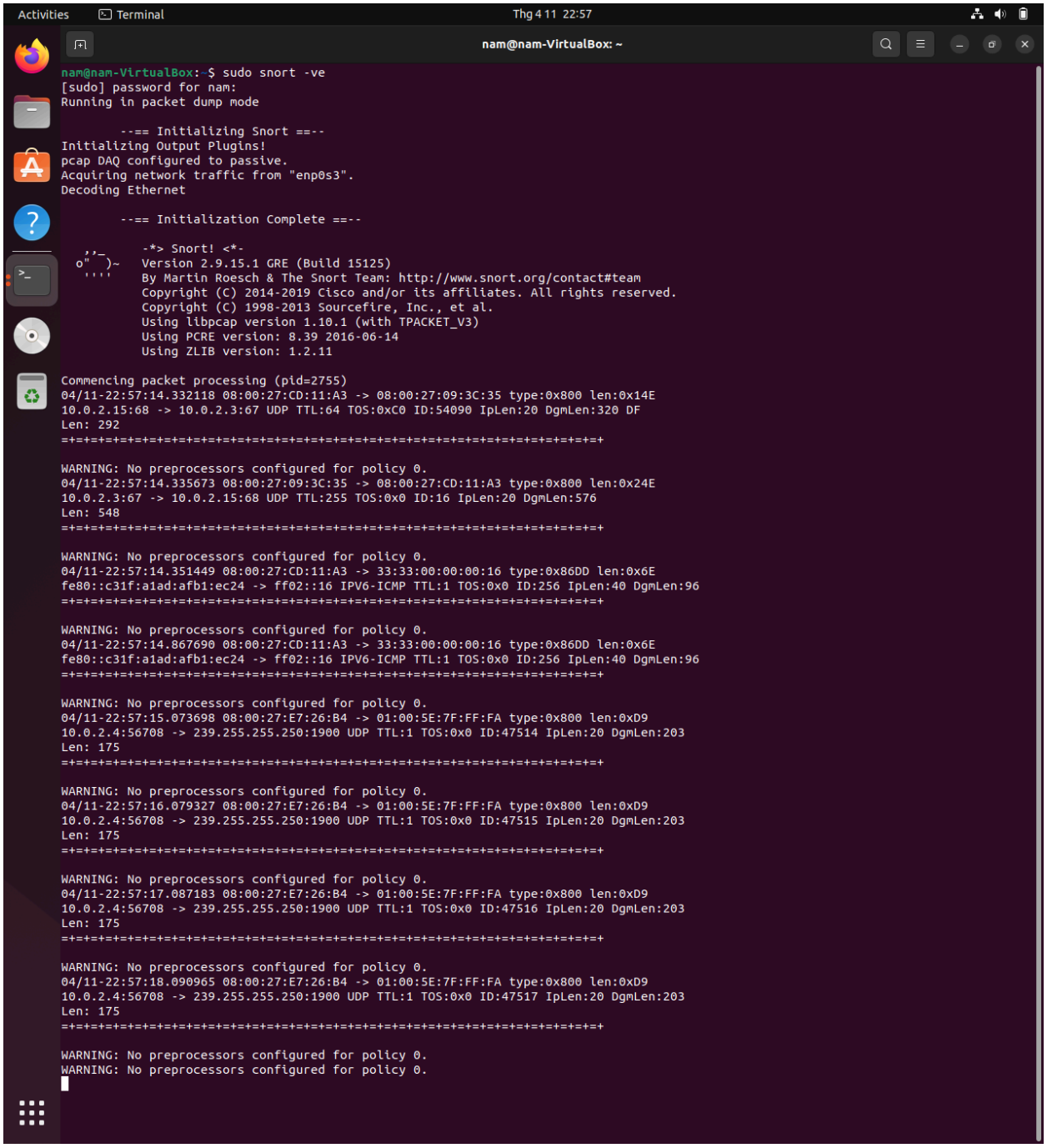

Activities
Terminal
Thg 4 11 22:52
nam@nam-VirtualBox: ~
WARNING: No preprocessors configured for policy 0.
04/11-22:51:15.881795 10.0.2.4:52593 -> 239.255.255.250:1900
UDP TTL:1 TOS:0x0 ID:47497 IpLen:20 DgmLen:203
Len: 175
WARNING: No preprocessors configured for policy 0.
04/11-22:51:16.886794 10.0.2.4:52593 -> 239.255.255.250:1900
UDP TTL:1 TOS:0x0 ID:47498 IpLen:20 DgmLen:203
Len: 175
WARNING: No preprocessors configured for policy 0.
04/11-22:51:17.888365 10.0.2.4:52593 -> 239.255.255.250:1900
UDP TTL:1 TOS:0x0 ID:47499 IpLen:20 DgmLen:203
Len: 175
04/11-22:51:41.700060 fe80::c31f:a1ad:afb1:ec24:5353 -> ff02::fb:5353
UDP TTL:255 TOS:0x0 ID:0 IpLen:40 DgmLen:93
Len: 45
04/11-22:51:41.700274 10.0.2.15:5353 -> 224.0.0.251:5353
UDP TTL:255 TOS:0x0 ID:14399 IpLen:20 DgmLen:73 DF
Len: 45
WARNING: No preprocessors configured for policy 0.
04/11-22:51:44.823251 10.0.2.4 -> 10.0.2.15
ICMP TTL:128 TOS:0x0 ID:28668 IpLen:20 DgmLen:60
Type:8 Code:0 ID:1 Seq:16 ECHO
WARNING: No preprocessors configured for policy 0.
04/11-22:51:44.823275 10.0.2.15 -> 10.0.2.4
ICMP TTL:64 TOS:0x0 ID:36299 IpLen:20 DgmLen:60
Type:0 Code:0 ID:1 Seq:16 ECHO REPLY
WARNING: No preprocessors configured for policy 0.
04/11-22:51:45.861366 10.0.2.4 -> 10.0.2.15
ICMP TTL:128 TOS:0x0 ID:28669 IpLen:20 DgmLen:60
Type:8 Code:0 ID:1 Seq:17 ECHO
WARNING: No preprocessors configured for policy 0.
04/11-22:51:45.861384 10.0.2.15 -> 10.0.2.4
ICMP TTL:64 TOS:0x0 ID:36336 IpLen:20 DgmLen:60
Type:0 Code:0 ID:1 Seq:17 ECHO REPLY
WARNING: No preprocessors configured for policy 0.
04/11-22:51:46.900454 10.0.2.4 -> 10.0.2.15
ICMP TTL:128 TOS:0x0 ID:28670 IpLen:20 DgmLen:60
Type:8 Code:0 ID:1 Seq:18 ECHO
WARNING: No preprocessors configured for policy 0.
04/11-22:51:46.900486 10.0.2.15 -> 10.0.2.4
ICMP TTL:64 TOS:0x0 ID:36472 IpLen:20 DgmLen:60
Type:0 Code:0 ID:1 Seq:18 ECHO REPLY
WARNING: No preprocessors configured for policy 0.
04/11-22:51:47.944160 10.0.2.4 -> 10.0.2.15
ICMP TTL:128 TOS:0x0 ID:28671 IpLen:20 DgmLen:60
Type:8 Code:0 ID:1 Seq:19 ECHO
WARNING: No preprocessors configured for policy 0.
04/11-22:51:47.944179 10.0.2.15 -> 10.0.2.4
ICMP TTL:64 TOS:0x0 ID:36663 IpLen:20 DgmLen:60

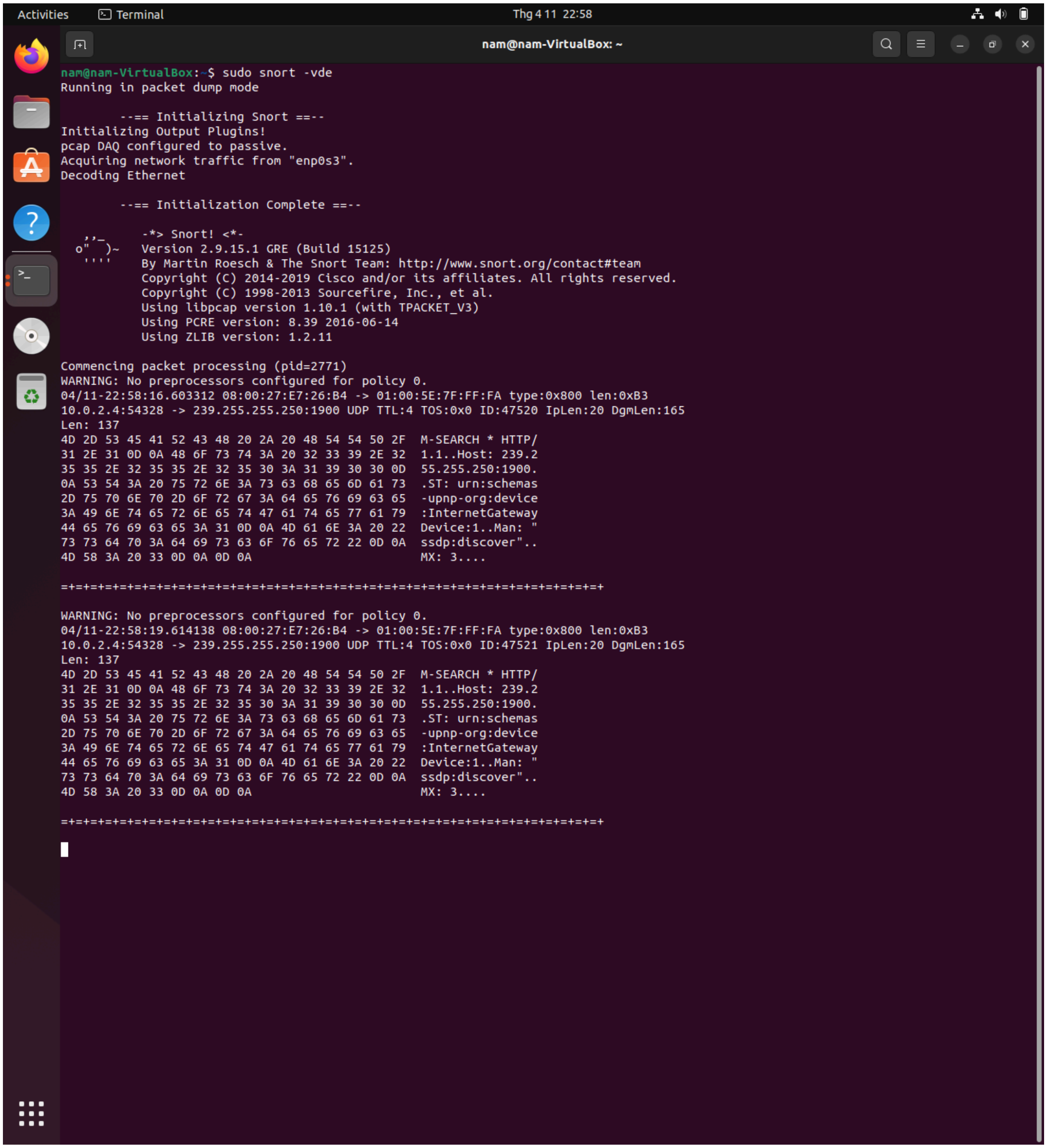

Activities
Terminal
Thg 4 11 22:53
nam@nam-VirtualBox: ~
nam@nam-VirtualBox:~$ sudo snort -v -i lo
[sudo] password for nam:
Running in packet dump mode
--== Initializing Snort ==--
Initializing Output Plugins!
pcap DAQ configured to passive.
Acquiring network traffic from "lo".
Decoding Ethernet
--== Initialization Complete ==--
-*> Snort! <*-
Version 2.9.15.1 GRE (Build 15125)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.10.1 (with TPACKET_V3)
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.2.11
Commencing packet processing (pid=2683)


Activities
Terminal
Thg 4 11 22:54
nam@nam-VirtualBox: ~
nam@nam-VirtualBox:~$ ping 127.0.0.1
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.019 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.028 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.030 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.030 ms
64 bytes from 127.0.0.1: icmp_seq=5 ttl=64 time=0.053 ms
64 bytes from 127.0.0.1: icmp_seq=6 ttl=64 time=0.028 ms
64 bytes from 127.0.0.1: icmp_seq=7 ttl=64 time=0.029 ms
64 bytes from 127.0.0.1: icmp_seq=8 ttl=64 time=0.028 ms

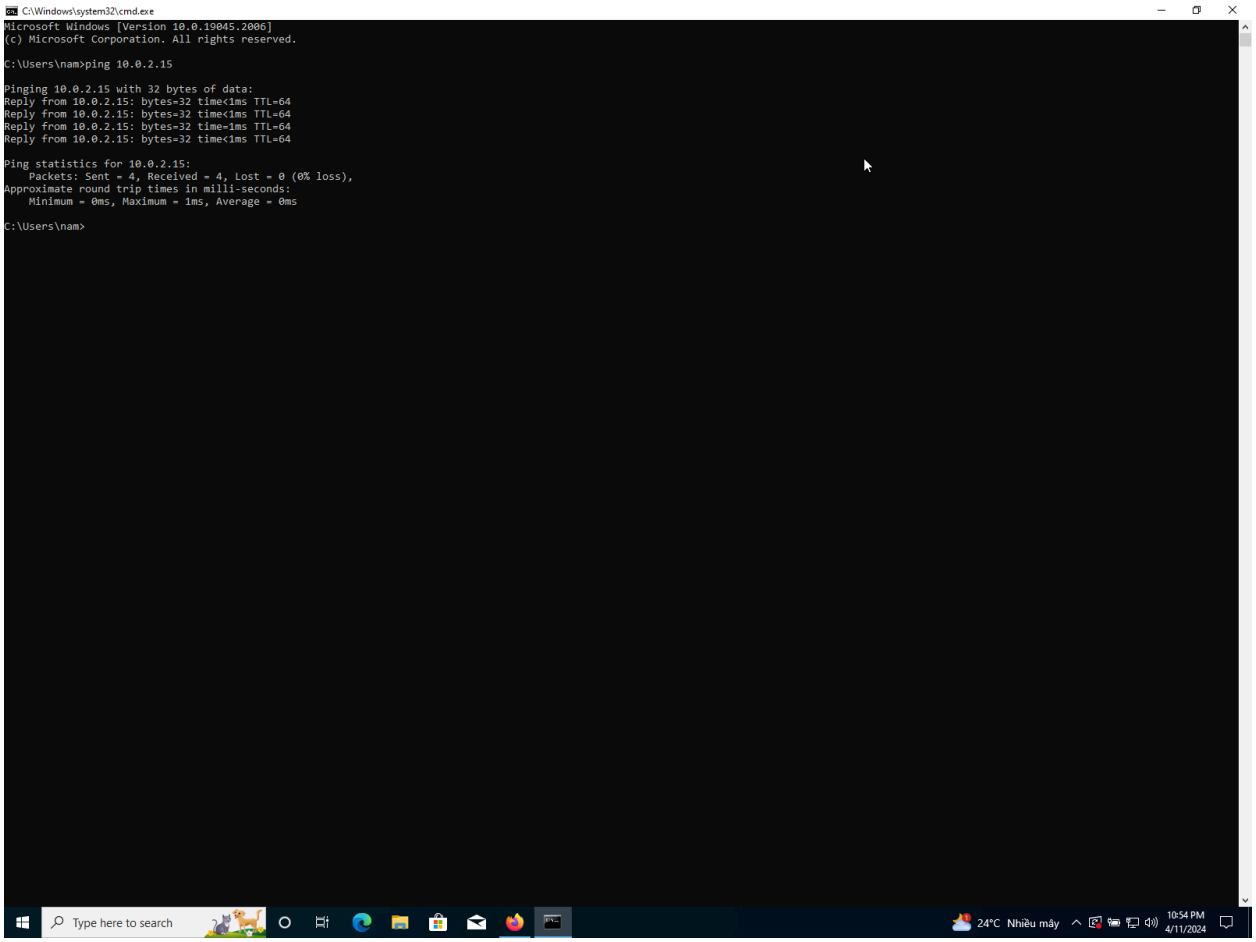

Activities
Terminal
Thg 4 11 22:54
nam@nam-VirtualBox: ~
WARNING: No preprocessors configured for policy 0.
04/11-22:54:09.332854 127.0.0.1 -> 127.0.0.1
ICMP TTL:64 TOS:0x0 ID:6934 IpLen:20 DgmLen:84 DF
Type:8 Code:0 ID:12 Seq:6 ECHO
WARNING: No preprocessors configured for policy 0.
04/11-22:54:09.332860 127.0.0.1 -> 127.0.0.1
ICMP TTL:64 TOS:0x0 ID:6935 IpLen:20 DgmLen:84
Type:0 Code:0 ID:12 Seq:6 ECHO REPLY
WARNING: No preprocessors configured for policy 0.
04/11-22:54:10.356111 127.0.0.1 -> 127.0.0.1
ICMP TTL:64 TOS:0x0 ID:7163 IpLen:20 DgmLen:84 DF
Type:8 Code:0 ID:12 Seq:7 ECHO
WARNING: No preprocessors configured for policy 0.
04/11-22:54:10.356118 127.0.0.1 -> 127.0.0.1
ICMP TTL:64 TOS:0x0 ID:7164 IpLen:20 DgmLen:84
Type:0 Code:0 ID:12 Seq:7 ECHO REPLY
WARNING: No preprocessors configured for policy 0.
04/11-22:54:11.380012 127.0.0.1 -> 127.0.0.1
ICMP TTL:64 TOS:0x0 ID:7213 IpLen:20 DgmLen:84 DF
Type:8 Code:0 ID:12 Seq:8 ECHO
WARNING: No preprocessors configured for policy 0.
04/11-22:54:11.380019 127.0.0.1 -> 127.0.0.1
ICMP TTL:64 TOS:0x0 ID:7214 IpLen:20 DgmLen:84
Type:0 Code:0 ID:12 Seq:8 ECHO REPLY
WARNING: No preprocessors configured for policy 0.
04/11-22:54:12.403623 127.0.0.1 -> 127.0.0.1
ICMP TTL:64 TOS:0x0 ID:7450 IpLen:20 DgmLen:84 DF
Type:8 Code:0 ID:12 Seq:9 ECHO
WARNING: No preprocessors configured for policy 0.
04/11-22:54:12.403630 127.0.0.1 -> 127.0.0.1
ICMP TTL:64 TOS:0x0 ID:7451 IpLen:20 DgmLen:84
Type:0 Code:0 ID:12 Seq:9 ECHO REPLY
WARNING: No preprocessors configured for policy 0.
04/11-22:54:13.428985 127.0.0.1 -> 127.0.0.1
ICMP TTL:64 TOS:0x0 ID:7485 IpLen:20 DgmLen:84 DF
Type:8 Code:0 ID:12 Seq:10 ECHO
WARNING: No preprocessors configured for policy 0.
04/11-22:54:13.428992 127.0.0.1 -> 127.0.0.1
ICMP TTL:64 TOS:0x0 ID:7486 IpLen:20 DgmLen:84
Type:0 Code:0 ID:12 Seq:10 ECHO REPLY
WARNING: No preprocessors configured for policy 0.
04/11-22:54:14.451725 127.0.0.1 -> 127.0.0.1
ICMP TTL:64 TOS:0x0 ID:7690 IpLen:20 DgmLen:84 DF
Type:8 Code:0 ID:12 Seq:11 ECHO
WARNING: No preprocessors configured for policy 0.
04/11-22:54:14.451734 127.0.0.1 -> 127.0.0.1
ICMP TTL:64 TOS:0x0 ID:7691 IpLen:20 DgmLen:84
Type:0 Code:0 ID:12 Seq:11 ECHO REPLY
WARNING: No preprocessors configured for policy 0.

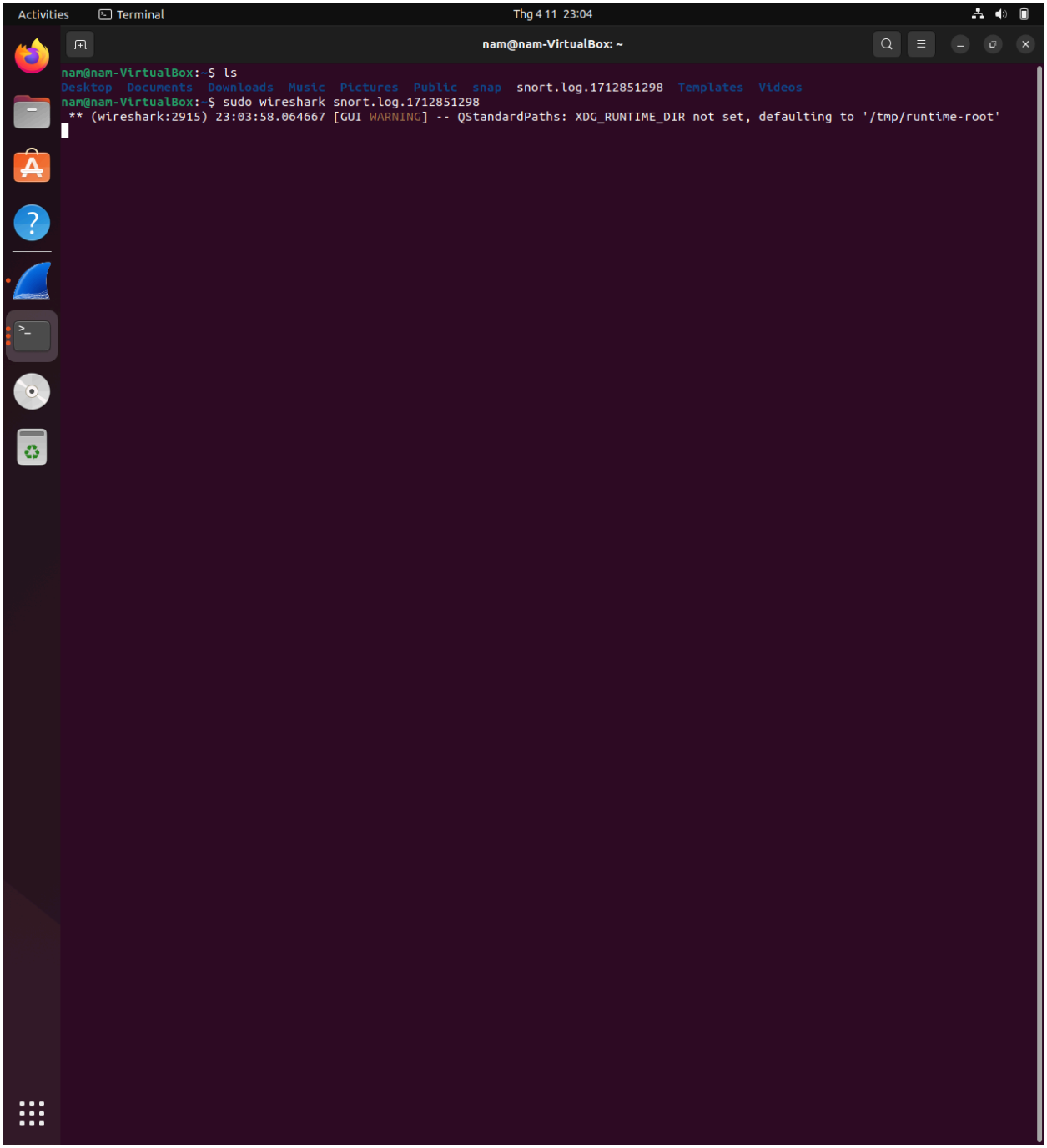

Activities
Terminal
Thg 4 11 22:55
nam@nam-VirtualBox: ~
nam@nam-VirtualBox:~$ sudo snort -vd
Running in packet dump mode
--== Initializing Snort ==--
Initializing Output Plugins!
pcap DAQ configured to passive.
Acquiring network traffic from "enp0s3".
Decoding Ethernet
--== Initialization Complete ==--
-*> Snort! <*-
Version 2.9.15.1 GRE (Build 15125)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.10.1 (with TPACKET_V3)
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.2.11
Commencing packet processing (pid=2720)
WARNING: No preprocessors configured for policy 0.
04/11-22:55:15.012400 10.0.2.4:56797 -> 239.255.255.250:1900
UDP TTL:1 TOS:0x0 ID:47510 IpLen:20 DgmLen:203
Len: 175
4D 2D 53 45 41 52 43 48 20 2A 20 48 54 54 50 2F M-SEARCH * HTTP/
31 2E 31 0D 0A 48 4F 53 54 3A 20 32 33 39 2E 32 1.1..HOST: 239.2
35 35 2E 32 35 35 2E 32 35 30 3A 31 39 30 30 0D 55.255.250:1900.
0A 4D 41 4E 3A 20 22 73 73 64 70 3A 64 69 73 63 .MAN: "ssdp:disc
6F 76 65 72 22 0D 0A 4D 58 3A 20 31 0D 0A 53 54 over"..MX: 1..ST
3A 20 75 72 6E 3A 64 69 61 6C 2D 6D 75 6C 74 69 : urn:dial-multi
73 63 72 65 65 6E 2D 6F 72 67 3A 73 65 72 76 69 screen-org:servi
63 65 3A 64 69 61 6C 3A 31 0D 0A 55 53 45 52 2D ce:dial:1..USER-
41 47 45 4E 54 3A 20 4D 69 63 72 6F 73 6F 66 74 AGENT: Microsoft
20 45 64 67 65 2F 31 32 33 2E 30 2E 32 34 32 30 Edge/123.0.2420
2E 36 35 20 57 69 6E 64 6F 77 73 0D 0A 0D 0A .65 Windows....
WARNING: No preprocessors configured for policy 0.
04/11-22:55:16.017780 10.0.2.4:56797 -> 239.255.255.250:1900
UDP TTL:1 TOS:0x0 ID:47511 IpLen:20 DgmLen:203
Len: 175
4D 2D 53 45 41 52 43 48 20 2A 20 48 54 54 50 2F M-SEARCH * HTTP/
31 2E 31 0D 0A 48 4F 53 54 3A 20 32 33 39 2E 32 1.1..HOST: 239.2
35 35 2E 32 35 35 2E 32 35 30 3A 31 39 30 30 0D 55.255.250:1900.
0A 4D 41 4E 3A 20 22 73 73 64 70 3A 64 69 73 63 .MAN: "ssdp:disc
6F 76 65 72 22 0D 0A 4D 58 3A 20 31 0D 0A 53 54 over"..MX: 1..ST
3A 20 75 72 6E 3A 64 69 61 6C 2D 6D 75 6C 74 69 : urn:dial-multi
73 63 72 65 65 6E 2D 6F 72 67 3A 73 65 72 76 69 screen-org:servi
63 65 3A 64 69 61 6C 3A 31 0D 0A 55 53 45 52 2D ce:dial:1..USER-
41 47 45 4E 54 3A 20 4D 69 63 72 6F 73 6F 66 74 AGENT: Microsoft
20 45 64 67 65 2F 31 32 33 2E 30 2E 32 34 32 30 Edge/123.0.2420
2E 36 35 20 57 69 6E 64 6F 77 73 0D 0A 0D 0A .65 Windows....
WARNING: No preprocessors configured for policy 0.
04/11-22:55:17.045108 10.0.2.4:56797 -> 239.255.255.250:1900
UDP TTL:1 TOS:0x0 ID:47512 IpLen:20 DgmLen:203
Len: 175
4D 2D 53 45 41 52 43 48 20 2A 20 48 54 54 50 2F M-SEARCH * HTTP/
31 2E 31 0D 0A 48 4F 53 54 3A 20 32 33 39 2E 32 1.1..HOST: 239.2
35 35 2E 32 35 35 2E 32 35 30 3A 31 39 30 30 0D 55.255.250:1900.
0A 4D 41 4E 3A 20 22 73 73 64 70 3A 64 69 73 63 .MAN: "ssdp:disc
6F 76 65 72 22 0D 0A 4D 58 3A 20 31 0D 0A 53 54 over"..MX: 1..ST
3A 20 75 72 6E 3A 64 69 61 6C 2D 6D 75 6C 74 69 : urn:dial-multi
73 63 72 65 65 6E 2D 6F 72 67 3A 73 65 72 76 69 screen-org:servi
63 65 3A 64 69 61 6C 3A 31 0D 0A 55 53 45 52 2D ce:dial:1..USER-
41 47 45 4E 54 3A 20 4D 69 63 72 6F 73 6F 66 74 AGENT: Microsoft
20 45 64 67 65 2F 31 32 33 2E 30 2E 32 34 32 30 Edge/123.0.2420
2E 36 35 20 57 69 6E 64 6F 77 73 0D 0A 0D 0A .65 Windows....

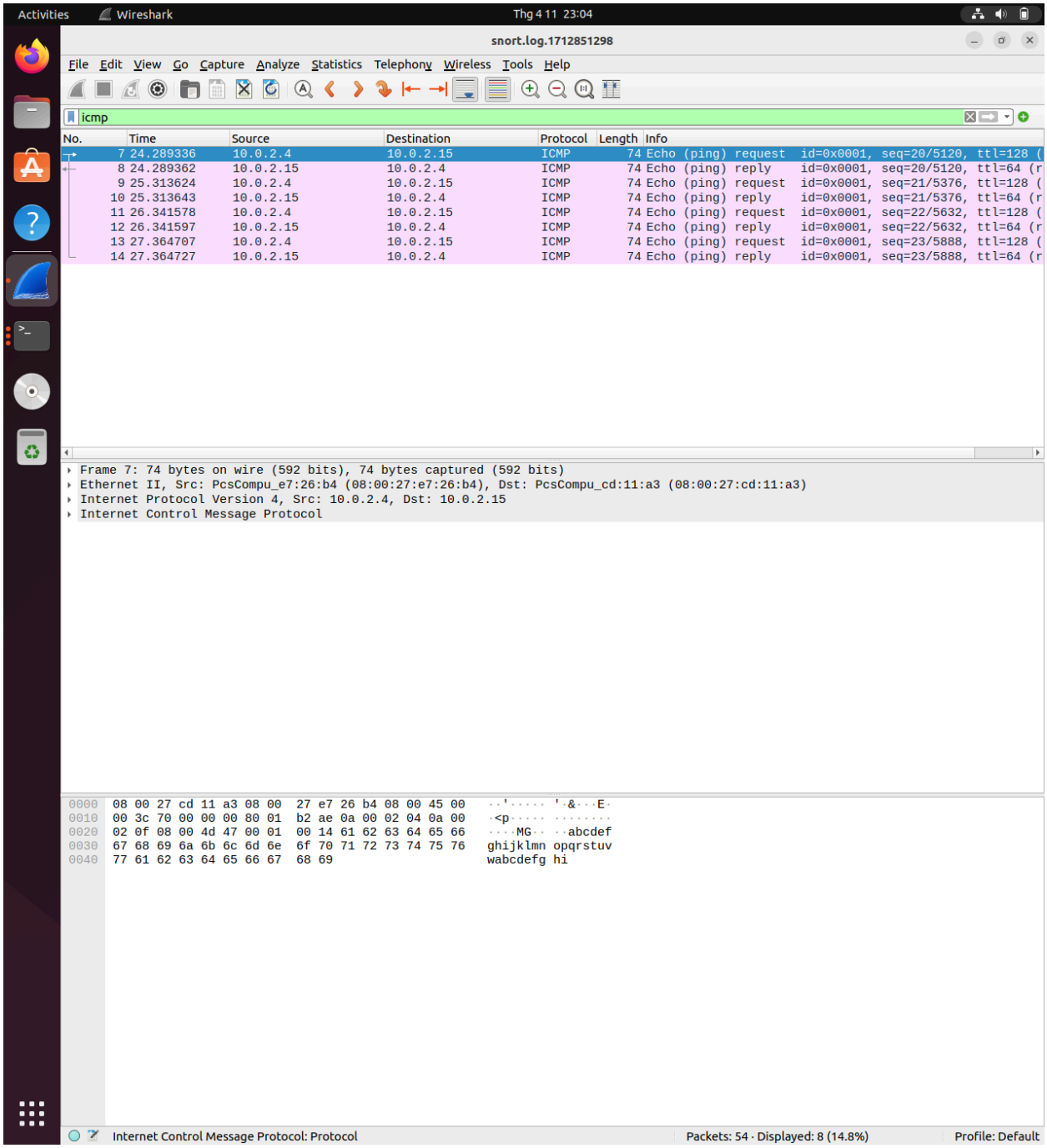

Activities
Terminal
Thg 4 11 22:57
nam@nam-VirtualBox: ~
nam@nam-VirtualBox:~$ sudo snort -ve
[sudo] password for nam:
Running in packet dump mode
--== Initializing Snort ==--
Initializing Output Plugins!
pcap DAQ configured to passive.
Acquiring network traffic from "enp0s3".
Decoding Ethernet
--== Initialization Complete ==--
-*> Snort! <*-
Version 2.9.15.1 GRE (Build 15125)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.10.1 (with TPACKET_V3)
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.2.11
Commencing packet processing (pid=2755)
04/11-22:57:14.332118 08:00:27:CD:11:A3 -> 08:00:27:09:3C:35 type:0x800 len:0x14E
10.0.2.15:68 -> 10.0.2.3:67 UDP TTL:64 TOS:0xC0 ID:54090 IpLen:20 DgmLen:320 DF
Len: 292
WARNING: No preprocessors configured for policy 0.
04/11-22:57:14.335673 08:00:27:09:3C:35 -> 08:00:27:CD:11:A3 type:0x800 len:0x24E
10.0.2.3:67 -> 10.0.2.15:68 UDP TTL:255 TOS:0x0 ID:16 IpLen:20 DgmLen:576
Len: 548
WARNING: No preprocessors configured for policy 0.
04/11-22:57:14.351449 08:00:27:CD:11:A3 -> 33:33:00:00:00:16 type:0x86DD len:0x6E
fe80::c31f:a1ad:afb1:ec24 -> ff02::16 IPV6-ICMP TTL:1 TOS:0x0 ID:256 IpLen:40 DgmLen:96
WARNING: No preprocessors configured for policy 0.
04/11-22:57:14.867690 08:00:27:CD:11:A3 -> 33:33:00:00:00:16 type:0x86DD len:0x6E
fe80::c31f:a1ad:afb1:ec24 -> ff02::16 IPV6-ICMP TTL:1 TOS:0x0 ID:256 IpLen:40 DgmLen:96
WARNING: No preprocessors configured for policy 0.
04/11-22:57:15.073698 08:00:27:E7:26:B4 -> 01:00:5E:7F:FF:FA type:0x800 len:0xD9
10.0.2.4:56708 -> 239.255.255.250:1900 UDP TTL:1 TOS:0x0 ID:47514 IpLen:20 DgmLen:203
Len: 175
WARNING: No preprocessors configured for policy 0.
04/11-22:57:16.079327 08:00:27:E7:26:B4 -> 01:00:5E:7F:FF:FA type:0x800 len:0xD9
10.0.2.4:56708 -> 239.255.255.250:1900 UDP TTL:1 TOS:0x0 ID:47515 IpLen:20 DgmLen:203
Len: 175
WARNING: No preprocessors configured for policy 0.
04/11-22:57:17.087183 08:00:27:E7:26:B4 -> 01:00:5E:7F:FF:FA type:0x800 len:0xD9
10.0.2.4:56708 -> 239.255.255.250:1900 UDP TTL:1 TOS:0x0 ID:47516 IpLen:20 DgmLen:203
Len: 175
WARNING: No preprocessors configured for policy 0.
04/11-22:57:18.090965 08:00:27:E7:26:B4 -> 01:00:5E:7F:FF:FA type:0x800 len:0xD9
10.0.2.4:56708 -> 239.255.255.250:1900 UDP TTL:1 TOS:0x0 ID:47517 IpLen:20 DgmLen:203
Len: 175
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.


Activities
Terminal
Thg 4 11 22:58
nam@nam-VirtualBox: ~
nam@nam-VirtualBox:~$ sudo snort -vde
Running in packet dump mode
--== Initializing Snort ==--
Initializing Output Plugins!
pcap DAQ configured to passive.
Acquiring network traffic from "enp0s3".
Decoding Ethernet
--== Initialization Complete ==--
-*> Snort! <*-
Version 2.9.15.1 GRE (Build 15125)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.10.1 (with TPACKET_V3)
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.2.11
Commencing packet processing (pid=2771)
WARNING: No preprocessors configured for policy 0.
04/11-22:58:16.603312 08:00:27:E7:26:B4 -> 01:00:5E:7F:FF:FA type:0x800 len:0xB3
10.0.2.4:54328 -> 239.255.255.250:1900 UDP TTL:4 TOS:0x0 ID:47520 IpLen:20 DgmLen:165
Len: 137
4D 2D 53 45 41 52 43 48 20 2A 20 48 54 54 50 2F M-SEARCH * HTTP/
31 2E 31 0D 0A 48 6F 73 74 3A 20 32 33 39 2E 32 1.1..Host: 239.2
35 35 2E 32 35 35 2E 32 35 30 3A 31 39 30 30 0D 55.255.250:1900.
0A 53 54 3A 20 75 72 6E 3A 73 63 68 65 6D 61 73 .ST: urn:schemas
2D 75 70 6E 70 2D 6F 72 67 3A 64 65 76 69 63 65 -upnp-org:device
3A 49 6E 74 65 72 6E 65 74 47 61 74 65 77 61 79 :InternetGateway
44 65 76 69 63 65 3A 31 0D 0A 4D 61 6E 3A 20 22 Device:1..Man: "
73 73 64 70 3A 64 69 73 63 6F 76 65 72 22 0D 0A ssdp:discover"..
4D 58 3A 20 33 0D 0A 0D 0A MX: 3....
=+
WARNING: No preprocessors configured for policy 0.
04/11-22:58:19.614138 08:00:27:E7:26:B4 -> 01:00:5E:7F:FF:FA type:0x800 len:0xB3
10.0.2.4:54328 -> 239.255.255.250:1900 UDP TTL:4 TOS:0x0 ID:47521 IpLen:20 DgmLen:165
Len: 137
4D 2D 53 45 41 52 43 48 20 2A 20 48 54 54 50 2F M-SEARCH * HTTP/
31 2E 31 0D 0A 48 6F 73 74 3A 20 32 33 39 2E 32 1.1..Host: 239.2
35 35 2E 32 35 35 2E 32 35 30 3A 31 39 30 30 0D 55.255.250:1900.
0A 53 54 3A 20 75 72 6E 3A 73 63 68 65 6D 61 73 .ST: urn:schemas
2D 75 70 6E 70 2D 6F 72 67 3A 64 65 76 69 63 65 -upnp-org:device
3A 49 6E 74 65 72 6E 65 74 47 61 74 65 77 61 79 :InternetGateway
44 65 76 69 63 65 3A 31 0D 0A 4D 61 6E 3A 20 22 Device:1..Man: "
73 73 64 70 3A 64 69 73 63 6F 76 65 72 22 0D 0A ssdp:discover"..
4D 58 3A 20 33 0D 0A 0D 0A MX: 3....
=+

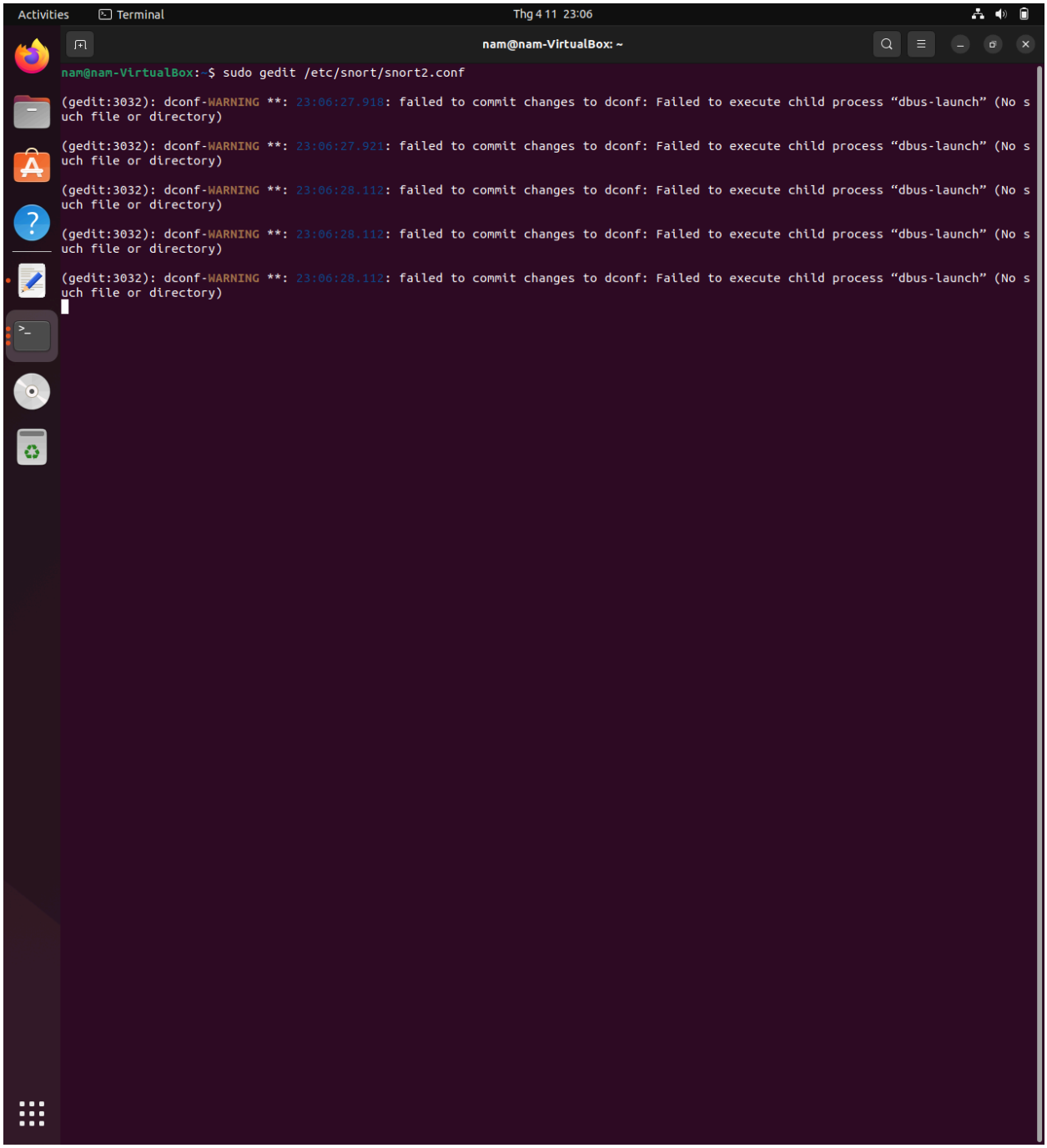
Lab 13.03

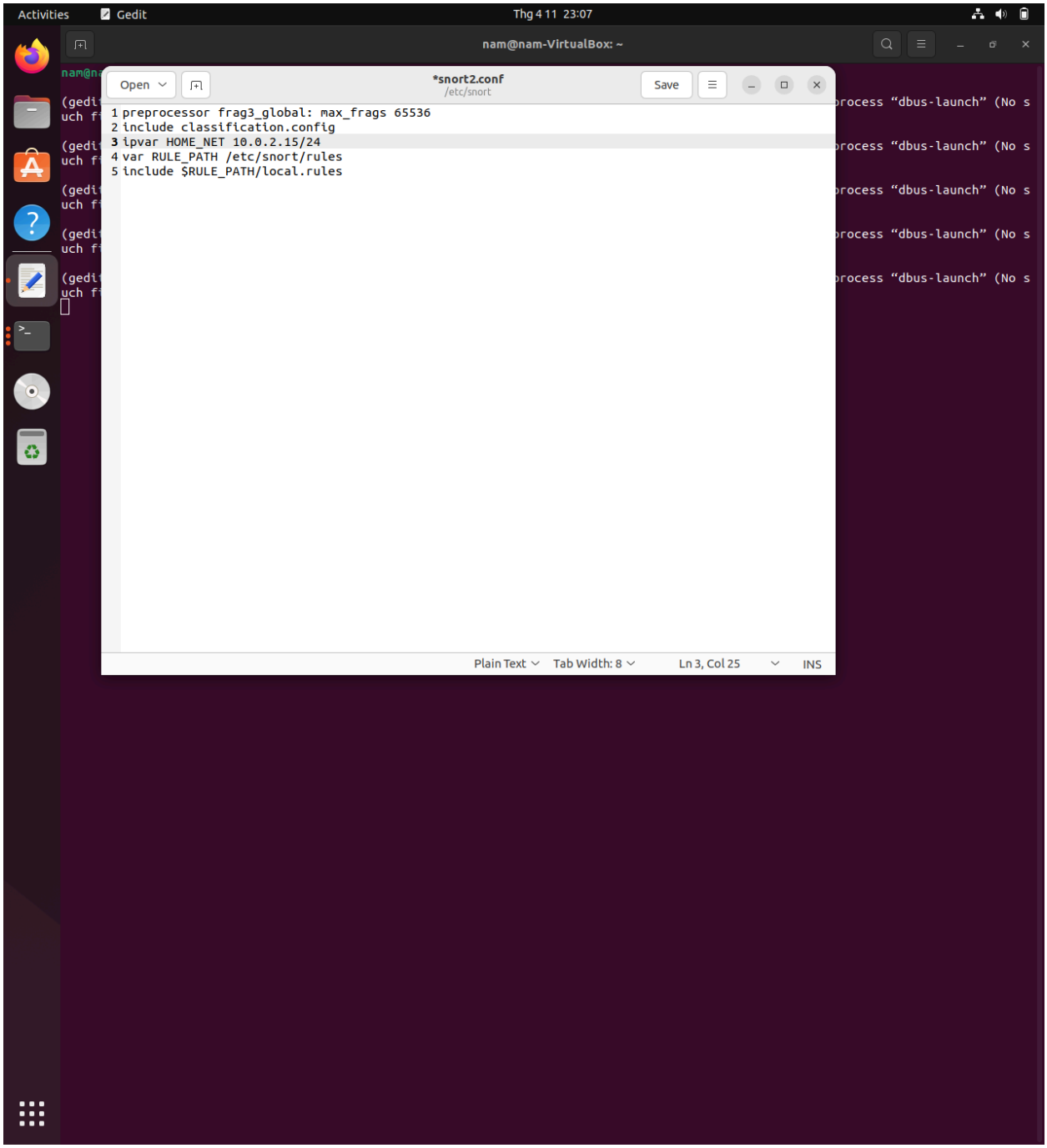

C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.19045.2006]
(c) Microsoft Corporation. All rights reserved.
C:\Users\nam>ping 10.0.2.15
Pinging 10.0.2.15 with 32 bytes of data:
Reply from 10.0.2.15: bytes=32 time<1ms TTL=64
Reply from 10.0.2.15: bytes=32 time<1ms TTL=64
Reply from 10.0.2.15: bytes=32 time<1ms TTL=64
Reply from 10.0.2.15: bytes=32 time<1ms TTL=64
Ping statistics for 10.0.2.15:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\Users\nam>
Type here to search
24°C Nhiều mây
10:54 PM
4/11/2024

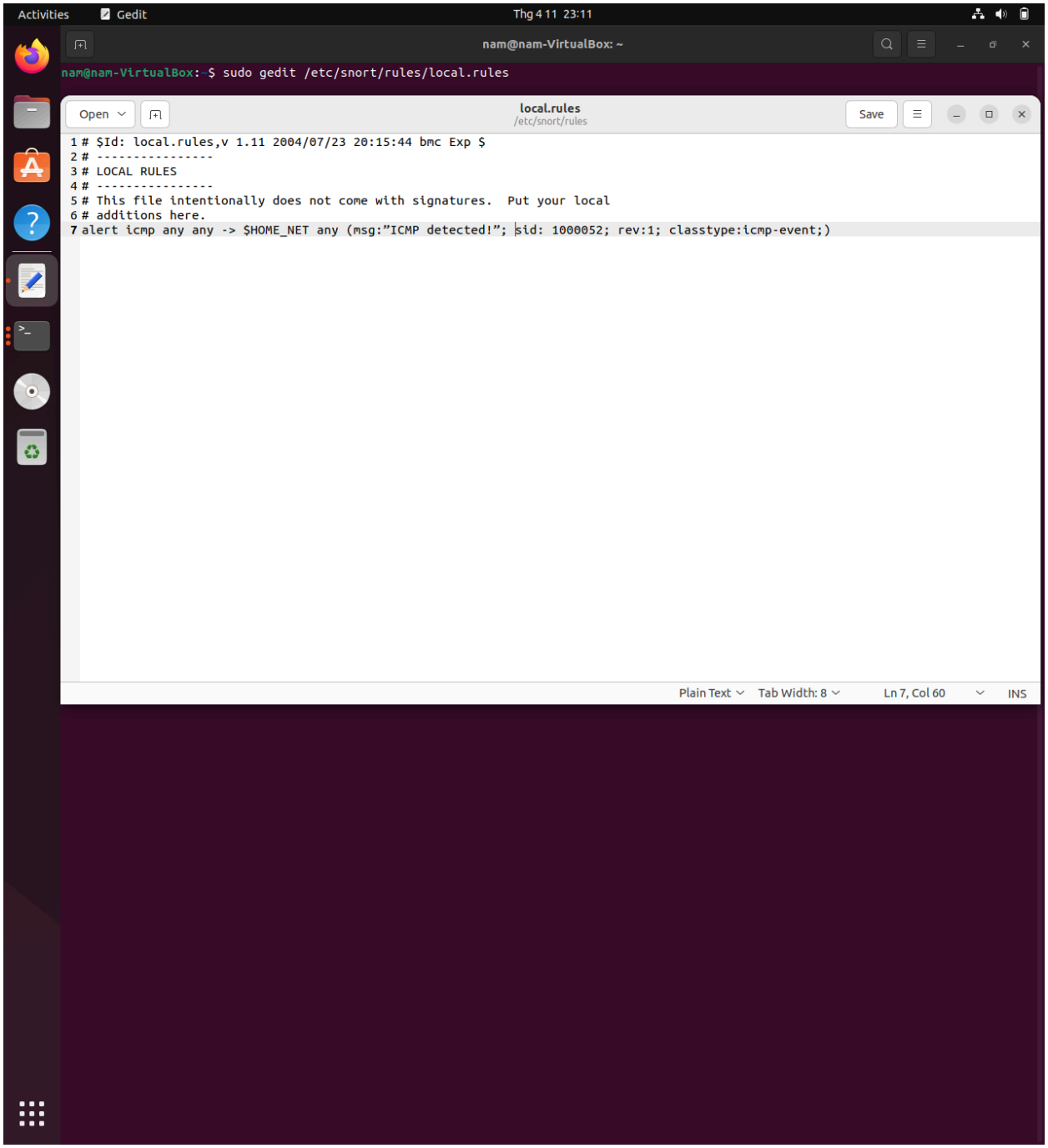

Activities
Terminal
Thg 4 11 23:04
nam@nam-VirtualBox: ~
nam@nam-VirtualBox:~$ ls
Desktop Documents Downloads Music Pictures Public snap snort.log.1712851298 Templates Videos
nam@nam-VirtualBox:~$ sudo wireshark snort.log.1712851298
** (wireshark:2915) 23:03:58.064667 [GUI WARNING] -- QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'

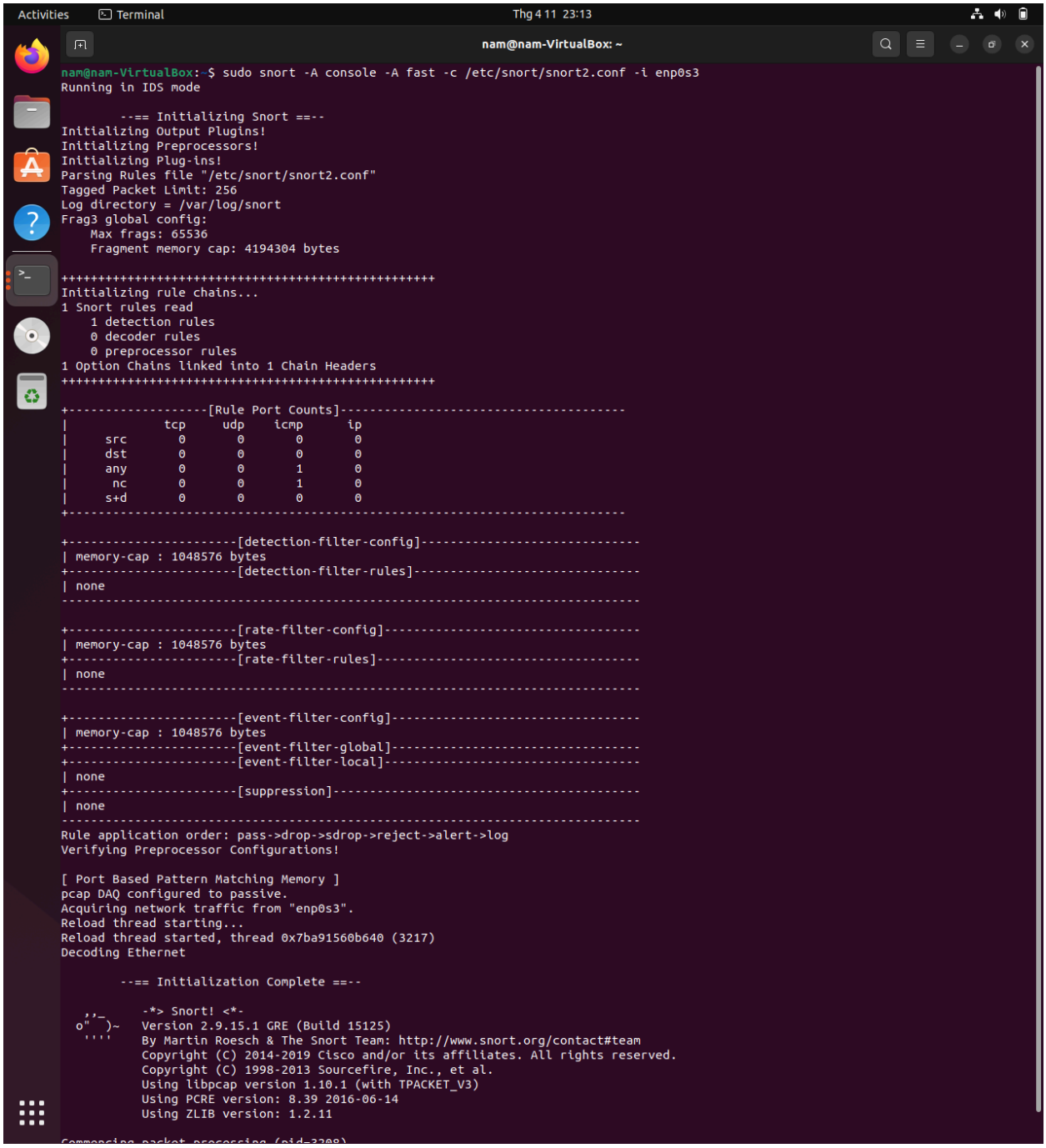

Activities
Wireshark
Thg 4 11 23:04
snort.log.1712851298
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
No. Time Source Destination Protocol Length Info
7 24.289336 10.0.2.4 10.0.2.15 ICMP 74 Echo (ping) request id=0x0001, seq=20/5120, ttl=128 (
8 24.289362 10.0.2.15 10.0.2.4 ICMP 74 Echo (ping) reply id=0x0001, seq=20/5120, ttl=64 (r
9 25.313624 10.0.2.4 10.0.2.15 ICMP 74 Echo (ping) request id=0x0001, seq=21/5376, ttl=128 (
10 25.313643 10.0.2.15 10.0.2.4 ICMP 74 Echo (ping) reply id=0x0001, seq=21/5376, ttl=64 (r
11 26.341578 10.0.2.4 10.0.2.15 ICMP 74 Echo (ping) request id=0x0001, seq=22/5632, ttl=128 (
12 26.341597 10.0.2.15 10.0.2.4 ICMP 74 Echo (ping) reply id=0x0001, seq=22/5632, ttl=64 (r
13 27.364707 10.0.2.4 10.0.2.15 ICMP 74 Echo (ping) request id=0x0001, seq=23/5888, ttl=128 (
14 27.364727 10.0.2.15 10.0.2.4 ICMP 74 Echo (ping) reply id=0x0001, seq=23/5888, ttl=64 (r
Frame 7: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
Ethernet II, Src: PcsCompu_e7:26:b4 (08:00:27:e7:26:b4), Dst: PcsCompu_cd:11:a3 (08:00:27:cd:11:a3)
Internet Protocol Version 4, Src: 10.0.2.4, Dst: 10.0.2.15
Internet Control Message Protocol
0000 08 00 27 cd 11 a3 08 00 27 e7 26 b4 08 00 45 00
0010 00 3c 70 00 00 00 80 01 b2 ae 0a 00 02 04 0a 00
0020 02 0f 08 00 4d 47 00 01 00 14 61 62 63 64 65 66
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76
0040 77 61 62 63 64 65 66 67 68 69
Internet Control Message Protocol: Protocol
Packets: 54 · Displayed: 8 (14.8%)
Profile: Default

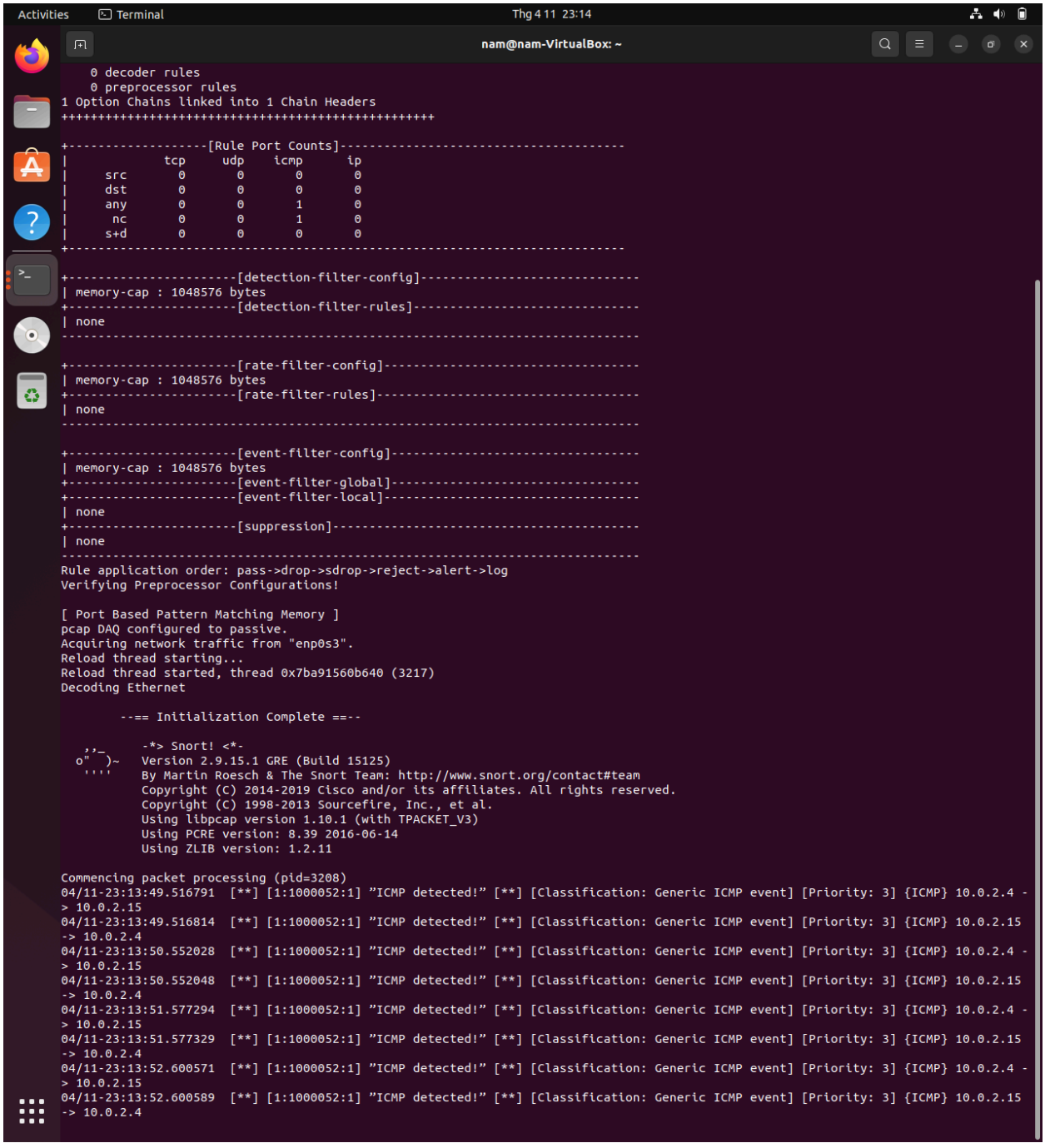
Lab 13.04

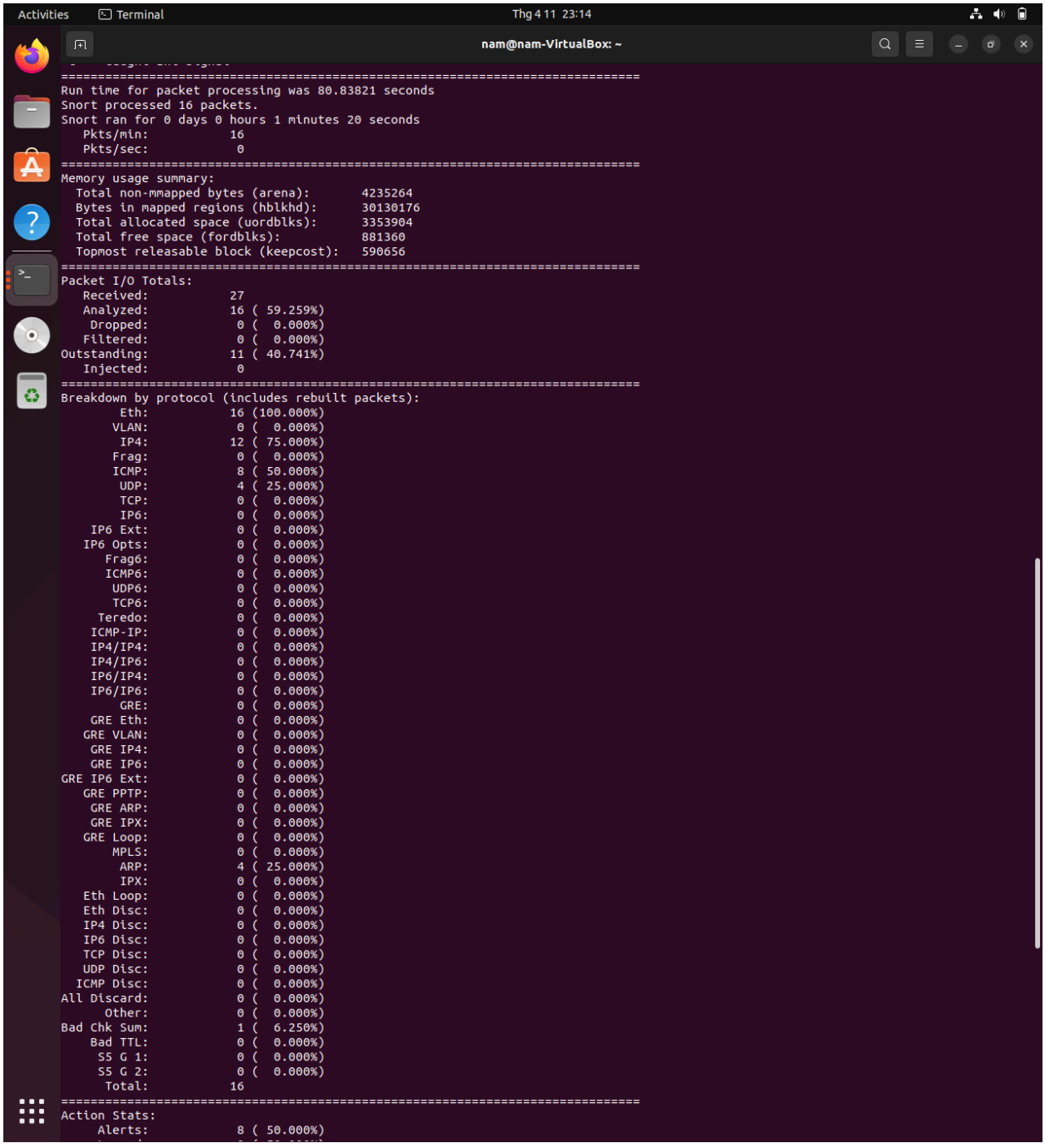

Activities
Terminal
Thg 4 11 23:06
nam@nam-VirtualBox: ~
nam@nam-VirtualBox:~$ sudo gedit /etc/snort/snort2.conf
(gedit:3032): dconf-WARNING **: 23:06:27.918: failed to commit changes to dconf: Failed to execute child process “dbus-launch” (No such file or directory)
(gedit:3032): dconf-WARNING **: 23:06:27.921: failed to commit changes to dconf: Failed to execute child process “dbus-launch” (No such file or directory)
(gedit:3032): dconf-WARNING **: 23:06:28.112: failed to commit changes to dconf: Failed to execute child process “dbus-launch” (No such file or directory)
(gedit:3032): dconf-WARNING **: 23:06:28.112: failed to commit changes to dconf: Failed to execute child process “dbus-launch” (No such file or directory)
(gedit:3032): dconf-WARNING **: 23:06:28.112: failed to commit changes to dconf: Failed to execute child process “dbus-launch” (No such file or directory)

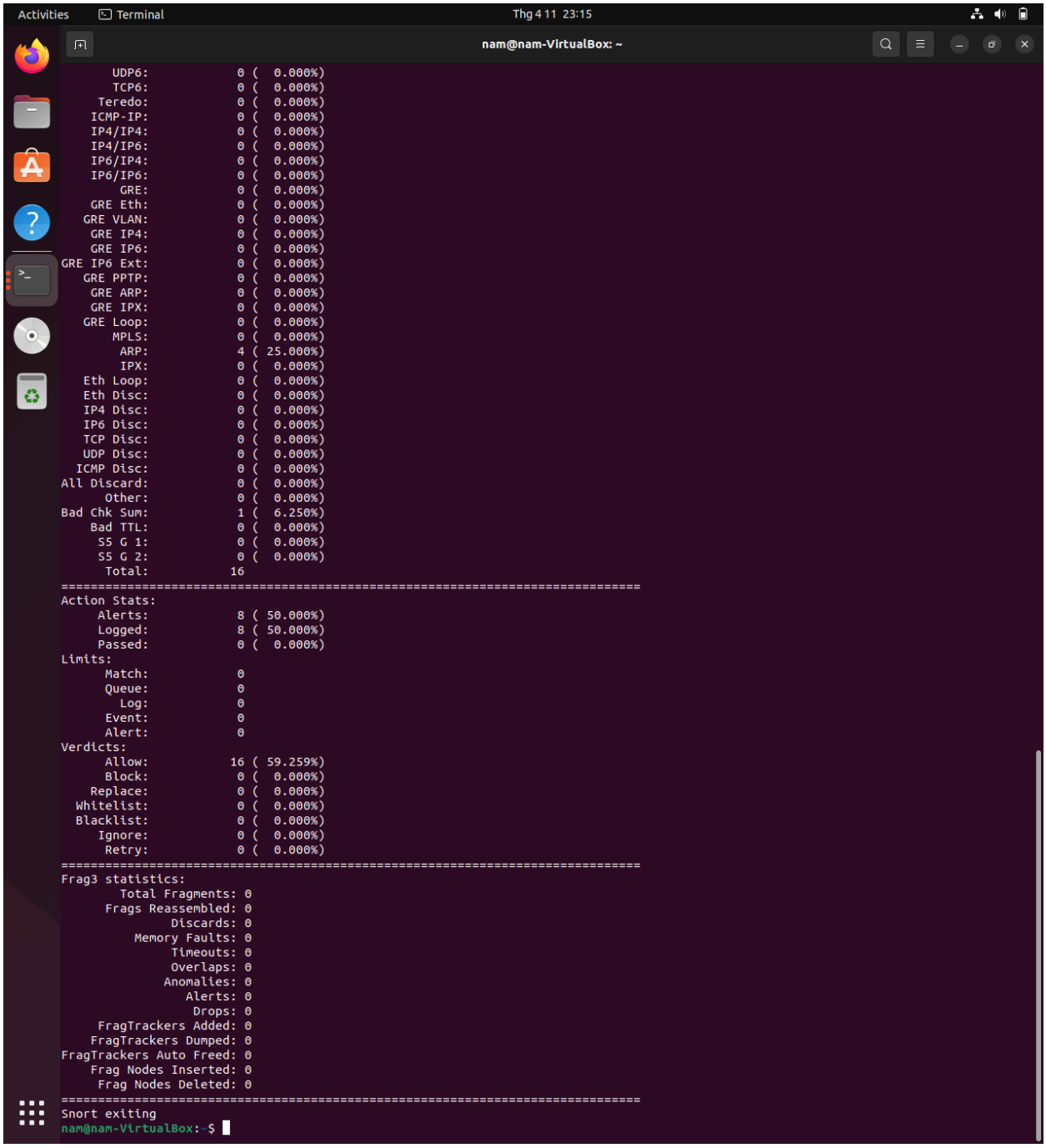

Activities
Gedit
Thg 4 11 23:07
nam@nam-VirtualBox: ~
Open
*snort2.conf
/etc/snort
Save
1 preprocessor frag3_global: max_frags 65536
2 include classification.config
3 ipvar HOME_NET 10.0.2.15/24
4 var RULE_PATH /etc/snort/rules
5 include $RULE_PATH/local.rules
Plain Text
Tab Width: 8
Ln 3, Col 25
INS

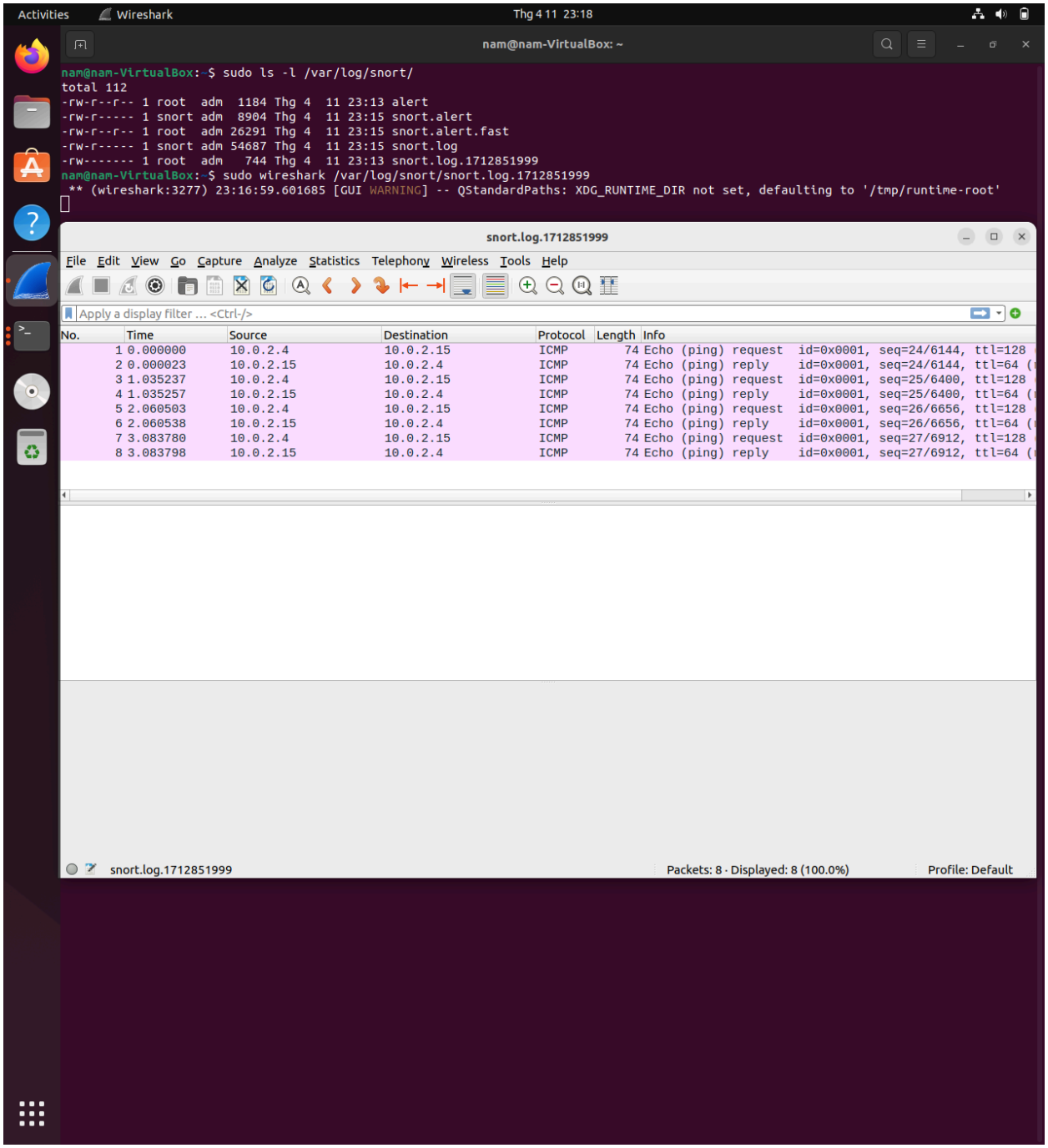

Activities
Gedit
Thg 4 11 23:11
nam@nam-VirtualBox: ~
nam@nam-VirtualBox:~$ sudo gedit /etc/snort/rules/local.rules
Open
local.rules
/etc/snort/rules
Save
1 # $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
2 # ----------------
3 # LOCAL RULES
4 # ----------------
5 # This file intentionally does not come with signatures. Put your local
6 # additions here.
7 alert icmp any any -> $HOME_NET any (msg:"ICMP detected!"; sid: 1000052; rev:1; classtype:icmp-event;)
Plain Text
Tab Width: 8
Ln 7, Col 60
INS

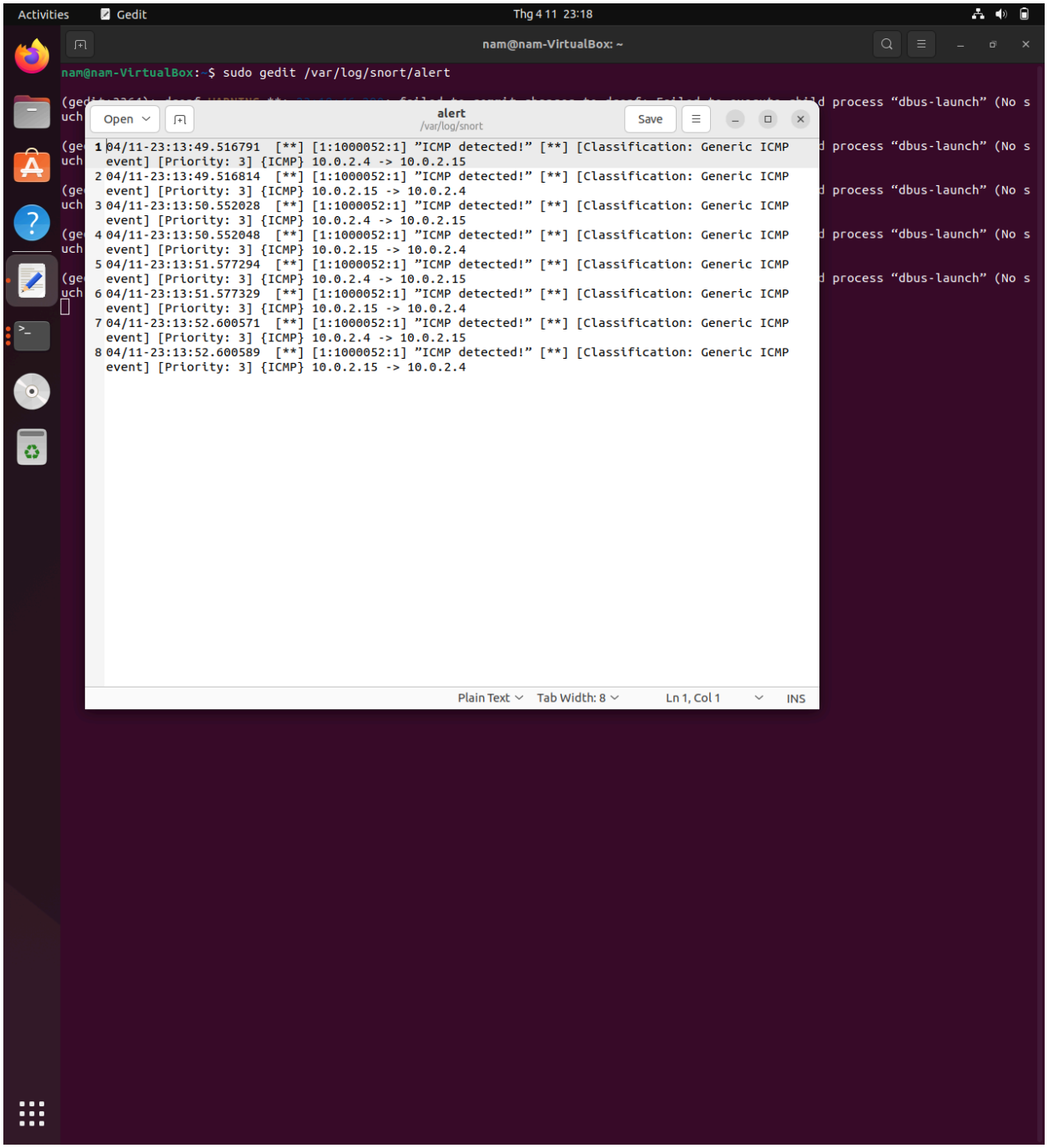

Activities
Terminal
Thg 4 11 23:13
nam@nam-VirtualBox: ~
nam@nam-VirtualBox:~$ sudo snort -A console -A fast -c /etc/snort/snort2.conf -i enp0s3
Running in IDS mode
--== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "/etc/snort/snort2.conf"
Tagged Packet Limit: 256
Log directory = /var/log/snort
Frag3 global config:
Max frags: 65536
Fragment memory cap: 4194304 bytes
Initializing rule chains...
1 Snort rules read
1 detection rules
0 decoder rules
0 preprocessor rules
1 Option Chains linked into 1 Chain Headers
[Rule Port Counts]
tcp udp icmp ip
src 0 0 0 0
dst 0 0 0 0
any 0 0 1 0
nc 0 0 1 0
s+d 0 0 0 0
[detection-filter-config]
memory-cap : 1048576 bytes
[detection-filter-rules]
none
[rate-filter-config]
memory-cap : 1048576 bytes
[rate-filter-rules]
none
[event-filter-config]
memory-cap : 1048576 bytes
[event-filter-global]
[event-filter-local]
none
[suppression]
none
Rule application order: pass->drop->sdrop->reject->alert->log
Verifying Preprocessor Configurations!
[Port Based Pattern Matching Memory]
pcap DAQ configured to passive.
Acquiring network traffic from "enp0s3".
Reload thread starting...
Reload thread started, thread 0x7ba91560b640 (3217)
Decoding Ethernet
--== Initialization Complete ==--
-*> Snort! <*-
Version 2.9.15.1 GRE (Build 15125)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.10.1 (with TPACKET_V3)
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.2.11

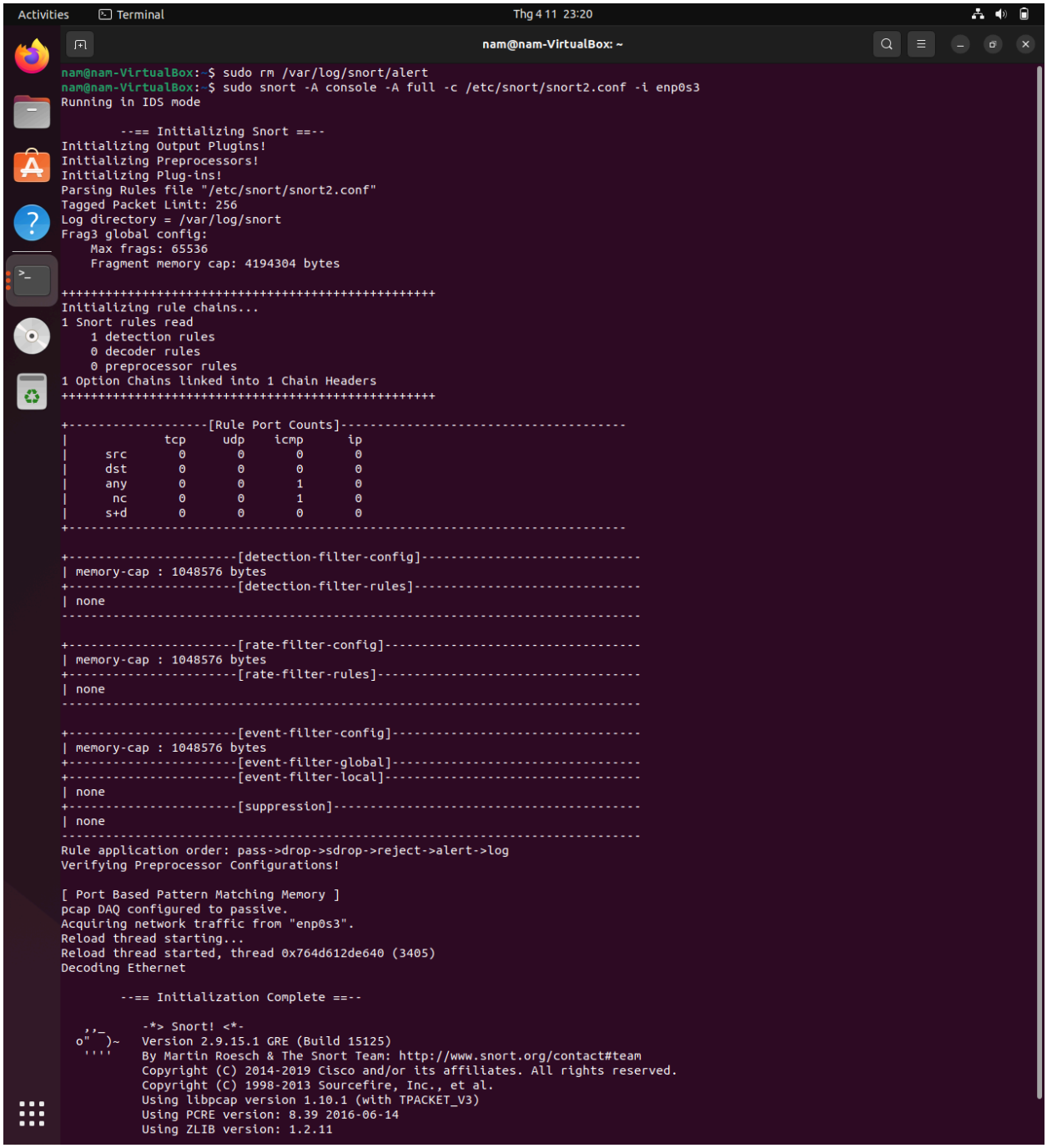

Activities
Terminal
Thg 4 11 23:14
nam@nam-VirtualBox: ~
0 decoder rules
0 preprocessor rules
1 Option Chains linked into 1 Chain Headers
[Rule Port Counts]
tcp udp icmp ip
src 0 0 0 0
dst 0 0 0 0
any 0 0 1 0
nc 0 0 1 0
s+d 0 0 0 0
[detection-filter-config]
memory-cap : 1048576 bytes
[detection-filter-rules]
none
[rate-filter-config]
memory-cap : 1048576 bytes
[rate-filter-rules]
none
[event-filter-config]
memory-cap : 1048576 bytes
[event-filter-global]
[event-filter-local]
none
[suppression]
none
Rule application order: pass->drop->sdrop->reject->alert->log
Verifying Preprocessor Configurations!
[Port Based Pattern Matching Memory]
pcap DAQ configured to passive.
Acquiring network traffic from "enp0s3".
Reload thread starting...
Reload thread started, thread 0x7ba91560b640 (3217)
Decoding Ethernet
--== Initialization Complete ==--
-*> Snort! <*-
Version 2.9.15.1 GRE (Build 15125)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.10.1 (with TPACKET_V3)
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.2.11
Commencing packet processing (pid=3208)
04/11-23:13:49.516791 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.2.4 -> 10.0.2.15
04/11-23:13:49.516814 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.2.15 -> 10.0.2.4
04/11-23:13:50.552028 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.2.4 -> 10.0.2.15
04/11-23:13:50.552048 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.2.15 -> 10.0.2.4
04/11-23:13:51.577294 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.2.4 -> 10.0.2.15
04/11-23:13:51.577329 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.2.15 -> 10.0.2.4
04/11-23:13:52.600571 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.2.4 -> 10.0.2.15
04/11-23:13:52.600589 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.2.15 -> 10.0.2.4


Activities
Terminal
Thg 4 11 23:14
nam@nam-VirtualBox: ~
Run time for packet processing was 80.83821 seconds
Snort processed 16 packets.
Snort ran for 0 days 0 hours 1 minutes 20 seconds
Pkts/min: 16
Pkts/sec: 0
Memory usage summary:
Total non-mmapped bytes (arena): 4235264
Bytes in mapped regions (hblkhd): 30130176
Total allocated space (uordblks): 3353904
Total free space (fordblks): 881360
Topmost releasable block (keepcost): 590656
Packet I/O Totals:
Received: 27
Analyzed: 16 (59.259%)
Dropped: 0 (0.000%)
Filtered: 0 (0.000%)
Outstanding: 11 (40.741%)
Injected: 0
Breakdown by protocol (includes rebuilt packets):
Eth: 16 (100.000%)
VLAN: 0 (0.000%)
IP4: 12 (75.000%)
Frag: 0 (0.000%)
ICMP: 8 (50.000%)
UDP: 4 (25.000%)
TCP: 0 (0.000%)
IP6: 0 (0.000%)
IP6 Ext: 0 (0.000%)
IP6 Opts: 0 (0.000%)
Frag6: 0 (0.000%)
ICMP6: 0 (0.000%)
UDP6: 0 (0.000%)
TCP6: 0 (0.000%)
Teredo: 0 (0.000%)
ICMP-IP: 0 (0.000%)
IP4/IP4: 0 (0.000%)
IP4/IP6: 0 (0.000%)
IP6/IP4: 0 (0.000%)
IP6/IP6: 0 (0.000%)
GRE: 0 (0.000%)
GRE Eth: 0 (0.000%)
GRE VLAN: 0 (0.000%)
GRE IP4: 0 (0.000%)
GRE IP6: 0 (0.000%)
GRE IP6 Ext: 0 (0.000%)
GRE PPTP: 0 (0.000%)
GRE ARP: 0 (0.000%)
GRE IPX: 0 (0.000%)
GRE Loop: 0 (0.000%)
MPLS: 0 (0.000%)
ARP: 4 (25.000%)
IPX: 0 (0.000%)
Eth Loop: 0 (0.000%)
Eth Disc: 0 (0.000%)
IP4 Disc: 0 (0.000%)
IP6 Disc: 0 (0.000%)
TCP Disc: 0 (0.000%)
UDP Disc: 0 (0.000%)
ICMP Disc: 0 (0.000%)
All Discard: 0 (0.000%)
Other: 0 (0.000%)
Bad Chk Sum: 1 (6.250%)
Bad TTL: 0 (0.000%)
S5 G 1: 0 (0.000%)
S5 G 2: 0 (0.000%)
Total: 16
Action Stats:
Alerts: 8 (50.000%)


Activities
Terminal
Thg 4 11 23:15
nam@nam-VirtualBox: ~
UDP6: 0 (0.000%)
TCP6: 0 (0.000%)
Teredo: 0 (0.000%)
ICMP-IP: 0 (0.000%)
IP4/IP4: 0 (0.000%)
IP4/IP6: 0 (0.000%)
IP6/IP4: 0 (0.000%)
IP6/IP6: 0 (0.000%)
GRE: 0 (0.000%)
GRE Eth: 0 (0.000%)
GRE VLAN: 0 (0.000%)
GRE IP4: 0 (0.000%)
GRE IP6: 0 (0.000%)
GRE IP6 Ext: 0 (0.000%)
GRE PPTP: 0 (0.000%)
GRE ARP: 0 (0.000%)
GRE IPX: 0 (0.000%)
GRE Loop: 0 (0.000%)
MPLS: 0 (0.000%)
ARP: 4 (25.000%)
IPX: 0 (0.000%)
Eth Loop: 0 (0.000%)
Eth Disc: 0 (0.000%)
IP4 Disc: 0 (0.000%)
IP6 Disc: 0 (0.000%)
TCP Disc: 0 (0.000%)
UDP Disc: 0 (0.000%)
ICMP Disc: 0 (0.000%)
All Discard: 0 (0.000%)
Other: 0 (0.000%)
Bad Chk Sum: 1 (6.250%)
Bad TTL: 0 (0.000%)
S5 G 1: 0 (0.000%)
S5 G 2: 0 (0.000%)
Total: 16
Action Stats:
Alerts: 8 (50.000%)
Logged: 8 (50.000%)
Passed: 0 (0.000%)
Limits:
Match: 0
Queue: 0
Log: 0
Event: 0
Alert: 0
Verdicts:
Allow: 16 (59.259%)
Block: 0 (0.000%)
Replace: 0 (0.000%)
Whitelist: 0 (0.000%)
Blacklist: 0 (0.000%)
Ignore: 0 (0.000%)
Retry: 0 (0.000%)
Frag3 statistics:
Total Fragments: 0
Frags Reassembled: 0
Discards: 0
Memory Faults: 0
Timeouts: 0
Overlaps: 0
Anomalies: 0
Alerts: 0
Drops: 0
FragTrackers Added: 0
FragTrackers Dumped: 0
FragTrackers Auto Freed: 0
Frag Nodes Inserted: 0
Frag Nodes Deleted: 0
Snort exiting
nam@nam-VirtualBox:~$


Activities
Wireshark
Thg 4 11 23:18
nam@nam-VirtualBox: ~
nam@nam-VirtualBox:~$ sudo ls -l /var/log/snort/
total 112
-rw-r--r-- 1 root adm 1184 Thg 4 11 23:13 alert
-rw-r----- 1 snort adm 8904 Thg 4 11 23:15 snort.alert
-rw-r--r-- 1 root adm 26291 Thg 4 11 23:15 snort.alert.fast
-rw-r----- 1 snort adm 54687 Thg 4 11 23:15 snort.log
-rw------- 1 root adm 744 Thg 4 11 23:13 snort.log.1712851999
nam@nam-VirtualBox:~$ sudo wireshark /var/log/snort/snort.log.1712851999
** (wireshark:3277) 23:16:59.601685 [GUI WARNING] -- QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
snort.log.1712851999
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000 10.0.2.4 10.0.2.15 ICMP 74 Echo (ping) request id=0x0001, seq=24/6144, ttl=128
2 0.000023 10.0.2.15 10.0.2.4 ICMP 74 Echo (ping) reply id=0x0001, seq=24/6144, ttl=64
3 1.035237 10.0.2.4 10.0.2.15 ICMP 74 Echo (ping) request id=0x0001, seq=25/6400, ttl=128
4 1.035257 10.0.2.15 10.0.2.4 ICMP 74 Echo (ping) reply id=0x0001, seq=25/6400, ttl=64
5 2.060503 10.0.2.4 10.0.2.15 ICMP 74 Echo (ping) request id=0x0001, seq=26/6656, ttl=128
6 2.060538 10.0.2.15 10.0.2.4 ICMP 74 Echo (ping) reply id=0x0001, seq=26/6656, ttl=64
7 3.083780 10.0.2.4 10.0.2.15 ICMP 74 Echo (ping) request id=0x0001, seq=27/6912, ttl=128
8 3.083798 10.0.2.15 10.0.2.4 ICMP 74 Echo (ping) reply id=0x0001, seq=27/6912, ttl=64
snort.log.1712851999
Packets: 8 · Displayed: 8 (100.0%)
Profile: Default

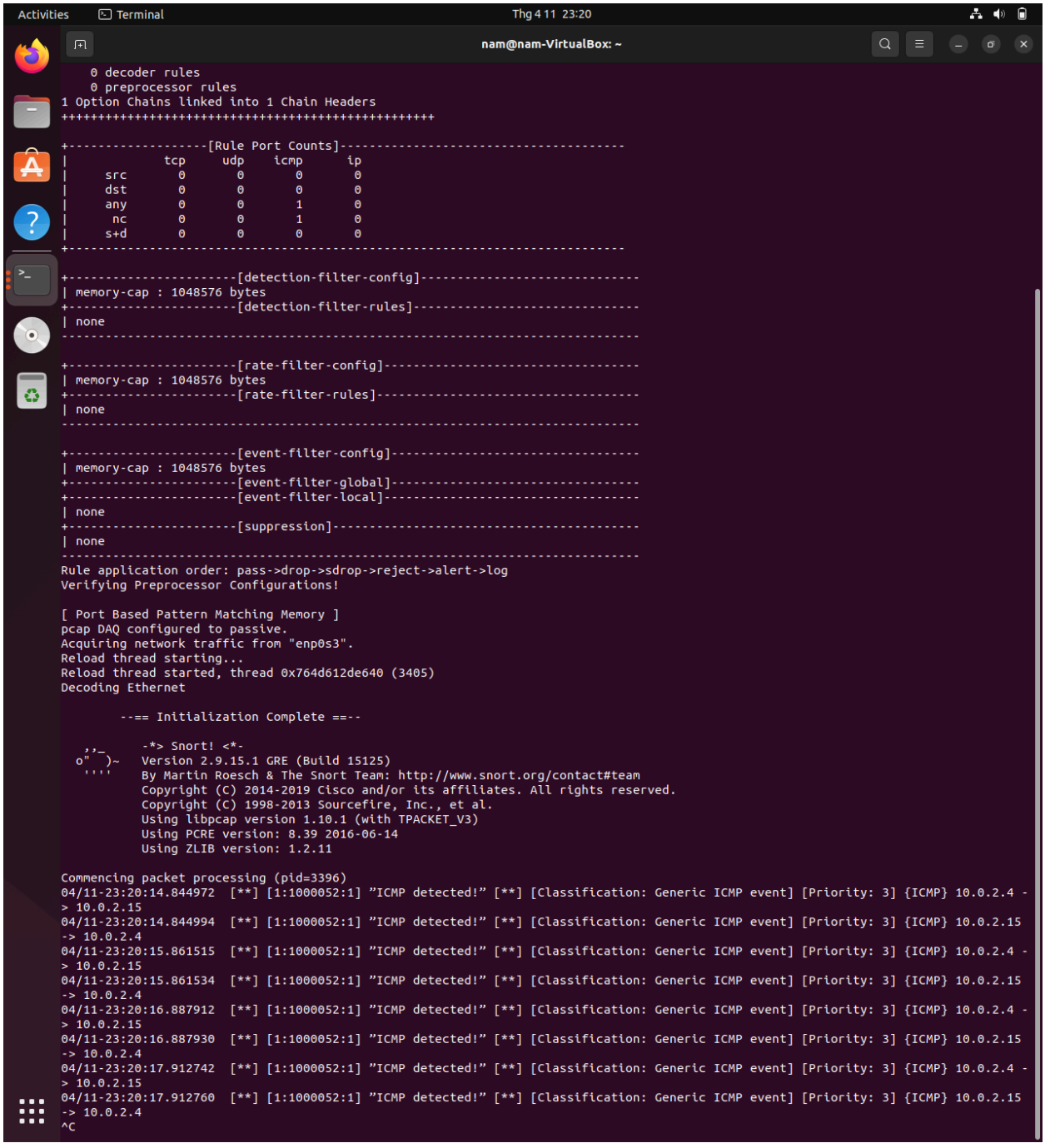

Activities
Gedit
Thg 4 11 23:18
nam@nam-VirtualBox: ~
nam@nam-VirtualBox:~$ sudo gedit /var/log/snort/alert
Open
alert
/var/log/snort
Save
1 04/11-23:13:49.516791 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.2.4 -> 10.0.2.15
2 04/11-23:13:49.516814 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.2.15 -> 10.0.2.4
3 04/11-23:13:50.552028 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.2.4 -> 10.0.2.15
4 04/11-23:13:50.552048 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.2.15 -> 10.0.2.4
5 04/11-23:13:51.577294 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.2.4 -> 10.0.2.15
6 04/11-23:13:51.577329 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.2.15 -> 10.0.2.4
7 04/11-23:13:52.600571 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.2.4 -> 10.0.2.15
8 04/11-23:13:52.600589 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.2.15 -> 10.0.2.4
Plain Text
Tab Width: 8
Ln 1, Col 1
INS

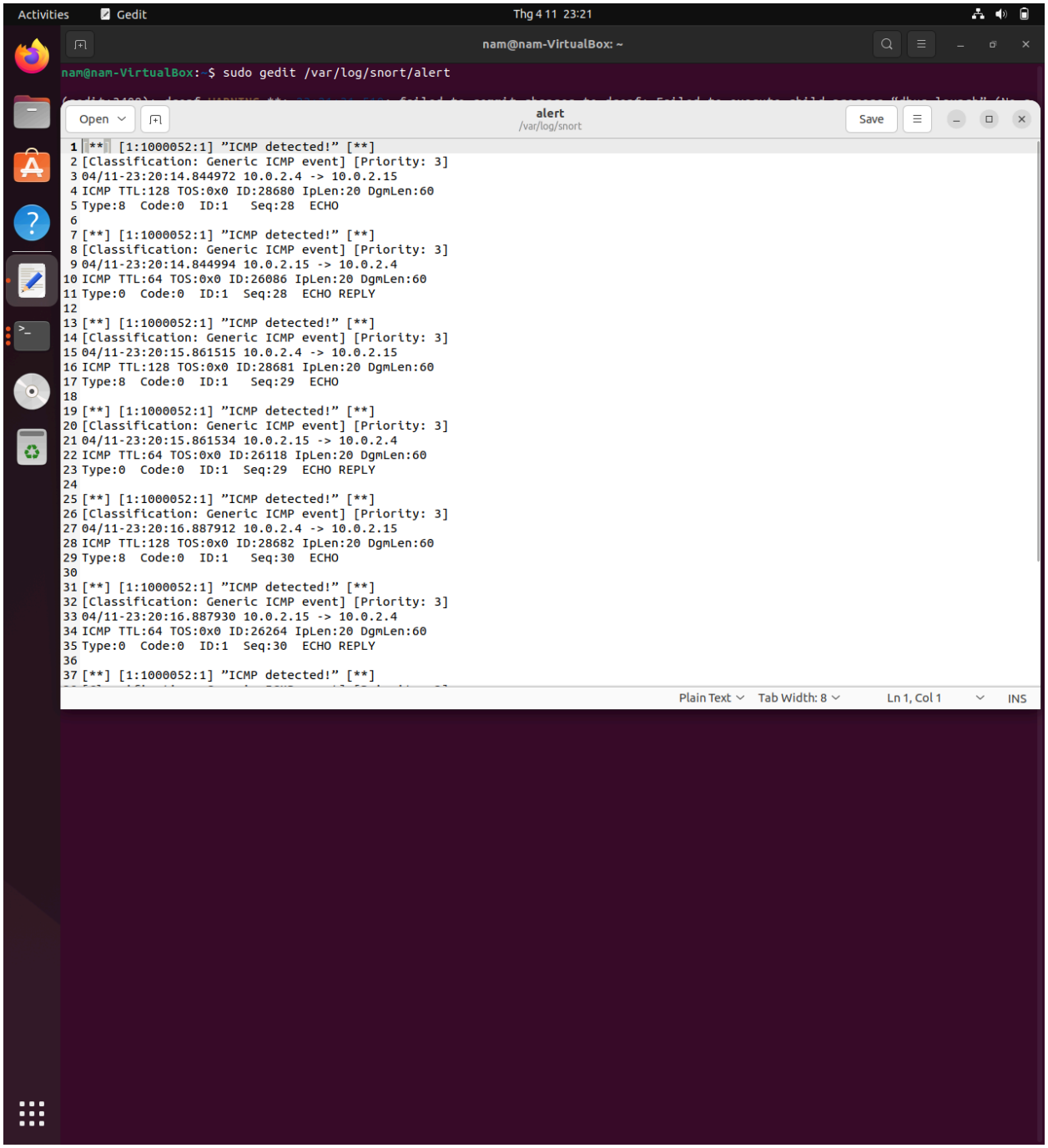

Activities
Terminal
Thg 4 11 23:20
nam@nam-VirtualBox: ~
nam@nam-VirtualBox:~$ sudo rm /var/log/snort/alert
nam@nam-VirtualBox:~$ sudo snort -A console -A full -c /etc/snort/snort2.conf -i enp0s3
Running in IDS mode
--== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "/etc/snort/snort2.conf"
Tagged Packet Limit: 256
Log directory = /var/log/snort
Frag3 global config:
Max frags: 65536
Fragment memory cap: 4194304 bytes
++
Initializing rule chains...
1 Snort rules read
1 detection rules
0 decoder rules
0 preprocessor rules
1 Option Chains linked into 1 Chain Headers
++
+------------------[Rule Port Counts]-------------------------------------
| tcp udp icmp ip
| src 0 0 0 0
| dst 0 0 0 0
| any 0 0 1 0
| nc 0 0 1 0
| s+d 0 0 0 0
+--
+----------------------[detection-filter-config]---------------------------
| memory-cap : 1048576 bytes
+----------------------[detection-filter-rules]----------------------------
| none

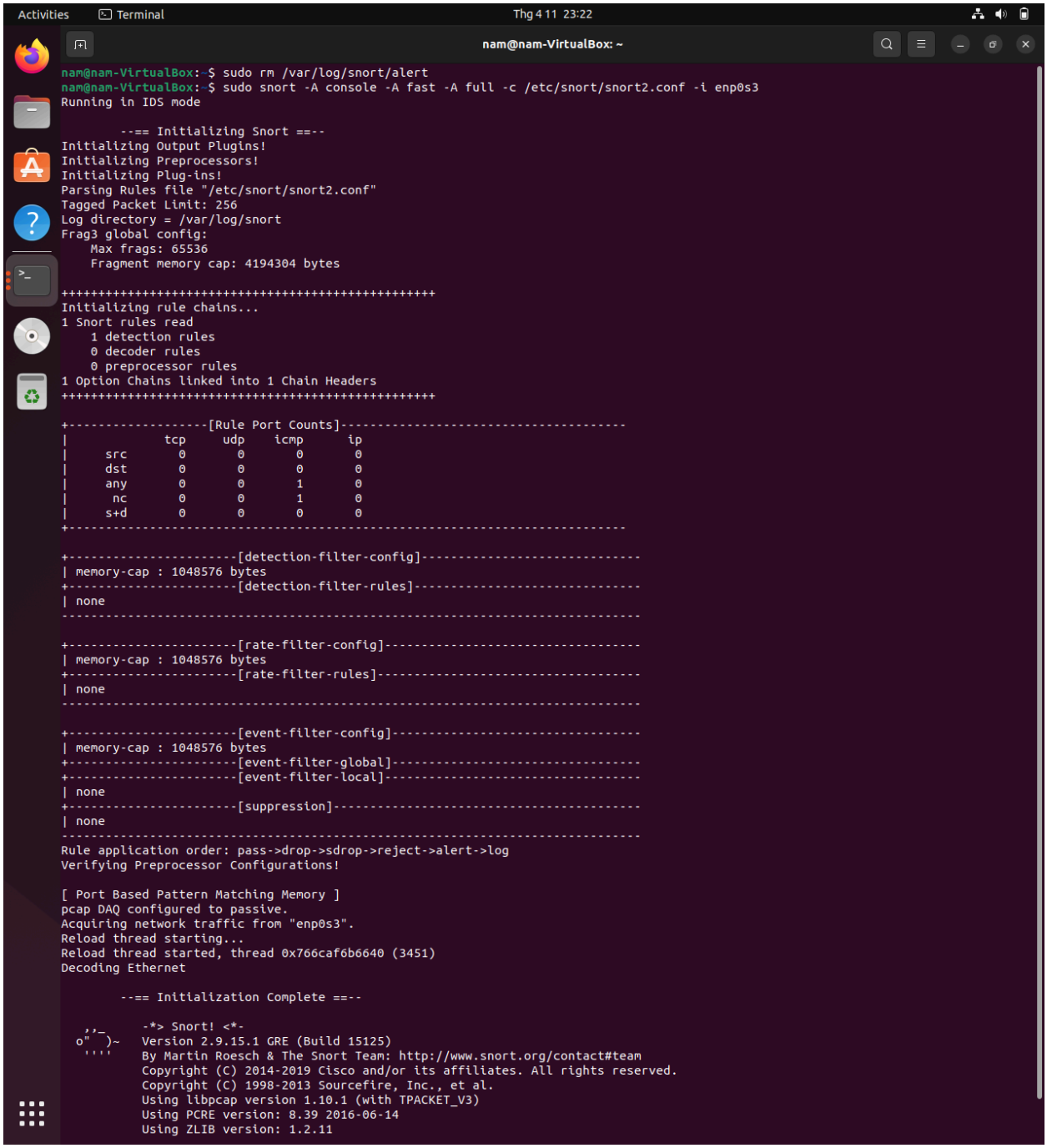
+----------------------[rate-filter-config]--------------------------------
| memory-cap : 1048576 bytes
+----------------------[rate-filter-rules]---------------------------------
| none

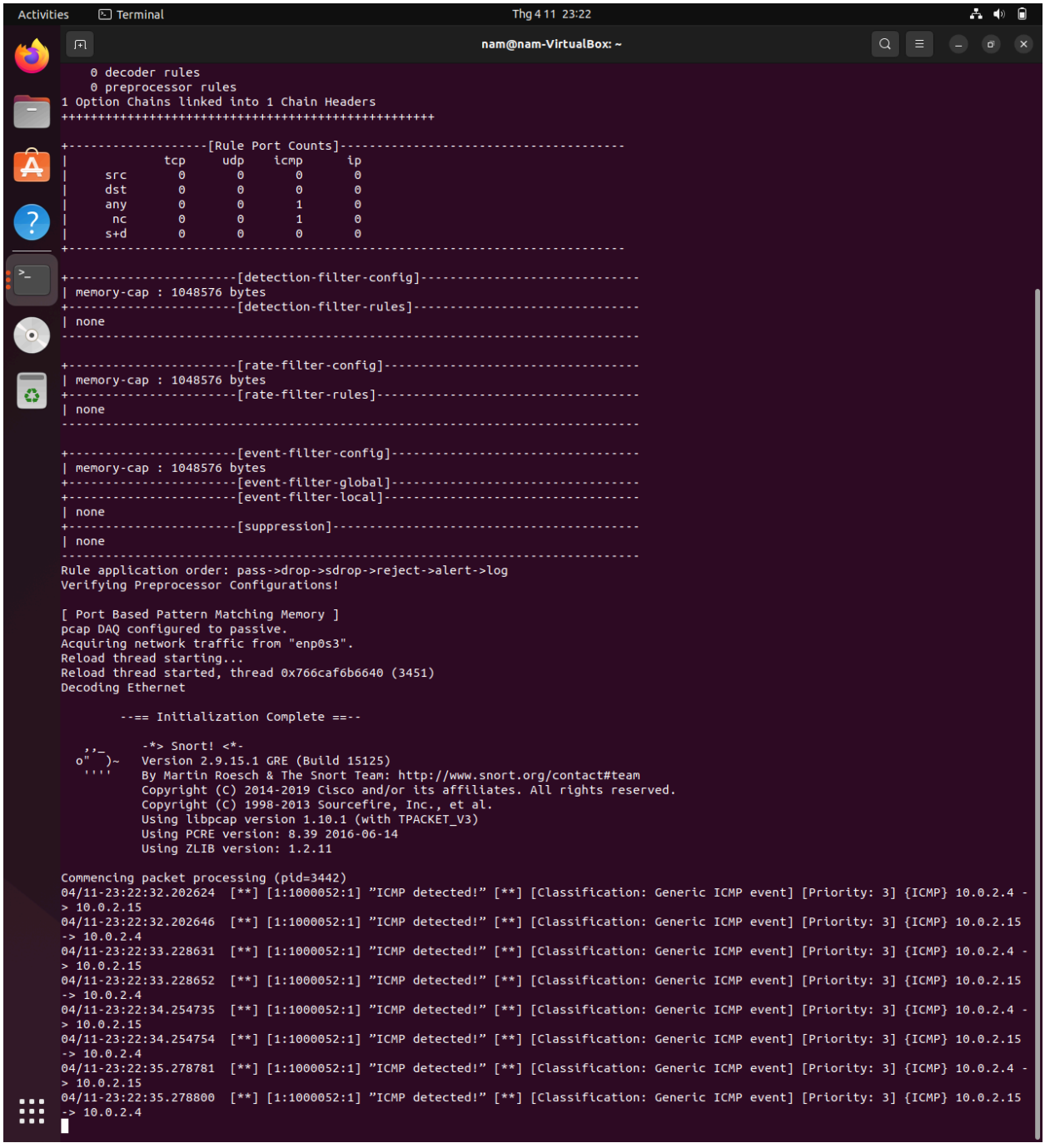
+----------------------[event-filter-config]-------------------------------
| memory-cap : 1048576 bytes
+----------------------[event-filter-global]-------------------------------
+----------------------[event-filter-local]--------------------------------
| none
+----------------------[suppression]---------------------------------------
| none

Rule application order: pass->drop->sdrop->reject->alert->log
Verifying Preprocessor Configurations!
[Port Based Pattern Matching Memory]
pcap DAQ configured to passive.
Acquiring network traffic from "enp0s3".
Reload thread starting...
Reload thread started, thread 0x764d612de640 (3405)
Decoding Ethernet
--== Initialization Complete ==--
-*> Snort! <*-
Version 2.9.15.1 GRE (Build 15125)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.10.1 (with TPACKET_V3)
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.2.11


Activities
Terminal
Thg 4 11 23:20
nam@nam-VirtualBox: ~
0 decoder rules
0 preprocessor rules
1 Option Chains linked into 1 Chain Headers
+------------------[Rule Port Counts]-------------------------------------
| tcp udp icmp ip
| src 0 0 0 0
| dst 0 0 0 0
| any 0 0 1 0
| nc 0 0 1 0
| s+d 0 0 0 0
+----------------------[detection-filter-config]---------------------------
| memory-cap : 1048576 bytes
+----------------------[detection-filter-rules]----------------------------
| none
+----------------------[rate-filter-config]--------------------------------
| memory-cap : 1048576 bytes
+----------------------[rate-filter-rules]---------------------------------
| none
+----------------------[event-filter-config]-------------------------------
| memory-cap : 1048576 bytes
+----------------------[event-filter-global]-------------------------------
+----------------------[event-filter-local]--------------------------------
| none
+----------------------[suppression]---------------------------------------
| none
Rule application order: pass->drop->sdrop->reject->alert->log
Verifying Preprocessor Configurations!
[Port Based Pattern Matching Memory]
pcap DAQ configured to passive.
Acquiring network traffic from "enp0s3".
Reload thread starting...
Reload thread started, thread 0x764d612de640 (3405)
Decoding Ethernet
--== Initialization Complete ==--
-*> Snort! <*-
Version 2.9.15.1 GRE (Build 15125)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.10.1 (with TPACKET_V3)
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.2.11
Commencing packet processing (pid=3396)
04/11-23:20:14.844972 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.2.4 -> 10.0.2.15
04/11-23:20:14.844994 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.2.15 -> 10.0.2.4
04/11-23:20:15.861515 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.2.4 -> 10.0.2.15
04/11-23:20:15.861534 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.2.15 -> 10.0.2.4
04/11-23:20:16.887912 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.2.4 -> 10.0.2.15
04/11-23:20:16.887930 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.2.15 -> 10.0.2.4
04/11-23:20:17.912742 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.2.4 -> 10.0.2.15
04/11-23:20:17.912760 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.2.15 -> 10.0.2.4
^C


Activities
Gedit
Thg 4 11 23:21
nam@nam-VirtualBox: ~
nam@nam-VirtualBox:~$ sudo gedit /var/log/snort/alert
Open
alert
/var/log/snort
Save
1 [**] [1:1000052:1] "ICMP detected!" [**]
2 [Classification: Generic ICMP event] [Priority: 3]
3 04/11-23:20:14.844972 10.0.2.4 -> 10.0.2.15
4 ICMP TTL:128 TOS:0x0 ID:28680 IpLen:20 DgmLen:60
5 Type:8 Code:0 ID:1 Seq:28 ECHO
6
7 [**] [1:1000052:1] "ICMP detected!" [**]
8 [Classification: Generic ICMP event] [Priority: 3]
9 04/11-23:20:14.844994 10.0.2.15 -> 10.0.2.4
10 ICMP TTL:64 TOS:0x0 ID:26086 IpLen:20 DgmLen:60
11 Type:0 Code:0 ID:1 Seq:28 ECHO REPLY
12
13 [**] [1:1000052:1] "ICMP detected!" [**]
14 [Classification: Generic ICMP event] [Priority: 3]
15 04/11-23:20:15.861515 10.0.2.4 -> 10.0.2.15
16 ICMP TTL:128 TOS:0x0 ID:28681 IpLen:20 DgmLen:60
17 Type:8 Code:0 ID:1 Seq:29 ECHO
18
19 [**] [1:1000052:1] "ICMP detected!" [**]
20 [Classification: Generic ICMP event] [Priority: 3]
21 04/11-23:20:15.861534 10.0.2.15 -> 10.0.2.4
22 ICMP TTL:64 TOS:0x0 ID:26118 IpLen:20 DgmLen:60
23 Type:0 Code:0 ID:1 Seq:29 ECHO REPLY
24
25 [**] [1:1000052:1] "ICMP detected!" [**]
26 [Classification: Generic ICMP event] [Priority: 3]
27 04/11-23:20:16.887912 10.0.2.4 -> 10.0.2.15
28 ICMP TTL:128 TOS:0x0 ID:28682 IpLen:20 DgmLen:60
29 Type:8 Code:0 ID:1 Seq:30 ECHO
30
31 [**] [1:1000052:1] "ICMP detected!" [**]
32 [Classification: Generic ICMP event] [Priority: 3]
33 04/11-23:20:16.887930 10.0.2.15 -> 10.0.2.4
34 ICMP TTL:64 TOS:0x0 ID:26264 IpLen:20 DgmLen:60
35 Type:0 Code:0 ID:1 Seq:30 ECHO REPLY
36
37 [**] [1:1000052:1] "ICMP detected!" [**]
Plain Text
Tab Width: 8
Ln 1, Col 1
INS

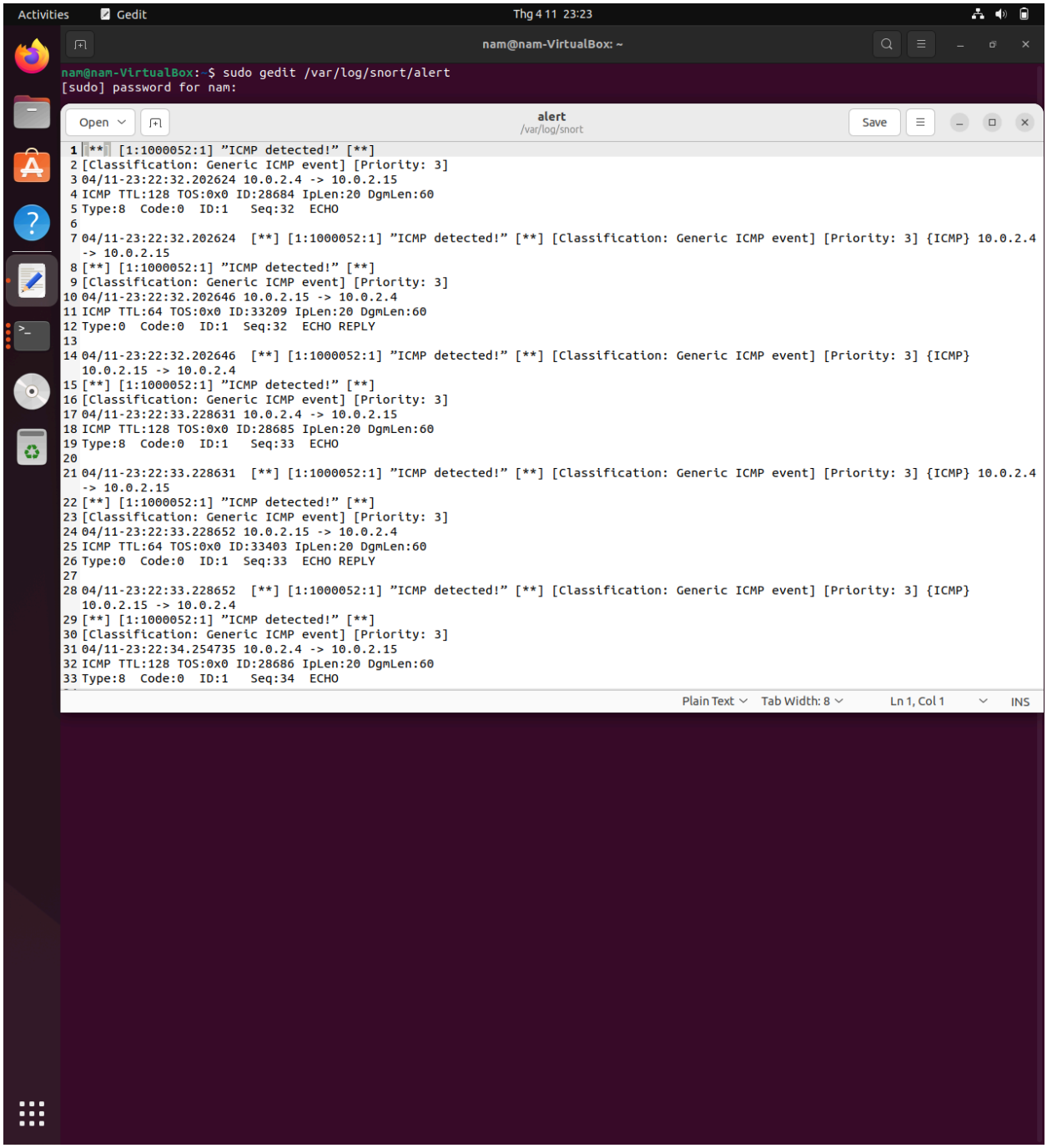

Activities
Terminal
Thg 4 11 23:22
nam@nam-VirtualBox: ~
nam@nam-VirtualBox:~$ sudo rm /var/log/snort/alert
nam@nam-VirtualBox:~$ sudo snort -A console -A fast -A full -c /etc/snort/snort2.conf -i enp0s3
Running in IDS mode
--== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "/etc/snort/snort2.conf"
Tagged Packet Limit: 256
Log directory = /var/log/snort
Frag3 global config:
Max frags: 65536
Fragment memory cap: 4194304 bytes
Initializing rule chains...
1 Snort rules read
1 detection rules
0 decoder rules
0 preprocessor rules
1 Option Chains linked into 1 Chain Headers
[Rule Port Counts]
tcp udp icmp ip
src 0 0 0 0
dst 0 0 0 0
any 0 0 1 0
nc 0 0 1 0
s+d 0 0 0 0
[detection-filter-config]
memory-cap : 1048576 bytes
[detection-filter-rules]
none
[rate-filter-config]
memory-cap : 1048576 bytes
[rate-filter-rules]
none
[event-filter-config]
memory-cap : 1048576 bytes
[event-filter-global]
[event-filter-local]
none
[suppression]
none
Rule application order: pass->drop->sdrop->reject->alert->log
Verifying Preprocessor Configurations!
[Port Based Pattern Matching Memory]
pcap DAQ configured to passive.
Acquiring network traffic from "enp0s3".
Reload thread starting...
Reload thread started, thread 0x766caf6b6640 (3451)
Decoding Ethernet
--== Initialization Complete ==--
-*> Snort! <*-
Version 2.9.15.1 GRE (Build 15125)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.10.1 (with TPACKET_V3)
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.2.11

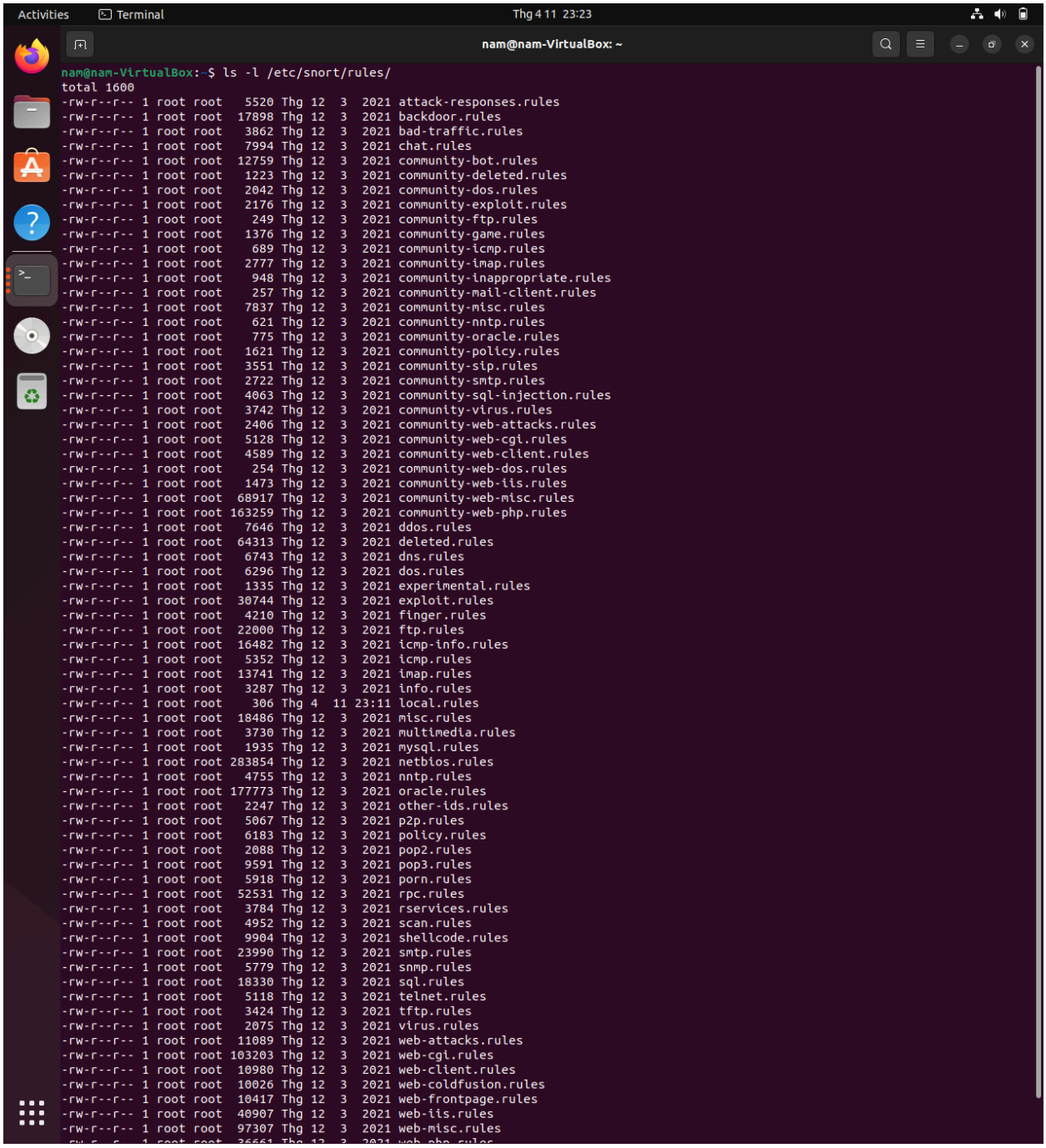

Activities
Terminal
Thg 4 11 23:22
nam@nam-VirtualBox: ~
0 decoder rules
0 preprocessor rules
1 Option Chains linked into 1 Chain Headers
+++
+------------------[Rule Port Counts]-------------------------------------
| tcp udp icmp ip
| src 0 0 0 0
| dst 0 0 0 0
| any 0 0 1 0
| nc 0 0 1 0
| s+d 0 0 0 0
+---
+----------------------[detection-filter-config]---------------------------
| memory-cap : 1048576 bytes
+----------------------[detection-filter-rules]----------------------------
| none

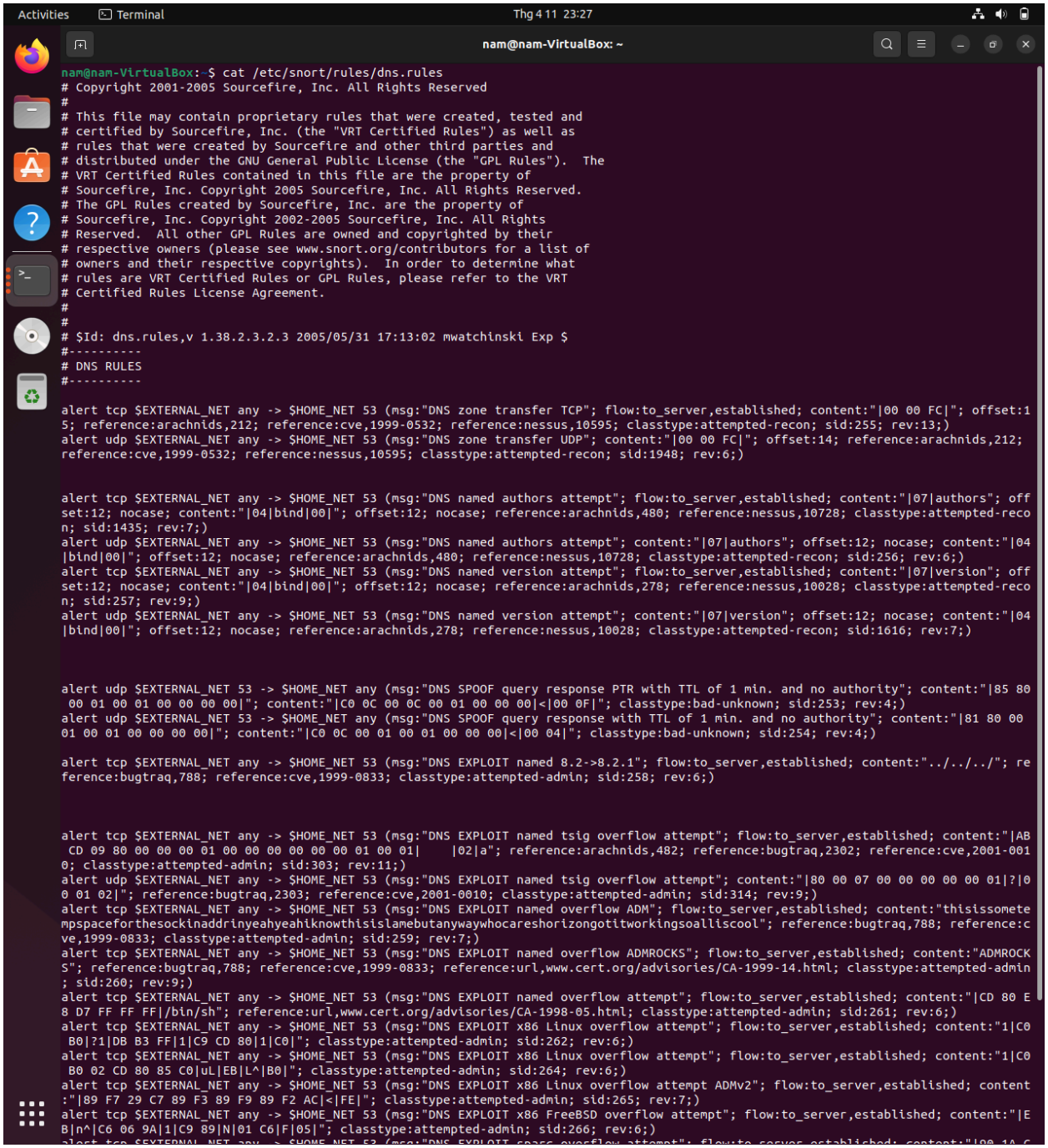
+----------------------[rate-filter-config]--------------------------------
| memory-cap : 1048576 bytes
+----------------------[rate-filter-rules]---------------------------------
| none

+----------------------[event-filter-config]-------------------------------
| memory-cap : 1048576 bytes
+----------------------[event-filter-global]-------------------------------
+----------------------[event-filter-local]--------------------------------
| none
+----------------------[suppression]---------------------------------------
| none

Rule application order: pass->drop->sdrop->reject->alert->log
Verifying Preprocessor Configurations!
[Port Based Pattern Matching Memory]
pcap DAQ configured to passive.
Acquiring network traffic from "enp0s3".
Reload thread starting...
Reload thread started, thread 0x766caf6b6640 (3451)
Decoding Ethernet
--== Initialization Complete ==--
-*> Snort! <*-
Version 2.9.15.1 GRE (Build 15125)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.10.1 (with TPACKET_V3)
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.2.11
Commencing packet processing (pid=3442)
04/11-23:22:32.202624 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.2.4 -> 10.0.2.15
04/11-23:22:32.202646 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.2.15 -> 10.0.2.4
04/11-23:22:33.228631 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.2.4 -> 10.0.2.15
04/11-23:22:33.228652 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.2.15 -> 10.0.2.4
04/11-23:22:34.254735 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.2.4 -> 10.0.2.15
04/11-23:22:34.254754 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.2.15 -> 10.0.2.4
04/11-23:22:35.278781 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.2.4 -> 10.0.2.15
04/11-23:22:35.278800 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.2.15 -> 10.0.2.4


Activities
Gedit
Thg 4 11 23:23
nam@nam-VirtualBox: ~
nam@nam-VirtualBox:~$ sudo gedit /var/log/snort/alert
[sudo] password for nam:
Open
alert
/var/log/snort
Save
1 [**] [1:1000052:1] "ICMP detected!" [**]
2 [Classification: Generic ICMP event] [Priority: 3]
3 04/11-23:22:32.202624 10.0.2.4 -> 10.0.2.15
4 ICMP TTL:128 TOS:0x0 ID:28684 IpLen:20 DgmLen:60
5 Type:8 Code:0 ID:1 Seq:32 ECHO
6
7 04/11-23:22:32.202624 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.2.4
-> 10.0.2.15
8 [**] [1:1000052:1] "ICMP detected!" [**]
9 [Classification: Generic ICMP event] [Priority: 3]
10 04/11-23:22:32.202646 10.0.2.15 -> 10.0.2.4
11 ICMP TTL:64 TOS:0x0 ID:33209 IpLen:20 DgmLen:60
12 Type:0 Code:0 ID:1 Seq:32 ECHO REPLY
13
14 04/11-23:22:32.202646 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP}
10.0.2.15 -> 10.0.2.4
15 [**] [1:1000052:1] "ICMP detected!" [**]
16 [Classification: Generic ICMP event] [Priority: 3]
17 04/11-23:22:33.228631 10.0.2.4 -> 10.0.2.15
18 ICMP TTL:128 TOS:0x0 ID:28685 IpLen:20 DgmLen:60
19 Type:8 Code:0 ID:1 Seq:33 ECHO
20
21 04/11-23:22:33.228631 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.2.4
-> 10.0.2.15
22 [**] [1:1000052:1] "ICMP detected!" [**]
23 [Classification: Generic ICMP event] [Priority: 3]
24 04/11-23:22:33.228652 10.0.2.15 -> 10.0.2.4
25 ICMP TTL:64 TOS:0x0 ID:33403 IpLen:20 DgmLen:60
26 Type:0 Code:0 ID:1 Seq:33 ECHO REPLY
27
28 04/11-23:22:33.228652 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP}
10.0.2.15 -> 10.0.2.4
29 [**] [1:1000052:1] "ICMP detected!" [**]
30 [Classification: Generic ICMP event] [Priority: 3]
31 04/11-23:22:34.254735 10.0.2.4 -> 10.0.2.15
32 ICMP TTL:128 TOS:0x0 ID:28686 IpLen:20 DgmLen:60
33 Type:8 Code:0 ID:1 Seq:34 ECHO
Plain Text
Tab Width: 8
Ln 1, Col 1
INS


Activities
Terminal
Thg 4 11 23:23
nam@nam-VirtualBox: ~
nam@nam-VirtualBox:~$ ls -l /etc/snort/rules/
total 1600
-rw-r--r-- 1 root root   5520 Thg 12 3 2021 attack-responses.rules
-rw-r--r-- 1 root root 17898 Thg 12 3 2021 backdoor.rules
-rw-r--r-- 1 root root   3862 Thg 12 3 2021 bad-traffic.rules
-rw-r--r-- 1 root root   7994 Thg 12 3 2021 chat.rules
-rw-r--r-- 1 root root 12759 Thg 12 3 2021 community-bot.rules
-rw-r--r-- 1 root root   1223 Thg 12 3 2021 community-deleted.rules
-rw-r--r-- 1 root root   2042 Thg 12 3 2021 community-dos.rules
-rw-r--r-- 1 root root   2176 Thg 12 3 2021 community-exploit.rules
-rw-r--r-- 1 root root   249 Thg 12 3 2021 community-ftp.rules
-rw-r--r-- 1 root root   1376 Thg 12 3 2021 community-game.rules
-rw-r--r-- 1 root root   689 Thg 12 3 2021 community-icmp.rules
-rw-r--r-- 1 root root   2777 Thg 12 3 2021 community-imap.rules
-rw-r--r-- 1 root root   948 Thg 12 3 2021 community-inappropriate.rules
-rw-r--r-- 1 root root   257 Thg 12 3 2021 community-mail-client.rules
-rw-r--r-- 1 root root   7837 Thg 12 3 2021 community-misc.rules
-rw-r--r-- 1 root root   621 Thg 12 3 2021 community-nntp.rules
-rw-r--r-- 1 root root   775 Thg 12 3 2021 community-oracle.rules
-rw-r--r-- 1 root root   1621 Thg 12 3 2021 community-policy.rules
-rw-r--r-- 1 root root   3551 Thg 12 3 2021 community-sip.rules
-rw-r--r-- 1 root root   2722 Thg 12 3 2021 community-smtp.rules
-rw-r--r-- 1 root root   4063 Thg 12 3 2021 community-sql-injection.rules
-rw-r--r-- 1 root root   3742 Thg 12 3 2021 community-virus.rules
-rw-r--r-- 1 root root   2406 Thg 12 3 2021 community-web-attacks.rules
-rw-r--r-- 1 root root   5128 Thg 12 3 2021 community-web-cgi.rules
-rw-r--r-- 1 root root   4589 Thg 12 3 2021 community-web-client.rules
-rw-r--r-- 1 root root   254 Thg 12 3 2021 community-web-dos.rules
-rw-r--r-- 1 root root   1473 Thg 12 3 2021 community-web-iis.rules
-rw-r--r-- 1 root root 68917 Thg 12 3 2021 community-web-misc.rules
-rw-r--r-- 1 root root 163259 Thg 12 3 2021 community-web-php.rules
-rw-r--r-- 1 root root   7646 Thg 12 3 2021 ddos.rules
-rw-r--r-- 1 root root 64313 Thg 12 3 2021 deleted.rules
-rw-r--r-- 1 root root   6743 Thg 12 3 2021 dns.rules
-rw-r--r-- 1 root root   6296 Thg 12 3 2021 dos.rules
-rw-r--r-- 1 root root   1335 Thg 12 3 2021 experimental.rules
-rw-r--r-- 1 root root 30744 Thg 12 3 2021 exploit.rules
-rw-r--r-- 1 root root   4210 Thg 12 3 2021 finger.rules
-rw-r--r-- 1 root root 22000 Thg 12 3 2021 ftp.rules
-rw-r--r-- 1 root root 16482 Thg 12 3 2021 icmp-info.rules
-rw-r--r-- 1 root root   5352 Thg 12 3 2021 icmp.rules
-rw-r--r-- 1 root root 13741 Thg 12 3 2021 imap.rules
-rw-r--r-- 1 root root   3287 Thg 12 3 2021 info.rules
-rw-r--r-- 1 root root   306 Thg 4 11 23:11 local.rules
-rw-r--r-- 1 root root 18486 Thg 12 3 2021 misc.rules
-rw-r--r-- 1 root root   3730 Thg 12 3 2021 multimedia.rules
-rw-r--r-- 1 root root   1935 Thg 12 3 2021 mysql.rules
-rw-r--r-- 1 root root 283854 Thg 12 3 2021 netbios.rules
-rw-r--r-- 1 root root   4755 Thg 12 3 2021 nntp.rules
-rw-r--r-- 1 root root 177773 Thg 12 3 2021 oracle.rules
-rw-r--r-- 1 root root   2247 Thg 12 3 2021 other-ids.rules
-rw-r--r-- 1 root root   5067 Thg 12 3 2021 p2p.rules
-rw-r--r-- 1 root root   6183 Thg 12 3 2021 policy.rules
-rw-r--r-- 1 root root   2088 Thg 12 3 2021 pop2.rules
-rw-r--r-- 1 root root   9591 Thg 12 3 2021 pop3.rules
-rw-r--r-- 1 root root   5918 Thg 12 3 2021 porn.rules
-rw-r--r-- 1 root root 52531 Thg 12 3 2021 rpc.rules
-rw-r--r-- 1 root root   3784 Thg 12 3 2021 rservices.rules
-rw-r--r-- 1 root root   4952 Thg 12 3 2021 scan.rules
-rw-r--r-- 1 root root   9904 Thg 12 3 2021 shellcode.rules
-rw-r--r-- 1 root root 23990 Thg 12 3 2021 smtp.rules
-rw-r--r-- 1 root root   5779 Thg 12 3 2021 snmp.rules
-rw-r--r-- 1 root root 18330 Thg 12 3 2021 sql.rules
-rw-r--r-- 1 root root   5118 Thg 12 3 2021 telnet.rules
-rw-r--r-- 1 root root   3424 Thg 12 3 2021 tftp.rules
-rw-r--r-- 1 root root   2075 Thg 12 3 2021 virus.rules
-rw-r--r-- 1 root root 11089 Thg 12 3 2021 web-attacks.rules
-rw-r--r-- 1 root root 103203 Thg 12 3 2021 web-cgi.rules
-rw-r--r-- 1 root root 10980 Thg 12 3 2021 web-client.rules
-rw-r--r-- 1 root root 10026 Thg 12 3 2021 web-coldfusion.rules
-rw-r--r-- 1 root root 10417 Thg 12 3 2021 web-frontpage.rules
-rw-r--r-- 1 root root 40907 Thg 12 3 2021 web-iis.rules
-rw-r--r-- 1 root root 97307 Thg 12 3 2021 web-misc.rules



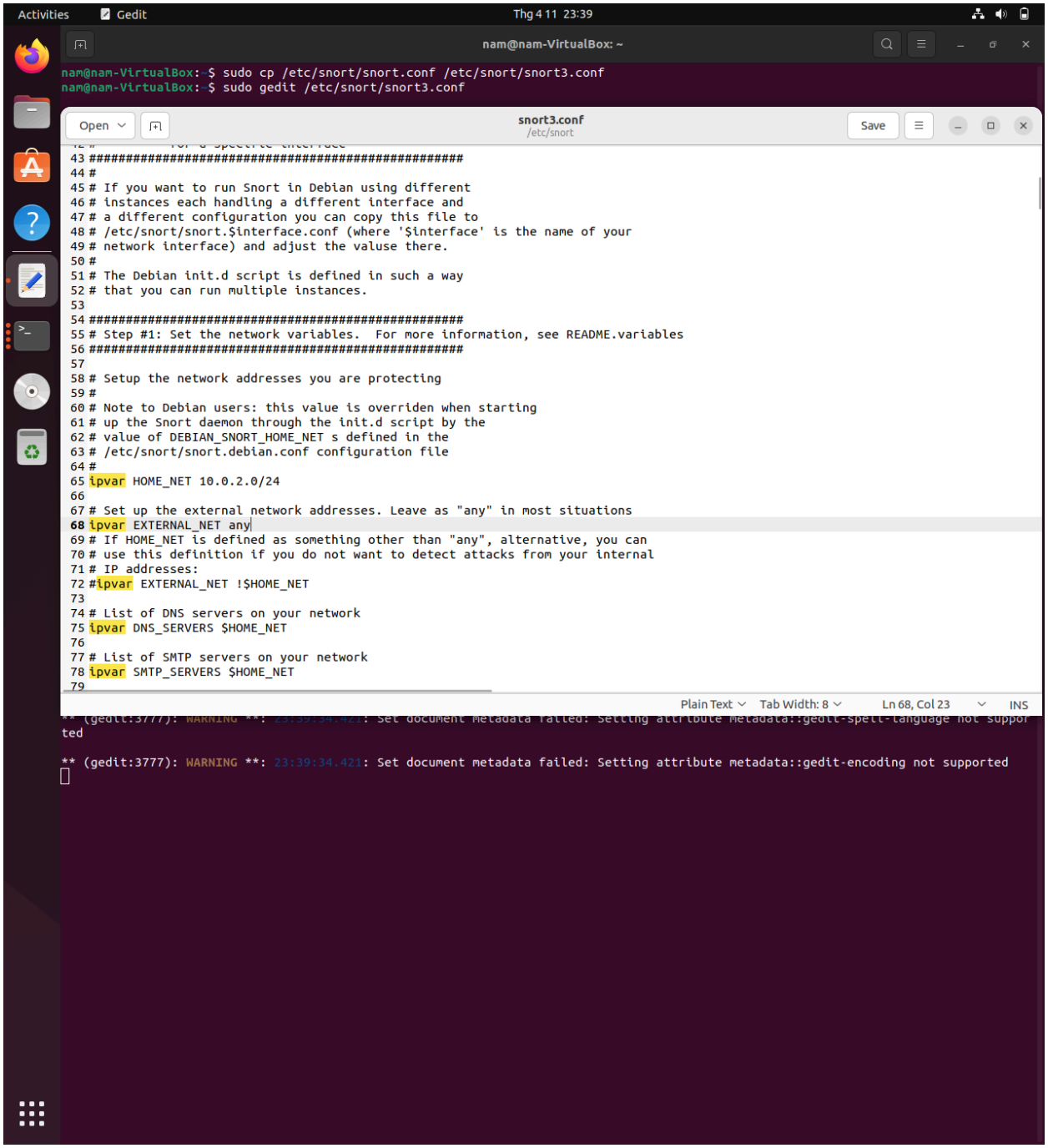
2c, The 5 most interesting categories are backdoor.rules, ddos.rules, virus.rules, community-sql-injection.rules, community-virus.rules

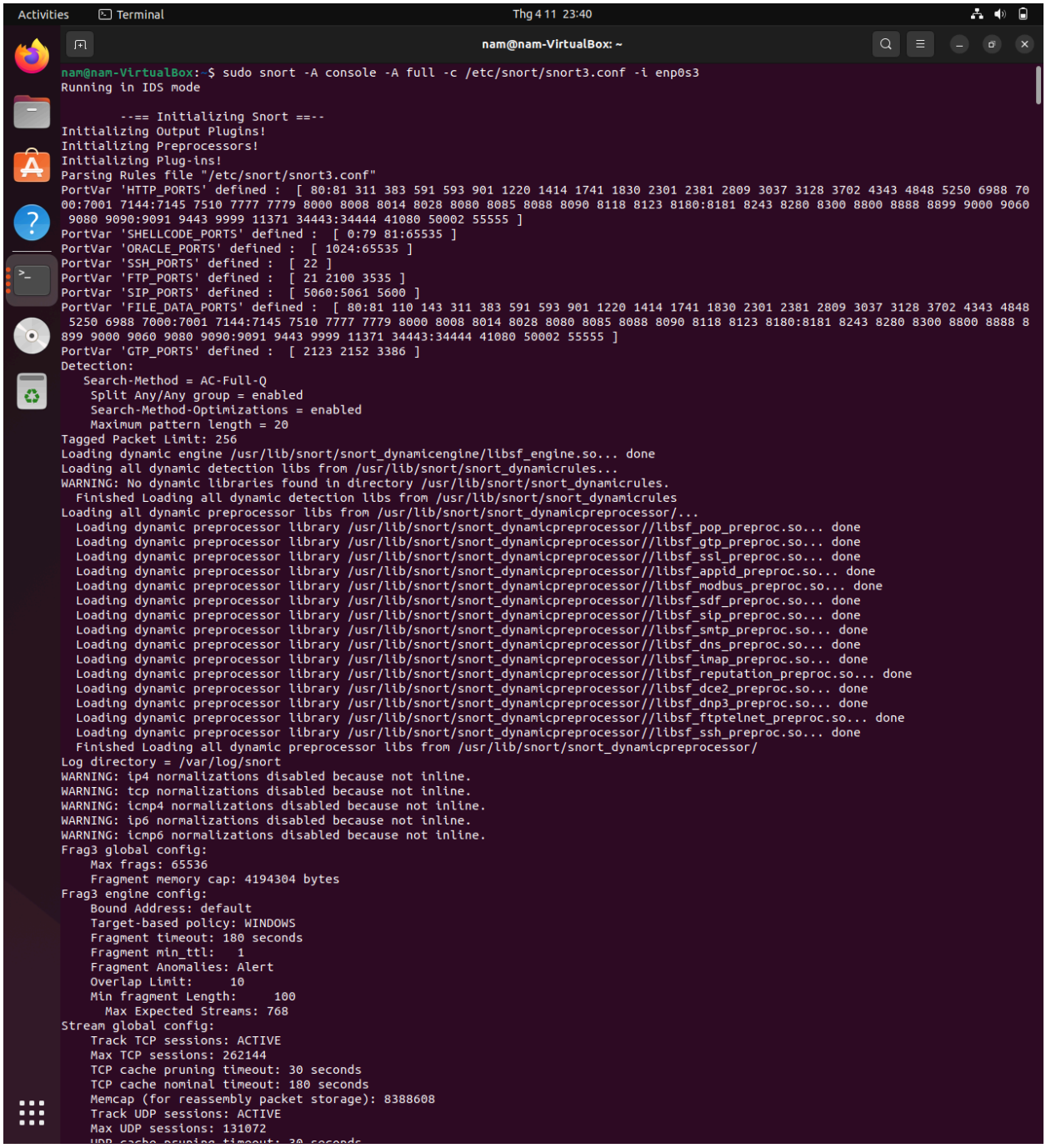
2d, The 5 most important rules individual rules are

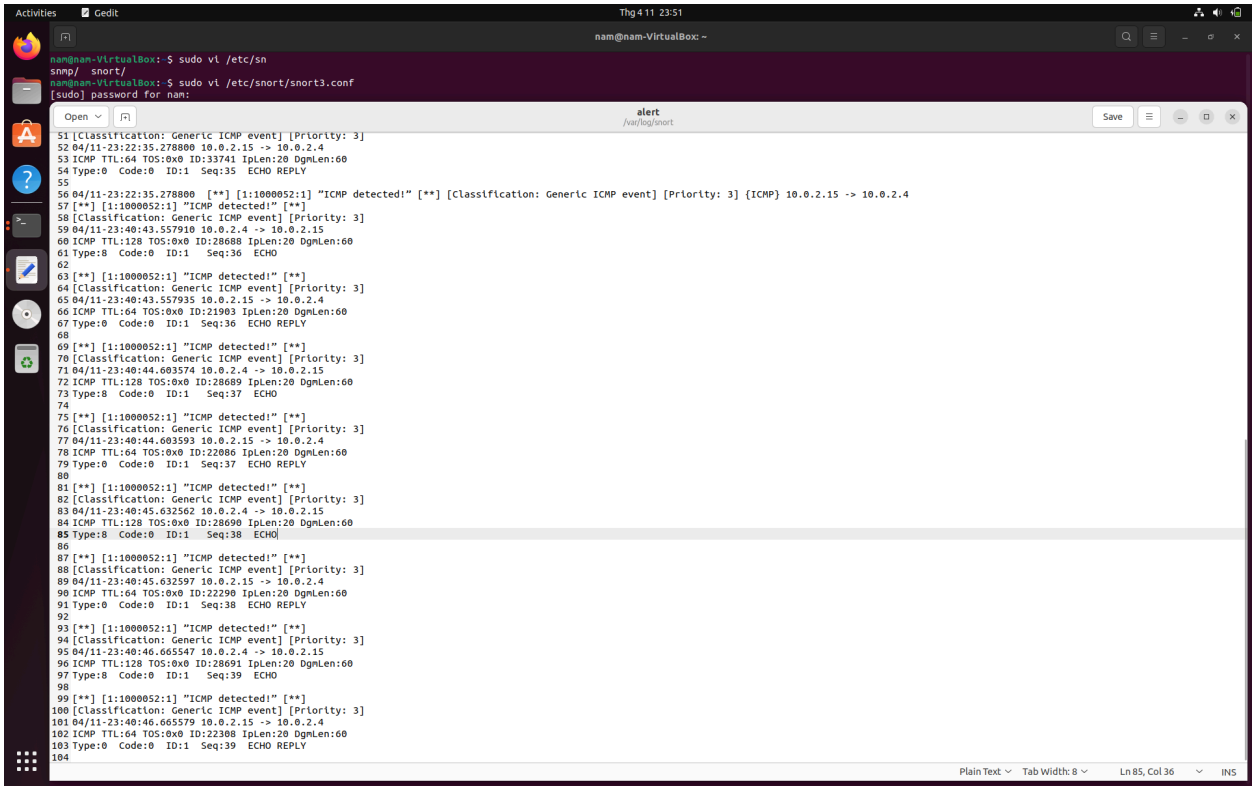
- alert tcp $HOME_NET any -> $EXTERNAL_NET 25 (msg:"VIRUS OUTBOUND bad file attachment"; flow:to_server,established; content:"Content-Disposition|3A|"; nocase; pcre:"/filename\s*=\s*.*?\.(?=[abcdehijlmnoprsvwx])(a(d[ep]|s[dfx])|c([ho]m|li|md|pp)|d(iz|ll|ot)|e(m[fl]|xe)|h(lp|sq|ta)|jse?|m(d[abew]|s[ip])|p(p[st]|if|[lm]|ot)|r(eg|tf)|s(cr|[hy]s|wf)|v(b[es]?|cf|xd)|w(m[dfsz]|p[dmsz]|s[cfh])|xl[tw]|bat|ini|lnk|nws|ocx)[\x27\x22\n\r\s]/iR"; classtype:suspicious-filename-detect; sid:721; rev:8;)

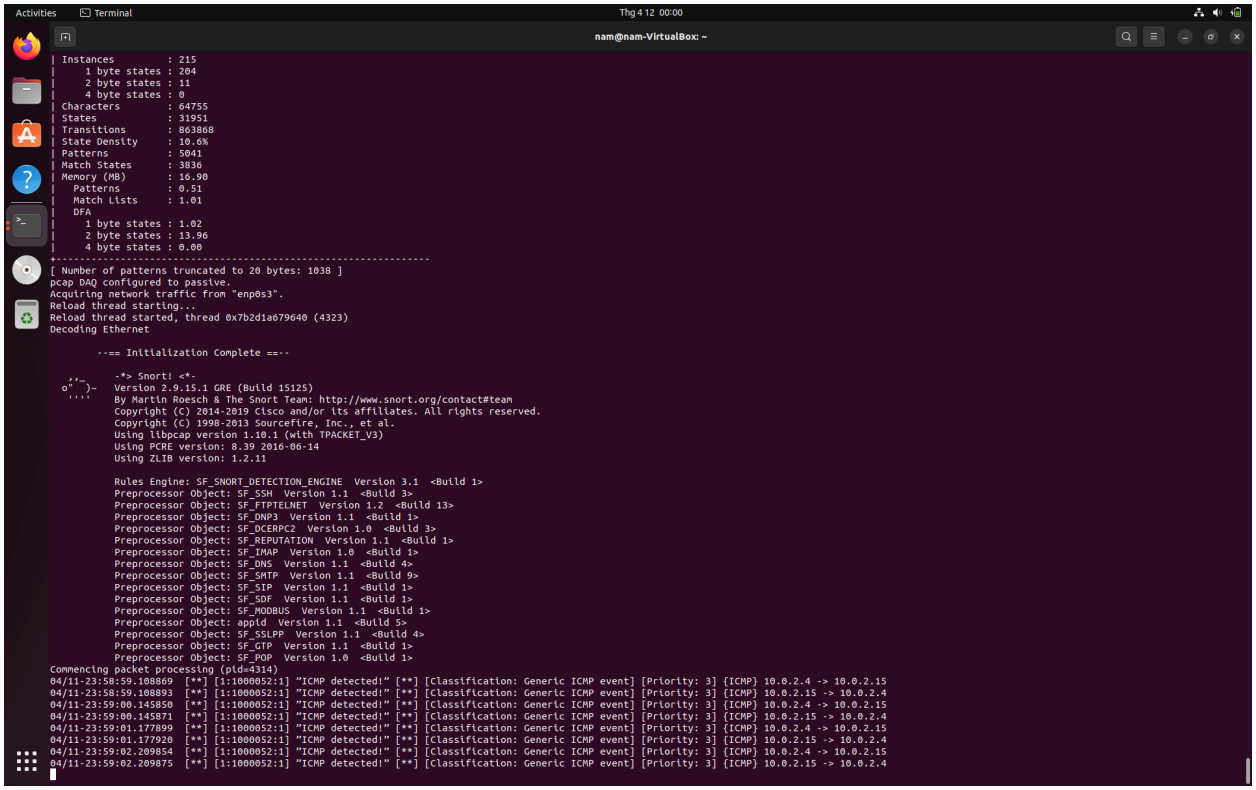
- alert tcp $EXTERNAL_NET any -> $HOME_NET 27665 (msg:"DDOS Trin00 Attacker to Master default mdie password"; flow:established,to_server; content:"killme"; classtype:bad-unknown; sid:235; rev:2;)
- alert icmp $EXTERNAL_NET any <> $HOME_NET any (msg:"DDOS Stacheldraht handler->agent niggahbitch"; icmp_id:9015; itype:0; content:"niggahbitch"; reference:url,staff.washington.edu/dittrich/misc/stacheldraht.analysis; classtype:attempted-dos; sid:1854; rev:7;)
- alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"COMMUNITY SQL-INJECTION WIZZ ForumAuthDetails Sql Injection attempt"; flow:to_server,established; uricontent:"/ForumAuthDetails.php"; nocase; uricontent:"AuthID|3D|"; nocase; uricontent:"union"; nocase; uricontent:"select"; nocase; uricontent:"from"; nocase; uricontent:"ForumUser"; nocase; uricontent:"where"; nocase; reference:bugtraq,15410; reference:url,www.osvdb.org/displayvuln.php?osvdb_id=20845; classtype:web-application-attack; sid:100000193; rev:2;)

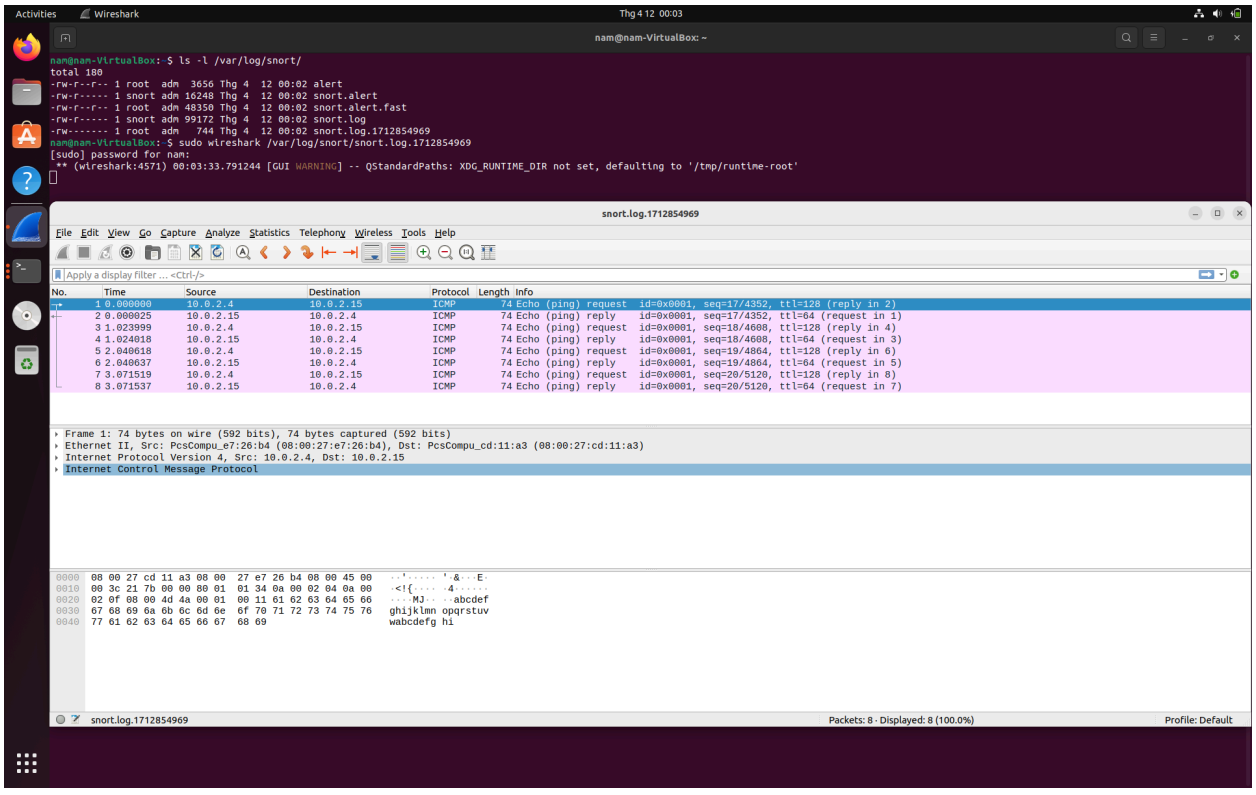
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"COMMUNITY SQL-INJECTION Diesel Joke Script Sql Injection attempt"; flow:to_server,established; uricontent:"/category.php"; nocase; uricontent:"id="; uricontent:"union"; nocase; uricontent:"select"; nocase; uricontent:"admin"; nocase; reference:bugtraq,18760; classtype:web-application-attack; sid:100000691; rev:2;)


Activities
Gedit
Thg 4 11 23:39
nam@nam-VirtualBox: ~
nam@nam-VirtualBox:~$ sudo cp /etc/snort/snort.conf /etc/snort/snort3.conf
nam@nam-VirtualBox:~$ sudo gedit /etc/snort/snort3.conf
Open
snort3.conf
/etc/snort
Save
43 ##
44 #
45 # If you want to run Snort in Debian using different
46 # instances each handling a different interface and
47 # a different configuration you can copy this file to
48 # /etc/snort/snort.$interface.conf (where '$interface' is the name of your
49 # network interface) and adjust the valuse there.
50 #
51 # The Debian init.d script is defined in such a way
52 # that you can run multiple instances.
53
54 ##
55 # Step #1: Set the network variables. For more information, see README.variables
56 ##
57
58 # Setup the network addresses you are protecting
59 #
60 # Note to Debian users: this value is overriden when starting
61 # up the Snort daemon through the init.d script by the
62 # value of DEBIAN_SNORT_HOME_NET s defined in the
63 # /etc/snort/snort.debian.conf configuration file
64 #
65 ipvar HOME_NET 10.0.2.0/24
66
67 # Set up the external network addresses. Leave as "any" in most situations
68 ipvar EXTERNAL_NET any
69 # If HOME_NET is defined as something other than "any", alternative, you can
70 # use this definition if you do not want to detect attacks from your internal
71 # IP addresses:
72 #ipvar EXTERNAL_NET !$HOME_NET
73
74 # List of DNS servers on your network
75 ipvar DNS_SERVERS $HOME_NET
76
77 # List of SMTP servers on your network
78 ipvar SMTP_SERVERS $HOME_NET
79
Plain Text
Tab Width: 8
Ln 68, Col 23
INS
** (gedit:3777): WARNING **: 23:39:34.421: Set document metadata failed: Setting attribute metadata::gedit-spell-language not supported
** (gedit:3777): WARNING **: 23:39:34.421: Set document metadata failed: Setting attribute metadata::gedit-encoding not supported


Activities
Terminal
Thg 4 11 23:40
nam@nam-VirtualBox: ~
nam@nam-VirtualBox:~$ sudo snort -A console -A full -c /etc/snort/snort3.conf -i enp0s3
Running in IDS mode
--== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "/etc/snort/snort3.conf"
PortVar 'HTTP_PORTS' defined : [80:81 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 3702 4343 4848 5250 6988 7000:7001 7144:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 50002 55555]
PortVar 'SHELLCODE_PORTS' defined : [0:79 81:65535]
PortVar 'ORACLE_PORTS' defined : [1024:65535]
PortVar 'SSH_PORTS' defined : [22]
PortVar 'FTP_PORTS' defined : [21 2100 3535]
PortVar 'SIP_PORTS' defined : [5060:5061 5600]
PortVar 'FILE_DATA_PORTS' defined : [80:81 110 143 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 3702 4343 4848 5250 6988 7000:7001 7144:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 50002 55555]
PortVar 'GTP_PORTS' defined : [2123 2152 3386]
Detection:
Search-Method = AC-Full-Q
Split Any/Any group = enabled
Search-Method-Optimizations = enabled
Maximum pattern length = 20
Tagged Packet Limit: 256
Loading dynamic engine /usr/lib/snort/snort_dynamicengine/libsf_engine.so... done
Loading all dynamic detection libs from /usr/lib/snort/snort_dynamicrules...
WARNING: No dynamic libraries found in directory /usr/lib/snort/snort_dynamicrules.
Finished Loading all dynamic detection libs from /usr/lib/snort/snort_dynamicrules
Loading all dynamic preprocessor libs from /usr/lib/snort/snort_dynamicpreprocessor/...
Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_pop_preproc.so... done
Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_gtp_preproc.so... done
Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_ssl_preproc.so... done
Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_appid_preproc.so... done
Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_modbus_preproc.so... done
Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_sdf_preproc.so... done
Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_sip_preproc.so... done
Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_smtp_preproc.so... done
Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_dns_preproc.so... done
Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_imap_preproc.so... done
Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_reputation_preproc.so... done
Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_dce2_preproc.so... done
Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_dnp3_preproc.so... done
Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_ftptelnet_preproc.so... done
Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_ssh_preproc.so... done
Finished Loading all dynamic preprocessor libs from /usr/lib/snort/snort_dynamicpreprocessor/
Log directory = /var/log/snort
WARNING: ip4 normalizations disabled because not inline.
WARNING: tcp normalizations disabled because not inline.
WARNING: icmp4 normalizations disabled because not inline.
WARNING: ip6 normalizations disabled because not inline.
WARNING: icmp6 normalizations disabled because not inline.
Frag3 global config:
Max frags: 65536
Fragment memory cap: 4194304 bytes
Frag3 engine config:
Bound Address: default
Target-based policy: WINDOWS
Fragment timeout: 180 seconds
Fragment min_ttl: 1
Fragment Anomalies: Alert
Overlap Limit: 10
Min fragment Length: 100
Max Expected Streams: 768
Stream global config:
Track TCP sessions: ACTIVE
Max TCP sessions: 262144
TCP cache pruning timeout: 30 seconds
TCP cache nominal timeout: 180 seconds
Memcap (for reassembly packet storage): 8388608
Track UDP sessions: ACTIVE
Max UDP sessions: 131072


Activities
Gedit
Thg 4 11 23:51
nam@nam-VirtualBox: ~
nam@nam-VirtualBox:~$ sudo vi /etc/sn
snmp/ snort/
nam@nam-VirtualBox:~$ sudo vi /etc/snort/snort3.conf
[sudo] password for nam:
Open
alert
/var/log/snort
Save
51 [Classification: Generic ICMP event] [Priority: 3]
52 04/11-23:22:35.278800 10.0.2.15 -> 10.0.2.4
53 ICMP TTL:64 TOS:0x0 ID:33741 IpLen:20 DgmLen:60
54 Type:0 Code:0 ID:1 Seq:35 ECHO REPLY
55
56 04/11-23:22:35.278800 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.2.15 -> 10.0.2.4
57 [**] [1:1000052:1] "ICMP detected!" [**]
58 [Classification: Generic ICMP event] [Priority: 3]
59 04/11-23:40:43.557910 10.0.2.4 -> 10.0.2.15
60 ICMP TTL:128 TOS:0x0 ID:28688 IpLen:20 DgmLen:60
61 Type:8 Code:0 ID:1 Seq:36 ECHO
62
63 [**] [1:1000052:1] "ICMP detected!" [**]
64 [Classification: Generic ICMP event] [Priority: 3]
65 04/11-23:40:43.557935 10.0.2.15 -> 10.0.2.4
66 ICMP TTL:64 TOS:0x0 ID:21903 IpLen:20 DgmLen:60
67 Type:0 Code:0 ID:1 Seq:36 ECHO REPLY
68
69 [**] [1:1000052:1] "ICMP detected!" [**]
70 [Classification: Generic ICMP event] [Priority: 3]
71 04/11-23:40:44.603574 10.0.2.4 -> 10.0.2.15
72 ICMP TTL:128 TOS:0x0 ID:28689 IpLen:20 DgmLen:60
73 Type:8 Code:0 ID:1 Seq:37 ECHO
74
75 [**] [1:1000052:1] "ICMP detected!" [**]
76 [Classification: Generic ICMP event] [Priority: 3]
77 04/11-23:40:44.603593 10.0.2.15 -> 10.0.2.4
78 ICMP TTL:64 TOS:0x0 ID:22086 IpLen:20 DgmLen:60
79 Type:0 Code:0 ID:1 Seq:37 ECHO REPLY
80
81 [**] [1:1000052:1] "ICMP detected!" [**]
82 [Classification: Generic ICMP event] [Priority: 3]
83 04/11-23:40:45.632562 10.0.2.4 -> 10.0.2.15
84 ICMP TTL:128 TOS:0x0 ID:28690 IpLen:20 DgmLen:60
85 Type:8 Code:0 ID:1 Seq:38 ECHO
86
87 [**] [1:1000052:1] "ICMP detected!" [**]
88 [Classification: Generic ICMP event] [Priority: 3]
89 04/11-23:40:45.632597 10.0.2.15 -> 10.0.2.4
90 ICMP TTL:64 TOS:0x0 ID:22290 IpLen:20 DgmLen:60
91 Type:0 Code:0 ID:1 Seq:38 ECHO REPLY
92
93 [**] [1:1000052:1] "ICMP detected!" [**]
94 [Classification: Generic ICMP event] [Priority: 3]
95 04/11-23:40:46.665547 10.0.2.4 -> 10.0.2.15
96 ICMP TTL:128 TOS:0x0 ID:28691 IpLen:20 DgmLen:60
97 Type:8 Code:0 ID:1 Seq:39 ECHO
98
99 [**] [1:1000052:1] "ICMP detected!" [**]
100 [Classification: Generic ICMP event] [Priority: 3]
101 04/11-23:40:46.665579 10.0.2.15 -> 10.0.2.4
102 ICMP TTL:64 TOS:0x0 ID:22308 IpLen:20 DgmLen:60
103 Type:0 Code:0 ID:1 Seq:39 ECHO REPLY
104
Plain Text
Tab Width: 8
Ln 85, Col 36
INS


Activities
Terminal
Thg 4 12 00:00
nam@nam-VirtualBox: ~
| Instances : 215
| 1 byte states : 204
| 2 byte states : 11
| 4 byte states : 0
| Characters : 64755
| States : 31951
| Transitions : 863868
| State Density : 10.6%
| Patterns : 5041
| Match States : 3836
| Memory (MB) : 16.90
| Patterns : 0.51
| Match Lists : 1.01
| DFA
| 1 byte states : 1.02
| 2 byte states : 13.96
| 4 byte states : 0.00
[Number of patterns truncated to 20 bytes: 1038]
pcap DAQ configured to passive.
Acquiring network traffic from "enp0s3".
Reload thread starting...
Reload thread started, thread 0x7b2d1a679640 (4323)
Decoding Ethernet
--== Initialization Complete ==--
-*> Snort! <*-
Version 2.9.15.1 GRE (Build 15125)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.10.1 (with TPACKET_V3)
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.2.11
Rules Engine: SF_SNORT_DETECTION_ENGINE Version 3.1 <Build 1>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Preprocessor Object: SF_SDF 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_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Commencing packet processing (pid=4314)
04/11-23:58:59.108869 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.2.4 -> 10.0.2.15
04/11-23:58:59.108893 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.2.15 -> 10.0.2.4
04/11-23:59:00.145850 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.2.4 -> 10.0.2.15
04/11-23:59:00.145871 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.2.15 -> 10.0.2.4
04/11-23:59:01.177899 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.2.4 -> 10.0.2.15
04/11-23:59:01.177920 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.2.15 -> 10.0.2.4
04/11-23:59:02.209854 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.2.4 -> 10.0.2.15
04/11-23:59:02.209875 [**] [1:1000052:1] "ICMP detected!" [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.2.15 -> 10.0.2.4


Activities
Wireshark
Thg 4 12 00:03
nam@nam-VirtualBox: ~
nam@nam-VirtualBox: $ ls -l /var/log/snort/
total 180
-rw-r--r-- 1 root adm 3656 Thg 4 12 00:02 alert
-rw-r----- 1 snort adm 16248 Thg 4 12 00:02 snort.alert
-rw-r--r-- 1 root adm 48350 Thg 4 12 00:02 snort.alert.fast
-rw-r----- 1 snort adm 99172 Thg 4 12 00:02 snort.log
-rw------- 1 root adm 744 Thg 4 12 00:02 snort.log.1712854969
nam@nam-VirtualBox: $ sudo wireshark /var/log/snort/snort.log.1712854969
[sudo] password for nam:
** (wireshark:4571) 00:03:33.791244 [GUI WARNING] -- QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
snort.log.1712854969
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000 10.0.2.4 10.0.2.15 ICMP 74 Echo (ping) request id=0x0001, seq=17/4352, ttl=128 (reply in 2)
2 0.000025 10.0.2.15 10.0.2.4 ICMP 74 Echo (ping) reply id=0x0001, seq=17/4352, ttl=64 (request in 1)
3 1.023999 10.0.2.4 10.0.2.15 ICMP 74 Echo (ping) request id=0x0001, seq=18/4608, ttl=128 (reply in 4)
4 1.024018 10.0.2.15 10.0.2.4 ICMP 74 Echo (ping) reply id=0x0001, seq=18/4608, ttl=64 (request in 3)
5 2.040618 10.0.2.4 10.0.2.15 ICMP 74 Echo (ping) request id=0x0001, seq=19/4864, ttl=128 (reply in 6)
6 2.040637 10.0.2.15 10.0.2.4 ICMP 74 Echo (ping) reply id=0x0001, seq=19/4864, ttl=64 (request in 5)
7 3.071519 10.0.2.4 10.0.2.15 ICMP 74 Echo (ping) request id=0x0001, seq=20/5120, ttl=128 (reply in 8)
8 3.071537 10.0.2.15 10.0.2.4 ICMP 74 Echo (ping) reply id=0x0001, seq=20/5120, ttl=64 (request in 7)
Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
Ethernet II, Src: PcsCompu_e7:26:b4 (08:00:27:e7:26:b4), Dst: PcsCompu_cd:11:a3 (08:00:27:cd:11:a3)
Internet Protocol Version 4, Src: 10.0.2.4, Dst: 10.0.2.15
Internet Control Message Protocol
0000 08 00 27 cd 11 a3 08 00 27 e7 26 b4 08 00 45 00
0010 00 3c 21 7b 00 00 80 01 01 34 0a 00 02 04 0a 00
0020 02 0f 08 00 4d 4a 00 01 00 11 61 62 63 64 65 66
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76
0040 77 61 62 63 64 65 66 67 68 69
snort.log.1712854969
Packets: 8 · Displayed: 8 (100.0%)
Profile: Default