Samuel Baidoo

Snort tutorial

Step 1: Installation

Open your terminal.

Update the package list to ensure you have the latest information on available packages:
sudo apt update

Install Snort using the package manager:

sudo apt install snort

You might be prompted to confirm the installation. Type "Y" and press Enter.

1. During the installation, you may be asked to configure your network interface. Choose the interface that connects to your network
2. After installation, Snort should be up and running.

Step 2: Configure Snort

1. Create a configuration file for Snort. You can use the default configuration as a starting point:
   sudo cp /etc/snort/snort.conf /etc/snort/snort.local.conf

   Edit the configuration file:

   sudo nano /etc/snort/snort.local.conf

   Customize your Snort rules, network settings, and include any additional rulesets as needed. Save the changes.

   Snort uses rules to detect suspicious network activity. You can find and download community rules from the Snort website: https://www.snort.org/community.

   You can also enable/disable specific rules in your configuration file.

   Step 4: Start Snort

1. Start Snort in Network Intrusion Detection mode:
   sudo snort -A console -q -u snort -g snort -c /etc/snort/snort.local.conf -i <your_network_interface>

   Replace **<your_network_interface>** with the appropriate network interface you configured earlier.

   Snort will start monitoring network traffic and generating alerts.

   Step 5: Test and Monitor

1. Generate some network traffic or attempt known attacks to test Snort's functionality.
2. Snort will generate alerts for any suspicious activity based on the defined rules.

Step 6: View Alerts

To view Snort alerts, you can check the `/var/log/snort/alert` file. You can also use Snorby, BASE, or other web interfaces to manage Snort alerts.

Step 7: Customization and Ongoing Management
Customize your rules and configurations based on your network's specific needs and monitor Snort regularly for security events.

This is a basic guide to get you started with Snort. For a production environment, you should consider additional security measures and consult Snort documentation and best practices.

1. Ensure you have a Linux-based system (e.g., Ubuntu) with administrative

privileges. 2. Install Snort using the package manager.

3. Create and customize a Snort configuration file.

4. Download community rules or create custom rules for specific network monitoring.

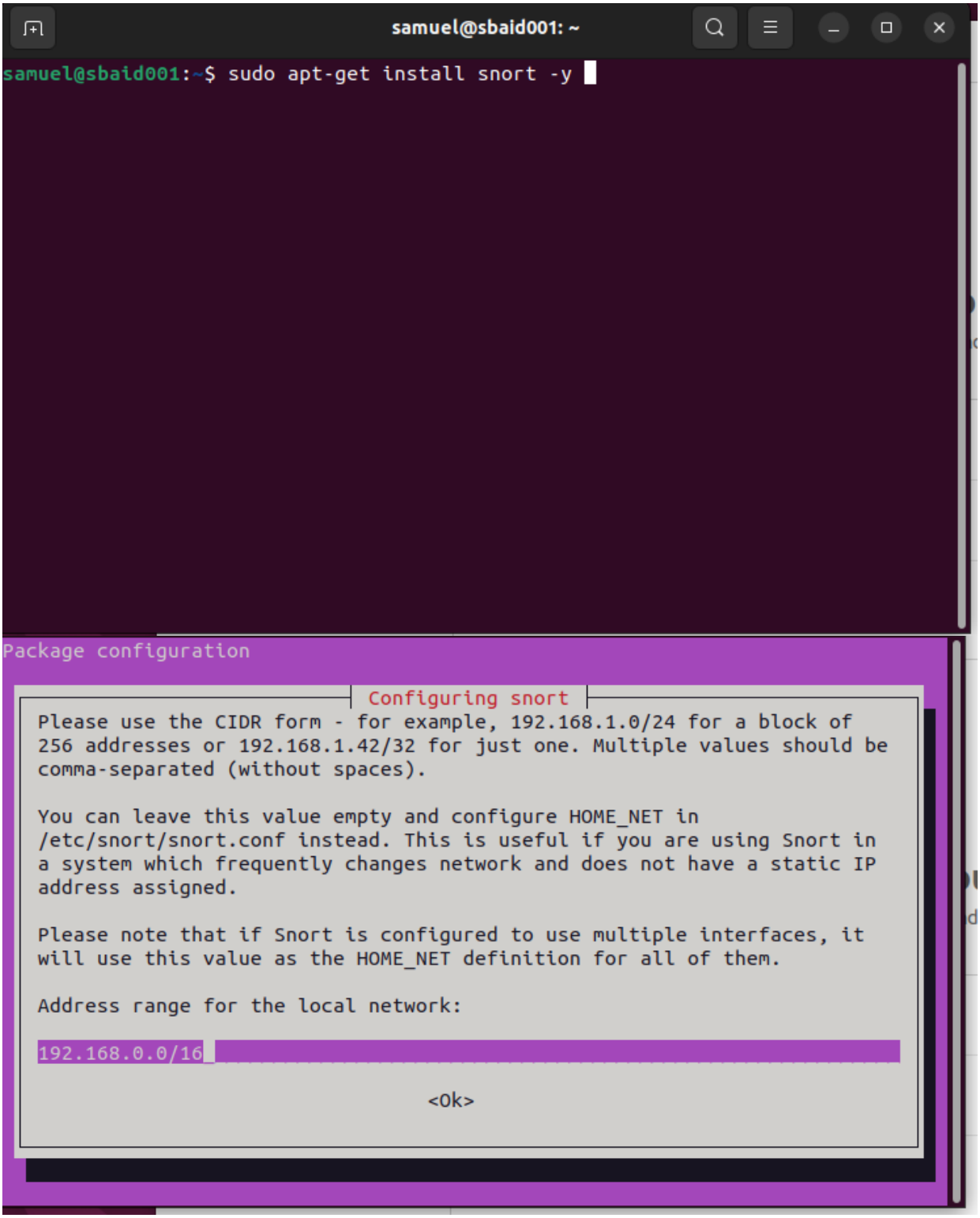
5. Start Snort in Network Intrusion Detection mode, monitoring network traffic. 6.

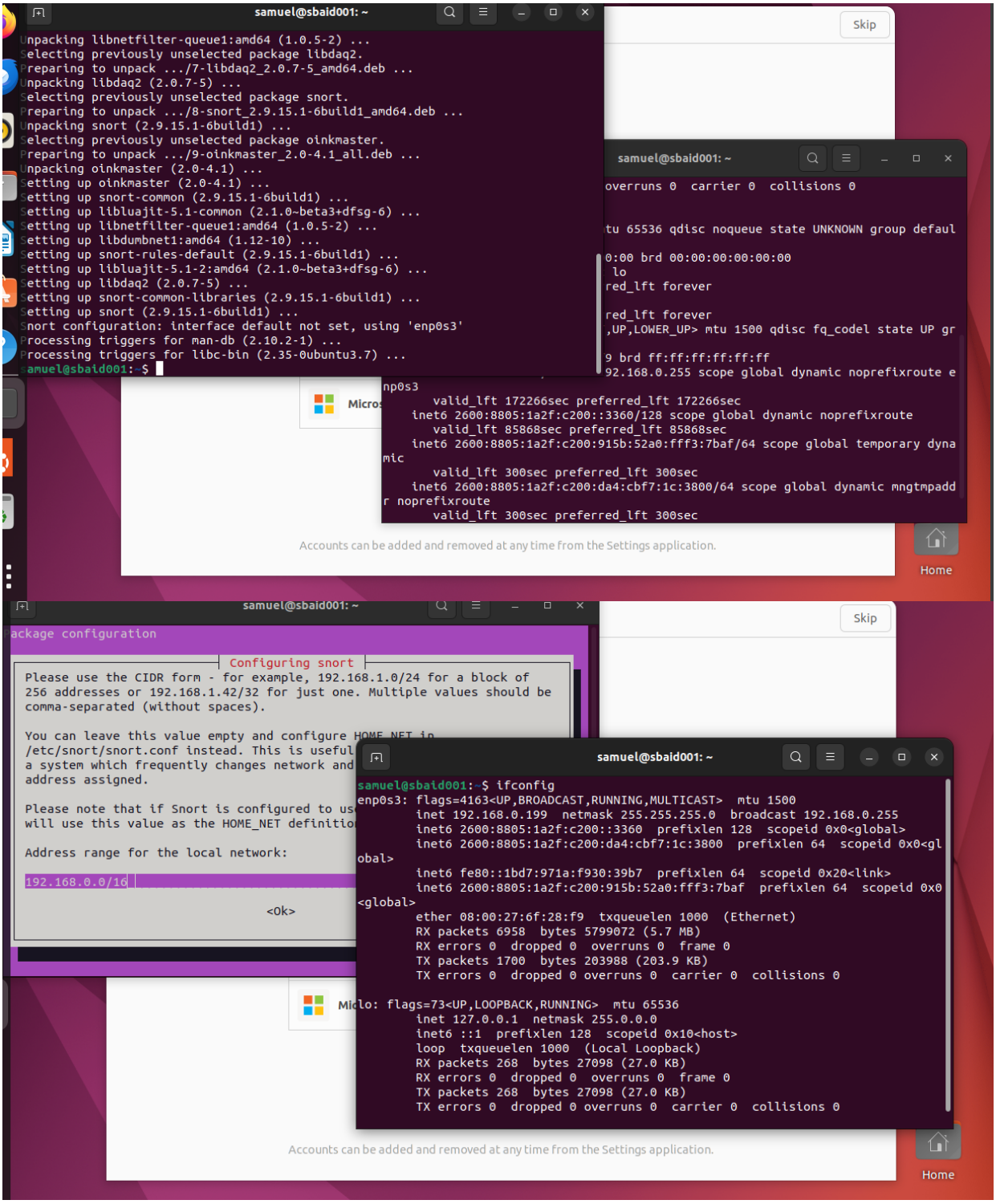
Test Snort by generating network activity and monitor alerts.

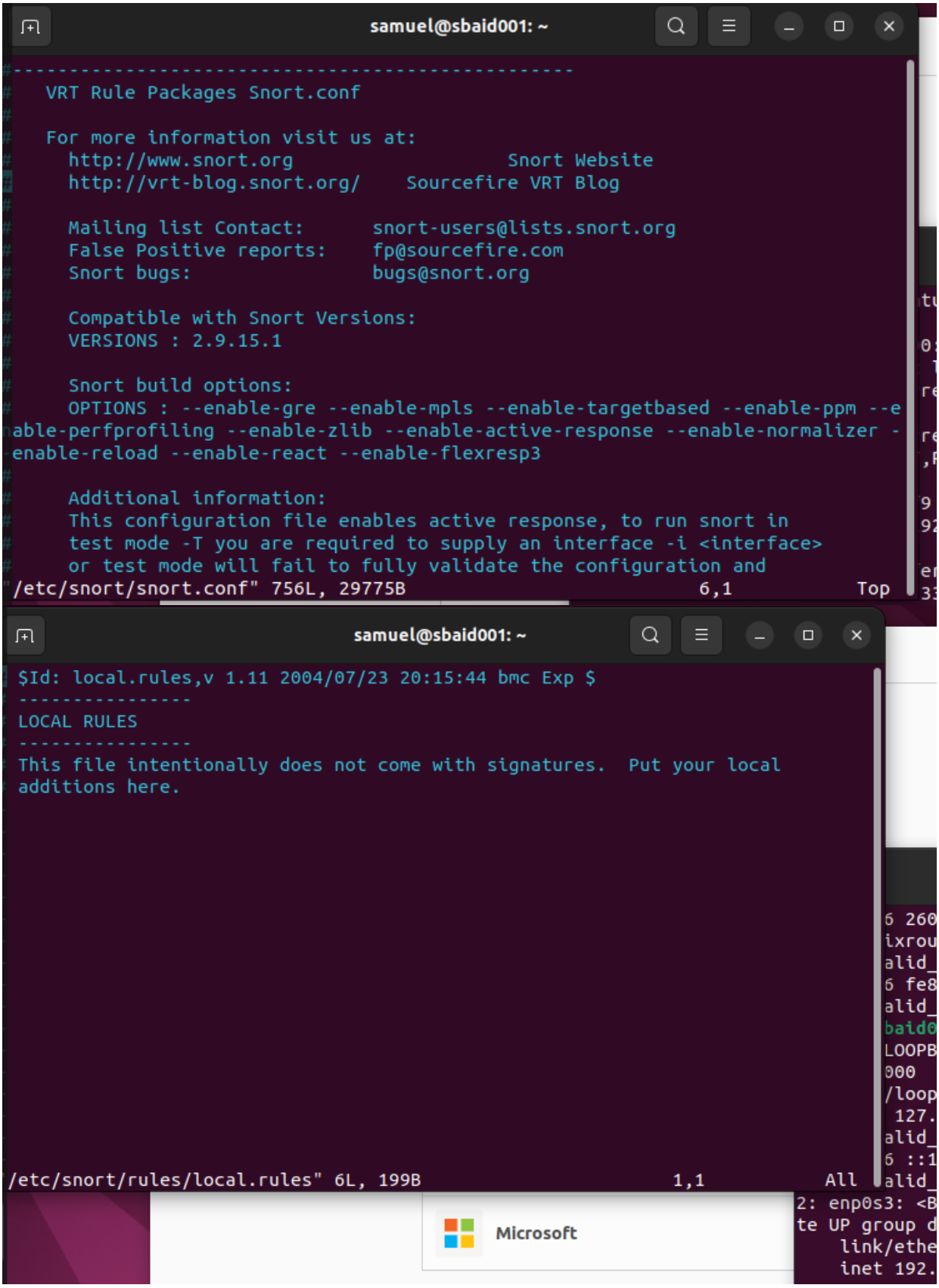
7. View alerts in the `/var/log/snort/alert` file and consider using web interfaces for management.

8. Customize and manage Snort's rules and configurations as needed for your network's security.

Include screenshots of key steps for reference. This guide provides a starting point; consult Snort documentation and best practices for production environments.

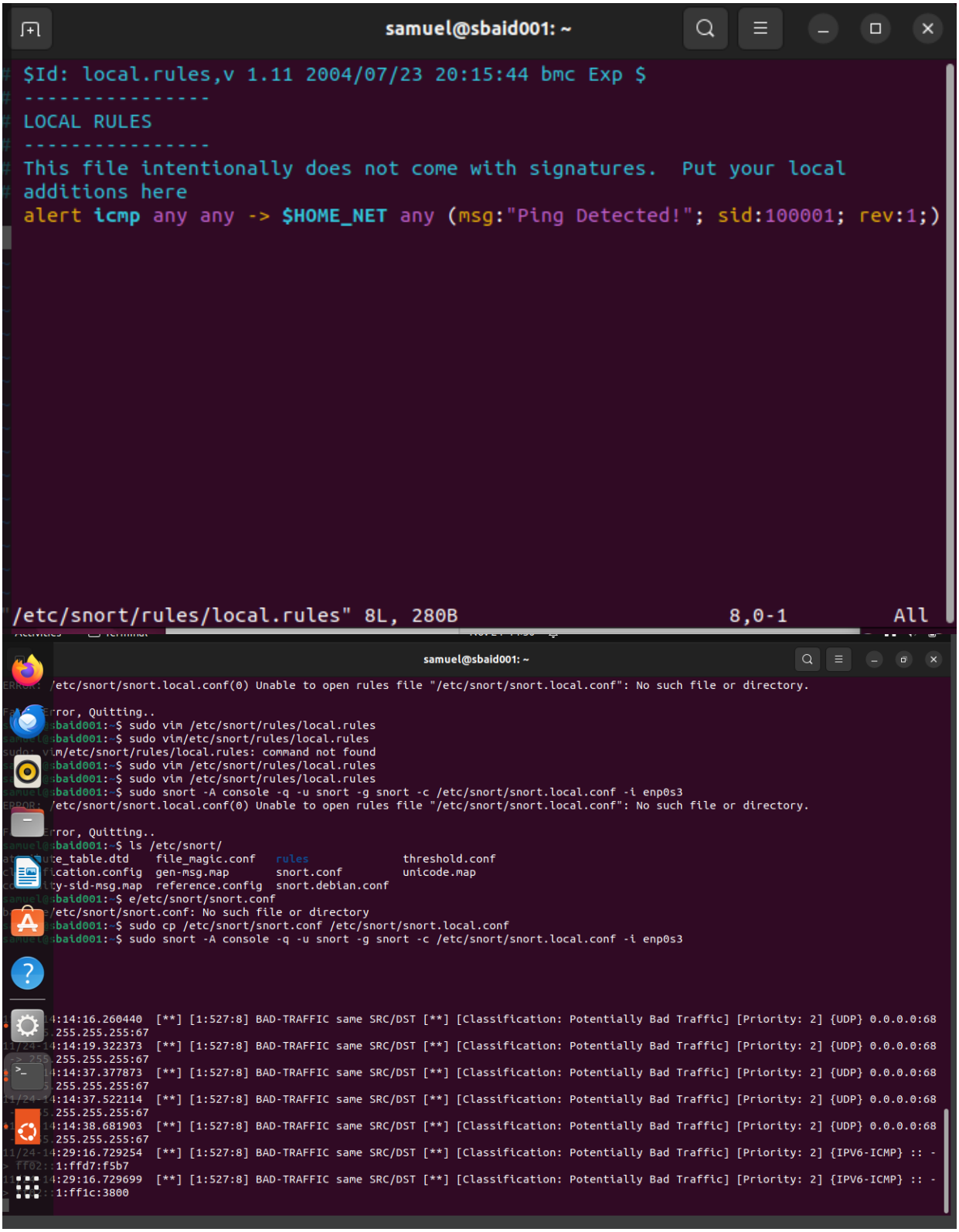

samuel@sbaid001: ~
samuel@sbaid001:~$ sudo apt-get install snort -y
Package configuration
Configuring snort
Please use the CIDR form - for example, 192.168.1.0/24 for a block of 256 addresses or 192.168.1.42/32 for just one. Multiple values should be comma-separated (without spaces).
You can leave this value empty and configure HOME_NET in /etc/snort/snort.conf instead. This is useful if you are using Snort in a system which frequently changes network and does not have a static IP address assigned.
Please note that if Snort is configured to use multiple interfaces, it will use this value as the HOME_NET definition for all of them.
Address range for the local network:
192.168.0.0/16
<Ok>


samuel@sbaid001: ~
Unpacking libnetfilter-queue1:amd64 (1.0.5-2) ...
Selecting previously unselected package libdaq2.
Preparing to unpack .../7-libdaq2_2.0.7-5_amd64.deb ...
Unpacking libdaq2 (2.0.7-5) ...
Selecting previously unselected package snort.
Preparing to unpack .../8-snort_2.9.15.1-6build1_amd64.deb ...
Unpacking snort (2.9.15.1-6build1) ...
Selecting previously unselected package oinkmaster.
Preparing to unpack .../9-oinkmaster_2.0-4.1_all.deb ...
Unpacking oinkmaster (2.0-4.1) ...
Setting up oinkmaster (2.0-4.1) ...
Setting up snort-common (2.9.15.1-6build1) ...
Setting up libluajit-5.1-common (2.1.0~beta3+dfsg-6) ...
Setting up libnetfilter-queue1:amd64 (1.0.5-2) ...
Setting up libdumbnet1:amd64 (1.12-10) ...
Setting up snort-rules-default (2.9.15.1-6build1) ...
Setting up libluajit-5.1-2:amd64 (2.1.0~beta3+dfsg-6) ...
Setting up libdaq2 (2.0.7-5) ...
Setting up snort-common-libraries (2.9.15.1-6build1) ...
Setting up snort (2.9.15.1-6build1) ...
Snort configuration: interface default not set, using 'enp0s3'
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for libc-bin (2.35-0ubuntu3.7) ...
samuel@sbaid001:~$
Skip
samuel@sbaid001: ~
overruns 0 carrier 0 collisions 0
tu 65536 qdisc noqueue state UNKNOWN group defaul
0:00 brd 00:00:00:00:00:00
lo
red_lft forever
red_lft forever
,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gr
9 brd ff:ff:ff:ff:ff:ff
92.168.0.255 scope global dynamic noprefixroute e
np0s3
valid_lft 172266sec preferred_lft 172266sec
inet6 2600:8805:1a2f:c200::3360/128 scope global dynamic noprefixroute
valid_lft 85868sec preferred_lft 85868sec
inet6 2600:8805:1a2f:c200:915b:52a0:fff3:7baf/64 scope global temporary dyna
mic
valid_lft 300sec preferred_lft 300sec
inet6 2600:8805:1a2f:c200:da4:cbf7:1c:3800/64 scope global dynamic mngtmpadd
r noprefixroute
valid_lft 300sec preferred_lft 300sec
Accounts can be added and removed at any time from the Settings application.
Home
samuel@sbaid001: ~
ackage configuration
Configuring snort
Please use the CIDR form - for example, 192.168.1.0/24 for a block of
256 addresses or 192.168.1.42/32 for just one. Multiple values should be
comma-separated (without spaces).
You can leave this value empty and configure HOME_NET in
/etc/snort/snort.conf instead. This is useful
a system which frequently changes network and
address assigned.
Please note that if Snort is configured to us
will use this value as the HOME_NET definitio
Address range for the local network:
192.168.0.0/16
<Ok>
Skip
samuel@sbaid001: ~
samuel@sbaid001:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.0.199 netmask 255.255.255.0 broadcast 192.168.0.255
inet6 2600:8805:1a2f:c200::3360 prefixlen 128 scopeid 0x0<global>
inet6 2600:8805:1a2f:c200:da4:cbf7:1c:3800 prefixlen 64 scopeid 0x0<gl
obal>
inet6 fe80::1bd7:971a:f930:39b7 prefixlen 64 scopeid 0x20<link>
inet6 2600:8805:1a2f:c200:915b:52a0:fff3:7baf prefixlen 64 scopeid 0x0
<global>
ether 08:00:27:6f:28:f9 txqueuelen 1000 (Ethernet)
RX packets 6958 bytes 5799072 (5.7 MB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 1700 bytes 203988 (203.9 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 268 bytes 27098 (27.0 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 268 bytes 27098 (27.0 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
Accounts can be added and removed at any time from the Settings application.
Home


samuel@sbaid001: ~
#---
VRT Rule Packages Snort.conf
#
For more information visit us at:
http://www.snort.org   Snort Website
http://vrt-blog.snort.org/   Sourcefire VRT Blog
#
Mailing list Contact: snort-users@lists.snort.org
False Positive reports: fp@sourcefire.com
Snort bugs: bugs@snort.org
#
Compatible with Snort Versions:
VERSIONS : 2.9.15.1
#
Snort build options:
OPTIONS : --enable-gre --enable-mpls --enable-targetbased --enable-ppm --e
nable-perfprofiling --enable-zlib --enable-active-response --enable-normalizer -
enable-reload --enable-react --enable-flexresp3
#
Additional information:
This configuration file enables active response, to run snort in
test mode -T you are required to supply an interface -i <interface>
or test mode will fail to fully validate the configuration and
"/etc/snort/snort.conf" 756L, 29775B 6,1 Top
samuel@sbaid001: ~
$Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $

LOCAL RULES

This file intentionally does not come with signatures. Put your local
additions here.
"/etc/snort/rules/local.rules" 6L, 199B 1,1 All
Microsoft


samuel@sbaid001: ~
$Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $

LOCAL RULES

This file intentionally does not come with signatures. Put your local
additions here
alert icmp any any -> $HOME_NET any (msg:"Ping Detected!"; sid:100001; rev:1;)
"/etc/snort/rules/local.rules" 8L, 280B 8,0-1 All
samuel@sbaid001: ~
/etc/snort/snort.local.conf(0) Unable to open rules file "/etc/snort/snort.local.conf": No such file or directory.
ror, Quitting..
baid001:~$ sudo vim /etc/snort/rules/local.rules
baid001:~$ sudo vim/etc/snort/rules/local.rules
m/etc/snort/rules/local.rules: command not found
baid001:~$ sudo vim /etc/snort/rules/local.rules
baid001:~$ sudo vim /etc/snort/rules/local.rules
baid001:~$ sudo snort -A console -q -u snort -g snort -c /etc/snort/snort.local.conf -i enp0s3
/etc/snort/snort.local.conf(0) Unable to open rules file "/etc/snort/snort.local.conf": No such file or directory.
ror, Quitting..
baid001:~$ ls /etc/snort/
e_table.dtd file_magic.conf rules threshold.conf
cation.config gen-msg.map snort.conf unicode.map
y-sid-msg.map reference.config snort.debian.conf
baid001:~$ e/etc/snort/snort.conf
/etc/snort/snort.conf: No such file or directory
baid001:~$ sudo cp /etc/snort/snort.conf /etc/snort/snort.local.conf
baid001:~$ sudo snort -A console -q -u snort -g snort -c /etc/snort/snort.local.conf -i enp0s3
4:14:16.260440 [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68
255.255.255:67
4:14:19.322373 [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68
255.255.255:67
4:14:37.377873 [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68
255.255.255:67
4:14:37.522114 [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68
255.255.255:67
4:14:38.681903 [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68
255.255.255:67
4:29:16.729254 [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {IPV6-ICMP} :: -
1:ffd7:f5b7
4:29:16.729699 [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {IPV6-ICMP} :: -
1:ff1c:3800