**ASSIGNMENT NO. 4**

**TITLE:** Configure and demonstrate Snort tool for intrusion.

**AIM:** Configure and demonstrate use of vulnerability assessment tools such as Snort tool for intrusion or SSL Web security.

**OBJECTIVE:** Study any vulnerability assessment tool such as Snort tool and use its implementation features.

**THEORY:**

**Introduction**

Snort is a popular choice for running a network intrusion detection system or NIDS for short. It monitors the package data sent and received through a specific network interface.

NIDS can catch threats targeting your system vulnerabilities using signature-based detection and protocol analysis technologies. NIDS software, when installed and configured appropriately, can identify the latest attacks, malware infections, compromised systems, and network policy violations.

**Platforms on which Snort runs**

Snort runs on most UNIX and various windows.

* UNIX
* Applet, MAC, BEOS, JBM, AIX, BSD open etc.
* LINUX
* Mandrake LINUX, Red Hat, SUSE LINUX etc.
* WINDOWS
* Windows server 2003/XP/2000/NT

**What can I do with Snort?**

Snort has three primary uses:

* It can be used as a straight packet sniffer like tcpdump.
* A packet logger (useful for network traffic debugging, etc).
* As a full-blown network intrusion prevention system.

**Installation**

1. Install dependencies

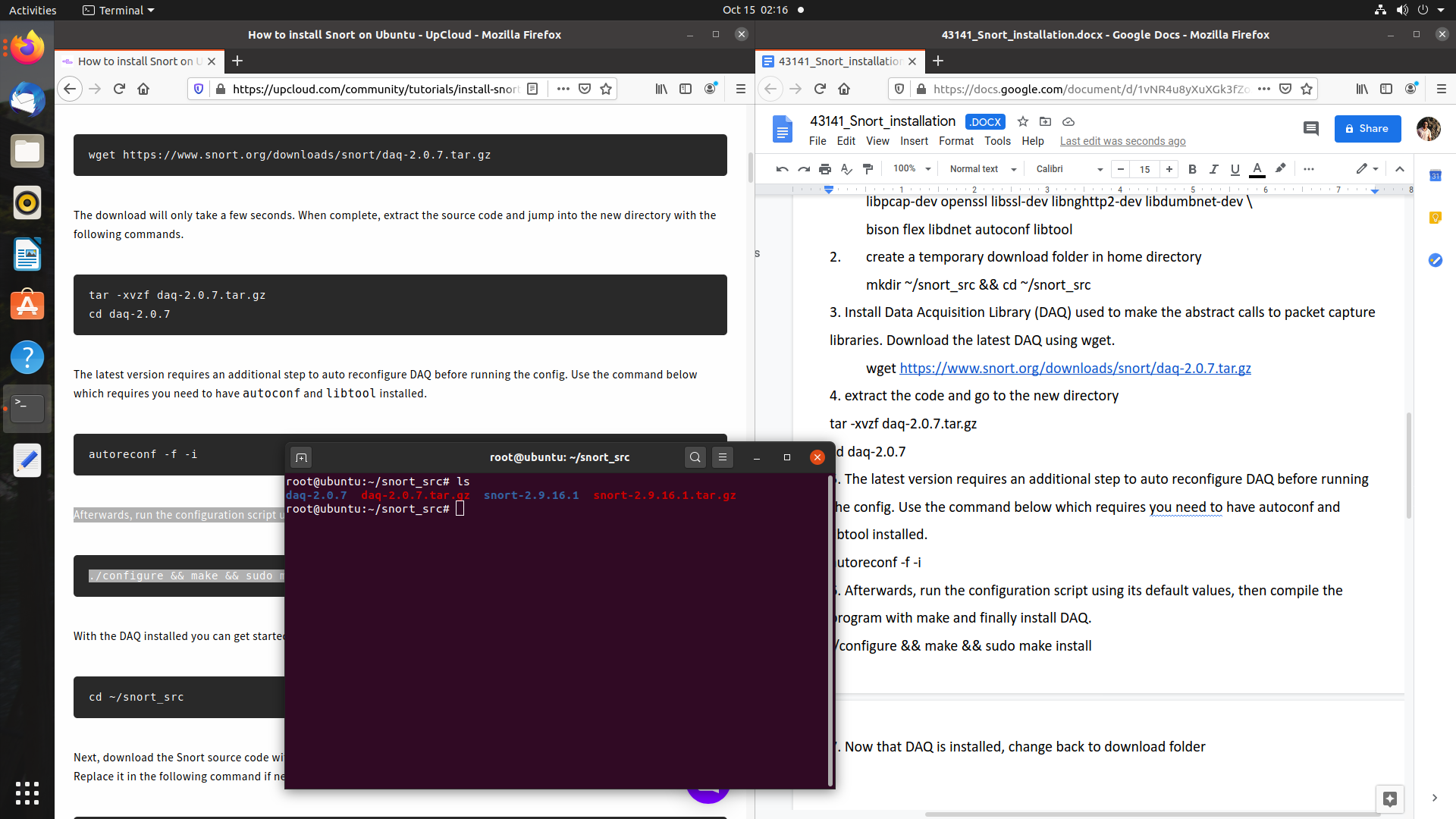
sudo apt install -y gcc libpcre3-dev zlib1g-dev libluajit-5.1-dev \

libpcap-dev openssl libssl-dev libnghttp2-dev libdumbnet-dev \

bison flex libdnet autoconf libtool

1. create a temporary download folder in home directory

mkdir ~/snort\_src && cd ~/snort\_src



1. Install Data Acquisition Library (DAQ) used to make the abstract calls to packet capture libraries. Download the latest DAQ using wget.

wget https://www.snort.org/downloads/snort/daq-2.0.7.tar.gz

1. Extract the code and go to the new directory

tar -xvzf daq-2.0.7.tar.gz

cd daq-2.0.7

1. The latest version requires an additional step to auto reconfigure DAQ before running the config. Use the command below which requires you need to have autoconf and libtool installed.

autoreconf -f -i

1. Afterwards, run the configuration script using its default values, then compile the program with make and finally install DAQ.

./configure && make && sudo make install

1. Now that DAQ is installed, change back to download folder
2. Next, download the Snort source code with wget.

Wget https://www.snort.org/downloads/snort/snort-2.9.16.1.tar.gz

1. Once the download is complete, extract the source and change into the new directory with these commands.

tar -xvzf snort-2.9.16.tar.gz

cd snort-2.9.16

1. Then configure the installation with sourcefire enabled, run make and make install

./configure --enable-sourcefire && make && sudo make install

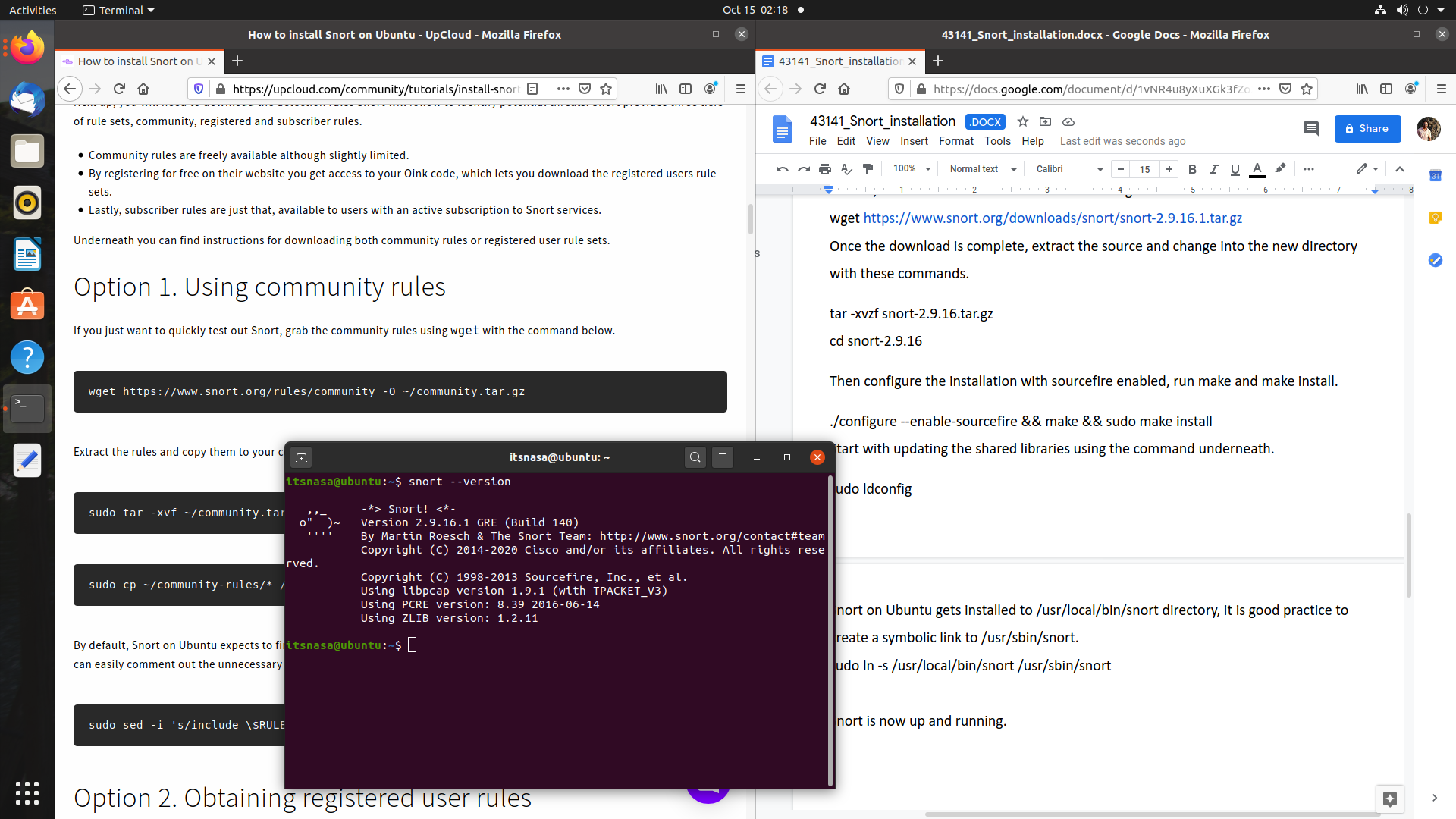
1. Start with updating the shared libraries using the command underneath.

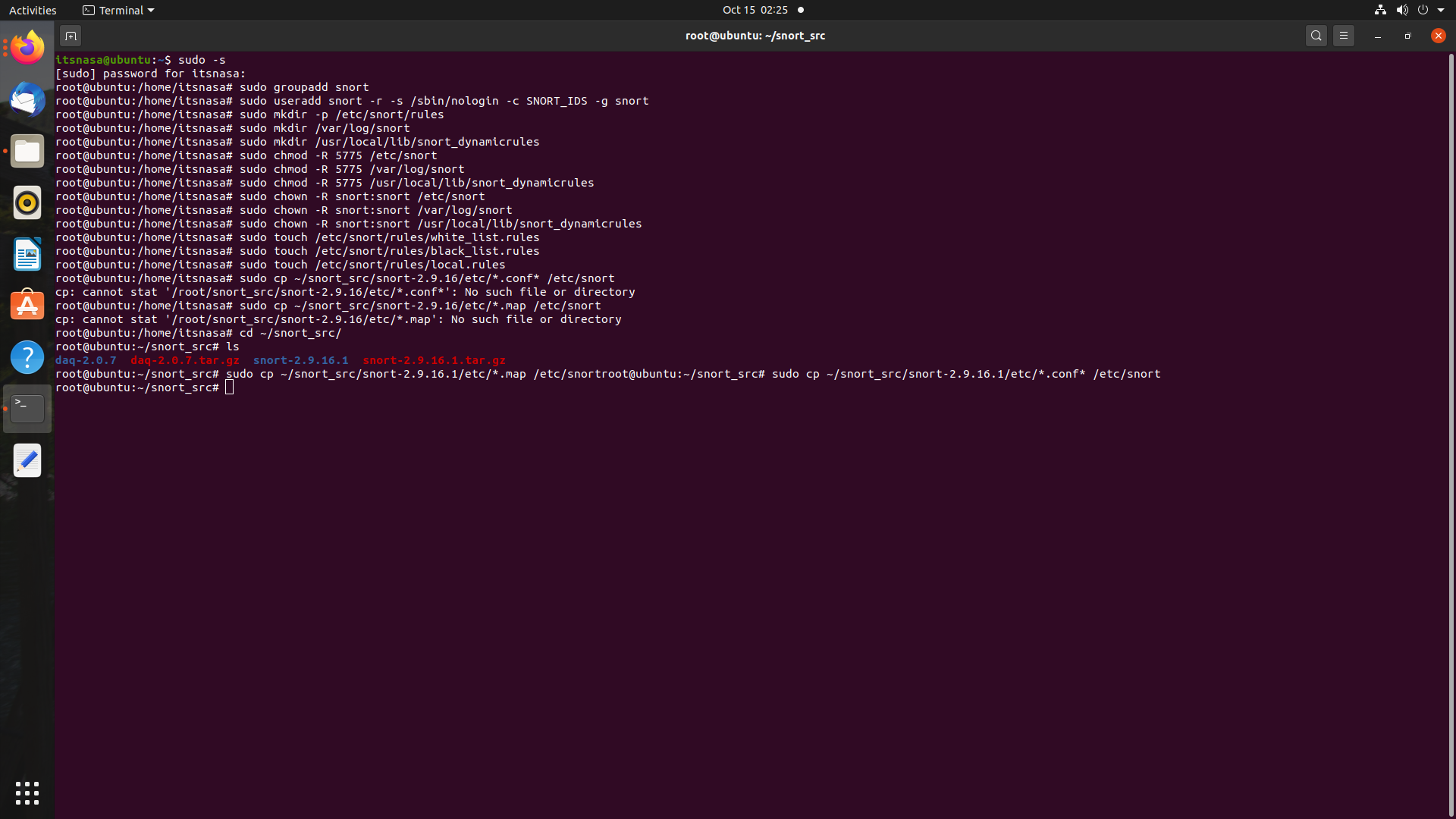
sudo ldconfig

1. Snort on Ubuntu gets installed to /usr/local/bin/snort directory, it is good practice to create a symbolic link to /usr/sbin/snort.

sudo ln -s /usr/local/bin/snort /usr/sbin/snort

Snort is now up and running.





**Setting rules for Snort**

1. Grab the community rules using wget with the command below.

wget https://www.snort.org/rules/community -O ~/community.tar.gz

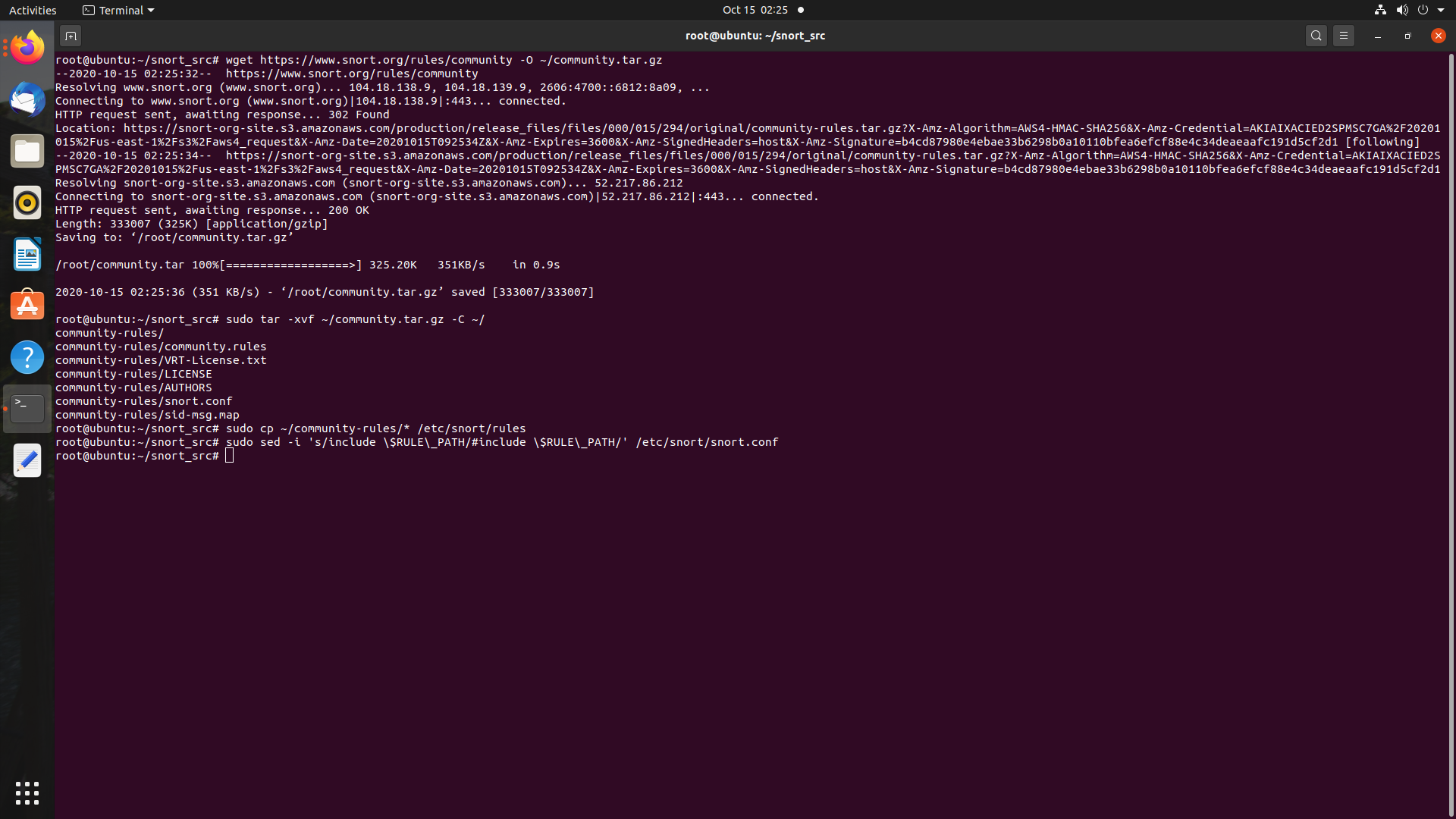
1. Extract the rules and copy them to your configuration folder.

sudo tar -xvf ~/community.tar.gz -C ~/

sudo cp ~/community-rules/\* /etc/snort/rules

1. By default, Snort on Ubuntu expects to find a number of different rule files which are not included in the community rules. You can easily comment out the unnecessary lines using the sed command underneath.

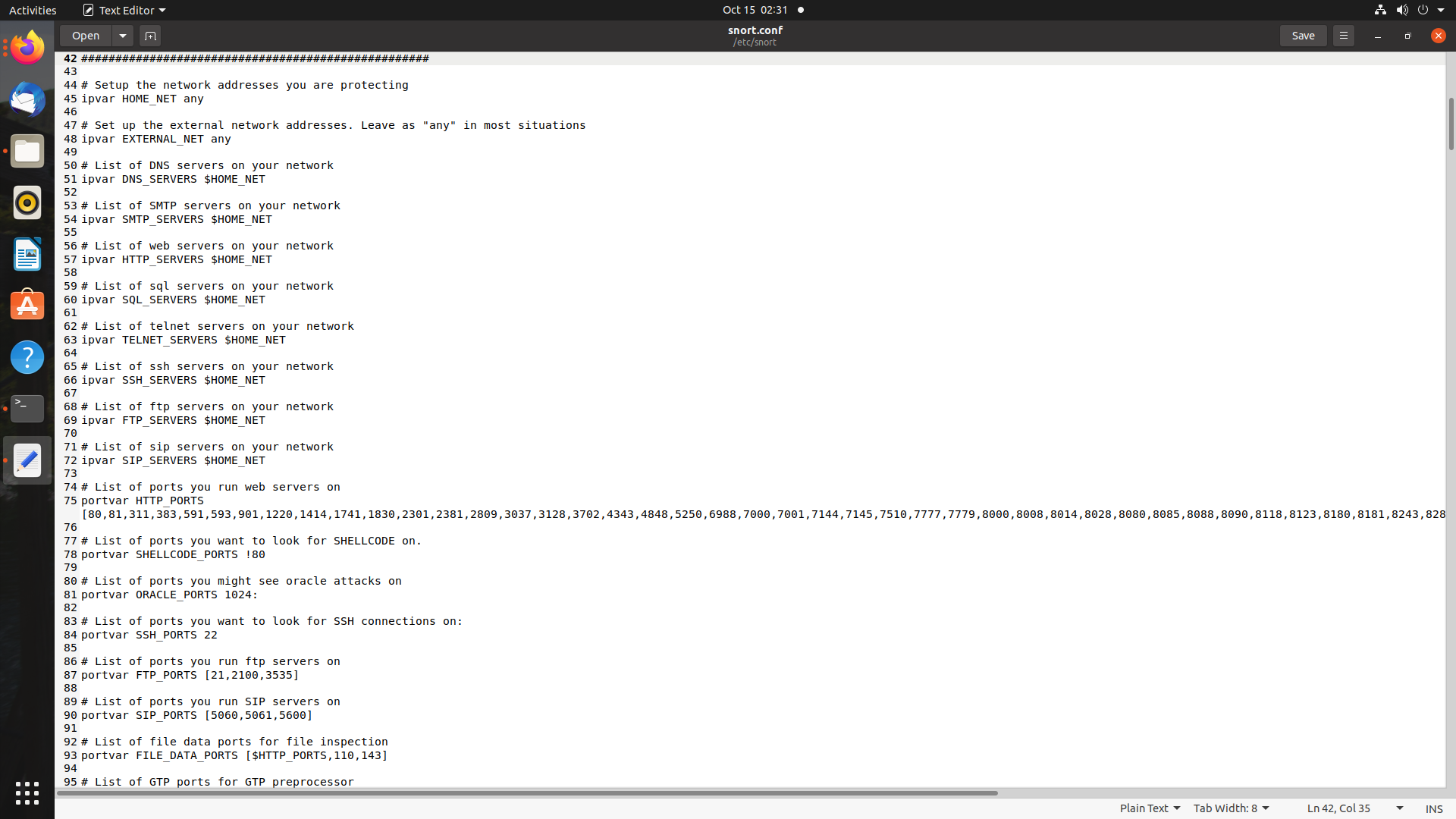
sudo sed -i 's/include \$RULE\\_PATH/#include \$RULE\\_PATH/' /etc/snort/snort.conf



## With the configuration and rule files in place, edit the snort.conf to modify a few parameters.

## Open the configuration file in your favourite text editor, for example using Gedit with the command below

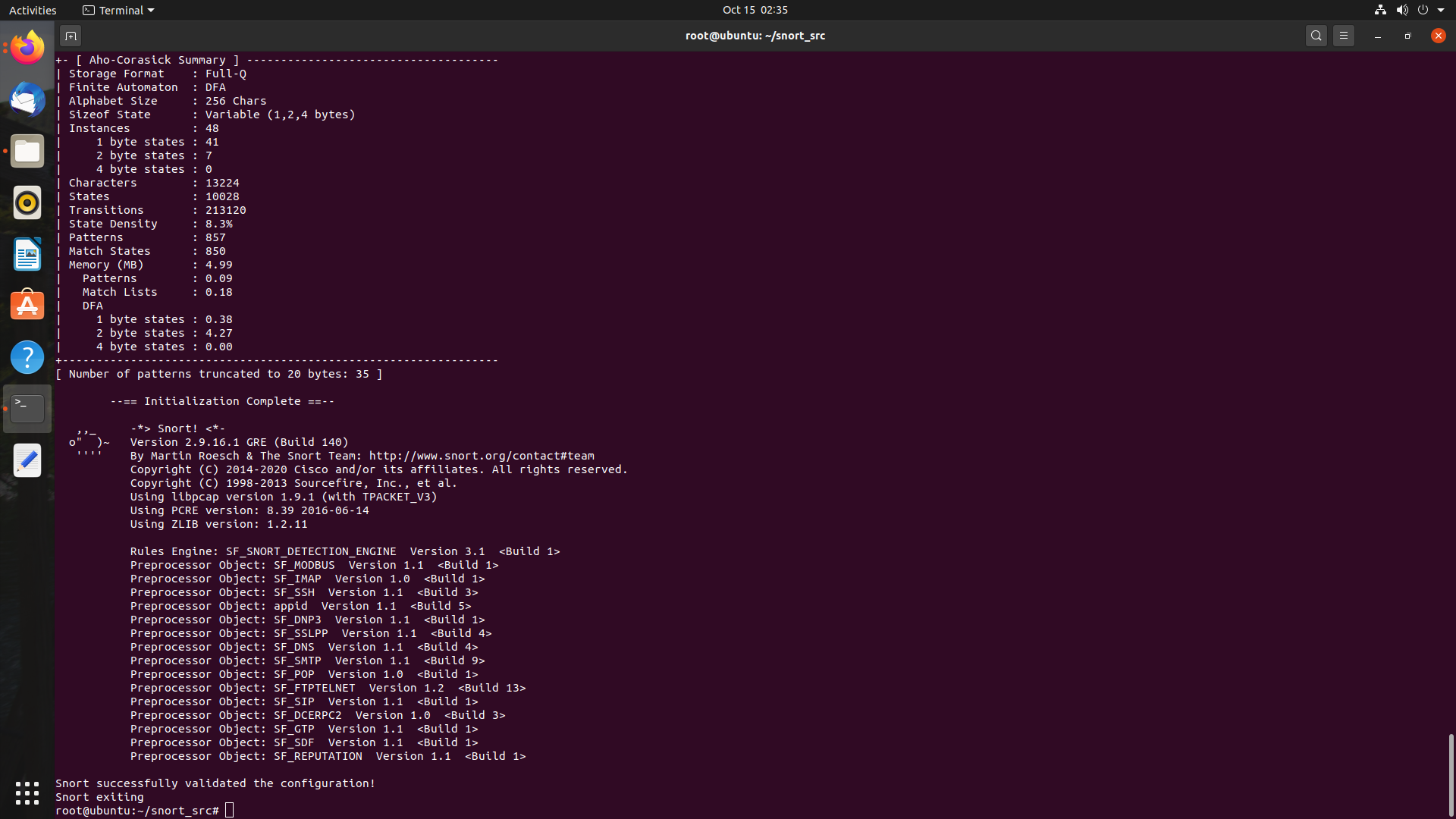
sudo gedit /etc/snort/snort.conf



Edit your path files.

Your Snort should now be ready to run. Test the configuration using the parameter -T to enable test mode.

sudo snort -T -c /etc/snort/snort.conf



## 

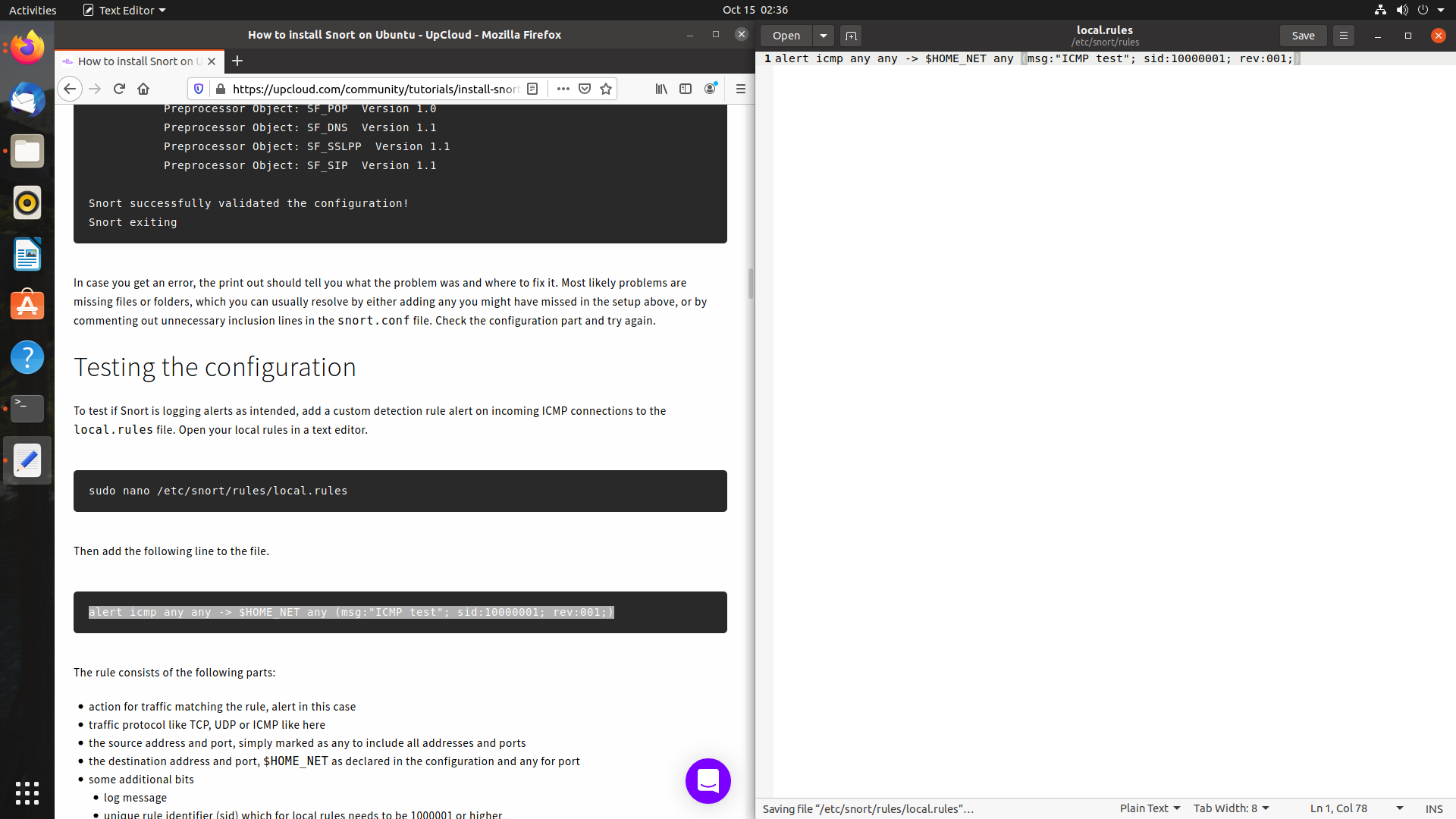
## Testing the configuration

To test if Snort is logging alerts as intended, add a custom detection rule alert on incoming ICMP connections to the local.rules file. Open your local rules in a text editor.

sudo nano /etc/snort/rules/local.rules

Then add the following line to the file.

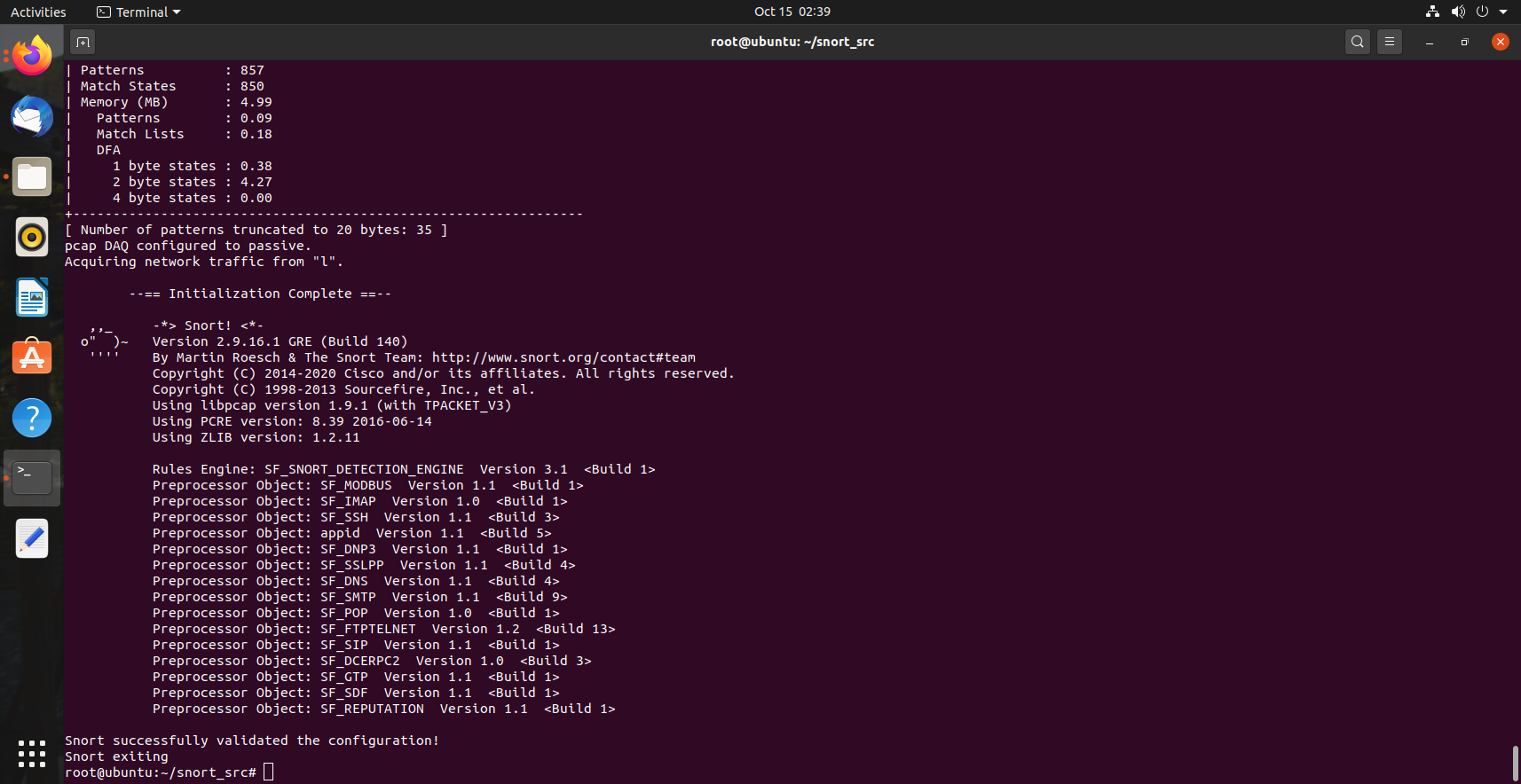
alert icmp any any -> $HOME\_NET any (msg:"ICMP test"; sid:10000001; rev:001;)



Save the local.rules and exit the editor.

Start Snort with -A console options to print the alerts to stdout. You will need to select the correct network interface with the public IP address of your server, for example, eth0.

sudo snort -A console -i eth0 -u snort -g snort -c /etc/snort/snort.conf



Check the file after some time.



It is successfully working.

**CONCLUSION**:

Thus, installation and implementation of snort is completed in this assignment.