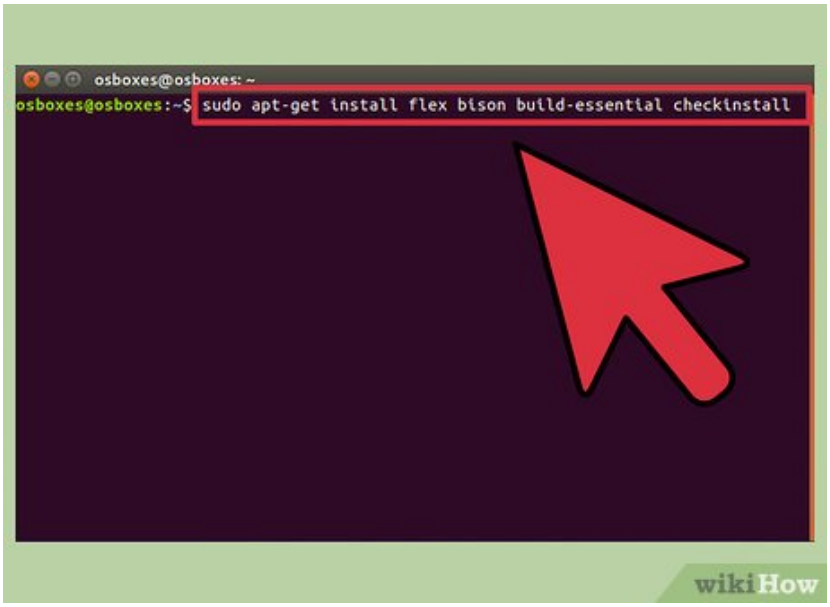
How to Set Up an Independent IDS/IPS Lab Enviroment (Using Snort, Pytbull, Eclipse and Tomcat)

This page is meant to help new software developers to set up an independent lab environment to run the IDS/IPS Snort as well as the testing framework Pytbull. Advanced users can also install Eclipse and Apache Tomcat, so as to be able to...

Part 1 of 5:

Prerequisites To Compiling Snort

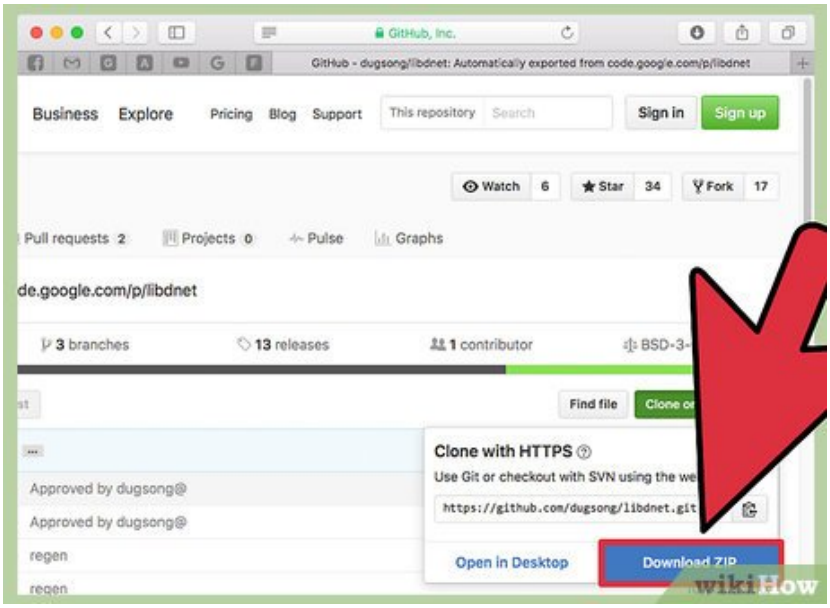
1. 

Install the required packets using:

1. Sudo apt-get install flex bison build-essential checkinstall
2. Sudo apt-get install libpcap-dev libnet1-dev libpcre3-dev
3. Sudo apt-get install libmysqlclient15-dev libnetfilter-queue-dev iptables-dev

Part 2 of 5:

Install Libdnet

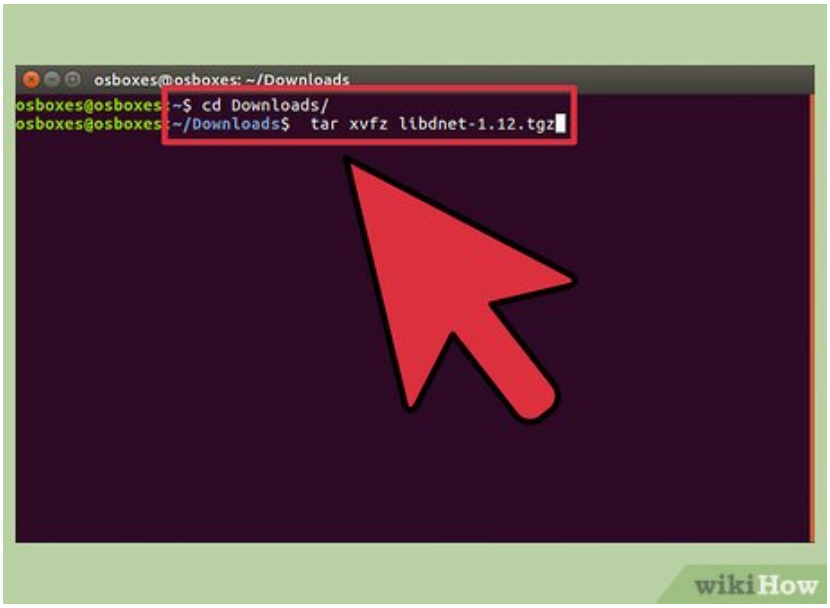
1. 

Download libdnet-1.12.tgz. Download from: https://code.google.com/p/libdnet/downloads/detail?name=libdnet-1.12.tgz&can=2&q=. Alternatively, you can search for it online.

2. 

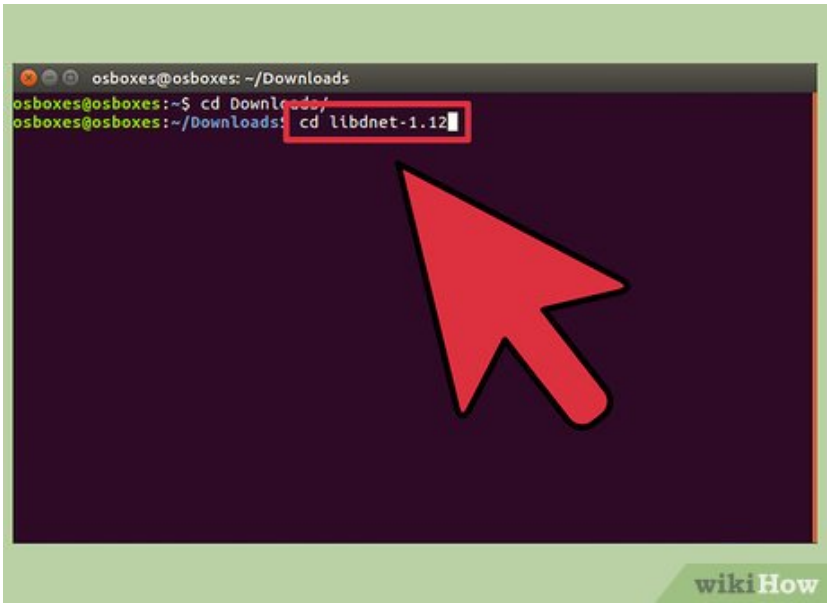
Switch to the directory where the file was saved (this should be Downloads):

1. cd Downloads

3. 

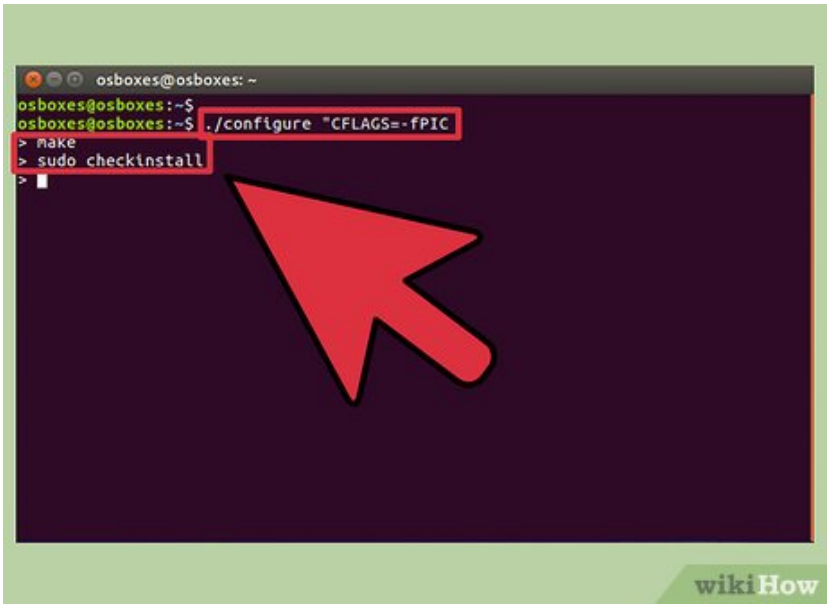
Untar the file

1. tar xvfz libdnet-1.12.tgz

4. 

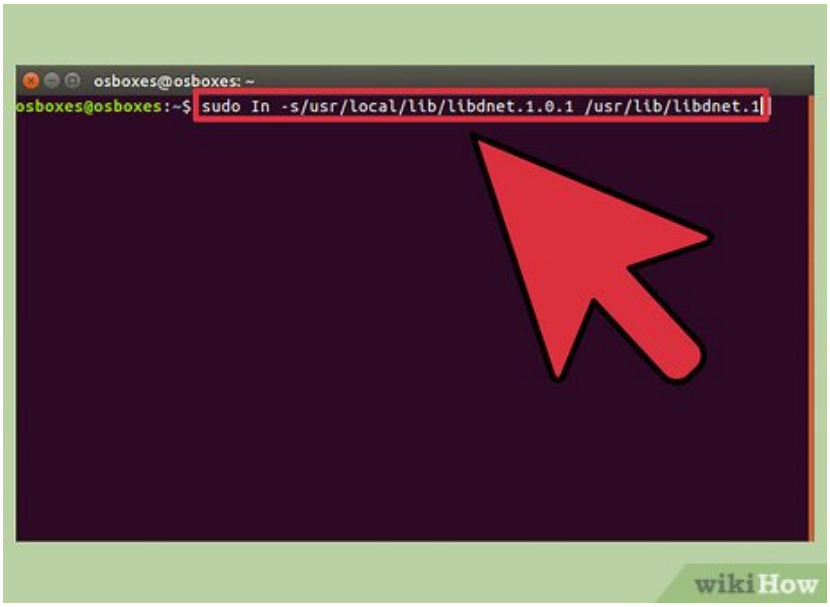
Change into libdnet-1.12 directory:

1. cd libdnet-1.12

5. 

Compile libdnet

1. ./configure "CFLAGS=-fPIC"
2. make
3. sudo checkinstall
    1. Type "y" and Enter when it reads "Should I create a default set of package docs? [y]: "
    2. Then when it reads ">>". Press Enter again
    3. Enter when it reads "Enter a number to change any of them or press ENTER to continue"
    4. Type "n" and Enter when it reads "Do you want me to list them? [n] "
    5. Type "y" and Enter when it reads "Should I exclude them from the package? (Saying yes is a good idea) [n]: "
4. Install the package:
5. sudo dpkg -i libdnet_1.12-1_amd64.deb

6. 

Create the required symbolic link

1. sudo ln -s /usr/local/lib/libdnet.1.0.1 /usr/lib/libdnet.1

Part 3 of 5:

Install DAQ (Data Acquisition Library)

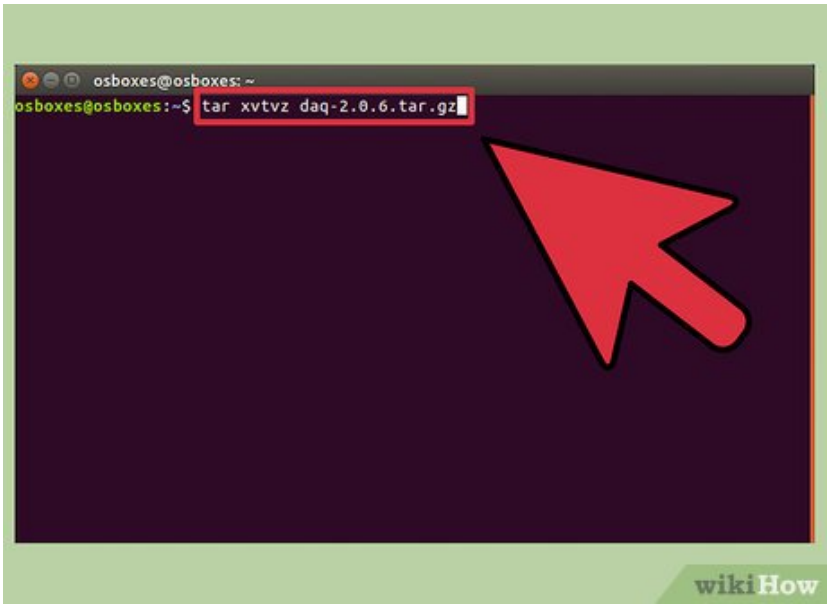
1. 

Download daq-2.0.4.tar.gz. Download it from: https://www.snort.org/downloads, or the https://www.snort.org, or search online for it.

2. 

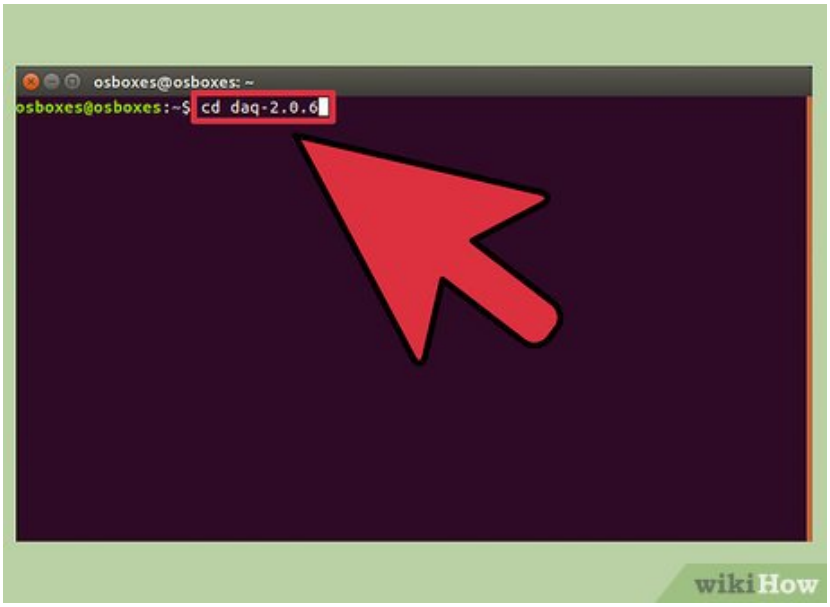
Switch to the directory where the file was saved (this should be Downloads):

1. If still inside libdnet-1.12 then type
    1. cd ..
2. If in main directory then type
    1. cd Downloads

3. 

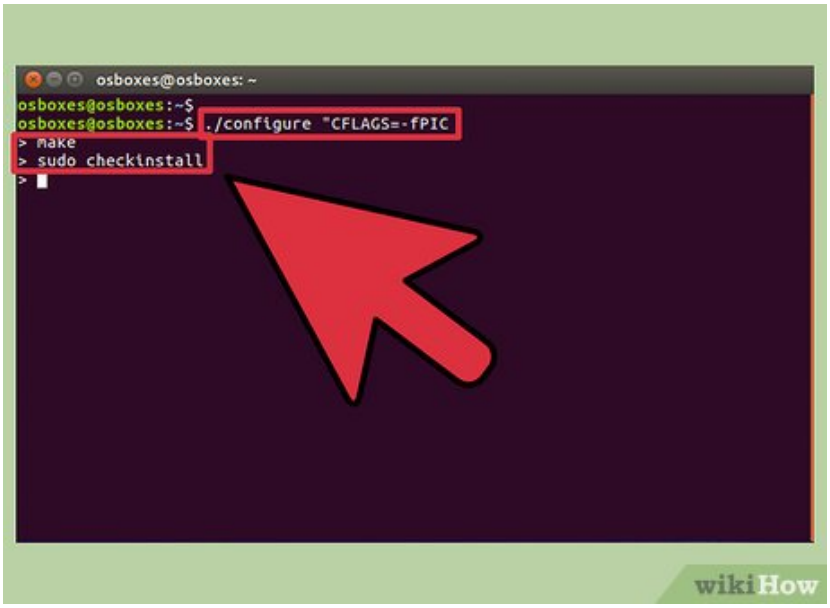
Untar the file:

1. tar xvfvz daq-2.0.4.tar.gz

4. 

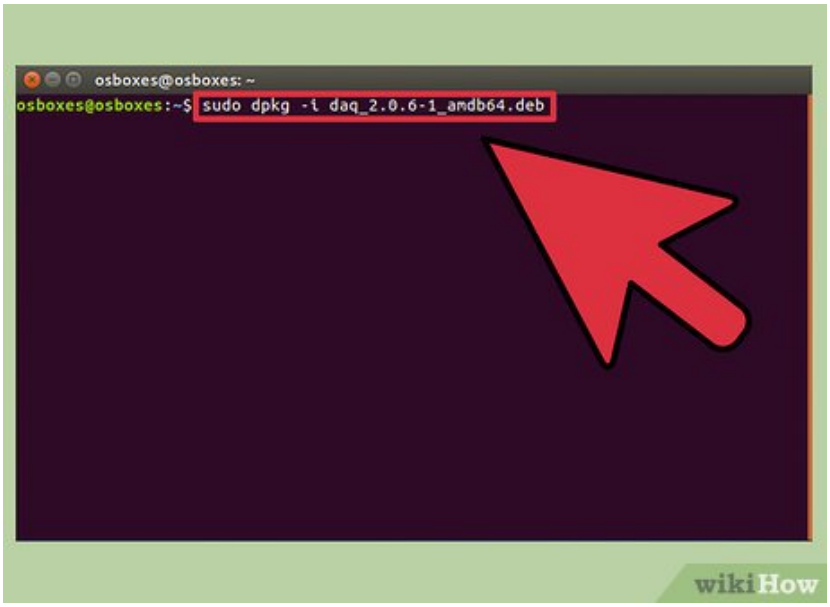
Change into daq-2.0.4 directory:

1. cd daq-2.0.4

5. 

Compile daq (Similar to how we compiled libdnet):

1. ./configure
2. make
3. sudo checkinstall
    1. Type "y" and Enter when it reads "Should I create a default set of package docs? [y]: "
    2. Then when it reads ">>". Press Enter again
    3. Enter when it reads "Enter a number to change any of them or press ENTER to continue"
    4. Type "n" and Enter when it reads "Do you want me to list them? [n] "
    5. Type "y" and Enter when it reads "Should I exclude them from the package? (Saying yes is a good idea) [n]: "

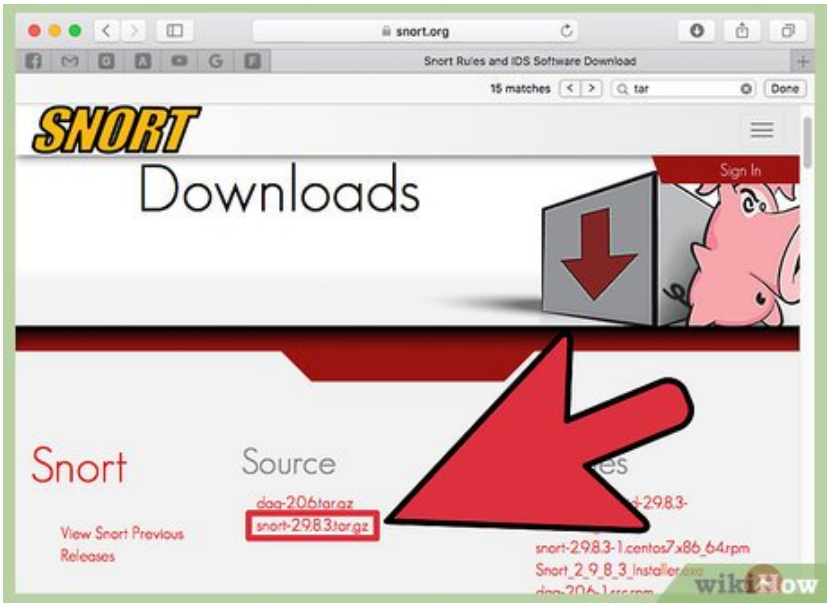
6. 

Install the package:

1. sudo dpkg -i daq_2.0.4-1_amd64.deb

Part 4 of 5:

Install and Configure Snort

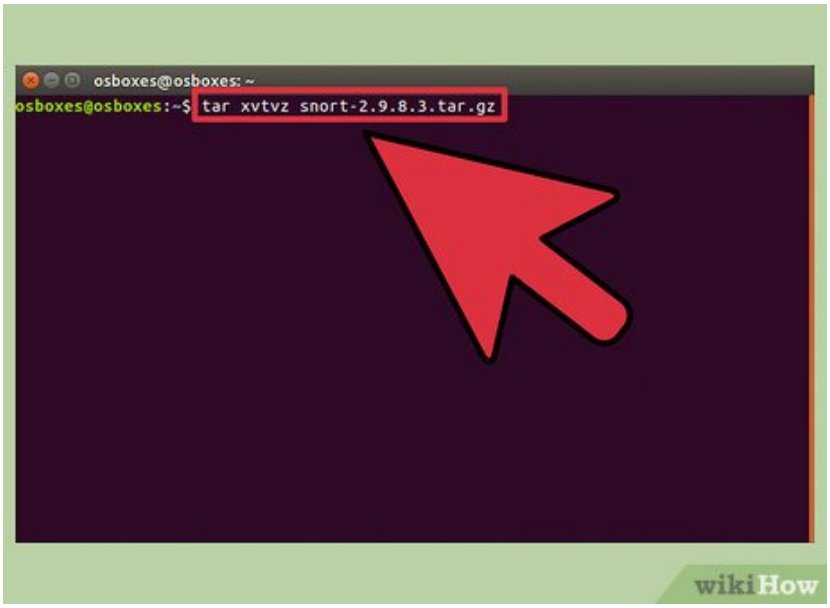
1. 

Download snort-2.9.7.0.tar.gz. Download it from https://www.snort.org/downloads or the https://www.snort.org or search for it online.

2. 

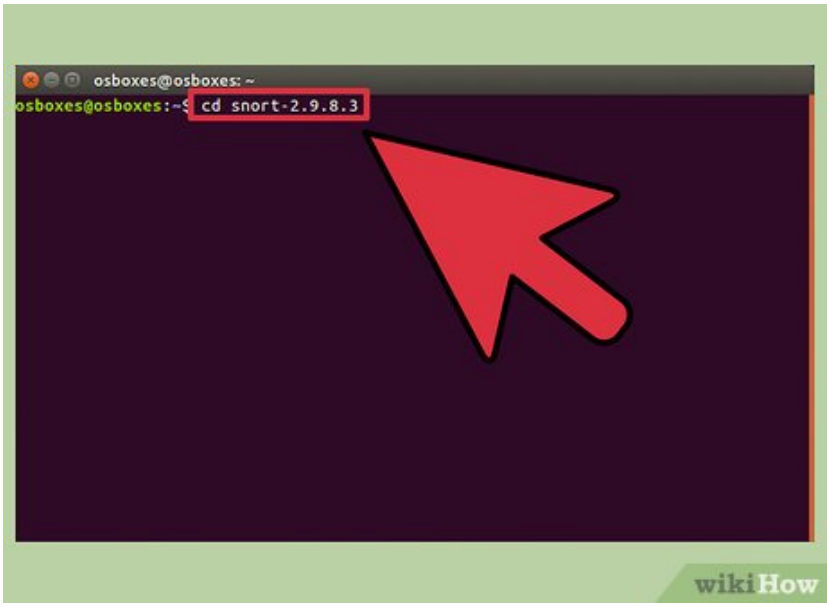
Switch to the directory where the file was saved (should be Downloads):

1. If still inside libdnet-1.12 or daq.2.0.4, then type
    1. cd ..
2. If in main directory then type
    1. cd Downloads

3. 

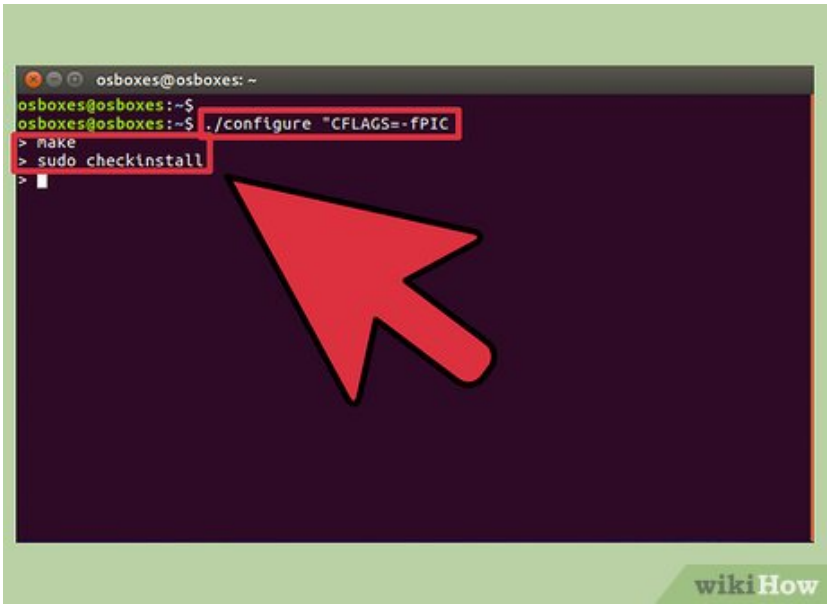
Untar the file:

1. tar xvfvz snort-2.9.7.0.tar.gz

4. 

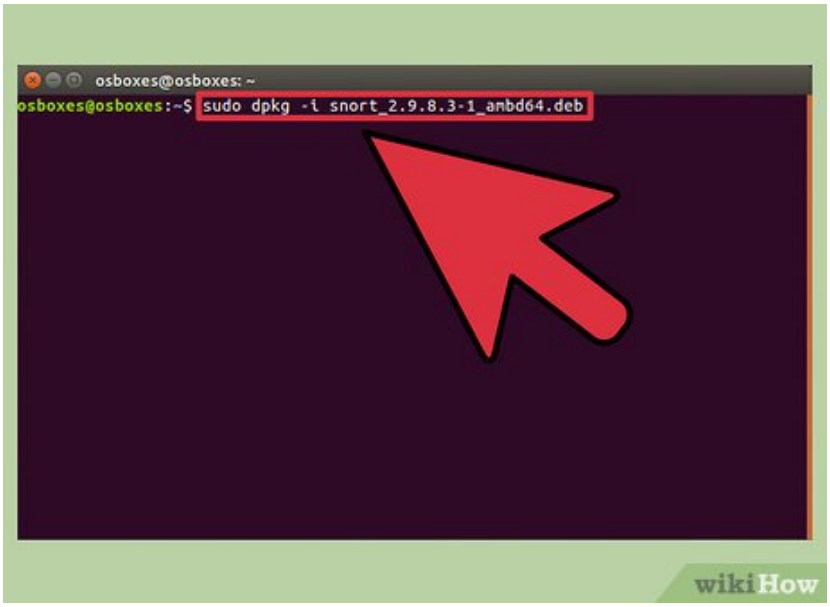
Change into snort-2.9.7.0 directory:

1. cd snort-2.9.7.0

5. 

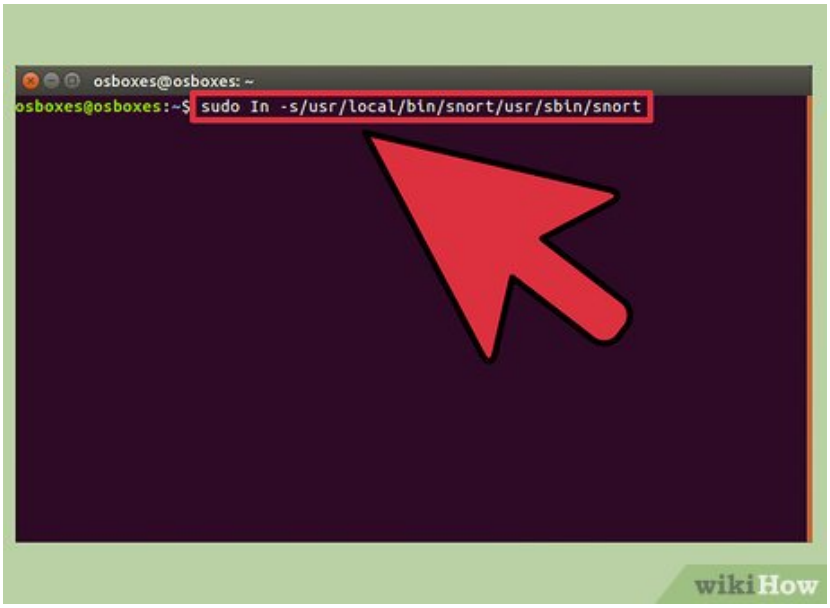
Compile snort (Similar to how we compiled libdnet and daw):

1. ./configure
2. make
3. sudo checkinstall
    1. Type "y" and Enter when it reads "Should I create a default set of package docs? [y]: "
    2. Then when it reads ">>". Press Enter again
    3. Enter when it reads "Enter a number to change any of them or press ENTER to continue"
    4. Type "n" and Enter when it reads "Do you want me to list them? [n] "
    5. Type "y" and Enter when it reads "Should I exclude them from the package? (Saying yes is a good idea) [n]: "

6. 

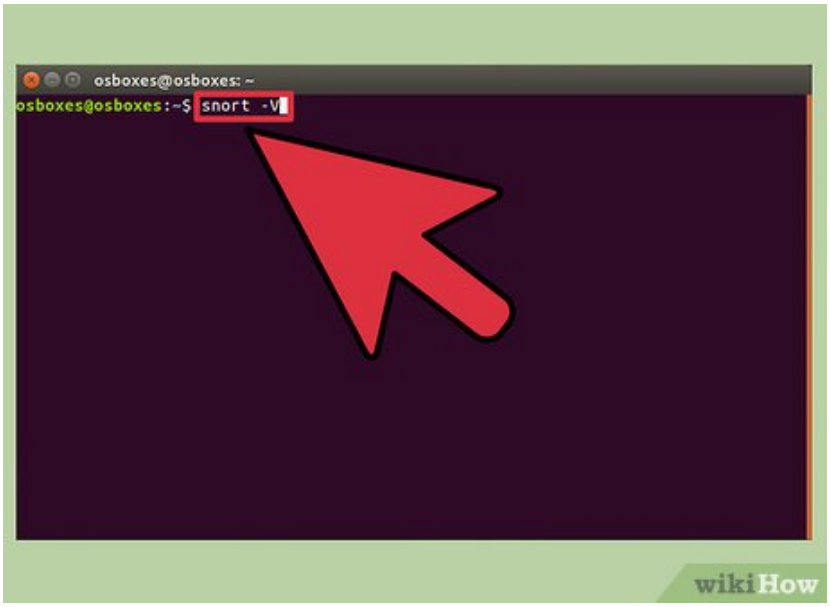
Install the package:

1. sudo dpkg -i snort_2.9.7.0-1_amd64.deb

7. 

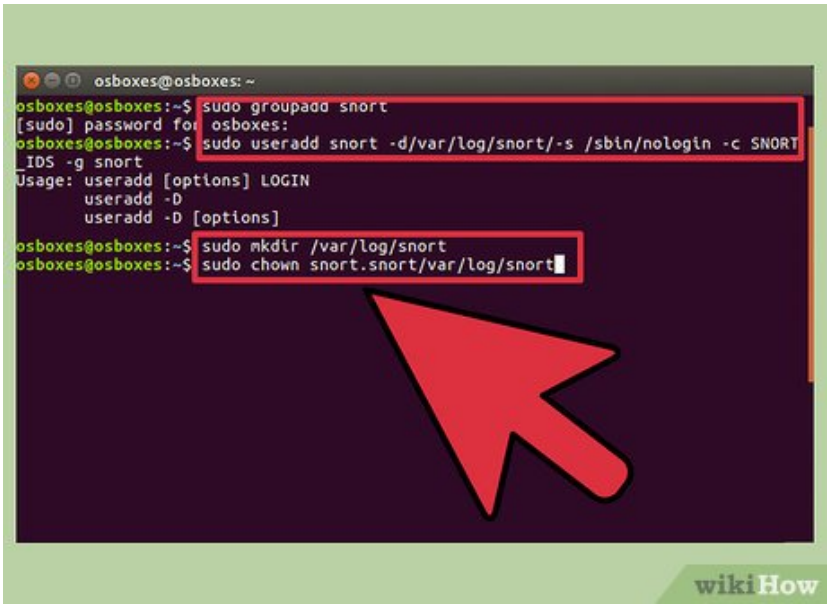
Create the required symbolic link:

1. sudo ln -s /usr/local/bin/snort /usr/sbin/snort
2. sudo ldconfig -v

8. 

Verify the snort version by typing:

1. snort -V

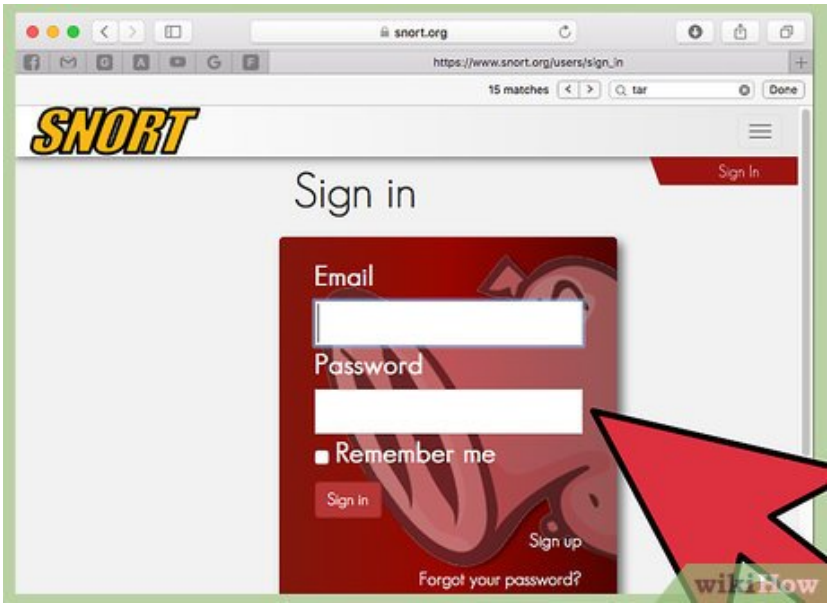
9. 

Make snort an individual user with no login for network security:

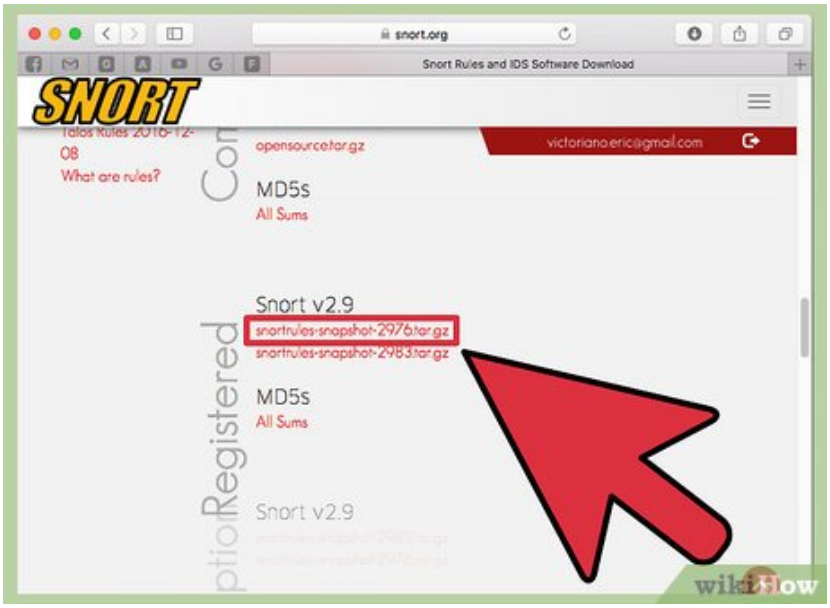
1. sudo groupadd snort
2. sudo useradd snort -d /var/log/snort/ -s /sbin/nologin -c SNORT_IDS -g snort
3. sudo mkdir /var/log/snort
4. sudo chown snort:snort /var/log/snort

Part 5 of 5:

Install and Configure Snort Rules

1. 

In order to download the default snort rule-set, you will have to create a log in at https://www.snort.org.

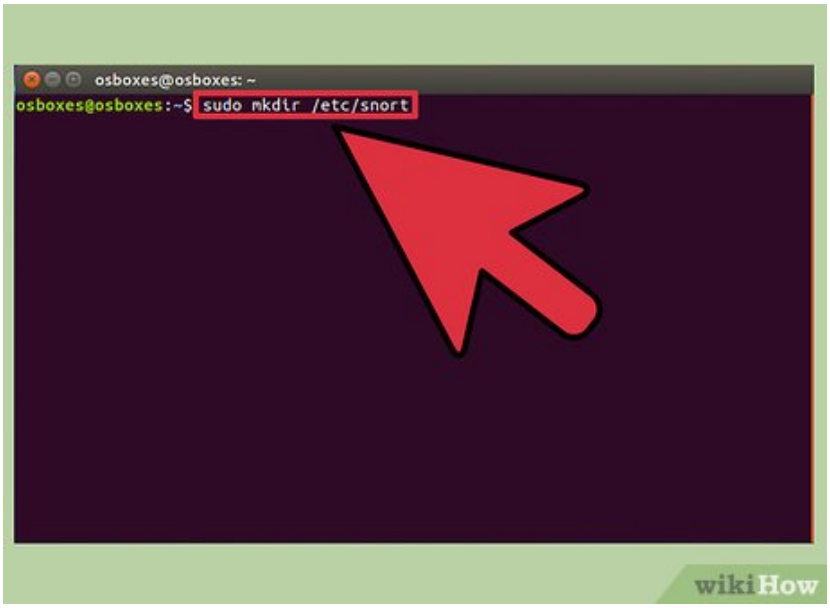
2. 

Download snortrules-snapshot-2970.tar.gz. Download it from https://www.snort.org/downloads or the https://www.snort.org or search online for it.

3. 

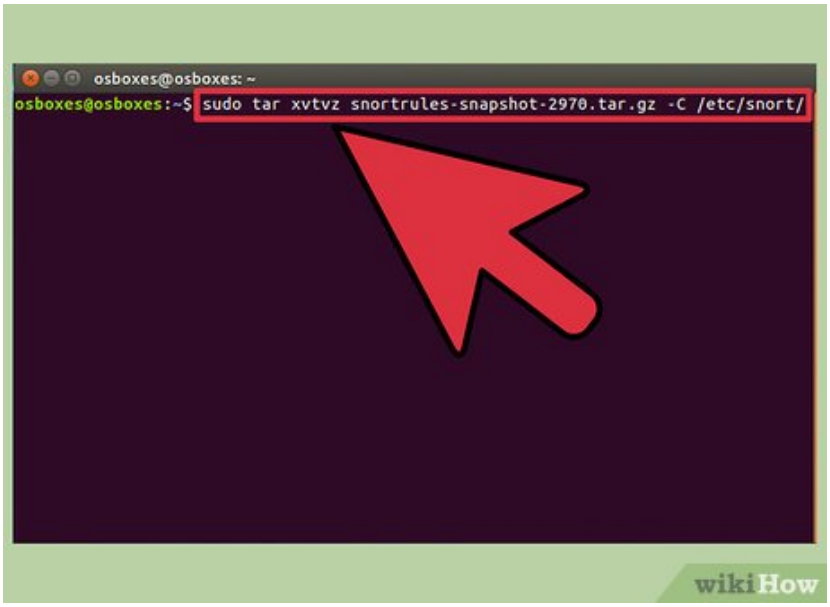
Switch to the directory where the file was saved (should be Downloads):

1. If still inside libdnet-1.12 or daq.2.0.4 or snort-2.9.7.0 then type
    1. cd ..
2. If in main directory then type
    1. cd Downloads

4. 

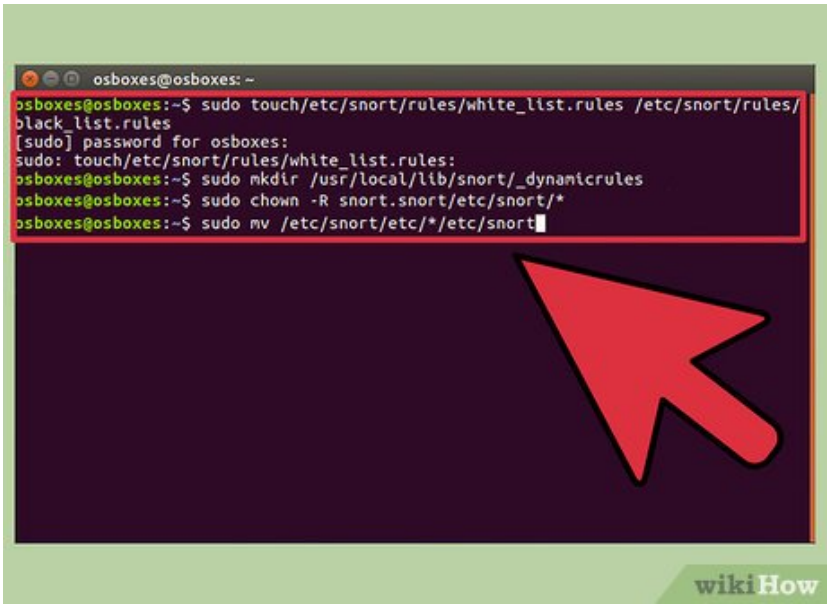
Make a new directory for the rules:

1. sudo mkdir /etc/snort

5. 

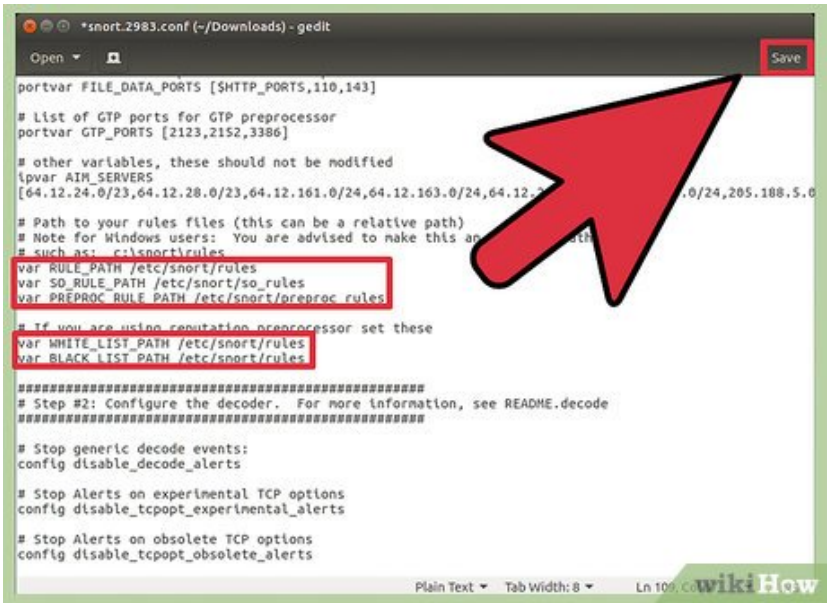
Untar the file

1. sudo tar xvfvz snortrules-snapshot-2970.tar.gz -C /etc/snort/

6. 

Configure the rule-set:

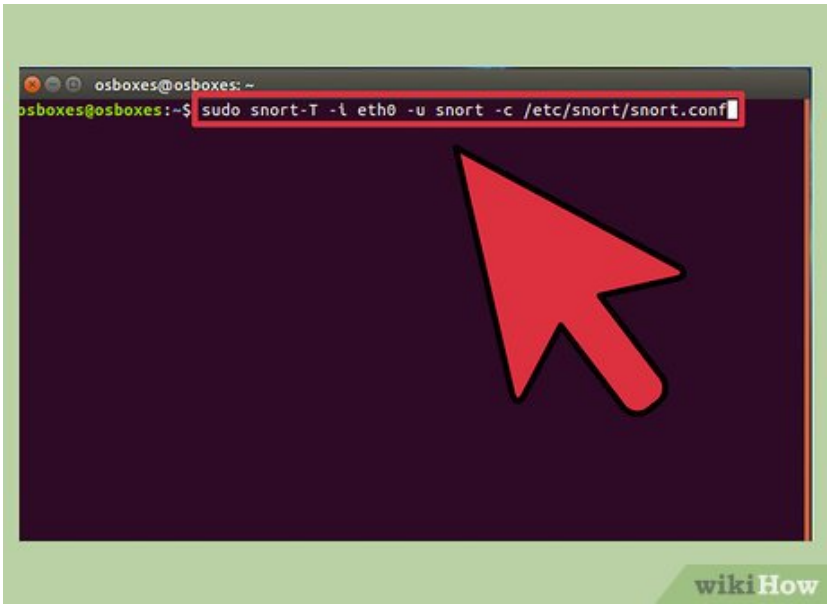
1. sudo touch /etc/snort/rules/white_list.rules /etc/snort/rules/black_list.rules
2. sudo mkdir /usr/local/lib/snort_dynamicrules
3. sudo chown -R snort:snort /etc/snort/*
4. sudo mv /etc/snort/etc/* /etc/snort/

7. 

Update snort config file:

1. Use any editor you are familiar with (vim, emac, gedit, pico) and open /etc/snort/snort.conf with sudo permissions. Eg: sudo vi /etc/snort/snort.conf
    1. Change Line 104 from "var RULE_PATH ../rules" to "var RULE_PATH /etc/snort/rules"
    2. Change Line 105 from "var SO_RULE_PATH ../so_rules" to "var SO_RULE_PATH /etc/snort/so_rules"
    3. Change Line 105 from "var PREPROC_RULE_PATH ../preproc_rules" to "var PREPROC_RULE_PATH /etc/snort/preproc_rules"

4. Change Line 109 from "var WHITE_LIST_PATH ../rules" to "var WHITE_LIST_PATH /etc/snort/rules"
5. Change Line 110 from "var BLACK_LIST_PATH ../rules" to "var BLACK_LIST_PATH /etc/snort/rules"
6. Save and Exit

8. 

Verify that snort is fully functional with the default rule-set listening to all the traffic on the network by running it in test mode.

1. sudo snort -T -i eth0 -u snort -g snort -c /etc/snort/snort.conf