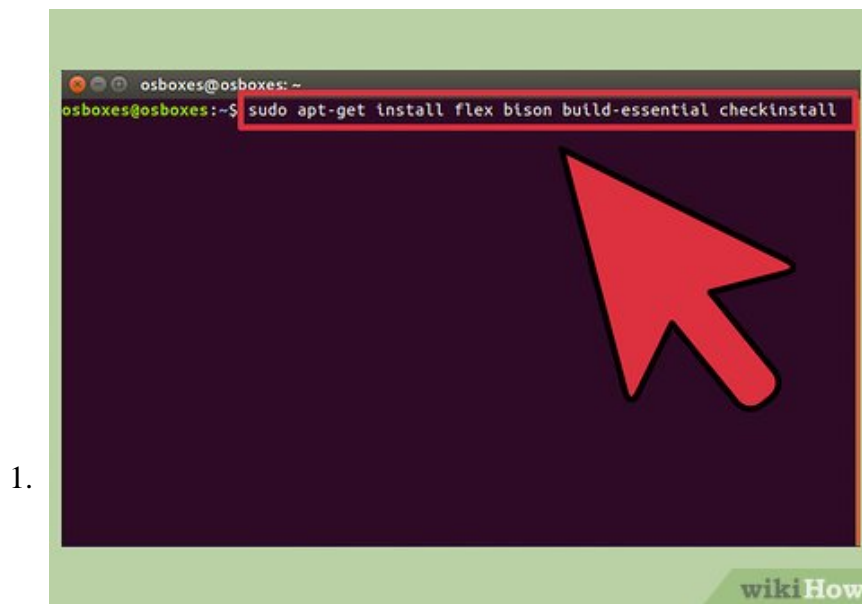


How to Set Up an Independent IDS/IPS Lab Environment (Using Snort, Pytball, Eclipse and Tomcat)

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 Pytball. Advanced users can also install Eclipse and Apache Tomcat, so as to be able to...

Part 1 of 5:

Prerequisites To Compiling Snort



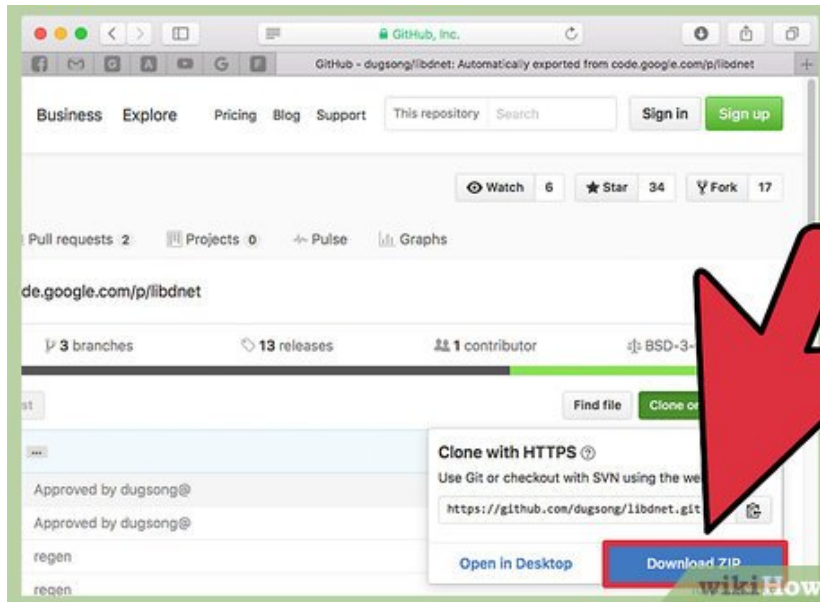
Install the required packets using:

1. Sudo apt-get install flex bison build-essential checkinstall
2. Sudo apt-get install libpcap-dev libnet1-dev libpcrc3-dev
3. Sudo apt-get install libmysqlclient15-dev libnetfilter-queue-dev iptables-dev

Part 2 of 5:

Install Libdnet

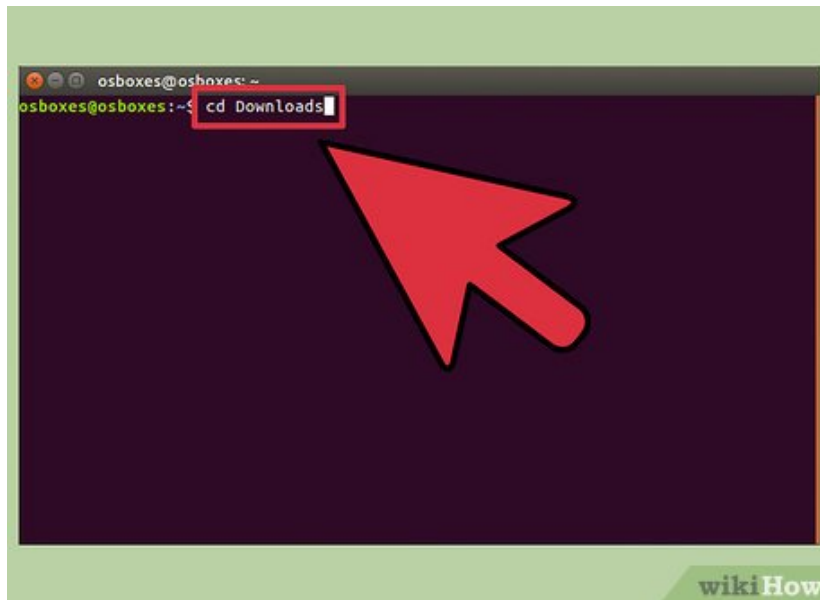
1.



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.

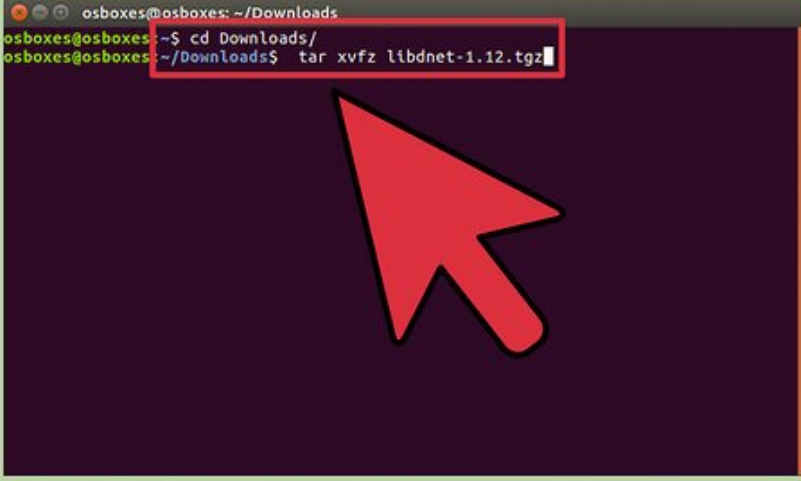
2.



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

1. cd Downloads

3.



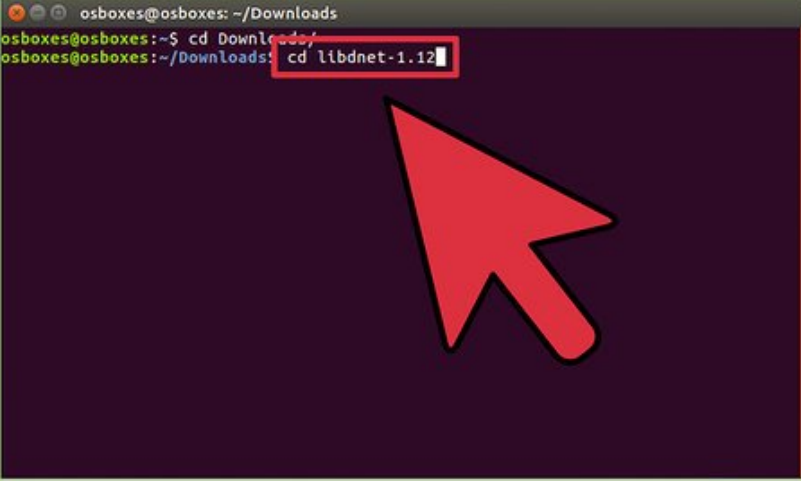
```
osboxes@osboxes: ~/Downloads
osboxes@osboxes:~$ cd Downloads/
osboxes@osboxes:~/Downloads$ tar xvfz libdnet-1.12.tgz
```

A terminal window with a dark purple background and a light green title bar. The title bar contains the text "osboxes@osboxes: ~/Downloads". The terminal shows the command "tar xvfz libdnet-1.12.tgz" being entered. A red mouse cursor points to the command. A red box highlights the command. The "wikiHow" logo is in the bottom right corner.

Untar the file

1. tar xvfz libdnet-1.12.tgz

4.



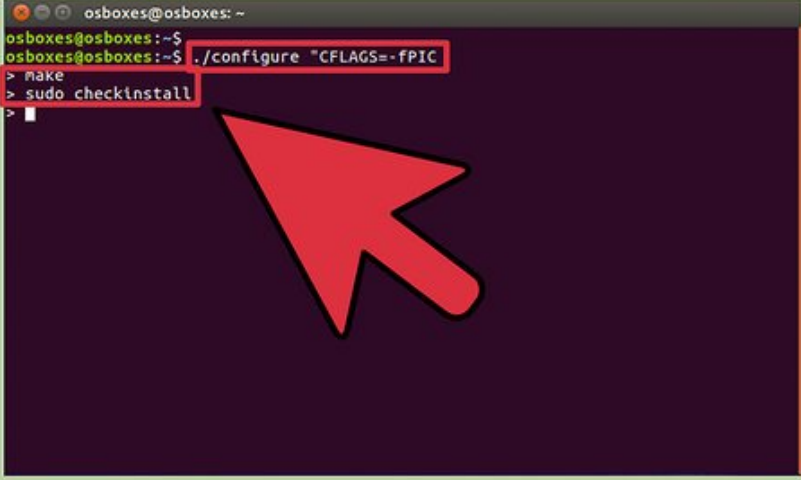
```
osboxes@osboxes: ~/Downloads
osboxes@osboxes:~$ cd Downloads/
osboxes@osboxes:~/Downloads$ cd libdnet-1.12
```

A terminal window with a dark purple background and a light green title bar. The title bar contains the text "osboxes@osboxes: ~/Downloads". The terminal shows the command "cd libdnet-1.12" being entered. A red mouse cursor points to the command. A red box highlights the command. The "wikiHow" logo is in the bottom right corner.

Change into libdnet-1.12 directory:

1. cd libdnet-1.12

5.



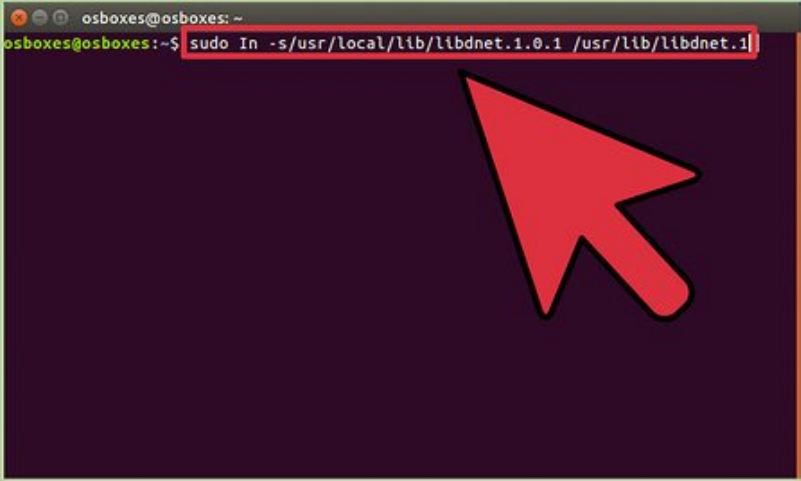
```
osboxes@osboxes: ~  
osboxes@osboxes:~$  
osboxes@osboxes:~$ ./configure "CFLAGS=-fPIC"  
> make  
> sudo checkinstall  
> |
```

A terminal window with a dark purple background. The prompt is `osboxes@osboxes: ~`. The user enters `./configure "CFLAGS=-fPIC"`, `make`, and `sudo checkinstall`. A red mouse cursor points to the `sudo checkinstall` command. The terminal shows a vertical bar after the command, indicating it is running. A "wikiHow" logo is in the bottom right corner.

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.



```
osboxes@osboxes: ~  
osboxes@osboxes:~$ sudo ln -s/usr/local/lib/libdnet.1.0.1 /usr/lib/libdnet.1
```

A terminal window with a dark purple background. The prompt is `osboxes@osboxes: ~`. The user enters `sudo ln -s/usr/local/lib/libdnet.1.0.1 /usr/lib/libdnet.1`. A red mouse cursor points to the command. A "wikiHow" logo is in the bottom right corner.

Create the required symbolic link

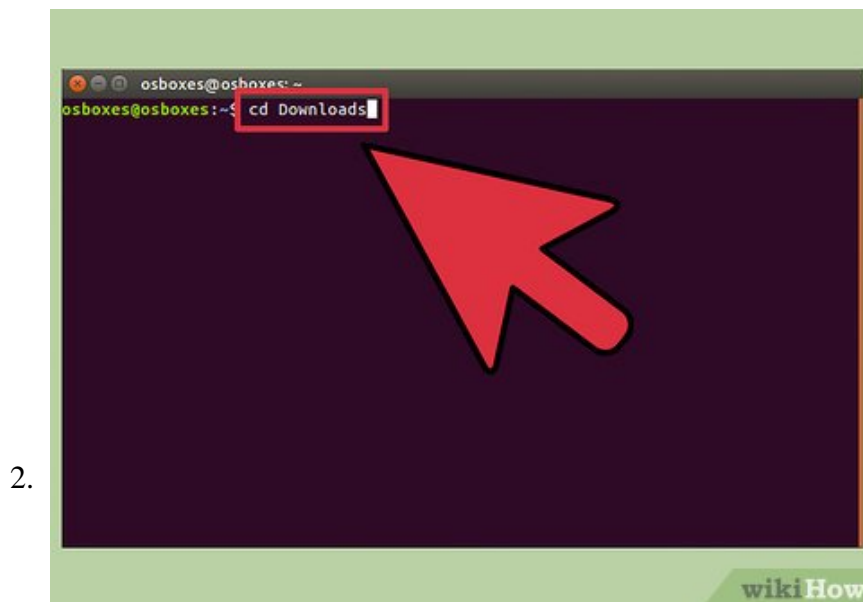
1. `sudo ln -s /usr/local/lib/libdnet.1.0.1 /usr/lib/libdnet.1`

Part 3 of 5:

Install DAQ (Data Acquisition Library)



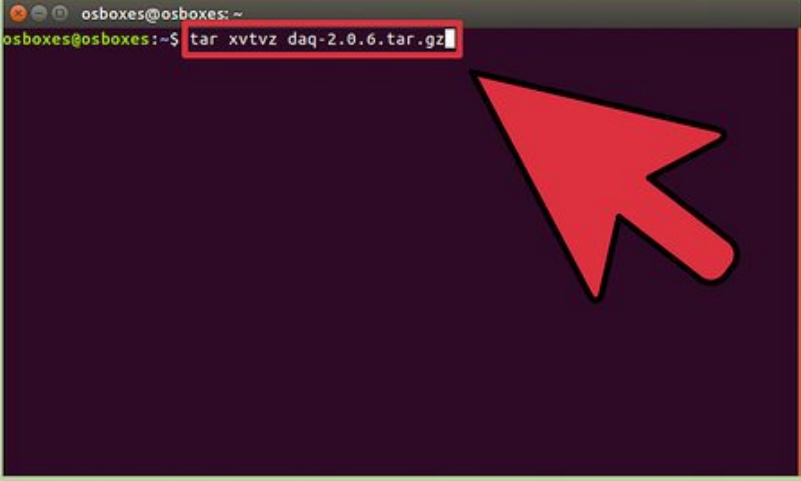
Download daq-2.0.4.tar.gz. Download it from: <https://www.snort.org/downloads>, or the <https://www.snort.org>, or search online for it.



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.



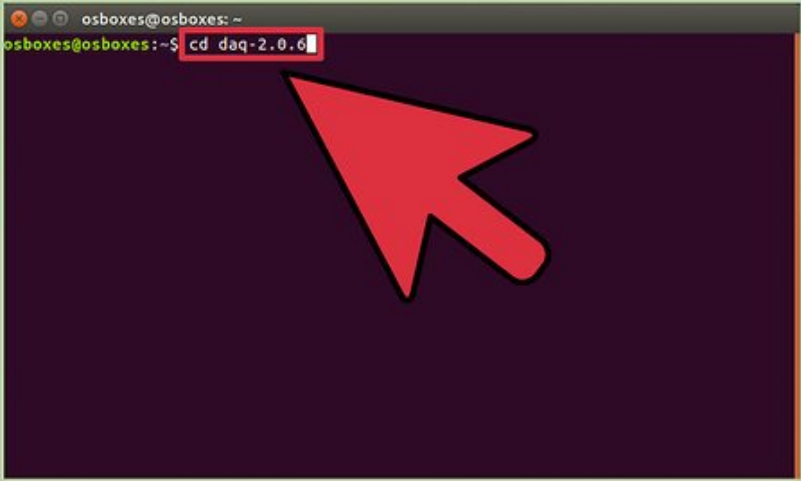
```
osboxes@osboxes: ~  
osboxes@osboxes:~$ tar xvtvz daq-2.0.6.tar.gz
```

A terminal window with a dark purple background and a light green header. The prompt is 'osboxes@osboxes: ~'. The command 'tar xvtvz daq-2.0.6.tar.gz' is entered and highlighted with a red box. A red mouse cursor points to the command. The 'wikiHow' logo is in the bottom right corner.

Untar the file:

1. tar xvfz daq-2.0.4.tar.gz

4.



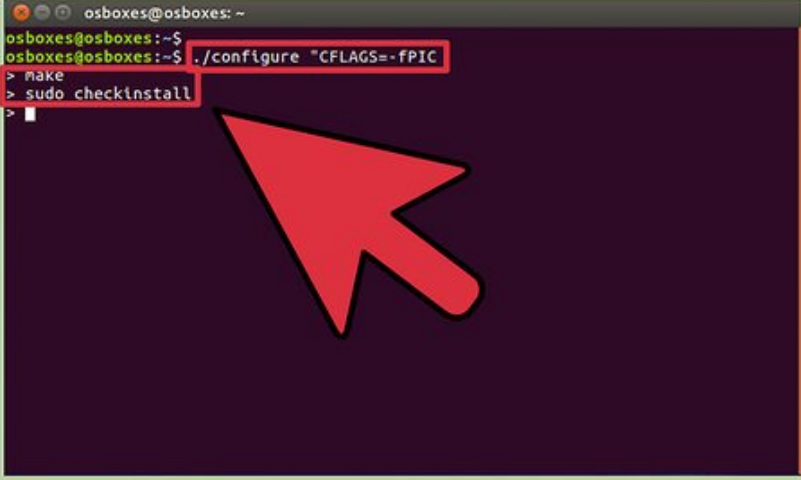
```
osboxes@osboxes: ~  
osboxes@osboxes:~$ cd daq-2.0.6
```

A terminal window with a dark purple background and a light green header. The prompt is 'osboxes@osboxes: ~'. The command 'cd daq-2.0.6' is entered and highlighted with a red box. A red mouse cursor points to the command. The 'wikiHow' logo is in the bottom right corner.

Change into daq-2.0.4 directory:

1. cd daq-2.0.4

5.



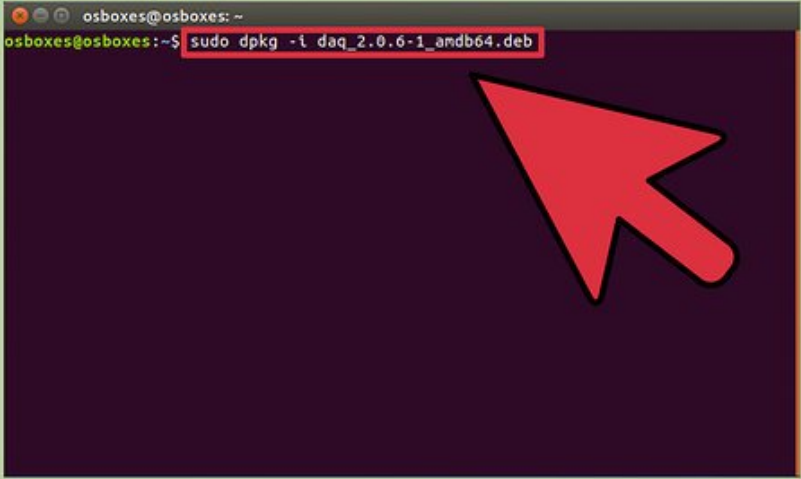
```
osboxes@osboxes: ~  
osboxes@osboxes:~$  
osboxes@osboxes:~$ ./configure "CFLAGS=-fPIC"  
> make  
> sudo checkinstall  
> |
```

A terminal window with a dark purple background. The prompt is 'osboxes@osboxes: ~'. The user has entered the following commands: './configure "CFLAGS=-fPIC"', 'make', and 'sudo checkinstall'. A red mouse cursor points to the 'sudo checkinstall' command. The terminal shows a vertical bar after the command, indicating it is running. A 'wikiHow' logo is in the bottom right corner.

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.



```
osboxes@osboxes: ~  
osboxes@osboxes:~$ sudo dpkg -i daq_2.0.6-1_amd64.deb
```

A terminal window with a dark purple background. The prompt is 'osboxes@osboxes: ~'. The user has entered the command 'sudo dpkg -i daq_2.0.6-1_amd64.deb'. A red mouse cursor points to the command. A 'wikiHow' logo is in the bottom right corner.

Install the package:

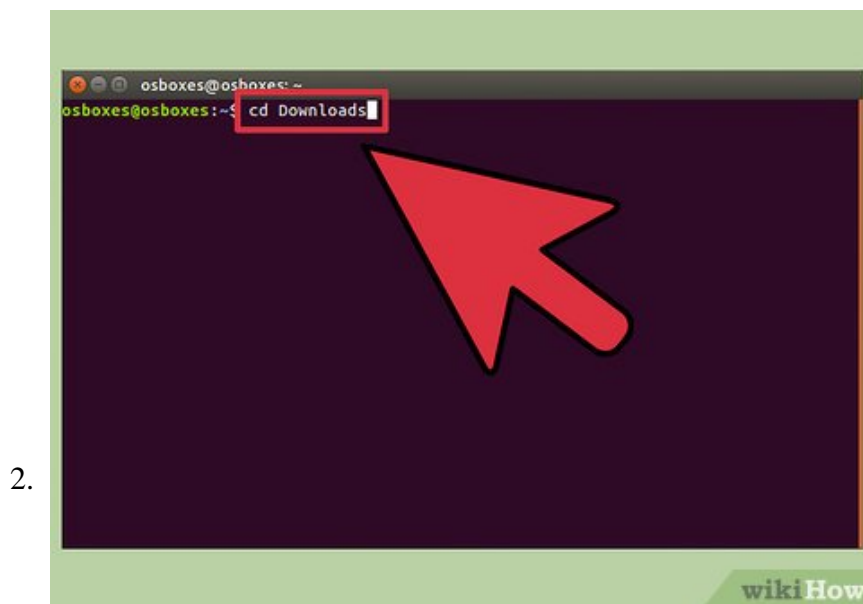
1. sudo dpkg -i daq_2.0.4-1_amd64.deb

Part 4 of 5:

Install and Configure Snort



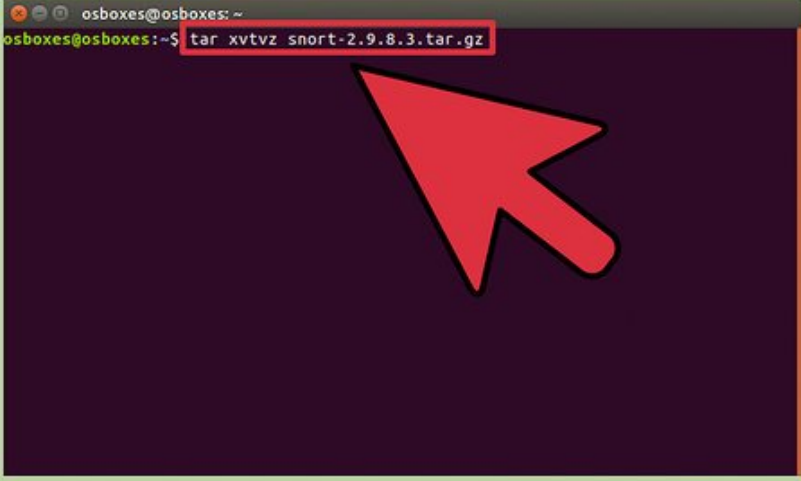
Download snort-2.9.7.0.tar.gz. Download it from <https://www.snort.org/downloads> or the <https://www.snort.org> or search for it online.



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.



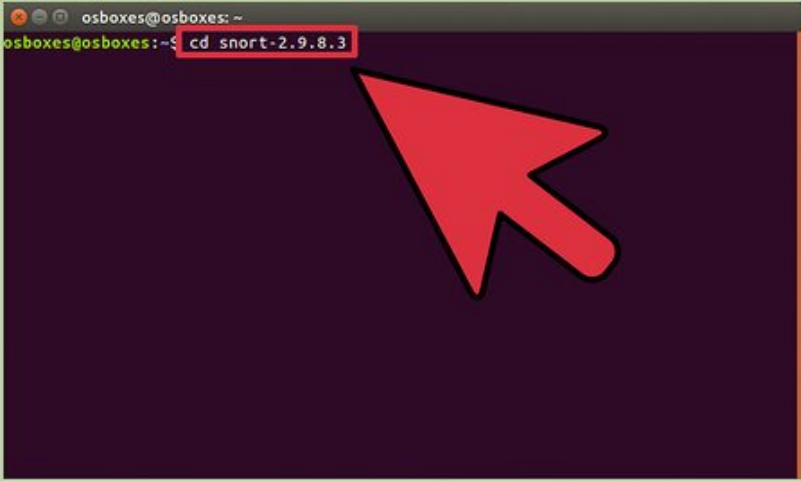
```
osboxes@osboxes: ~  
osboxes@osboxes:~$ tar xvtvz snort-2.9.8.3.tar.gz
```

A terminal window with a dark purple background. The prompt is `osboxes@osboxes: ~`. The command `tar xvtvz snort-2.9.8.3.tar.gz` is entered and highlighted with a red box. A red mouse cursor points to the command. The `wikiHow` logo is in the bottom right corner.

Untar the file:

1. `tar xvfz snort-2.9.7.0.tar.gz`

4.



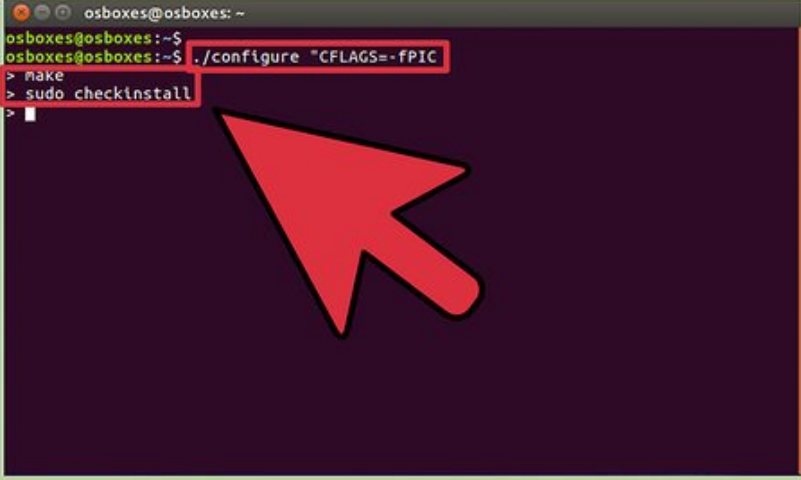
```
osboxes@osboxes: ~  
osboxes@osboxes:~$ cd snort-2.9.8.3
```

A terminal window with a dark purple background. The prompt is `osboxes@osboxes: ~`. The command `cd snort-2.9.8.3` is entered and highlighted with a red box. A red mouse cursor points to the command. The `wikiHow` logo is in the bottom right corner.

Change into snort-2.9.7.0 directory:

1. `cd snort-2.9.7.0`

5.



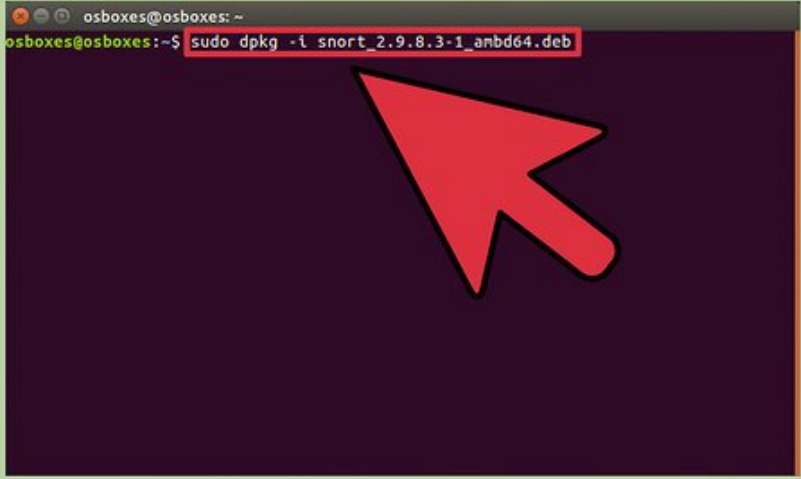
```
osboxes@osboxes: ~  
osboxes@osboxes:~$  
osboxes@osboxes:~$ ./configure "CFLAGS=-fPIC"  
> make  
> sudo checkinstall  
> |
```

A terminal window with a dark background and light text. The prompt is 'osboxes@osboxes: ~'. The user has entered three commands: './configure "CFLAGS=-fPIC"', 'make', and 'sudo checkinstall'. A red mouse cursor points to the 'sudo checkinstall' command. The terminal shows a vertical bar after the command, indicating it is running. A 'wikiHow' logo is in the bottom right corner.

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.



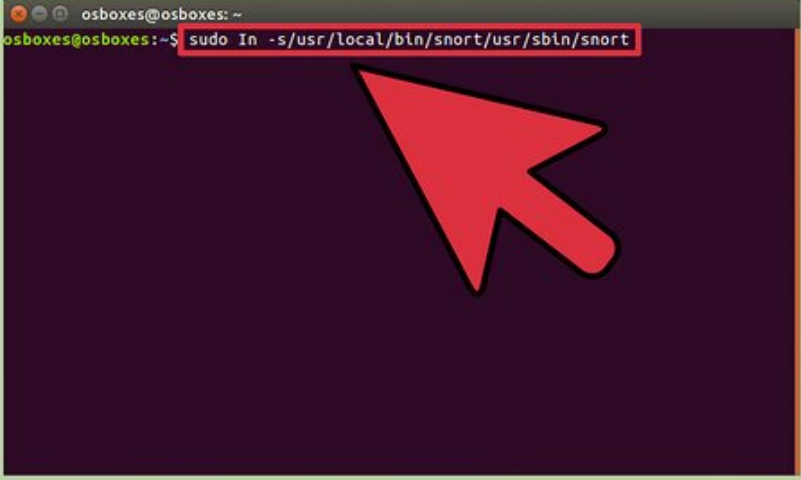
```
osboxes@osboxes: ~  
osboxes@osboxes:~$ sudo dpkg -i snort_2.9.8.3-1_amd64.deb
```

A terminal window with a dark background and light text. The prompt is 'osboxes@osboxes: ~'. The user has entered the command 'sudo dpkg -i snort_2.9.8.3-1_amd64.deb'. A red mouse cursor points to the command. A 'wikiHow' logo is in the bottom right corner.

Install the package:

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

7.




```
osboxes@osboxes: ~  
osboxes@osboxes:~$ sudo ln -s /usr/local/bin/snort /usr/sbin/snort
```

A terminal window with a dark background and light text. The prompt is 'osboxes@osboxes: ~'. The command 'sudo ln -s /usr/local/bin/snort /usr/sbin/snort' is entered and highlighted with a red box. A red mouse cursor points to the command. The 'wikiHow' logo is in the bottom right corner.

Create the required symbolic link:

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

8.

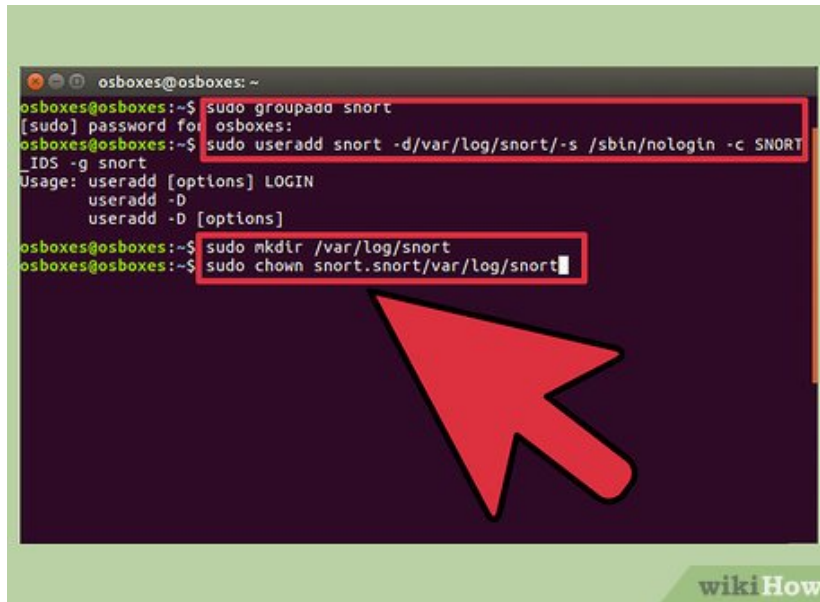


```
osboxes@osboxes: ~  
osboxes@osboxes:~$ snort -V
```

A terminal window with a dark background and light text. The prompt is 'osboxes@osboxes: ~'. The command 'snort -V' is entered and highlighted with a red box. A red mouse cursor points to the command. The 'wikiHow' logo is in the bottom right corner.

Verify the snort version by typing:

1. snort -V



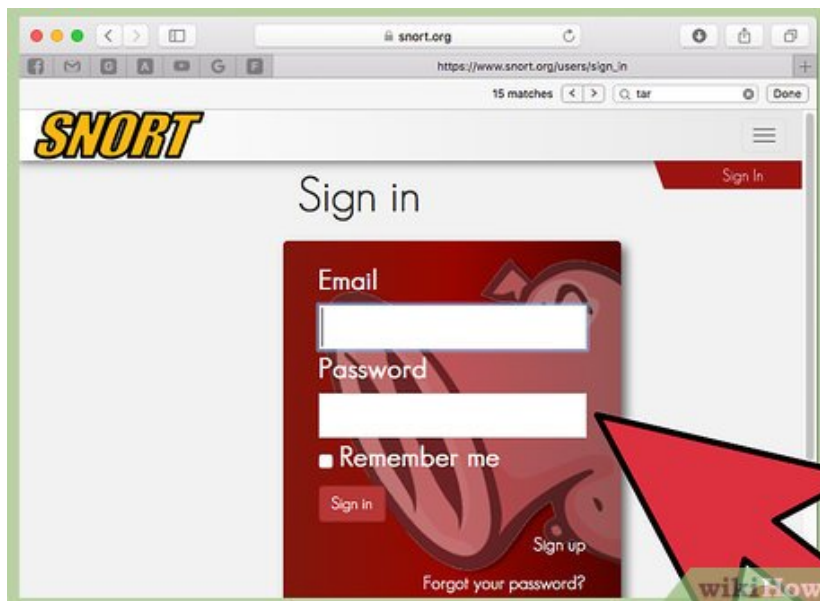
9.

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:

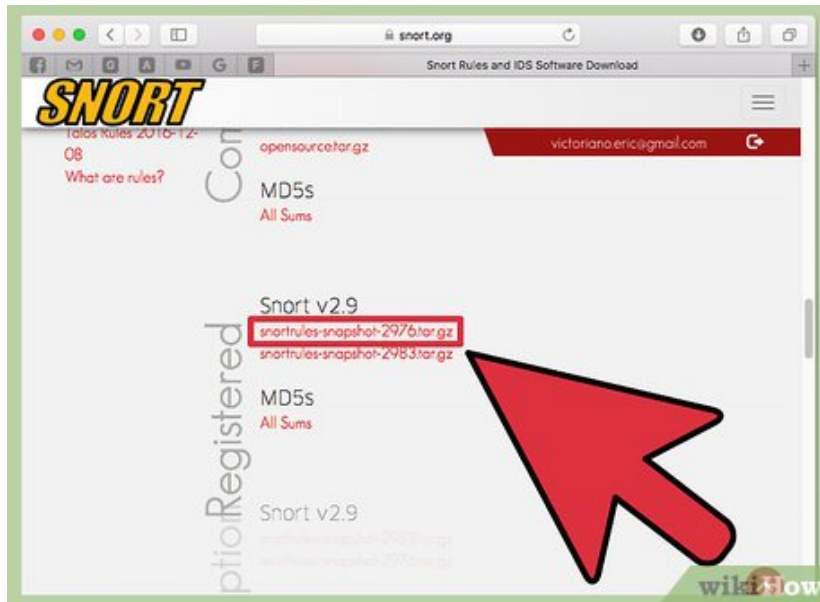
Install and Configure Snort Rules



1.

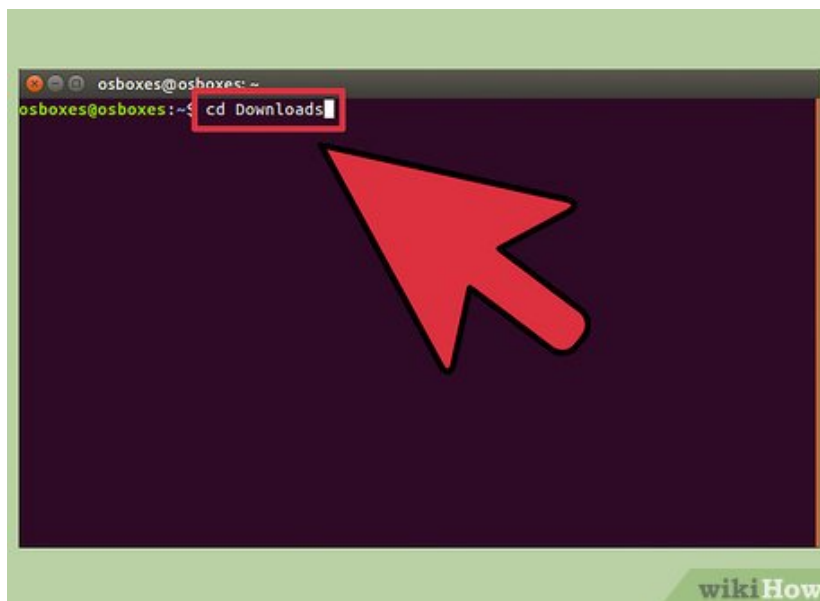
In order to download the default snort rule-set, you will have to create a log in at <https://www.snort.org>.

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.

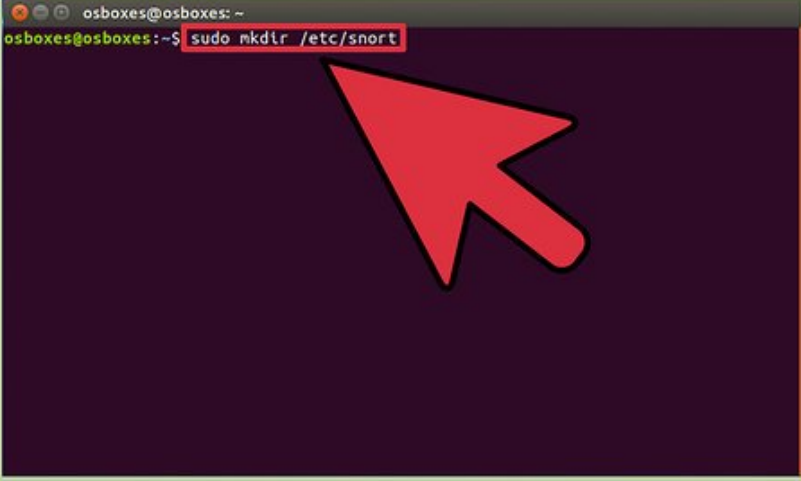
3.



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.



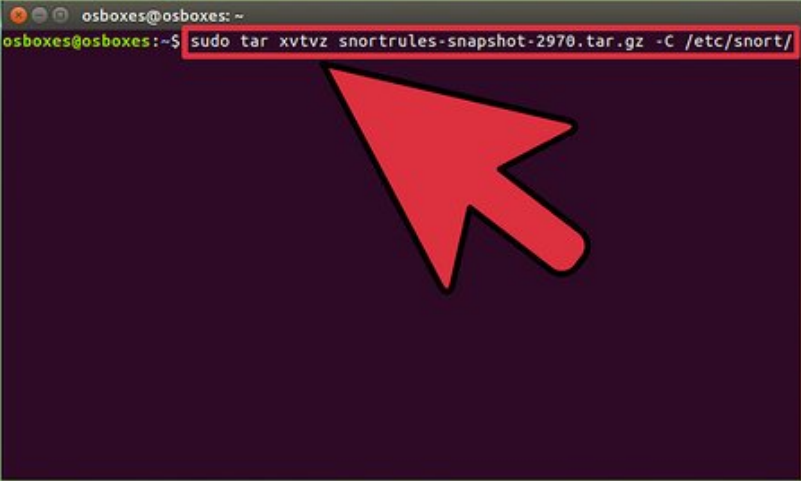
```
osboxes@osboxes: ~  
osboxes@osboxes:~$ sudo mkdir /etc/snort
```

A terminal window with a dark purple background and a light green header. The header shows the user 'osboxes' at 'osboxes: ~'. The prompt is 'osboxes@osboxes:~\$'. The command 'sudo mkdir /etc/snort' is entered and highlighted with a red box. A red mouse cursor points to the command. The 'wikiHow' logo is in the bottom right corner.

Make a new directory for the rules:

1. `sudo mkdir /etc/snort`

5.



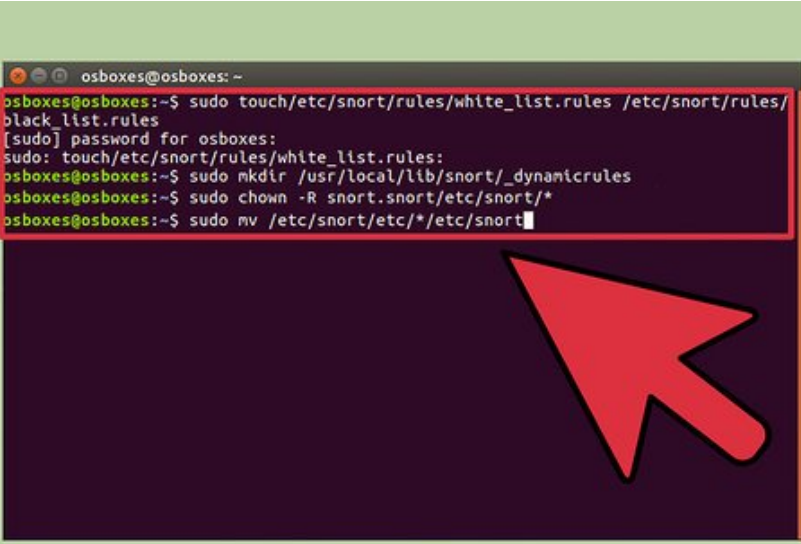
```
osboxes@osboxes: ~  
osboxes@osboxes:~$ sudo tar xvtvz snortrules-snapshot-2970.tar.gz -C /etc/snort/
```

A terminal window with a dark purple background and a light green header. The header shows the user 'osboxes' at 'osboxes: ~'. The prompt is 'osboxes@osboxes:~\$'. The command 'sudo tar xvtvz snortrules-snapshot-2970.tar.gz -C /etc/snort/' is entered and highlighted with a red box. A red mouse cursor points to the command. The 'wikiHow' logo is in the bottom right corner.

Untar the file

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

6.



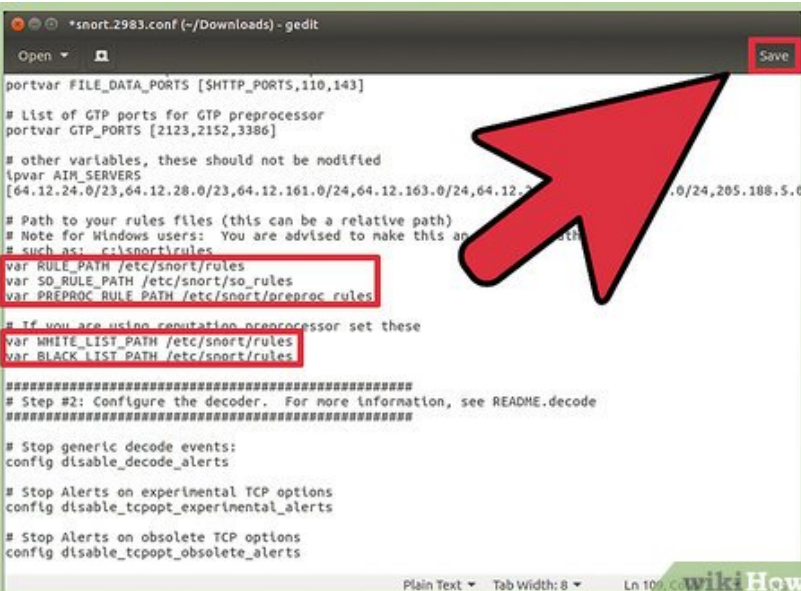
```
osboxes@osboxes:~$ sudo touch/etc/snort/rules/white_list.rules /etc/snort/rules/black_list.rules
[sudo] password for osboxes:
sudo: touch/etc/snort/rules/white_list.rules:
osboxes@osboxes:~$ sudo mkdir /usr/local/lib/snort_dynamicrules
osboxes@osboxes:~$ sudo chown -R snort:snort /etc/snort/*
osboxes@osboxes:~$ sudo mv /etc/snort/etc/* /etc/snort/
```

wikiHow

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.



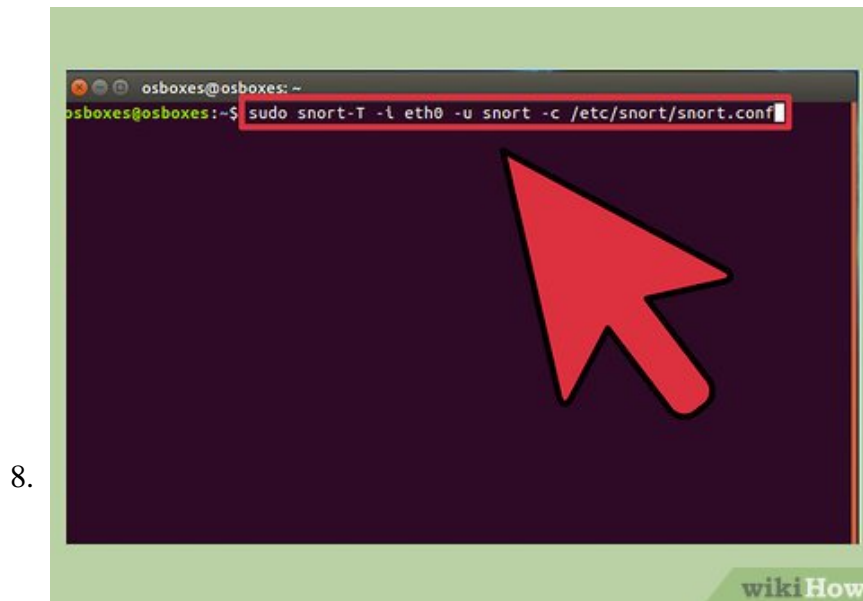
```
*snort.2983.conf (~/.Downloads) - gedit
Save
portvar FILE_DATA_PORTS [HTTP_PORTS,110,143]
# List of GTP ports for GTP preprocessor
portvar GTP_PORTS [2123,2152,3386]
# other variables, these should not be modified
ipvar AIM_SERVERS
[64.12.24.0/23,64.12.28.0/23,64.12.161.0/24,64.12.163.0/24,64.12.205.188.5.0
# Path to your rules files (this can be a relative path)
# Note for Windows users: You are advised to make this an
# such as: c:\snort\rules
var RULE_PATH /etc/snort/rules
var SO_RULE_PATH /etc/snort/so_rules
var PREPROC_RULE_PATH /etc/snort/preproc_rules
# If you are using reputation preprocessor set these
var WHITE_LIST_PATH /etc/snort/rules
var BLACK_LIST_PATH /etc/snort/rules
#####
# Step #2: Configure the decoder. For more information, see README.decode
#####
# Stop generic decode events:
config disable_decode_alerts
# Stop Alerts on experimental TCP options
config disable_tcpopt_experimental_alerts
# Stop Alerts on obsolete TCP options
config disable_tcpopt_obsolete_alerts
```

Plain Text Tab Width: 8 Ln 109 Co 68 wikiHow

Update snort config file:

1. Use any editor you are familiar with (vim, emacs, 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 106 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



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 -c /etc/snort/snort.conf`

You finished reading the article "**How to Set Up an Independent IDS/IPS Lab Environment (Using Snort, Pytbull, Eclipse and Tomcat)**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.