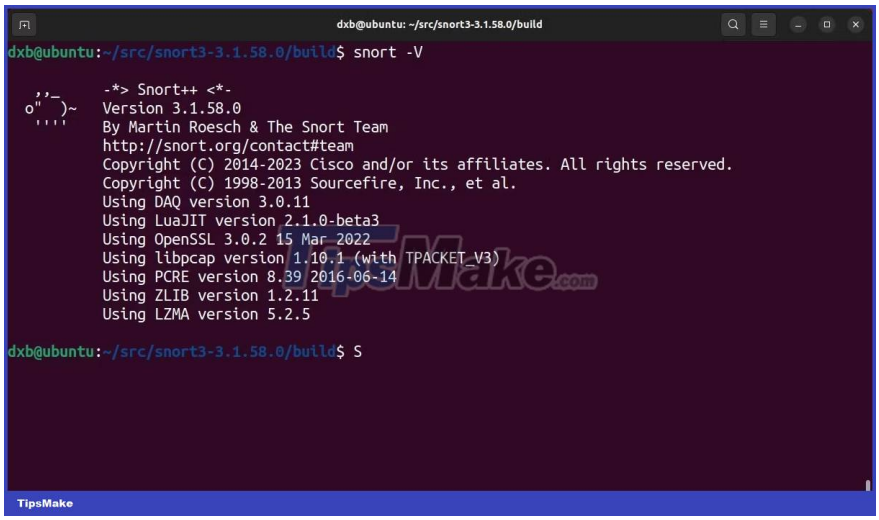
How to Install and Setup Snort IDS for Linux Network Security

If you are serious about network security, then installing an IPS or IDS solution is a must to strengthen the network perimeter and deflect potentially unwanted network traffic.

If you are serious about network security, then installing an IPS or IDS solution is a must to strengthen the network perimeter and deflect potentially unwanted network traffic.

Snort is one such famous, free and open source IPS/IDS solution. Learn how to install and set up Snort on Linux to protect your network from attacks through the following article!

What is Snort?



Snort is an open source Network Intrusion Prevention and Detection System (NIDS/IPS) software that helps protect your network by enforcing detection rules and filters, removing potentially malicious packets. included in your network.

With Snort, you'll be able to perform advanced network traffic logging, packet detection and analysis, and set up a powerful intrusion prevention system to protect your network from unwanted traffic. desirable and potentially harmful.

Prerequisites for installing Snort

Before installing Snort, you need to do some preliminary setup. This mainly includes updating and upgrading the system, as well as installing dependencies that Snort requires to function properly.

Start by updating and upgrading your system.

On Ubuntu and Debian-based Linux distributions:

```
sudo apt update && apt upgrade -y
```

On Arch Linux and its derivatives:

```
sudo pacman -Syu
```

On RHEL and Fedora:

```
sudo dnf upgrade
```

Once your system has been upgraded, continue to install the dependencies that Snort requires. These are the commands you need to run:

On Ubuntu and Debian, run:

```
sudo apt install -y build-essential autotools-dev libdumbnet-dev libluajit-5.1-d
```

On Arch Linux, run:

```
sudo pacman -S gperftools hwloc hyperscan ibdaqlibdnet libmnl libpcap libunwind
```

For RHEL and Fedora, run the following command:

```
sudo dnf install gcc gcc-c++ libnetfilter_queue-devel git flex bison zlib zlib-d
```

In addition, you also need to manually install the Data Acquisition Library, LibDAQ for Snort to work properly and also gperftools to generate build.

First, download the LibDAQ source files from the official website using the wget command. Then unzip the archive and move into the directory with cd. **Inside the directory, run the bootstrap** and **configure** scripts , then proceed to prepare the files with the **make** command and install it with the **make install command.**

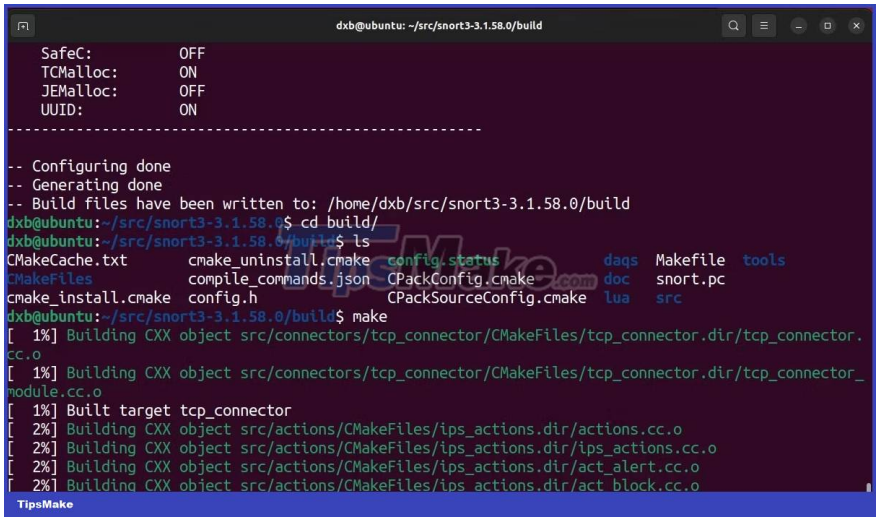
```
wget https://www.snort.org/downloads/snortplus/libdaq-3.0.11.tar.gz tar -xzvf li
```

After installing LibDAQ, you need to install one final dependency: gperftools. Start by grabbing the source files from the GitHub repo. Unzip the files, move into the directory and run the configuration script. Finally, install the package using **make** and **make install commands.**

```
wget https://github.com/gperftools/gperftools/releases/download/gperftools-2.10/
```

Once these dependencies have been installed, you can move on to the next steps to install Snort.

Install Snort from source on Linux



With the preliminary setup, you can now focus on the actual software installation. You will be building it from source, so first get the necessary build files.

Use the wget command or download the files manually from the official download page:

```
wget https://www.snort.org/downloads/snortplus/snort3-3.1.58.0.tar.gz
```

Download Snort

Once the archive containing the build files has finished downloading, extract it with the tar command:

```
tar -xzvf snort*
```

Move into the extracted directory, run the configuration script, use the make command to prepare the files, and finally install them with **make install** :

```
cd snort* ./configure_cmake.sh --prefix=/usr/local --enable-tcmalloc cd build ma
```

Now, Snort has been successfully installed in your system. However, you need to complete one more step. When new software is installed manually, the installation directory and required libraries may not be automatically included in the system default path. So you may get an error when starting the application.

To avoid this problem, you need to run the command ldconfig. It will sync the system's shared library cache with newly installed libraries and binaries. Run the ldconfig command from the root shell or use the sudo prefix:

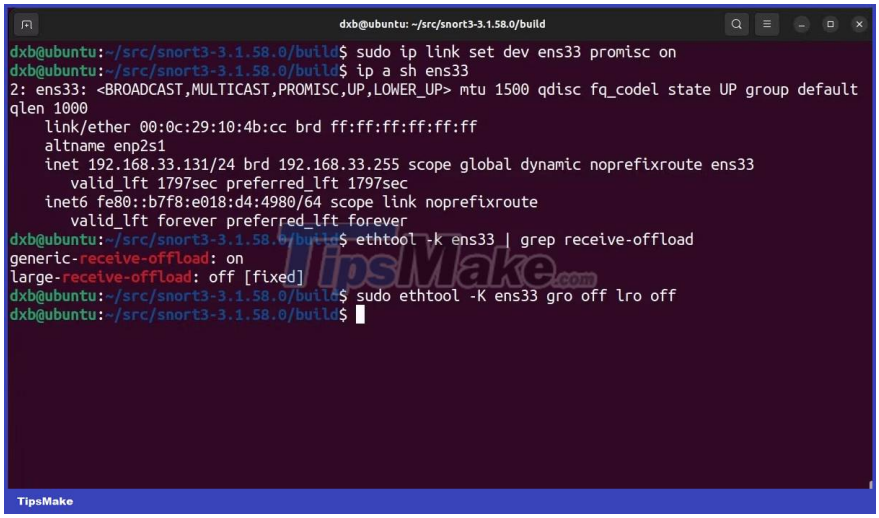
```
sudo ldconfig
```

You have now completed all the important steps required to install Snort. To verify the installation, run the Snort command with the -V flag and you should see an output that returns the version name and other data.

```
snort -V
```

Once you've verified the Snort installation, move on to the next steps to set it up as a full-blown IDS/IPS.

Initial Configuration of Snort on Linux



The effectiveness of Snort is almost entirely dependent on the quality of the rule sets it is powered with.

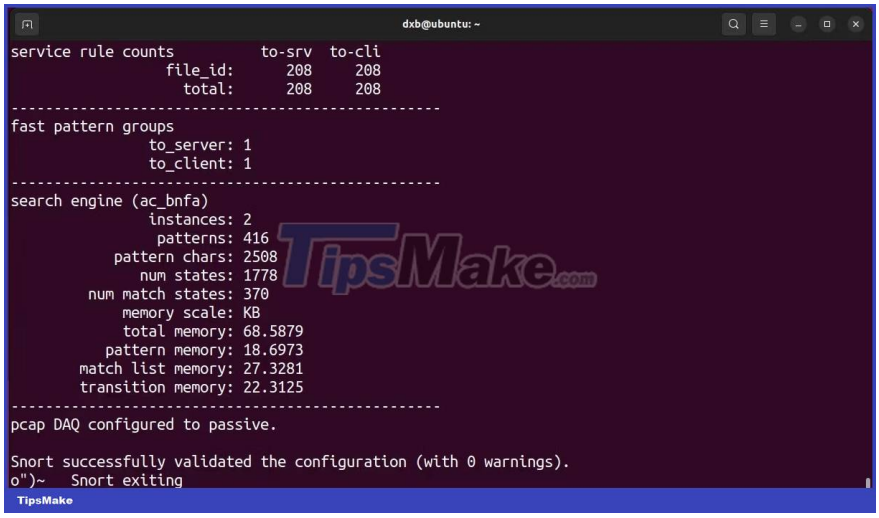
However, before setting up the rules, you need to configure the network cards to work with Snort and you also need to check how the default configuration is being handled by Snort. Start by configuring the network cards.

Put the network interface in promiscuous mode:

```
sudo ip link set dev interface_name promisc on
```

Using ethtool, disable Generic Receive Offload (GRO) and Large Receive Offload (LRO) to prevent larger network packets from being truncated:

```
sudo ethtool -K interface_name gro off lro off
```



Check out how Snort works with default configuration:

```
snort -c /usr/local/etc/snort/snort.lua
```

This will return a successful output, meaning you have installed and set up Snort correctly in your system. Now you can tinker with its features and experiment with different configurations to find the best set of rules to secure your network.

Set up rules and enforce them with Snort

With the basic settings in place, Snort is now ready to protect your network. As you know, Snort needs rule sets to determine traffic validity, let's set up a couple of free community-created rule sets for Snort.

Snort reads rule sets and configurations from specific directories. So, first, using the mkdir and touch commands, create a few important directories to store the rules and other related data for Snort:

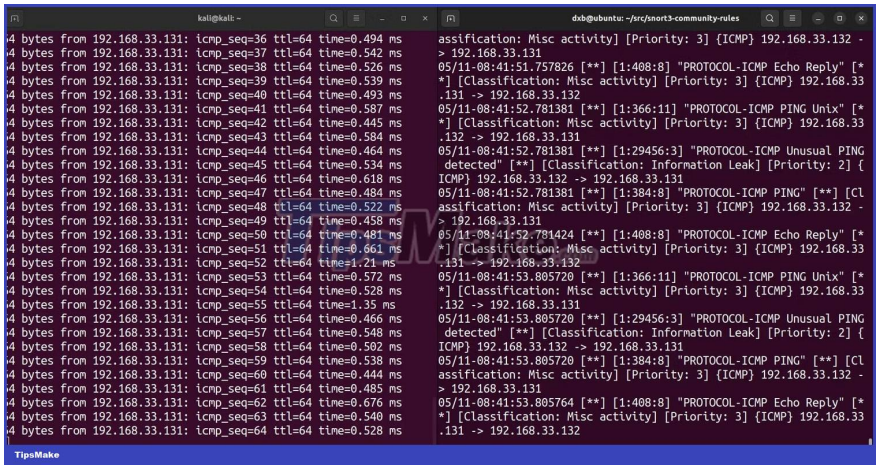
```
sudo mkdir -p /usr/local/etc/{lists,so_rules,rules} sudo touch /usr/local/etc/ru
```

With these directories created, you can download the community rule set from the official website using the wget command:

```
wget https://www.snort.org/downloads/community/snort3-community-rules.tar.gz
```

Once the rule set has finished downloading, unzip it and copy it to the **/usr/local/etc/rules/ directory.**

```
tar -xvzf snort3-com* cd snort3-com* cp * /usr/local/etc/rules/
```



To run Snort with the rule set, execute this command:

```
sudo snort -c /usr/local/etc/snort/snort.lua -R /usr/local/etc/rules/snort3-commu
```

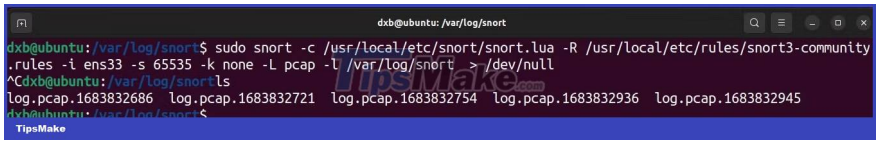
Command analysis:

1. **-c** sets the path to the default configuration file
2. **-R** sets the path to the rule set to execute
3. **-i** setup interface
4. **-s** remove snaplen limit
5. **-k** ignore the checksums

This will validate the configuration and enforce all rule sets on Snort. As soon as it detects any network disturbance, it will alert you with a console message.

If you want to create and enforce your own set of rules, you can learn more about them from the official documentation pages.

Set up logging with Snort



By default, Snort does not export any logs. You need to specify with the **-L** flag to start Snort in logging mode, specifying the log file type, and the **-l** flag to set the directory for Snort to dump logs.

Here is the command to start Snort with logging enabled:

```
sudo snort -c /usr/local/etc/snort/snort.lua -R /usr/local/etc/rules/snort3-commu
```

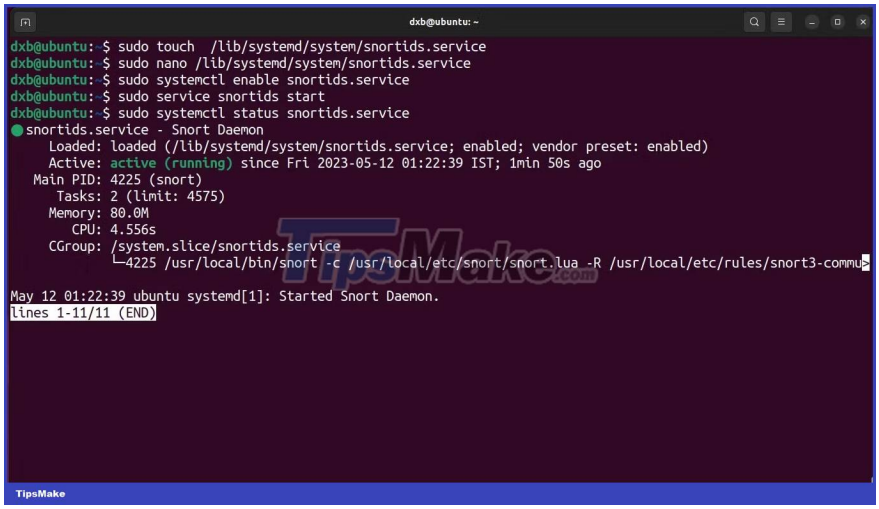
Command analysis:

1. **-c** sets the path to the default configuration file
2. **-R** sets the path to the rule set to execute
3. **-i** setup interface
4. **-s** remove snaplen limit
5. **-k** skip checksum
6. **-L** enables logging mode and defines log file type
7. **-l** defines the path where the log is stored

Note that in the example command, the logging directory is set to **/var/log/snort.** While this is the recommended method, you are free to store your logs elsewhere.

You can read the Snort log files from the directory you specified or pass them into SIEM software like Splunk for further analysis.

Add Snort as system startup daemon



Even though Snort has been installed and set up, you need to make sure it starts executing at startup and runs as a background daemon. Adding it as an autostart system service will ensure that Snort is up and running and protects your system every time it's online.

Here's how to add the Snort startup daemon on Linux:

1. Start by creating a new systemd service file:

```
touch /lib/systemd/system/snort.service
```

2. Open the file in a text editor of your choice and fill in the following data in the file. You can modify the flags to fit your needs:

```
[Unit] Description=Snort Daemon After=syslog.target network.target [Service] Type
```

3. Save and exit the file. Then, using the service and systemctl commands, fire up and start the script:

```
sudo systemctl enable snort.service sudo snort start
```

The Snort-based daemon should now be up and running. You can verify the status of the script with the command **systemctl status snort** .

While IDS implementation is a good practice, it is a passive measure, not an active one. The best way to improve and ensure the security of the network is to continuously test the network and look for errors to fix.

Penetration testing is a great way to find exploitable vulnerabilities and patch them.

You finished reading the article "**How to Install and Setup Snort IDS for Linux Network Security**" 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.