

# Tutorial Snort Wireless

Monday, 01 November 2004

#--- [ Tutorial Snort Wireless ] ---#

(c) 2004 by d.walther (d.walther@wireless-bern.ch) - Wireless-Bern.ch

-- Introduction --

-----

<http://snort-wireless.org>:

"The Snort-Wireless project is an attempt to make a scalable (and free!) 802.11 intrusion detection system that is easily integratable into an IDS infrastructure. It is completely backwards compatible with Snort 2.0.x and adds several additional features. Currently it allows for 802.11 specific detection rules through the new "wifi" rule protocol, as well as rogue AP, AdHoc network, and Netstumbler detection.

Many more new features are planned for future releases. Bascially, Snort-Wireless intends to eventually be the opensource answer to AirDefense."

If you find some errors or you are missing something, please contact me.

-- Requirements --

-----

- Download the Snort 2.1.1 source code

>> <http://www.snort.org/dl/old/snort-2.1.1.tar.gz>

- Download Snort-Wireless-Patch for Snort 2.1.1 from Sebastien Gracia

>> <http://snort-wireless.org/files/snort-2.1.1-wireless.patch.gz>

- Download the Snort 2.1.1 Wireless Database patch (only needed if you want to store the alerts and the logfiles into a database)

>> <http://www.wireless-bern.ch/downloads/snort-2.1.1-wireless-db.patch>

- You can also download the following file. This archive contains all files listed above.

>> <http://www.wireless-bern.ch/downloads/snort-wireless-db-2.1.1.tar.gz>

I have tested the Snort Wireless database patch with the PostgreSQL 7.4.5 database. It should also work with MySQL.

- If you want to compile Snort Wireless with database support you have also to download the source code of the desired database.

PostgreSQL >> <http://www.postgresql.org/mirrors-ftp.html>

MySQL >> <http://dev.mysql.com/get/Downloads/MySQL-4.1/mysql-4.1.7.tar.gz/from/pick#mirrors>

Please do not download the binaries. You will need the source code.

-- Installation --

-----

After you have downloaded all required files you can start with the installation.

First of all you have to extract the Snort 2.1.1 archive.

```
tar xvfz snort-2.1.1.tar.gz
```

The whole source code will be extracted in the directory named snort-2.1.1

Then you have to apply the two patches.

```
patch -p0 < snort-2.1.1-wireless.patch.gz
```

For the database support:

```
patch -p0 < snort-2.1.1-wireless-db.patch
```

After this step, you have successfully patched your snort 2.1.1

If you want to compile Snort Wireless with database support, so you have to compile your desired database first. For the installation of the database please refer to the following links.

PostgreSQL: <http://www.postgresql.org/docs/7.4/static/installation.html>

MySQL: <http://dev.mysql.com/doc/mysql/en/Installing.html>

Now you can compile Snort Wireless. Here you have different possibilities.

- Without database support

```
./configure --enable-wireless
```

- With MySQL support

```
./configure --enable-wireless --with-mysql
```

- With PostgreSQL support

```
./configure --enable-wireless --with-postgresql
```

- For static compilation (static linking of the libraries)

If you want the database support in the static version too, you have to enable it with the correct statement ("--with-mysql" or "--with-postgresql")

```
LDFLAGS=-static ./configure --enable-wireless
```

After you've ran the configure script you can compile and install snort with:

```
make
```

```
make install
```

Now you successfully compiled Snort Wireless and are able to monitor your wireless network.

If you use a database, you have to generate the database. Therefor Snort have a script for each database. You can deploy them the following way:

MySQL (database user = snort):

```
mysql -D snort -u root -p < snort-2.1.1/contrib/create_mysql
```

PostgreSQL (database user = snort):

```
psql snort < snort-2.1.1/contrib/create_postgresql
```

If you want to monitor your wireless network you have to have a wireless card (e.g. Orinoco Gold) which is able to switch into the monitor mode.

Snort Wireless isn't able to set your wireless card into the monitor mode so you have to set your wireless card in monitor mode manually before you start Snort Wireless.

If you are using an Orinoco card, you can also use the Orinoco channel hopper. This tiny tool could be interesting if you want to monitor several channels and not only one.

You can download the source code of the Orinoco hopper here: `orinoco_hopper.c` (compile with "gcc -o orinoco\_hopper orinoco\_hopper.c")

In Snort Wireless you have a lot of special rules and preprocessors for wireless monitoring.

You can set all options (including database connection) in the file `"/etc/snort.conf"`. For the configuration please read the Snort readme file.

Please start Snort Wireless the following way at the first time:

```
snort -?
```

This will print out all possible options for starting snort. So you can set some useful settings (e.g. `-w Dump 802.11 packets`).

```
-- Details about the database support --
```

```
-----
```

I've added an additionally table (`wifihdr`) for the wifi headers. In this table you will find all informations that are captured. I also modified the database output, that there will be stored the log and alert informations. So only specify the database support in the `snort.conf` file like that:

output database: log, (postgresql or mysql), user=snort password=xxx dbname=snort host=localhost

-- Disclaimer --

-----

These informations are supplied without liability. I take no responsibility for any errors and blue screens!

You will make this installation at your own risk.

-- References --

-----

- <http://snort-wireless.org>

- <http://www.snort.org>