

# Updating Snort 2.8.6 and Ubuntu 10.04 Using Automated Scripts

Author: David Gullett

Published: June 28, 2010

Version: 1.01

Copyright 2010, Symmetrix Technologies

<http://www.symmetrixtech.com>

---

## Table of Contents

### A. Introduction

1. Equipment Assumptions
2. Knowledge Assumptions
3. Use of the Backslash
4. End Result

### B. Procedure

1. Set up Oinkmaster
2. Create the Update Script
3. Create the Cron Job
4. Testing

### C. A Final Note

## A. Introduction

This document is designed to provide you with an easy way to keep your Snort 2.8.6 signatures and Ubuntu Linux 10.04 LTS OS updated. It builds on our previous Snort and Snort Report installation guides available at <http://www.symmetrixtech.com>.

### 1. Equipment Assumptions

A computer with Ubuntu 10.04 LTS and Snort 2.8.6 installed as described in our earlier guide is located here: <http://www.symmetrixtech.com/articles/004-snortinstallguide286.html>

### 2. Knowledge Assumptions

A working knowledge of Linux including SSH and editing configuration files with vi  
A basic knowledge of TCP/IP and network topologies

### 3. Use of the Backslash

There are many instances in this document where a command will not fit on one line so the commonly accepted backslash is used to split it into multiple lines. For example, this is one command, not two:

```
/usr/local/snort/bin/snort -D -u snort -g snort \  
-c /usr/local/snort/etc/snort.conf -i eth1
```

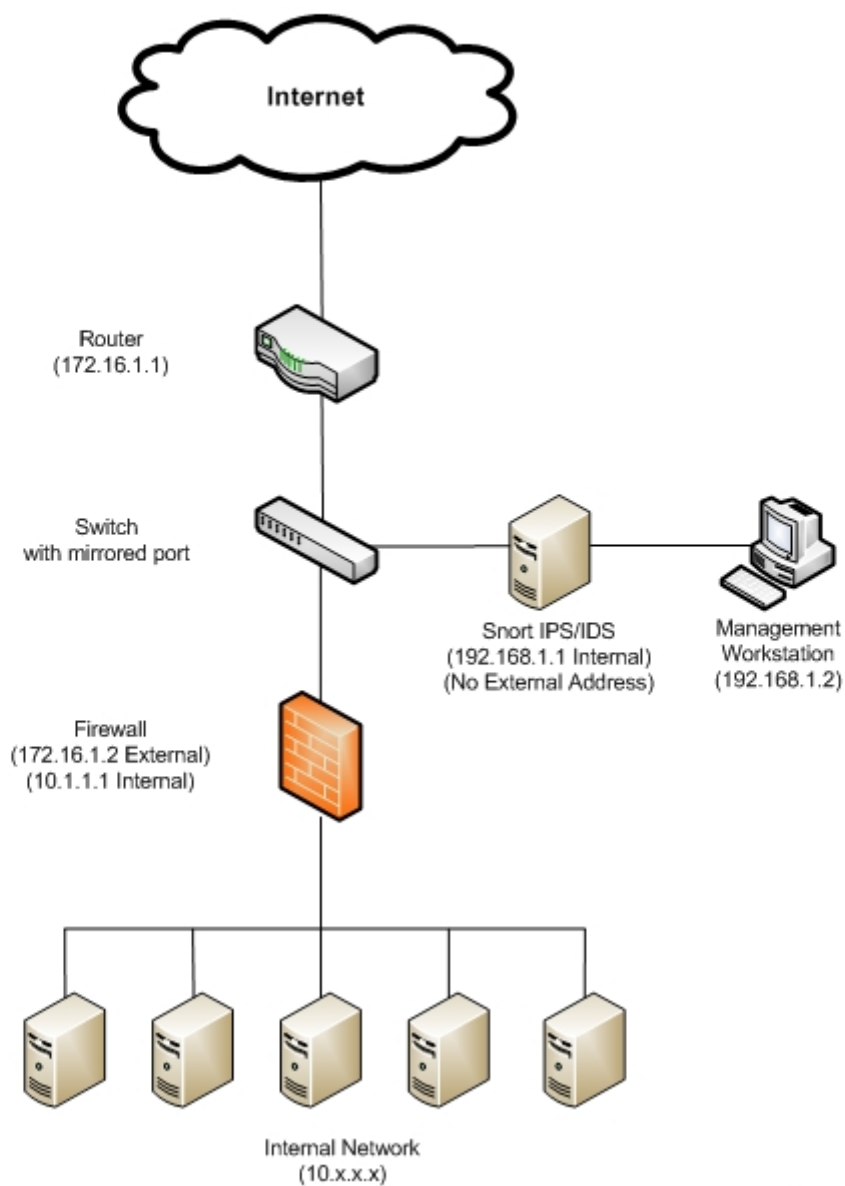
If you are copying and pasting you can leave the backslashes in place and Linux will understand it.

### 4. End Result

We're going to set up an automated cron job to assign an IP address to the external interface, update Snort and Ubuntu and then remove the IP address to restore the machine to the original configuration. This will help prevent a successful external attack on your IDS/IPS machine.

The following diagram illustrates the topology.

## Simple Snort Network Topology



Copyright 2010, Symmetrix Technologies

Figure 1 – Snort Network Topology

In the figure above, the network card on the Snort machine facing the traffic you are monitoring has no IP address. This is the card to which we're going to temporarily assign an IP address in order to be able to download the various updates. Again, the address will be removed at the end of the script. The window on this procedure should be reasonably brief depending on the speed of your Internet connection.

## B. Procedure

### 1. Set up Oinkmaster

#### Description

Oinkmaster is the tool provided by Sourcefire to automatically update the Snort signatures.

#### Getting an Oinkcode

In order to use this service you will need to generate an Oinkcode on <http://www.snort.org>. Log in to their site from any PC (you should already be registered if you have already set up Snort) and click on the “Get Rules” button. Scroll down to the bottom of the page and select “Use an Oinkcode.”

The site will generate a lengthy alphanumeric code for you and give you a variety of URLs with which to configure Oinkmaster. Make a note of the URL for the Snort 2.8.6 ruleset for the Registered User Release. This URL incorporates your Oinkcode and will look something similar to this (which we'll be using in a scripting example below):

#### Installation

Download Oinkmaster 2.0 from this location: <http://oinkmaster.sourceforge.net/download.shtml> Copy the tarball to your IDS/IPS box.

Open a command prompt on your Snort machine via the console or SSH and navigate to the directory where you copied Oinkmaster. Issue the following commands to unpack and install Oinkmaster:

```
tar zxvf oinkmaster-2.0.tar.gz
cd oinkmaster-2.0
sudo cp oinkmaster.pl /usr/local/bin/.
sudo cp oinkmaster.conf /usr/local/etc/.
mkdir /usr/local/snort/rules.backup
```

Now let's modify the Oinkmaster configuration file to contain your Oinkcode information.

```
sudo vi /usr/local/etc/oinkmaster.conf
```

Add a line towards the beginning of the file beginning with “url =” and ending with the information you obtained from snort.org in the previous step. It should look something similar to this (except all on one line and no spaces):

```
url = http://www.snort.org/pub-bin/oinkmaster.cgi/YOUROINKCODE/
      snortrules-snapshot-2860.tar.gz
```

Please note that this is a very basic Oinkmaster configuration. You should familiarize yourself with the other options in the oinkmaster.conf file.

## 2. Create the Update Script

```
sudo /usr/local/bin/oinkmaster.pl -b /usr/local/snort/rules.backup \  
-o /usr/local/snort/rules
```

Create a blank script file and make it executable by running the following commands:

```
sudo touch /usr/local/bin/snortupdate.sh  
sudo chmod 744 /usr/local/bin/snortupdate.sh  
sudo chown root:root /usr/local/bin/snortupdate.sh
```

Edit the file using 'vi /usr/local/bin/snortupdate.sh' from the command shell and paste the following script into the file (everything between the two long dashed lines):

```
-----  
#!/bin/sh  
# This is an example script to update Snort 2.8.6 and Ubuntu 10.04 LTS.  
# Copyright Symmetrix Technologies, 2010  
  
# Add IP address to eth1 - you will need to change the IP addresses to reflect  
# your network setup.  
# IMPORTANT - make sure you have a reachable DNS server specified in  
# /etc/resolve.conf or the updates will fail!  
ifconfig eth1 172.16.1.3 netmask 255.255.0.0  
route add default gateway 172.16.1.1  
  
# Run Oinkmaster to backup old rules and download the new rules  
/usr/local/bin/oinkmaster.pl -b /usr/local/snort/rules.backup \  
-o /usr/local/snort/rules  
  
# Download and apply updates to Ubuntu  
aptitude update  
aptitude -y safe-upgrade  
  
# Remove IP address from eth1  
ifconfig eth1 0.0.0.0  
  
# Restart Snort to apply new rules  
# Note: this is a quick and dirty way of restarting Snort that doesn't require  
# you to have a init.d script  
kill `cat /var/run/snort_eth1.pid`  
/usr/local/snort/bin/snort -D -u snort -g snort \  
-c /usr/local/snort/etc/snort.conf -i eth1  
-----
```

Be sure and modify the scripts to reflect the IP address values and name resolution in your network as mentioned above.

Also please note that on the line containing the 'kill' command those are not single apostrophes - they are backticks.

Save and exit the file.

### 3. Create the Cron Job

The next step is to create a cron job in the /etc/cron.d directory that will periodically call the update script. Sourcefire recommends you update no more frequently than once an hour but once a day is usually more than sufficient.

From the command prompt create the job with this command:

```
sudo vi /etc/cron.d/snortupdate
```

Paste this line into the file, save and exit:

```
0 2 * * * root /usr/local/bin/snortupdate.sh
```

That command will run the script as root at 2 AM once a day. Read the cron documentation if you need to fine-tune the update time.

### 4. Testing

To make sure this process is working there are several things you can do after a day or two:

1. Check the dates on the rule files by issuing 'ls -l /usr/local/snort/rules' from a shell on the Snort machine. Sourcefire does not necessarily update the registered signatures daily so it may be a while before you see newer file dates.
2. Examine the running processes by issuing the 'ps ax' command from the shell. You should see a line containing the Snort and barnyard processes.
3. Look at /var/log/syslog. You should see Snort restarting and dumping all of its quite extensive startup messages into that file.
4. Check Snort Report to see if you're getting updated data. The installation procedure for this software was documented in our previous guide located here: <http://www.symmetrixtech.com/articles/004-snortinstallguide286.html>

## C. A Final Note

As with any IDS/IPS system, this is not a 'set and forget' machine. An automated script, while very useful, does not ensure that nothing will go wrong occasionally. You need to routinely check on the triggered alerts and also make sure updates are being applied.

We also highly recommend signing up for the snort-users mailing list available at <http://www.snort.org> and following us on Twitter for new guides and updates to Snort Report here: <http://twitter.com/symmetrixtech> (don't worry, our feed is a low level of traffic).

-----

Visit us on the web at <http://www.symmetrixtech.com> for the latest news on Snort Report and to download the latest version.

Revision History:

2010-06-28 – 1.0 - Initial release

2010-06-30 – 1.01 – Revised to reflect the new Snort.org download location