Installing and configuring OinkMaster

By Patrick Harper | CISSP, RHCT, MCSE
with contributions and editing by Nick Oliver | CNE

http://www.InternetSecurityGuru.com

Acknowledgments:

I would like to thank all my friends and the people on the Ntsug-Users list that proofed this for me. My wife Kris, Nick Oliver (without him the spelling and punctuation for this and other documents would be horrible). Thanks to Andreas Ostling andreaso@it.su.se for writing OinkMaster. Also I would like to thank Marty and the Snort team for their great work. Thanks for staying true to open source, keep it up guys.

Comments or Corrections:

Please e-mail any comments or corrections to mailto:Patrick@internetsecurityguru.com

Nick Oliver has also made himself available for contact if for any reason I may be unavailable or running behind on my large and ever growing inbox. mailto:nwoliver@internetsecurityguru.com

The latest version of this document is located at http://www.internetsecurityguru.com/documents/.
Please use the most up to date version I will do my best to keep it updated.

Other Resources:

Snort users manual http://www.Snort.org/docs/writing_rules/
Snort FAQ http://www.Snort.org/docs/faq.html
The Snort user's mailing list http://lists.sourceforge.net/lists/listinfo/snort-users

OinkMaster mailing list http://lists.sourceforge.net/lists/listinfo/oinkmaster-users

http://oinkmaster.sourceforge.net/man.html gives you a good outline of the parameters you can use. OinkMaster's homepage is http://oinkmaster.sf.net/. You can find out a lot more about it there.

This document will help you install OinkMaster, a script that helps you keep your rules up to date on your Snort IDS system. It will also teach you to how set it up as a cron job (the way I do it is to just set it as a cron job running every night).

You need to create an account at http://www.snort.org so you can set up your oink code. This is a requirement for setting up OinkMaster. We will also explore the types of rules available and which ones you need. We will show you how to keep track of any rules that you have disabled. Disabling rules is not always he best way to tune, rather a combination of disabling, thresholding, and suppression should be used in most cases.

Types of rules on snort.org:

Sourcefire VRT Certified Rules - The Official Snort Ruleset (subscription release)
These rules are available to paid subscribers only, for the first 5 days after they are released. Sourcefire puts a lot of work into these and most people do not understand the amount of testing that they do to make sure the rules are the highest quality possible.

Personal Note: If you do not want to wait the 5 days, you have options.

1. You can write the rules yourself, set up a lab, test the results to make sure you not creating a nightmare for yourself and install them in your local.rules file.
2. You can keep an eye on the snort-sigs mailing list and see is someone else is doing the work so you don't have to.
3. You can go to http://www.bleedingsnort.com, they have some good rules that are released pretty quickly.
4. And this is a major suggestion. You should at least learn to read the basics of the rule language. Buy a book, read the docs on the Snort site, take one of the Sourcefire class's on rules, do something. While most of us will never be able to write rules as well as the VRT team does we can at least know what a rule is looking for.

Sourcefire VRT Certified Rules - The Official Snort Ruleset (registered user release)
These are the same rules as above, but they are all past the 5 day waiting period. These are the ones that we will be using in this doc and should be used on a regular basis. They are excellent rules and the amount of testing that goes into them is amazing. They are the same rules that are released to paying customers and Sourcefire appliances. For the small price of five days you get the benefit of all their experience, knowledge, and testing of the VRT team.

Sourcefire VRT Certified Rules - The Official Snort Ruleset (unregistered user release)
This is the basic set of rules that comes with the new version. They will be updated at the time of the next major Snort release. They do not change between releases.

Community Rules
Like the website says. "The Community Rulesets contain rules submitted by members of the open source community. While these rules are available as is, the VRT performs basic tests to ensure that new rules will not break Snort. These rules are distributed under the GPL and are freely available to all open source Snort users."

Getting Started

Prep the snort rules directory:
chown -R snort:snort /etc/snort/rules

Download OinkMaster
http://www.ip-solutions.net/~hhoffman/oinkmaster/oinkmaster-1.2-0.noarch.rpm

rpm –ivh oinkmaster-1.2-0.noarch.rpm

cd to /etc

Edit the oinkmaster.conf file and add the line modified to fit your environment. Put it where they start giving the examples of the download lines near the top of the oinkmaster.conf. You will see lines similar to the one below:

url = http://www.snort.org/pub-bin/oinkmaster.cgi/**<oinkcode here>/<filename>**

To check your version of snort execute snort –V like this
[root@www ~]# snort -V

```
   ,,_     -*> Snort! <*-
  o"  )~   Version 2.4.0 (Build 18)
   ""      By Martin Roesch & The Snort Team: http://www.snort.org/team.html
           (C) Copyright 1998-2005 Sourcefire Inc., et al.
```

For Snort 2.4.X you would use the filename:
snortrules-snapshot-2.4.tar.gz

And enter your Oinkcode in the URL. The oinkcode will look something like this:
5a08f649c16a278e1012e1c84bdc8fab9a70e2a4

The line will end up looking like this (this is one contiguous line):
url=http://www.snort.org/pub-bin/oinkmaster.cgi/
5a08f649c16a278e1012e1c84bdc8fab9a70e2a4/snortrules-snapshot-2.4.tar.gz

Execute the following command to make a list of what rules you have disabled. Re-run this anytime you do tuning to your sensor and turn off any rules. It will read what rules you have disabled and add them to a file that you will pass to OinkMaster. Make sure you are in /etc when you do this.

makesidex.pl /etc/snort/rules >autodisable.conf

This is the basic command to update the active rules. NEVER RUN THIS AS ROOT

```
oinkmaster.pl -C /etc/oinkmaster.conf -C /etc/autodisable.conf -o
/etc/snort/rules (this is one line, it always will be)
```

We will be running OinkMaster as snort, if you do not have a snort user I will show you how to create one below. If you installed Snort with my docs you have a user called snort, just do a crontab –u snort –e to edits the snort users crontab. Crontab lists the events that are run at a normal time interval for a user, ever user can have a crontab

As root do the following
groupadd snort
useradd -g snort snort –s /sbin/nologin

The following will make OinkMaster run at 5:30 every morning:

30 5 * * * /usr/bin/oinkmaster.pl -C /etc/oinkmaster.conf -C /etc/autodisable.conf -o /etc/snort/rules

That is one of the most basic ways to use cron. The other way is to create a script in the /usr/bin dir and use chmod +x to make it executable. This is the way I would do it.

cd /usr/bin
touch oinkdaily
chmod +x oinkdaily
vi oinkdaily

Then add the content you want. You can make it mail you when it is done, log to syslog, or a combination.

Many people use the mail feature but you need to make sure you have a valid hostname for a lot of mail servers. Give it an FQDN so that it is not calling itself localhost.localdomain. **Add** a line to the /etc/hosts file that looks something like this, except more reflecting of your network and host:

10.10.10.10 www www.mynetwork.com

To get the mail feature working, make the content of your oinkdaily file like the following:

oinkmaster.pl -C /etc/oinkmaster.conf -C /etc/autodisable.conf -o /etc/snort/rules 2>&1 | mail -s "oinkmaster" you@yourdomain.com

If you want to backup the files and mail yourself, you will need to create a backup directory then change the contents of your oinkdaily file. To accomplish this, do the following:

mkdir /etc/snort/backup
chown -R snort:snort /etc/snort/backup

Add "-b /etc/snort/backup" to your line so your oinkdaily file looks like this:

oinkmaster.pl -C /etc/oinkmaster.conf -C /etc/autodisable.conf -o /etc/snort/rules -b /etc/snort/backup 2>&1 | mail -s "oinkmaster" you@yourdomain.com

Once you get it the way you want, set up a cron entry for it. "cron –u snort –e" to open up the snort users crontab. Then make your entry. The following example will set it up for 5:30 am every morning.

30 5 * * * /usr/bin/oinkdaily

When it runs, it will e-mail you, and will look something like the information below. From time to time you may see errors on duplicate rules. This is ok and most likely just an error in the Ruleset from snort. For example, they might have left two rev's of the same rule in the snapshot.

```
Loading /etc/oinkmaster.conf
Loading /etc/autodisable.conf
Downloading file from http://www.snort.org/pub-
bin/oinkmaster.cgi/XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX/snortrules-
snapshot-2.4.tar.gz... done.
Archive successfully downloaded, unpacking... done.
Setting up rules structures...
WARNING: duplicate SID in your local rules, SID 2527 exists multiple
times, you may need to fix this manually!
done.
Processing downloaded rules... disabled 0, enabled 0, modified 0,
total=3672
Setting up rules structures...
WARNING: duplicate SID in your local rules, SID 2527 exists multiple
times, you may need to fix this manually!
done.
Comparing new files to the old ones... done.

[***] Results from Oinkmaster started 20051003 07:55:20 [***]

[*] Rules modifications: [*]
```

```
    None.

[*] Non-rule line modifications: [*]
    None.

[*] Added files: [*]
    None
```