

Installing Snort 2.8.5.2 on Windows 7  
by Kasey Efaw  
[snortguide@gmail.com](mailto:snortguide@gmail.com)

This guide is meant to assist the user in installing, configuring and running the Snort IDS technology on a Windows 7 (32-bit) operating system. This guide could easily be used for other Windows based Operating Systems, just remember with Vista and later you are working with the UAC. Configuring rules, deciphering alerts and tailoring to your specific network is beyond the scope of this guide. It is not advised to test an installation within a production environment and neither Snort or the Author offer any warranty against negative impacts to your systems that may be derived from following this guide.

I have received many e-mails as a result of my original guide (Snort Installation on Windows XP) and would like to thank the Open Source Community for their kind words and questions requiring troubleshooting. As a result of your feedback, this guide has been updated to answer some common questions as well as includes screen shots. In the future, I will have installation and usage videos posted on YouTube under the user name "snortguide".

Although it is recommended to perform the installation from a clean, formatted drive, this guide will work through the steps installed from within a virtual environment. With the exception of the operating system itself, all software is freely available (check Eula's for Commercial usage). All links are valid as of 1/31/2010 and different steps may be required if using a version differing from those listed below.

Microsoft Windows 7 Professional:

[http://store.microsoft.com/microsoft/Windows-7-Professional/product/B985134B?WT.mc\\_id=winonlinetest\\_shop3\\_PROfull\\_r3](http://store.microsoft.com/microsoft/Windows-7-Professional/product/B985134B?WT.mc_id=winonlinetest_shop3_PROfull_r3)

Mozilla Firefox 3.6:

<http://www.mozilla.com/en-US/products/download.html?product=firefox-3.6&os=win&lang=en-US>

Microsoft Security Essentials:

[http://www.microsoft.com/security\\_essentials/](http://www.microsoft.com/security_essentials/)

COMODO Firewall 3.14:

<http://www.comodo.com/home/download/download.php?prod=firewall>

Microsoft Baseline Security Analyzer 2.1.1:

<http://www.microsoft.com/downloads/details.aspx?FamilyID=b1e76bbe-71df-41e8-8b52-c871d012ba78&displaylang=en>

ActivePerl 5.10.1.1006:

<http://www.activestate.com/activeperl/>

Notepad++ 5.6.6

<http://sourceforge.net/projects/notepad-plus/files/notepad%2B%2B%20releases%20binary/npp%205.6.6%20bin/npp.5.6.6.Installer.exe/download>

Foxit Reader 3.1.4:

[http://download.cnet.com/Foxit-Reader/3000-10743\\_4-10313206.html?part=dl-116442&subj=dl&tag=button](http://download.cnet.com/Foxit-Reader/3000-10743_4-10313206.html?part=dl-116442&subj=dl&tag=button)

Kiwi Syslog Server 9.0.3:

<http://kiwisyslog.com/kiwi-syslog-server-download/>

7-Zip 4.65:

<http://sourceforge.net/projects/sevenzips/files/7-Zip/4.65/7z465.exe/download>

WinPcap 4.1.1:

<http://www.winpcap.org/install/default.htm>

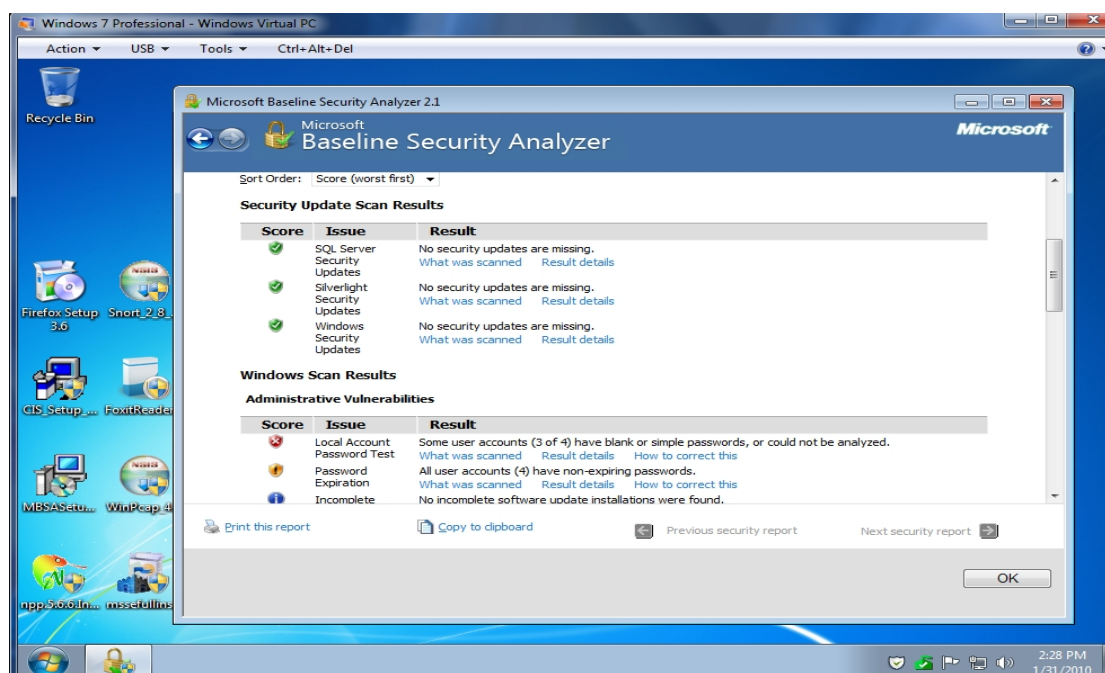
Snort 2.8.5.2

[http://dl.snort.org/snort-current/Snort\\_2\\_8\\_5\\_2\\_Installer.exe](http://dl.snort.org/snort-current/Snort_2_8_5_2_Installer.exe)

Oinkmaster 2.0

<http://sourceforge.net/projects/oinkmaster/files/oinkmaster/2.0/oinkmaster-2.0.tar.gz/download>

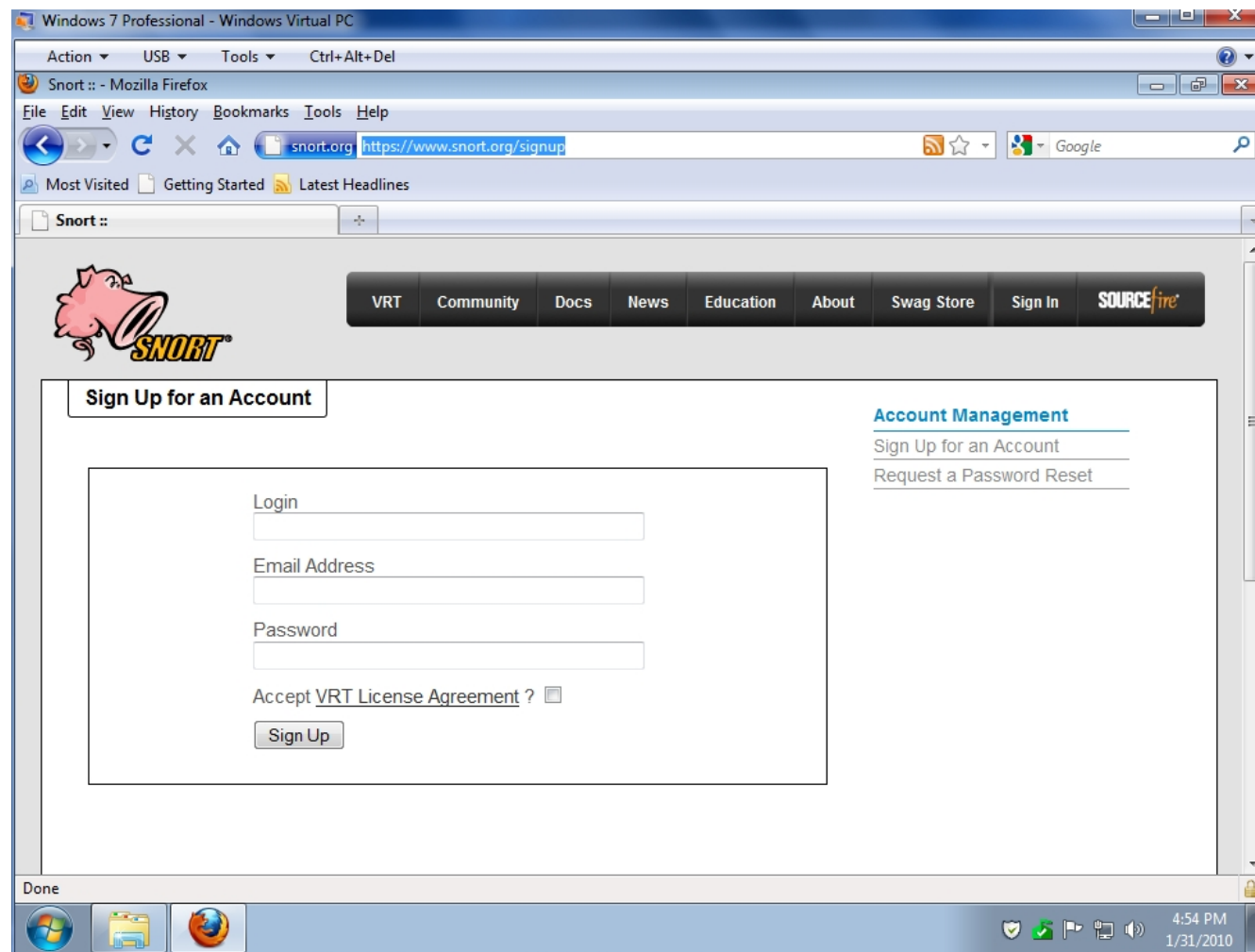
- 1) After installing the Operating System and downloading all of the software listed above, I would advise both copying of the software to an external drive as well as creating a System Restore Point. This will shorten reinstall times should something not work as expected.
- 2) With the exception of Oinkmaster, you should now systematically install all of the downloaded software. Note that you may substitute some of the software (ex. Use IE instead of Firefox or skip installing the Foxit Reader), however some software such as WinPcap are integral to running Snort in the method used in this guide.
  - a) When installing the software, take note of the following:
    - 1) I would recommend using the default options and allow the applicable components to be run as a service/at startup.
    - 2) When installing Kiwi, uncheck the Web Access, as it will expire after 30 days.
    - 3) During the installation and running of software, the COMODO Firewall will be triggered multiple times and you will need to Allow Kiwi access.
  - b) I would now ensure that the Operating System and all software are patched and updated. I would also run the Microsoft Baseline Security Analyzer and correct any anomalies as you see fit. It is also recommended that you search the Internet for guides on hardening the Windows 7 Operating System.



## Acquiring updated Rules and an Oinkcode:

If you haven't already done so, you will need to become a Registered member on the Snort website. This is needed in order to download and use the Sourcefire VRT Certified Rules. Snort will not be operating up to date without them (and Oinkmaster will not work).

<https://www.snort.org/signup>



After you have created an account, log in to the Snort website and copy your personalized Oinkcode (to be used by Oinkmaster). Also, download the Sourcefire VRT Certified Rules (registered-user release) – be sure to grab the “snapshot” version, as shown below.

Snort :: rules - Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://www.snort.org/start/rules

Most Visited Getting Started Latest Headlines

### Snort :: rules

Sourcefire vulnerability Research Team (VRT) Rules are the official rules of snort.org. Each rule is developed and tested using the same rigorous standards the VRT uses for Sourcefire customers. These rules are distributed under the VRT Certified Rules License Agreement. This license agreement allows you to study and modify VRT rules but restricts commercial redistribution. There are two ways Snort users can obtain these rules:

- Subscribers: Real-time access to VRT Certified Rules Updates requires a paid subscription.
- Registered Users: **Registered users** of Snort.org are able to download and use VRT rules free of charge 30 days after their initial release date

### Keeping your Snort Rules Updated

Users may opt to manually download and updates rules files, however most Snort users automate the process using Oinkmaster, an open source perl script. If you plan on using Oinkmaster to manage VRT Rules updates you'll need to login to snort.org and generate an Oinkcode to properly configure Oinkmaster.

**Click here** to download the latest VRT Rules.

For more information on the Sourcefire VRT visit: [VRT](#)

**Previous:** [Download Snort](#) | **Next:** [Documentation](#)

SHARE

Snort :: snort-rules - Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://www.snort.org/snort-rules

Most Visited Getting Started Latest Headlines

### Snort :: snort-rules

the most up to date Sourcefire VRT Certified Rules available. Real-time access requires a paid, annual subscription. For more information on a subscription [click here](#), or to purchase a VRT Rules subscription online visit the [VRT Store](#)

[advisory](#) | [change log](#)

Current	
<a href="#">snortrules-snapshot-CURRENT_s.tar.gz</a>	<a href="#">MD5</a> - 18 Jan, 2010

Snort v2.8	
<a href="#">snortrules-snapshot-2.8_s.tar.gz</a>	<a href="#">MD5</a> - 28 Jan, 2010

### Sourcefire VRT Certified Rules - The Official Snort Ruleset (registered-user release)

The Registered User Release makes Sourcefire VRT Certified Rules updates available to registered users of Snort.org free of charge 30-days after the initial release to subscribers.

[advisory](#) | [change log](#)

Current	
<a href="#">snortrules-snapshot-CURRENT.tar.gz</a>	<a href="#">MD5</a> - 15 Dec, 2009

Snort v2.8	
<a href="#">snortrules-snapshot-2.8.tar.gz</a>	<a href="#">MD5</a> - 15 Dec, 2009

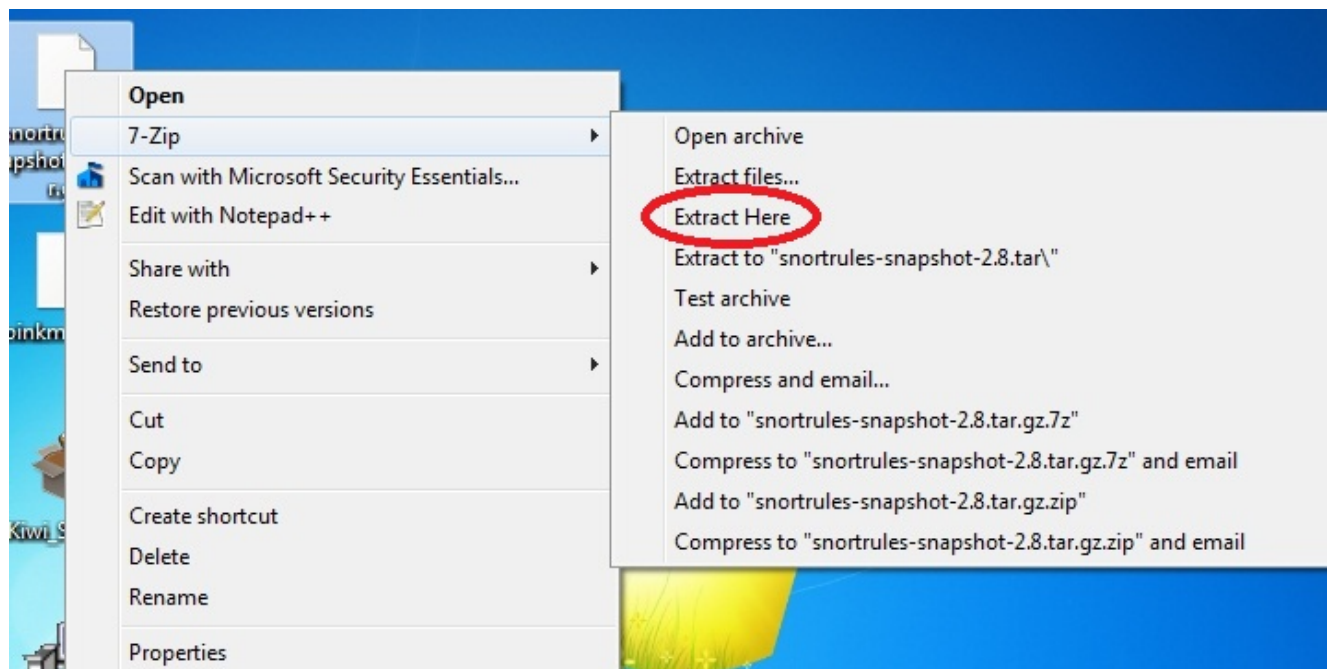
[Download Policy](#)



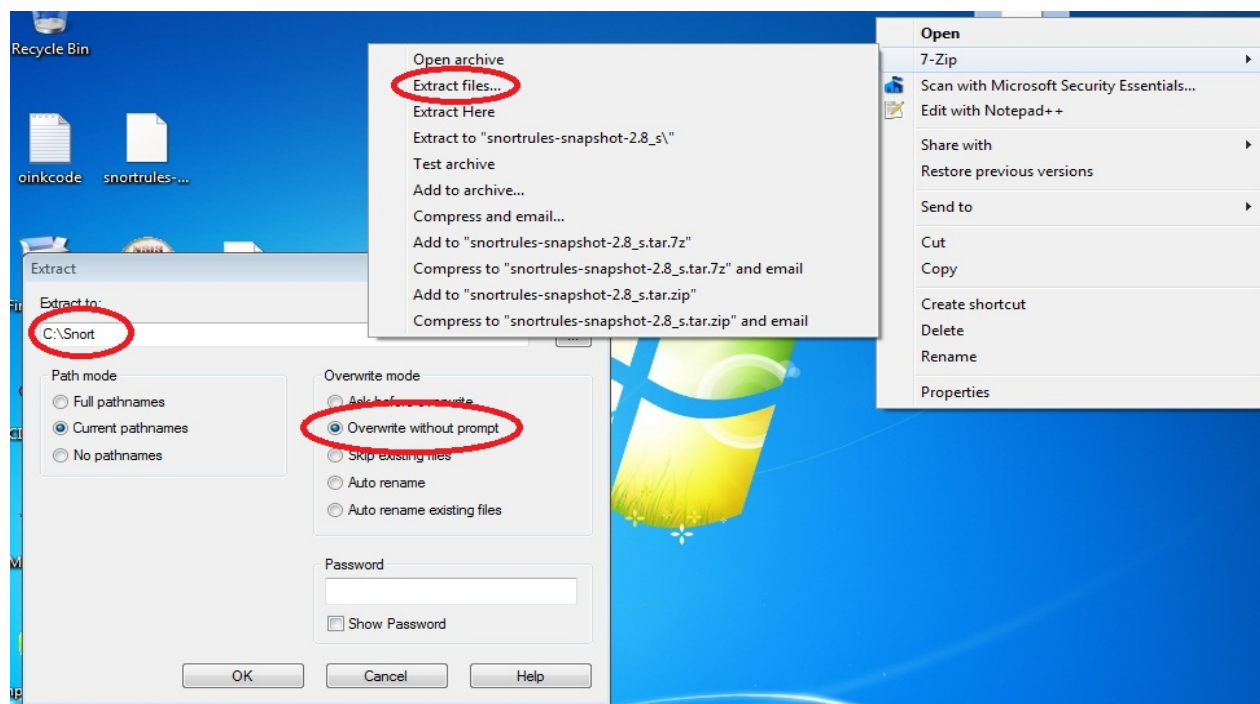
Applying our updated Rules:

**\*\*BEFORE APPLYING THESE UPDATED RULES, COPY THE FILE  
C:\SNORT\ETC\SNORT.CONF TO YOUR DESKTOP\*\***

Right-click on the snortrules-snapshot-2.8.tar.gz file that we downloaded and choose “Extract Here”:



Right-click on the newly extracted file (snortrules-snapshot-2.8\_s.tar) and choose “Extract files...”. Change the Path to C:\Snort and check “Overwrite without prompt”:



## Configuring the snort.conf File:

Edit the file you copied to your Desktop (snort.conf) with Notepad++ and perform the following:

Change lines 120-121 to read:

```
120 var RULE_PATH c:\snort\rules
121 var PREPROC_RULE_PATH c:\snort\preproc_rules
```

Change line 204 to read:

```
204 dynamicpreprocessor directory C:\Snort\lib\snort_dynamicpreprocessor
```

Change line 214 to read:

```
214 dynamicengine C:\Snort\lib\snort_dynamicengine\sf_engine.dll
```

Change line 324 to read:

```
324 dynamicengine C:\Snort\lib\snort_dynamicengine\sf_engine.dll
```

Change line 683 to read:

```
683 output alert_syslog: host=127.0.0.1:514, LOG_AUTH LOG_ALERT
```

Change line 771 to read:

```
771 include c:\snort\etc\classification.config
```

Change line 779 to read:

```
779 include c:\snort\etc\reference.config
```

Change (uncomment) line 863 to read:

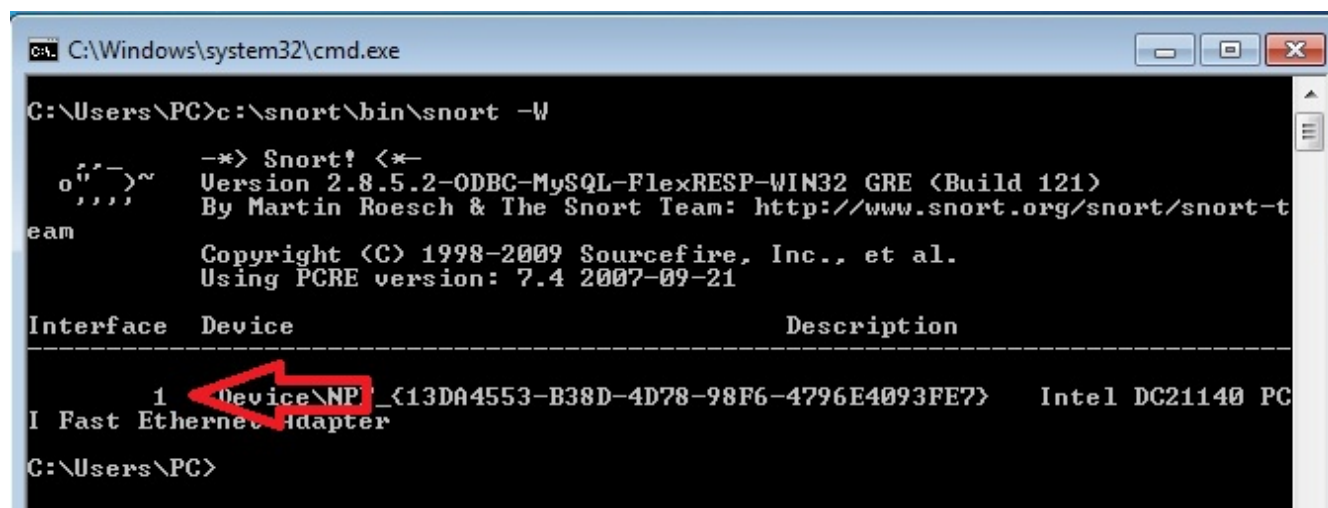
```
863 include $RULE_PATH/icmp-info.rules
```

Now save and close this file. Copy this file to c:\snort\etc and overwrite the existing one.

Keep in mind that you will need to tailor this file (especially the rule set section) and any other configuration files to further suit your IDS/IPS needs.

## Verifying Snort Operation:

Open a Command Prompt and run `c:\snort\bin\snort -W` (be sure to use a capital “W”)



```
C:\Windows\system32\cmd.exe

C:\Users\PC>c:\snort\bin\snort -W

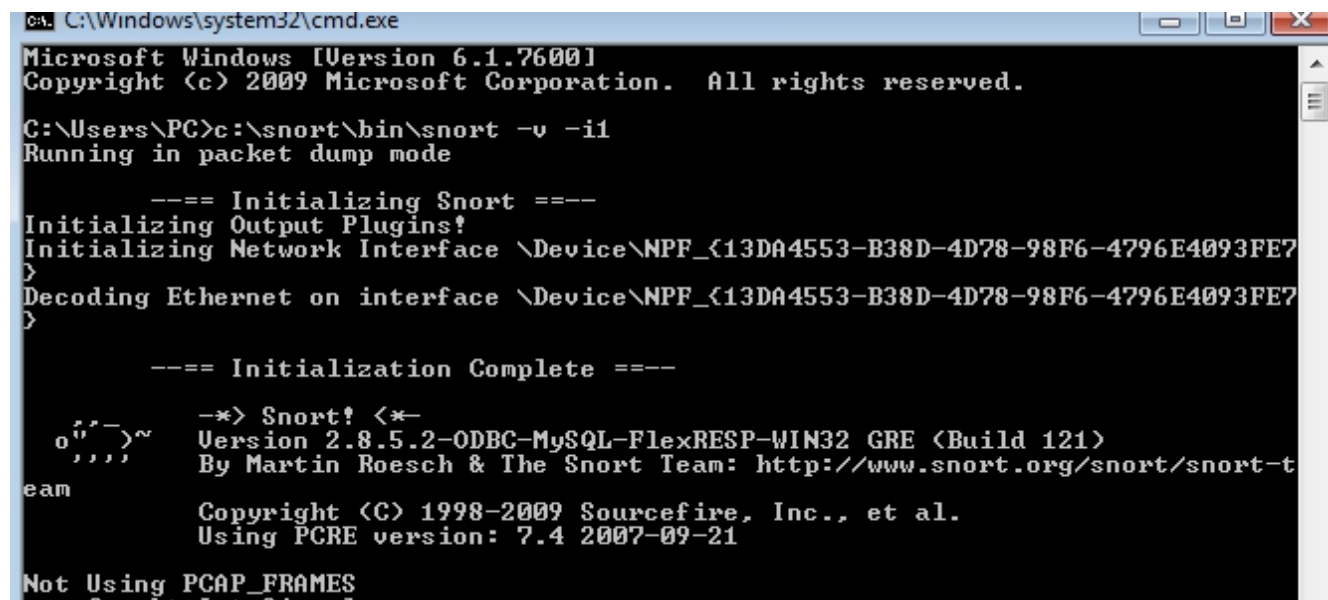
-*> Snort! <*-
Version 2.8.5.2-ODBC-MySQL-FlexRESP-WIN32 GRE <Build 121>
By Martin Roesch & The Snort Team: http://www.snort.org/snort/snort-team
Copyright <C> 1998-2009 Sourcefire, Inc., et al.
Using PCRE version: 7.4 2007-09-21

Interface  Device                                     Description
-----
1 \Device\NPF_{13DA4553-B38D-4D78-98F6-4796E4093FE7} Intel DC21140 PCI Fast Ethernet Adapter

C:\Users\PC>
```

Now run `c:\snort\bin\snort -v -iX` (replace X with your Device Interface number found from running the previous line)

After a couple of seconds you will see “Not Using PCAP\_FRAMES”. Snort is now running and will alert you if a Rule is triggered. If you have suspicious network traffic going across your interface, the command prompt window will rapidly scroll text.



```
C:\Windows\system32\cmd.exe

Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\PC>c:\snort\bin\snort -v -i1
Running in packet dump mode

==== Initializing Snort ====
Initializing Output Plugins!
Initializing Network Interface \Device\NPF_{13DA4553-B38D-4D78-98F6-4796E4093FE7}
Decoding Ethernet on interface \Device\NPF_{13DA4553-B38D-4D78-98F6-4796E4093FE7}

==== Initialization Complete ====

-*> Snort! <*-
Version 2.8.5.2-ODBC-MySQL-FlexRESP-WIN32 GRE <Build 121>
By Martin Roesch & The Snort Team: http://www.snort.org/snort/snort-team
Copyright <C> 1998-2009 Sourcefire, Inc., et al.
Using PCRE version: 7.4 2007-09-21

Not Using PCAP_FRAMES
```

While still leaving the Snort command prompt window open, launch a second command prompt window. From the new window, run the command `ping google.com`. If it hasn't occurred already, this ping command will trigger a Snort alert!

```

C:\Windows\system32\cmd.exe
02/01-19:42:25.895725 192.168.2.25:1900 -> 239.255.255.250:1900
UDP TTL:1 TOS:0x0 ID:32311 IpLen:20 DgmLen:528
Len: 500
=====
02/01-19:42:26.403466 192.168.2.26 -> 72.14.204.99
ICMP TTL:128 TOS:0x0 ID:648 IpLen:20 DgmLen:60
Type:8 Code:0 ID:1 Seq:11 ECHO
=====
02/01-19:42:26.463144 72.14.204.99 -> 192.168.2.26
ICMP TTL:51 TOS:0x0 ID:19385 IpLen:20 DgmLen:60
Type:0 Code:0 ID:1 Seq:11 ECHO REPLY
=====
02/01-19:42:27.379596 192.168.2.26 -> 72.14.204.99
ICMP TTL:128 TOS:0x0 ID:649 IpLen:20 DgmLen:60
Type:8 Code:0 ID:1 Seq:12 ECHO
=====
02/01-19:42:27.422801 72.14.204.99 -> 192.168.2.26
ICMP TTL:51 TOS:0x0 ID:19386 IpLen:20 DgmLen:60
Type:0 Code:0 ID:1 Seq:12 ECHO REPLY
=====

C:\Windows\system32\cmd.exe
C:\Users\PC>ping google.com

Pinging google.com [72.14.204.99] with 32 bytes of data:
Reply from 72.14.204.99: bytes=32 time=48ms TTL=51
Reply from 72.14.204.99: bytes=32 time=41ms TTL=51
Reply from 72.14.204.99: bytes=32 time=59ms TTL=51
Reply from 72.14.204.99: bytes=32 time=43ms TTL=51

Ping statistics for 72.14.204.99:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 41ms, Maximum = 59ms, Average = 47ms

C:\Users\PC>_
  
```

You can now close both command prompt windows, as we have verified that Snort is installed and alerting correctly in verbose mode. To test that our configuration file is correct, open a new command prompt window and type:

```
c:\snort\bin\snort -iX -s -l c:\snort\log\ -c c:\snort\etc\snort.conf (replace X with your Device Interface number)
```

If you have correctly entered all information, you should receive a graceful exit such as the screen shot below. If you receive a fatal error, you should first verify that you have typed all modifications correctly into the `snort.conf` file and then search through the file for entries matching your fatal error message.



```
Administrator: Command Prompt
Transitions      : 1.46M
-----
--== Initialization Complete ==--

-*> Snort! <*-
o''~>~
'''~>~
eam
Version 2.8.5.2-ODBC-MySQL-FlexRESP-WIN32 GRE <Build 121>
By Martin Roesch & The Snort Team: http://www.snort.org/snort/snort-team

Copyright (C) 1998-2009 Sourcefire, Inc., et al.
Using PCRE version: 7.4 2007-09-21

Rules Engine: SF_SNORT_DETECTION_ENGINE Version 1.11 <Build 17>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 3>
Preprocessor Object: SF_SSH Version 1.1 <Build 2>
Preprocessor Object: SF_SMTP Version 1.1 <Build 8>
Preprocessor Object: SF_FIPIELNET Version 1.2 <Build 12>
Preprocessor Object: SF_DNS Version 1.1 <Build 3>
Preprocessor Object: SF_DCERPC Version 1.1 <Build 5>
Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 2>

Snort successfully loaded all rules and checked all rule chains!
Snort exiting

C:\Windows\system32>
```

Verifying Kiwi Operation and Tying it to Snort:

Now open the Kiwi Syslog Server Console and type CTRL-T (you should see a test message appear, which indicates Kiwi is working)



Using Notepad++, create a file on your Desktop called Snortstart.bat and place the following line of code in it:

```
c:\snort\bin\snort -iX -s -l c:\snort\log\ -c c:\snort\etc\snort.conf (replace X with your Device Interface number)
```

Also create a shortcut on your Desktop for the Kiwi Syslog Server Console

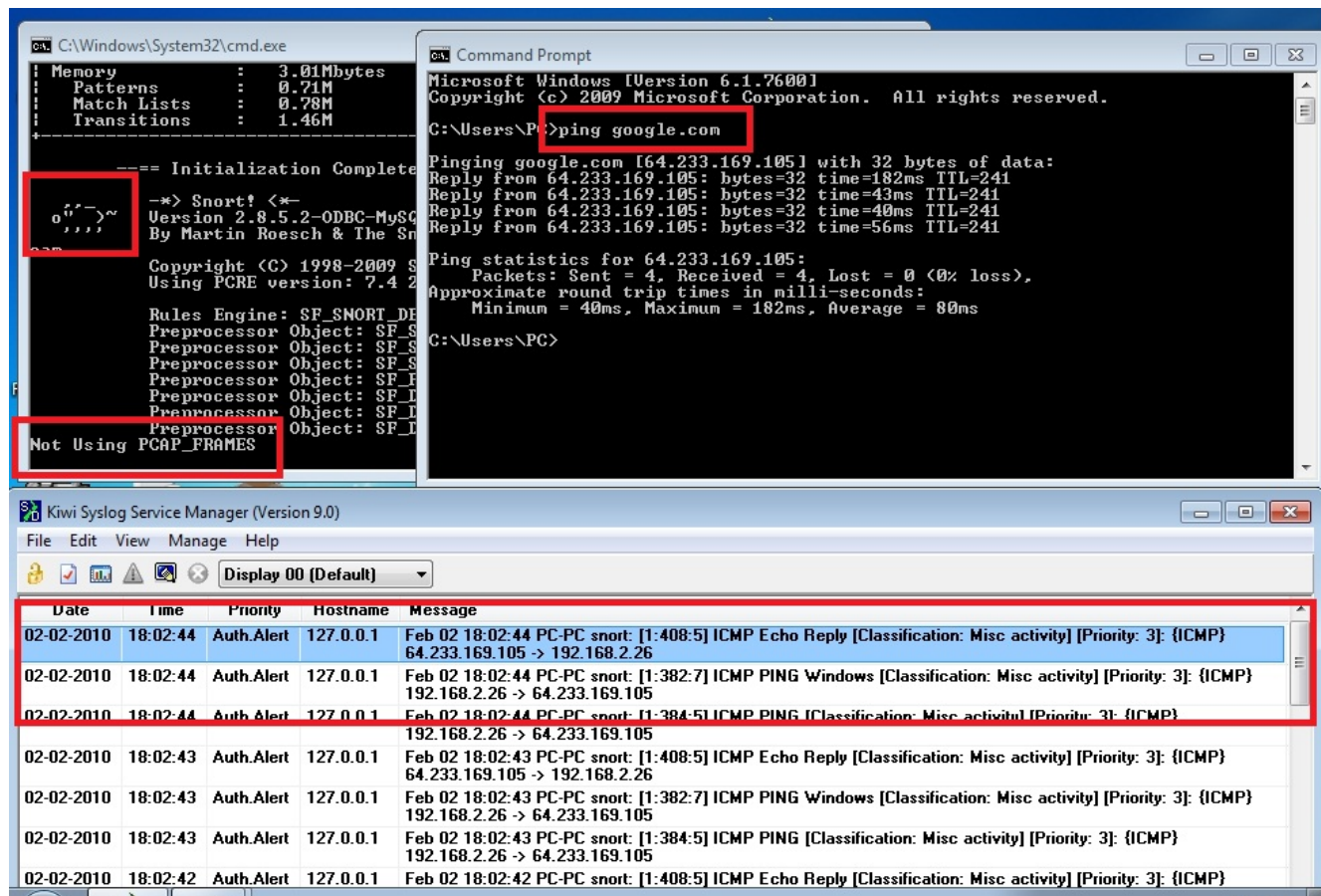
Open the Kiwi Syslog Server Console (if it isn't already)

Now right-click and run Snortstart.bat as an Administrator. Wait (about thirty seconds) until you see the familiar line "Not Using PCAP\_FRAMES" at the end.

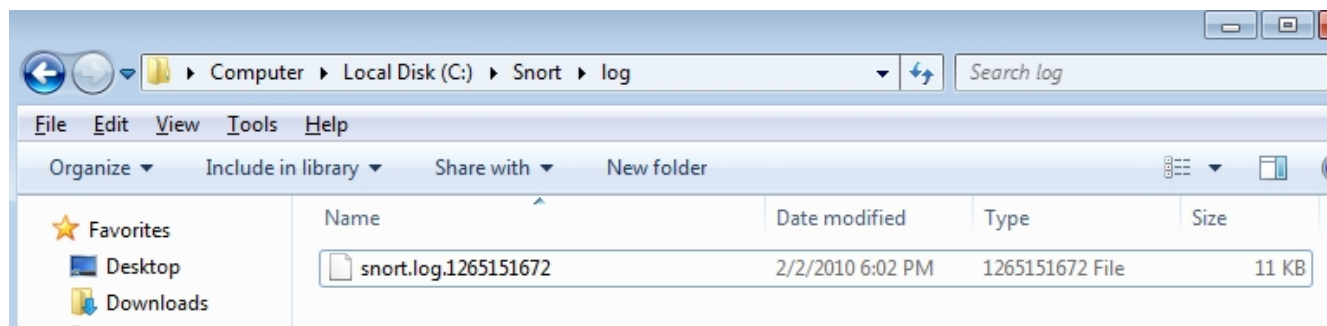
Finally, open another command prompt window and run: ping google.com

and.....

At this point you should see the Snort Alert outputting into Kiwi!!!!



Note that the reason why we have to run our batch file as an Administrator is that, in our current configuration, we need to maintain rights to not only output our alerts to Kiwi, but to write them to a log file.



At this point we have successfully installed Snort and have our Alerts being output to two sources. Our final step will be to configure Oinkmaster to help us update and manage our Rules.

## Configuring Oinkmaster and Verifying its Operation:

Right-click on the oinkmaster-2.0.tar.gz file that we downloaded and choose “Extract Here”

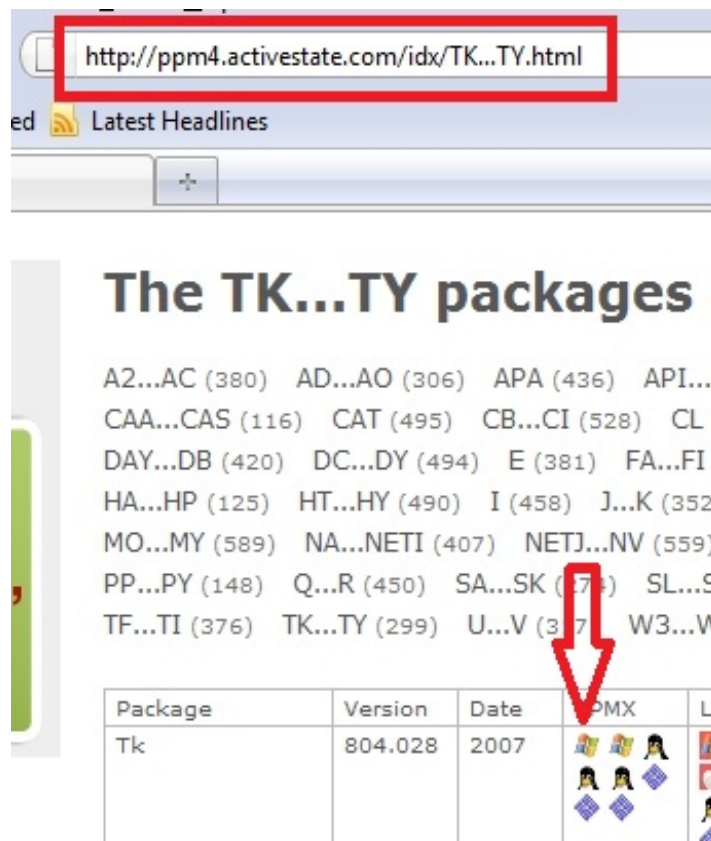
Right-click on this new file (oinkmaster-2.0.tar) and choose “Extract Here”

Now we have a new folder called oinkmaster-2.0. Move this new folder into c:\snort

Go to c:\snort and create a folder named: temp

Go to c:\snort\oinkmaster-2.0\contrib and copy the oinkgui file to your Desktop. Rename this file to: Update Snort Rules

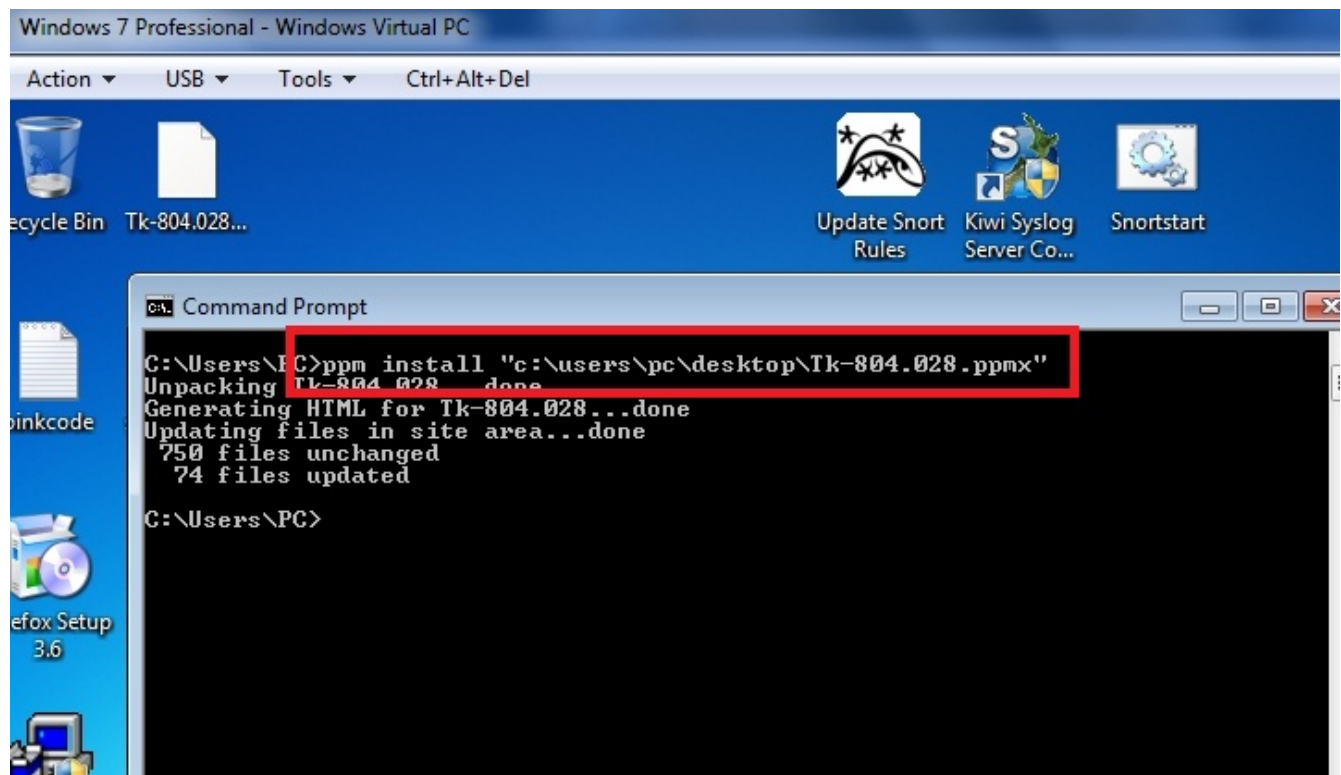
Now we have an additional module we need to download and install:



The screenshot shows a web browser window with the URL <http://ppm4.activestate.com/idx/TK...TY.html> highlighted in a red box. Below the URL bar, the page title is "The TK...TY packages". The page content displays a list of packages with their respective counts in parentheses: A2...AC (380), AD...AO (306), APA (436), API.../ (436), CAA...CAS (116), CAT (495), CB...CI (528), CL (495), DAY...DB (420), DC...DY (494), E (381), FA...FI (494), HA...HP (125), HT...HY (490), I (458), J...K (352), MO...MY (589), NA...NETI (407), NETJ...NV (559), PP...PY (148), Q...R (450), SA...SK (174), SL...S (494), TF...TI (376), TK...TY (299), U...V (377), W3...W (494). A red arrow points to the TK...TY package. Below the list is a table with the following columns: Package, Version, Date, PMX, and Location. The first row of the table shows the TK package with version 804.028 and date 2007. The PMX column contains icons representing different package managers or tools.

Package	Version	Date	PMX	Location
Tk	804.028	2007	Icons	

Once the file has been downloaded, open a command prompt window and type the line as shown below (note that your path name might be different. Once the installation has been complete, you can close the command prompt window.

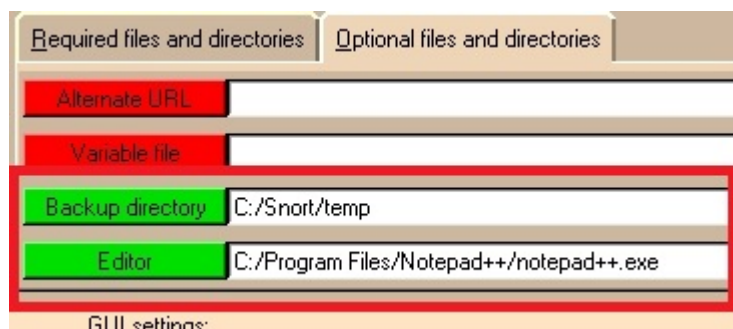
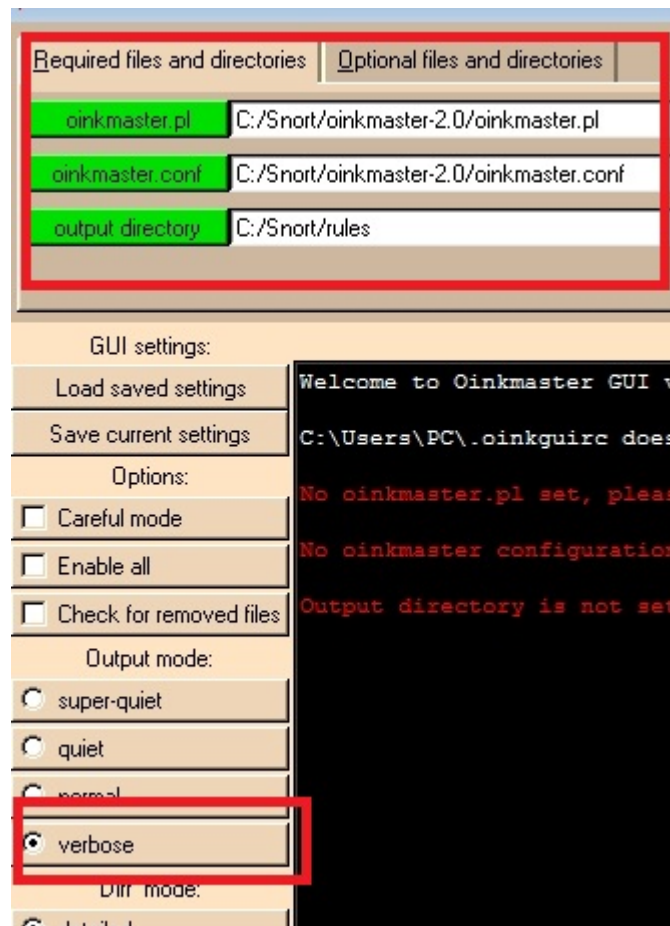


The screenshot shows a Windows 7 Professional desktop environment within a virtual PC. The desktop background is blue. In the top-left corner, there is a taskbar with icons for Recycle Bin, a document named 'Tk-804.028...', and a folder named 'pinkcode'. In the top-right corner, there are three application icons: 'Update Snort Rules', 'Kiwi Syslog Server Co...', and 'Snortstart'. A Command Prompt window is open in the center, displaying the following text:

```
C:\Users\PC>ppm install "c:\users\pc\desktop\Tk-804.028.ppmx"
Unpacking Tk-804.028...done
Generating HTML for Tk-804.028...done
Updating files in site area...done
750 files unchanged
74 files updated
C:\Users\PC>
```

The command prompt window has a red rectangular highlight around the command line: `ppm install "c:\users\pc\desktop\Tk-804.028.ppmx"`.

Now double-click on our Update Snort Rules file we have on the desktop and configure Oinkmaster to match the screen shots shown:

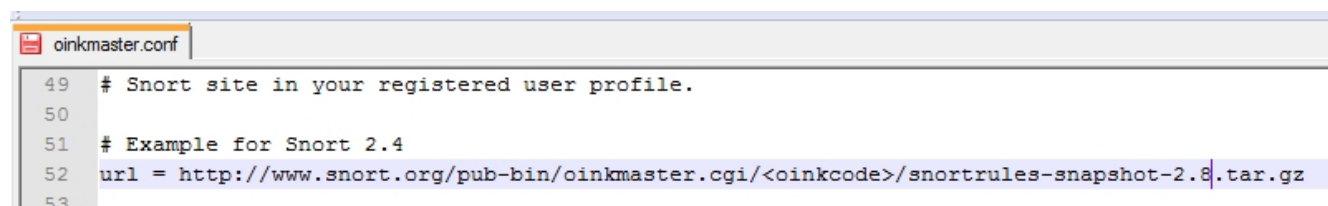


Note that your “Editor” path may be different than that shown.

Now go back to the “Required files and directories” tab and click “Edit” (to the right of the oinkmaster.conf file entry).



Change line 52 to read:



```
49 # Snort site in your registered user profile.
50
51 # Example for Snort 2.4
52 url = http://www.snort.org/pub-bin/oinkmaster.cgi/<oinkcode>/snortrules-snapshot-2.8.tar.gz
53
```

Where <oinkcode> is equal to the personal Oinkcode you downloaded from Snort.org earlier in this guide.

Now save your oinkmaster.conf file and close Notepad++

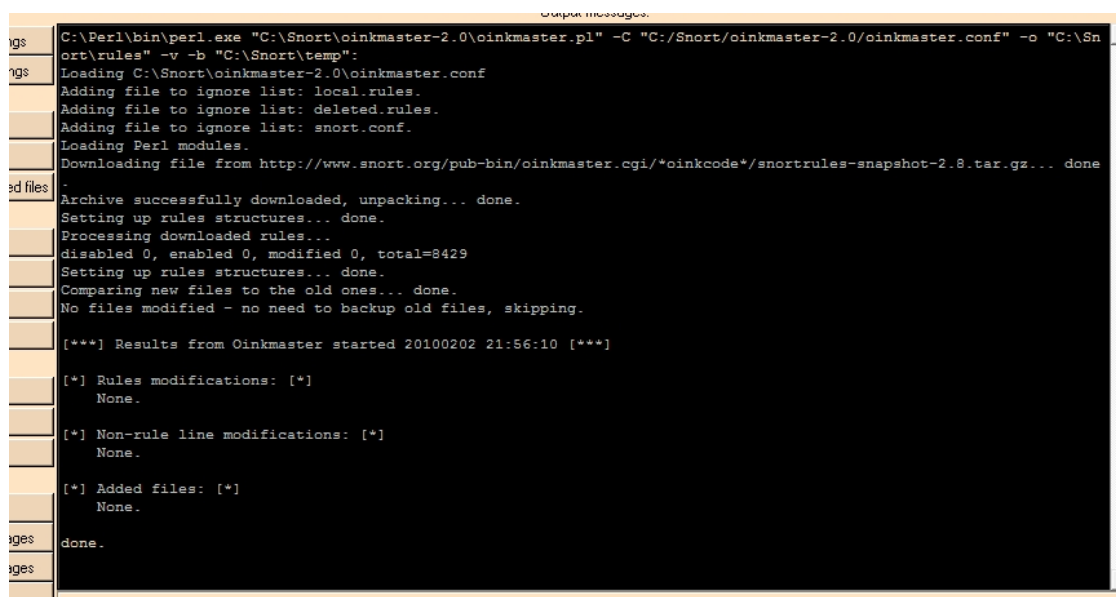
You are now back at the main Oinkmaster GUI page

Click “Save current settings”

Click “Update rules!”

After a few minutes of watching the rule update process, it will read: done.

Click “Exit” to close out of the Oinkmaster GUI.



```
C:\Perl\bin\perl.exe "C:\Snort\oinkmaster-2.0\oinkmaster.pl" -C "C:\Snort\oinkmaster-2.0\oinkmaster.conf" -o "C:\Sn
ort\rules" -v -b "C:\Snort\temp":
Loading C:\Snort\oinkmaster-2.0\oinkmaster.conf
Adding file to ignore list: local.rules.
Adding file to ignore list: deleted.rules.
Adding file to ignore list: snort.conf.
Loading Perl modules.
Downloading file from http://www.snort.org/pub-bin/oinkmaster.cgi/*oinkcode*/snortrules-snapshot-2.8.tar.gz... done
Archive successfully downloaded, unpacking... done.
Setting up rules structures... done.
Processing downloaded rules...
disabled 0, enabled 0, modified 0, total=8429
Setting up rules structures... done.
Comparing new files to the old ones... done.
No files modified - no need to backup old files, skipping.

[***] Results from Oinkmaster started 20100202 21:56:10 [***]

[*] Rules modifications: [*]
    None.

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

[*] Added files: [*]
    None.

done.
```

**\*\*REMEMBER THAT EVERY TIME YOU UPDATE THE RULES, YOU WILL NEED TO STOP AND THEN RESTART SNORT FOR THE NEW RULES TO TAKE EFFECT\*\***

Thanks again and keep the questions and comments coming!

-Kasey