**[Defending your network with Snort for Windows](https://ttcshelbyville.wordpress.com/2014/03/30/defending-your-network-with-snort-for-windows/)**

Posted on [Sunday, March 30, 2014 7:23 am](https://ttcshelbyville.wordpress.com/2014/03/30/defending-your-network-with-snort-for-windows/)by [TCAT Shelbyville IT Department](https://ttcshelbyville.wordpress.com/author/ttcshelbyville/)

[](https://ttcshelbyville.files.wordpress.com/2014/03/snortlogo.jpg)  
When you hear about Snort, the De facto of Intrusion Detection Systems, you think of Linux.  Snort offers a Windows setup and signatures that can be used with any operating system.

Snort should be a dedicated computer in your network.  This computer’s logs should be reviewed often to see malicious activities on your network.

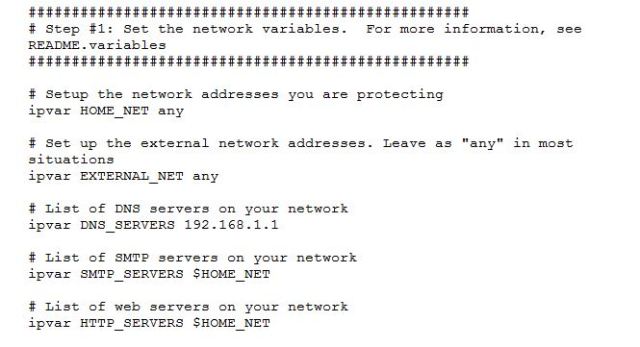
Steps to install Snort on Windows :  
1. Download Snort from the Snort.org website. (<http://www.snort.org/snort-downloads>)  
2. Download Rules from [here](https://www.snort.org/snort-rules). You must register to get the rules. (You should download these often)  
3. Double click on the .exe to install snort.  This will install snort in the “C:\Snort” folder.  
It is important to have [WinPcap](https://www.winpcap.org/install/" \t "_blank)installed  
4. Extract the Rules file. You will need WinRAR for the .gz file.  
5. Copy all files from the “rules” folder of the extracted folder.  Now paste the rules into “C:\Snort\rules” folder.  
6. Copy “snort.conf” file from the “etc” folder of the extracted folder.  You must paste it into “C:\Snort\etc” folder. Overwrite any      existing file.  Remember if you modify your snort.conf file and download a new file, you must modify it for Snort to work.  
7. Open a command prompt (cmd.exe) and navigate to folder “C:\Snort\bin” folder. ( at the Prompt, type cd\snort\bin)  
8. To start (execute) snort in sniffer mode use following command:  
snort -dev -i 3  
-i indicates the interface number.  You must pick the correct interface number.  In my case, it is 3.  
 -dev is used to run snort to capture packets on your network.

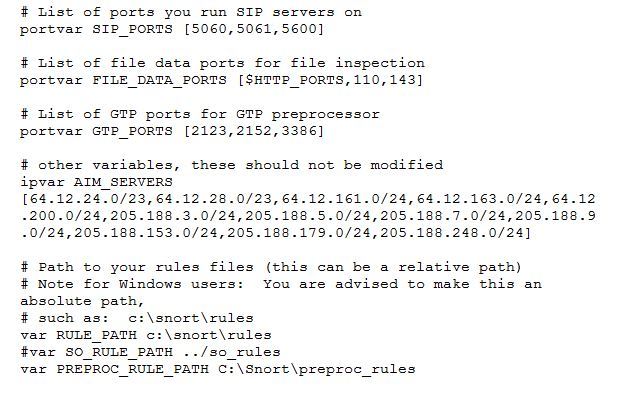
To check the interface list,  use following command:  
 snort   -W  
[](https://ttcshelbyville.files.wordpress.com/2014/03/finding-an-interface.jpg)

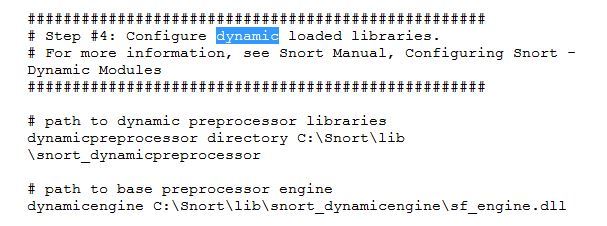
You can tell which interface to use by looking at the Index number and finding Microsoft.  As you can see in the above example, the other interfaces are for VMWare.  My interface is 3.

9. To run snort in IDS mode, you will need to configure the file “snort.conf” according to your network environment.  
10. To specify the network address that you want to protect in snort.conf file, look for the following line.  
var HOME\_NET 192.168.1.0/24  (You will normally see any here)  
11. You may also want to set the addresses of DNS\_SERVERS, if you have some on your network.

Example:

[](https://ttcshelbyville.files.wordpress.com/2014/03/example-snort.jpg)  
12. Change the RULE\_PATH variable to the path of rules folder.  
 var RULE\_PATH c:\snort\rules

[](https://ttcshelbyville.files.wordpress.com/2014/03/path-to-rules.jpg)  
13. Change the path of all library files with the name and path on your system. and you must change the path    of snort\_dynamicpreprocessorvariable.  
C:\Snort\lib\snort\_dynamiccpreprocessor  
You need to do this to all library files in the “C:\Snort\lib” folder. The old path might be: “/usr/local/lib/…”. you will need to    replace that path with your system path.  Using C:\Snort\lib  
14. Change the path of the “dynamicengine” variable value in the “snort.conf” file..  
Example:  
 dynamicengine C:\Snort\lib\snort\_dynamicengine\sf\_engine.dll

[](https://ttcshelbyville.files.wordpress.com/2014/03/libraries.jpg)

15 Add the paths for “include classification.config” and “include reference.config” files.  
  include c:\snort\etc\classification.config  
include c:\snort\etc\reference.config  
16. Remove the comment (#) on the line to allow ICMP rules, if it is  commented with a #.  
 include $RULE\_PATH/icmp.rules  
17. You can also remove the comment of ICMP-info rules comment, if it is commented.  
 include $RULE\_PATH/icmp-info.rules  
18. To add log files to store alerts generated by snort,  search for the “output log” test in snort.conf and add the following line:  
output alert\_fast: snort-alerts.ids  
19.  Comment (add a #) the  whitelist $WHITE\_LIST\_PATH/white\_list.rules and the blacklist

Change the nested\_ip inner , \  to nested\_ip inner #, \  
20. Comment out (#) following lines:  
#preprocessor normalize\_ip4  
#preprocessor normalize\_tcp: ips ecn stream  
#preprocessor normalize\_icmp4  
#preprocessor normalize\_ip6  
#preprocessor normalize\_icmp6

21. Save the “snort.conf” file.  
22. To start snort in IDS mode, run the following command:

snort -c c:\snort\etc\snort.conf -l c:\snort\log -i 3  
(Note: 3 is used for my interface card)

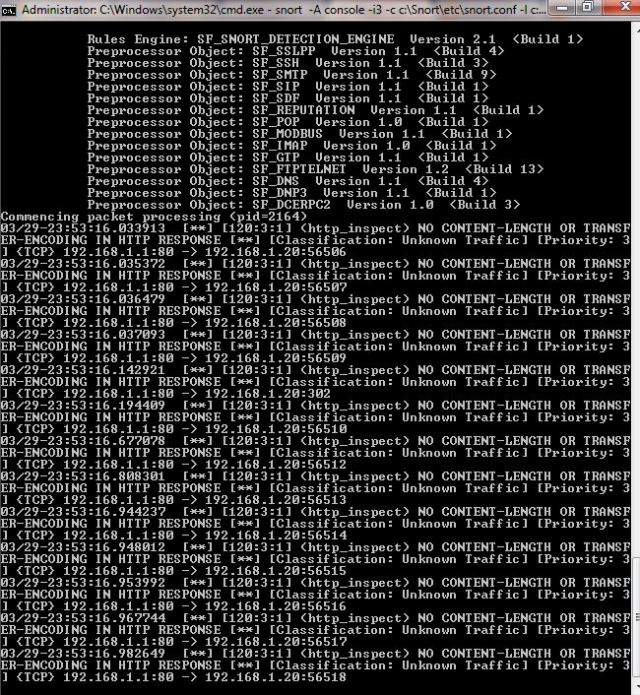
If a log is created, select the appropriate program to open it.  You can use WordPard or NotePad++ to read the file.

To generate Log files in ASCII mode, you can use following command while running snort in IDS mode:  
snort -A console -i3 -c c:\Snort\etc\snort.conf -l c:\Snort\log -K ascii

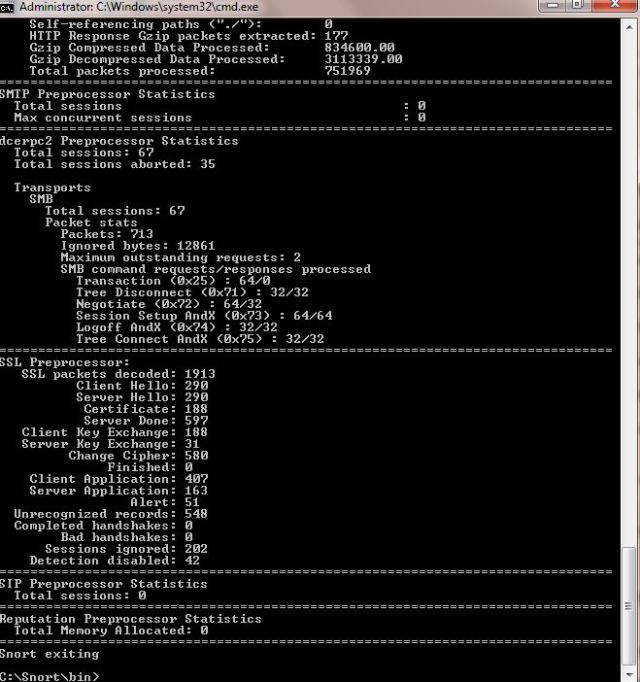
23. Scan the computer that is  running snort from another computer by using PING or NMap (ZenMap).

After scanning or during the scan you can check the snort-alerts.ids file in the log folder to insure it is logging properly.  You will see IP address folders appear.

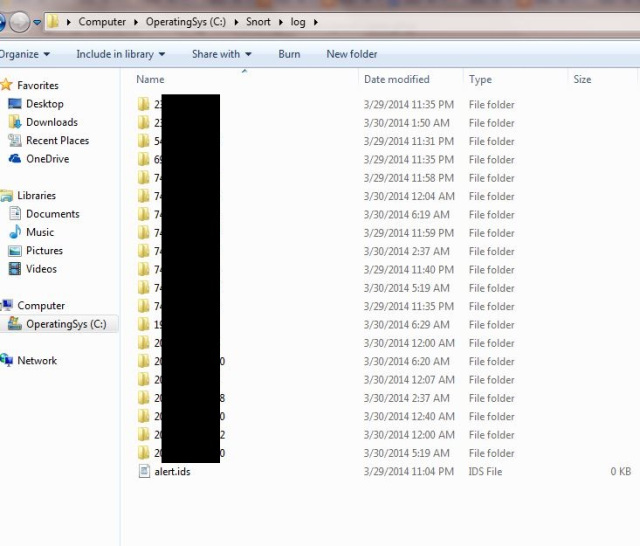
Snort monitoring traffic –

[](https://ttcshelbyville.files.wordpress.com/2014/03/traffic.jpg)

Snort’s detailed report when scanning has stopped –

[](https://ttcshelbyville.files.wordpress.com/2014/03/termination.jpg)

Log files –

[](https://ttcshelbyville.files.wordpress.com/2014/03/logs.jpg)