Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Snort Install on Win2000/XP with Acid, and MySQL

Snort is a lightweight Network Intrusion Detection System, capable of performing realtime traffic analysis and packet logging on IP networks."1 Snort spies on all of the packets going through a specific network that it is set up to monitor and alerts when it finds specific predefined patterns (defined in the Rules) that could be malicious. Snort works with many different operating systems and platforms. It can be used as a Packet Sniffer, Packet Logger or Network Intrusion Detection System. Snort is very a powerful, cu...

Copyright SANS Institute
Author Retains Full Rights

AD

Christina Neal
Version 1.3 GSEC

Snort Install on Win2000/XP with Acid, and MySQL

Overview

"Snort is a lightweight Network Intrusion Detection System, capable of performing real-time traffic analysis and packet logging on IP networks."[1] Snort spies on all of the packets going through a specific network that it is set up to monitor and alerts when it finds specific predefined patterns (defined in the Rules) that could be malicious. Snort works with many different operating systems and platforms. It can be used as a Packet Sniffer, Packet Logger or Network Intrusion Detection System. Snort is very a powerful, customizable, flexible and scalable tool because of its open-sourced nature. Best of all, Snort is free.

The purpose of this paper is to detail using Snort as a Network Intrusion Detection System. Unfortunately Snort is not just a simple executable file that one could click next all the way through. There are many different applications that need to be installed to make Snort run. This paper is designed with as much detail as possible to help "newbies" easily install and configure Snort 1.8.6 on Windows 2000/XP. Many Snort installation instructions are very arcane, they leave out important details, and do not explain exactly why certain things are being installed or configured a specific way. This document is intended for people with little technical experience. They will be able to successfully install Snort with little difficulty and understand the different steps along the way. These procedures are quite long and meticulous, but people with little or no Snort expertise have successfully tested them.

Important Information

Most Snort installation instructions recommend installing everything to the **C:** drive. However, many people prefer to install their OS to the **C:** drive exclusively and then install any applications to a different drive such as **E:**. I will detail installing everything to the **E:\.** WinZip 8.1 is used in this example to uncompress files.

Prepare to Download the Correct Files

Create a Temporary Directory, in this example we will create **E:\Snorttemp** to save all of the files that need to be downloaded. You may want to download the files into individual folders under the Snorttemp directory to organize the files.
Using a batch file similar to this would make this process easier:

```
E:
md snorttemp
```

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

```
cd snorttemp
md winzip
md snort
md WinPcap
md packetbuild
md mysql
md php
md phplot
md adodb
md acid
md runasservicefiles
md dbtools
md idscenter
```

Batch File Tips

- To create a batch file open Windows Explorer
- Click on the **C:** drive (or **D:** or **E:**)
- Click on File
- Click on New
- Click on Text Document
- Name the file maketempdir.bat

NOTE: To view the .bat extension and to make sure that the file isn't being saved as maketempdir.bat.txt click on **Tools** from the File menu, and then click on **Folder Options**. Click on the **View** tab. Under the advanced settings uncheck the box next to **Hide Extensions for Known File Types.** Click on **Apply**, then **OK**.

- Right click on the newly created file and choose **Edit**
- Copy and paste the example batch file from above to the file (this will save a lot of typing)
- Make any necessary drive letter changes within the file to match your environment (Choosing **Edit** on the **File** menu and then **Replace** is a quick way to replace **E:** with **D:** or **C**: all at once)
- Click on **File**, then **Save**
- Open the command prompt
- Navigate to where the maketempdir.bat is located
- Run maketempdir.bat
- View the command prompt window for any errors
- Browse to the newly create directory and subdirectories to verify that this operation was successful

<u>Download the Correct Files</u>

The following files are needed to make and entire Snort installation that uses MySql, and Acid. Explanations of the files and what they are used for will be found under the

© SANS Institute 2002, Author retains full rights.

installation notes for each individual application later in this document. Download and save each of the following files into their respective Snorttemp subdirectory:

Download WinZip 8.1 if needed:
http://www.winzip.com/linkdl.cgi?http://download.com.com/3405-20-871449.html
Download Snort 1.8.6 for MySql:
http://www.silicondefense.com/software/snort-win32/snort_1.8.6/Snort-1.8.6b105-Win32-MySQL-Static.zip
Download WinPcap 2.3:
http://WinPcap.polito.it/install/bin/WinPcap_2_3.exe (WinPcap is also included in the Libnet PacketBuild download)
Download PacketBuild1.2 (Libnet):
http://www.securitybugware.org/libnetnt/PacketBuild-1.2.zip
Download MySQL Shareware 3.23.49
http://www.mysql.com/downloads/download.php?file=Downloads/MySQL-3.23/mysql-3.23.49-win.zip
Download PHP 4.1.2:
http://www.php.net/do_download.php?download_file=php-4.1.2-Win32.zip
Download PHPLot 4.4.6:
http://prdownloads.sourceforge.net/phplot/phplot-4.4.6.tar.gz
Download ADODB 1.90:
http://phplens.com/lens/dl/adodb190.zip
Download ACID 0.9.6b21:
http://www.andrew.cmu.edu/~rdanyliw/snort/acid-0.9.6b21.tar.gz
Download Run As Service Files:
http://www.silicondefense.com/software/snort-win32/binaries/Service_Files.zip
Download DBTools:
http://www.dbtools.com.br/download.php

Libnet Install

"Libnet is an API (Application Programming Interface) to help with the construction and handling of network packets."[2] Libnet is a C library that can be used on many of today's architectures without needing to be rewritten for different the operating systems. Hackers use this library to construct network packets for spoofing and other exploits. The control of the packets that Libnet allows is also very useful for creating network security applications.

Here is how to install Libnet:

- Extract **PacketBuild-1.2.zip** to the **E:\Snorttemp\Packetbuild** temporary folder
- Use the command prompt to navigate to the folder to which the files were extracted
- Run **compiler.bat** from the command prompt

The compiler.bat sets up the environment and different variables to prepare the computer for the makefile.win step. An interesting thing to try before you run compiler.bat is to type in **Path** at the command prompt and press **Enter.** Take a

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

screen print or remember what it looks like. Then after running compiler.bat, type **Path** again and press enter. You should see a change.

Note: Compiling means rebuilding the actual executable program from its source code

- Move to the Libnet-1.0.2c directory
- Type:
  make -f makefile.win
- Press **Enter**

This file does the actual compiling, or building of the executable from the source code and then installs the program by copying the necessary dll's to the correct place. You should notice a file LibnetNT.dll in the (Systemroot)/System32 of the computer after following these steps to install Libnet.

WinPcap Install

"WinPcap is a Win32 port of libpcap (a widely used network programming API for capturing and sending network packets)."[3] The driver allows the ability to capture raw packets and send them to Win32 platforms. There are many tools that use WinPcap.

- Double click on the **WinPcap23.exe** to run the setup
- Click **Next**
- Click on **Yes** to agree to the license agreement
- Click **Next** on the information windows that says that WinPcap was correctly installed
- Click **Finish**
- Reboot the computer

To verify that WinPcap correctly installed check **Add/Remove Programs**. You can also search for **packet.dll** and **wpcap.dll** in the (systemroot)/system32 folder. Another avenue to check would be to click on **Start/Run** and type in **MSINFO32,** then press enter. This will bring up a system information screen. If you expand Software Environment then click on System Drivers you should see a driver named **NPF (NetGroup Packet Filter)**, which should have a status of 'Running'.

WinPcap doesn't always install correctly. Make sure that you are installing the correct version for the operating system. Windows XP needs version 2_3 or later. Before you try to install WinPcap, be sure that an older version of WinPcap is not already installed on the computer by checking Add/Remove Programs and by deleting the packet.dll and the wpcap.dll from the system. Occasionally, the dll's do install correctly, but the NPF service does not install which means that WinPcap isn't actually running. In order to force the service into being created, you will need to download the WinPcap Developers Pack from http://WinPcap.polito.it/install/bin/WPdpack_2_3.zip . After installing WinPcap, run TestApp.exe from the WPdpack\Examples\TestApp of the Development Pack download folder. Choose the adapter that you would like WinPcap to be bound to then press enter. You should see something similar to the following:

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

```
Packet length, captured portion: 60, 60
00000000 : 01 80 c2 00 00 00 00 d0 ba f1 8a d3 00 26 42 42 .Ç┬....╨╢±è╙.&BB
00000010 : 03 00 00 00 00 00 20 00 00 30 a3 a9 e0 11 00 00 ......  ..0ú┌α...
00000020 : 00 13 80 00 00 d0 ba f1 8a c1 80 21 01 00 14 00 ..Ç..╨╢±è┴Ç!....
00000030 : 02 00 0f 00 00 00 00 00 00 00 00 00            ............
```

To end the TestApp program press **<CTRL><C>.** If you open up **MSINFO32** now, the NPF service should installed.

Snort Install

Preparation

Unzip **Snort-1.8.6b105-Win32-MySQL-Static.zip** into a subdirectory by right clicking on the file, then clicking on **Winzip**, then clicking **Extract to**…

Note: The easiest way to do this is to extract everything within the temp folder to centralize all of the original files and then copy those directories into the destination working Snort directory. Most of the work is done for you with this batch file, but you MUST change the drive letter and directory name to match your particular setup.

Batch File Copy

The Snort directories and files can be copied manually or a batch file containing the following commands can be used:

E:
REM (This next line will create the working Snort directory)
md snort
REM (This next line will change to that Snort directory)
cd snort
REM (The following lines will create the necessary subfolders)
md rules
md php
md logs
md adodb
md phplot
REM (Change the **E:\Snorttemp** to a different directory is applicable)
cd **E:\Snorttemp\Snort-1.8.6b105-Win32-MySQL-Static.zip\snort**
REM (The following lines copy the necessary files to their destination directory)
copy *.rules **E:\Snort\Rules**
copy classification.config **E:\Snort\Rules**
copy snort.exe **E:\Snort**
copy snort.conf **E:\Snort**
cd contrib
copy create_MySQL **E:\Snort**

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

NOTE: Here, the Temporary Snort directory is named 'Snorttemp' and the files were extracted to a subdirectory named Snort-1.8.6b105-Win32-MySQL-Static\Snort.

Manual Copy

- To copy the files manually, create the following directories: **E:\Snort, E:\Snort\Rules, E:\Snort\Adodb, E:\Snort\PHP, E:\Snort\Logs and E:\Snort\PhpLot**
- Open the directory where Snort was extracted. Click on **View**, and then choose **Details**. Then Click on **View, Arrange Icons By…. Type**.
- Copy all of the Files that are the **Rules** type to **E:\Snort\Rules**
- Copy the **classification.config** file to **E:\Snort\Rules**
- Copy **snort.exe** to **E:\Snort**
- Copy **snort.conf** to **E:\Snort**
- Change to the Contrib directory
- Copy the **Create_MySQL** file to **E:\Snort**

MySQL Install

"MySQL is the world's most popular Open Source Database, designed for speed, power and precision in mission critical, heavy load use."[4] It also costs much less than Microsoft's SQL Server.

- Open the **MySQL-3.23.49-win.zip** with Winzip.
- Double click on **Setup.exe**
- Click on **OK** to extract the files to a temporary folder
- Click on **Next** at the **Welcome and Information** screen
- At the **Choose Destination Location** screen click on Browse and change the path to be **E:\MySQL**
- Click **OK** to create the folder and then click **Next**
- Choose the **Typical** Setup Type and click **Next**
- Click on **Finish** to complete the Setup
- Browse to **E:\MySQL\Bin** and double click on **WinMySQLAdmin.exe**
  This is the Admin tool for MySql. If nothing pops up on your desktop, check your short cut bar for an icon that looks like a traffic light. Right click on the traffic light and choose '**Show me'**.
- Click on the **my.ini** tab
  This is the main setup of MySql.
- Uncomment the **port=3306**. In this example we will use port 3306, but it is recommended that you change it to something different for security reasons since it is the default. This is the port that MySql runs on. You will see this port later in the Snort.conf, in the acid_conf.php, and in the DBTools configuration.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

- Change the **Username** and **Password** from Root and Sally to something else since this is the default and would be easily guessable if used. Here we will use Root and Sally as an example.
- Change the path of the following lines to be **E:\MySQL** instead of **C:**
  basedir=E:/MySQL
  Set this to the installation path of MySql
  datadir=e:/MySQL/data
  Set this to the location of the data directory
  Server=e:/MySQL/bin/MySQLd-nt.exe
  This specifies the correct version of MySql to start.
- Click on **Save Modifications**
- Click on **Create Icon on Start Menu**. This will make SQL start after every reboot.
- On the top right hand side of the WinMySQLAdmin window right click on the stoplight and click on **Win NT, Start this service** if the traffic light is not green. Red obviously means that the service is stopped. This is also where you can minimize the window to the task bar by clicking on **Hide me**.

DBTools Install

"DBTools is a WIN32 application to manage Database Servers."[5] This program is great for people who do not like command line. There aren't as many features as the Microsoft SQL GUI, but it's the same basic idea. It's very easy to use.

- Double Click on **Setup-1012.exe** that was downloaded from the DBTools website.
- Click **Next** to continue with the DBTools install
- Click **Yes** again
- Click **Next** on the license agreement
- Select the destination directory or type in the path **E:\Program Files\DBTools1012**
- Click **Next**
- Select a Program Group
- Click on **Install**
- Click on **Finish**

DBTools Configuration

- Open the DBTools Manager
- Click on **Server Manager** from Start, Programs…
- Click on **Server**
- Click on **Add**
- In the Properties box put in the **Server Name** (Anything will work, here we'll use 'Snort') and **Hostname** ('localhost' will work)
- Type in the **Port Number** that you will use, here we will use 3306

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

- Type in the **Username** which will be 'Root' because that is what we specified in the my.ini file of MySql
- Type in the **Password** which will be 'Sally' because we also specified that in the my.ini
- Leave the **Database** name blank- You are just configuring the server, the database will be created later
- Click on **Server**, then click on **Save**
- Click on **Link**
- Click on Test **Link**. This checks to see if there is a MySql server running on port 3306 that can be attached to using the name Root with the password Sally
- Click **OK** to the Connection Successful dialogue box
- Exit Server Manager
- Click **Yes** to Reload the Profile
- On the left hand side expand Snort
- Right Click on **Databases**
- Click on **Create**
- Type in 'Snort' for the database name
- Click **OK**-You just created the Snort database that Snort will log to
- Right Click on **Users**
- Click on **Create**
- Under the User Properties type in User ID 'Snort'- here we are using Snort as an example, but you should use something unique and hard to guess for better security
- Type in the Password 'snort' and confirm by typing it in again- again, this is an example, use something unique and not easily guessable
- For the Set privilege on Database use the pull down menu to choose Snort- this allows the user that we just created to have access to the database that we also created
- Click on **OK**
- Right click on the user Snort
- Click on **Privileges**
- **Select, Insert, Update** and **Delete** should already be checked for the Snort database
- Put a check in the **Create** box as well- this will allow Snort to log new alerts to the database
- Click on **Save**, then **OK**
- Click on **Close**

Close DBTools

Create MySQL Tables for Acid

The Acid console pulls information from the MySQL database. This process sets up the tables for Acid Web site to pull from.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

- Open a command Prompt
- From **E:\MySql\Bin**> type:

MySQL -u Snort -p Snort < E:\Snort\Create_MySql and press enter.

This command starts the MySql application using the username Snort and loads tables into the database Snort from a file named create_mysql.

MySQL- runs the application
-u specifies the user name
-p tells it to prompt for a password
Snort is the name of the database, not the password
< E:\Snort\Create_MySQL- tells it to load the tables from the create_MySQL file

NOTE: This is case sensitive so be careful. If you get an Access denied error check the case on the User name and Database name in DBTools. Also, if you type MySQL –h at the command prompt you will be taken to a help screen.

- Type in the **Password**, which is also case sensitive when prompted, and press **Enter**
- If there are no errors and you are brought back to a prompt then the command probably was successful
- Verify that the tables were successfully created by opening DBTools Manager
- Click on the Snort database. Expand databases. You should see many tables listed on the right hand side such as: Data, Detail, Encoding, Event etc.

Close the command prompt and DBTools.

<u>Snort.conf</u>

Snort.conf is the configuration file that tells Snort what to do when it starts up. There are four sections to the Snort.conf file. The four sections are: Network Variables for your network, Preprocessors, Output plug-ins, and Rule set customization. This file can be configured to monitor a specific IP, a set of IPs or a Network range. $HOME_NET is used for most of the Network Variables, but putting in the specific IP address could be beneficial. Putting in a specific IP Addresses is useful if you have a small network and know every Web Server, SMTP Server and/or SQL Server that you own and monitor. This will help form the snort rules more towards your specific network setup and will generate less false positives.

NOTE: Brackets are used when there is more than one IP Address or Network range specified.

The Snort.conf is best viewed when opened with WordPad. Right click on **E:\Snort\Snort.conf** while holding down the shift key, then choosing **Open with**, **Choose Program** and scroll down to **WordPad**, then click **OK**.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Network Variables

The Network Variable section defines the home address range, external address range, Web Servers, Mail Servers and DNS Servers.

Home Address Range

Home Address range will look like this in an unmodified Snort.conf:

var HOME_NET any (var is the keyword for variable)

"This setting will monitor your entire network by default."[6]

To monitor a single host with an IP Address of x.x.x.1, change the **any** to x.x.x.1/32. The /32 represents how many bits are in the subnet mask. Because this is monitoring the localhost, the subnet is 255.255.255.255. If you are not getting any alerts, you may want to check this section to be sure that the subnet mask is correct.

var HOME_NET x.x.x.1/32

To monitor the entire network x.x.x.0 with a subnet mask of 255.255.255.0 (24 bits) configure the HOME_NET section of the Snort.conf like so:

var HOME_NET x.x.x.0/24

NOTE: The IP Address x.x.x.1 and range x.x.x.0 would be actual IP Addresses and ranges; the x's were for example purposes only. For a better understanding of IP Addressing and Subnetting http://www.mcsefreak.com/subnetting.htm has a very educational guide.

External Address range

Change **var EXTERNAL_NET any** to

var EXTERNAL_NET !$HOME_NET

This tells Snort that any IP Address other than those specified as HOME_NET, which has already been defined, are external. "!" means "not".

SMTP Servers

Configure the SMTP section to

var SMTP $HOME_NET

Setting specific IP Addresses for your mail servers in this section will reduce the number of false alerts, but setting it to **$HOME_NET** will set it to monitor what is specifed in the **$HOME_NET** section

Web Servers

To configure your Web Servers set the variable to

var HTTP_SERVERS $HOME_NET for a large Network.

Again if you set this to be the IP Addresses of your Web Servers, the number of false alerts will be minimized, but you can set it to **$HOME_NET** as well. It may not be practical to type in the IP Addresses of 100 Web servers.

SQL Servers

Configure the SQL Server section to be

var SQL_SERVERS $HOME_NET

This works the same as the Web and SMTP server configuration. You can specify the servers or just leave it as **$HOME_NET**

DNS Servers

Configure the DNS Server Section to be

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

var DNS_SERVERS [10.20.30.100/24,10.20.30.101/24]
Configuring this section will prevent false DNS related scan alarms.

At the bottom of the Network Variable section is a line that specifies where the RULE files are located. Be sure to configure the entire path as shown or Snort may not start correctly:

var RULE_PATH E:\Snort\Rules

Configure Preprocessors

"Preprocessors provide for complex functions, such as TCP stream reassembly, IP defragging, or HTTP request normalization. Preprocessors are only called once per packet, can directly manipulate packet data, and even call the detection engine directly with their modified data."[7] The Snort.conf file does a very good job at explaining the different preprocessors. Martin Roesch also has good documentation on the Preprocessors in Chapter 2 of the Snort User's Manual found here: http://www.snort.org/docs/writing_rules/chap2.html. Preprocessors are great for catching specific alerts but can be very processor intensive in some cases. The following preprocessors are enabled by default in the Snort.conf:

preprocessor frag2
This preprocessor provides IP deframentation and detects fragmentation attacks.

preprocessor stream4: detect_scans
This preprocessor generates alerts on detection of stealth portscans.

preprocessor stream4_reassemble
This preprocessor reassembles traffic on specific ports and alerts on bad streams. The default port list is 21,23,25,53,80,143,110,513. Click here for an explanation of the port numbers http://www.iana.org/assignments/port-numbers . You can change this preprocessor to reassemble all ports by setting the port options with "all". This could be very processor intensive depending on the amount of traffic and the performance of the Snort computer.

preprocessor http_decode: 80 -unicode –cginull
'This preprocessor normalizes the HTTP requests by converting Unicode representations of characters into their ASCII equivalent and then passes them on to Snort to matching against the rules. The –unicode and –cginull will prevent false alerts such as CGI Null Byte attacks and IIS Unicode attacks that are sometimes triggered by sites that use muilt-bye characters.'[8]

preprocessor rpc_decode: 111
This preprocessor normalizes RPC traffic on a given port numbers that RPC services are running on. The 111 is the RPC service used by protocols for lookup.

preprocessor bo: -nobrute
This preprocessor detects Back Orifice traffic. The –nobrute turns off the brute forcing of the key space of the protocol to find the Back Orifice traffic. Performance can be severely impacted by turning on brute force.

preprocessor telnet_decode

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

This preprocessor normalizes telnet and FTP traffic by reassembling the traffic into data that can be matched against the rules.
preprocessor portscan-ignorehosts: 0.0.0.0
You should uncomment this preprocessor line and configure it with the IP Addresses of the DNS Servers to prevent false DNS alerts. Put any IP Addresses or networks in this section that port scans should be ignored.
Note: To uncomment simply remove the '#' in front of preprocessor

Configure Output Plugins
Output Plugins allow Snort to support a large number of logging and alerting output capabilities. These include logging to tcpdump files, different types of databases, text files, syslogs and alerting by WinPopUp messages and SNMP. In this example we will only log to a MySQL database. By default everything is commented out so you will need to uncomment the following line:
output database: log, MySQL, user=root password=test dbname=db host=localhost

NOTE: Be sure not to confuse the MySql with MSSQL. They look very similar so it's easy to uncomment out the wrong one.

log- This will alert to the alert.ids file
MySQL- This will alert to the MySQL database
user- This is the SQL user that has access to select, insert, update, delete and create privileges to the MySQL database. In this example we will use 'Snort'
password- This is the password that has been created for the above user. In this example we will use 'Snort'
dbname- This is the name of the Snort database. In this example we will use 'Snort'
host- This is the name of the SQL Server. In this example the SQL Server will be local, so 'localhost' will be used.

The following line will be found at the end of the Output Plugins section:
include classification.config
Change that line to include the entire path to the classification.config like so:
include E:\Snort\Rules\Classification.config
The classification.config is used to classify and prioritize alerts when they come in. This can be tailored to your specific needs but in this example we will leave it as default.

Customize your Ruleset
The last section of the Snort.conf is used to customize the rulesets. Here you will find text that looks similar tothis:
include $RULE_PATH/bad-traffic.rules
include $RULE_PATH/exploit.rules
include $RULE_PATH/scan.rules
This is only a small portion of the Ruleset section. You will find many more like this in the Snort.conf. There are many default rules ready to be used or custom rules may be

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

created. These rules are located in the snort\rules folder where you can get even more specific and detailed with alerts. Depending on your specific network environment certain rules should be commented out to prevent false positives or extra traffic. Under the Network Variables section above the $Rule_Path was specified. If you did not specify the $Rule_Path above then the entire path would need to be typed in for each rule that is included. This process could take up a lot of time.

For more understanding on rules and writing rules http://www.snort.org/docs/writing_rules/chap2.html#tth_chAp2 is a great place to start. It's very important that you do understand the rules and that you are able to customize them to fit you specific network for better security.

Save Snort.conf

Save and close the Snort.conf. That should complete the Snort installation customization.

Test Snort

- Open up a command prompt
- At the **E:\Snort**> type **snort –W**
  This will list all of the available network interfaces. Here we'll use 1.
- At the **E:\Snort**> type **snort –v –i1**
  This will start Snort in verbose mode and will listen on adapter 1.
- Press **Enter**
- Snort should start and you should see alerts similar to this:

04/02-16:16:36.588218 x.x.x.x:21472 -> x.x.x.x:80
TCP TTL:126 TOS:0x0 ID:30854 IpLen:20 DymLen:40 DF
A* Seq: 0x747D7EE0 Ack: 0x866AE7FE Win: 0x4470 TcpLen: 20

NOTE: The x.x.x.x would be actual IP addresses. If you receive and error verify that WinPcap is installed correctly or uninstall and reinstall it

- Hold down the **<crtl>** and **<c>** keys on the keyboard to kill the instance of Snort
- At the same prompt type in **Snort -c E:\Snort\Snort.conf -l E:\Snort\Logs –i1,** press **Enter**
  This will start Snort using the rules file **E:\Snort\Snort.conf** and will log to the directory **E:\Snort\Logs** the traffic on network interface 1
- You should see something similar to this:

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

```
C:\WINNT\System32\cmd.exe - snort -c e:\snort\snort.conf -l e:\snort\logs -i1
database: database name  = snort
database:          port  = 3999
database:          host  = localhost
database:   sensor name  = [redacted]:\Device\Packet_E190x1

database:      sensor id  = 1
database: schema version  = 104
database: using the "log" facility
882 Snort rules read...
882 Option Chains linked into 125 Chain Headers
0 Dynamic rules
+++++++++++++++++++++++++++++++++++++++++++++++++++

Rule application order: ->activation->dynamic->alert->pass->log

        --== Initialization Complete ==--

-*> Snort! <*-
Version 1.8.3-MySQL-WIN32 (Build 92)
By Martin Roesch (roesch@sourcefire.com, www.snort.org)
1.7-WIN32 Port By Michael Davis (mike@datanerds.net, www.datanerds.net/~mike)
1.8-WIN32 Port By Chris Reid (chris.reid@codecraftconsultants.com)
1.8-Win32 Port Compiled By Michael Steele (michaels@silicondefense.com, www.sili
          (based on code from 1.7 port)
```

NOTE: The blank space after 'sensor name' would be the name of the host.

- Look in the log **E:\Snort\Logs** for the log file that should be created named alert.ids
- Press **<Ctrl>** **<C>** to kill the process

Create the Snort Service

To create the Snort service you could use SrvAny or FireDaemon. Here we will use SRVAny. The service will automatically start Snort every time the computer is rebooted. I have taken the instructions written by Michael Steele for how to install SrvAny directly from the Silicon Defense site at http://www.silicondefense.com/techsupport/winsnortacid-iis_1.8.6.htm. I wanted to include everything that you needed in this document to install Snort, but it seemed unnecessary to go into any more detail than Mr. Steele has already.

The following instructions are taken directly from the following Website: http://www.silicondefense.com/techsupport/winsnortacid-iis_1.8.6.htm

"You will need to uncompress the file called "ServiceTools.exe" into your root folder. Note: Our root folder is "**C:\WINNT**", but yours might be "**C:\WINDOWS**", or "**C:\WINNT4**".
Note: There are two files included in the archive, one is called srvany.exe and the another is called Instsrv.exe. These are the two files that are required to run Snort as a service.

- Open a command prompt window.
- Navigate to the root folder of the operating system.

Note: Our root folder is "**C:\WINNT**", but yours might be "**C:\WINDOWS**", or "**C:\WINNT4**".

- You must install the SRVANY service. At a command prompt type: instsrv srvany <PATH TO ROOT folder>\srvany.exe
- At that same prompt type: INSTSRV.EXE snort <PATH TO ROOT FOLDER>\SRVANY.EXE
- Now start the Registry Editor From the run box (BACKUP YOUR REGISTRY!!!!!)

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

• Locate the following sub key:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Snort and select it.
• From the Edit pull down menu select New, select Key, and then type: Parameters
• Select the new Parameter key, right mouse click, select NEW, select String Value, and type: Application
• Right Mouse Click the new Application String, select Modify, and type:
E:\Snort\Snort.exe
• Right Mouse Click the Parameter Key again, select New, select String Value, and type: AppParameters
• Right Mouse Click the new AppParameters String, select Modify
• Type: -c **E:\Snort\Snort.conf** -l **E:\Snort\Logs** -ix
• Right Mouse Click the Parameter Key again, select New, select String Value, and type: AppDirectory
• Right Mouse Click the new AppDirectory String, select Modify
• Type: **E:\Snort**
Note: When you tested Snort use that same -ix (x is the number of the NIC to place the sensor on)
• From the Start Menu go to Programs / Administrative Tools and Open the Services applet in Administrative Tools. Select Snort from the services window, right click on Snort, choose Properties, and under startup type select Automatic (this will allow snort to be active when there is no one logged on)."[9]

PHP Install

PHP (PHP:Hypertext Processor) is an open-source server-side scripting language used for creating dynamic Web pages quickly. PHP's syntax is very similar to C, Java and Perl. PHP allows database enabled web pages by offering connectivity to many different databases such as MySQL. PHP also has command line functionality and can also be used to create windowing applications.

- Unzip **php-4.1.2-Win32.zip** into the **E:\Snort\Php** folder

NOTE: If you choose to put the PHP floder elsewhere be sure that there are no spaces in the path because the spaces will cause the server to crash.

- Copy **php4ts.dll** from **E:\Snort\Php** to **C:\Winnt or C:\Windows\ System32** folder
  This will ensure that the php4ts.dll will be found since C**:\Windows\System32** is already in your path statement
- Copy **phpini-dist** from **E:\Snort\Php** to **C:\Winnt or C:\Windows**
- Rename that file to **php.ini**
- Use WordPad to open and edit the php.ini file
- Change the following lines to:
  max_execution_time = 60
  extension_dir = **E:\Snort\Php\Extensions** - Make sure that the drive letter is correct . This tells PHP where to get its extensions.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

session.save_path = **E:\Snort\Php\Sessiondata** -Make sure that the drive letter is correct. This is where the temporary session data is stored.

NOTE: Create a folder under E:\Snort\Php named 'sessiondata' or the ACID console will not work

- Save the File and Exit

IIS Install

IIS (Internet Information Server) is Microsoft's Web Server that is included with Windows 2000/XP. It's very easy to use and can be used in a number of different ways.

- Go into **Add/Remove Programs**
- Click on **Add/Remove Windows Components**
- Click on **Internet Information Services**
- Click on **Details**
- Make sure that the following are selected:
  Common Files-These are required IIS program files
  FrontPage 2000 Server Extensions- Allows support for Web Applications created in FrontPage or Visual Interdev
  Internet Information Services Snap-In- Installs the management console for IIS
  World Wide Web Service-Installs the service that responds to HTTP requests
- Click on **OK**
- Click on **Next**

NOTE: You will probably need the XP or 2000 CD to copy files

- Click on **Finish**
- Close Add/Remove Programs

IIS Configuration

This section details how to associate the PHP application with the .PHP extension in order for PHP scripts to be run from the Web browser.

- Open the **Internet Information Services** Console
- Expand the **Server** name
- Expand **Web Sites**
- Right Click on **Default Web Site** and Open **Properties**
- Click on the **Home Directory** Tab
- Click on **Configuration** near the bottom
- Under Application mappings click on **ADD**
- Browse to or type in **E:\Snort\Php\Php.exe**
- Type in **.php** for the Extension
- Check the **Script Engine** Check box
- Click on **OK** all the way out of Properties

NOTE: Make sure the that I_User has Execute rights to the **E:\Snort\Php** directory

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

ADODB Install

"ADODB is a set of advanced PHP database wrapper classes."[10] A wrapper is data that precedes or frames the main data or a program that sets up another program so that it can run successfully. Windows programmers find programming with ADODB easy because of its similarities with ADO. It can be easily configured to use many different databases.

- UnZip the **adodb190.zip** into the **E:\Snort\Adodb** folder
- Edit the **E:\Snort\Adodb\Adodb.inc.php** with Wordpad

This is the files that contains the functions that can be used by all of the different databases that ADODB supports.

- Find the following line and edit it to show the location of the ADODB folder: **$ADODB_Database = 'E:\Snort\Adodb'**
- Save the file and Exit

PHPLot Install

"PHPLOT is a PHP graphics class for creating charts and plots in native PHP"[11] This used PHP to create pretty little graphs in the ACID console of the alert data. It allows you to enter in the criteria, choose which kind of graph you would like (thin bar, bar or line) and away it graphs…

- Unzip the **phplot-4.4.6.zip** into the **E:\Snort\Phplot** directory

Acid Viewer Install

'The Analysis Console for Intrusion Databases (ACID) is a PHP-based analysis engine to search and process a database of security events generated by various IDS's, firewalls, and network monitoring tools."[12] This console is very useful for viewing Snort alerts in many different ways. You can search or view by source, destination, alert type, alerts times, port numbers and or protocols. You can create alert groups and email alerts and delete alerts all from this console.

- Create a folder named '**Acid**' under the **C:\Inetpub\Wwwroot** folder (your wwwroot folder may be located elsewhere)
- Unzip the **acid-0.9.6b21.zip** into this folder
- Open and Edit the **acid_conf.php** file with Wordpad
- Make the following changes to the file to give it the needed Snort database information:
  DBlib_path = "**E:\Snort\ADODB**" – This is the database abstraction library variable
  $alert_dbname = "snort"; - This is the name of the Database that we created earlier in DBTools Manager.
  $alert_host = "localhost"; - This is the name of the server. 'Localhost' will work
  $alert_port = "3306"; - This is the port number specified earlier in WinMySqlAdmin that MySql runs on
  $alert_user = "snort"; - This is the user that we created earlier in DBTools

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Manager
$alert_password = "snort"; - This is the password that we created ealier in DBTools Manager

$archive_dbname = "snort"; - This is the archive database
$archive_host = "localhost"; - The name of the server that has the archive database
$archive_port = "3306"; - The port number that the archive database is listening on
$archive_user = "snort"; - The user that has access to the archive database
$archive_password = "snort"; -The password of that user

$ChartLib_path = "**E:\Snort\Phplot**" – This is the entire path of the PhpLot graphing library.
NOTE: Be sure to use double quotation marks around each setting or ACID will not work. Also, keep in mind that your username and password should be different than what is provided in this example.

- Reboot your computer

Acid Viewer Configuration

- After rebooting browse to http://localhost/Acid/Index.html
- You will receive an error the first time you run Acid
- Click on '**Go to the Setup Page'** when this error appears
- At the Setup Page click '**Create ACID AG'** to finish the configuration.
- Go to the http://localhost/Acid/Index.html website again. The Acid Console should successfully come up.

Securing IIS

Because this is a Microsoft Web Server and it has the database of all the alerts on it along with the log files, it is important to make sure that the Web Server is secure. If someone were able to hack in through you Web Server it would be easy for him or her to cover his or her tracks. Here are a few suggestions for securing IIS:

- Disable anonymous access to the website and lock down the security of the folder **C:\Inetpub\Wwwroot\Acid** by not allowing 'Everyone' to be able to access it. To do this:
    1. Open up the IIS MMC
    2. Expand the server name
    3. Expand WebSites
    4. Right Click on the default website (or the website that contains the Acid folder)
    5. Click on Properties
    6. Click on the Directory Security tab
    7. Under the Anonymous access and Authentication Control click on Edit

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

8. Uncheck the Anonymous Access box
9. Click OK
10. Click OK to exit the properties window
11. Close the IIS Management Console
12. Browse to the Acid folder under the inetpub\wwwroot
13. Right click on the folder
14. Click on Sharing and Security
15. Click on the Security tab
16. Click on Everyone, Users or both
17. Click on Remove
18. Remove any other users who should not access this site
19. Click on OK

- Download and Install Windows update from http://v4.windowsupdate.microsoft.com/en/default.asp . This will scan your computer and tell you what updates you need to download and install. Installing this on your pc will allow it to automatically, behind the scenes, check for updates and will alert you when there is one that should be installed.
- Keep up with the latest service packs and security updates by subscribing to the Microsoft Security Notification Service list http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/notify.asp
- Microsoft's Secure IIS 5 Check List has a lot good suggestions for securing IIS. Definitely apply the HiSecWeb.inf security template, disable netbios, enable logging, remove sample applications, and remove unused script mappings. All of this is detailed here: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/chklist/iis5chk.asp
- You should also install Microsoft's Baseline Security Analyzer from http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/Tools/mbsahome.asp . This tool has a pretty little GUI that scans for missing hotfixes and vulnerabilities in Windows 2000 and XP as well as IIS and other Microsoft products. It's very helpful, easy to use, and provides nice reports.

Additional Windows 2000/XP Security Measures

- You may want to look at the NSA (National Security Agency) website for additional Security Recommendation Guides and Security Templates. If this is what the government has come up with for their security doesn't it make sense that we use it too?
- Make sure that the computer has Antivirus software installed on it and up to date. Most Antivirus software has the ability to perform automatic updates, which will save you some administration.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

- If you do not have one already, put a Software Firewall on the Computer such as BlackIce or ZoneAlarm. This will provide an added layer of protection and detection. Set it to the most paranoid level of protection possible. You may need to open up ports for the IP Address of the computer that you use to view the ACID Console from.
- Use a third-party program such as ISS (Internet Security Scanner) or Nmap to scan the computer for any vulnerabilities or unwanted ports open that the Microsoft security analyzers may not have picked up on.

Brief IDSCenter Description

I originally detailed instructions of how to install and configure IDSCenter with Snort but I decided to take it out. If you are interested in finding out more about IDSCenter go to http://www.mysunrise.ch/users/rkistler/. I have been using IDSCenter for a few months now and I don't feel that it has helped me very much. It's a great product, but I'm used to looking at the ACID console and the Alert.ids. It has some useful functions such as integrating with BlackIce and log rotating.

Periodic MYSQL Maintenance

Depending on the amount of traffic being logged the Snort database can become quite large and will cause the Acid viewer to take a long time to run queries and display alerts. When this happens the easiest way to fix it is to delete the Snort database and recreate it. You should back up the database to a file first. This way you have the evidence if you ever need to go back and track an alert or hacker down.

- Open DBTools Manager
- Expand the Server name
- Expand Databases
- Right click on Snort
- Click on Dump Database
- Put in the path and filename for the backup file
- Click on Save
- Right Click on Snort again
- Choose Drop Database
- Click on Yes to verify that you want to delete this database
- Expand Users
- Right click on Snort
- Click on Drop

The database and user have been deleted. Now you need to recreate the database, recreate the user and run the create_mysql command to recreate the tables.

- Right Click on **Databases**
- Click on **Create**
- Type in 'Snort' for the database name
- Click **OK**-You just created the Snort database that Snort will log to

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

- Right Click on **Users**
- Click on **Create**
- Under the User Properties type in User ID 'Snort'- Here we are using Snort as an example, but you should use something unique and hard to guess for better security
- Type in the Password 'snort' and confirm by typing it in again- Again, this is an example, use something unique and not easily guessable
- For the Set privilege on Database use the pull down menu to choose Snort- This allows the user that we just created to have access to the database that we also created
- Click on **OK**
- Right click on the user Snort
- Click on **Privileges**
- **Select, Insert, Update** and **Delete** should already be checked for the Snort database
- Put a check in the **Create** box as well-This will allow Snort to log new alerts to the database
- Click on **Save**, then **OK**
- Click on **Close**
- Open a command Prompt
- From **E:\MySQL\Bin**> type:
- MySQL -u Snort -p Snort < **E:\Snort\Create_MySQL** and press enter
- Expand Snort in DBTools to verify that the tables were create
- Browse to the ACID console http://localhost/Acid/Index.html
- You will receive an error the first time you run Acid
- Click on '**Go to the Setup Page'** when this error appears
- At the Setup Page click '**Create ACID AG'** to complete the Acid Alert Group configuration.
- Go to the http://localhost/Acid/Index.html website again. The Acid Console should successfully come up.

I hope this document helps. Good Luck!

References and Useful Links

Elfering, Dave. "Snort and Windows 2000, A practical Guide"
http://www.synaxis.org/around/sansug/snort-w2k.pdf
Rode, Kenneth. "Snort – Free Graphical IDS for the Windows Environment" 6 April 2001. http://rr.sans.org/intrusion/snort3.php

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Bull, Jon. "Snort's Place in a Windows 2000 Environment" 17, May 2001. http://www.snort.org/docs/snort-win32.doc
Richard, Jeff. "Configuring Snort, MySQL, and ACID on Windows NT." 3, May 2001 http://rr.sans.org/intrusion/ACID.php
"Hands on Intrusion Detection FAQ" http://www.sans.org/conference/IDSFAQ.htm

Citations

[1] "More Info About Snort." http://www.snort.org/about.html
[2] Disk, Jitsu. "libnetnt." 07 February, 2002. http://www.securitybugware.org/libnetnt/
[3] Norberg, Stefan. "WinPcap Brings Unix Network Tools to Windows." 05 December 2000. http://security.oreilly.com/news/securingnt2_1200.html
[4] "The MySQL AB Company." http://www.mysql.com/
[5] "Information about DBTools Software." http://www.dbtools.com.br/Info.php
[6] Steele,Michael. "Snort 1.8.6 for Windows NT Server / 2000 / XP using IIS, MySQL and Acid to view and graph alerts." 18 February 2002. http://www.silicondefense.com/techsupport/winsnortacid-iis_1.8.6.htm
[7] Dubrawsky, Ido "Freeware Intrusion Detection Tools." http://www.samag.com/documents/s=1147/sam0108o/0108o.htm
[8] Neophasis Archives, John Berkers, August 3, 2001 http://archives.neohapsis.com/archives/snort/2001-08/0075.html
[9] "Snort 1.8.6 for Windows NT Server / 2000 / XP using IIS, MySQL and Acid to view and graph alerts..." Steele, Michael, April 18, 2002, http://www.silicondefense.com/techsupport/winsnortacid-iis_1.8.6.htm
[10] "ADODB 1.72." http://software.linux.com/projects/adodb1/
[11] Ottenheimer, A."PHPlot." 12 March 2001. http://freshmeat.net/projects/phplot/?topic_id=92%2C100%2C75%2C135%2C809
[12] Danyliw,Roman "Acid Console for Intrusion Databases" http://www.andrew.cmu.edu/~rdanyliw/snort/snortacid.html

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: June 19th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**