



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at <http://www.giac.org/registration/gsec>

**A practical guide to running SNORT on Red Hat Linux
7.2 and Management Using IDS Policy Manger
MySQL+IIS+ACIDFrom your Workstation.**

**William Metcalf
GIAC Security Essentials Certification
April 02, 2002
v1.3**

© SANS Institute 2000 - 2005, Author retains full rights.

Introduction

In the brief time that I have been on this planet the state of computing has changed drastically. The high-powered computers and blink of the eye internet connectivity once reserved for universities and major corporations has now become a staple in small businesses around the United States and the world. As more and more these small businesses get connected to the global network we call the internet, we must focus our attention on securing these systems. It used to be that hacking systems such as these could only be done by high skilled programmers and network gurus. This has also changed with the birth of “script kiddies” who are hackers who use programs and scripts that are freely available and easy to use to attack such systems. Firewalls and virus protection software add layers of security but in most cases this is not enough.

SNORT which is a free NIDS (*Network Intrusion Detection System*) adds another layer to your security blanket. To give you a better picture of what I mean by this, I will quote Wes Simonds of Search Networking as saying “If a firewall is the initial gate, Snort is the highly-trained Doberman pack that roams the company grounds pawing at intruders, sniffing at their packets in a deceptively unobtrusive manner and occasionally when things are manifestly uncool biting them gently in half.” SNORT will watch and analyze your network traffic and will alert you when there are possible hacking attempts against your computer system(s). SNORT was originally written by Martin Roesch for *nix operating systems, and according to one study can keep up with the heavy weights such as Cisco and ISS (Study done by the Gartner Group <http://www.gartner.com/DisplayTechOverview?id=320015>). I will show you how to setup snort on Red Hat 7.2 and I will show you how to manage your sensor and view alerts from your windows 2000 workstation.

Getting Started

There are a few things that we are going to need to get started:

Access to the internet

Access to a cd-burner

A computer dedicated to Red Hat and snort.

A computer used as a management workstation. This can be your desktop. In this example I use windows 2000 but this configuration should work for any Windows NT variant.

A hub to monitor, if you are in a switched network you must setup a monitor port for the sensor where the traffic you desire to watch can be mirrored to. If this is the case you must configure your sensor with two network cards. One Network card to plug into the monitor port and one to communicate with your management workstation.

Two static IP address on your network. Assign one to the sensor and one to the management workstation.

Snort on Red Hat Linux 7.2

Installing Red Hat

1. Burn the Red Hat 7.2 ISO images to CD the ISO images should be enigma-i386-disc1.iso and enigma-i386-disc2.iso, most cd-writing software supports ISO images. I know that Roxio Easy CD Creator and Ahead Nero Burning ROM both support this format.
2. Configure your bios to auto-boot from cd-rom. If your bios does not support auto-booting to cd consult the red hat 7.2 documentation <http://www.redhat.com/docs> for creating an installation boot disk. Insert Red Hat disc 1 into your cd-rom and reboot your computer.
3. After your computer posts a text based Red Hat Linux Installation screen will appear. Press the <Enter> key to continue
4. On the Language Selection Screen select **English** as the language you wish to use during install. Select the **next** button to proceed to the keyboard configuration screen.
5. Select your keyboard model, layout and select enable dead keys. Select the **next** button to proceed to the Mouse Configuration screen.
6. Select your mouse type and select whether or not to emulate three buttons. Select the **next** button to proceed to the Red Hat welcome screen.
7. Select the **next** button to proceed to the Installation Type screen.
8. Select the custom installation radio button. Select the next button to proceed to the Disk Partitioning Setup screen.
9. Select the **Have the installer automatically partition for you** radio button. Select the **next** button to proceed to the Auto Partitioning screen.
10. Select the **Remove all partitions on this system** radio button. Uncheck the **Review Results** check box. Select **next** button to proceed to the warning prompt.
11. At the warning prompt click **Yes**, this will take you to the Boot Loader Configuration screen.
12. On the Boot Loader Configuration accept the defaults and select the **next** button to proceed to the Boot Loader Password Configuration screen.
13. Check the **Use a Grub Password?** Checkbox. Enter your password in each twice once in the **password** box and once in the **confirm** box. I suggest using mixed case numbers and special characters with a minimum length of eight characters. Select the **next** button to proceed to the Network Configuration Screen.
14. Configure your network card(s) as suited for your network, I can't really help you here if you don't know what to input into these boxes contact somebody on your network team to get these settings. Once you have configured your network card select the **next** button to proceed to the Firewall Configuration Screen.

15. Select the No Firewall radio button. If you put a firewall in place snort will not be able to see the traffic from anything that you block. Select the **next** button to proceed to the Additional Language Support screen.
16. Select any additional languages you may need and select the **next** button to proceed to the Time Zone Selection Screen.
17. Select your time zone by selecting it out of the list or by clicking on the point in your region on the map that represents your time zone. Select the **next** button to proceed to the Account Configuration Screen.
18. Enter your root account password once into the **Root Password:** box and once into the **Confirm** box. Once again use mixed case letters special characters and numbers. Make the password longer than eight characters. Select the **next** button to proceed to the authentication configuration screen.
19. Select the defaults and then select the **next** button to proceed to the Package Group Selection screen.
20. Uncheck all of the check boxes that are checked by default. Check the **Select individual packages** check box and select the **next** button to proceed to the Individual Package Selection screen.
21. Select the Flat View radio button. Select the Check box next to following items:
 - autoconf
 - automake
 - binutils
 - cpp
 - freetype
 - ftp
 - gcc
 - gcc-c++
 - gcc3
 - gcc3-c++
 - gd
 - glibc-devel
 - kernal-headers
 - libgcc
 - libjpeg
 - libpcap
 - libpng
 - libstdc++-devel
 - libstdc++3
 - libstdc++3devel
 - linuxconf
 - lynx
 - m4
 - make
 - mysqlclient9
 - openssh

opensshserver
perl
wget

Uncheck the checkbox next to **sendmail**, it should be toward the bottom of the list. Select the next button to proceed to the Unresolved Dependencies screen.

Accept the default setting on this page and select the next button to proceed to the About to Install screen.

22. Accept the default settings on this page and select the next button to proceed to the installing packages screen.
23. Red Hat will automatically begin installing you can probably go smoke a cigarette or grab a cup of coffee and come back..... Great you've returned and the Red Hat installation should prompt you for disc 2. Insert disc 2 and select the **Ok** button. It should starting installing packages automatically from disc 2. Once Red Hat is done copying files it will automatically take you to the Boot disk Creation screen.
24. It is optional to you whether or not you want to create a boot disk but it is always a good idea. Check or uncheck the check box as you see fit and then select the next button to proceed to the Congratulations screen.
25. Select Exit and Red Hat will reboot eject the cd-rom and bring up a logon prompt.

© SANS Institute 2000 - 2005. All rights reserved.

Installing Snort 1.8.4

Download the following RPM's by using wget which I will explain in a minute or by using a different computer and downloading the the RPM's and burning them to CD or copying them to floppies.

<http://www.snort.org/dl/binaries/RPMS/snort-1.8.4-1snort.i386.rpm>

<http://www.snort.org/dl/binaries/RPMS/libnet-1.0.2a-1snort.i386.rpm>

<http://www.snort.org/dl/binaries/RPMS/snort-mysql+flexresp-1.8.4-1snort.i386.rpm>

<http://mysql.orst.edu/Downloads/MySQL-3.23/MySQL-shared-3.23.49a-1.i386.rpm>

<http://mysql.orst.edu/Downloads/MySQL-3.23/MySQL-devel-3.23.49a-1.i386.rpm>

<http://mysql.orst.edu/Downloads/MySQL-3.23/MySQL-client-3.23.49a-1.i386.rpm>

1. Log into the sensor as user root and when prompted input the password that you assigned to the root user. You should now have a shell prompt, if you inputted your hostname into the network configuration screen your prompt will be [username@hostname homedir]# enter the following commands:

```
mkdir /snort-install
```

```
cd /snort-install
```

2. Now we need to get those RPM packages that we downloaded copied to the snort-install directory.

To use **wget** on your sensor that has access to the internet enter the following commands

```
wget http://www.snort.org/dl/binaries/RPMS/snort-1.8.4-1snort.i386.rpm
```

```
wget http://www.snort.org/dl/binaries/RPMS/libnet-1.0.2a-1snort.i386.rpm
```

```
wget http://www.snort.org/dl/binaries/RPMS/snort-mysql+flexresp-1.8.4-1snort.i386.rpm
```

```
wget http://mysql.orst.edu/Downloads/MySQL-3.23/MySQL-shared-3.23.49a-1.i386.rpm
```

```
wget http://mysql.orst.edu/Downloads/MySQL-3.23/MySQL-devel-3.23.49a-1.i386.rpm
```

```
wget http://mysql.orst.edu/Downloads/MySQL-3.23/MySQL-client-3.23.49a-1.i386.rpm
```

To copy from a floppy drive format the floppy disks and copy the RPMS to the disks. enter the following command mount /dev/fd# where # is the number of your floppy drive. In Linux almost all things start at zero so for most systems with only one floppy drive type the following

```
mount /dev/fd0
```

```
cp /mnt/floppy/* /snort-install
```

```
umount /dev/fd0
```

insert your second floppy so on and so on. Enter the following commands again.

```
mount /dev/fd0  
cp /mnt/floppy/* /snort-install  
umount /dev/fd0
```

To copy from a cd-rom burn the RPMS to a cd and enter the following commands

```
mount /dev/cdrom  
cp /mnt/cdrom/* /snort-install  
umount /dev/cdrom
```

3. Double check and make sure that all of your RPM packages are in the /snort-install directory by doing the following

```
cd /snort-install  
ls
```

you should see the following:

```
libnet-1.0.2a-1snort.i386.rpm  
libpcap-0.6.2-9.i386.rpm  
MySQL-shared-3.23.49a-1.i386.rpm  
snort-1.8.4-1snort.i386.rpm  
snort-mysql+flexresp-1.8.4-1snort.i386.rpm  
MySQL-devel-3.23.49a-1.i386.rpm  
MySQL-client-3.23.49a-1.i386.rpm
```

4. To install the packages type the following commands:

```
rpm -v -i /snort-install/libnet-1.0.2a-1snort.i386.rpm  
rpm -v -i /snort-install/MySQL-shared-3.23.49a-1.i386.rpm  
rpm -v -i /snort-install/ MySQL-client-3.23.49a-1.i386.rpm  
rpm -v -i /snort-install/ MySQL-devel-3.23.49a-1.i386.rpm  
rpm -v -i /snort-install/snort-1.8.4-1snort.i386.rpm  
rpm -v -i /snort-install/snort-mysql+flexresp-1.8.4-1snort.i386.rpm
```

5. Run the following commands to get the snort daemon to start automatically

```
vi /etc/rc.d/init.d/snortd  
press the <insert> key  
find the lines that read
```

```
daemon /usr/sbin/snort -A fast -b -l /var/log/snort -d -D \  
-I $INTERFACE -c /etc/snort/snort.conf
```

note: If you are using two network cards you must configure the \$INTERFACE variable to reflect the interface that is plugged into a promiscuous port on your switch.

change these lines to be

```
daemon /usr/sbin/snort-mysql+flexresp -D \  
-i $INTERFACE -c /etc/snort/snort.conf
```

next find the line that reads

```
killproc snort
```

change this to be

```
killproc snort-mysql+flexresp
```

finally change the line that reads

```
status snort
```

change this to be

```
status snort-mysql+flexresp
```

press the <Esc> key

press the <Shift> plus <:;> keys

press the <w> key

press the <q> key

this should take you back to your shell prompt. Type the following to test your Snort Daemon.

```
service snortd start
```

Should return

```
Starting snort: [ OK ]
```

```
service snortd status
```

Should return something like

```
snort-mysql+flexresp (pid 959) is running...
```

```
service snortd stop
```

Should return

```
Stopping snort: [ OK ]
```

Now we are going to setup snort to run at startup by typing in the following commands

```
cd /etc/rc3.d  
ln -s /etc/rc.d/init.d/snortd S40snortd
```

reboot your sensor by typing in the following command

```
shutdown -r now
```

Look for the following line during the initialization of Linux

```
Starting snort: [ OK ]
```

You can check any alerts that snort is logging by typing in the following commands:

```
vi /var/log/snort/alert
```

you should get screen with your alerts you can use the up and down arrow buttons or the <page up>, <page down> buttons to maneuver through the document. To exit the document type the following commands:

```
<Ctrl>plus<q>
```

this should take you back to your shell prompt. Type the following to log out of the console.

```
exit
```

Viola you are snorting!!!! Now to tune your sensor to watch your network, get rid of pesky port scan messages and to get it log to a MySQL Database.

© SANS Institute 2000-2005, Author retains full rights.

The Management Workstation:

Create a directory on your local hard drive c:\snortM Download the following items to a folder on your local hard drive for the rest of the paper we are going to assume that you downloaded everything into c:\snortM

Win Zip

<ftp://ftpx.download.com/pub/win95/utilities/filecomp/winzip81.exe>

Putty

<http://the.earth.li/~sgtatham/putty/latest/x86/putty.exe>

IDS Policy Manager

<http://www.activeworx.com/downloads/IDSPolMan-1.2.full.zip>

MySQL Server

<http://mysql.orst.edu/Downloads/MySQL-3.23/mysql-3.23.49-win.zip>

PHP Lot

<http://www.silicondefense.com/software/snort-win32/binaries/phplot-4.4.6.zip>

PHP

http://www.php.net/do_download.php?download_file=php-4.2.0-installer.exe

ACID

<http://www.silicondefense.com/software/snort-win32/binaries/acid-0.9.6b20.zip>

ADODB

<http://www.silicondefense.com/software/snort-win32/binaries/adodb172.zip>

Snort 1.8.4 tar

<http://www.snort.org/dl/snort-1.8.4.tar.gz>

Install WinZip

Install WinZip by running c:\snortM\winzip81.exe accepting all of the defaults

Install Activeworx IDS Policy Manager

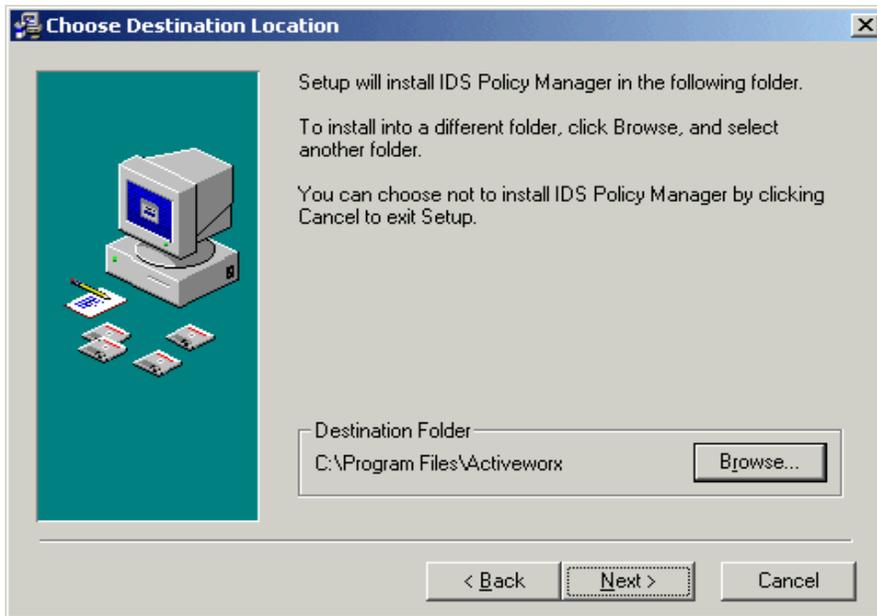
Extract all of the files in c:\snortM\IDSPolMan-1.2.full.zip by double-clicking on the zip file and extracting all files to a directory let's say c:\snortM\IDSpol

Navigate to c:\snortM\IDSpol and run IDSPMFULL1.2 to setup your IDS Policy Manager.

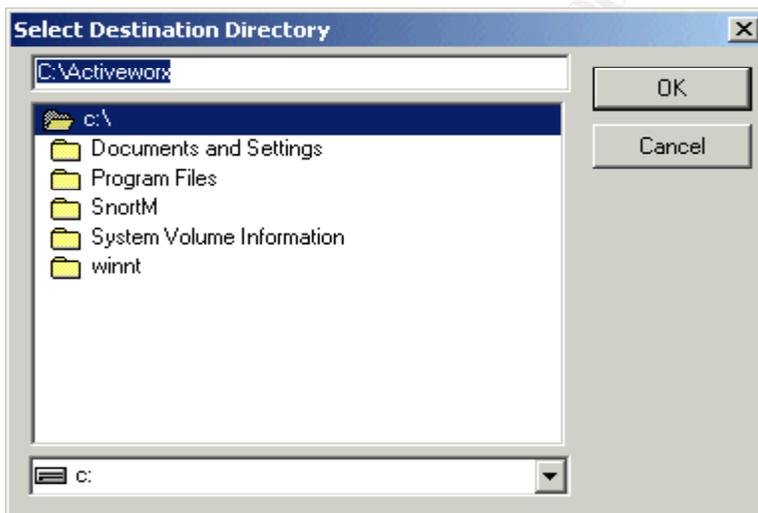
1. On the Screen above Select the Next button



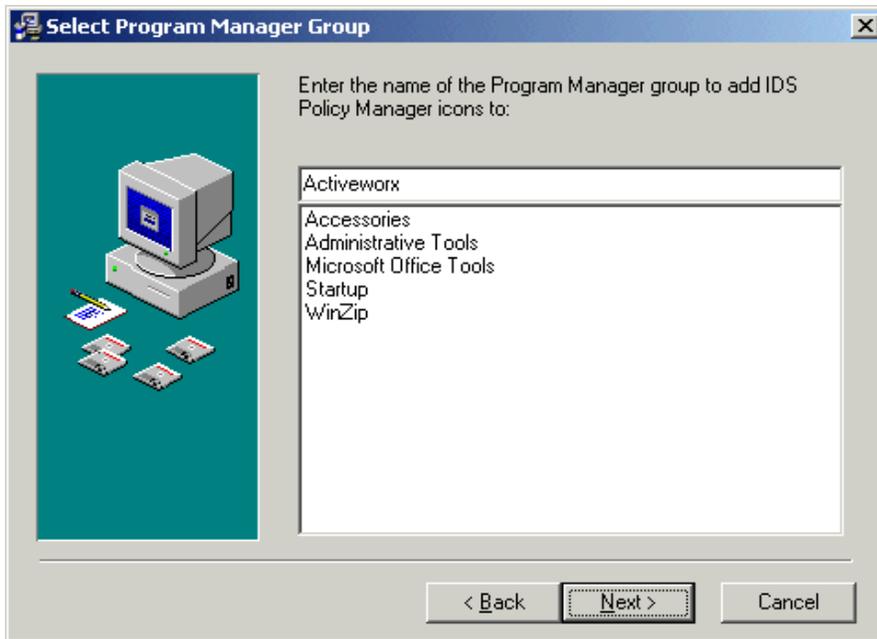
2. On the Screen below press the browse button to change to default path that IDS policy Manger installs in. The space in the path name i.e. "c:\program files" causes problems with secure copy which IDS policy Manager uses to upload files to your sensor. Choose something like C:\Activeworx



3. When you hit the Browse button you should get this change your path and hit the OK button. When you return to the Choose Destination Location Screen press the Next button.

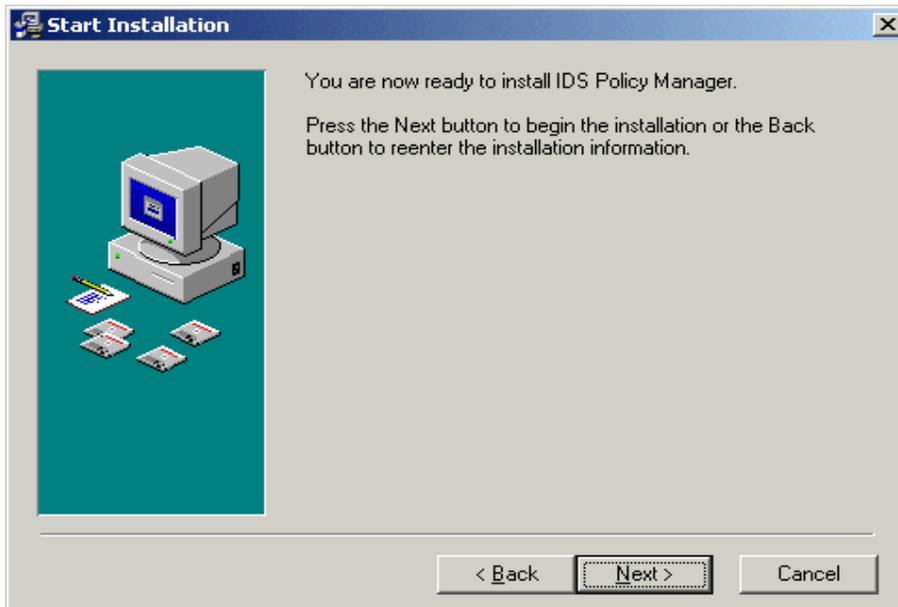


4. Accept the defaults on the screen below so just hit the next button.



© SANS Institute 2000 - 2005, Author retains full rights.

5. Once Again just hit the next button on the screen below.



Setup will install the VB6 runtimes and IDS Policy Manger and exit quietly.

6. Navigate to the directory where you installed IDS Policy Manager and create directories for each one of your sensors. i.e. make directories

C:\Activeworks\Sensor1

C:\Activeworks\Sensor2

Go into the Official Folder in the directory where you installed IDS Policy Manger and select all of its contents and copy them into your Sensor directories.

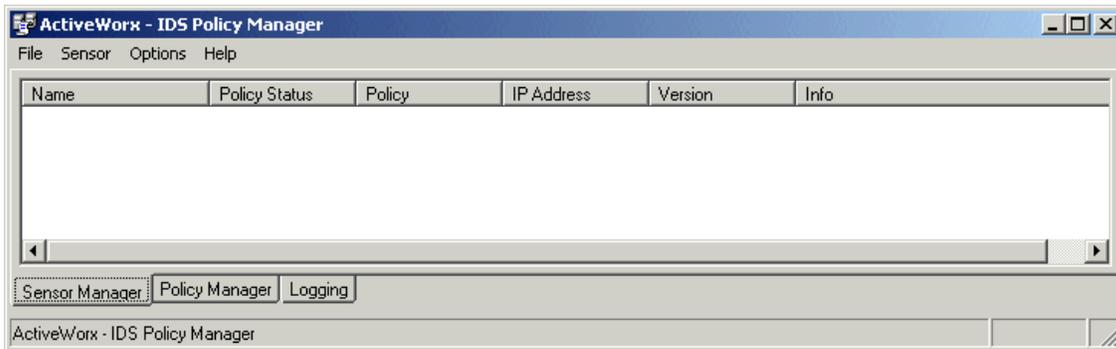
7. Now go to start→programs→Activeworx→IDS Policy Manager

You should get something like the screen below I said yes it will take you to the website when new versions are available

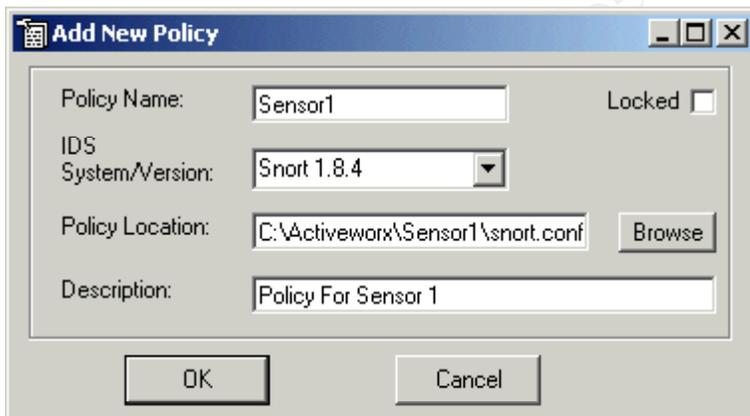


Now you should have a screen like the one below. Select the Policy Manger tab, now

select Policy → Add Policy



8. You should get a screen like the one below. Enter your policy name for your first sensor in this example the IDS/System Version is Snort 1.8.4 so leave the default setting there. In your Policy Location field enter C:\Activeworx\Sensor1\snort.conf remember this is the folder that we created to hold our first sensor's configuration files. Press the Ok button and you should have a new entry in your window called Sensor1. Repeat the above steps for any other sensors you may have changing the Policy Name, Policy Location, and Description.



9. Now go back to the Sensor Manager screen by selecting the Sensor Manger tab. From the menu bar select Sensor → Add Sensor. The box below should open up, Enter all of your information as follows about your sensor.

Sensor Name: For this example it was Sensor1

IP Address of Sensor: In this example 192.168.1.222 (This will change depending on your network)

IDS System: For this example it is Snort 1.8.4 (default)

Policy: Sensor1 This the policy that we just created

Upload Protocol scp (default) Port: 22 (default) This is part Secure Copy part of the SSH daemon package on our Sensor.

Username: root

Password: (The secure password that you entered when you installed Red Hat on the Sensor)

Password(Confirm): (The secure password that you entered when you installed Red Hat on the Sensor)

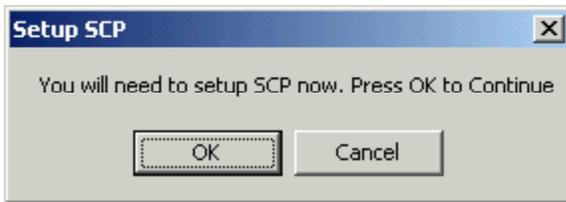
Upload Directory: /etc/snort (Remember this where we are reading the snort configuration file from.

The screenshot shows a dialog box titled "Add Sensor" with the following fields and values:

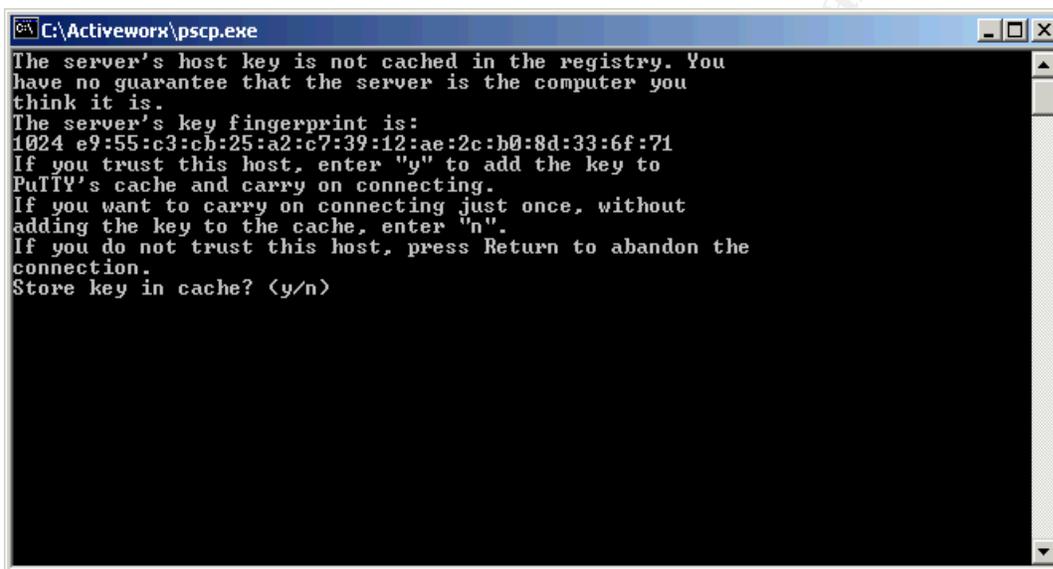
- Sensor Name: Sensor1
- Sensor Information:
 - IP Address of Sensor: 192.168.1.222
 - IDS System: Snort 1.8.4
 - Policy: Sensor1
- Upload Information:
 - Upload Protocol: scp
 - Port: 22
 - Username: root
 - Password: [masked]
 - Password(Confirm): [masked]
 - Upload Directory: /etc/snort

Buttons: OK, Cancel

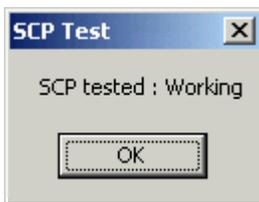
10. When you press the Ok button you will be prompted with the following box. Telling you that you need to setup Secure Copy. Press the OK button to proceed



You should get the screen below as to whether or not you want to store the remote key in your cache press the <y> key and the <Enter> key



If all is well you should get the following screen. Press the OK button and this should take you back to the Sensor Manger Screen.



We will come back and work on the settings in a minute next we are going to setup a MySQL Database for snort to log to.

INSTALL MYSQL

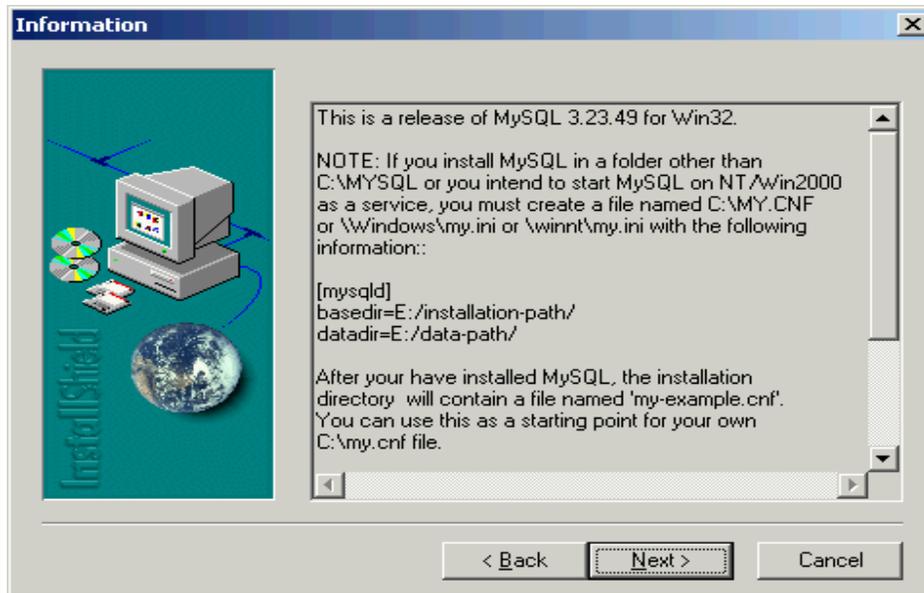
Extract all of the files in c:\snortM\mysql-3.23.49-win.zip by double-clicking on the zip file and extracting all files to a directory let's say c:\snortM\sqlinst

Navigate to c:\snortM\sqlinst and run Setup.exe to setup your MySQL Database.

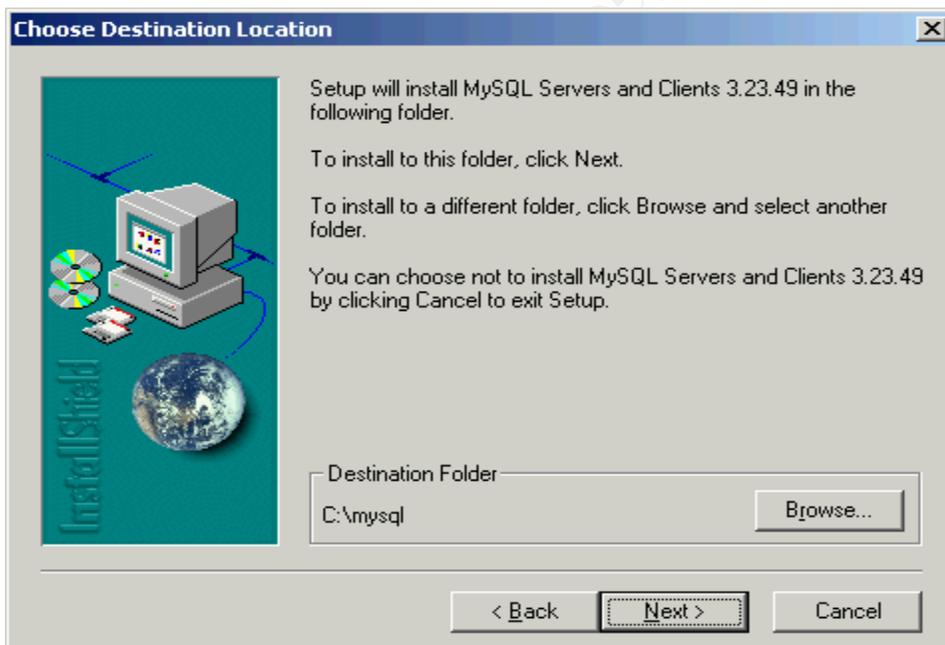
1. On the Screen below Select Next button to proceed to another information screen.



2. On this information screen it tells you what you need to get mysql to run if you are not going to install it in c:\msql. Press the Next button to proceed to the Choose Destination Location Screen.



3. On the screen below select the default installation directory by selecting the Next button.



4. On this screen select the default "Typical" installation by selecting the Next button. Setup will proceed to install MySQL.



© SANS Institute 2000 - 2005, Author retains full rights.

5. Once completed you should get the screen below. Press the Finish button to exit setup



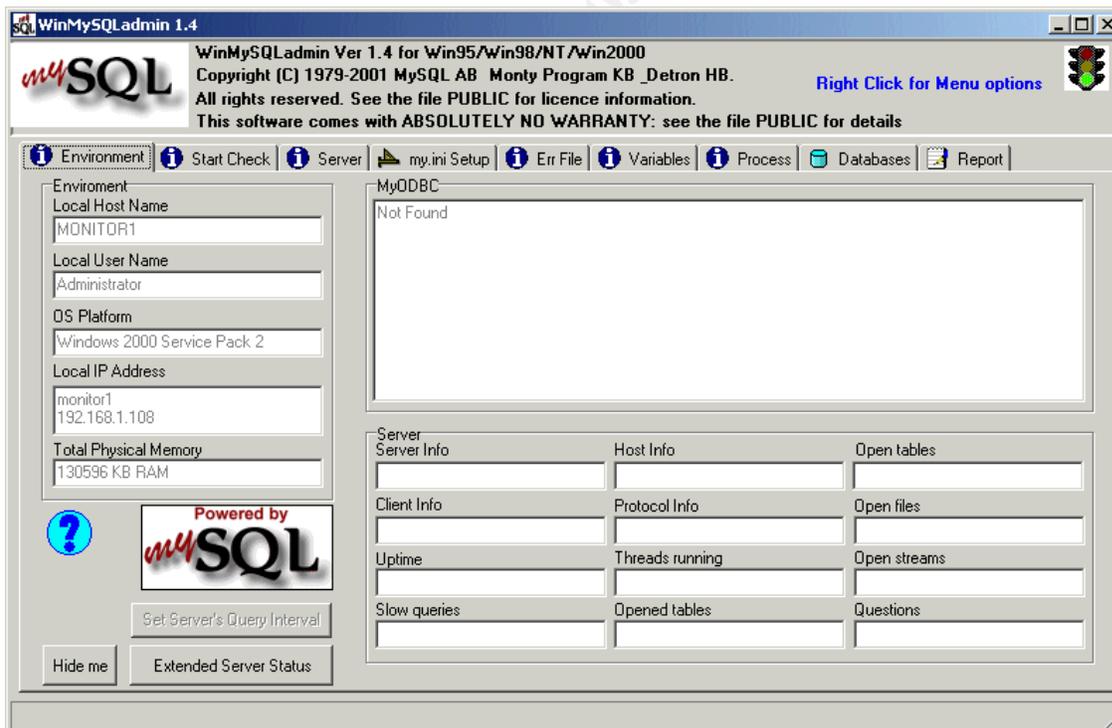
****Most of The Information below on configuring IIS, MySQL, and Acid have been taken from papers written by Michael Steele of Silicon Defense only slightly modified for this paper. <http://www.silicondefense.com/techsupport/windows.htm> ****

6. Navigate to c:\mysql\bin\winmysqladmin.exe alternate click and hold navigate to "send to" select "desktop as shortcut."

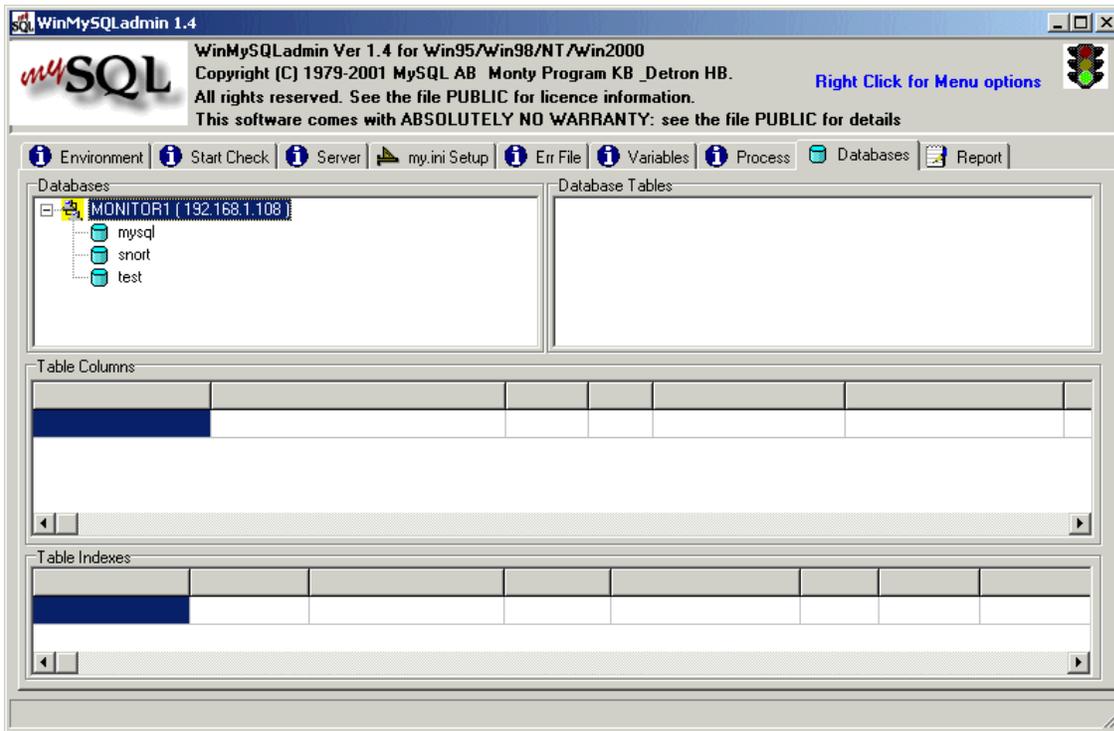
Go to your desktop and double click on the shortcut to winmysqladmin.exe to get the box below. Enter the username: "root" password: "****" where **** is the password that you want. And then press the OK button.



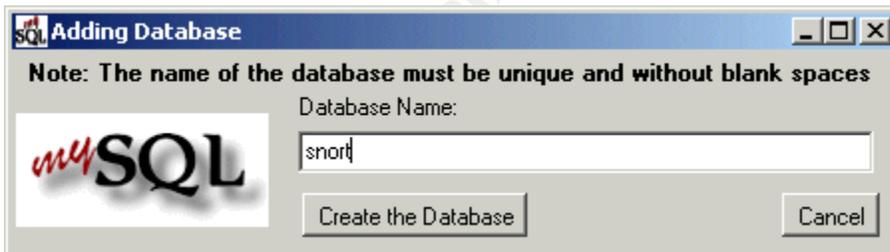
7. Alternate click on the stop light in the taskbar on the lower right side of your screen. And select Show Me from the menu. You should get the screen below.



8. Select the databases tab to bring up the databases screen.



9. Select the line that has your computer name on it and alternate click and select create new database. Name your database snort. Select create the database.



If all goes well you should see the following box. Select the Ok button to proceed.



Press the Cancel button to get out of the Adding Database box.

10. Extract the create_mysql script from snort-1.8.4.tar using WinZip into c:\snortM\snortdb

Uncheck the use folder names checkbox if checked.

11. Open a shell window by going to Start→Run→cmd.exe Enter the following commands in your shell window:

```
cd c:\mysql\bin
```

```
MySQL grant INSERT,SELECT,CREATE,DELETE on snort.* to snort;
```

```
grant INSERT,SELECT,CREATE,DELETE on snort.* to  
sensor1@192.168.1.222;
```

(change the above to match your network environment where sensor1 is your sensor name and 192.168.1.222 is the address of your sensor. You will have to create a user for every sensor you create.)

```
exit
```

```
MySQL -u snort snort < c:\SnortM\snortdb\create_mysql
```

```
Exit ( To exit the shell window)
```

Install IIS

Insert your windows2000 cd into your cd-rom

1. Go to Start→Settings→Control Panel→Add/Remove programs
2. Select the Add/Remove Windows Components button.
3. Highlight Internet Information Services and Select the Details button.
4. Select the button that says Front Page Server Extensions 2000(This will install all other needed components)

5. Select the Ok button

6. Select Next

The System will begin copying files from the CD
Once finished you will get the following screen,

7. Select the Finish button to exit the installation.

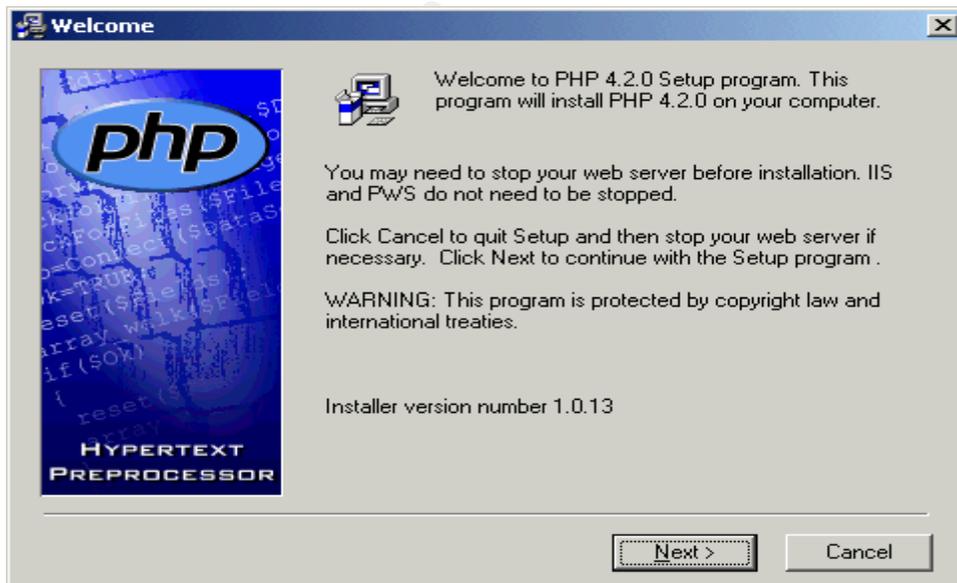


8. Patch IIS Microsoft Windows Update Web page supports updates for IIS you can access this by opening an Internet Explorer window and selecting Tools→Windows Update from the menu bar. Or type the following into your address bar <http://windowsupdate.microsoft.com> . Install all patches under critical updates, this may take multiple reboots.

Install PHP

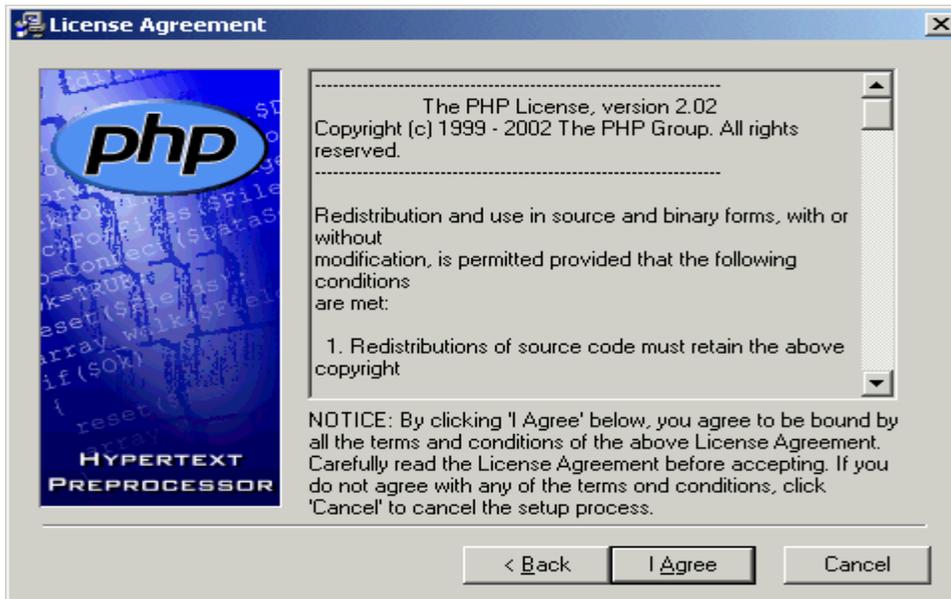
Navigate to the directory `c:\snortM\phpinst\` and run `php-4.2.0-installer.exe`.

1. On the screen below select the next button to proceed to the License Agreement Screen.

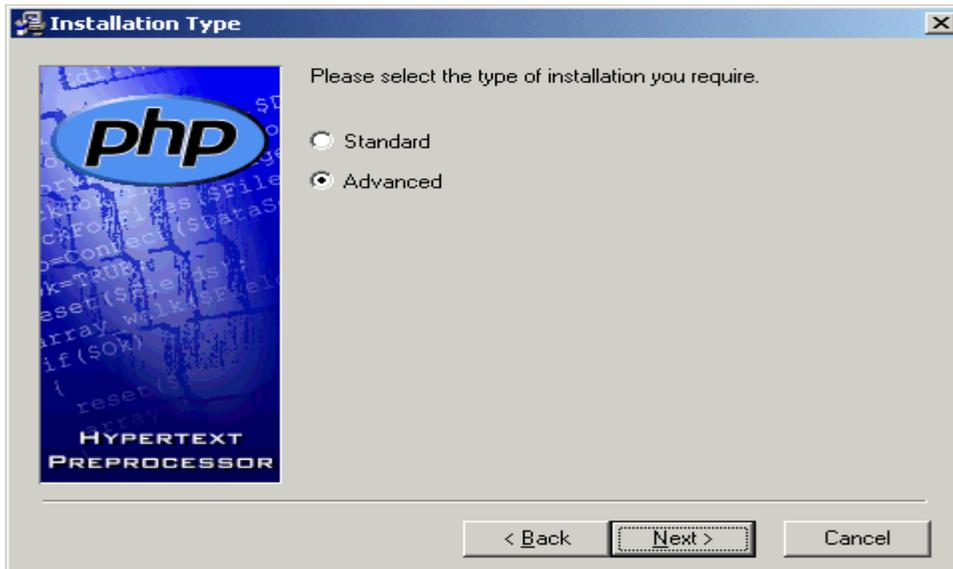


2. On the Screen Below Select the I Agree button to proceed to the Installation Type

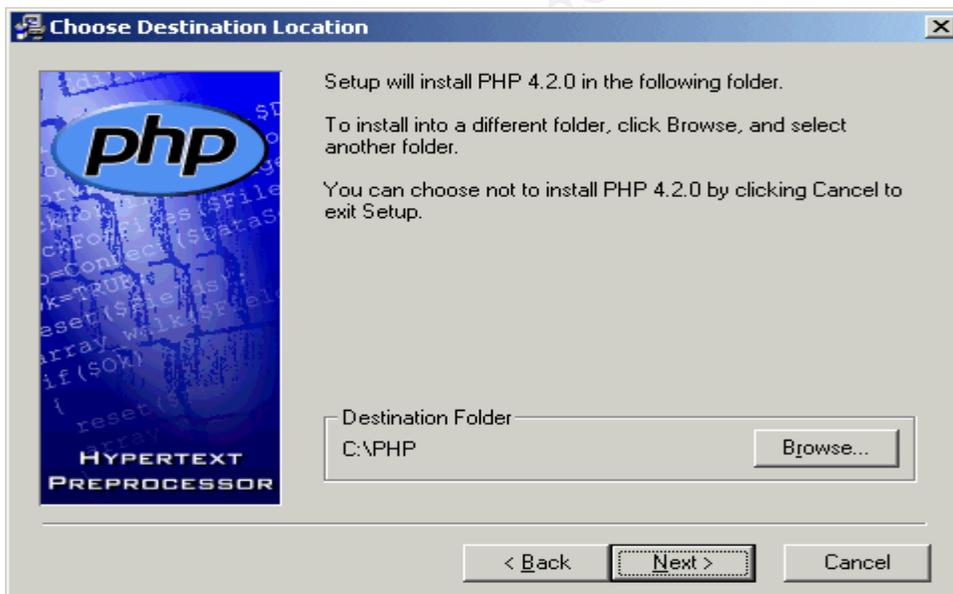
screen.



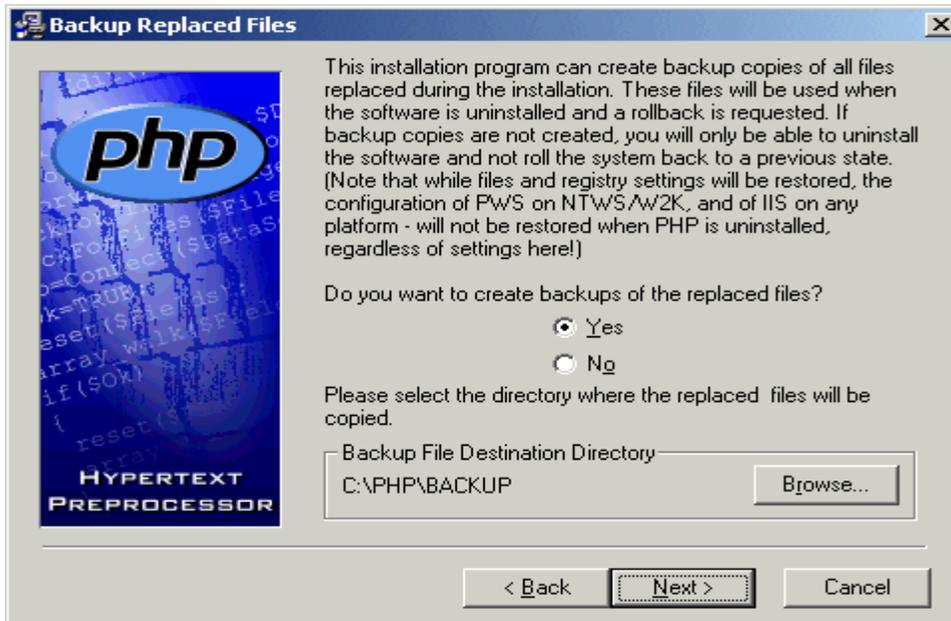
3. On the Screen below Select the Advanced radio button. Select the Next button to proceed to the Choose Destination Location screen.



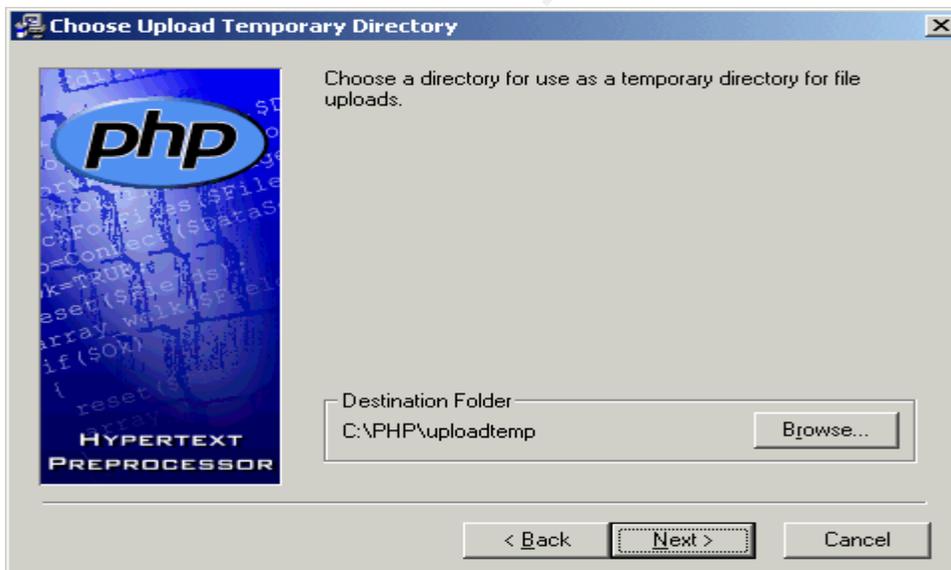
4. On the screen below accept the defaults and press the next button to proceed to the Backup Replaced Files screen.



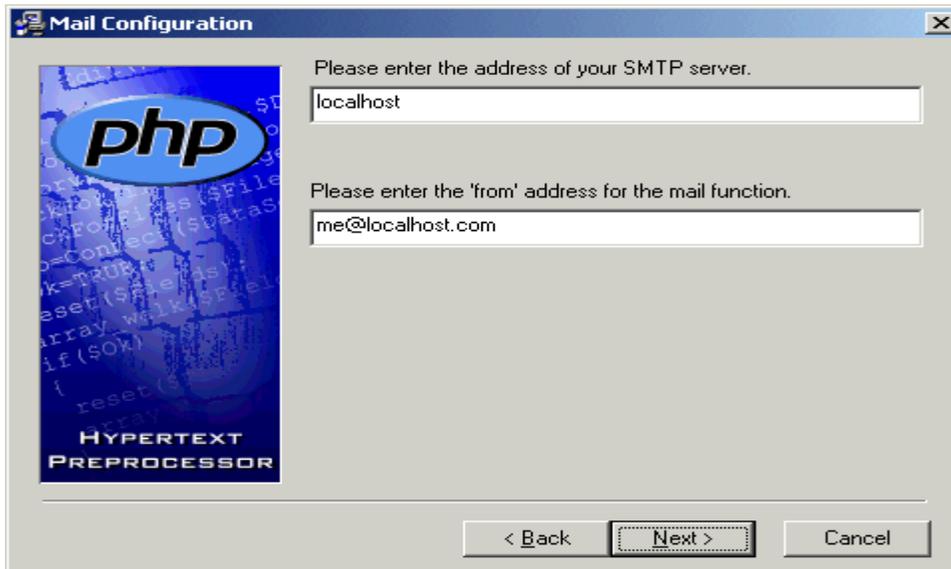
5. On the screen below accept the defaults and select the next button to proceed to the Choose Upload Temporary Directory.



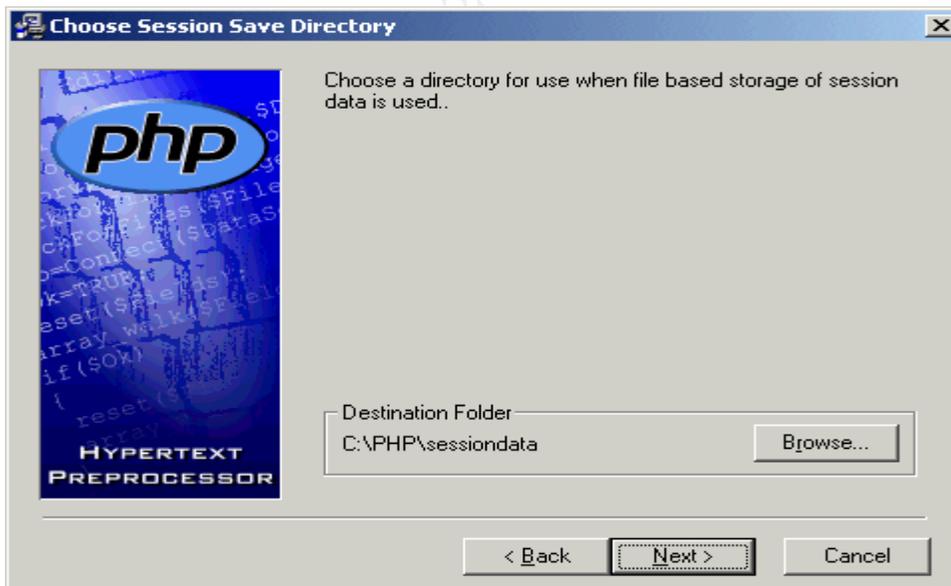
6. On the screen below Select the next button to proceed to the Mail Configuration screen.



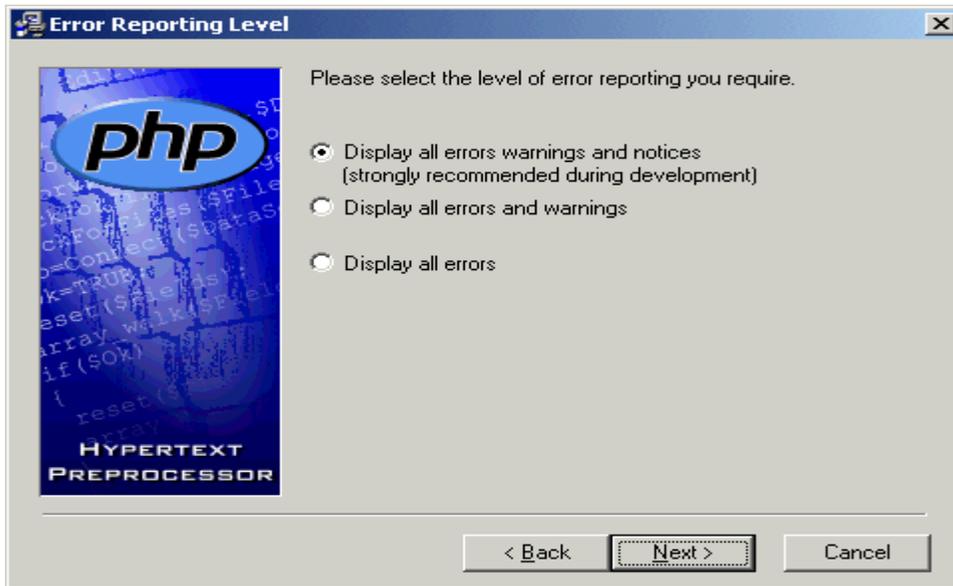
7. On the screen below press the next button to proceed to the Choose Session Save Directory.



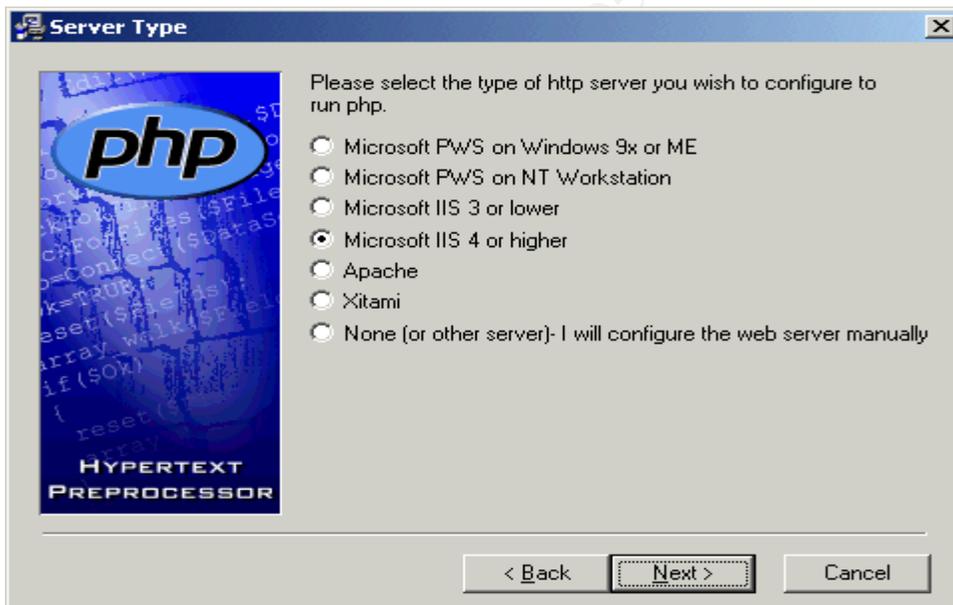
8. On the screen below select the next button to proceed to Error Reporting Level screen.



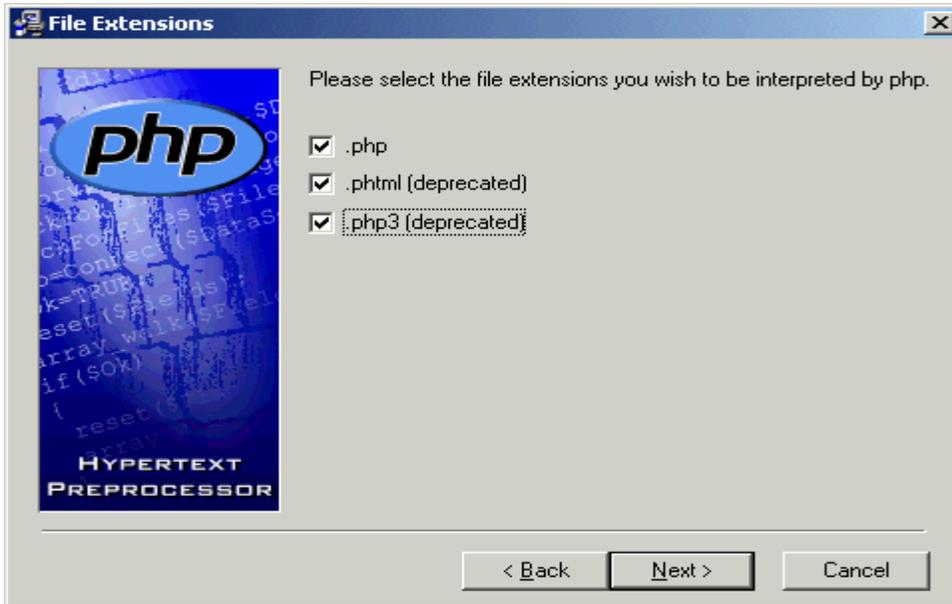
9. On the screen below select the next button to proceed to the Server Type screen.



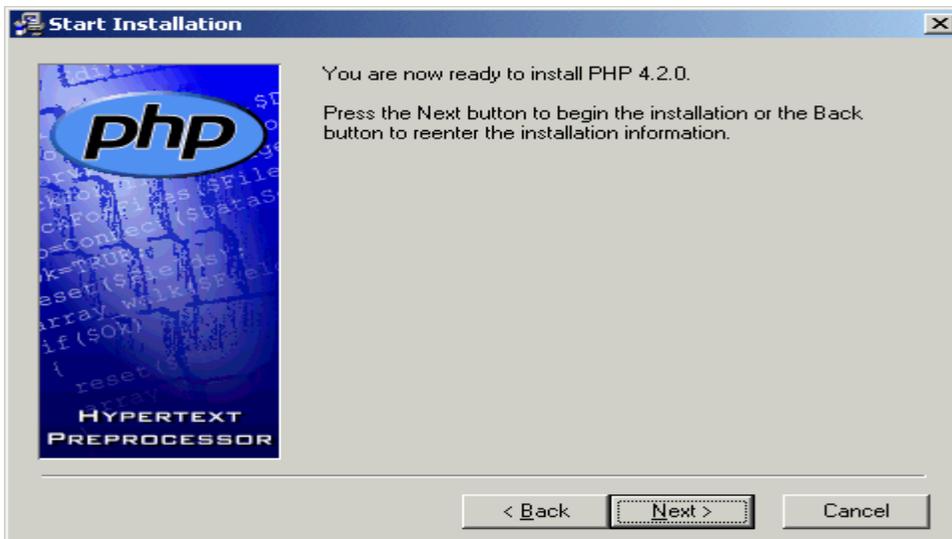
10. On the Screen below select the Microsoft IIS 4 or higher radio button and select the next button to proceed to the File Extensions screen.



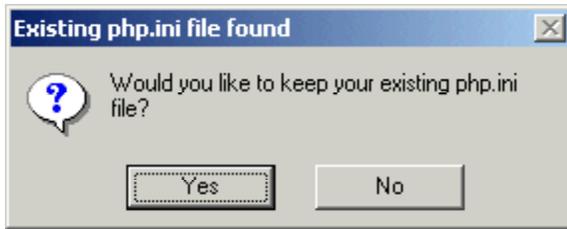
11. On the screen below select all three check boxes and select the next button to proceed the Start Installation screen.



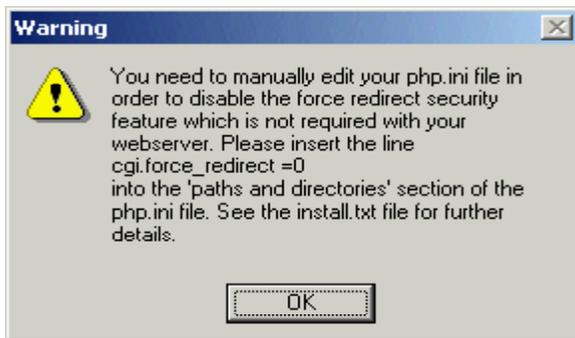
12. On the screen below select the next button to start installation.



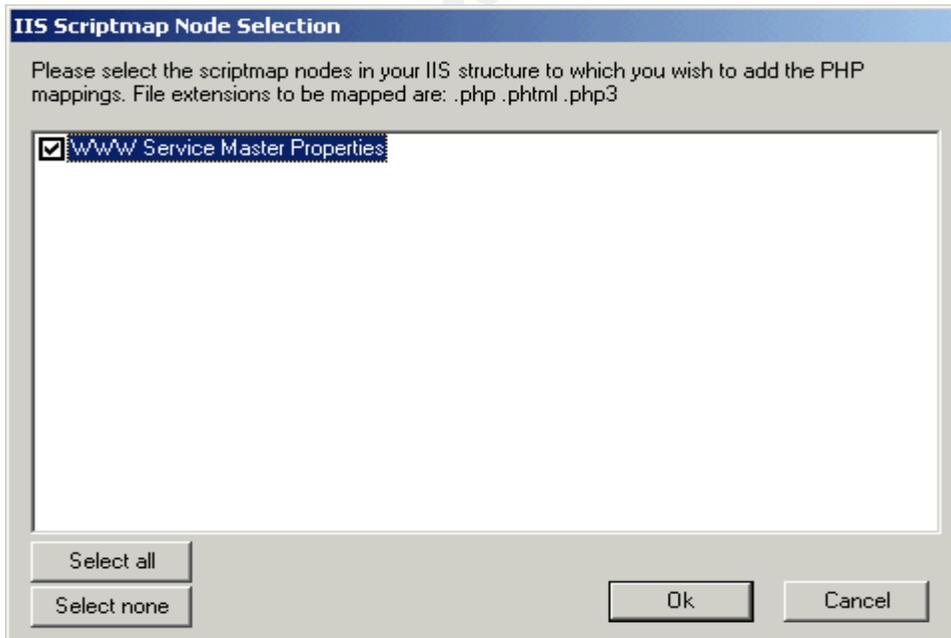
Setup will prompt with the box below select the Yes button.



Select the Ok button to proceed to IIS Script Node Selection.



Select the WWW Service Master Properties checkbox and select the OK button to proceed to the Installation complete screen.



13. Press the OK button to exit setup.



Install Acid and Configure its Components

Navigate to c:\snortM and Extract the following with the use folder names option checked in WinZip

adodb172.zip to C:\snortM\ADODB

acid-0.9.6b20.zip to c:\inetpub\wwwroot(Location of your root web folder)

phplot-4.4.6.zip to c:\snortM\

1. Navigate to c:\snortM\ADODB and open adodb.inc.php in WordPad.

Change the line:

```
$ADODB_Database = “”;
```

To read

```
$ADODB_Database = ‘C:\snortM\adodb’;
```

2. Navigate to c:\inetpub\wwwroot\acid and open acid_conf.php with WordPad

Change the line that reads

```
$DBlib_path = “”;
```

To read

```
$DBlib_path = “C:\snortM\adodb”;
```

Change the lines that read

```
$alert_dbname = “snort_log”;  
$alert_host = “localhost”;  
$alert_port = “”;  
$alert_user = “root”;  
$alert_password = “mypassword”;  
  
/* Archive DB connection parameters */  
$archive_dbname = “snort_archive”;  
$archive_host = “localhost”;
```

```

$archive_port      = "";
$archive_user      = "root";
$archive_password = "mypassword";

To Read
$alert_dbname      = "snort";
$alert_host        = "localhost";
$alert_port        = "";
$alert_user        = "snort";
$alert_password    = "";

/* Archive DB connection parameters */
$archive_dbname    = "snort";
$archive_host      = "localhost";
$archive_port      = "";
$archive_user      = "snort";
$archive_password = "";

```

and then change

```
$ChartLib_path = "";
```

To read

```
$ChartLib_path = "c:\snortM\phplot";
```

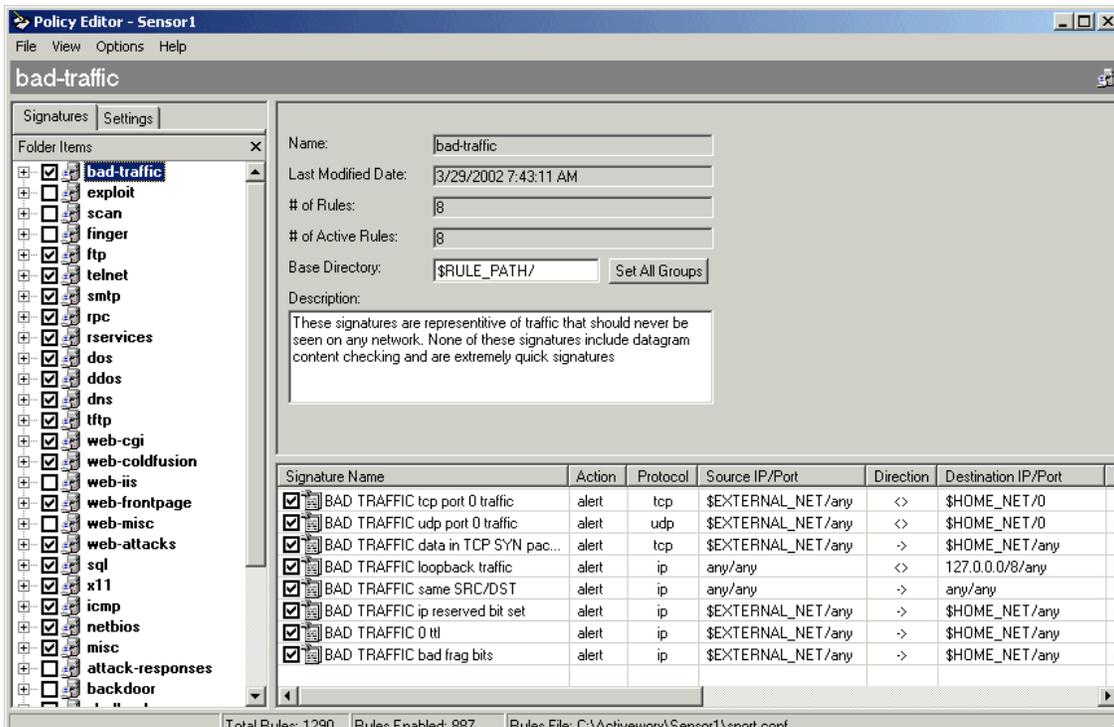
Reboot your management workstation now.

Configuring Your Sensor

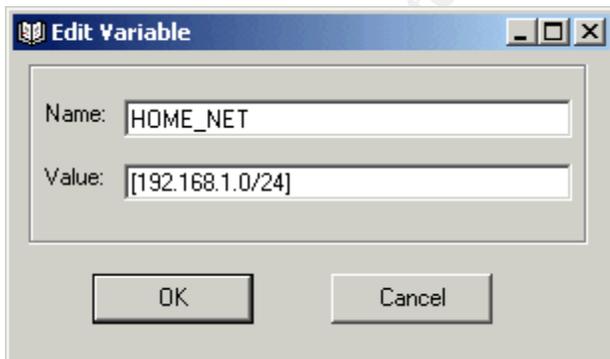
Once your management workstation has rebooted open IDS Policy Manager by going to Start→programs→ IDS Policy Manager.

1. Select the Policy Manager Tab and Highlight the Sensor1 entry in the Policy Manger screen and press <Ctrl>plus<O> to bring up the Policy Editor. You should have the screen below. Select the Settings tab to pull up the settings screen.

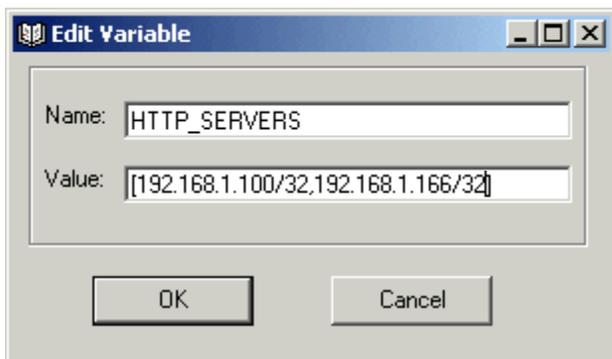
© SANS Institute 2000 - 2005, Author retains full rights.



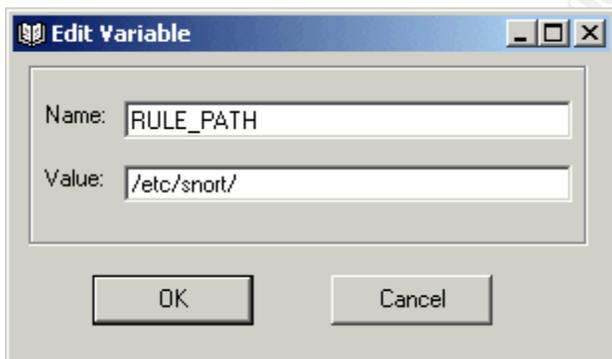
2. On the Settings screen under the variables tab we are going to change the variables to reflect our network. \$HOME_NET is the network that we wish to monitor. I usually choose the network that I'm on for example if we are on a 192.168.1. network with a net mask of 255.255.255.0 then we are using a 24 bit mask so our HOME_NET entry would be like this. Once completed uncheck the default entry HOME_NET = any



3. Next input your HTTP servers. I have two of them so my entry would look something like this. Once again Since these computers have a mask of 255.255.255.255 they have a 32-bit mask hence the /32. Using this logic do the Same for the SQL_SERVERS and DNS_SERVERS variables.



4. Edit the RULE_PATH variable to be /etc/snort remember this is the directory on the sensor where the snort daemon is pulling it's configuration from.



5. In the Left Hand Side of the screen select the Logging button and check the Database checkbox.

Enter the name of your sensor in the Sensor Name field .

Enter the name of the MySQL database we created which in this case was snort, into the DB Name field.

Select the mysql entry out of the DB Type drop down menu.

Select the log entry entry out of the Log Rule Type drop down menu.

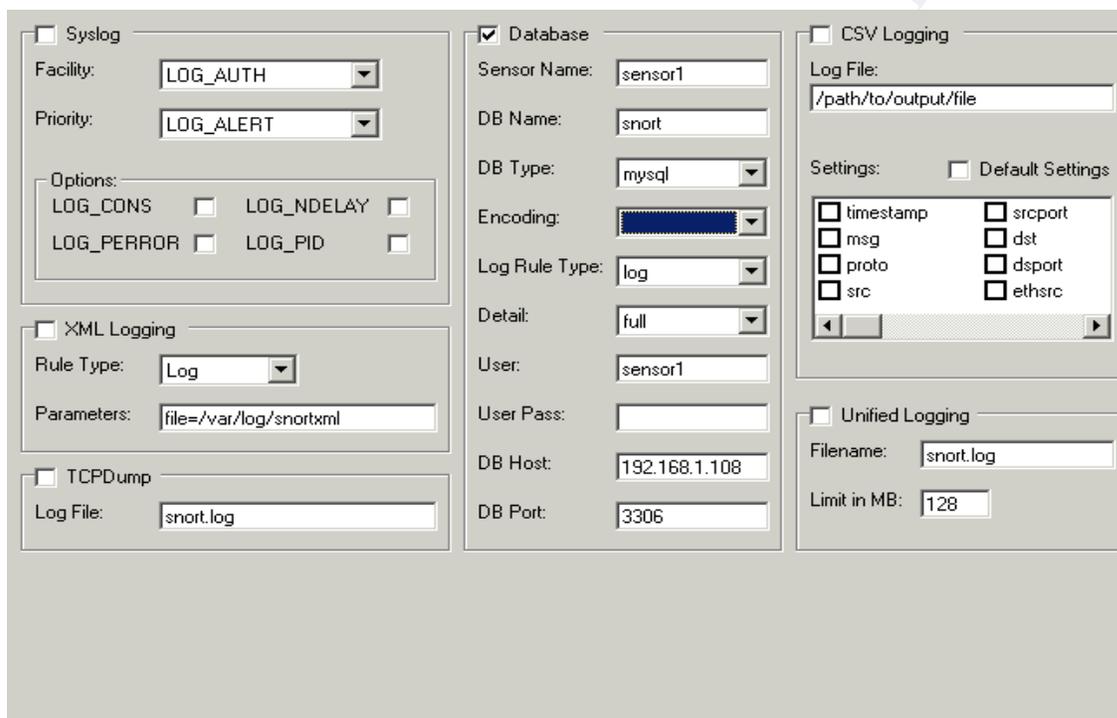
Enter the user that we created for this sensor into the User field. In mysql it adds @ip address you connect from to your username so we just need to put in sensor1 MySQL will see it as [sensor1@192.168.1.222](#)

In this case we have not yet set a password on our sensor1@192.168.1.1 so leave the User Pass: field blank.

The DB Host is the address of our management system in my case it is 192.168.1.108 this will change based on your environment.

In the DB port field enter 3306 this is the default port that MySQL listens on.

Once finished select file→Save and Exit

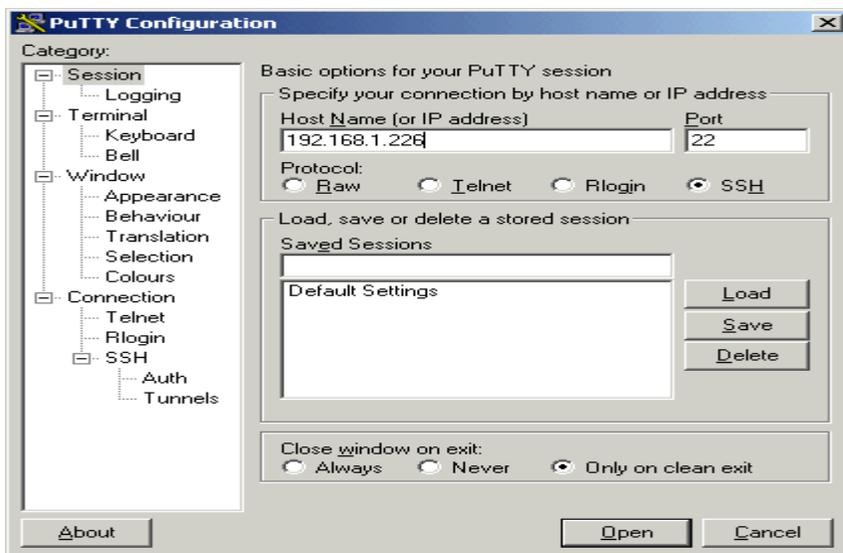


The screenshot displays the Snort configuration window for logging. It is divided into several sections:

- Syslog:** Facility is set to LOG_AUTH and Priority to LOG_ALERT. Options for LOG_CONS, LOG_NDELAY, LOG_PERROR, and LOG_PID are all unchecked.
- Database:** This section is checked. Sensor Name is 'sensor1', DB Name is 'snort', DB Type is 'mysql', Encoding is set to a blue icon, Log Rule Type is 'log', Detail is 'full', User is 'sensor1', User Pass is blank, DB Host is '192.168.1.108', and DB Port is '3306'.
- CSV Logging:** Log File is '/path/to/output/file'. Settings are not default, with options for timestamp, msg, proto, src, srcport, dst, dsport, and ethsrc, all of which are unchecked.
- XML Logging:** Rule Type is 'Log' and Parameters are 'file=/var/log/snortxml'.
- TCPDump:** Log File is 'snort.log'.
- Unified Logging:** Filename is 'snort.log' and Limit in MB is '128'.

6. This will take you back to the Policy Manger window. Select the Sensor Manger tab, Highlight your sensor (in my case Sensor1) and press the <Ctrl>plus<P> keys. This will upload your policy to your sensor.

7. Now we need to test our configuration. Navigate to c:\snortM and select putty.exe, you should get the screen below. Enter the IP address of your sensor and select the SSH radio button and select the Open button.



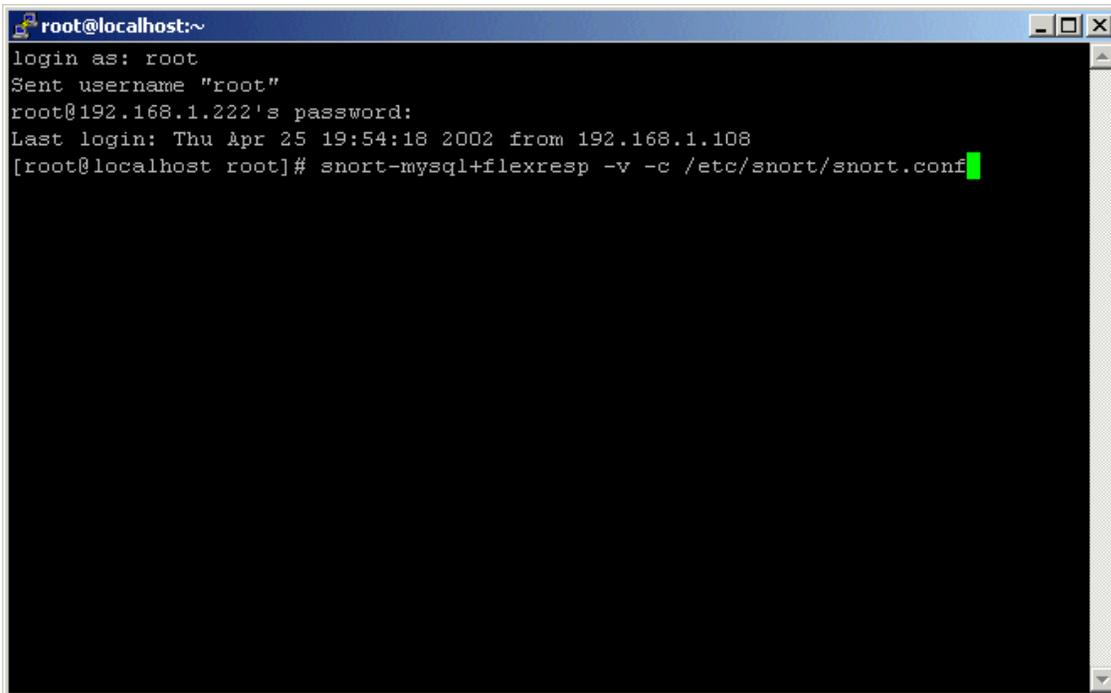
8. When we setup SCP in IDS Policy it should have cached the servers host key as SCP is part of SSH. If for whatever reason the key is not in your local cache you will receive the prompt below. Select the Yes button.



9. You should get a screen like the one below, log in as root with your secure password. Now we are going to test are snort configuration by entering the following commands

snort-mysql+flexresp -v -c /etc/snort/snort.conf

The `-v` means verbose mode and the `-c` is the switch to tell the snort executable which configuration file to use.



```
root@localhost:~
login as: root
Sent username "root"
root@192.168.1.222's password:
Last login: Thu Apr 25 19:54:18 2002 from 192.168.1.108
[root@localhost root]# snort-mysql+flexresp -v -c /etc/snort/snort.conf
```

10. Snort will give you a short summary of the options that you have enabled and then it should start showing you the traffic that is passing over its interface. Press the <Ctrl>plus<C> keys to kill snort.

If you don't get a screen with traffic passing over it double check the configuration settings in IDS policy manger.

11. Great you snort is working with configuration file that we have produced. Now restart the snortd service by typing the following into your putty session.

```
service snortd stop
service snortd start
```

Viewing Alerts with ACID

Open a Internet Explorer browser window and type the following into address bar <http://127.0.0.1/acid/index.html> You should get a screen where Acid tells you that it has an error.

1. Select the go to Setup Page link.
2. Select Create ACID AG.
3. When this is complete return to the address above you should get the Acid main screen. Select the number next to the The Total Number of Alerts line. Now you should something like the screen below. If nothing is there don't worry it will probably take some time to see your first alert.

ID	Signature	Timestamp	Source Address	Dest. Address	Layer 4 Proto
#0-(1-7)	[url] SCAN Proxy attempt	2002-04-25 00:23:09	192.168.1.102	192.168.1.222:1080	TCP
#1-(1-1)	ICMP supescan echo	2002-04-25 00:22:50	192.168.1.100	192.168.1.222	ICMP
#2-(1-2)	spp_portscan detected from 192.168.1.100 (THRESHOLD 4 connections exceeded in 0 seconds)	2002-04-25 00:22:50	192.168.1.100	unknown	IP
#3-(1-3)	spp_portscan from 192.168.1.100: 104 connections across 1 hosts: TCP(104), UDP(0)	2002-04-25 00:22:54	192.168.1.100	unknown	IP
#4-(1-4)	spp_portscan from 192.168.1.100: 131 connections across 1 hosts: TCP(131), UDP(0)	2002-04-25 00:22:58	192.168.1.100	unknown	IP
#5-(1-5)	spp_portscan from 192.168.1.100: 148 connections across 1 hosts: TCP(148), UDP(0)	2002-04-25 00:23:02	192.168.1.100	unknown	IP
#6-(1-6)	spp_portscan from 192.168.1.100: 141 connections across 1 hosts: TCP(141), UDP(0)	2002-04-25 00:23:06	192.168.1.100	unknown	IP
#7-(1-8)	spp_portscan from 192.168.1.100: 125 connections across 1 hosts: TCP(125), UDP(0)	2002-04-25 00:23:10	192.168.1.100	unknown	IP
#8-(1-13)	INFO - Possible Squid Scan	2002-04-25 00:23:29	192.168.1.100	192.168.1.222:3128	TCP
#9-(1-14)	INFO - Possible Squid Scan	2002-04-25 00:23:29	192.168.1.100	192.168.1.222:3128	TCP
#10-(1-16)	INFO - Possible Squid Scan	2002-04-25 00:23:30	192.168.1.100	192.168.1.222:3128	TCP
#11-(1-9)	spp_portscan from 192.168.1.100: 142 connections across 1 hosts: TCP(142), UDP(0)	2002-04-25 00:23:14	192.168.1.100	unknown	IP
#12-(1-10)	spp_portscan from 192.168.1.100: 127 connections across 1 hosts: TCP(127), UDP(0)	2002-04-25 00:23:18	192.168.1.100	unknown	IP
#13-(1-11)	spp_portscan from 192.168.1.100: 151 connections across 1 hosts: TCP(151), UDP(0)	2002-04-25 00:23:22	192.168.1.100	unknown	IP
#14-(1-12)	spp_portscan from 192.168.1.100: 128 connections across 1 hosts: TCP(128), UDP(0)	2002-04-25 00:23:26	192.168.1.100	unknown	IP
#15-(1-15)	spp_portscan from 192.168.1.100: 127 connections across 1 hosts: TCP(127), UDP(0)	2002-04-25 00:23:30	192.168.1.100	unknown	IP
#16-(1-18)	SCAN Proxy attempt	2002-04-25 00:23:34	192.168.1.100	192.168.1.222:8080	TCP
#17-(1-17)	spp_portscan from 192.168.1.100: 147 connections across 1 hosts: TCP(147), UDP(0)	2002-04-25 00:23:34	192.168.1.100	unknown	IP
#18-(1-19)	spp_portscan from 192.168.1.100: 81 connections across 1 hosts: TCP(81), UDP(0)	2002-04-25 00:25:54	192.168.1.100	unknown	IP
#19-(1-20)	spp_portscan from 192.168.1.100: 10 connections across 1 hosts: TCP(10), UDP(0)	2002-04-25 00:25:59	192.168.1.100	unknown	IP
#20-(1-21)	spp_portscan from 192.168.1.100: 2 connections across 1 hosts: TCP(2), UDP(0)	2002-04-25 00:26:05	192.168.1.100	unknown	IP
#21-(1-22)	spp_portscan from 192.168.1.100: 1 connections across 1 hosts: TCP(1), UDP(0)	2002-04-25 00:26:09	192.168.1.100	unknown	IP
#22-(1-30)	[url] SCAN Proxy attempt	2002-04-25 00:41:19	192.168.1.166	192.168.1.222:1080	TCP
#23-(1-36)	INFO - Possible Squid Scan	2002-04-25 00:41:40	192.168.1.166	192.168.1.222:3128	TCP
#24-(1-37)	INFO - Possible Squid Scan	2002-04-25 00:41:41	192.168.1.166	192.168.1.222:3128	TCP
#25-(1-38)	INFO - Possible Squid Scan	2002-04-25 00:41:41	192.168.1.166	192.168.1.222:3128	TCP
#26-(1-40)	SCAN Proxy attempt	2002-04-25 00:41:45	192.168.1.166	192.168.1.222:8080	TCP
#27-(1-42)	SCAN Proxy attempt	2002-04-25 00:41:46	192.168.1.166	192.168.1.222:8080	TCP
#28-(1-23)	spp_portscan from 192.168.1.100: 1 connections across 1 hosts: TCP(1), UDP(0)	2002-04-25 00:39:34	192.168.1.100	unknown	IP
#29-(1-24)	spp_portscan: End of portscan from 192.168.1.100. TOTAL time(201s) hosts(1) TCP(1566) UDP(0)	2002-04-25 00:41:02	192.168.1.100	unknown	IP
#30-(1-25)	spp_portscan detected from 192.168.1.166 (THRESHOLD 4 connections exceeded in 0 seconds)	2002-04-25 00:41:02	192.168.1.166	unknown	IP
#31-(1-26)	spp_portscan from 192.168.1.166: 129 connections across 1 hosts: TCP(129), UDP(0)	2002-04-25 00:41:06	192.168.1.166	unknown	IP
#32-(1-27)	spp_portscan from 192.168.1.166: 151 connections across 1 hosts: TCP(151), UDP(0)	2002-04-25 00:41:10	192.168.1.166	unknown	IP
#33-(1-28)	spp_portscan from 192.168.1.166: 141 connections across 1 hosts: TCP(141), UDP(0)	2002-04-25 00:41:14	192.168.1.166	unknown	IP
#34-(1-29)	spp_portscan from 192.168.1.166: 130 connections across 1 hosts: TCP(130), UDP(0)	2002-04-25 00:41:18	192.168.1.166	unknown	IP
#35-(1-31)	spp_portscan from 192.168.1.166: 137 connections across 1 hosts: TCP(137), UDP(0)	2002-04-25 00:41:22	192.168.1.166	unknown	IP
#36-(1-32)	spp_portscan from 192.168.1.166: 140 connections across 1 hosts: TCP(140), UDP(0)	2002-04-25 00:41:26	192.168.1.166	unknown	IP
#37-(1-33)	spp_portscan from 192.168.1.166: 124 connections across 1 hosts: TCP(124), UDP(0)	2002-04-25 00:41:30	192.168.1.166	unknown	IP
#38-(1-34)	spp_portscan from 192.168.1.166: 111 connections across 1 hosts: TCP(111), UDP(0)	2002-04-25 00:41:34	192.168.1.166	unknown	IP
#39-(1-35)	spp_portscan from 192.168.1.166: 148 connections across 1 hosts: TCP(148), UDP(0)	2002-04-25 00:41:38	192.168.1.166	unknown	IP
#40-(1-39)	spp_portscan from 192.168.1.166: 146 connections across 1 hosts: TCP(146), UDP(0)	2002-04-25 00:41:42	192.168.1.166	unknown	IP
#41-(1-41)	spp_portscan from 192.168.1.166: 139 connections across 1 hosts: TCP(139), UDP(0)	2002-04-25 00:41:46	192.168.1.166	unknown	IP
#42-(1-43)	spp_portscan from 192.168.1.166: 85 connections across 1 hosts: TCP(85), UDP(0)	2002-04-25 00:47:51	192.168.1.166	unknown	IP
#43-(1-44)	spp_portscan from 192.168.1.166: 3 connections across 1 hosts: TCP(3), UDP(0)	2002-04-25 00:47:57	192.168.1.166	unknown	IP
#44-(1-45)	[arachNIDS] ICMP webtrends scanner	2002-04-25 00:55:33	192.168.1.100	192.168.1.222	ICMP
#45-(1-46)	[arachNIDS] ICMP webtrends scanner	2002-04-25 17:00:49	192.168.1.100	192.168.1.222	ICMP
#46-(2-2)	[url] SCAN Proxy attempt	2002-04-25 17:37:26	192.168.1.166	192.168.1.226:1080	TCP
#47-(2-3)	[url] SCAN Proxy attempt	2002-04-25 17:37:26	192.168.1.166	192.168.1.226:1080	TCP
#48-(2-4)	[url] SCAN Proxy attempt	2002-04-25 17:37:27	192.168.1.166	192.168.1.226:1080	TCP
#49-(2-1)	ICMP supescan echo	2002-04-25 17:37:08	192.168.1.166	192.168.1.226	ICMP

Congratulations you have just made yourself a snort sensor.

Conclusion

Snort provides small and enterprise environments alike a robust and reliable Intrusion Detection System. While I gave you an example of the basic setup of snort there is still a great deal of tuning that needs to be done at this point. More than likely you will need to use IDS policy manger to enable/disable certain signatures to suit your environment. For more information on rules consult the Snort Users Manual included in the Snort-1.8.4.tar.gz or on the snort website at http://www.snort.org/docs/writing_rules/

For all of you who work in a pure win32 environment have no fear. Silicon Defense updates a binary of snort ported for the win32 Operating Systems. They Also have extensive documentation on the Setup of snort on win32. <http://www.silicondefense.com>

The Sensor that we created is relatively secure due to the fact the we stripped down the normally bloated install of Red Hat. The packages that we installed need to be updated due to potential exploits in them. There is documentation on how to do this included in the Center For Internet Security Linux Benchmark v1.0.0. This can be obtained from <http://www.cisecurity.org>

For future updates of Snort I have included all that is needed to compile the latest version of snort in its binary format. At the time I completed this writing they had released a binary only version of snort 1.8.6. Out of the box the binary does not support MySQL to upgrade to the most recent version of snort you would do the following on your snort sensor with internet access.

```
cd /snort-install  
wget http://www.snort.org/dl/snort-1.8.6.tar.gz  
tar -xzf snort-1.8.6.tar.gz  
cd /snort-install/snort-1.8.6.tar.gz  
./configure --with-mysql  
make  
make install
```

this will place the snort binary into /usr/local/bin
change your snortd script accordingly.

Also depending on what rules you have enabled you may need to update to the new rule set. If you download snortrules.tar.gz from <http://www.snort.org/dl/signatures/snortrules.tar.gz> you can extract these files into a new directory in your ActiveWorx folder and create a new policy by pointing IDS policy manger to the updated snort.conf.

I hope that this paper was both helpful and informative and provides the reader with enough information to build a IDS sensor on the cheap.

Technical Reviewers

Dave Snell MCSE, CNE Enterprise Network Administrator City of Kansas City, Missouri
Rochelle Richeson Systems Analyst City of Kansas City, Missouri
David Evans Enterprise Network Administrator City of Kansas City, Missouri

Resources

Snort Users Manual available from:
http://www.snort.org/docs/writing_rules/

ActiveWorx FAQ available from:
<http://www.activeworx.com/idspm/faq.htm>

Snort 1.8.6b105 **RELEASE** running IIS / MySQL Acid... (Michael Steel) available from
http://www.silicondefense.com/techsupport/winsnortacid-iis_1.8.6.htm

Red Hat Linux 7.2 Official Reference Guide available from
<http://www.redhat.com/docs/manuals/linux/RHL-7.2-Manual/ref-guide/>
MySQL Manual available from:
<http://http://www.mysql.com/doc/>

Bad Packets: Snort -- the Dobermans behind the firewall (Wes Simonds) available from:
http://searchnetworking.techtarget.com/originalContent/0,289142,sid7_gci804882,00.html

Intrusion Detection Systems (IDSs): Perspective (The Gartner Group) available from:
<http://www.gartner.com/DisplayTechOverview?id=320015>

Network Intrusion Detection Using Snort (Dave Wreski & Christopher Pallack) available from :
http://www.linuxsecurity.com/feature_stories/using-snort.html

PHP : Manual : FAQ available from:
<http://www.php.net/manual/en/faq.php>

The Putty User Manual available from:
<http://the.earth.li/~sgtatham/putty/0.52/html/doc/>

Center For Internet Security Linux Benchmark v1.0.0. Available from:
<http://www.cisecurity.org>

Red Hat Certified Engineer Study Guide (Bill McCarty :Sybex: ISBN 0-7821-2793-2)

© SANS Institute 2000 - 2005, Author retains full rights.