

# **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 permited 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

# 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 Roesh 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 <a href="http://www.gartner.com/DisplayTechOverview?id=320015">http://www.gartner.com/DisplayTechOverview?id=320015</a>). 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-i386disc1.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 autobooting to cd consult the red hat 7.2 documentation <u>http://www.redhat.com/docs</u> 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 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++3libstdc++3devel linuxconf lvnx m4make 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.

# **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-devel-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 My-SQL-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  $\setminus$ 

-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 In -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

## 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

🖫 Welcome		×
	Welcome to IDS Policy Manager Setup program. This program will install IDS Policy Manager on your computer. It is strongly recommended that you exit all Windows programs before running this Setup Program. Click Cancel to quit Setup and close any programs you have running. Click Next to continue with the Setup program . WARNING: This program is protected by copyright law and international treaties.	
	Unauthorized reproduction or distribution of this program, or an portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.	y
	<u>N</u> ext> Cancel	

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

覺 Choose Destination Lo	cation	1
	Setup will install IDS Policy Manager in the following folder. To install into a different folder, click Browse, and select another folder. You can choose not to install IDS Policy Manager by clicking Cancel to exit Setup.	
	Destination Folder C:\Program Files\Activeworx Browse	2
	< <u>B</u> ack <u>Next&gt;</u> Cancel	

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.

Select Destination Directory	×
D:VActiveworx	ОК
<ul> <li>c:\</li> <li>Documents and Settings</li> <li>Program Files</li> <li>SnortM</li> <li>System Volume Information</li> <li>winnt</li> </ul>	Cancel

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

覺 Select Program Manag	er Group				×	
	Enter the name Policy Manage	e of the Progra er icons to:	m Manager group to	add IDS		
	Activeworx					
	Accessories Administrative Microsoft Offic Startup WinZip	Tools ce Tools				
		< <u>B</u> ack	Next >	Cancel	-	

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

覺 Start Installation	×	1
	You are now ready to install IDS Policy Manager. Press the Next button to begin the installation or the Back button to reenter the installation information.	
	< <u>B</u> ack <u>Next&gt;</u> Cancel	

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 $\rightarrow$  programs $\rightarrow$  Activeworx $\rightarrow$ 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

Check for	Updates 🔀
٩	Would you like IDS Policy Manager to Auto Check for updates on Startup?
	<u>Yes</u> <u>N</u> o

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

#### select Policy→Add Policy

🛃 ActiveWo	rx - IDS P	olicy Manager					
File Sensor	Options	Help					
Name		Policy Status	Policy	IP Address	Version	Info	
	·····:						
Sensor Manag	<u>ger j</u> Policy	Manager Logging	J				
ActiveWorx - IE	)S Policy M	anager					

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.

add New Policy	/	
Policy Name:	Sensor1	Locked 🗖
IDS System/Version	Snort 1.8.4	
Policy Location:	C:\Activeworx\Sensor1\snort.conf	Browse
Description:	Policy For Sensor 1	
OK	Cancel	
	\$ <b>9</b>	

9. Now go back to the Sensor Manager screen by selecting the Sensor Manger tab. From the menu bar select Sensor  $\rightarrow$  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.

🚯 Add Sensor	×
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:	*******
Password(Confirm):	*******
Upload Directory:	/etc/snort
ОК	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

Setup SCP	×
You will need to setup SCP now. Press OK to Continu	ie
OK Cancel	

You should get the screen below as to whether or not you want to store the remote key in your cach 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.

Welcome	×
	Welcome to the MySQL Servers and Clients 3.23.49 Setup program. This program will install MySQL Servers and Clients 3.23.49 on your computer.
	It is strongly recommended that you exit all Windows programs before running this Setup program. Click Cancel to guit Setup and then close any programs you
	have running. Click Next to continue with the Setup program.
	WARNING: This program is protected by copyright law and international treaties.
Insta	portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.
	<u>N</u> ext > Cancel

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.

Choose Destination Loca	tion
	Setup will install MySQL Servers and Clients 3.23.49 in the following folder. To install to this folder, click Next. To install to a different folder, click Browse and select another folder. You can choose not to install MySQL Servers and Clients 3.23.49 by clicking Cancel to exit Setup.
Insta	Destination Folder C:\mysql Browse
	< <u>B</u> ack <u>Next</u> Cancel

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

Setup Type			×	
	Click the type o	of Setup you prefer, then click Next.		
	• Typical	Program will be installed with the most common options. Recommended for most users.		
	C <u>C</u> ompact	Program will be installed with minimum required options.		
Install Sheld	C Cystom	You may choose the options you want to install. Recommended for advanced users.		
		< <u>B</u> ack <u>N</u> ext > Cancel		

<u>Rac</u>

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

Setup Complete		
	Setup has finished installing MySQL Servers and Clients 3.23.49 on your computer. Setup can launch the Read Me file and MySQL Servers and Clients 3.23.49. Choose the options you want below.	
Instal ISHeld	Click Finish to complete Setup.	
	< Back Finish	

\*\*\*\*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. <u>http://www.silicondefense.com/techsupport/windows.htm</u> \*\*\*\*\*

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.

💑 WinMySQLadmin Quick Setup				
MSQ	ļL,	by T.C DataKo	nsultAB	101
Create the my ini file with default values and the	user below. Recon	nmended to no	ovice user.	
User name root	<u>Password</u>			
WinMySQLadmin Ver 1.4	?	Cancel	ОК	

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.

💑 WinMySQLadmin 1.4			_	
WinMySQLadmin Ver Copyright (C) 1979-21 All rights reserved. S This software comes	1.4 for Win95/Wir 001 MySQL AB Ma ee the file PUBLIC with ABSOLUTELY	n98/NT/Win2000 onty Program KB _Detron HB. : for licence information. Y NO WARRANTY: see the file PUBL	Right Click for Menu options	8
🚺 Environment 🚺 Start Check 🚺 Server	📔 📥 my.ini Setup 🛛 🕻	🚺 Err File 🚺 Variables 🚺 Process	🖯 Databases 🛃 Report	
Enviroment Local Host Name MONITOR1	MyODBC Not Found			
Local User Name Administrator				
OS Platform Windows 2000 Service Pack 2				
Local IP Address				
monitor1 192.168.1.108	Server			
Total Physical Memory	Server Info	Host Info	Open tables	_
130596 КВ НАМ				_
Powered by	Client Info	Protocol Info	Open files	-
MySQL	Uptime	Threads running	Open streams	-
Set Server's Query Interval	Slow queries	Opened tables	Questions	-
Hide me Extended Server Status	,			
				11.

8. 5	Select the	databases	tab to	bring up	the	databases screen.
------	------------	-----------	--------	----------	-----	-------------------

💑 WinMySQLadmin 1.	4			<u>_   X</u>
MYSQL	WinMySQLadmin Ver 1.4 for Win95/Win98/NT/Win200 Copyright (C) 1979-2001 MySQL AB Monty Program KE All rights reserved. See the file PUBLIC for licence info This software comes with ABSOLUTELY NO WARRAN	0 _Detron HB. rmation. 'Y: see the file PUBL!	Right Click for Menu options IC for details	8
1 Environment	Start Check 🚺 Server 📥 my.ini Setup 🚺 Err File 🚺	/ariables 🚺 Process	🖯 Databases 🛃 Report	
Databases	Database	ables		
	92 168 1 108)			
Table Columns	- 112-			
				F
Table Indexes				
				F

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.

💑 Adding Database		_ 🗆 🗵
Note: The name of th	e database must be unique and with	out blank spaces
	Database Name:	
MySOL	snort	
	Create the Database	Cancel

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

WinMyS(	LAdmin 1.4	×
<b>i</b>	The database was crea	ated
	OK	

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 $\rightarrow$ Run $\rightarrow$ 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  $\rightarrow$  Settings  $\rightarrow$  Control Panel  $\rightarrow$  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.

Windows Components Wizard		$\mathbf{X}$	
	Completing the Windows Components Wizard You have successfully completed the Windows Components Wizard.		
Windows 2000	To close this wizard, click Finish.		
	< <u>B</u> ack <b>Finish</b>		

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 <a href="http://windowsupdate.microsoft.com">http://windowsupdate.microsoft.com</a>. 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.

🖥 License Agreement				×
	The PHP License, Copyright (c) 1999 - 2002 The reserved. Redistribution and use in source without modification, is permitted provid conditions are met: 1. Redistributions of source ca copyright	version 2.02 PHP Group. All righ  e and binary forms ded that the followin ode must retain the	nts , with or ng e above	10.
HYPERTEXT PREPROCESSOR	NOTICE: By clicking 'I Agree' b all the terms and conditions of the Carefully read the License Agree do not agree with any of the ter 'Cancel' to cancel the setup pro-	elow, you agree to he above License a ement before acce ms ond conditions, icess.	be bound by Agreement. pting. If you click	
	< <u>B</u> ack	l <u>A</u> gree	Cancel	

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

🚰 Installation Type		×	
	Please select the type of installation you require.		
Hypertext Preprocessor	<ul> <li>Advanced</li> </ul>		
	< <u>B</u> ack Next > Cancel		

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

覺 Choose Destination Loc	ation	×
	Setup will install PHP 4.2.0 in the following folder.	
	To install into a different folder, click Browse, and select another folder.	
	You can choose not to install PHP 4.2.0 by clicking Cancel to exit Setup.	
Hypertext Preprocessor	Destination Folder C:\PHP Browse	
	< <u>B</u> ack <u>Next</u> > Cancel	

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

월 Backup Replaced Files		×	
HYPERTEXT PREPROCESSOR	This installation program can create backup copies of all files replaced during the installation. These files will be used when the software is uninstalled and a rollback is requested. If backup copies are not created, you will only be able to uninstall the software and not roll the system back to a previous state. (Note that while files and registry settings will be restored, the configuration of PWS on NTWS/W2K, and of IIS on any platform - will not be restored when PHP is uninstalled, regardless of settings here!) Do you want to create backups of the replaced files? © Yes © No Please select the directory where the replaced files will be copied. Backup File Destination Directory C:\PHP\BACKUP Browse		
	< <u>B</u> ack <u>Next&gt;</u> Cancel	_	

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

screen.		
🛃 Choose Upload Tempora	ary Directory	×
	Choose a directory for use as a temporary directory for file uploads.	
HYPERTEXT PREPROCESSOR	Destination Folder C:\PHP\uploadtemp Browse	]
	< <u>B</u> ack <u>Next&gt;</u> Cancel	

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.

🛃 Choose Session Save Di	irectory	×
	Choose a directory for use when file based storage of session data is used	
HYPERTEXT	Destination Folder C:\PHP\sessiondata <u>Br</u> owse	
	< <u>B</u> ack <u>Next</u> Cancel	_

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.

월 Server Type	×
HYPERTEXT PREPROCESSOR	Please select the type of http server you wish to configure to run php. Microsoft PWS on Windows 9x or ME Microsoft PWS on NT Workstation Microsoft IIS 3 or lower Microsoft IIS 4 or higher Apache Xitami None (or other server)- I will configure the web server manually
	< <u>B</u> ack Next> Cancel

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

覺 File Extensions	X	1
HYPERTEXT PREPROCESSOR	Please select the file extensions you wish to be interpreted by php.	
	< <u>B</u> ack <u>N</u> ext > Cancel	

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

覺 Start Installation		×
Hypertext Preprocessor	You are now ready to install PHP 4.2.0. Press the Next button to begin the installation or the Back button to reenter the installation information.	
	< <u>B</u> ack <u>Next</u> > Cancel	

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.

IIS Scriptmap Node Selection	
Please select the scriptmap nodes in your IIS structure to which y mappings. File extensions to be mapped are: .php .phtml .php3	ou wish to add the PHP
WWW Service Master Properties	
Colort all	
Select none	Ok Cancel

13. Press the OK button to exit setup.

Installa	tion complete	×
	PHP 4.2.0 has been successfully installed.	
$\sim$	Press the OK button to exit this installation.	
	NT users may need to set appropriate permissions for the various php files and directories. Usually IUSR_MachineName will need read write access to the uploadtmp and session directories, and execute access for php.exe and php4ts.dll.	
	ОК	

# 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 $\rightarrow$  programs $\rightarrow$  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

Policy Editor - Sensor1									IX
File View Options Help									
bad-traffic									đ
Signatures Settings									
Folder Items	×	Name:	bad-traffic						
🕀 🗹 🛃 bad-traffic		Last Modified Date:	3/29/2002 7:43:11 A	м		_			
I ⊞ □ 🛃 exploit		# of Rules:	8			-			
i ⊕ □ 🛃 finger		# of Active Rules:	8			_			
		Base Directory:	SBULE PATH/	c	et All Group				
		Description:	Janoce_FAIII/		et Air aroup	<u> </u>			
⊡ V A rpc		These signatures are i	epresentitive of traffic I	hat should	l never he	_			
		seen on any network.	None of these signatu	es include	datagram				
		content checking and	are extremely quick sig	gnatures					
		·							
🕀 🗹 🛃 web-cgi									
🕀 🗹 🛃 web-coldfusion		Cianatura Mama		Action	Protocol	Courses ID/Dort	Direction	Destination ID /Port	
			n port 0 traffic	alert	FIDIDCOI	VEXTERNAL NET/anu	Direction	CHOME NET/0	
			dn nort A traffic	alert	udn	\$EXTERNAL_NET/any	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	\$HOME_NET/0	
⊕ veb-attacks		BAD TRAFFIC d	ata in TCP SYN pac	alert	tcp	\$EXTERNAL_NET/any	->	\$HOME_NET/any	r
🗄 🗹 🛃 sql		🗹 🗑 BAD TRAFFIC Id	opback traffic	alert	ip	any/any	$\diamond$	127.0.0.0/8/any	t
		BAD TRAFFIC S	ame SRC/DST	alert	ip	any/any	->	any/any	t
E Maria Icmp		BAD TRAFFIC ip	reserved bit set	alert	ip	\$EXTERNAL_NET/any	->	\$HOME_NET/any	r
		BAD TRAFFIC 0	ttl	alert	ip	\$EXTERNAL_NET/any	->	\$HOME_NET/any	r
· · · · · · · · · · · · · · · · · · ·		M BE BAD TRAFFIC B	ad trag bits	alert	IP	\$EXTERNAL_NET/any	->	\$HUME_NET/any	r
🕀 🗖 🗿 backdoor	Ţ	•							
	al Bu	les: 1290 Bules Enabl	ed: 887 Bules File	r C·\Activ	ewory\Sep	■ sor1\sport.conf			

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

ß	🛿 Edit V	ariable		
	Name:	HOME_NET		
	Value:	[192.168.1.0/24]		
		OK	Cancel	

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.

ß	😻 Edit Variable						
	Name:	HTTP SERVERS					
	Value:	[192 168 1 100/32 192 168 1 166/37]					
	[[132.166.1.100/32,132.166.1.166/32]						
	Г	OK Cancel					

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.

😻 Edit V	ariable		
Name:	RULE_PATH		
Value:	/etc/snort/		
L	OK	Cancel	

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 <u>sensor1@192.168.1.222</u> In this case we have not yet set a password on our <u>sensor1@192.168.1.1</u> 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.

	Database :		
Facility: LOG_AUTH	Sensor Name:	sensor1	Log File:
Priority: LOG_ALERT	DB Name:	snort	/path/to/output/file
	DB Type:	mysql 💌	Settings: 🔲 Default Settings
LOG_CONS 🗖 LOG_NDELAY 🗖	Encoding:		timestamp srcport
	Log Rule Type:	log 🔽	proto dsport
XML Logging	Detail:	full	
Rule Type: Log	User:	sensor1	
Parameters: file=/var/log/snortxml	User Pass:		Unified Logging
	DB Host:	192.168.1.108	Filename: snort.log
Log File: snort.log	DB Port:	3306	Limit in MB: 128

Once finished select file $\rightarrow$ Save and Exit

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.

😤 PuTT¥ Configura	tion	I I
Category:	Basic options for your PuTTY session Specify your connection by host name or IP address Host Name (or IP address) Port	
	192.168.1.226     122       Protocol:     ○ <u>B</u> aw     ○ <u>I</u> elnet     ○ Rlogin     ● SS <u>H</u> Load, save or delete a stored session       Council Session	
Selection     Colours     Connection     Telnet     Rlogin     SSH     Auth	Default Settings	
Tunnels	Close <u>w</u> indow on exit: C Always O Never O Only on clean exit	<b>1</b> 2
About	<u>Open</u> <u>C</u> ancel	

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.

PuTTY Se	ecurity Alert				
The server's host key is not cached in the registry. If have no guarantee that the server is the computer of think it is. The server's key fingerprint is: 1024 40:1c:fc:12:79:ef:70:75:31:8c:31:77:fd:da:60 If you trust this host, hit Yes to add the key to PuTTY's cache and carry on connecting. If you want to carry on connecting just once, without adding the key to the cache, hit No. If you do not trust this host, hit Cancel to abandon to connection.					
	Yes No Cancel				

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.



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.<u>http://127.0.0.1/acid/index.html</u>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.

Internet           Value         0	or a cid: (	🗿 ACID: Query Results - Microsoft Internet Explorer								
Lite - · · · · · · · · · · · · · · · · · ·	Ble Edit Vew Favorites Iools Help									
Notes         Control         Control <thcontrol< th=""> <thcontrol< th=""> <thcon< th=""><th colspan="10">→ Elsek + → → ② ② ③ ③ ③ ③ Search @Feventes ③Hatery PL- ④ 题 &gt; ●</th></thcon<></thcontrol<></thcontrol<>	→ Elsek + → → ② ② ③ ③ ③ ③ Search @Feventes ③Hatery PL- ④ 题 > ●									
ID         < Signature >         Signature >         Signature >         Class >         Clas >         Class >	Address	http://127.0.0.1/acid	/acid_gry_main.php?8num_result_rows=-18submit=Query+D88xurrent_view=-1				▼ 🖓 Go 🛛 Links <sup>30</sup>			
D         < (Signature)						Durt.				
F         #0(17)         [UR] SCNI Providement         2020.04/25 00 22:00         192/186.1100         192/186.122/180         102/18           F         #1(14)         spp_porticine from 192.186.1100         (Trement and the second)         2020.04/25 00 22:00         192/186.1100         192/186.122/180.1100         Uninknown         IP           F         #1(14)         spp_porticine from 192.186.1100         140 connections across 1 hous: TCP(14), UCP(0)         2020.04/25 00 22:00         192/186.1100         Uninknown         IP           F         #1(16)         ssp_porticine from 192.186.1100         140 connections across 1 hous: TCP(14), UCP(0)         2020.04/25 00 22:00         192/186.1100         Uninknown         IP           F         #1(16)         ssp_porticine from 192.186.1100         125 connections across 1 hous: TCP(14), UCP(0)         2020.04/25 00 22:00         192/186.1100         Uninknown         IP           F         #1(14)         ssp_porticine from 192.186.1100         127 connections across 1 hous: TCP(14), UCP(0)         2020.04/25 00 22:00         192/186.1100         Uninknown         IP           F         #1(14)         ssp_porticine from 192.186.1100         127 connections across 1 hous: TCP(14), UCP(0)         2020.04/25 00 22:14         192/186.1100         1100 connections across 1 hous: TCP(14), UCP(0)         2020.04/25 00 22:14         192/186.1100		ID	< Signature >	< Timestamp >	Address	< Dest.	Layer 4			
F         #14-10         T2:168-100		#0-(1-7)	furfl SCAN Proxy attempt	2002-04-25 00:23:09	192,168,1,100,1849	192.168.1.222 1080	TCP			
F         R2(12)         spp_portician free State Non 192 (196) (107) (THE SHULD 2 connections access floats TCP (141), UCP (0)         2020.42-50 (22:54)         192.198.1100         unknown         IP           F         64(1-4)         spp_portician free 192.681.100 (14) connections access floats TCP (143), UCP (0)         2020.42-50 (22:54)         192.198.1100         unknown         IP           F         64(1-4)         spp_portician free 192.681.100 (14) connections access floats TCP (143), UCP (0)         2020.42-50 (22:54)         192.198.1100         unknown         IP           F         64(1-4)         spp_portician free 192.681.100 (14) connections access floats TCP (14), UCP (0)         2020.42-50 (22:64)         192.198.1100 (14) connections (15:151) connections access floats TCP (14), UCP (0)         2020.42-50 (22:64)         192.198.1100 (14) connections (15:151) connections access floats TCP (14), UCP (0)         2020.42-50 (22:64)         192.198.1100 (14) connections (15:151) connections access floats TCP (14), UCP (0)         2020.42-50 (22:161) (15:100 (14) connections access floats TCP (14), UCP (0)         2020.42-50 (22:18) (12:161, 12:22:132) TCP (14) (14) connections access floats TCP (14), UCP (0)         2020.42-50 (22:18) (12:161, 12:22:132) TCP (14) (14) connections access floats TCP (14), UCP (0)         2020.42-50 (22:18) (12:161, 12:22:132) TCP (14) (14) (14) connections access floats TCP (12), UCP (0)         2020.42-50 (22:18) (12:161, 12:22:18) (12:161, 12:22:18) (12:161, 12:22:18) (12:161, 12:22:18) (12:161, 12:22:18) (12:161, 12:22:18) (12:161, 12:22:18) (12:161, 12:22:18) (12:161, 12:22:18) (12:16		#1-(1-1)	ICMP superscan echo	2002-04-25 00:22:50	192,168,1,100	192.168.1.222	ICMP			
r       #34(13)       spc_poticantion 192,1681.100       104 connections across 1 hosts TCP(14),UDP(0)       2002,042,500,225.8       192,1881.100       unknown       P         r       #44(14)       spc_poticantion 192,1681.100       146 connections across 1 hosts TCP(14),UDP(0)       2002,042,500,225.8       192,1881.100       unknown       P         r       #44(14)       spc_poticantion 192,1881.100       140 connections across 1 hosts TCP(14),UDP(0)       2002,042,500,232.8       122,1881.100       unknown       P         r       #44(14)       spc_poticantion 192,1881.100       140 connections across 1 hosts TCP(14),UDP(0)       2002,042,500,233.8       122,1881.100       unknown       P         r       #104(1+6)       MEO       Possible Spaid Sciant       2002,042,500,233.8       192,1881.100       unknown       P         r       #104(1+6)       MEO       Possible Spaid Sciant       2002,042,500,233.8       192,1881.100       unknown       P         r       #104(1+6)       MEO       Possible Spaid Sciant       2002,042,500,233.8       192,1881.100       unknown       P         r       #124,110       spc_poticantion 192,1881.100       127 connections across 1 hosts TCP(14),UDP(0)       2002,042,500,23.8       192,1881.100       unknown       P         r       #124,110 </td <td>Г</td> <td>#2-(1-2)</td> <td>spp_portscan detected from 192.168.1.100 (THRESHOLD 4 connections exceeded in 0 seconds)</td> <td>2002-04-25 00:22:50</td> <td>192,168,1,100</td> <td>unknown</td> <td>IP</td>	Г	#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			
r         #44(14)         spi_potsam form 152:081.100         31 comections across 1 hosts TCY(13), UCP(0)         2002/44:25 0023.02         152:081.100         unknown         P           r         #6-16.0         spi_potsam form 152:081.100         41 comections across 1 hosts TCY(14), UCP(0)         2002/44:25 0023.02         152:081.100         unknown         P           r         r4-14.0         spi_potsam form 152:081.100         41 comections across 1 hosts TCY(14), UCP(0)         2002/44:25 0023.02         152:081.100         unknown         P           r         r4-14.0         spi_potsam form 152:081.100         12 comections across 1 hosts TCY(12), UCP(0)         2002/44:25 0023.03         192:081.100 2/78         192:081.100 2/78         192:081.100         unknown         P           r         r40(1-16)         spi_potsam form 152:081.100         12 comections across 1 hosts TCY(12), UCP(0)         2002/44:25 0023.14         192:081.100         unknown         P           r         r413(1-11)         spi_potsam form 152:081.100         14 comections across 1 hosts TCY(13), UCP(0)         2002/44:25 0023.24         129:081.100         unknown         P           r         r413(1-11)         spi_potsam form 152:081.100         12 comections across 1 hosts TCY(13), UCP(0)         2002/44:25 0023.24         129:081.100         unknown         P		#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			
F         45-(1.6)         spp_potscant fom 192,168.1.100         148 connections across 1 hosts TCP(14),UCP(0)         2002,04.25 00.23.00         192,168.1.100         unknown         P           F         47-(1.6)         spp_potscant fom 192,168.1.100         135 connections across 1 hosts TCP(14),UCP(0)         2002,04.25 00.23.01         192,168.1.100         unknown         P           F         47-(1.6)         spp_potscant fom 192,168.1.100         125 connections across 1 hosts TCP(14),UCP(0)         2002,04.25 00.23.01         192,168.1.100         120,168.1.222,31.28         TCP           F         470,11.6)         spp_potscant fom 192,168.1.100         127 connections across 1 hosts TCP(14),UCP(0)         2003,04.25 00.23.81         192,168.1.100         120,168.1.222,31.28         TCP           F         471,116         spp_potscant fom 192,168.1.100         127 connections across 1 hosts TCP(14),UCP(0)         2003,04.25 00.23.81         192,168.1.100         unknown         P           F         474,11.10         spp_potscant fom 192,168.1.100         127 connections across 1 hosts TCP(14),UCP(0)         2003,04.25 00.23.81         192,168.1.100         unknown         P           F         474,113         spp_potscant fom 192,168.1.100         126 connections across 1 hosts TCP(14),UCP(0)         2003,04.25 00.23.81         192,168.1.100         unknown         P <tr< td=""><td>Г</td><td>#4-(1-4)</td><td>spp_portscan from 192.168.1.100: 131 connections across 1 hosts: TCP(131), UDP(0)</td><td>2002-04-25 00:22:58</td><td>192.168.1.100</td><td>unknown</td><td>IP</td></tr<>	Г	#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			
F         #64(4)         spp_portsentrom 192:188.1.00         Lonenctions across 1 hosts TCP(141), UDP(0)         2002.04.25 00.23 00         192:188.1.00         unknown         P           F         #64(14)         NPO - Possible Squid Scan         2002.04.25 00.23 00         192:188.1.00 <td< td=""><td></td><td>#5-(1-5)</td><td>spp_portscan from 192.168.1.100: 148 connections across 1 hosts: TCP(148), UDP(0)</td><td>2002-04-25 00:23:02</td><td>192.168.1.100</td><td>unknown</td><td>IP</td></td<>		#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			
□         #7.(14)         spp_potision from 192.168.1.00         120 (28.1.00)         unknown         P           □         #8(-1.14)         NEO - Possible Squid Scan         2002.04.25 00.23.0         192.168.1.100.278		#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			
F         #8(1-3)         INFO-Possible Squid Scan         2002-04-25 00:23:2         192:188.1100.2478         192:188.122:23128         TCP           F         #0(1-16)         INFO-Possible Squid Scan         2002-04-25 00:23:0         192:188.1100.2478         192:188.122:23128         TCP           F         #11(-16)         spp_portscan from 192:188.1100         150: comections across 1 tosts: TCP(14), UDP(0)         2002-04-25 00:23:0         192:188.1100         192:188.1188         192:188.1188         192:188.1188 </td <td></td> <td>#7-(1-8)</td> <td>spp_portscan from 192.168.1.100: 125 connections across 1 hosts: TCP(125), UDP(0)</td> <td>2002-04-25 00:23:10</td> <td>192.168.1.100</td> <td>unknown</td> <td>IP</td>		#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			
Γ         #9(11-4)         INFO- Possible Squid Scan         2002.0425 00 232.9         192.168.1.100.2478         192.168.1.00.2478         192.168.1.00.2478         192.168.1.00.2478         192.168.1.00.2478         192.168.1.00.2478         192.168.1.00.2478         192.168.1.00.2478         192.168.1.00.2478         192.168.1.00.2478         192.168.1.00.2478         192.168.1.00.2478         192.168.1.00.2478         192.168.1.00.2478         192.168.1.00.2478         192.168.1.00.2478         192.168.1.00         unknown         P           Γ         #13.(1.11)         spp_portican from 122.168.1.100.157 corrections across 1 hosts TCP(13), ULPP(0)         2002.04.25 00.23.24         192.168.1.100         unknown         P           Γ         #13.(1.11)         spp_portican from 122.168.1.100.17 corrections across 1 hosts TCP(13), ULPP(0)         2002.04.25 00.23.24         192.168.1.100         unknown         P           Γ         #16.(1.16)         spp_portican from 192.168.1.100         100 corrections across 1 hosts TCP(13), ULPP(0)         2002.04.25 00.25 54         192.168.1.100         unknown         P           Γ         #19.(1.16)         #19.100.116.100         #100.2000.44.25 00.25 65         192.168.1.100         unknown         P           Γ         #19.(1.10)         #100.1000.4000.4000.4000.4000.4000.4000.		#8-(1-13)	INFO - Possible Squid Scan	2002-04-25 00:23:29	192.168.1.100:2478	192.168.1.222:3128	TCP			
F         #10(1-16)         NP-O - Possible Squid Scan         2002.04.25 (02.33.0)         192.168.1.100         227.81         122.138.1.100         unknown         P           F         #12(1-16)         spp_pottcan from 192.168.1.100         127 connections across 1 hosts: TCP(142), UDP(0)         2002.04.25 (02.314)         192.168.1.100         unknown         P           F         #13(1-11)         spp_pottcan from 192.168.1.100         127 connections across 1 hosts: TCP(13), UDP(0)         2002.04.25 (02.32.4)         192.168.1.100         unknown         P           F         #14(1-12)         spp_pottcan from 192.168.1.100         127 connections across 1 hosts: TCP(17), UDP(0)         2002.04.25 (02.32.4)         192.168.1.100         unknown         P           F         #14(1-12)         spp_pottcan from 192.168.1.100         127 connections across 1 hosts: TCP(10), UDP(0)         2002.04.25 (02.32.4)         192.168.1.100         unknown         P           F         #19(1-20)         spp_pottcan from 192.168.1.100         102 connections across 1 hosts: TCP(10), UDP(0)         2002.04.25 (02.32.4)         192.168.1.100         unknown         P           F         #21(1-22)         spp_pottcan from 192.168.1.100         102 connections across 1 hosts: TCP(10), UDP(0)         2002.04.25 (02.456)         192.168.1.160         122.168.1.222.180.100         unknown		#9-(1-14)	INFO - Possible Squid Scan	2002-04-25 00:23:29	192.168.1.100:2478	192.168.1.222:3128	TCP			
Γ         #11-(1-6)         spp_potscan from 192:168.1.100         142 connections across 1 hosts: TCP(142), UDP(0)         2002.04.25 (02.314         192:168.1.100         unknown         P           Γ         #13:(1-10)         spp_potscan from 192:168.1.100         T31 connections across 1 hosts: TCP(13), UDP(0)         2002.04.25 (02.32.2)         192:168.1.100         unknown         P           Γ         #14:(1-12)         spp_potscan from 192:168.1.100         T3 connections across 1 hosts: TCP(13), UDP(0)         2002.04.25 (02.32.6)         192:168.1.100         unknown         P           Γ         #16:(1-16)         spp_potscan from 192:168.1.100         Ta connections across 1 hosts: TCP(147), UDP(0)         2002.04.25 (02.32.4)         192:168.1.100         unknown         P           Γ         #16:(1-16)         spp_potscan from 192:168.1.100         10 connections across 1 hosts: TCP(147), UDP(0)         2002.04.25 (02.54         192:168.1.100         unknown         P           Γ         #16:(1-20)         spp_potscan from 192:168.1.100         10 connections across 1 hosts: TCP(14), UDP(0)         2002.04.25 (02.54         192:168.1.100         unknown         P           Γ         #21:61:100         ta connections across 1 hosts: TCP(10), UDP(0)         2002.04.25 (00.414         192:168.1.166         120:168.1.222:180         TCP           Γ         #22:161:		#10-(1-16)	INFO - Possible Squid Scan	2002-04-25 00:23:30	192.168.1.100:2478	192.168.1.222:3128	TCP			
F       #12(1-10)       spp_potstan from 192:168.1.100       127 cometodia scross 1 hosts TCP(127), UDP(0)       2002.04.25 00:23.26       192:168.1.100       unknown       P         F       #14(1-12)       spp_potstan from 192:168.1.100       128 cometodia scross 1 hosts TCP(127), UDP(0)       2002.04.25 00:23.26       192:168.1.100       unknown       P         F       #16(1-16)       spp_potstan from 192:168.1.100       128 cometodia scross 1 hosts TCP(127), UDP(0)       2002.04.25 00:23.46       192:168.1.100       unknown       P         F       #16(1-16)       spp_potstan from 192:168.1.100       17 cometodia scross 1 hosts TCP(10), UDP(0)       2002.04.25 00:23.44       192:168.1.100       unknown       P         F       #18(1-19)       spp_potstan from 192:168.1.100       11 cometodia scross 1 hosts TCP(10), UDP(0)       2002.04.25 00:25.54       192:168.1.100       unknown       P         F       #18(1-19)       spp_potstan from 192:168.1.100       1 cometodia scross 1 hosts TCP(10), UDP(0)       2002.04.25 00:25.59       192:168.1.20       unknown       P         F       #22(1-30)       Lung SCAN Froxy attempt       2000.04.25 00:24.59       192:168.1.00       unknown       P         F       #22(1-30)       Lung SCAN Froxy attempt       2000.04.25 00:41.16       192:168.1.20       122:168.1.222:10.102       122:168.		#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			
Γ         #13(1-11)         spc_portscan from 192:168.1.100.151 connections across 1 hosts TCP(13), UDP(0)         2002.04-25.00.23.2         192:168.1.100         unknown         P           Γ         #16(1-16)         spc_portscan from 192:168.1.100.127 connections across 1 hosts TCP(127), UDP(0)         2002.04-25.00.23.8         192:168.1.100.414         unknown         P           Γ         #16(1-16)         spc_portscan from 192.168.1.100.147 connections across 1 hosts TCP(147), UDP(0)         2002.04-25.00.23.8         192:168.1.100.414         192.168.1.100.147         unknown         P           Γ         #174(1-17)         spc_portscan from 192.168.1.100.10 connections across 1 hosts TCP(147), UDP(0)         2002.04-25.00.23.54         192:168.1.100         unknown         P           Γ         #184(1-20)         spc_portscan from 192.168.1.100.10 connections across 1 hosts TCP(10), UDP(0)         2002.04-25.00.25.54         192:168.1.100         unknown         P           Γ         #224(1-30)         spc_portscan from 192.168.1.100.10 connections across 1 hosts TCP(10), UDP(0)         2002.04-25.00.26.05         192:168.1.166.100         unknown         P           Γ         #224(1-30)         spc_portscan from 192.168.1.166 Start         TCP         2002.04-25.00.24.25         192.168.1.166.100         192.168.1.166.100         192.168.1.166.1100         192.168.1.166.1100         192.168.1.166.1100 <td< td=""><td></td><td>#12-(1-10)</td><td>spp_portscan from 192.168.1.100: 127 connections across 1 hosts: TCP(127), UDP(0)</td><td>2002-04-25 00:23:18</td><td>192.168.1.100</td><td>unknown</td><td>IP</td></td<>		#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			
F         #14(-12)         spp_portscan from 192:168.1.100         unknown         IP           F         #16(-14)         spp_portscan from 192:168.1.00         unknown         IP           F         #16(-14)         SCAM Proxy attempt         2002:04-25:00:23:0         192:168.1.00         unknown         IP           F         #17(-17)         spp_portscan from 192:168.1.00         100:00:00:00:23:4         192:168.1.00         unknown         IP           F         #16(-14)         spp_portscan from 192:168.1.00         100:00:00:00:00:25:59         192:168.1.00         unknown         IP           F         #16(-14)         spp_portscan from 192:168.1.00         100:00:00:00:00:00:00:00:00:00:00:00:00:		#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			
Γ         #16(14)         Sep_ports and rom 192. (88.1.100. 127 connections across 1 hosts: TCP(137), UDP(0)         2002.04.25 00.23.34         192. (88.1.100. 2014         Punknown         P           Γ         #17(147)         sep_ports and rom 192. (88.1.00. 147 connections across 1 hosts: TCP(147), UDP(0)         2002.04.25 00.23.34         192. (88.1.100. 2014         Punknown         P           Γ         #18(1-19)         sep_ports and rom 192. (88.1.100. 137 connections across 1 hosts: TCP(14), UDP(0)         2002.04.25 00.25 59         192. (86.1.100. unknown         P           Γ         #19(1-20)         sep_ports and rom 192. (88.1.100. 1 connections across 1 hosts: TCP(1), UDP(0)         2002.04.25 00.25 59         192. (86.1.100. unknown         P           Γ         #22(1-22)         sep_ports and rom 192. (88.1.100. 1 connections across 1 hosts: TCP(1), UDP(0)         2002.04.25 00.21 60         192. (86.1.166.357         19		#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			
Γ         #16(-14)         SCAN Provy attempt         2002-04-25 00 2334         192/168/.100.2514         192/168/.100.1         192/168/.100.1         192/168/.120.2512         192/168/.120.2512         192/168/.120.2512         192/168/.120.2512         192/168/.120.2512         192/168/.120.2512         192/168/.120.2512         192/168/.120.2512         192/168/.120.2512         192/168/.120.2512         192/168/.120.2512         192/168/.120.2512         192/168/.120.2512         192/168/.122.23128         170         192/168/.122.23128         170         192/168/.122.23128         170         192/168/.122.23128         170         192/168/.122.23128         170         192/168/.122.23128         170         192/168/.122.23128		#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			
Γ         #17(1-17)         spp_portscantrom 192(188.1.00)         1/2 connections across 1 hots: ICP(14), UDP(0)         2002-0425 00 255 9         192(188.1.00)         unknown         P           Γ         #19(1-20)         spp_portscantrom 192(188.1.00)         1/2 connections across 1 hots: ICP(14), UDP(0)         2002-0425 00 255 9         192(188.1.00)         unknown         P           Γ         #22(1-22)         spp_portscantrom 192(188.1.100.2 connections across 1 hots: ICP(14), UDP(0)         2002-0425 00 265 9         192(188.1.100         unknown         P           Γ         #22(1-22)         spp_portscantrom 192(188.1.100.2 connections across 1 hots: ICP(14), UDP(0)         2002-0425 00 265 9         192(188.1.106 428         192(188.1.106 418		#16-(1-18)	SCAN Proxy attempt	2002-04-25 00:23:34	192.168.1.100:2614	192.168.1.222:8080	TCP			
Γ         #18(1-19)         spp_portscant from 192:168.1.100         1 connections across 1 hosts TCP(10), UDP(0)         2002:04:25 00:25 54         192:168.1.100         unknown         P           r         #20(1-21)         spp_portscant from 192:168.1.100         2 connections across 1 hosts TCP(10), UDP(0)         2002:04:25 00:25 59         192:168.1.100         unknown         P           r         #21(1-22)         spp_portscant from 192:168.1.100         1 connections across 1 hosts TCP(10), UDP(0)         2002:04:25 00:25 09         192:168.1.168 428         192:168.1.122:1080         TCP           r         #22(1-30)         [url] SCAN Provy attempt         2002:04:25 00:4119         192:168.1.166 428         192:168.1.122:2183         TCP           r         #22(1-30)         [url] SCAN Provy attempt         2002:04:25 00:4141         192:168.1.166 428         192:168.1.122:2183         TCP           r         #26(1-40)         SCAN Provy attempt         2002:04:25 00:4145         192:168.1.166 423         192:168.1.122:1783         TCP           r         #26(1-40)         SCAN Provy attempt         2002:04:25 00:416         192:168.1.102         192:168.1.122:183         TCP           r         #26(1-40)         SCAN Provy attempt         2002:04:25 00:410         192:168.1.100         unknown         P           r <td></td> <td>#17-(1-17)</td> <td>spp_portscan from 192.168.1.100: 147 connections across 1 hosts: TCP(147), UDP(0)</td> <td>2002-04-25 00:23:34</td> <td>192.168.1.100</td> <td>unknown</td> <td>IP</td>		#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			
μ         μ	Г	#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			
F         #20-(1-21)         spp_portscan from 192.168.1.00         zoomstons stross 1 hosts TCP(1), UDP(0)         2002.04.25 00.26.05         192.168.1.100         unknown         P           F         #22-(1-30)         [url]SCAN Prox attempt         2002.04.25 00.24.05         192.168.1.166.238         192.168.1.22.21080         TCP           F         #22-(1-30)         [url]SCAN Prox attempt         2002.04.25 00.24.10         192.168.1.166.228         192.168.1.22.2138         TCP           F         #22-(1-30)         [NFO - Possible Squid Scan         2002.04.25 00.4141         192.168.1.166.4238         192.168.1.22.2138         TCP           F         #26-(1-40)         SCAN Prox attempt         2002.04.25 00.4145         192.168.1.166.4238         192.168.1.22.2080         TCP           F         #26-(1-40)         SCAN Prox attempt         2002.04.25 00.4145         192.168.1.166.423         192.168.1.122.2080         TCP           F         #26-(1-42)         spp_portscan from 192.168.1.100         TCP         2002.04.25 00.4145         192.168.1.166.423         192.168.1.122.20800         TCP           F         #26-(1-42)         spp_portscan from 192.168.1.100         TCP         2002.04.25 00.4110         192.168.1.122.20800         TCP           F         #26-(1-42)         spp_portscan from 192.168.1.166<		#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			
Γ         #221(122)         spp_portscan from 192.168.1.100         1 connections across 1 hosts TCP(1), UDP(0)         2002.042.50 02619         192.168.1.60.07         118.7 key         P           Γ         #223(1.36)         NFO - Possible Squid Scan         2002.042.50 04140         192.168.1.664.278         182.168.1.222.128         TCP           Γ         #225(1.36)         NFO - Possible Squid Scan         2002.042.50 04140         192.168.1.664.278         182.168.1.222.128         TCP           Γ         #255(1.36)         NFO - Possible Squid Scan         2002.042.50 04141         192.168.1.1664.248         192.168.1.1664.242 <td></td> <td>#20-(1-21)</td> <td>spp_portscan from 192.168.1.100: 2 connections across 1 hosts: TCP(2), UDP(0)</td> <td>2002-04-25 00:26:05</td> <td>192.168.1.100</td> <td>unknown</td> <td>P</td>		#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	P			
□         #22(130)         [un]SCAN Prov attempt         2002/04/25 00/4119         192/168.1.166/368         192/168.1.22/21080         TCP           □         #22(13-16)         INFO- Possible Squid Scan         2002/04/25 00/4141         192/168.1.166/428         192/168.1.166/428         192/168.1.166/428         192/168.1.166/428         192/168.1.166/428         192/168.1.166/428         192/168.1.22/218         TCP           □         #25(1-36)         INFO- Possible Squid Scan         2002/04/25 00/4141         192/168.1.166/428         192/168.1.22/218         TCP           □         #25(1-40)         SCAN Provy attempt         2002/04/25 00/4145         192/168.1.166/423         192/168.1.12/20/2000         TCP           □         #26(1-40)         SCAN Provy attempt         2002/04/25 00/4145         192/168.1.166/423         192/168.1.12/20/2000         TCP           □         #26(1-40)         SCAN Provy attempt         2002/04/25 00/416         192/168.1.166/100         unknown         IP           □         #26(1-40)         SCAN Provy attempt         2002/04/25 00/410         192/168.1.166/423         192/168.1.166/423         192/168.1.166/423         192/168.1.166/423         192/168.1.166/423         192/168.1.166/423         192/168.1.166/423         192/168.1.166/423         192/168.1.166/423         192/168.1.166/423         19		#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	P			
Γ         R#0-Possible Squid Scan         2002/04/25 00/4140         192/168.1166/428         192/188.1222.31/28         ΓCP           Γ         R25(136)         INFO-Possible Squid Scan         2002/04/25 00/4140         192/168.1166/428         192/188.1222.31/28         ΓCP           Γ         R25(136)         INFO-Possible Squid Scan         2002/04/25 00/4141         192/168.1166/428         192/188.1222.31/28         TCP           Γ         R25(136)         INFO-Possible Squid Scan         2002/04/25 00/4141         192/168.1166/428         192/188.1222.31/28         TCP           Γ         R27(142)         Spp_portscan from 192/168.1100         TCOME to scale         2002/04/25 00/4146         192/168.1166/4423         192/188.1122.2000         TCP           Γ         R27(142)         Spp_portscan from 192.168.1100         TCOME to scale         Scale         192/168.1166         100         Unknown         P           Γ         R23(126)         Spp_portscan from 192.168.1166         1166/142         Concord Scale		#22-(1-30)	[url] SCAN Proxy attempt	2002-04-25 00:41:19	192.168.1.166:3657	192.168.1.222:1080	TCP			
□       #24-131)       INFO-Possible Squid Scan       2002/04/25 00/4141       192/163.1166/4286       192/163.1166/1282       192/163.1166/1282       192/163.1166/1282       193/168/1222.0000       TCP         F       #23/1426       spp_portscan dot opticsan from 192/168.1166       1100.1102/102/102       192/168.1166       unknown       IP         F       #33/1426       spp_portscan from 192/168.1166       1100.1166/126		#23-(1-36)	INFO - Possible Squid Scan	2002-04-25 00:41:40	192.168.1.166.4288	192.168.1.222.3128	TCP			
L         LPO-Position Square         2002/04/25 00/4141         192/165.1166/428         192/165.1166/423		#24-(1-37)	INFO - Possible Squid Scan	2002-04-25 00:41:41	192.168.1.166:4288	192.168.1.222.3128	TOP			
I         I/2         SUCAN Proxy attempt         2002/04/25 00/4149         19/2/165/1106/4423         19/2/165/1106/4433         19/2/165/1106/4433         19/2/165/1106/4433         19/2/165/1106/4433         19/2/165/1106/4433         19/2/165/1106/4433         19/2/165/1106/4433         19/2/165/1106/4433         19/2/165/1106/4433         19/2/165/1106/4433         19/2/165/1106/4433         19/2/165/1106/4433         19/2/165/1106/4433         19/2/165/1166/433         10/2/16/210/4433         19/2/165/1166/433         10/2/16/210/4433         10/2/16/210/4433         10/2/16/210/4433         10/2/16/210/4433         10/2/16/210/4433         10/2/16/210/4433         10/2/16/210/4433         10/2/16/210/4433         10/2/16/210/4433         10/2/16/210/4433         10/2/16/210/4433         10/2/16/210/4433         10/2/16/210/4433         10/2/16/210/4433         10/2/16/210/4433         10/2/16/210/4433         1		#25-(1-38)	INFO - Possible Squid Scan	2002-04-25 00:41:41	192.168.1.166:4288	192.168.1.222.3128	TOP			
L         P221(142)         Spp_portscan from 192.168.1.100. T connections across 1 hosts TCP(1), UDP(0)         2002.04.2.8 00.4146         192.168.1.108.1.100. T connections across 1 hosts TCP(1), UDP(0)         2002.04.2.8 00.4146         192.168.1.100. T connections across 1 hosts TCP(1), UDP(0)         2002.04.2.8 00.4126         192.168.1.100. T connections across 1 hosts TCP(1), UDP(0)         2002.04.2.8 00.4126         192.168.1.100. T connections across 1 hosts TCP(1), UDP(0)         2002.04.2.8 00.4126         192.168.1.100. T connections across 1 hosts TCP(1), UDP(0)         2002.04.2.8 00.4126         192.168.1.108. T unknown         P           C         #31.142.5         spp_portscan from 192.168.1.168.1166         1168 T100 connections across 1 hosts TCP(151), UDP(0)         2002.04.2.8 00.410         192.168.1.166         unknown         P           C         #33.1.28         spp_portscan from 192.168.1.166.131 connections across 1 hosts TCP(151), UDP(0)         2002.04.2.5 00.4114         192.168.1.166         unknown         P           C         #33.1.28         spp_portscan from 192.168.1.166.130 connections across 1 hosts TCP(140), UDP(0)         2002.04.25 00.4112         192.168.1.166         unknown         P           C         #33.1.43         spp_portscan from 192.168.1.166.130 connections across 1 hosts TCP(140), UDP(0)         2002.04.25 00.4122         192.168.1.166         unknown         P           C         #33.1.43         spp_portscan from 192.168.1.166		#20-(1-40)	SCAN Proxy attempt	2002-04-25 00:41:45	192.108.1.100.4423	192.168.1.222.8080	TCP			
Γ         #22(1+2)         Spp_DDtScint (mt) 192/163/106         Control Lotting Loops 1,005         Control Loops 1,005         Co		#27-(1-42)	SUAN Proxy attempt	2002-04-25 00:41:46	192.168.1.166.4423	192.168.1.222.8080	ICP			
L       spp_botscate End or postscate and on 192. res. 1.00: TOT Rep. (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)		#20-(1-23)	spp_botscar from 192.166.1.100. T connections across 1 fibers (2014) TCDI(0)	2002-04-25 00:39:34	192.100.1.100	unknown	P			
□       http://www.minimative/control/action/sectors/actions/		#29-(1-24)	spp_botscar. End of poisscar from 192, 166, 1100, 100 Ac une(2015) hosts(1) (CP(1566) 0DP(0)	2002-04-25 00:41:02	192.168.1.100	unknown	IP			
□       eV1(120)       spp_potscal from 192 (681.166 1/2 contrections across 1 hots TCP (151), UDP(0)       2002/04:25 00.41.06       192.1681.166       unknown       P         □       #33(1-28)       spp_potscal from 192 (681.166       156 1/2 contrections across 1 hots TCP (151), UDP(0)       2002/04:25 00.41.16       192.1681.166       unknown       P         □       #33(1-28)       spp_potscal from 192 (681.166       156 1/2 contrections across 1 hots TCP (151), UDP(0)       2002/04:25 00.41.18       192.1681.166       unknown       P         □       #33(1-28)       spp_potscal from 192 (681.166       136 contrections across 1 hots TCP (150), UDP(0)       2002/04:25 00.41.18       192.1681.166       unknown       P         □       #33(1-28)       spp_potscal from 192 (681.166       137 contrections across 1 hots TCP (140), UDP(0)       2002/04:25 00.41.22       192.168.1.166       unknown       P         □       #33(1-36)       spp_potscal from 192 (681.166       142 contrections across 1 hots TCP (140), UDP(0)       2002/04:25 00.41.30       192.168.1.166       unknown       P         □       #33(1-36)       spp_potscal from 192 (681.166       142 contrections across 1 hots TCP (140), UDP(0)       2002/04:25 00.41.30       192.168.1.66       unknown       P         □       #43(1-41)       spp_potscal from 192.168.1.166       145 contrections acro		#30-(1-20)	spp_portscan detected from 192,168,1,166 (TRRESHOLD 4 connections exceeded in 0 seconds)	2002-04-25 00:41:02	192,108,1,100	unknown	P			
□       #32(132)       spp_portscan from 192,168,1.168       100 contextions across 1 hosts TCP(141),UDP(0)       2002,042,50,04114       192,168,1.166       unknown       P         □       #33(132)       spp_portscan from 192,168,1.166       130 contextions across 1 hosts TCP(141),UDP(0)       2002,042,50,04114       192,168,1.166       unknown       P         □       #33(132)       spp_portscan from 192,168,1.166       130 contextions across 1 hosts TCP(130),UDP(0)       2002,042,50,04114       192,168,1.166       unknown       P         □       #33(134)       spp_portscan from 192,168,1.166       140 contextions across 1 hosts TCP(130),UDP(0)       2002,042,50,0412       192,168,1.166       unknown       P         □       #33(134)       spp_portscan from 192,168,1.166       142 contextions across 1 hosts TCP(140),UDP(0)       2002,042,50,0413       192,168,1.166       unknown       P         □       #33(134)       spp_portscan from 192,168,1.166       142 contextions across 1 hosts TCP(140),UDP(0)       2002,042,50,0413       192,168,1.166       unknown       P         □       #44,145)       spp_portscan from 192,168,1.166       146 contextons across 1 hosts TCP(140),UDP(0)       2002,042,50,04146       192,168,1.166       unknown       P         □       #44,143)       spp_portscan from 192,168,1.166       146 contextons across 1 hosts TCP		#31-(1-20)	spp_botscan from 192,168,1166,123 connections across 1 hosts: TCP(123), UDD(0)	2002-04-25 00:41:06	192.100.1.100	unknown	IP			
L         cross11260         Sup_Distant Indin 192.168.1.166         Lot College 100         2002/04-25 00:41.14         192.168.1.168         Unit Norm         IP           F         6434(1-26)         Sup_Dottsant Indin 192.168.1.166         130 connections across 1 hosts TCP(180), UDP(0)         2002/04-25 00:41.16         192.168.1.166         Unit Norm         IP           F         6434(1-32)         Sup_Dottsant from 192.168.1.166         130 connections across 1 hosts TCP(180), UDP(0)         2002/04-25 00:41.22         192.168.1.166         Unit Norm         IP           F         6434(1-32)         Sup_Dottsant from 192.168.1.166         142 connections across 1 hosts TCP(140), UDP(0)         2002/04-25 00:41.22         192.168.1.166         Unit Norm         IP           F         6434(1-32)         Sup_Dottsant from 192.168.1.166         142 connections across 1 hosts TCP(140), UDP(0)         2002/04-25 00:41.34         192.168.1.166         Unit Norm         IP           F         6434(1-35)         Sup_Dottsant from 192.168.1.166         146 connections across 1 hosts TCP(146), UDP(0)         2002/04-25 00:41.34         192.168.1.166         Unit Norm         IP           F         643(1-45)         Sup_Dottsant from 192.168.1.166.146 connections across 1 hosts TCP(146), UDP(0)         2002/04-25 00:41.36         192.168.1.166         Unit Norw         IP           F		#32-(1-27)	spp_botscar from 192.166.1.166.111 connections across 1 hosts: TCP(101), UDD(0)	2002-04-25 00:41.10	102 160 1 166	unknown	IP			
Image: Provide and the set of t		#34 (1 20)	spp_portscan from 192,169,1166,120 connections across 1 hosts: TC (147, 0DP(0))	2002-04-25 00:41:14	102 160 1 166	unknown				
r         #S61132         spp_portscan from 192.168.1166         140 connections across 1 hosts TCP(140), UDP(0)         2002.244.250.41.26         192.168.1165         unknown         IP           r         #S71133         spp_portscan from 192.168.1166         142 connections across 1 hosts TCP(140), UDP(0)         2002.244.250.41.26         192.168.1166         unknown         IP           r         #S71133         spp_portscan from 192.168.1166         114 connections across 1 hosts TCP(140), UDP(0)         2002.04.250.041.36         192.168.1166         unknown         IP           r         #S37(1-35)         spp_portscan from 192.168.1166         114 connections across 1 hosts TCP(140), UDP(0)         2002.04.250.041.34         192.168.1166         unknown         IP           r         #S37(1-39)         spp_portscan from 192.168.1166         114 connections across 1 hosts TCP(146), UDP(0)         2002.04.250.041.42         192.168.1166         unknown         IP           r         #41(1-41)         spp_portscan from 192.168.1.166         3 connections across 1 hosts TCP(130), UDP(0)         2002.04.250.047.57         192.168.1.166         unknown         IP           r         #44.1-450         [arachNIDS](CMP webtend's scanner         2002.04.250.047.57         192.168.1.166         unknown         IP           r         #44.2-4.1-450         [arachNIDS](CM		#35-(1-31)	sop_portscan from 192,168,1,166, 137 connections across 1 hosts, TCP(130), ODP(0)	2002-04-25 00:41:18	192,168,1,166	unknown	IP			
Image: Product inform         Spp_portscan from		#36-(1-32)	sop_portscan from 192,168,1,166, 140 connections across 1 hosts, TCP(140), UDP(0)	2002-04-25 00:41:22	192,168,1,166	unknown	IP			
Image: Constraint of the second second in the second sec		#37-(1-33)	spp_portecan from 192 168 1166: 124 connections across 1 hosts: TC(134) UDP(0)	2002-04-25 00:41:20	192 169 1 166	unknown	IP			
Image: Product Control (1-4)         Spp_portscant from (1-4)         Control (1-4)         Contro (1-4)		#38.(1.34)	spp_portecan from 192,168,1166,111 connections across 1 hosts: TC (124, DDP(0))	2002-04-25 00:41:50	192 169 1 166	unknown	IP			
r         #40(1-39)         spp_portscan from 192,168,1.166         466 connections across 1 hosts TCP(148),UDP(0)         2002,242,250,4142         192,168,1.166         unknown         IP           r         #41(1-41)         spp_portscan from 192,168,1.166         130 connections across 1 hosts TCP(148),UDP(0)         2002,242,250,4142         192,168,1.166         unknown         IP           r         #41(1-41)         spp_portscan from 192,168,1.166         35 connections across 1 hosts TCP(130),UDP(0)         2002,042,250,047,51         192,168,1.166         unknown         IP           r         #43,1(-44)         spp_portscan from 192,168,1.166         35 connections across 1 hosts TCP(130),UDP(0)         2002,042,500,47,51         192,168,1.166         unknown         IP           r         #44,1-450         [arachNIDS] (CMP webtends scanner         2002,042,500,07,53         192,168,1.166         192,168,1.222         ICMP           r         #44,1-450         [arachNIDS] (CMP webtends scanner         2002,042,57,173,26         192,168,1.166,400         192,168,1.226,100         TCP           r         #44,2-43         [uni] SCNN Prow atempt         2002,042,57,173,26         192,168,1.166,4003         192,168,1.226,100         TCP           r         #44,2-44         [uni] SCNN Prow atempt         2002,042,57,173,72         192,168,1.166,4003		#39.(1.35)	spp_portscan from 192.168.1.166: 148 connections across 1 hosts: TCP(148) LIDP(0)	2002-04-25 00:41:34	192 168 1 166	unknown	IP			
□         #41-(1-41)         spp_portscan from 192.168.1.166         139 connections across 1 hots: 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         139 connections across 1 hots: TCP(139),UDP(0)         2002.04.25 00.47.51         192.168.1.166         unknown         IP           □         #42-(1-43)         spp_portscan from 192.168.1.166         136 connections across 1 hots: TCP(139),UDP(0)         2002.04.25 00.47.51         192.168.1.166         unknown         IP           □         #44-(1-45)         [arachNIDS]/CMP webtends scanner         2002.04.25 00.47.51         192.168.1.100         192.168.1.222         ICMP           □         #44-(1-45)         [arachNIDS]/CMP webtends scanner         2002.04.25 10.04         192.168.1.206         108.1226         108.1226         108.1226         108.1226         108.1226         108.1226         108.1226         108.1226         108.1226         108.142.41         192.168.1.266         109.148.1226         108.1266         108.1266         108.1266         108.1266         108.1266         108.148.1403         192.168.1.266         108.148.126         108.1266         108.148.1403         192.168.1.266         108.148.126         108.148.1266         108.148.1266         108.148.126 <td< td=""><td></td><td>#40-(1-39)</td><td>spp_portscan from 192 168 1 166: 146 connections across 1 hosts: TC(146) UIDP(0)</td><td>2002-04-25 00:41:30</td><td>192 168 1 166</td><td>unknown</td><td>ID</td></td<>		#40-(1-39)	spp_portscan from 192 168 1 166: 146 connections across 1 hosts: TC(146) UIDP(0)	2002-04-25 00:41:30	192 168 1 166	unknown	ID			
□         #424(1-43)         spp_portscan from 192.168.1.166 45 connections across 1 hosts: TCP(65), UDP(0)         2002.04.25 00.47.51         192.168.1.166         unknown         µp           □         #434(1-44)         spp_portscan from 192.168.1.166 3 connections across 1 hosts: TCP(65), UDP(0)         2002.04.25 00.47.51         192.168.1.166         unknown         µp           □         #443(1-44)         spp_portscan from 192.168.1.166 3 connections across 1 hosts: TCP(35), UDP(0)         2002.04.25 00.47.51         192.168.1.166         unknown         µp           □         #443(1-46)         [arachNIDS][CMP webtends scanner         2002.04.25 01.47.57         192.168.1.100         192.168.1.222         ICMP           □         #445(1-46)         [arachNIDS][CMP webtends scanner         2002.04.25 17.07.26         192.168.1.168.100         192.168.1.226 10.00         TCP           □         #44-12-3         [uni]SCNN Prow attempt         2002.04.25 17.37.26         192.168.1.166.4403         192.168.1.226 10.00         TCP           □         #44-2.4         [uni]SCNN Prow attempt         2002.04.25 17.37.27         192.168.1.166 4403         192.168.1.26 10.00         TCP           □         #44-2.4         [uni]SCNN Prow attempt         2002.04.25 17.37.08         192.168.1.166 4403         192.168.1.26 10.00         TCP           □		#41-(1-41)	spp_portscan from 192 168 1 166: 139 connections across 1 hosts: TC(139, UDP(0)	2002-04-25 00:41:42	192 168 1 166	unknown	ID			
#43-(1-44)         spo_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] (CMP webtends scanner         2002.04.25 00.47.57         192.168.1.100         192.168.1.22         ICMP           #44-(1-45)         [arachNIDS] (CMP webtends scanner         2002.04.25 00.47.57         192.168.1.20         192.168.1.22         ICMP           #44-(1-45)         [arachNIDS] (CMP webtends scanner         2002.04.25 17.37.26         192.168.1.22         ICMP           #44-(2-2)         [unt] SCAN Proxy attempt         2002.04.25 17.37.26         192.168.1.168.4403         192.168.1.226 1080         TCP           #44-(2-4)         [unt] SCAN Proxy attempt         2002.04.25 17.37.27         192.168.1.166.4403         192.168.1.226 1080         TCP           #44-(2-4)         [unt] SCAN Proxy attempt         2002.04.25 17.37.27         192.168.1.166.4403         192.168.1.226 1080         TCP           #49-(2-1)         ICMP Superscan echo         2002.04.25 17.37.27         192.168.1.166.4403         192.168.1.226 1080         TCP           #49-(2-1)         ICMP Superscan echo         2002.04.25 17.37.08         192.168.1.166         ICMP         Image: ICMP         Image: ICMP         Image: ICMP         Image: ICMP         Image: ICMP		#42-(1-43)	spp_portscan from 192 168 1 166: 65 connections across 1 hosts: TCP(65) LIDP(0)	2002-04-25 00:47:51	192 168 1 166	unknown	IP			
r         #44(145)         [arachNIDS] ICMP webtends scanner         2002.04.25 00.55.33         192.168.1.100         192.168.1.222         ICMP           r         #45(146)         [arachNIDS] ICMP webtends scanner         2002.04.25 00.55.33         192.168.1.00         192.168.1.222         ICMP           r         #46-146)         [arachNIDS] ICMP webtends scanner         2002.04.25 17.07.26         192.168.1.168.4103         192.168.1.226.1080         TCP           r         #46-122)         [un] SCAN Prox atempt         2002.04.25 17.37.26         192.168.1.168.4403         192.168.1.266.1080         TCP           r         #44-24)         [un] SCAN Prox atempt         2002.04.25 17.37.27         192.168.1.168.4403         192.168.1.226.1080         TCP           r         #44-24.1         [un] SCAN Prox atempt         2002.04.25 17.37.27         192.168.1.166.4403         192.168.1.266.1000         TCP           r         #44-24.1         [un] SCAN Prox atempt         2002.04.25 17.37.08         192.168.1.166.4403         192.168.1.266.1000         TCP           r         #49-24.11         ICMP superscan echo         2002.04.25 17.37.08         192.168.1.166         192.168.1.266.1000         TCP		#43-(1-44)	spp. portscan from 192.168.1.166: 3 connections across 1 hosts: TCP(3) LIDP(0)	2002-04-25 00:47:57	192,168,1,166	unknown	IP			
□         #45-(1-46)         [arachNIDS] ICMP webtrends scamer         2002-04-25 17:00-49         192.168.1.100         192.168.1.222         ICMP           □         #46-(2-2)         [uri] SCAN Proxy attempt         2002-04-25 17:37.26         192.168.1.166.4403         192.168.1.26:1080         TCP           □         #47-(2-3)         [uri] SCAN Proxy attempt         2002-04-25 17:37.26         192.168.1.166.4403         192.168.1.26:1080         TCP           □         #44-(2-4)         [uri] SCAN Proxy attempt         2002-04-25 17:37.27         192.168.1.166.4403         192.168.1.26:1080         TCP           □         #48-(2-4)         [uri] SCAN Proxy attempt         2002-04-25 17:37.27         192.168.1.26:1080         TCP           □         #49-(2-1)         ICMP superscan echo         2002-04-25 17:37.26         192.168.1.26:1080         TCP           □         #49-(2-1)         ICMP superscan echo         2002-04-25 17:37.06         192.168.1.26:1080         TCP           □         #49-(2-1)         ICMP superscan echo         2002-04-25 17:37.06         192.168.1.26         ICMP         u		#44-(1-45)	[arachNIDS] ICMP webtrends scanner	2002-04-25 00:55:33	192,168,1,100	192,168,1,222	ICMP			
r         #48/2/2)         [urt] SCAN Proxy attempt         2002/04/25 17/37/26         192/168/1/266/1080         TCP           r         #447/2/3)         [urt] SCAN Proxy attempt         2002/04/25 17/37/26         192/168/1/266/1080         TCP           r         #48/2/4/1         [urt] SCAN Proxy attempt         2002/04/25 17/37/27         192/168/1/26/1080         TCP           r         #48/2/4/1         [urt] SCAN Proxy attempt         2002/04/25 17/37/27         192/168/1/26/1080         TCP           r         #48/2/4/1         [urt] SCAN Proxy attempt         2002/04/25 17/37/27         192/168/1/26/1080         TCP           r         #48/2/4/1         [urt] SCAN Proxy attempt         2002/04/25 17/37/08         192/168/1/26/1080         TCP           r         #48/2/4/1         [urt] SCAN Proxy attempt         2002/04/25 17/37/08         192/168/1/26/1080         TCP           r         #49/2/11         ICMP superscan echo         2002/04/25 17/37/08         192/168/1/26/1080         TCP		#45-(1-46)	[arachNIDS] ICMP webtrends scanner	2002-04-25 17:00:49	192,168,1,100	192,168,1,222	ICMP			
□         #47-[2-3]         [url] SCAN Proxy attempt         2002-04-25 17:37.26         192.168.1.166.4403         192.168.1.226 1080         TCP           □         #48-[2-4]         [url] SCAN Proxy attempt         2002-04-25 17:37.27         192.168.1.166.4403         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 superscan echo         2002-04-25 17:37.08         192.168.1.166         192.168.1.226 ICMP         □		#46-(2-2)	[url] SCAN Proxy attempt	2002-04-25 17:37:26	192,168,1,166;4403	192,168,1,226;1080	TCP			
□         #48-[2-4]         [urt] SCAN Proxy attempt         2002-04-25 17:37:27         192.168.1.166.4403         192.168.1.226 1060         TCP           □         #49-[2-1]         ICMP superscan echo         2002-04-25 17:37:08         192.168.1.166         192.168.1.226 1060         TCP		#47-(2-3)	[url] SCAN Proxy attempt	2002-04-25 17:37:26	192,168,1,166:4403	192,168,1,226;1080	TCP			
ICMP superscan echo         2002-04-25 17:37.08         192.168.1.166         192.168.1.226         ICMP           Image: Strategy of the superscan echo         2002-04-25 17:37.08         192.168.1.166         192.168.1.226         ICMP		#48-(2-4)	[url] SCAN Proxy attempt	2002-04-25 17:37:27	192,168,1,166;4403	192,168,1,226:1080	TCP			
		#49-(2-1)	ICMP superscan echo	2002-04-25 17:37:08	192.168.1.166	192.168.1.226	ICMP .			
	ø					Ini 👛 Ini	ternet			

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. <u>http://www.silicondefense.com</u>

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 <a href="http://www.cisecurity.org">http://www.cisecurity.org</a>

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 <u>http://www.snort.org/dl/snort-1.8.6.tar.gz</u> tar -xzvf 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 <u>http://www.snort.org/dl/signatures/snortrules.tar.gz</u> you can extract these files into a new directory in you 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 <a href="http://www.silicondefense.com/techsupport/winsnortacid-iis\_1.8.6.htm">http://www.silicondefense.com/techsupport/winsnortacid-iis\_1.8.6.htm</a>

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: <u>http://www.gartner.com/DisplayTechOverview?id=320015</u>

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/htmldoc/

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)