Course # 03-60-564

Security and Privacy on the Internet

Instructor: Dr. A. K. Aggarwal

Project:

Snort Testing with Acid, MySQL, PHP, IIS, ADODB under Windows XP

Submitted By:

Ahmedur Rahman

Lawangeen Khan

Zillur Rahman

Due Date: March 09, 2006

Table of Contents

Introduction:

Intrusion Detection is strength of detecting inappropriate activity. Security is a big issue for all networks in today's enterprise environment. Many methods have been developed to secure the network infrastructure and communication over the Internet. One relatively new method is intrusion detection methods, which started appearing in the last few years. Using intrusion detection methods, you can collect and use information from known types of attacks and find out if someone is trying to attack your network or particular hosts. In this document we have wrote about a IDS called **Snort** with its some other add-ons as our course project work.

Installation:

For this project we had to install the following components:

- WinPcap
- ADODB
- MySQL
- DBTools
- IIS
- PHP
- PHPLot
- SNORT
- ACID
- JPGraph
- CommView

WINPCAP Installation:

WinPcap is the industry-standard tool for link-layer network access in Windows environments: it allows applications to capture and transmit network packets bypassing the protocol stack, and has additional useful features, including kernel-level packet filtering, a network statistics engine and support for remote packet capture. WinPcap consists of a driver, that extends the operating system to provide low-level network access, and a library that is used to easily access the low-level network layers. The driver allows the ability to capture raw packets and send them to Win32 platforms.

WinPcap installation is very straightforward. At first we downloaded the exe file from the following link:

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

For this project we have used WinPcap 3.1 version. After downloading the exe file we followed the following steps:

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

ADODB Installation:

We have used ADODB version 4.72. ADOdb is a database abstraction library for PHP and Python based on the same concept as Microsoft's ActiveX Data Objects. It allows developers to write applications in a fairly consistent way regardless of the underlying database storing the information. The advantage is that the database can be changed without re-writing every call to it in the application. It is important to note that ADOdb uses SQL.

We downloaded the ADODB version 4.72 from the following link:

http://prdownloads.sourceforge.net/adodb/adodb472.zip?download

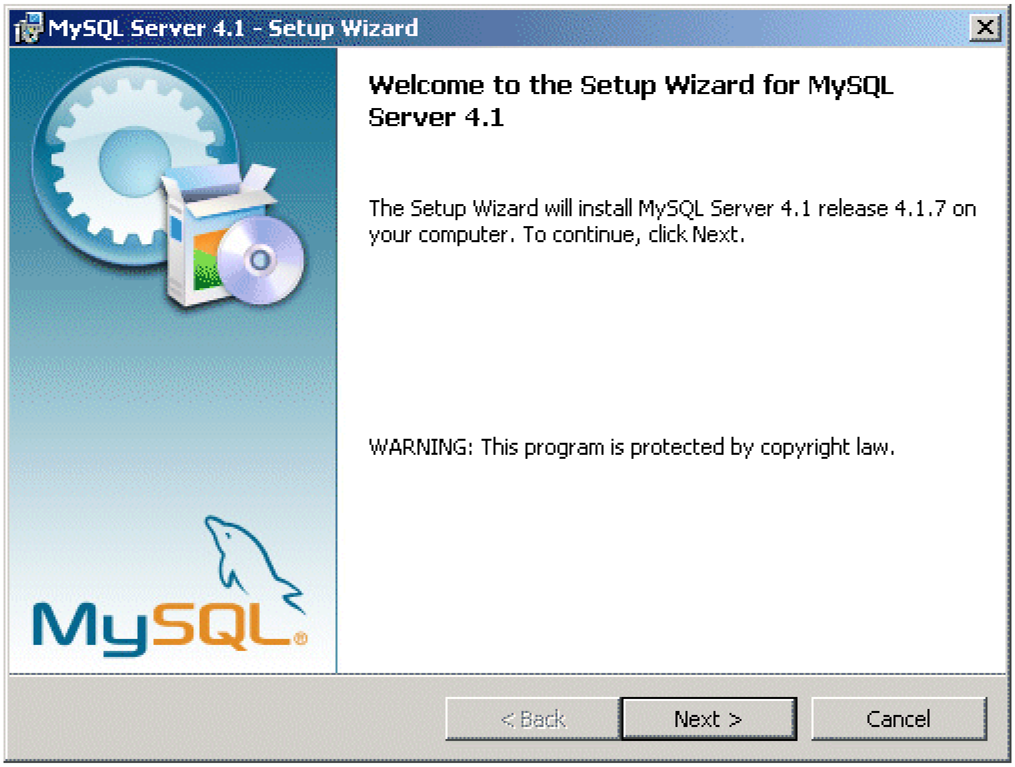
We have downloaded the zip file and extracted it into **Inetpub/wwwroot** folder. It is extracted into the computer where Snort, MySQL, PHP, ACID reside. For this version we did not need to modify the adodb.inc.php file.

MySQL Installation:

For this project we have used MySQL Server version 4.1. The installation process is easy and windows installer is also available, which we have used. The download link of this installer was as follows:

http://dev.mysql.com/downloads/mysql/4.1.html

We have downloaded the windows installer from the webpage. At first we have downloaded the zip file and extracted in C drive (or you can choose any place). Extracted it and then double clicked the setup.exe file. The following screen will appear:



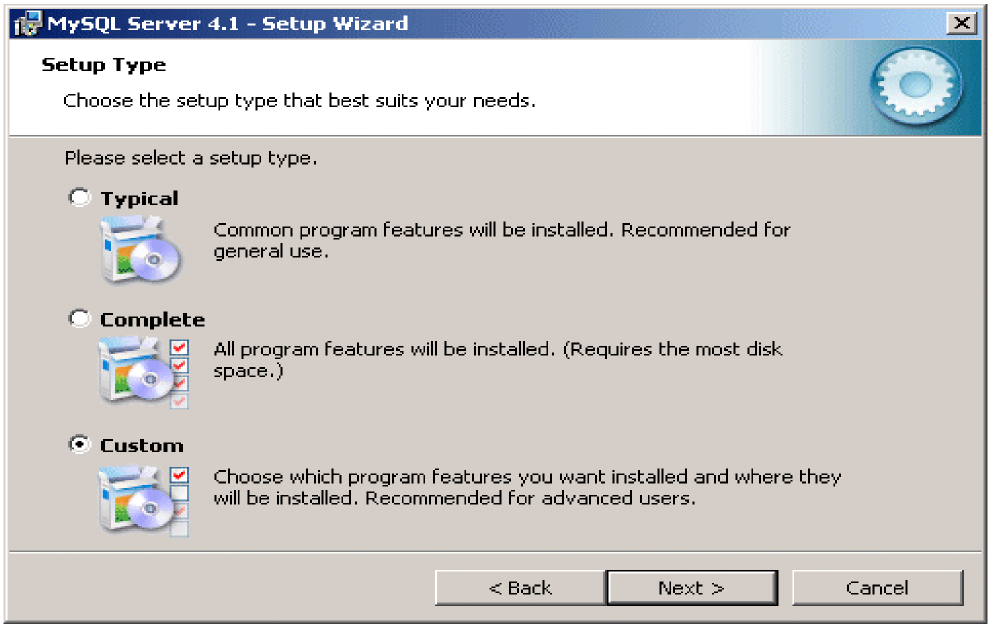
Welcome to the Setup Wizard for MySQL Server 4.1

The Setup Wizard will install MySQL Server 4.1 release 4.1.7 on your computer. To continue, click Next.

WARNING: This program is protected by copyright law.

Screen 1: Welcome screen

Click <Next> to start the installation wizard.



Setup Type

Choose the setup type that best suits your needs.

Please select a setup type.

○ **Typical**

Common program features will be installed. Recommended for general use.

○ **Complete**

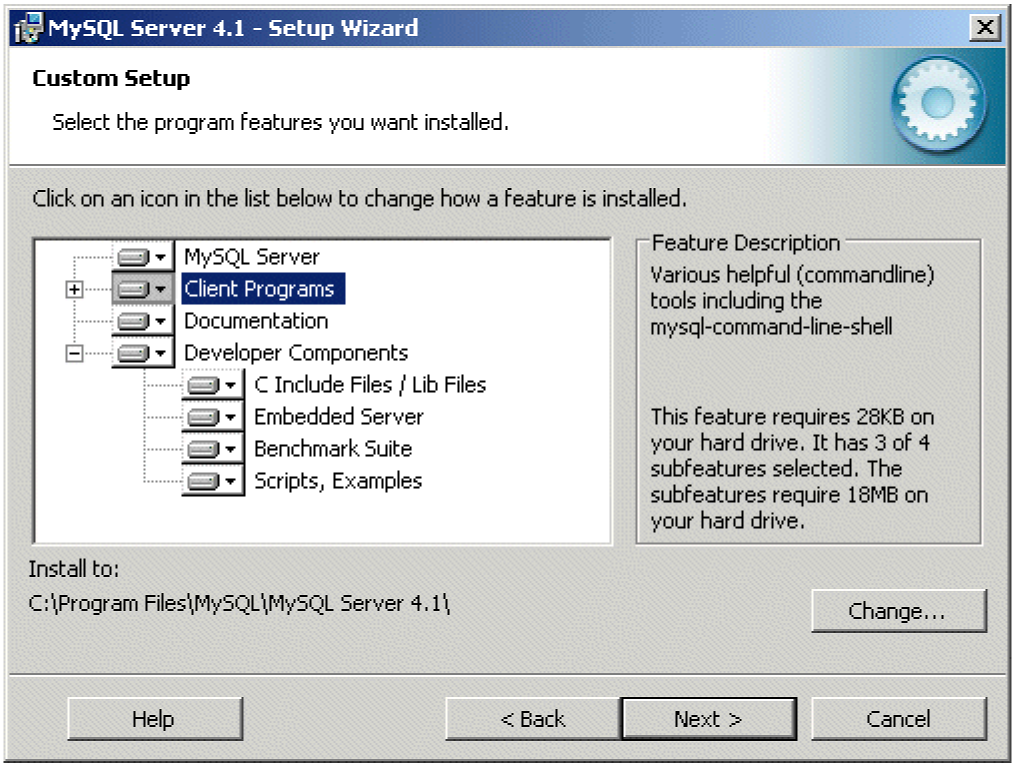
All program features will be installed. (Requires the most disk space.)

● **Custom**

Choose which program features you want installed and where they will be installed. Recommended for advanced users.

Screen 2: Setup Type Screen

To install the Developer Components, we will need to use the Custom setup type and click <Next> to continue.



MySQL Server 4.1 - Setup Wizard

Custom Setup

Select the program features you want installed.

Click on an icon in the list below to change how a feature is installed.

- MySQL Server
- Client Programs
- Documentation
- Developer Components
  - C Include Files / Lib Files
  - Embedded Server
  - Benchmark Suite
  - Scripts, Examples

Feature Description

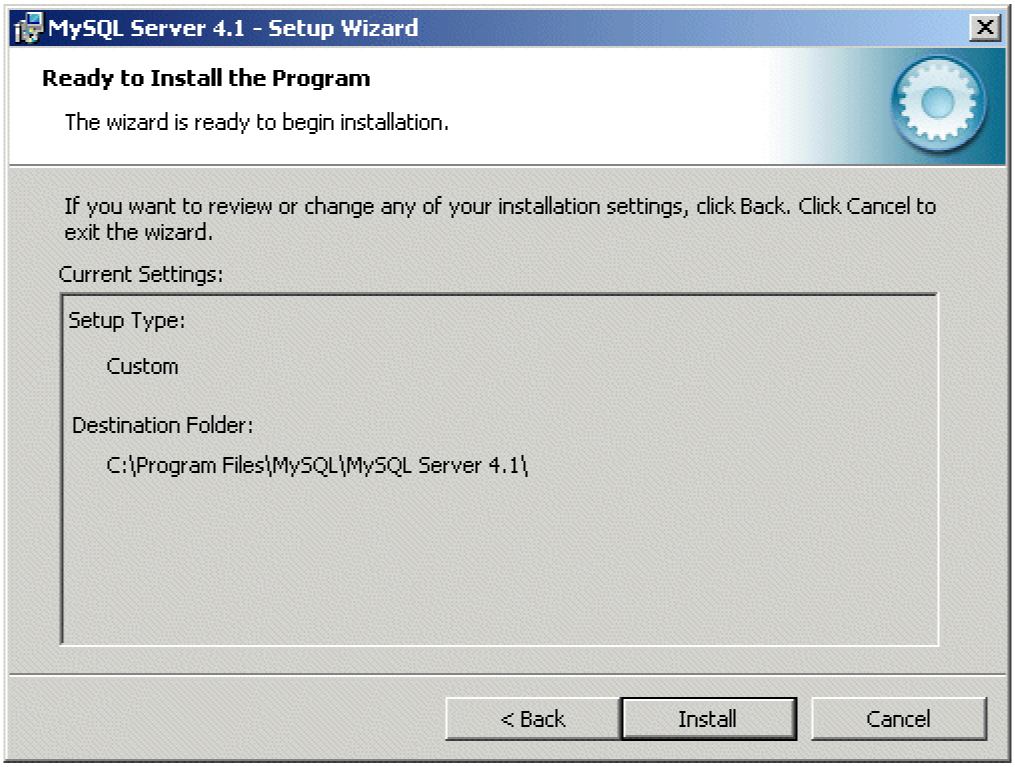
Various helpful (commandline) tools including the mysql-command-line-shell

This feature requires 28KB on your hard drive. It has 3 of 4 subfeatures selected. The subfeatures require 18MB on your hard drive.

Install to:
C:\Program Files\MySQL\MySQL Server 4.1\

Screen 3: Custom Setup Screen

Within the Custom Setup screen, select the Developer Components we would like to install and click <Next> to continue.



Ready to Install the Program

The wizard is ready to begin installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

Current Settings:

Setup Type:

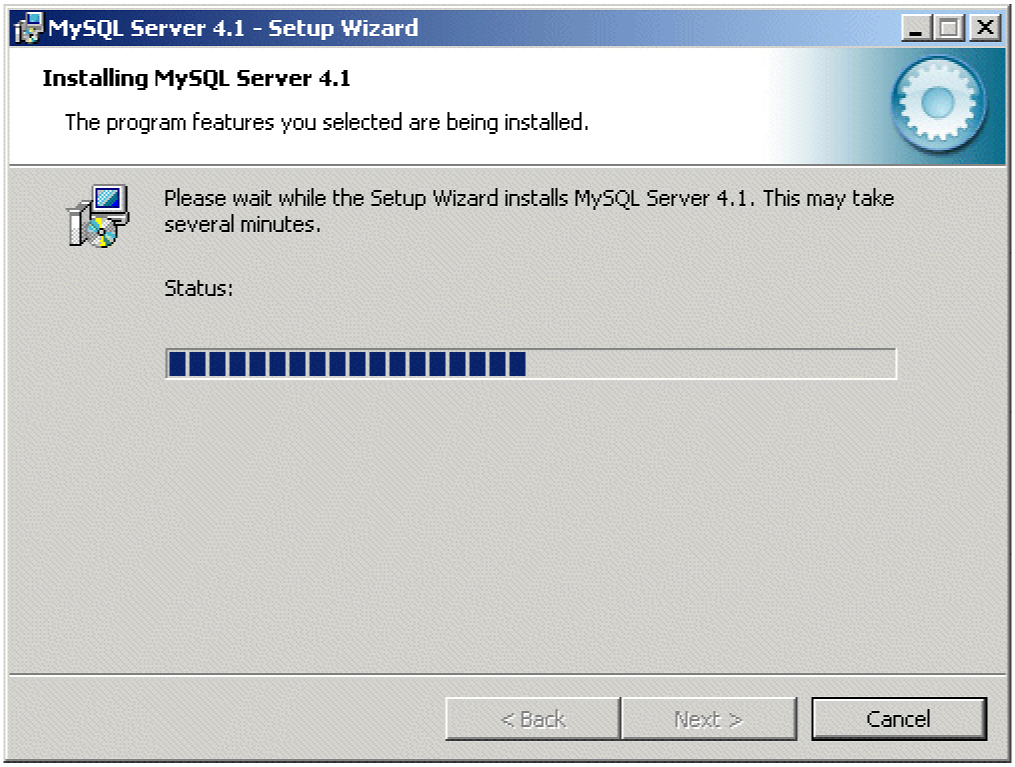
Custom

Destination Folder:

C:\Program Files\MySQL\MySQL Server 4.1\

Screen 4: Confirmation Screen

This is the confirmation screen. Review all choices and click <Install> to start the installation process.


MySQL Server 4.1 - Setup Wizard

Installing MySQL Server 4.1

The program features you selected are being installed.

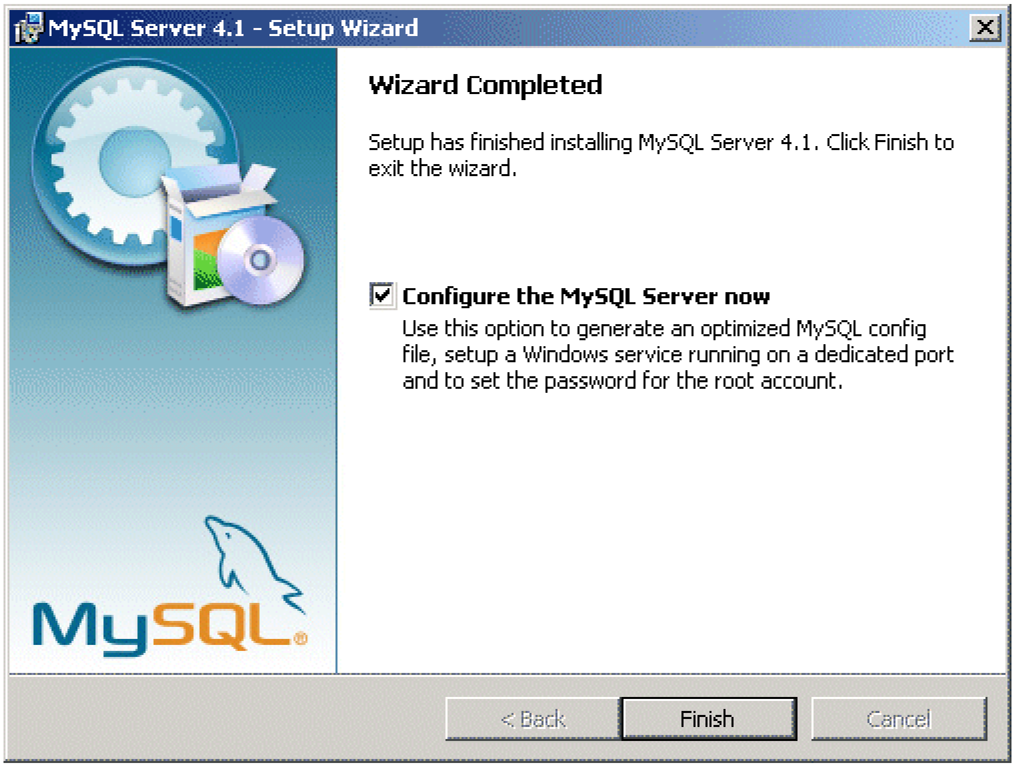
Please wait while the Setup Wizard installs MySQL Server 4.1. This may take several minutes.

Status:

Screen 5: Progress Screen

The installation process will now begin and all progress will be displayed.

Then a screen will be displayed for registration/ sign-up purpose with MySQL. We skipped that phase and clicked <Skip>.



MySQL Server 4.1 - Setup Wizard

Wizard Completed

Setup has finished installing MySQL Server 4.1. Click Finish to exit the wizard.

☑ **Configure the MySQL Server now**

Use this option to generate an optimized MySQL config file, setup a Windows service running on a dedicated port and to set the password for the root account.

Screen 6: Wizard Completed Screen

The installation is now complete. The checkbox for this configuration wizard is checked by default. We made our selection and click <Finish> to continue.

The next section provides using the MySQL Server Instance Configuration Wizard.

MySQL Server Instance Configuration Wizard:

- Click <Next> to start the wizard.
- Typically choose the Detailed Configuration option. Make your selection and click <Next> to continue.
- Since we will be doing mostly development, we keep the default Developer Machine option. Click <Next> to continue.
- We chose Multifunctional Database as our selection and clicked <Next> to continue.
- Click <Next> to continue.

- We chose DSS/ OLAP as we don’t need a heavy connection. Click <Next> to continue.
- We kept the default port of 3306. Click <Next> to continue.
- We chose Standard Character Set and clicked <Next> to continue.
- We checked the box Install as Windows Service and clicked <Next> to continue.
- Check Modify Security Setting box and select a password for root. In this case we selected “snort” as password.
- Click <Execute> and after that click <Finish> to complete the wizard.

Testing the Installation:

Ensure that the MySQL Software, (the MySQL Service), is running and you have set up the initial MySQL grant tables containing the privileges that determine how users are allowed to connect to the server. This is normally done with the when you configured the instance using the MySQL Server Instance Configuration Wizard.

For our tests, we put the MySQL bin directory in the PATH environment variable:

```
PATH=%PATH%;C:\Program Files\MySQL\MySQL Server 4.1\bin
```

MySQL Server Commands

mysqlshow - (All Databases)

To test the mySQL setup execute the following command:

```
C:\> mysqlshow -u root -p
Enter password: *****
+-----------+
| Databases |
+-----------+
| mysql     |
| test      |
+-----------+
C:\>
```

Configuring MySQL to use with Snort and ACID:

Reset the password to pre-4.1 style for each user that needs to use a pre-4.1 client program. This can be done using the SET PASSWORD statement and the OLD_PASSWORD() function:

```
mysql> SET PASSWORD FOR
   ➔ 'some_user'@'some_host' = OLD_PASSWORD('newpwd');
```

For our case we used the following command:

```
mysql> SET PASSWORD FOR
   ➔ 'root'@'localhost' = OLD_PASSWORD('snort');
```

We also added the following line into my.ini file:

old_passwords

DBTools Installation:

We downloaded the DBTools Manager Professional 3.1 from the following link:

http://www.dbtools.com.br/EN/downloads/downloads.php?file_id=9

DBTools Install

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

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

DBTools Configuration

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

- Type in the **Username** which will be 'Root' because that is what we specified in the my.ini file of MySql
- Type in the **Password** which will be 'Sally' because we also specified that in the my.ini
- Leave the **Database** name blank- You are just configuring the server, the database

will be created later

- Click on **Server**, then click on **Save**
- Click on **Link**
- Click on Test **Link**. This checks to see if there is a MySql server running on port 3306 that can be attached to using the name Root with the password Sally
- Click **OK** to the Connection Successful dialogue box
- Exit Server Manager
- Click **Yes** to Reload the Profile
- On the left hand side expand Snort
- Right Click on **Databases**
- Click on **Create**
- Type in 'Snort' for the database name
- Click **OK**-You just created the Snort database that Snort will log to
- For the Set privilege on Database use the pull down menu to choose Snort- this allows the user that we just created to have access to the database that we also created
- Click on **OK**
- Put a check in the **Create** box as well- this will allow Snort to log new alerts to the database
- Click on **Save**, then **OK**
- Click on **Close**

Close DBTools

IIS Installation:

For this installation we needed the Windows XP Professional Installation CD-ROM. After inserting the CD when it pops up for the installation then we exit that window.

Then START > Control Panel > Add or Remove Programs > Add/Remove Windows Components > Check the IIS service > NEXT.

Then just following the installer prompt will successfully install the IIS in the computer.

Testing IIS:

To test the IIS, we went to Control Panel > Administrative Tools > Services. We have found that IIS Admin is started, which means that it is working properly.

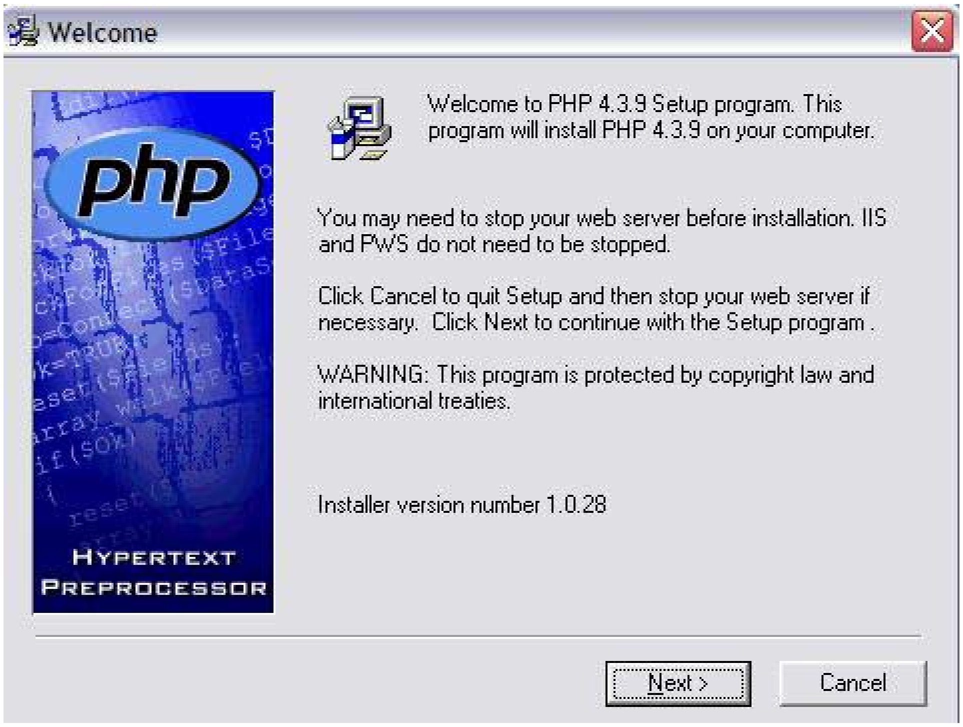
PHP Installation:

To download the PHP installer we followed the following link:

http://ca.php.net/get/php-4.3.9-installer.exe/from/a/mirror

Then we chose CA.PHP.NET as a mirror. Choosing other mirror will also work. Then click <Run>. It will start the installer.

The following welcome screen will be shown:



Welcome to PHP 4.3.9 Setup program. This program will install PHP 4.3.9 on your computer.

You may need to stop your web server before installation. IIS and PWS do not need to be stopped.

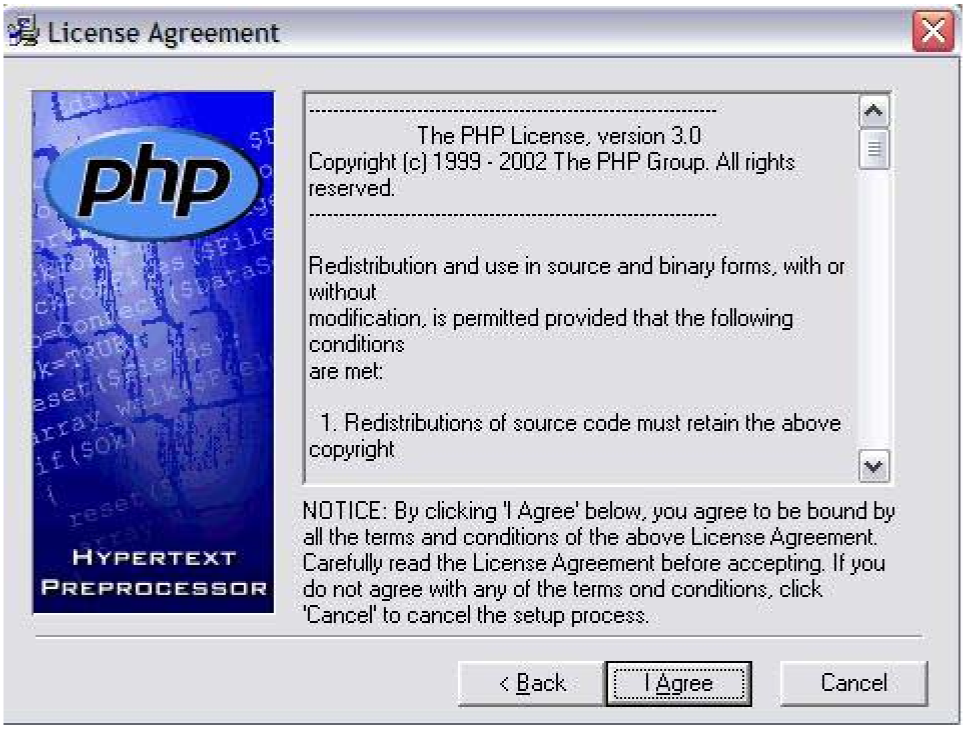
Click Cancel to quit Setup and then stop your web server if necessary. Click Next to continue with the Setup program .

WARNING: This program is protected by copyright law and international treaties.

Installer version number 1.0.28

Screen: Welcome screen

Click <Next>.

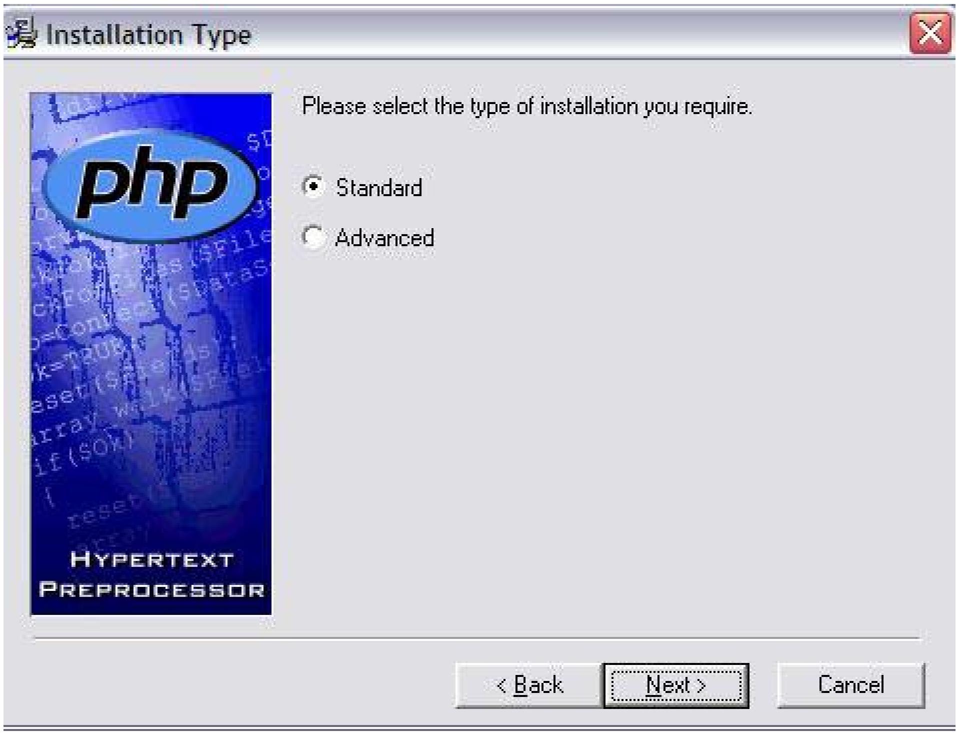


```
-------------------------------------------------------------------
                 The PHP License, version 3.0
Copyright (c) 1999 - 2002 The PHP Group. All rights
reserved.
-------------------------------------------------------------------

Redistribution and use in source and binary forms, with or
without
modification, is permitted provided that the following
conditions
are met:

  1. Redistributions of source code must retain the above
copyright
```

NOTICE: By clicking 'I Agree' below, you agree to be bound by all the terms and conditions of the above License Agreement. Carefully read the License Agreement before accepting. If you do not agree with any of the terms ond conditions, click 'Cancel' to cancel the setup process.

Screen: License Agreement

Click <I Agree> to proceed.

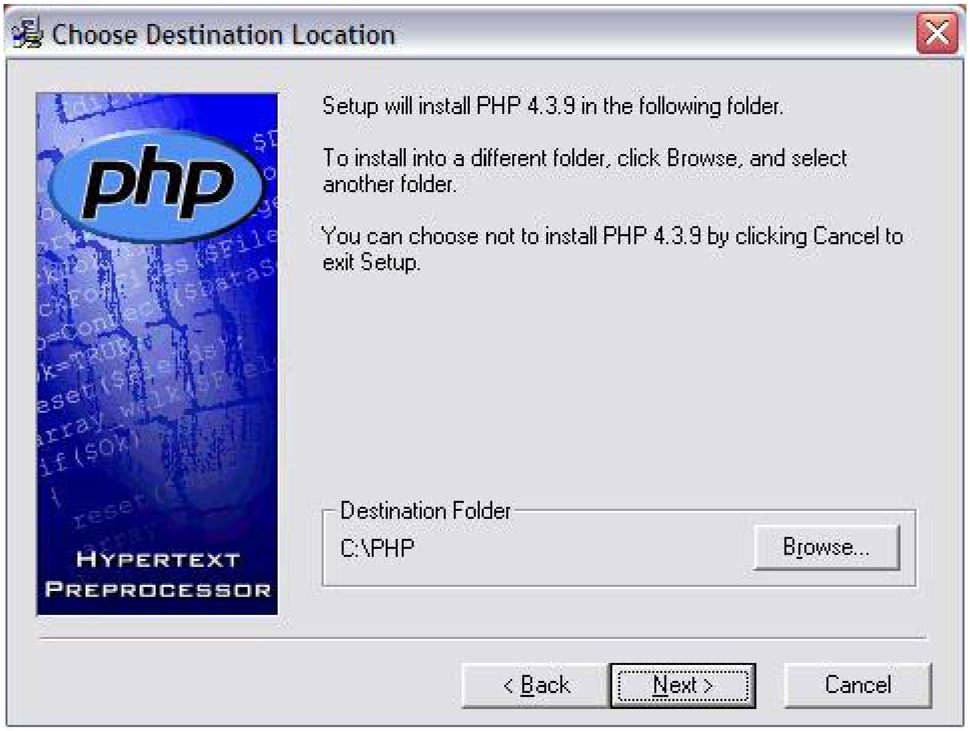


Please select the type of installation you require.

● Standard

○ Advanced

Check mark Standard and click <Next> to continue.



Setup will install PHP 4.3.9 in the following folder.

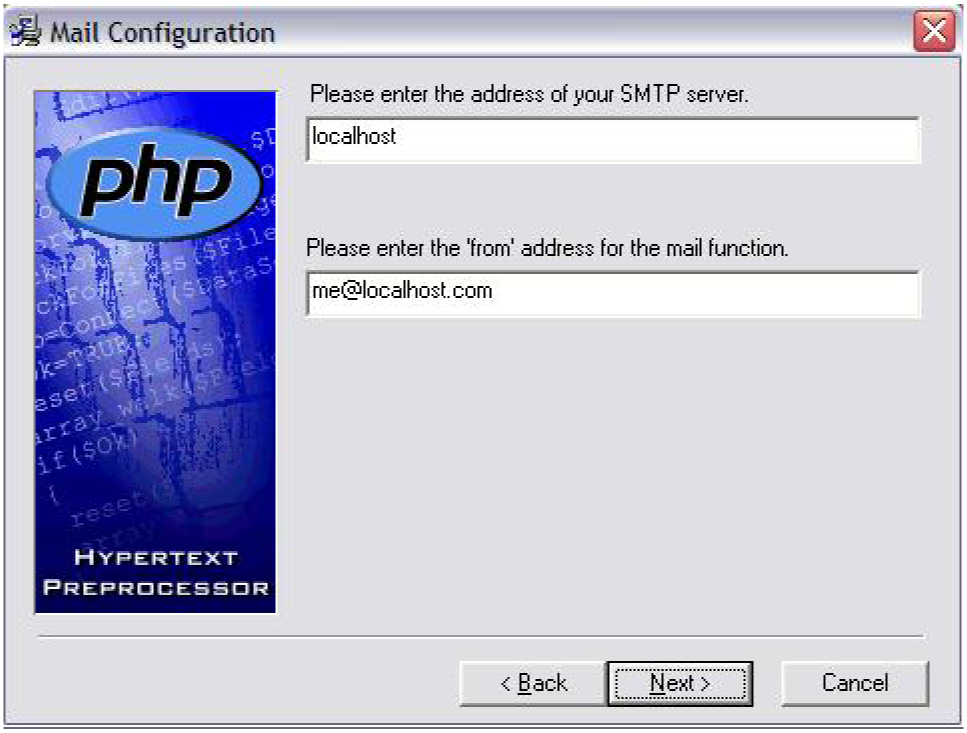
To install into a different folder, click Browse, and select another folder.

You can choose not to install PHP 4.3.9 by clicking Cancel to exit Setup.

Destination Folder

C:\PHP

Click <Next> to install.



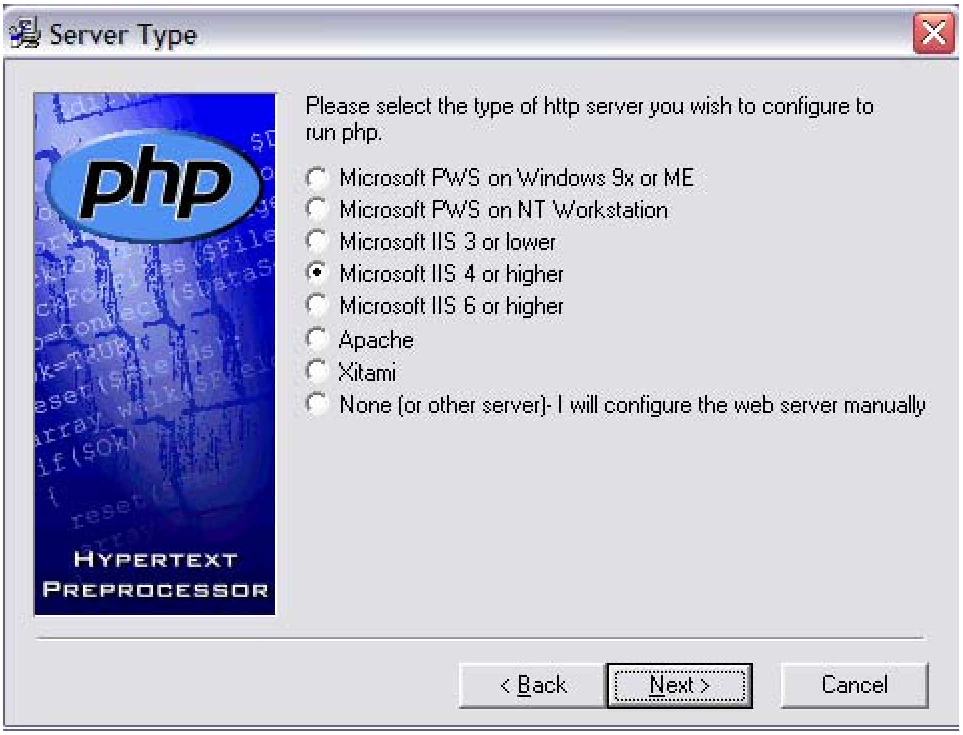
Please enter the address of your SMTP server.

localhost

Please enter the 'from' address for the mail function.

me@localhost.com

Click <Next> to continue.

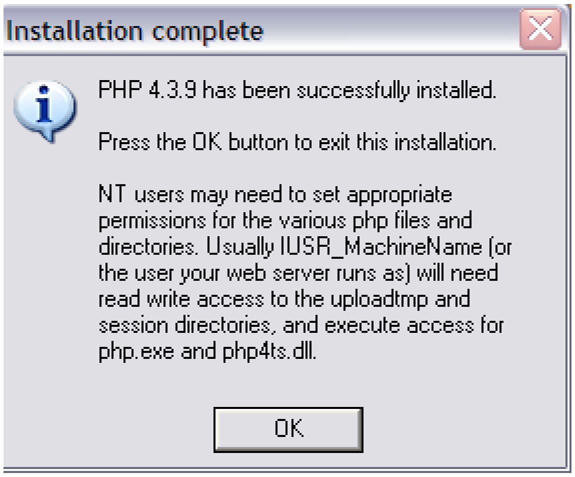

Server Type

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
○ Microsoft IIS 6 or higher
○ Apache
○ Xitami
○ None (or other server)- I will configure the web server manually

Since our IIS version was 5.x,we chose Microsoft IIS 4 or higher. Then Click <Next>.

Then again a confirmation window will be shown and click <Next> to that window. Then the following window will show the progress of the installation and when successfully completed the following window will be shown.


Installation complete

PHP 4.3.9 has been successfully installed.

Press the OK button to exit this installation.

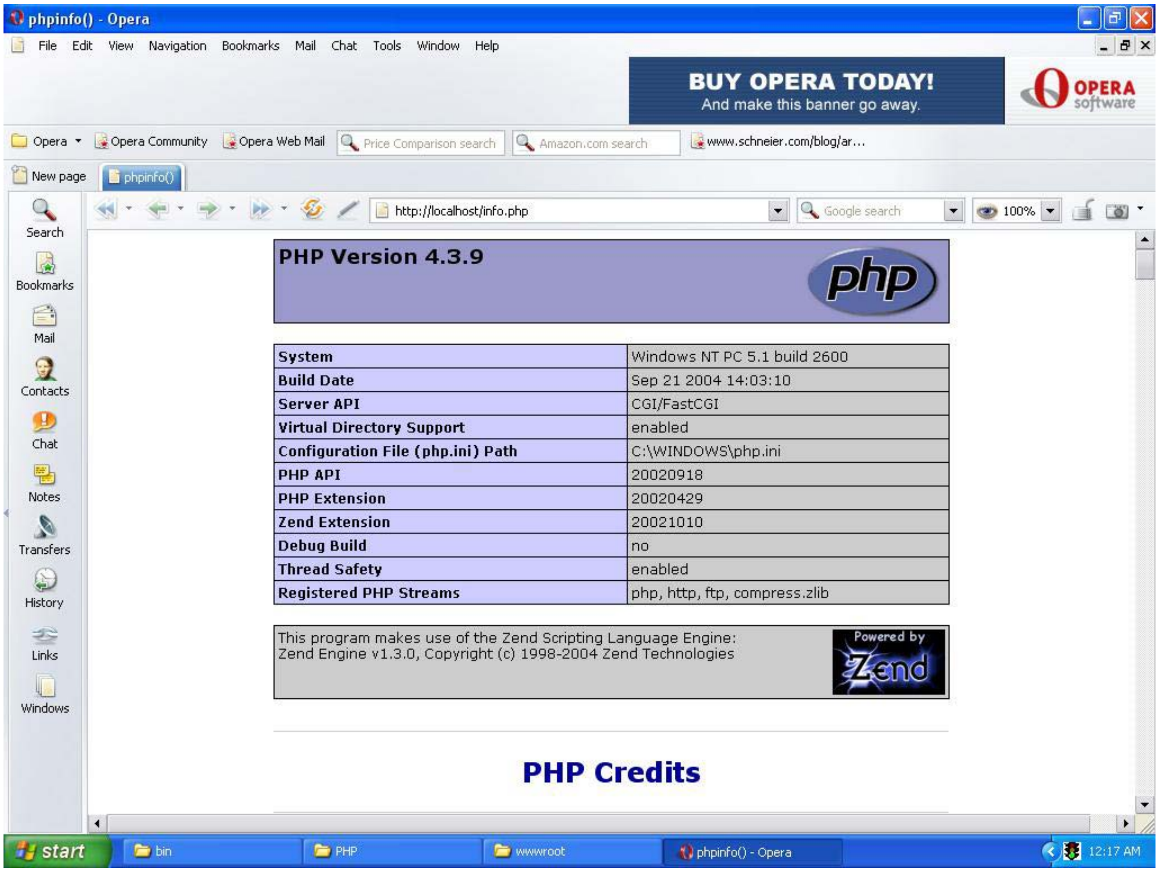
NT users may need to set appropriate permissions for the various php files and directories. Usually IUSR_MachineName (or the user your web server runs as) will need read write access to the uploadtmp and session directories, and execute access for php.exe and php4ts.dll.

Click <OK> to finish the installation.

Testing the PHP:

To test the PHP, we made a sample php file as follows:

- Open notepad
- Type: <?phpinfo() ?>
- Save the file as “info.php”
- Place the file in C:\Inetpub\wwwroot\
- Open the browser and type http://localhost/info.php
- If the page shows something like below, then the installation is successful.



PHP Version 4.3.9

System	Windows NT PC 5.1 build 2600
Build Date	Sep 21 2004 14:03:10
Server API	CGI/FastCGI
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\WINDOWS\php.ini
PHP API	20020918
PHP Extension	20020429
Zend Extension	20021010
Debug Build	no
Thread Safety	enabled
Registered PHP Streams	php, http, ftp, compress.zlib

This program makes use of the Zend Scripting Language Engine:
Zend Engine v1.3.0, Copyright (c) 1998-2004 Zend Technologies

PHP Credits

PHPLOT Installation

We downloaded PHPLOT from the following link:

http://prdownloads.sourceforge.net/phplot/phplot-5.0rc1.tar.bz2?download

The version we used here is 5.0rcl. After downloading it we extracted it into C:\Inetpub\wwwroot\phplot. PHPLOT is usually required for graphical information to be showed by ACID.

SNORT Installation

Snort is a versatile, lightweight network IDS, capable of performing real-time traffic analysis and packet logging on IP networks. It can perform protocol analysis, content searching/matching. It can be used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI (Common Gateway Interface) attacks, SMB probes, OS fingerprinting attempts, and more. Snort uses a flexible rules language to describe traffic that it should collect or pass, and includes a detection engine utilizing a modular plug-in architecture. Snort has real-time alerting capability as well, incorporating alerting mechanisms for Syslog, user- specified files, a UNIX socket, or WinPopup messages to Windows clients using Samba's smbclient. Snort has three primary uses. It can be used as a straight packet sniffer like tcpdump or as a packet logger that is useful for network traffic debugging. It can also be used as a full-blown network intrusion detection system.

Snort logs packets in either tcpdump binary format or in Snort's decoded ASCII format to logging directories.

We have downloaded the snort version 2.4.3 from the following link:

http://www.snort.org/dl/binaries/win32/Snort_243_Installer.exe

To install snort 2.4.3 just double click on the Snort_243_Installer.exe file.

- Copy all of the Files that are the **Rules** type to **C:\Snort\Rules**

- Change to the Contrib directory
- Copy the **Create_MySQL** file to **C:\Snort**

Then we have to configure the snort.conf file located at C:\Snort\etc\ according to our usage.

Configuring snort.conf:

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

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

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

Network Variables

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

Home Address Range

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

var HOME_NET any (var is the keyword for variable)

This setting will monitor your entire network by default. To monitor a single host with an IP Address of x.x.x.1, change the **any** to x.x.x.1/32. The /32 represents how many bits are in the subnet mask. Because this is monitoring the localhost, the subnet is 255.255.255.255. If you are not getting any alerts, you may want to check this section to be sure that the subnet mask is correct. **var HOME_NET x.x.x.1/32** To monitor the entire network x.x.x.0 with a subnet mask of 255.255.255.0 (24 bits) configure the HOME_NET section of the Snort.conf like so: **var HOME_NET x.x.x.0/24**

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

External Address range

Change **var EXTERNAL_NET any** to

var EXTERNAL_NET !$HOME_NET

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

SMTP Servers

Configure the SMTP section to

var SMTP $HOME_NET

Setting specific IP Addresses for your mail servers in this section will reduce the number of false alerts, but setting it to **$HOME_NET** will set it to monitor what is specifed in the **$HOME_NET** section **Web Servers** To configure your Web Servers set the variable to **var HTTP_SERVERS $HOME_NET** for a large Network. Again if you set this to be the IP Addresses of your Web Servers, the number of false alerts will be minimized, but you can set it to **$HOME_NET** as well. It may not be practical to type in the IP Addresses of 100 Web servers.

SQL Servers

Configure the SQL Server section to be

var SQL_SERVERS $HOME_NET

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

DNS Servers

Configure the DNS Server Section to be

var DNS_SERVERS [10.20.30.100/24,10.20.30.101/24]

Configuring this section will prevent false DNS related scan alarms. At the bottom of the Network Variable section is a line that specifies where the RULE files are located. Be sure to configure the entire path as shown or Snort may not start correctly:

var RULE_PATH C:\Snort\Rules

Configure Preprocessors

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

preprocessor frag2

This preprocessor provides IP deframentation and detects fragmentation attacks.

preprocessor stream4: detect_scans

This preprocessor generates alerts on detection of stealth portscans.

preprocessor stream4_reassemble

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

preprocessor http_decode: 80 -unicode –cginull

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

preprocessor rpc_decode: 111

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

preprocessor bo: -nobrute

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

preprocessor telnet_decode

This preprocessor normalizes telnet and FTP traffic by reassembling the traffic into data that can be matched against the rules.

preprocessor portscan-ignorehosts: 0.0.0.0

You should uncomment this preprocessor line and configure it with the IP Addresses of the DNS Servers to prevent false DNS alerts. Put any IP Addresses or networks in this section that port scans should be ignored.

Note: To uncomment simply remove the ‘#’ in front of preprocessor

Configure Output Plugins

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

output database: log, MySQL, user=root password=snort dbname=snort host=localhost
NOTE: Be sure not to confuse the MySql with MSSQL. They look very similar so it's easy to uncomment out the wrong one.

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

The following line will be found at the end of the Output Plugins section:
include classification.config

Change that line to include the entire path to the classification.config like so:
include C:\Snort\Rules\Classification.config

The classification.config is used to classify and prioritize alerts when they come in. This can be tailored to your specific needs but in this example we will leave it as default.

Customize your Ruleset
The last section of the Snort.conf is used to customize the rulesets. Here you will find text that looks similar tothis:

include $RULE_PATH/bad-traffic.rules

include $RULE_PATH/exploit.rules

include $RULE_PATH/scan.rules

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

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

Save Snort.conf

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

Test Snort

- Open up a command prompt
- At the **C:\Snort>** type **snort –W**

This will list all of the available network interfaces. Here we'll use 2, since 2 is our Ethernet network adapter card..

- At the **C:\Snort>** type **snort –v –i2**

This will start Snort in verbose mode and will listen on adapter 2.

- Press **Enter**
- Snort should start and you should see alerts similar to this:

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

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

- Hold down the **<crtl>** and **<c>** keys on the keyboard to kill the instance of Snort
- At the same prompt type in **Snort -c C:\Snort\Snort.conf -l C:\Snort\log –i2,** press **Enter**

This will start Snort using the rules file **C:\Snort\Snort.conf** and will log to the directory **C:\Snort\Logs** the traffic on network interface 1

- You should see something similar to this:

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

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

NOTE: The above snort configuration chapter has been taken from http://www.sans.org/rr/whitepapers/detection/362.php

JPGraph Installation:

JpGraph is a Object-Oriented Graph creating library for PHP >= 4.3.1 The library is completely written in PHP and ready to be used in any PHP scripts (both CGI/APXS/CLI versions of PHP are supported).

The library can be used to create numerous types of graphs either on-line or written to a file. JpGraph makes it easy to draw both "quick and dirty" graphs with a minimum of code as well as complex graphs which requires a very fine grained control. The library assigns context sensitive default values for most of the parameters which minimizes the learning curve. ACID will use this JPGraph for creating bar, chart, pie graph to show us the alerts.

We have downloaded the JPGraph version 1.20.3 from the following location:

http://www.aditus.nu/jpgraph/jpdownload.php

After downloading the file we extracted it into C:\Inetpub\wwwroot folder. There is no configuration is needed for JPGraph.

ACID Installation

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

Just extract the zip file from the following link and place the extracted folder named acid in the right place:

http://www.andrew.cmu.edu/~rdanyliw/snort/acid-0.9.6b21.tar.gz

- Create a folder named '**Acid**' under the **C:\Inetpub\wwwroot** folder
- Unzip the **acid-0.9.6b21.zip** into this folder
- Open and Edit the **acid_conf.php** file with Wordpad

Configuring acid_conf.php:

- Make the following changes to the file to give it the needed Snort database information:

DBlib_path = "**C:\Inetpub\wwwroot\ADODB**" – This is the database abstraction library variable

$alert_dbname = "snort"; - This is the name of the Database that we created earlier in DBTools Manager.

$alert_host = "localhost"; - This is the name of the server. ‘Localhost’ will work

$alert_port = "3306"; - This is the port number specified earlier in WinMySqlAdmin that MySql runs on

$alert_user = "root"; - This is the user that we created earlier in DBTools

Manager

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

$archive_dbname = "snort"; - This is the archive database

$archive_host = "localhost"; - The name of the server that has the archive database

$archive_port = "3306"; - The port number that the archive database is listening on

$archive_user = "root"; - The user that has access to the archive database

$archive_password = "snort"; -The password of that user

$ChartLib_path = "**C:\Inetpub\wwwroot\jpgraph-1.20.3\src**" – This is the entire path of the Jpgraph graphing library.

NOTE: Be sure to use double quotation marks around each setting or ACID will not work. Also, keep in mind that your username and password should be different than what is provided in this example.

- Reboot your computer

Acid Viewer Configuration

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

should successfully come up.

CommView Installation:

CommView is a powerful network monitor and analyzer designed for LAN administrators, security professionals, network programmers, home users…virtually anyone who wants a full picture of the traffic flowing through a PC or LAN segment. Loaded with many user-friendly features, CommView combines performance and flexibility with an ease of use unmatched in the industry.

This application captures every packet on the wire to display important information such as a list of packets and network connections, vital statistics, protocol distribution charts, and so on. You can examine, save, filter, import and export captured packets, view protocol decodes down to the lowest layer with full analysis of over 70 widespread protocols.

We have downloaded CommView 5.1 from the following link:
http://www.download-by.net/network-and-internet/network-monitoring/21450,commview,dl.html

To install commview after extracting we just need to double-click the exe file and it will guide us through windows installer wizard.

We downloaded this software in the another pc from which one we will be sending packets to the machine where snort, acid, mysql, php reside.

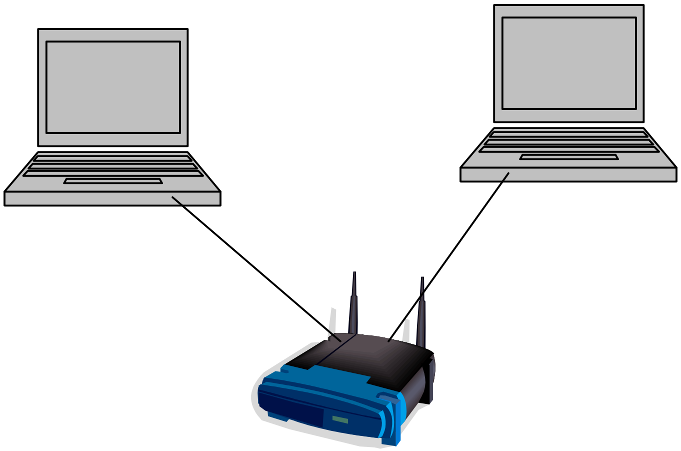
TESTING THE TOTAL SYSTEM:

Preparing the test-bed:

Equipments:

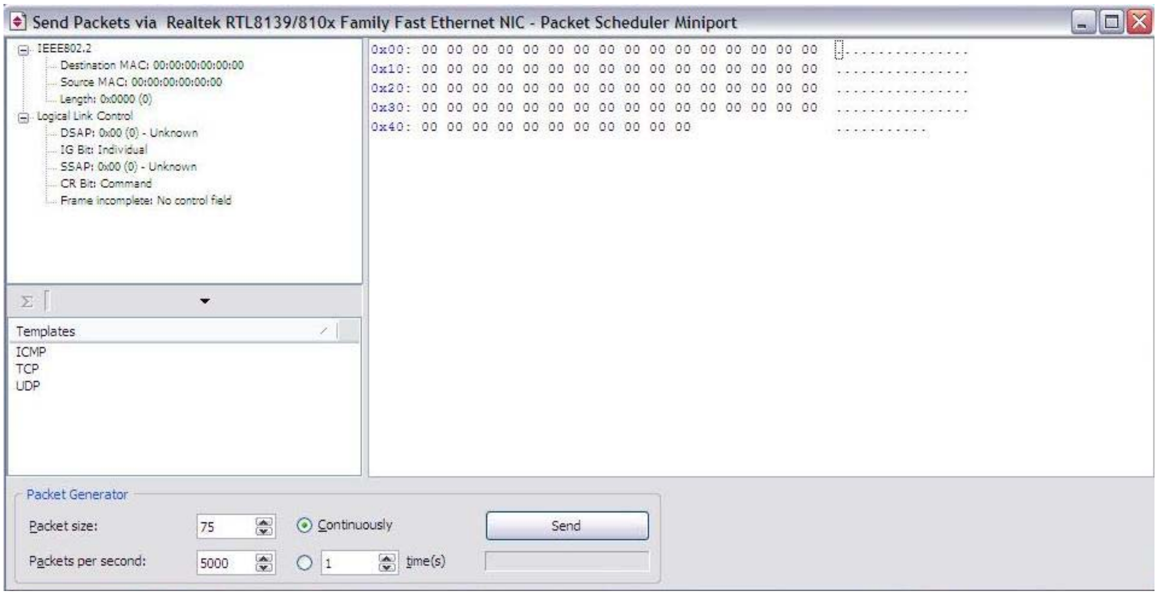
1. Laptop 1: Intel Centrino 1.5 Ghz, 512 MB RAM, 2MB L2 cache, 60 GB hard disk. Software installed:
    - Windows XP home edition SP2
    - CommView 5.1
2. Laptop 2: Pentium 4 1.5 GHz, 256 MB RAM, 60 GB hard drive. Software installed:
    - Windows XP Professional SP2
    - MySQL Server 4.1
    - DBTools Manager Professional 3.1
    - PHP 4.3.9
    - SNORT 2.4.3
    - PHPLOT 5.0rcl
    - Jpgraph 1.20.3
    - ACID 0.9.6b21

3. D-link Ethernet Broadband Router model: DI-740UP



Step 1: Generate Packet in Laptop 1:

- Open CommView
- Go to Tools>Packet Generator. A window like below will open:



Send Packets via Realtek RTL8139/810x Family Fast Ethernet NIC - Packet Scheduler Miniport

```
⊟ IEEE802.2
    Destination MAC: 00:00:00:00:00:00
    Source MAC: 00:00:00:00:00:00
    Length: 0x0000 (0)
⊟ Logical Link Control
    DSAP: 0x00 (0) - Unknown
    IG Bit: Individual
    SSAP: 0x00 (0) - Unknown
    CR Bit: Command
    Frame incomplete: No control field
```

```
0x00: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0x10: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0x20: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0x30: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0x40: 00 00 00 00 00 00 00 00 00 00 00                 ...........
```

Templates
ICMP
TCP
UDP

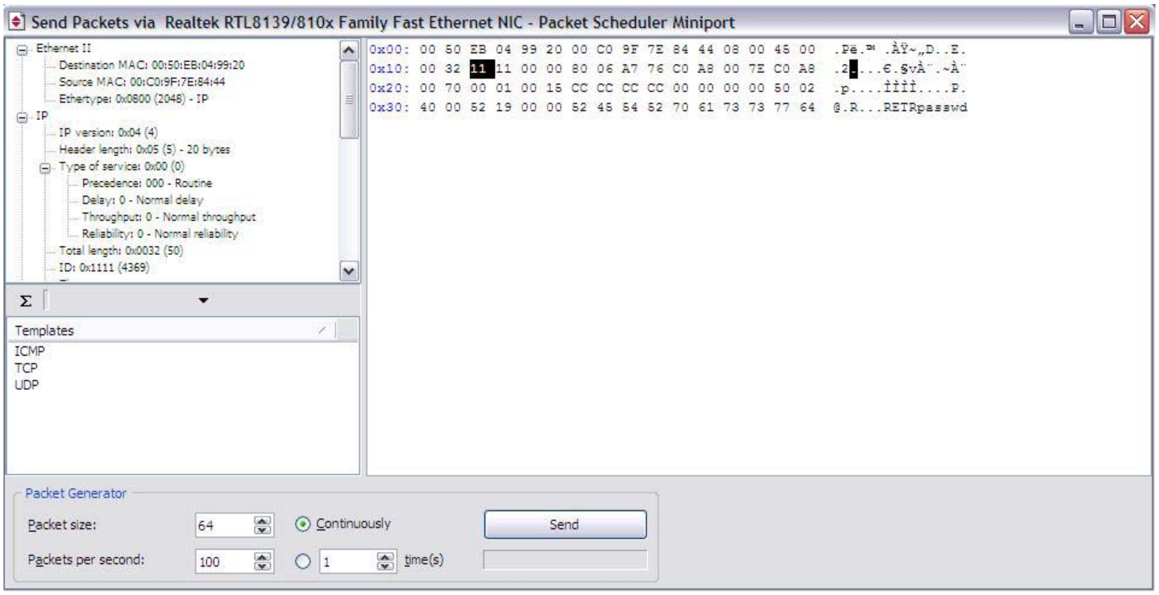
Packet Generator

Packet size: 75 — ● Continuously

Packets per second: 5000 — ○ 1 time(s)

- Select the type of packet (TCP/ UDP/ ICMP)

- Write destination MAC, source MAC, dest IP, source IP
- Place contents of the packets after from Urgent Pointer.
- Calculate the total length.
- Click on checksum button. If all checksums show correct then the packet is ready.
- All information will have to be in hex format.
- A sample packet with sid:356 is shown below:



Send Packets via Realtek RTL8139/810x Family Fast Ethernet NIC - Packet Scheduler Miniport

```
Ethernet II
    Destination MAC: 00:50:EB:04:99:20
    Source MAC: 00:C0:9F:7E:84:44
    Ethertype: 0x0800 (2048) - IP
IP
    IP version: 0x04 (4)
    Header length: 0x05 (5) - 20 bytes
    Type of service: 0x00 (0)
        Precedence: 000 - Routine
        Delay: 0 - Normal delay
        Throughput: 0 - Normal throughput
        Reliability: 0 - Normal reliability
    Total length: 0x0032 (50)
    ID: 0x1111 (4369)
```

```
0x00: 00 50 EB 04 99 20 00 C0 9F 7E 84 44 08 00 45 00  .Pë.™ .ÀŸ~„D..E.
0x10: 00 32 11 11 00 00 80 06 A7 76 C0 A8 00 7E C0 A8  .2....€.§vÀ¨.~À¨
0x20: 00 70 00 01 00 15 CC CC CC CC 00 00 00 00 50 02  .p....ÌÌÌÌ....P.
0x30: 40 00 52 19 00 00 52 45 54 52 70 61 73 73 77 64  @.R...RETRpasswd
```

Templates

ICMP
TCP
UDP

Packet Generator

Packet size: 64 ● Continuously

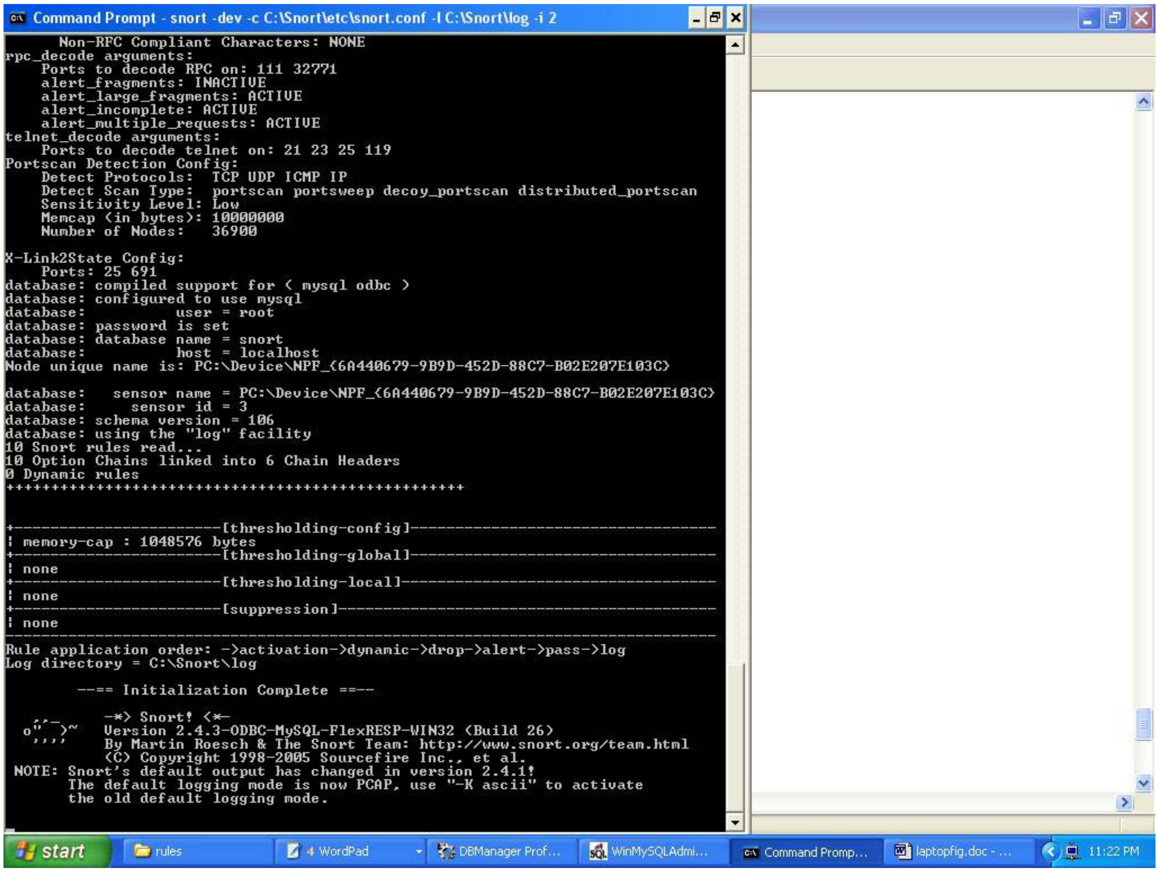
Packets per second: 100 ○ 1 time(s)

Step 2: Start SNORT:

- Go to command prompt. Go to C:\Snort\bin
- Give the following command:

  C:\Snort\bin>snort –dev –c C:\snort\etc\snort.conf –l C:\snort\log –i2

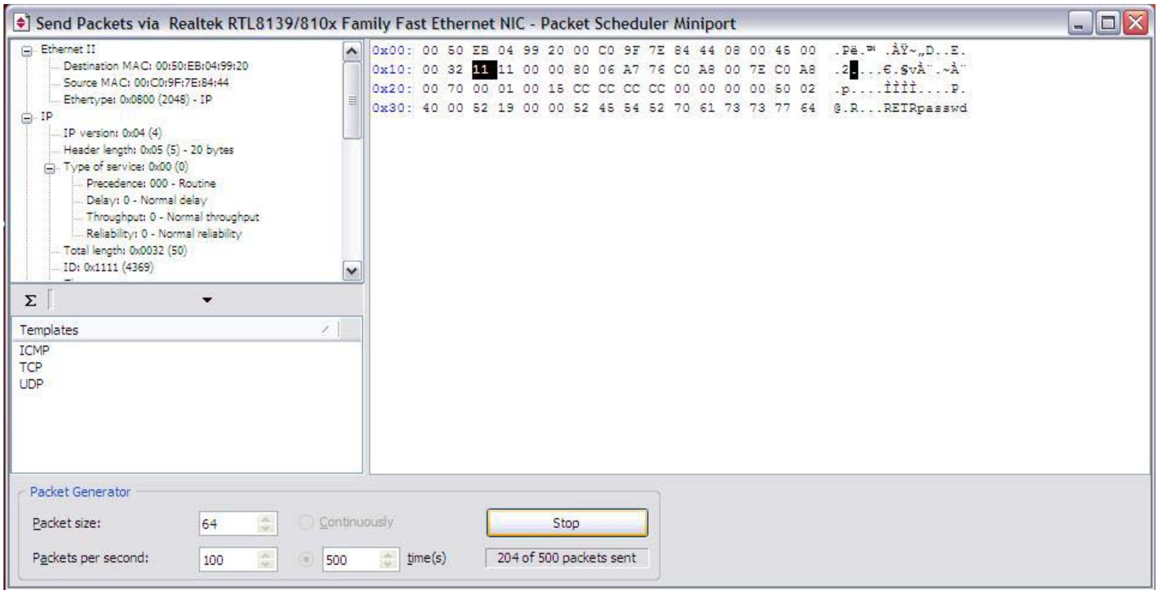
The screenshot will be like below:



```
       Non-RFC Compliant Characters: NONE
rpc_decode arguments:
    Ports to decode RPC on: 111 32771
    alert_fragments: INACTIVE
    alert_large_fragments: ACTIVE
    alert_incomplete: ACTIVE
    alert_multiple_requests: ACTIVE
telnet_decode arguments:
    Ports to decode telnet on: 21 23 25 119
Portscan Detection Config:
    Detect Protocols:  TCP UDP ICMP IP
    Detect Scan Type:  portscan portsweep decoy_portscan distributed_portscan
    Sensitivity Level: Low
    Memcap (in bytes): 10000000
    Number of Nodes:   36900

X-Link2State Config:
    Ports: 25 691
database: compiled support for ( mysql odbc )
database: configured to use mysql
database:          user = root
database: password is set
database: database name = snort
database:          host = localhost
Node unique name is: PC:\Device\NPF_{6A440679-9B9D-452D-88C7-B02E207E103C}

database:   sensor name = PC:\Device\NPF_{6A440679-9B9D-452D-88C7-B02E207E103C}
database:     sensor id = 3
database: schema version = 106
database: using the "log" facility
10 Snort rules read...
10 Option Chains linked into 6 Chain Headers
0 Dynamic rules
+++++++++++++++++++++++++++++++++++++++++++++++++++


+-----------------------[thresholding-config]----------------------------------
| memory-cap : 1048576 bytes
+-----------------------[thresholding-global]----------------------------------
| none
+-----------------------[thresholding-local]-----------------------------------
| none
+-----------------------[suppression]------------------------------------------
| none
-------------------------------------------------------------------------------
Rule application order: ->activation->dynamic->drop->alert->pass->log
Log directory = C:\Snort\log

        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.4.3-ODBC-MySQL-FlexRESP-WIN32 (Build 26)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/team.html
           (C) Copyright 1998-2005 Sourcefire Inc., et al.
 NOTE: Snort's default output has changed in version 2.4.1!
       The default logging mode is now PCAP, use "-K ascii" to activate
       the old default logging mode.
```

Step 3: Send Packet:

- We can choose the packet sending options (like sending rate, how many times/ continuous etc).
- Then press the Send button in CommView.



Send Packets via Realtek RTL8139/810x Family Fast Ethernet NIC - Packet Scheduler Miniport

```
Ethernet II
    Destination MAC: 00:50:EB:04:99:20
    Source MAC: 00:C0:9F:7E:84:44
    Ethertype: 0x0800 (2048) - IP
IP
    IP version: 0x04 (4)
    Header length: 0x05 (5) - 20 bytes
    Type of service: 0x00 (0)
        Precedence: 000 - Routine
        Delay: 0 - Normal delay
        Throughput: 0 - Normal throughput
        Reliability: 0 - Normal reliability
    Total length: 0x0032 (50)
    ID: 0x1111 (4369)
```

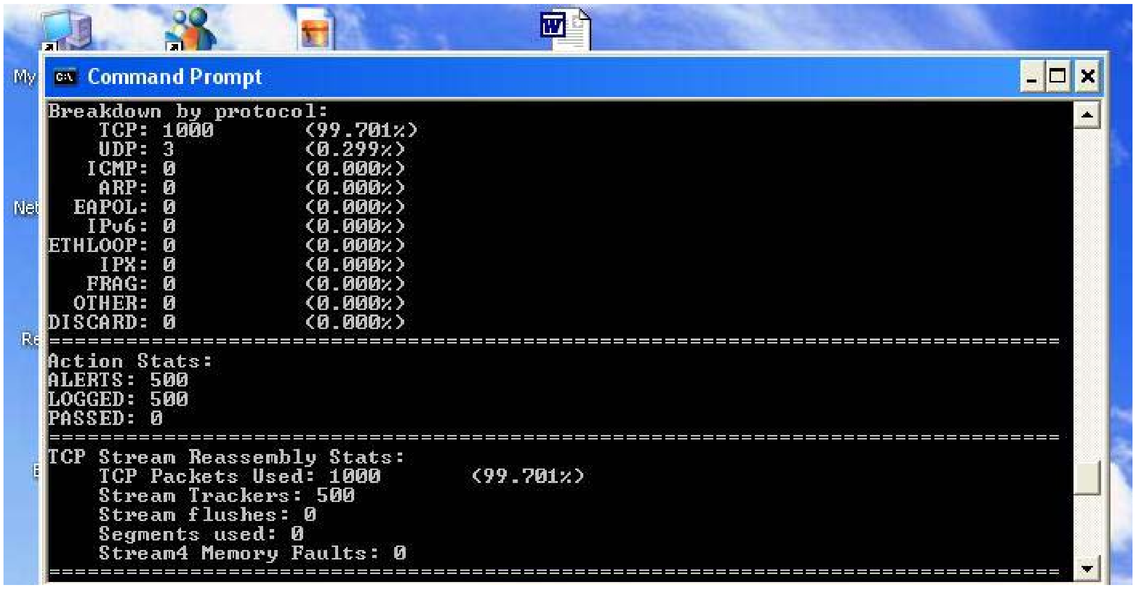
```
0x00: 00 50 EB 04 99 20 00 C0 9F 7E 84 44 08 00 45 00  .Pë.™ .ÀŸ~„D..E.
0x10: 00 32 11 11 00 00 80 06 A7 76 C0 A8 00 7E C0 A8  .2....€.§vÀ¨.~À¨
0x20: 00 70 00 01 00 15 CC CC CC CC 00 00 00 00 50 02  .p....ÌÌÌÌ....P.
0x30: 40 00 52 19 00 00 52 45 54 52 70 61 73 73 77 64  @.R...RETRpasswd
```

Templates: ICMP, TCP, UDP

Packet Generator
Packet size: 64
Packets per second: 100
○ Continuously
● 500 time(s)
204 of 500 packets sent

Step 4: See at Snort:

- Snort will show that it is getting packets continuously. When done press CTR+C
- Snort screen will show that it has generated and logged alerts successfully.

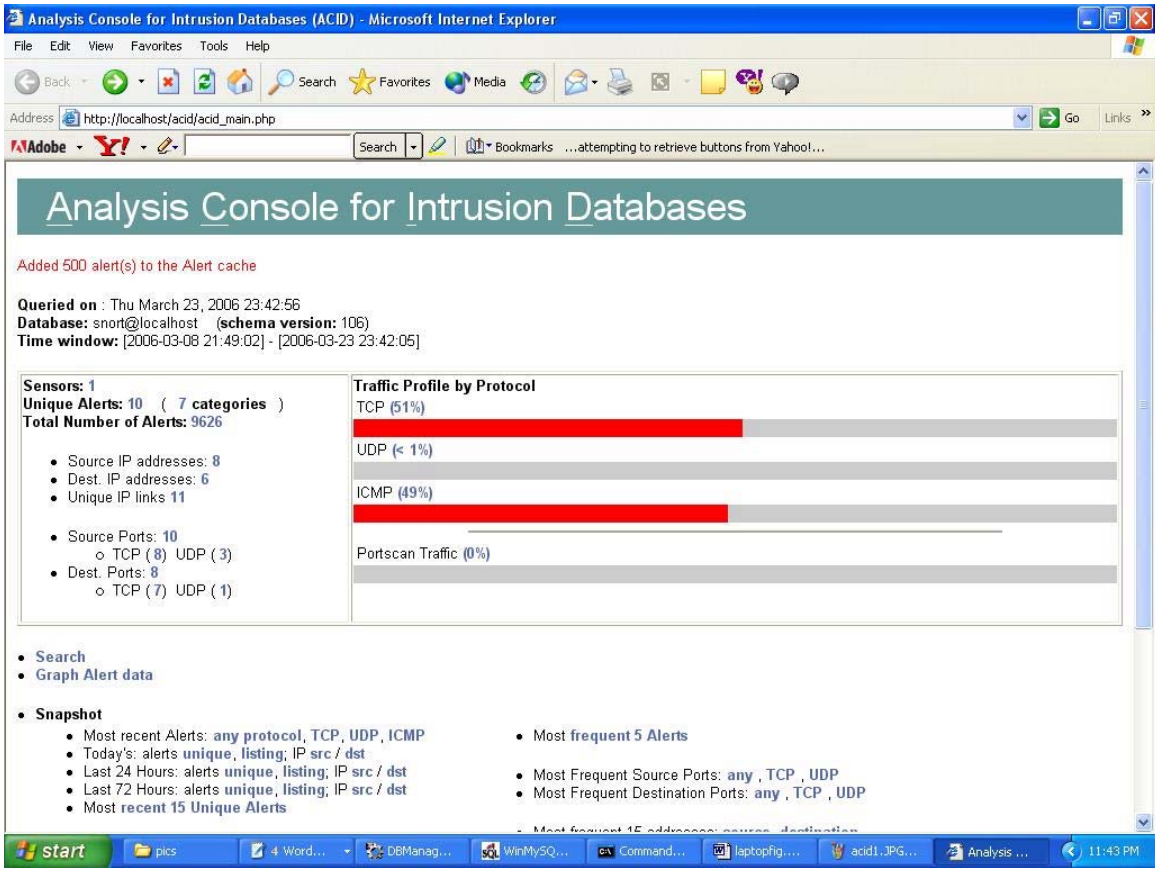


Command Prompt

```
Breakdown by protocol:
    TCP: 1000       (99.701%)
    UDP: 3          (0.299%)
   ICMP: 0          (0.000%)
    ARP: 0          (0.000%)
  EAPOL: 0          (0.000%)
   IPv6: 0          (0.000%)
ETHLOOP: 0          (0.000%)
    IPX: 0          (0.000%)
   FRAG: 0          (0.000%)
  OTHER: 0          (0.000%)
DISCARD: 0          (0.000%)
================================================================================
Action Stats:
ALERTS: 500
LOGGED: 500
PASSED: 0
================================================================================
TCP Stream Reassembly Stats:
    TCP Packets Used: 1000       (99.701%)
    Stream Trackers: 500
    Stream flushes: 0
    Segments used: 0
    Stream4 Memory Faults: 0
================================================================================
```

Step 5: ACID viewer:

- Open the browser and type http://localhost/acid/index.html
- It will take to the main page of ACID. There it will show that it has added all the alerts in the cache.



Analysis Console for Intrusion Databases (ACID) - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Media
Address
Go
Links
Adobe
Search
Bookmarks
…attempting to retrieve buttons from Yahoo!…
start
pics
4 Word…
DBManag…
WinMySQ…
Command…
laptopfig.…
acid1.JPG…
Analysis …
11:43 PM

http://localhost/acid/acid_main.php

Analysis Console for Intrusion Databases

Added 500 alert(s) to the Alert cache

Queried on : Thu March 23, 2006 23:42:56
Database: snort@localhost (**schema version:** 106)
Time window: [2006-03-08 21:49:02] - [2006-03-23 23:42:05]

Sensors: 1
Unique Alerts: 10 (7 **categories**)
Total Number of Alerts: 9626

- Source IP addresses: 8
- Dest. IP addresses: 6
- Unique IP links 11

- Source Ports: 10
  - TCP (8) UDP (3)
- Dest. Ports: 8
  - TCP (7) UDP (1)

Traffic Profile by Protocol

TCP (51%)

UDP (< 1%)

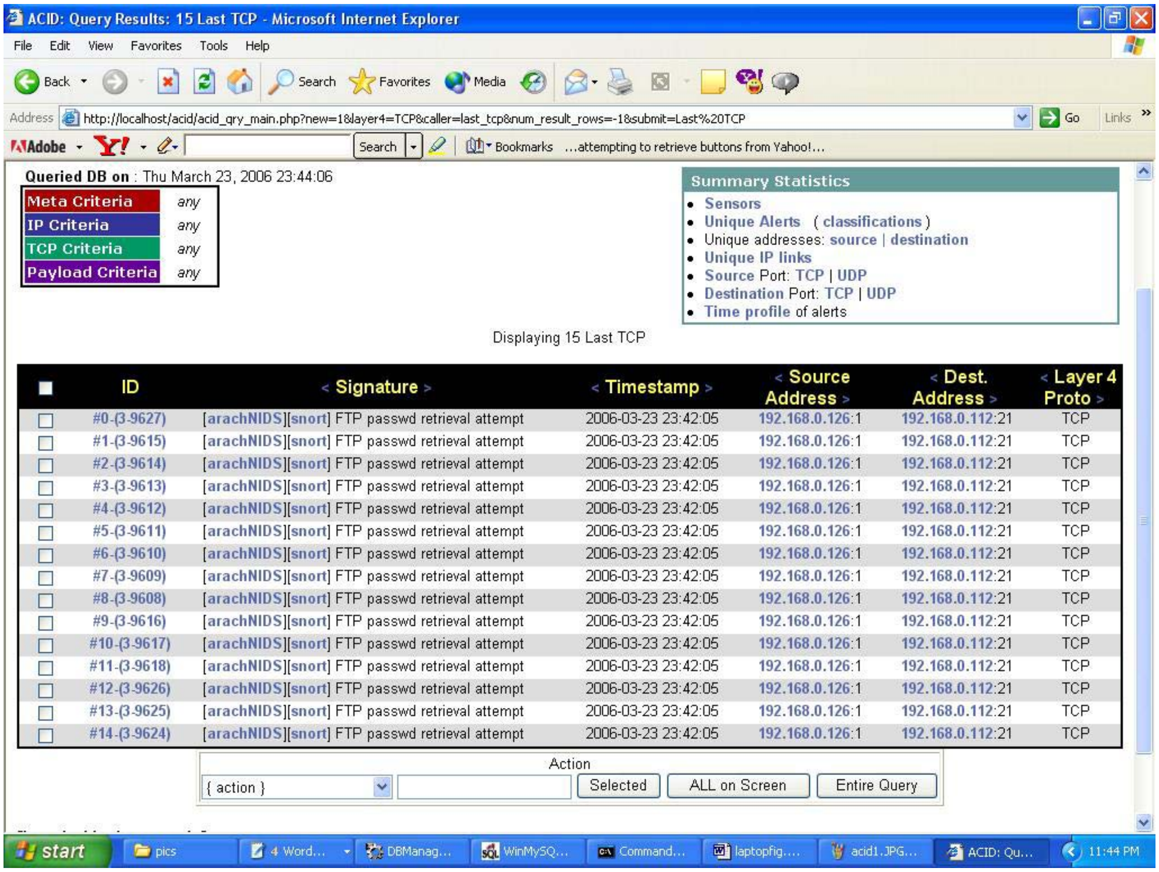
ICMP (49%)

Portscan Traffic (0%)

- Search
- Graph Alert data

- **Snapshot**
  - Most recent Alerts: any protocol, TCP, UDP, ICMP
  - Today's: alerts unique, listing; IP src / dst
  - Last 24 Hours: alerts unique, listing; IP src / dst
  - Last 72 Hours: alerts unique, listing; IP src / dst
  - Most recent 15 Unique Alerts
  - Most frequent 5 Alerts
  - Most Frequent Source Ports: any , TCP , UDP
  - Most Frequent Destination Ports: any , TCP , UDP

- View snapshot of alerts generated by ACID.


File Edit View Favorites Tools Help
Back Search Favorites Media
Go Links
Adobe Search Bookmarks ...attempting to retrieve buttons from Yahoo!...
start pics 4 Word... DBManag... WinMySQ... Command... laptopfig.... acid1.JPG... ACID: Qu... 11:44 PM

ACID: Query Results: 15 Last TCP - Microsoft Internet Explorer

Address: http://localhost/acid/acid_qry_main.php?new=1&layer4=TCP&caller=last_tcp&num_result_rows=-1&submit=Last%20TCP

Queried DB on : Thu March 23, 2006 23:44:06

Meta Criteria	any
IP Criteria	any
TCP Criteria	any
Payload Criteria	any

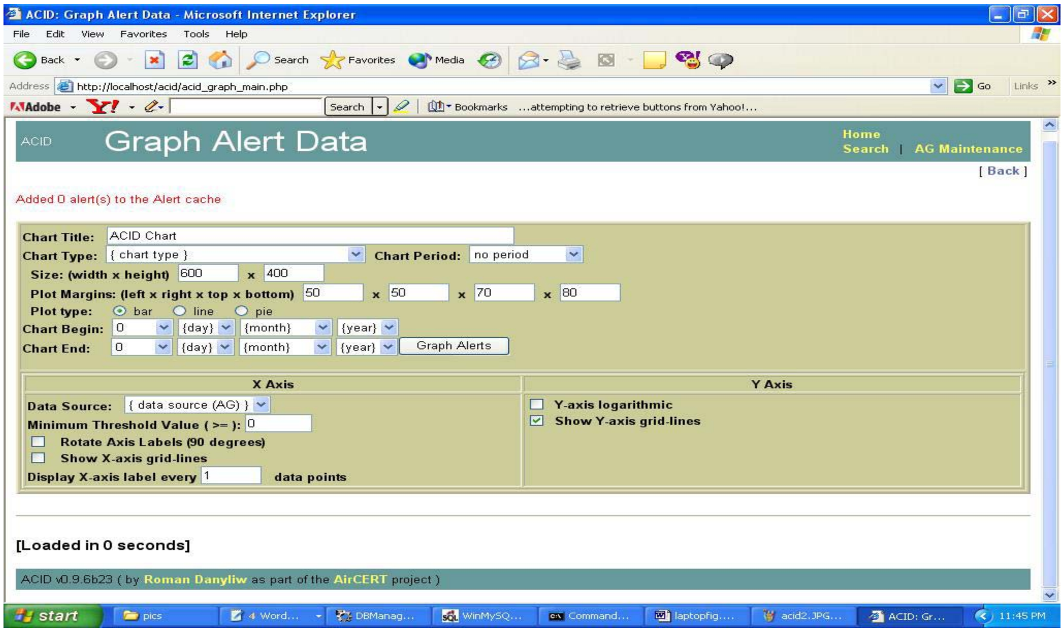
Summary Statistics
- Sensors
- Unique Alerts (classifications)
- Unique addresses: source | destination
- Unique IP links
- Source Port: TCP | UDP
- Destination Port: TCP | UDP
- Time profile of alerts

Displaying 15 Last TCP

□	ID	< Signature >	< Timestamp >	< Source Address >	< Dest. Address >	< Layer 4 Proto >
□	#0-(3-9627)	[arachNIDS][snort] FTP passwd retrieval attempt	2006-03-23 23:42:05	192.168.0.126:1	192.168.0.112:21	TCP
□	#1-(3-9615)	[arachNIDS][snort] FTP passwd retrieval attempt	2006-03-23 23:42:05	192.168.0.126:1	192.168.0.112:21	TCP
□	#2-(3-9614)	[arachNIDS][snort] FTP passwd retrieval attempt	2006-03-23 23:42:05	192.168.0.126:1	192.168.0.112:21	TCP
□	#3-(3-9613)	[arachNIDS][snort] FTP passwd retrieval attempt	2006-03-23 23:42:05	192.168.0.126:1	192.168.0.112:21	TCP
□	#4-(3-9612)	[arachNIDS][snort] FTP passwd retrieval attempt	2006-03-23 23:42:05	192.168.0.126:1	192.168.0.112:21	TCP
□	#5-(3-9611)	[arachNIDS][snort] FTP passwd retrieval attempt	2006-03-23 23:42:05	192.168.0.126:1	192.168.0.112:21	TCP
□	#6-(3-9610)	[arachNIDS][snort] FTP passwd retrieval attempt	2006-03-23 23:42:05	192.168.0.126:1	192.168.0.112:21	TCP
□	#7-(3-9609)	[arachNIDS][snort] FTP passwd retrieval attempt	2006-03-23 23:42:05	192.168.0.126:1	192.168.0.112:21	TCP
□	#8-(3-9608)	[arachNIDS][snort] FTP passwd retrieval attempt	2006-03-23 23:42:05	192.168.0.126:1	192.168.0.112:21	TCP
□	#9-(3-9616)	[arachNIDS][snort] FTP passwd retrieval attempt	2006-03-23 23:42:05	192.168.0.126:1	192.168.0.112:21	TCP
□	#10-(3-9617)	[arachNIDS][snort] FTP passwd retrieval attempt	2006-03-23 23:42:05	192.168.0.126:1	192.168.0.112:21	TCP
□	#11-(3-9618)	[arachNIDS][snort] FTP passwd retrieval attempt	2006-03-23 23:42:05	192.168.0.126:1	192.168.0.112:21	TCP
□	#12-(3-9626)	[arachNIDS][snort] FTP passwd retrieval attempt	2006-03-23 23:42:05	192.168.0.126:1	192.168.0.112:21	TCP
□	#13-(3-9625)	[arachNIDS][snort] FTP passwd retrieval attempt	2006-03-23 23:42:05	192.168.0.126:1	192.168.0.112:21	TCP
□	#14-(3-9624)	[arachNIDS][snort] FTP passwd retrieval attempt	2006-03-23 23:42:05	192.168.0.126:1	192.168.0.112:21	TCP

Action
{ action } | Selected | ALL on Screen | Entire Query

- Click on Graph Alert Data. You can choose your options on how to view the graph. We have three options line, bar, pie.


File Edit View Favorites Tools Help
Back Search Favorites Media
Go Links
Adobe Search Bookmarks ...attempting to retrieve buttons from Yahoo!...
Home
Search | AG Maintenance
[Back]
Graph Alerts
start pics 4 Word... DBManag... WinMySQ... Command... laptopfig.... acid2.JPG... ACID: Gr... 11:45 PM

ACID: Graph Alert Data - Microsoft Internet Explorer

Address: http://localhost/acid/acid_graph_main.php

ACID Graph Alert Data

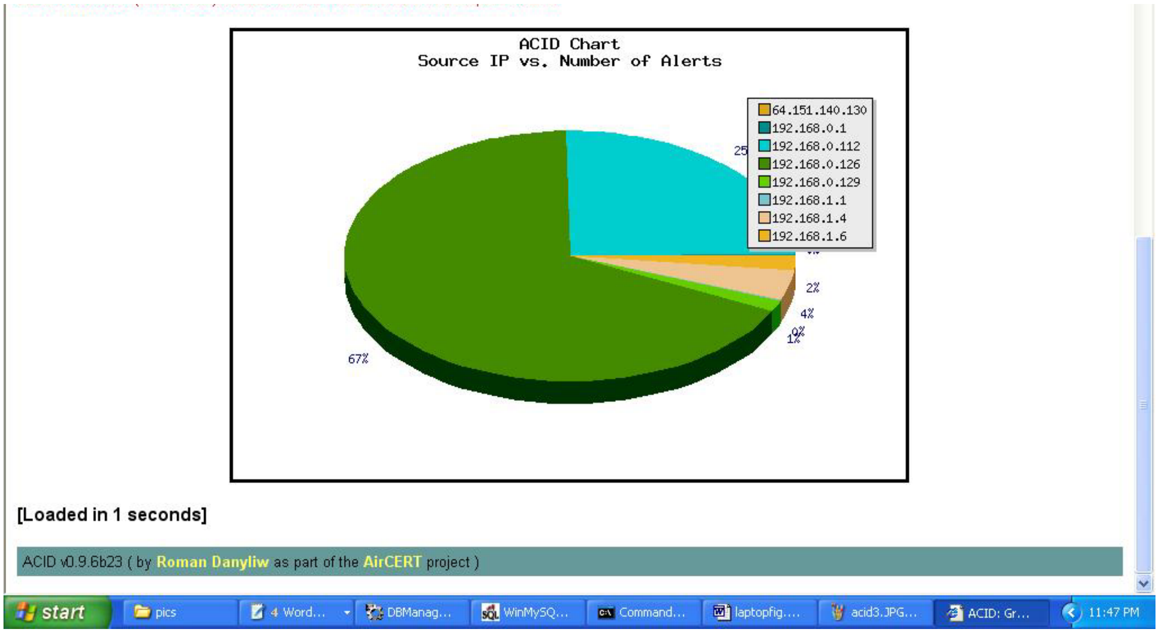
Added 0 alert(s) to the Alert cache

Chart Title: ACID Chart
Chart Type: { chart type } **Chart Period:** no period
Size: (width x height) 600 x 400
Plot Margins: (left x right x top x bottom) 50 x 50 x 70 x 80
Plot type: ● bar ○ line ○ pie
Chart Begin: 0 {day} {month} {year}
Chart End: 0 {day} {month} {year}

X Axis	Y Axis
Data Source: { data source (AG) } **Minimum Threshold Value (>=):** 0 □ **Rotate Axis Labels (90 degrees)** □ **Show X-axis grid-lines** **Display X-axis label every** 1 **data points**	□ **Y-axis logarithmic** ☑ **Show Y-axis grid-lines**

[Loaded in 0 seconds]

ACID v0.9.6b23 (by Roman Danyliw as part of the AirCERT project)

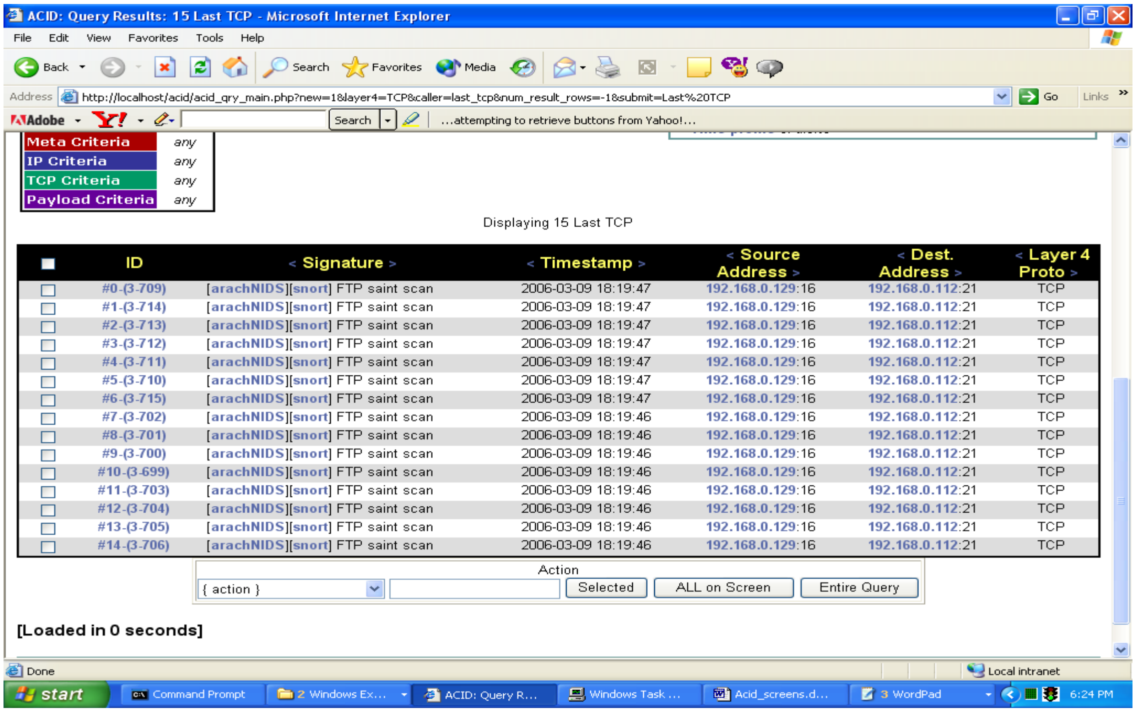


[Loaded in 1 seconds]

ACID v0.9.6b23 (by Roman Danyliw as part of the AirCERT project)

Below is shown another snapshot for sid: 358:

Sid: 358 FTP saint attack



http://localhost/acid/acid_qry_main.php?new=1&layer4=TCP&caller=last_tcp&num_result_rows=-1&submit=Last%20TCP

Meta Criteria	any
IP Criteria	any
TCP Criteria	any
Payload Criteria	any

Displaying 15 Last TCP

□	ID	< Signature >	< Timestamp >	< Source Address >	< Dest. Address >	< Layer 4 Proto >
□	#0-(3-709)	[arachNIDS][snort] FTP saint scan	2006-03-09 18:19:47	192.168.0.129:16	192.168.0.112:21	TCP
□	#1-(3-714)	[arachNIDS][snort] FTP saint scan	2006-03-09 18:19:47	192.168.0.129:16	192.168.0.112:21	TCP
□	#2-(3-713)	[arachNIDS][snort] FTP saint scan	2006-03-09 18:19:47	192.168.0.129:16	192.168.0.112:21	TCP
□	#3-(3-712)	[arachNIDS][snort] FTP saint scan	2006-03-09 18:19:47	192.168.0.129:16	192.168.0.112:21	TCP
□	#4-(3-711)	[arachNIDS][snort] FTP saint scan	2006-03-09 18:19:47	192.168.0.129:16	192.168.0.112:21	TCP
□	#5-(3-710)	[arachNIDS][snort] FTP saint scan	2006-03-09 18:19:47	192.168.0.129:16	192.168.0.112:21	TCP
□	#6-(3-715)	[arachNIDS][snort] FTP saint scan	2006-03-09 18:19:47	192.168.0.129:16	192.168.0.112:21	TCP
□	#7-(3-702)	[arachNIDS][snort] FTP saint scan	2006-03-09 18:19:46	192.168.0.129:16	192.168.0.112:21	TCP
□	#8-(3-701)	[arachNIDS][snort] FTP saint scan	2006-03-09 18:19:46	192.168.0.129:16	192.168.0.112:21	TCP
□	#9-(3-700)	[arachNIDS][snort] FTP saint scan	2006-03-09 18:19:46	192.168.0.129:16	192.168.0.112:21	TCP
□	#10-(3-699)	[arachNIDS][snort] FTP saint scan	2006-03-09 18:19:46	192.168.0.129:16	192.168.0.112:21	TCP
□	#11-(3-703)	[arachNIDS][snort] FTP saint scan	2006-03-09 18:19:46	192.168.0.129:16	192.168.0.112:21	TCP
□	#12-(3-704)	[arachNIDS][snort] FTP saint scan	2006-03-09 18:19:46	192.168.0.129:16	192.168.0.112:21	TCP
□	#13-(3-705)	[arachNIDS][snort] FTP saint scan	2006-03-09 18:19:46	192.168.0.129:16	192.168.0.112:21	TCP
□	#14-(3-706)	[arachNIDS][snort] FTP saint scan	2006-03-09 18:19:46	192.168.0.129:16	192.168.0.112:21	TCP

Action

{ action } | Selected | ALL on Screen | Entire Query

[Loaded in 0 seconds]

Conclusion:

In this document we have tried to sketch a details view on how to implement SNORT with the add-on ACID. Hopefully this will help others in doing same kind of work in future.

Implementing the whole project was time consuming as we had to encounter various types of problems at different levels and we had to spend much time on debugging the problems. However it was very interesting and we could learna lot from this project. We have successfully checked 10 signatures (sid # 270, 473, 359, 655, 478, 1458, 1071, 356, 358 and 1755) on our implementation. Since creating packets with each sid each time requires same process, we have included only two samples in this paper. However if you require any further information please do not hesitate to contact us anytime.

References:

- http://www.securitydocs.com/library/1737
- http://www.andrew.cmu.edu/user/rdanyliw/snort/acid_config.html
- http://www.idevelopment.info/data/MySQL/DBA_tips/Installing/WIN417_4.shtml
- http://www.andrew.cmu.edu/user/rdanyliw/snort/snortdb/snortdb_install.html
- http://www.iis-resources.com/modules/AMS/article.php?storyid=273