Snort on Window Server 2003

Sunil Vakharia
Sunil_Vakharia → *hotmail.com*

CONTENTS

Introduction

There is a lot documentation on Snort on Linux and considerable on Snort for Windows too. But most of the documentation deals with older versions. So I thought let me create one for the latest version of Snort environment. The setup that I am talking about is running **Snort 2.3.3 on Windows Server 2003 with PHP5 and SQL 2000 SP4**. All other components are also the latest available for public use.

Copyright and Disclaimer

Environment Assumptions

Although these assumptions are *not* pre-requisites, for successful setup, they are recommended.

Hard-disk partitioning

The system partition should contain minimum applications and hardly any data.
In our case, the following was the partition summary.

C:	System Partition	4 GB
D:	Swap Partition	1.5 GB ([2 x 512 MB RAM] + some free space)
E:	Data and Applications Includes the following Applications: • Snort • ADODB • PHP • PHPlot • JpGraph • SQL Server • BASE Data Website Root (WWW) SQL Database	35 GB

SQL User accounts

Note: If you have an Active Directory environment, create a Domain User account, else create a Local User account.
Create a user account *sqlserv* for running SQL 2000 service, which you would be installing shortly. This user account should be an ordinary user (not belonging to any other group except Users/ Domain Users)

Folder creation

Create the following folders in E:
DATABASE
MSSQL
PHP5
Snort
WWW
WWW→base
WWW→adodb
WWW→phplot
WWW→base

Final Layout
The final folder structure would be as shown below

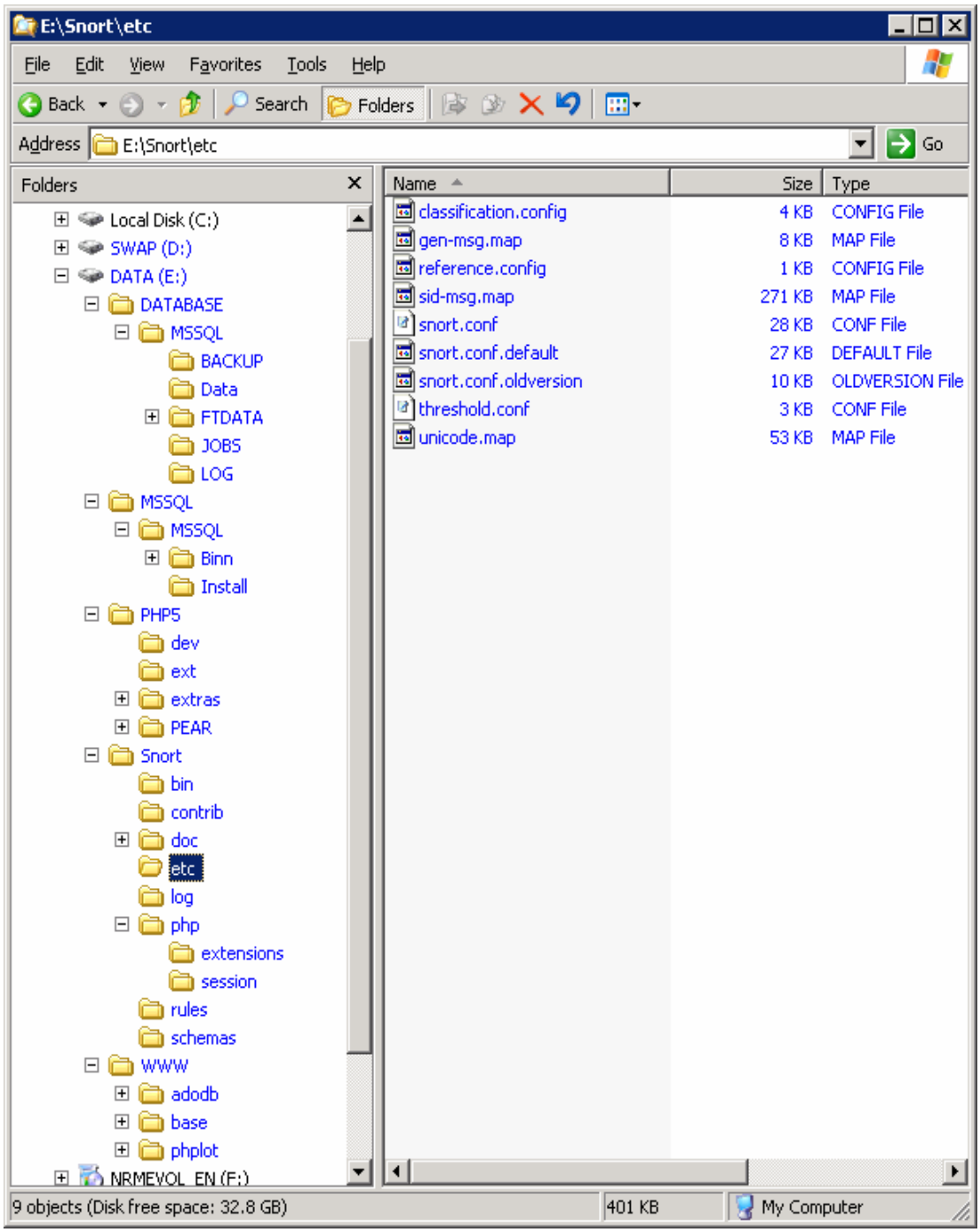

Figure 1: Final Layout

Components

Following components are involved:

Component	What it does?	Version Used	Where to get?	Notes
WinPcap	Packet Capture Library	3.0	http://www.winpcap.org/	3.1 beta4 does not work with Snort 2.3.3 Build 14
Snort	Actual IDS	2.3.3 Build 14	http://www.snort.org	Latest available as of creation of this document
IIS 6	Webserver	6	Windows 2003 CD	None
SQL Server	Database	2000 SP4	http://www.microsoft.com/sql	None
PHP	Scripting language	5.0.4	http://www.php.net	Don't use the installer version!
ADODB	Database Abstraction Library	4.63	http://adodb.sourceforge.net/	
PHPlot	A graph library, written in PHP, for dynamic charts	5.0rc2	http://sourceforge.net/projects/phplot/	
JpGraph	An Object-Oriented Graph creating library	2.0beta	http://www.aditus.nu/jpgraph/jpdownload.php	1.x stable doesn't work with PHP5
BASE	provides a web front-end to query and analyze the alerts	1.1.2	http://secureideas.sourceforge.net/	ACID doesn't seem to work with the other product versions being used.

Installation

WinPcap

Follow onscreen instructions to install Winpcap 3.0 (Winpcap 3.1 beta4 does not work with Snort 2.3.3 Build 14)

Snort

1. Follow onscreen instructions to install Snort 2.3.3 Build 14
2. Installation Directory: E:\Snort

Checkpoint

From the command prompt, type the following:

```
cd E:\Snort\bin
snort.exe -W
```

This will give you a list of interfaces. If this doesn't work, then WinPcap is not installed correctly.

```
snort -v -i1
```

This will get snort running in packet dump mode (-v is for verbose and –i is for selecting the interface)

Next you need to edit the *snort.conf* file to suit your requirements
We changed the following settings:
var HOME_NET 10.10.1.0/24
var DNS_SERVERS 10.10.1.XXX
var RULE_PATH E:\snort\rules
output database: log, mssql, dbname=IDSDB user=snortuser password=xxxxxx
include e:\snort\etc\classification.config
include e:\snort\etc\reference.config

IIS 6

Note: To install Internet Information Services 6, you would need the Windows Server 2003 CD.

1. Follow these steps to install IIS 6
   - Go to Control Panel→ Add/Remove Programs → Check Application Server. Click on Details

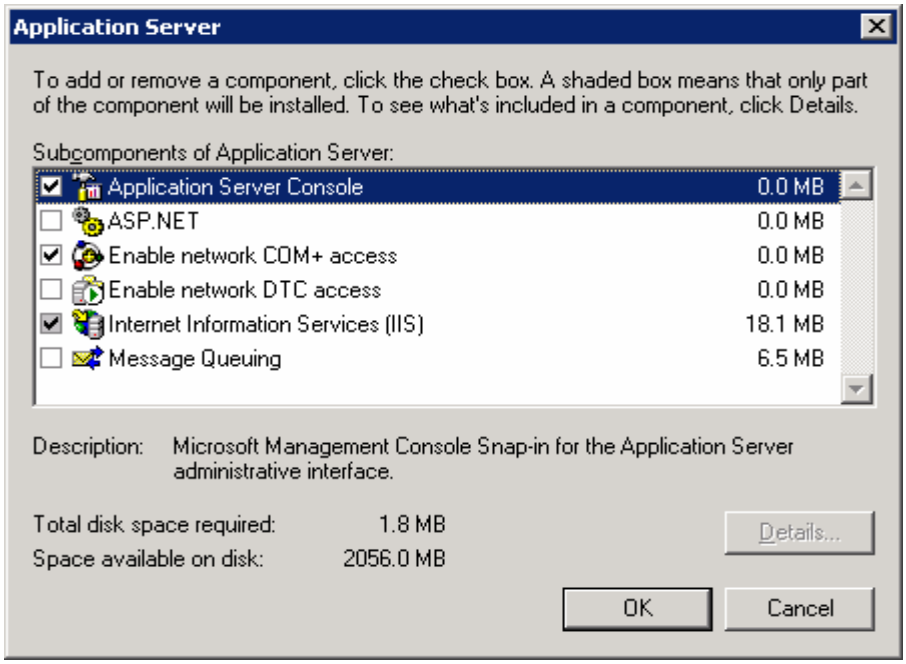

Figure 2: IIS components

- Ensure that the following are checked:
    1. Application Server Console
    2. Enable network COM+ access
    3. Internet Information Services (IIS)
       Select the following subcomponents of IIS
        a. Common Files
        b. IIS Manager
        c. WWW Service

Checkpoint

Launch your browser and point it to http://localhost. If you get an "Under construction" page, then your web server is working fine.

The Default Website root would be C:\INETPUB\WWWROOT after installation.
Use IIS Manager snap-in to change that to E:\WWW (Created above)

Copy the iisstart.htm and pagerror.gif files to E:\WWW. Restart your WWW service.
Launch your browser once again and point it to http://localhost. If you get an "Under construction" page, then your web server is working fine.

SQL Server

1. Begin installation of SQL 2000. During installation, there will be a series of prompt and parameters. The following are the changes during the course of installation.

    - Program directory= E:\MSSQL
    - Data file directory= E:\DATABASE
    - During the component installation step, uncheck the following
        - Developer Tools
        - Books online
        - Server component
            - Upgrade Tools
            - Replication Support
            - Debug symbols

    - When prompted to choose an account to run the SQL service, change from the default LocalSystem to the domain/local user *sqlserv* as the service account.

2. Once installation is through, install Service Pack 4 (or atleast Service Pack 3a)

3. After Service Pack is installed, SQL would operate in Windows Authentication. But in order for Snort to work with SQL, you would need to change this to Mixed mode authentication.
   To do so, from Enterprise Manager, expand the group containing your SQL server and right click on it and select Properties. Change the Authentication to *SQL Server and Windows*, Audit level to *All*.

   Note: The Startup service account should already be the *sqlserv* account

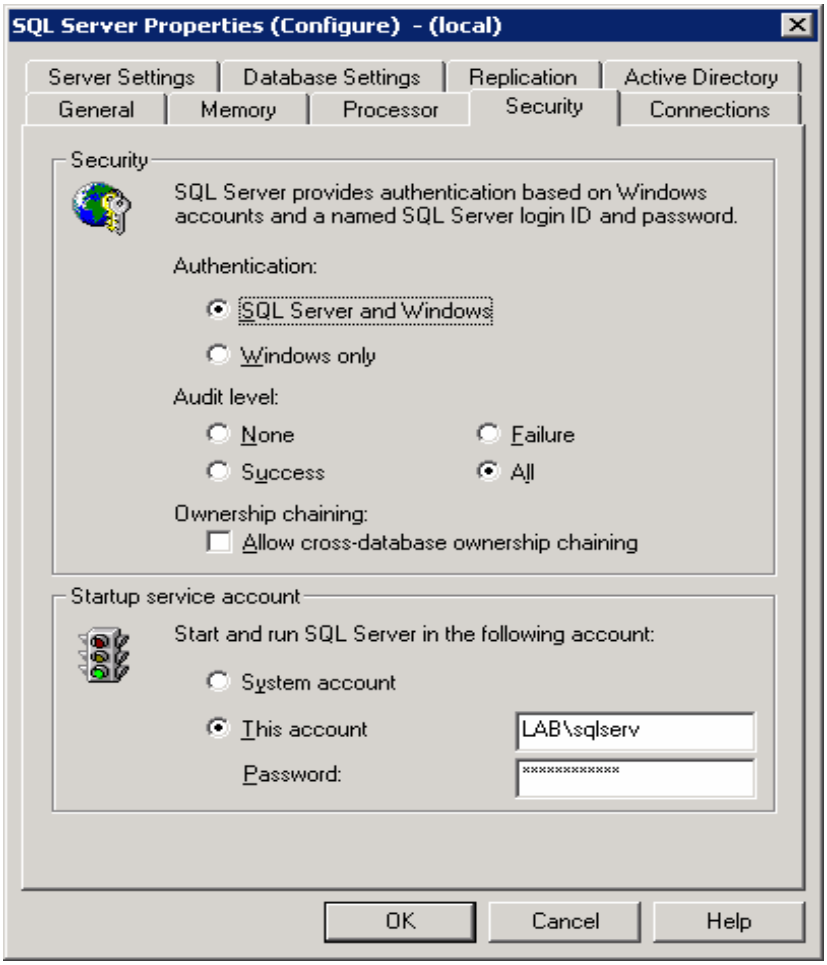

Figure 3: SQL server properties

4. Next, using Enterprise Manager, do the following:
    a. Create a new database: IDSDB. Ensure that the Datafile and Log file are in E:\Database directory.
    b. Create a login within SQL and call it *snortuser*. Snort will use this login to connect to SQL and insert data.
    c. Give access to IDSDB database only.

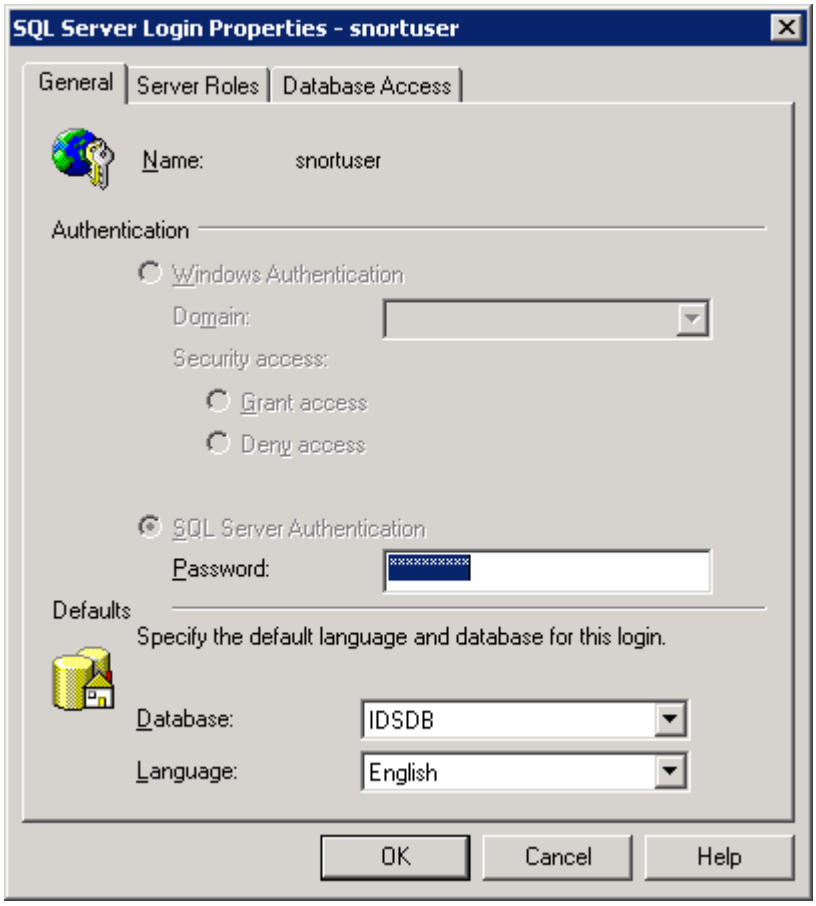

Figure 4: snortuser properties

Type of role:
public
INSERT, SELECT, UPDATE, DELETE

5. Using SQL Query Analyzer, copy-paste the content in the script create_mssql located in E:\Snort\schemas. Make sure that in Query Analyzer, the database selected is IDSDB. After pasting the query, execute it. The output should say: 1 row affected.

Checkpoint

You can check the database connectivity for the user *snortuser*.
From command prompt
`Osql -localhost -U snortuser -d IDSDB`
Enter the password at the prompt
Type a simple query such as **`select * from data; go`**

PHP

1. Download and extract the PHP Windows zip package to E:\PHP5 (See Figure 1 above)
   Create E:\Snort\php\Session directory
   Assign permissions. Create E:\Snort\php\extensions directory <-NOT NEEDED?->
2. Copy **E:\PHP5\php.ini-recommended** to **%SystemRoot%\php.ini**. The system-root would typically be C:\Windows or C:\WinNT
3. Copy php5ts.dll to %SystemRoot%\system32
4. Edit php.ini now and make the following changes.
   - doc_root ="e:\www"
   - extension_dir = "E:\PHP5\ext"
   - session.save_path = "E:\Snort\php\session"
   - error_reporting = E_ALL
   - Uncomment php_mssql.dll and php_gd2.dll
     - ;extension=php_gd2.dll → extension=php_gd2.dll
     - ;extension=php_mssql.dll → extension=php_mssql.dll

Serving PHP pages with IIS

Using IIS Manager Snap-in, add the extensions .php and .php5 and map them to E:\PHP5\php5isapi.dll

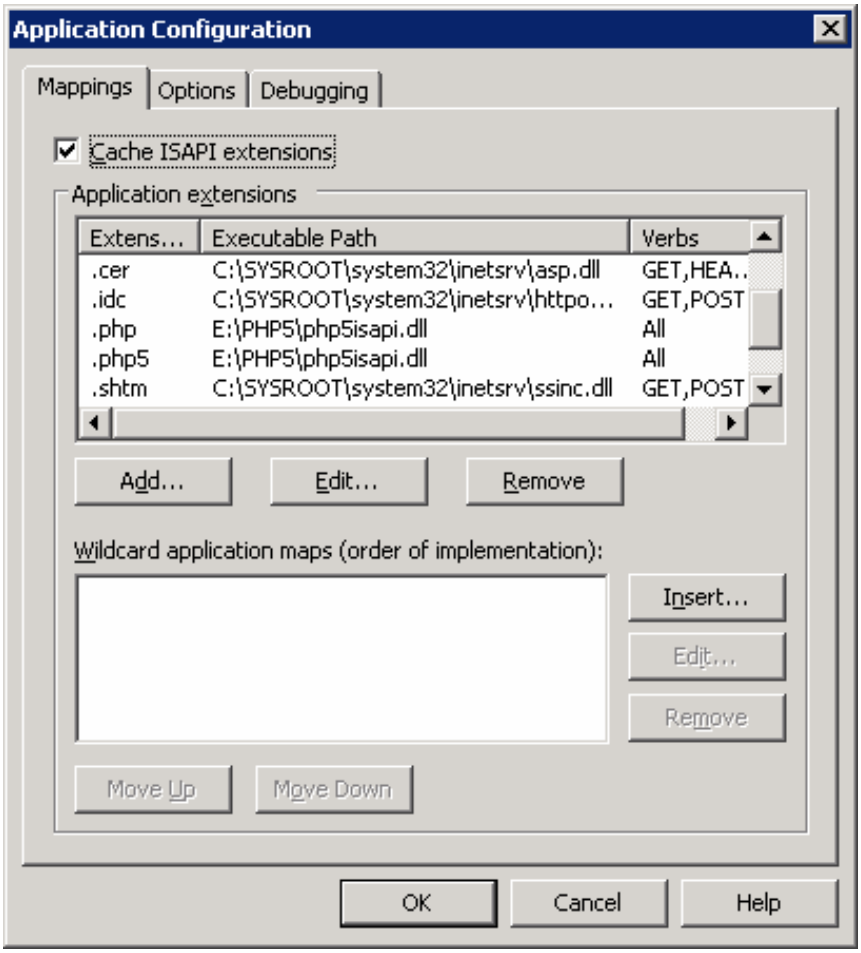

Figure 5: PHP mappings in IIS

Checkpoint

1. Create a file in E:\WWW\test.php
2. Copy paste the following content via Notepad
   Today is <? print strftime("%m/%d/%Y"); ?>
3. Save this file and use your browser to navigate it (http://localhost/test.php). You should be able to see a message: Today is XX/XX/2005

Congratulations!! Your IIS can now server PHP pages.

ADODB

1. Extract ADODB 4.63 to E:\WWW\adodb
2. Edit Adodb.inc.php
   - Change the following line
     if (!defined('ADODB_DIR')) define('ADODB_DIR',dirname(__FILE__));
     TO
     if (!defined('ADODB_DIR')) define('ADODB_DIR','E:\WWW\adodb');

Checkpoint

1. Edit the test.php created above and replace the contents with the following. Replace 'xxx' with 'your_password'

```
Today is <? print strftime("%m/%d/%Y"); ?>
<?php
include('adodb/adodb.inc.php');
$conn = &ADONewConnection("mssql");  // create a connection
$conn->Connect('localhost', 'snortuser', 'xxx', 'IDSDB') or die('Fail');

$conn->debug =1;
$query = 'select * from icmphdr';
$conn->SetFetchMode(ADODB_FETCH_ASSOC);
$rs = $conn->Execute($query);
echo "<pre>";
while( !$rs->EOF ) {
      $output[] = $rs->fields;
      var_dump($rs->fields);
      $rs->MoveNext();
      print "<p>";
}
die();
```

2. Save it and browse it via the browser.
3. You should be able to view the contents of the table icmphdr

PHPlot

1. Extract PHPlot 5.0 RC2 to E:\WWW\phplot
   That's it! Test the examples within this directory via your browser.

JpGraph

1. Download JpGraph 2.0(beta) for PHP5
2. Extract to E:\WWW\JpGraph
3. Copy all files from *src* directory to E:\WWW\phplot
4. Delete E:\WWW\JpGraph

BASE

1. Download and extract the BASE zip file to E:\WWW\base folder
2. Copy the *base_conf.php.dist* and paste it in the same directory. Rename the new file as *base_conf.php*
3. Edit the *base_conf.php* file.

$BASE_urlpath = "";	→	$BASE_urlpath = ".";
$DBlib_path = "";	→	$DBlib_path = "E:\www\adodb";
$DBtype = "mysql";	→	$DBtype = "mssql";
$alert_dbname = "snort_log";	→	$alert_dbname = "IDSDB";
$alert_host = "localhost";	→	(No change)
$alert_port = "";	→	(No change)
$alert_user = "root";	→	$alert_user = "snortuser";
$alert_password = "mypassword";	→	$alert_password = "xxx";

4. Make changes to Archive database settings if required.

Final Checkpoint

1. Using your browser go to http://localhost/base/base_main.php
   An error stating 'the underlying database snort@local appears to be invalid' will appear the first time BASE is run.
2. Select the link 'Setup page' when this error appears.
3. Then select 'Create BASE AG' button to complete the BASE Alert Group configuration. A message stating 'The underlying Alert DB is configured for usage with BASE' will appear, and the database is completely configured.

4. Return to a browser and retype: http://localhost/base/base_main.php

5. Note: It may take a little while to start seeing alerts just let it go, and BASE will auto refresh.

Hardening

Some security aspects have already been covered in the process mentioned above. However there are still aspects that need to be considered.
This section will be updated in the next version of the document.

Customization

Once the IDS is in place you would notice a lot of false-positives. Eliminating these would generally involve a lot of understanding of the network traffic that is flowing and the applications involved. Although this is an environment specific configuration, certain base-line configurations can still be recommended.
This section will be updated in the next version of the document.

Updates

Snort signatures need to be updated regularly to detect newer threat vectors. Oikmaster can be used to simplify this process (This will be covered in the next version of the document)

References

http://www.snort.org
http://www.winpcap.org/
http://www.microsoft.com/sql
http://www.php.net
http://adodb.sourceforge.net
http://sourceforge.net/projects/phplot
http://www.aditus.nu/jpgraph/jpdownload.php
http://secureideas.sourceforge.net/

To do list

1. Details on security/ hardening aspects of the following:
    a. Webserver
    b. Database permissions for snortuser etc.
    c. NTFS permissions
2. Removal of unnecessary files such as examples, documentation files etc.
3. Considerations for stealth mode deployment
4. Considerations for deployment in a switched environment
5. Rule customizations
6. Signature update details
7. Oinkmaster to be included
8. Database/ Log related details
    a. Backup procedures
    b. Offline Log analysis using tools
    c. Event co-relation in multi-sensor environments.
9. References to be added

Feedback

Constructive feedback is most welcome. Redirect your comments to sunil_vakharia AT hotmail.com