

# CS470 Computer Security Intrusion Detection Project Due Date:

The objective of this project is to familiarize you with Intrusion Detection Systems (IDS), IDS Tools, IDS signatures and rules, the configuration and implementation of common open-source IDS tools, and the analysis and identification of possible system infections, compromises and other problems that will trigger an incident response process.

You are required to install and put into production an IDS on a Windows 2000 platform. The IDS will be configured to use the following open-source software: Snort, PHP, MySQL, and WinPcap. In addition, you need to install a Graphical User Interface (GUI) to facilitate the management of the IDS:

- **(required)** IDS Policy Manager and Honeynet Security Console ([www.activeworx.org](http://www.activeworx.org))
- *(optional)* ACID (Analysis Console for Intrusion Database) (<http://www.andrew.cmu.edu/user/rdanyliw/snort/snortacid.html>)

All the necessary open-source software/programs that you need for this project are saved in c:\IDS. To get you started, I have summarized the procedures below.

1. Install Internet Information Service (IIS) (*already done for you!*)
2. Install PHP
  - a. Use the Windows PHP installer: **install-php4.3.10**
  - b. Default installation will be in **c:\php4**. Add this and **c:\php4\php** to your default **PATH**.
  - c. Edit the **php.ini** file found in c:\WINNT
    - i. Set the document root and cgi.force\_redirect:  
**doc\_root = "c:\Inetpub\wwwroot"**  
**cgi.force\_redirect=0**
    - ii. Enable the extension(s) in php.ini you want to use by uncommenting the extension=php\_\*.dll lines in php.ini. This is done by deleting the leading ; from the extension you want to load. For the IDS, we need the following:  
  
**extension=php\_adodb.dll**  
**extension=php\_gd2.dll**
  - d. Start the Microsoft Management Console (**Start→Programs→Administrative Tools→Internet Service Manager**). Click on 'AH261-xx' (xx is the number of your station) and right click on 'Default Web Site' and select 'Properties'.

Under 'Home Directory', 'Virtual Directory', or 'Directory', click on the 'Configuration' button, and then enter the 'Mappings' tab. Click 'Add' and in the 'Executable' box type: **C:\php4\php\php.exe**. In the 'Extension' box, type the file name extension (e.g. .php) you want associated with PHP scripts. Check the 'Script engine' checkbox. You may also like to check the 'check that file exists' box - for a small performance penalty.

e. Check your PHP installation by using the following URL address on your web browser: <http://localhost/phpadmin>

3. Install MySQL

- a. Extract the setup file from mysql-5.0.18-win32.zip. Run the Windows installer (setup file). Select 'Complete' install. Skip the MySQL.com sign-up. Configure the MySQL server and choose 'Server Machine' for the MySQL Server Instance Configuration. Use 'sn0rtDB2006' as the root password.
- b. Install the MySQL Administrator program.

4. Install WinPcap. Use the WinPcap Windows installer.

5. Install Snort (A network intrusion detection system).

- a. Run the Snort installer. Accept all of the default settings.
- b. Test snort, using a command console, by listing all interfaces.  
**C:\snort\bin\> snort -W**
- c. Edit snort's configuration file (snort.conf).

Make snort log to MySQL by uncommenting the following line (change "log" to "alert"):

```
output database: alert, mysql, user=root password=sn0rtDB2006 dbname=snort_db
host=localhost
```

Set the path where the rules are defined. Replace

```
var RULE_PATH ../rules
with
var RULE_PATH c:\Snort\rules
```

6. Create database for snort

- a. Invoke a MySQL command line client. Execute the following commands:

```
mysql> create database snort_db;
mysql> use snort_db;
mysql> source c:/snort/schemas/create_mysql;
mysql> exit;
```

- b. Use the MySQL Administrator to create a user (snortUser) with password 'sn0rtDB2006'. Assign all privileges to snortUser for the schema 'snort\_db'.

7. Install a GUI management console for the IDS. Enough spoon feeding...you are on your own. The source files are:

- a. idspm.v1.8.1 (for IDS Policy Manager )
- b. hsc.v2.6.0.4 (for HoneyNet Security Console)
- c. acid-0.9.6b23.tar.gz (for ACID) (*note: this is optional*)

8. You are required to write Snort rules that will satisfy the following requirements:

- a. Alert and log system reconnaissance activities. (Test this using nmap)
- b. Alert and log attacks on the web server. (Test this using Unicode exploits)
- c. Alert and log ftp, telnet, mysql (database) activities.

9. Write and submit a report on all your findings and analysis.

9. Install ADODB Library. Extract contents of adodb tar file to C:\Inetpub\wwwroot\adodb.
  - a. Edit the adodb.inc.php. Set the ADODB\_Database

10. Install ACID (Analysis Console for Intrusion Database)

- a. Extract contents of ACID tar file to C:\Inetpub\wwwroot\acid.
- b. Edit the acid\_conf.php file using the following values:

```
$DBlib_path      = "C:\Inetpub\wwwroot\adodb";  
$alert_dbname    = "snort_db";  
$alert_host      = "localhost";  
$alert_port      = "3306";  
$alert_user      = "snortUser";  
$alert_password  = "sn0rtDB2006";
```

- c. Start ACID: <http://localhost/acid/index.html>