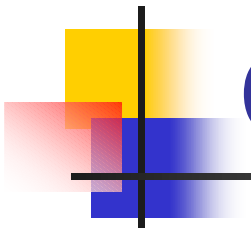
Snort & Windows 2000

A Practical Guide

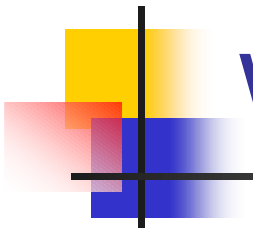
David Elfering

Based on paper by Michael Steele



Objective

- Windows 2000
  - Flexible, enterprise ready
  - Leverage 2000's crypto capabilities
  - Distributed, economical, web based NIDS architecture
  - Web server
    - Either IIS or Apache will work
- Snort
  - Free & open
  - Is this cats & dogs living together?

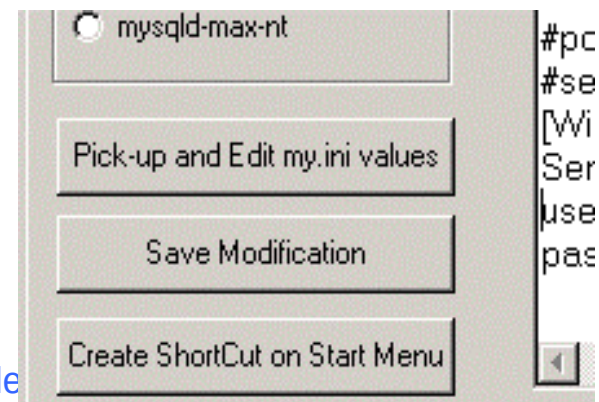


WinPcap

- Download
  - http://netgroup-serv.polito.it/winpcap/install/
- Install
  - Simple “click-n-shoot” operation
  - For problems see WinPcap FAQ

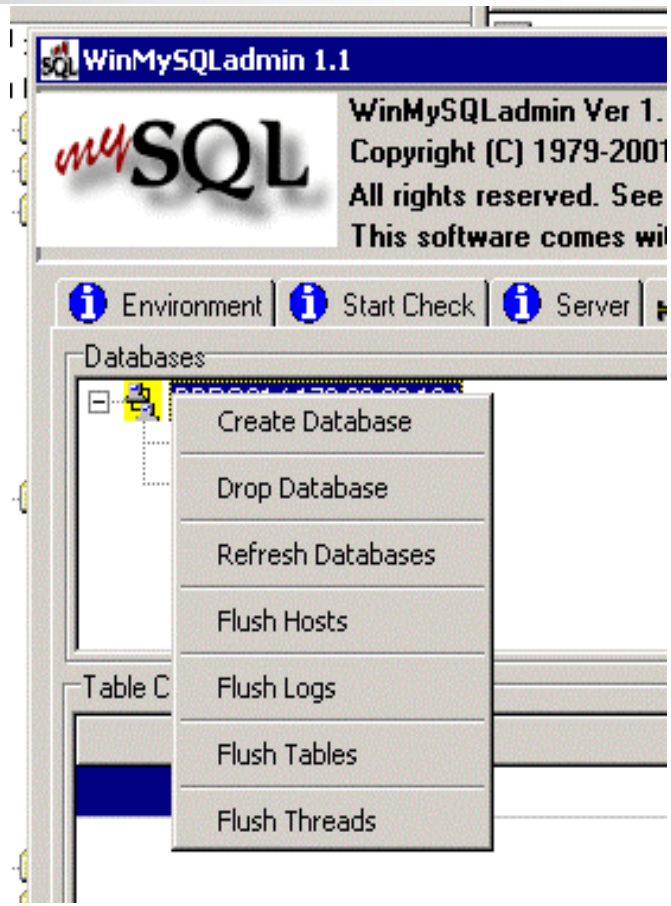
MySQL – Installation

- Download: http://www.mysql.com
- Choose "typical" as installation type
  - Note: Install from control panel on W2K Server
  - Password?
- Open WinMySQLAdmin
- Create "Start Menu" item
  - Located on my.ini Setup



MySQL – Create the Database

- Create & Configure SNORT database
  - Right Click MySQL icon in the system tray (select "show me")
  - Select Database tab and "Create Database" to create "snort" database



MySQL – Setting Permissions

- Execute C:\MySQL\bin\MySQL
  - Type "\u mysql;
  - Type "grant INSERT,SELECT,CREATE,DELETE on snort.* to snort@localhost;"

```
C:\mysql\bin>mysql
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 7 to server version: 3.23.38-nt

Type 'help;' or '\h' for help. Type '\c' to clear the buffer

mysql> \u mysql
Database changed
mysql> grant insert,select,create,delete on snort.* to snort@localhost;
Query OK, 0 rows affected (0.00 sec)
```

  - Now type "\u mysql" then "show tables;"
  - Now try "select * from user;"

Snort

- -Download
  - Snort-win32 MySQL binary
  - Grab “Snortrules.tar.gz”
  - Grab “Snort.conf”
- -Install
  - Create 3 Folders:
  - "C:\Snort\" - "C:\Snort\Bin\" - "C:\Snort\Logs\"
  - Install Snort into "C:\Snort\Bin" folder
    - This is a manual copy – no setup file needed

Snort (2)

- Install the latest FULL set of rules and snort.conf file
- Edit the snort.conf file
  - To reflect your HOME_NET

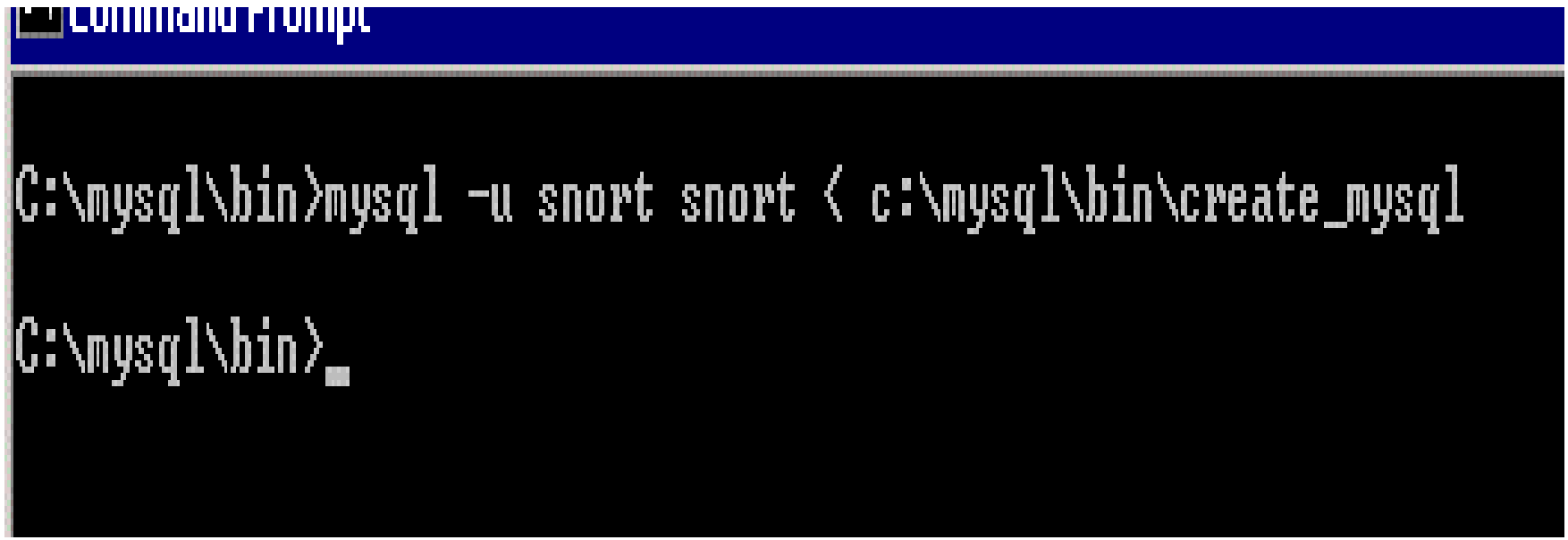
```
#var HOME_NET $eth0_ADDRESS

var HOME_NET 10.1.1.0/24
```

  - Remove # before “output database: log, mysql
- Copy the file called "create_mysql" from the "contrib" folder of Unix tar
  - http://www.snort.org/Files/snort-1.7.tar.gz

Snort Database Creation

- Execute it "C:\MySQL\Bin>MySQL -u snort snort < C:\MySQL\Bin\create_mysql“



Snort – Finishing the Setup

- Be sure to “hard code” snort.conf rules
  - Should look like this:

```
#============================================
#include c:\snort\bin\local.rules
include c:\snort\bin\exploit.rules
include c:\snort\bin\scan.rules
include c:\snort\bin\finger.rules
include c:\snort\bin\ftp.rules
include c:\snort\bin\telnet.rules
include c:\snort\bin\smtp.rules
include c:\snort\bin\rpc.rules
```

- Test SNORT
  - C:\snort\bin\snort –c snort.conf –l c:\snort\logs
  - Should fire up and log to MySQL
  - If you get no error messages, you’re ok!

Snort – What You Should See

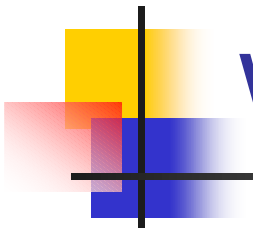
- Now test Snort

```
C:\snort\bin>snort -c snort.conf -l c:\snort\logs

          --=== Initializing Snort ===--

Initializing Network Interface \Device\Packet_<DFC
989>
Decoding Ethernet on interface \Device\Packet_<DFC
989>
Initializing Preprocessors!
Initializing Plug-ins!
Initializating Output Plugins!

++++++++++++++++++++++++++++++++++++++++++++++++++
Initializing rule chains...
Using LOCAL time
database: compiled support for ( mysql )
database: configured to use mysql
database:             user = snort
database: database name = snort
database:             host = localhost
database:    sensor name = BBRO01
database:      sensor id = 1
database: using the "log" facility
1119 Snort rules read...
1119 Option Chains linked into 155 Chain Headers
```



Web Server Time

- How-to assumes IIS 5.0
  - May want to harden it a bit ☺
  - Ships with Windows
- Apache will work great too
  - Free, which is usually good
  - ftp://httpd.apache.org/dist/httpd

PHP

- -Download: www.php.net/downloads.php

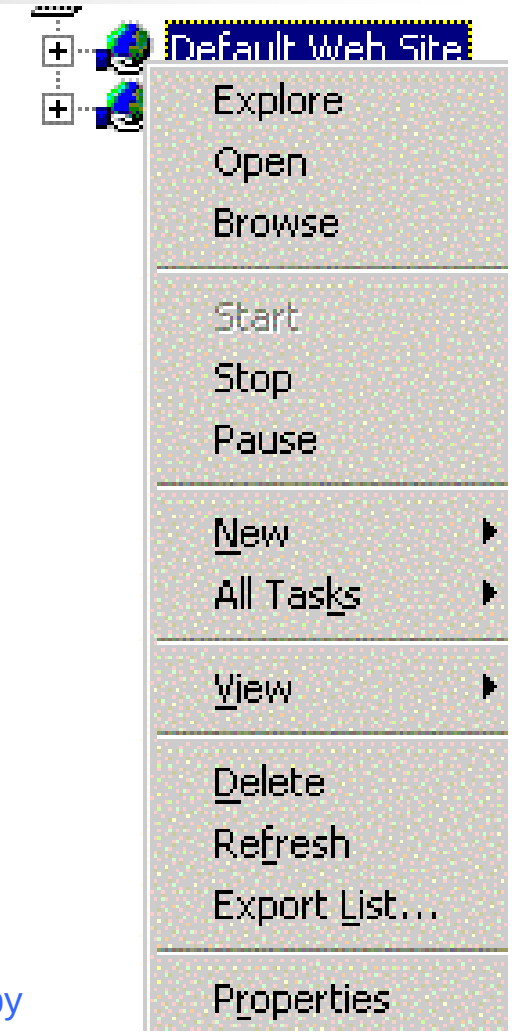
  Win32 Binaries

  - PHP 4.0.5 [4,590Kb] - 30 April 2001

- -Install
  - -Create c:\usr and copy mibs directory in
  - -Copy DLL's into winnt\system32 directory (avoid overwrites)
  - -Copy php.ini-dist to server root (c:\) & rename to php.ini
    - -Do not edit the php.ini file

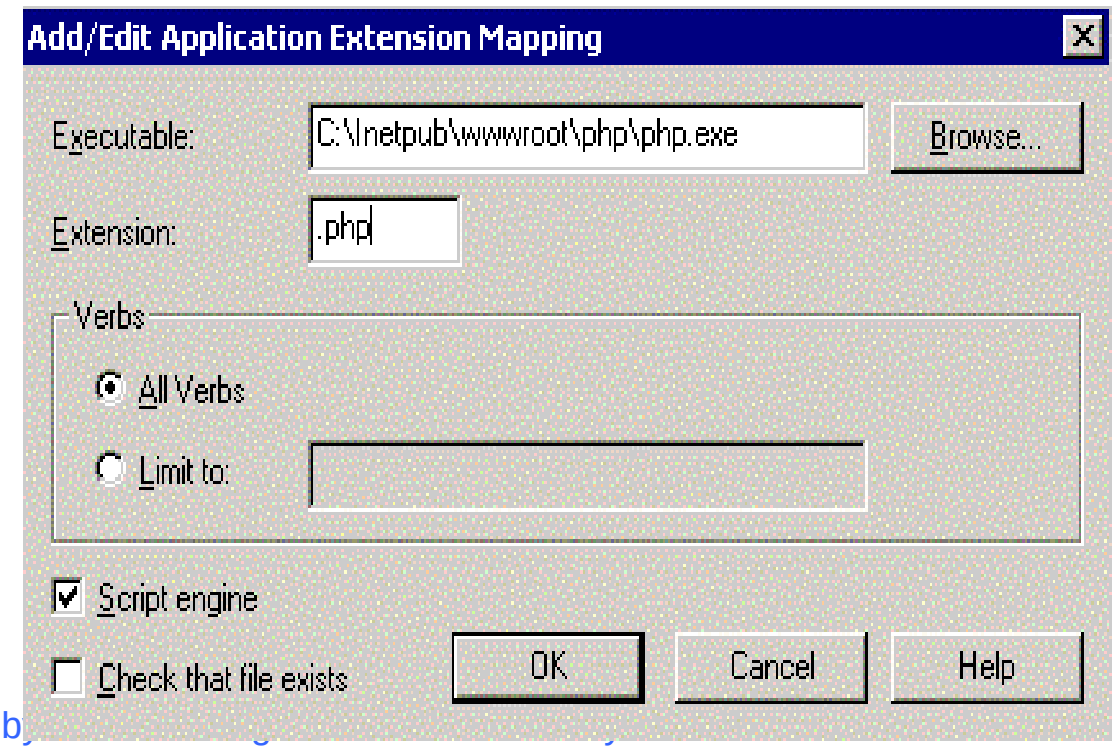
Make PHP Executable

- Now Add a new entry to IIS Application Mappings
  - Control Panel -> Administrative Tools -> Internet Services Manager -> Default Web Site
  - Select right-click then properties



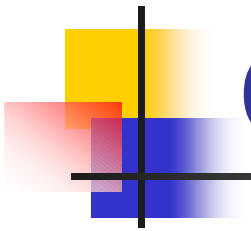
IIS – Adding PHP Extension

- Use the path to php.exe as the Executable, supply .php as the extension



Final PHP Installation

- Leave 'Method exclusions', blank, and check the Script engine checkbox
- Put a .php file under your Web server's document root and check if it works
- Voila!



Checkpoint!

- Where are we at?
  - MySQL
    - Installed & configured
  - Snort
    - Installed, configured & logging to database
  - PHP
    - Installed and tested
  - Now tackle ADODB & ACID

Getting ACID & ADODB

- This setup was on ACID 0.9.6b9
  - http://acidlab.sourceforge.net
- ADODB version 1.11
  - http://php.weblogs.com/adodb

ADODB & ACID Setup - 1

- Adds hooks between DB & web GUI
- Drop “ACID” into C:\inetpub\wwwroot
- Drop the “ADODB” directory into c:\
- Edit acid_conf.php in the acid folder

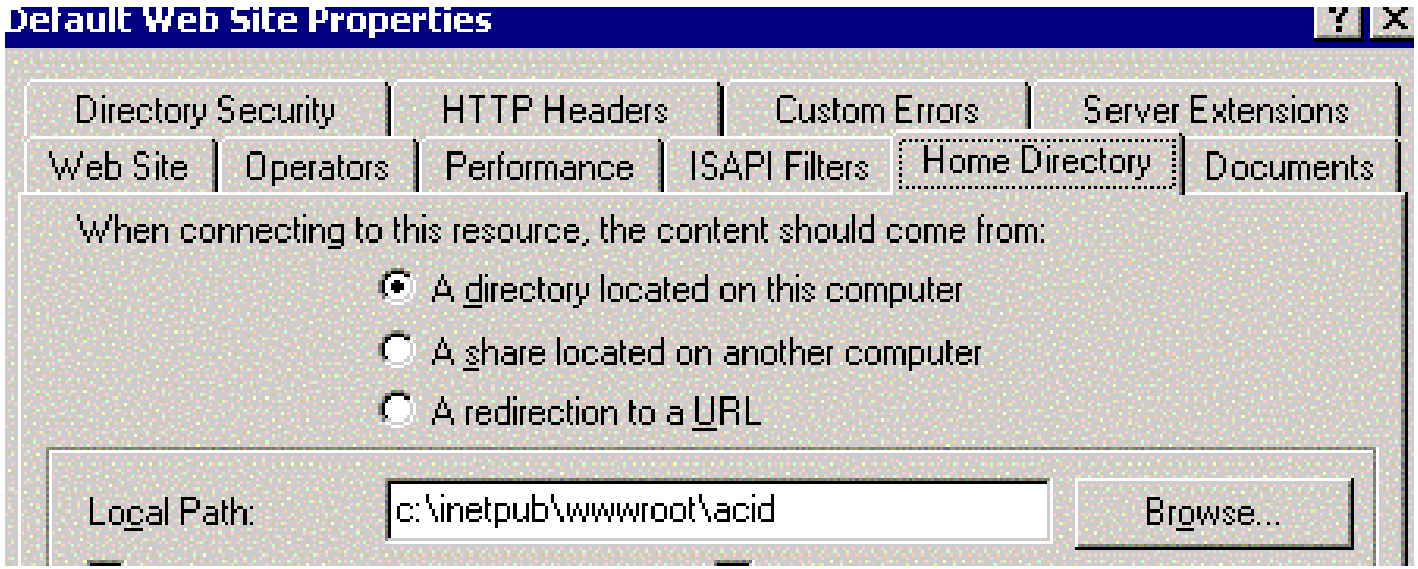
```
 */
$alert_dbname   = "snort";
$alert_host     = "localhost";
$alert_port     = "";
$alert_user     = "admin";
$alert_password = "snort";
```

Acid Setup PT-1

- Open Microsoft Management Console
- Right click on your Web server node (will most probably appear as 'Default Web Server'), and select 'Properties'.
- Select 'Home Directory', click on the 'Configuration' button.

Set ACID Homepage

- Now set ACID as the web root



ACID/ADODB Gotcha's - 1

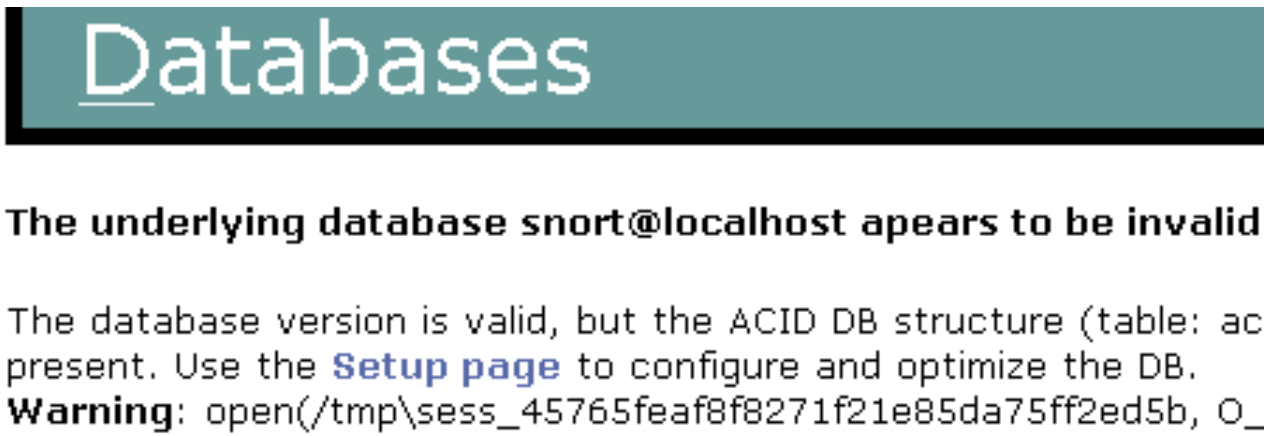
- Be sure to set this in acid_conf.php

```
/* Path to the DB abstraction library */
$DBlib_path = "c:\adodb";
```

- Now open the web site in a browser
  - http://127.0.0.1 if on Snort server

Web Based Steps - 1

- Now we should see:



- Not much farther to go!

ACID/ADODB Gotcha's - 2

- Click on the "setup" link to get this:

Operation	Description	Status
ACID tables	Adds tables to extend the Snort DB to support the ACID functionality	Create ACID AG
Search Indexes	(Optional) Adds indexes to the Snort DB to optimize the speed of the queries	DONE

- Click "Create ACID AG"

ACID/ADODB Finishing Up

- Now we see

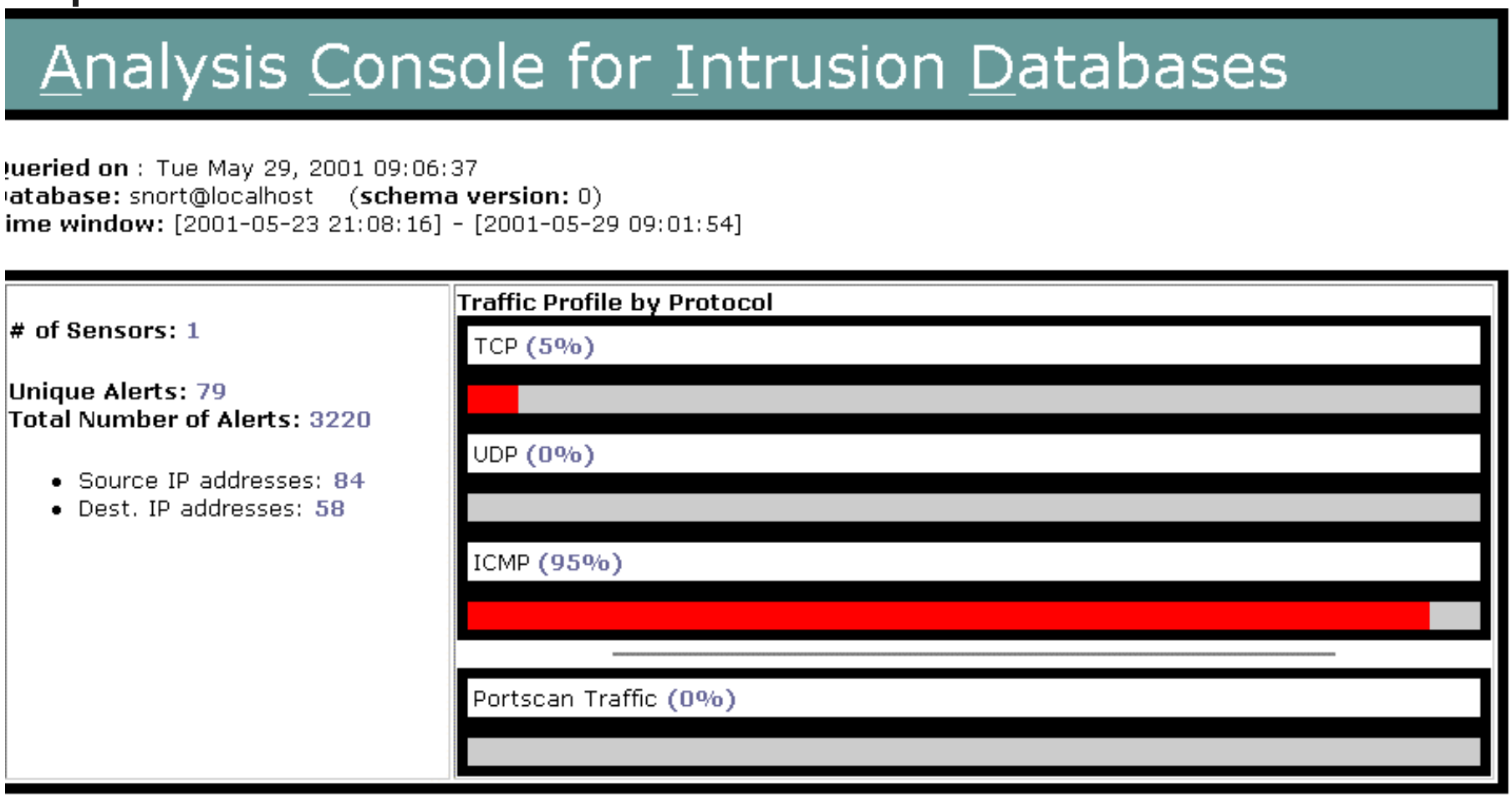
Successfully created 'acid_ag'

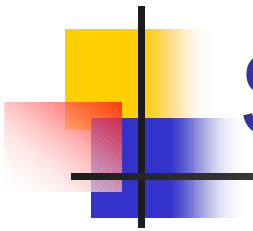
Successfully created 'acid_ag_alert'

Operation	Description	Status
ACID tables	Adds tables to extend the Snort DB to support the ACID functionality	DONE
Search Indexes	(Optional) Adds indexes to the Snort DB to optimize the speed of the queries	DONE

The underlying Alert DB is configured for usage with ACID.

Voila! An IDS is Born!





Securing the Server

- Restricting IP access to IIS
- Setting up SSL
- Setting up Windows 2000 encryption

Securing the IIS Server

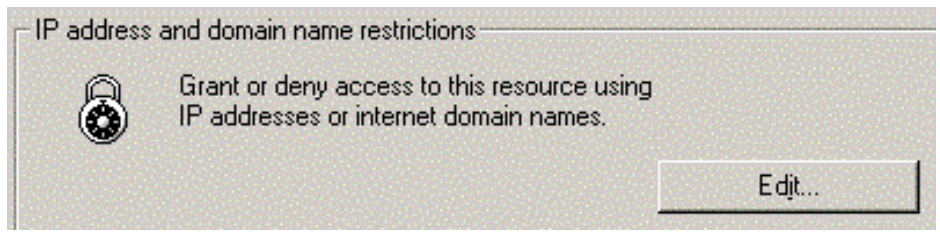
- IIS – Surely you're kidding right?
  - My names not surely ☺
- Only allow "authorized" users
  - Restrict IP addresses to web site
  - Use el-cheapo firewall

Restricting IIS Access

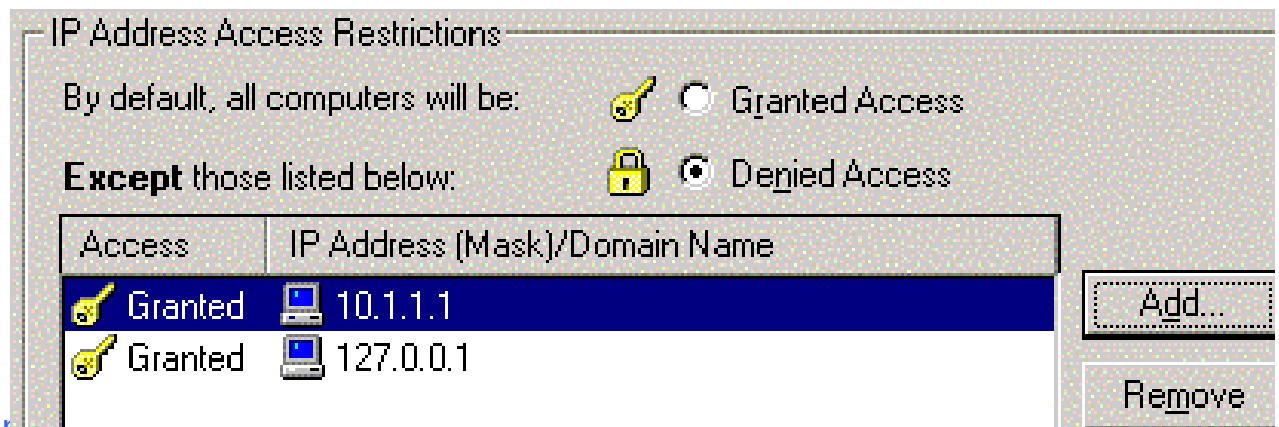
- Head to Control Panel/Administrative Tools/Administrative Tools
- Open “Internet Services Manager”
  - Right-click “Default Web Site” properties
    - Select “Directory Security” tab
    - Remove “Anonymous Access”

IIS Address Restrictions

- Now set IIS to only allow certain IP's
  - Select "IP address and domain name restrictions"



  - Set this to be VERY restrictive



Setting Up SSL Encryption

- Only log in using strong crypto
- Easy to get a “test” certificate
- Certificate are cheap insurance

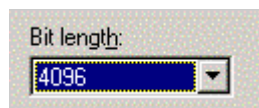
Getting a Certificate

- VeriSign outlines the following steps:’
  - Confirm Domain
  - Obtain Proof of Right
  - *Generate CSR (private key docs!)*
  - Submit CSR
  - Complete Application
  - Wait for Processing
  - Install your ID

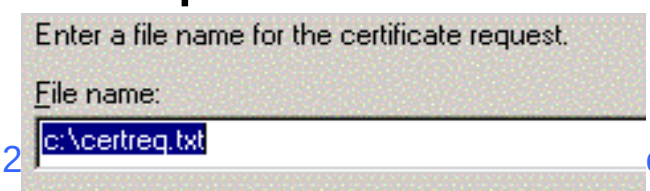
IIS Certificate Step One

- Select Directory Security/Secure Communications/Server Certificate
- Now follow the wizard!

  - Create a new certificate (CSR)
  - Prepare request now but send it later
  - Use longer key lengths



  - Fill in organization info as required
  - Drop the request on the drive



What is a CSR?

- Your web server's CSR public key that you ask a certificate authority to "sign"
- Your server will produce a plain text block like this:

```
-----BEGIN CERTIFICATE REQUEST----
MIIBujCCASMCAQAwejELMAkGA1UEBhMCQ0ExEzARBgNVBAgTClRFc3QgU3RhdGUx
ETAPBgNVBAcTCENvbG9yYWR0MRswGQYDVQQKExJDYW5hZGlhbiBUZXN0IE9yZy4x
EjAQBgNVBAsTCU9VIE9mZmljZTESMBAGA1UEAxMJd3d3LmV4LmNhMIGfMA0GCSqG
SIb3DQEBAQUAA4GNADCBiQKBgQD5PIij2FNa+Zfk1OHtptspcSBkfkfZ3jFxYA6y
po3+YbQhO3PLTvNfQj9mhb0xWyvoNvL8Gnp1GUPgiw9GvRao603yHebgc2bioAKo
TkWTmW+C8+Ka42wMVrgcW32rNYmDnDWOSBWWR1L1j1YkQBK1nQnQzV3U/h0mr+AS
E/nV7wIDAQABoAAwDQYJKoZIhvcNAQEEBQADgYEAAAhxY1dcw6P8cDEDG4UiwB0D
OoQnFb3WYVl7d4+6lfOtKfuL/Ep0blLWXQoVpOICF3gfAF6wcAbeg5MtiWwTwvXR
tJ2jszsZbpOuIt0WU1+cCYivxuTi18CQNQrsrD4s2ZJytkzDTAcz1Nmiuh93eqYw
+kydUyRYlOMEIomNFIQ=

-----END CERTIFICATE REQUEST-----
```

IIS SSL Certificate Step Two

- Should see “ You have successfully completed the Web Server Certificate wizard. A certificate request was created and saved to the file: “
- Free “test” certs available from Thawte
  - http://www.thawte.com
  - Past the contents of “certreq.txt”

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIGCTCCA/ECAQAwbzENMAsGA1UEAxMEdGVzdDERMA8GA1UECxMIU2VjdXJpdHkx
GzAZBgNVBAoTEldlcm5lciBFbnRlcnByaXNlczEOMAwGA1UEBxMFT21haGExETAP
BgNVBAgTCE51YnJhc2thMQswCQYDVQQGEwJVUzCCAiIwDQYJKoZIhvcNAQEBBQAD
ggIPADCCAgoCggIBALYEQqhqXxxbBySkav/YLK5eatt4T6kKNco25Q4SQeEJAPQF
WqE9ND6hKsvBq7VTU4/SDb+ccw6IiGcbFf/pCcnCxGFWP1zhX2BqqXeuLFF3APS8
bjxas7zE1NNGViWOwSxg3OCmcMF/RzhVmkYbN8iKGwvOcwvWXuiOrVRbRW7G4rXs
HKJqeHi9pMhyYrwy4twsLnEZVoq3KWyddaJLXSwKzcMAN8ne3enUjFzPMSjtRi+k
oadgEd+VatKCFZSnauCgvIWx53Nvpo1Ui77nuvTKw5gI1c8w+eACd/S54LZkOAHj
sqRWTT7zqyAMYClostqY3aLpQeBZbBKQwERLLYCyVHT5zk5DDFA+n3W5V48XV48a
```

Finishing Certificate Install

- Other options for “test” certificate
  - Test duration can be up to 365 days
  - Don’t change any other settings
- You should get this:

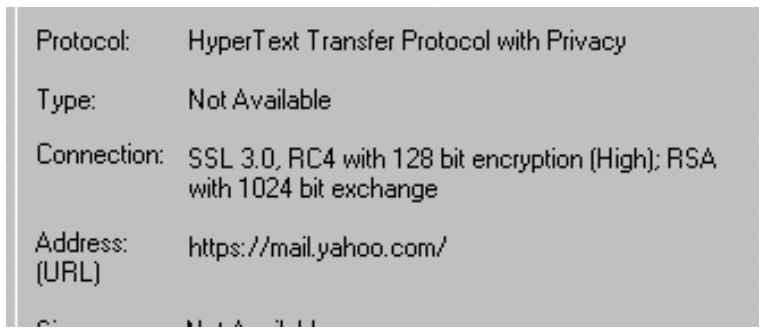
```
Here is your certificate:


-----BEGIN CERTIFICATE-----
MIIEGDCCA4GgAwIBAgIDGsy1MA0GCSq
QTEiMCAGA1UECBMZRk9SIFRFU1RJTkc
VGhhd3R1IEN1cnRpZmljYXRpb24xFzA
GgYDVQQDExNUaGF3dGUgVGVzdCBDQSB
```

- Now rerun “Server Certificate” wizard
  - Paste the certificate contents via notepad to your hard drive for input to wizard

Now Test It!

- Netscape and Explorer both give connection information



Security: This is a secure document that uses a high-grade encryption key for U.S. domestic use only (RC4, 128 bit).

Certificate:

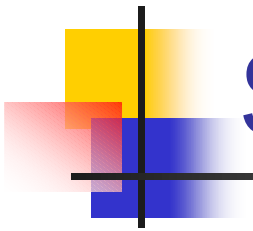
This Certificate belongs to:	**This Certificate was issued by:**
login.yahoo.com	Secure Server Certification Authority
Yahoo	RSA Data Security, Inc.
Yahoo	US
Santa Clara, California, US	

Serial Number: 17:DF:FF:A2:A1:12:81:04:E1:19:48:1B:23:A5:28:D5

This Certificate is valid from Mon Feb 21, 2000 to Wed Feb 21, 2001

Certificate Fingerprint:

B2:4C:67:B7:74:D9:D7:A9:12:71:54:71:BB:89:0F:2E

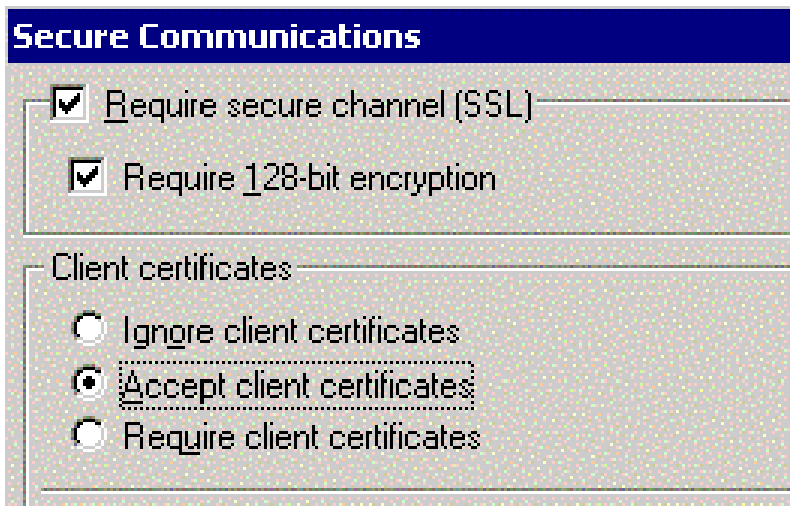


Server Side Crypto Settings

- What about governing crypto at the server?
- If we control the endpoint, then the battle tilts in our favor
- Netscape & IIS allow different degrees of control

Require Strong Crypto!

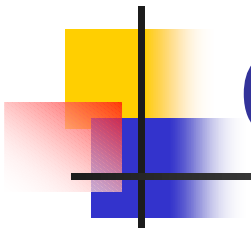
- Set IIS to only allow strong SSL
  - Default Web Site Properties/Directory Security/Secure Communications/Edit



  - This disallows unencrypted logins

Checkpoint

- At this point we should
  - Have an operational Snort probe
  - Have strongly encrypted access
- Test the connection
  - https://insert.your.server.address
  - Login using user/password
  - Tell browser to accept the certificate
    - It may complain, but ignore it ☺

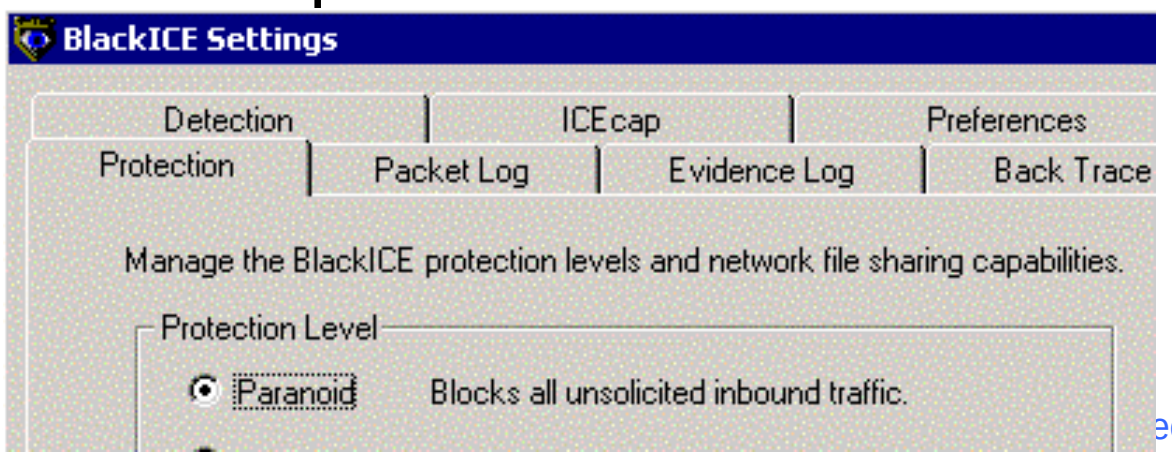


Cheap Firewall Protection

- We will demo BlackIce
  - Simple setup
  - There are others
    - Sygate, Symantec, ZoneAlarm, etc.
  - BlackIce is simple, cheap and effective
    - $40, a credit card and 20 minutes are all you need ☺

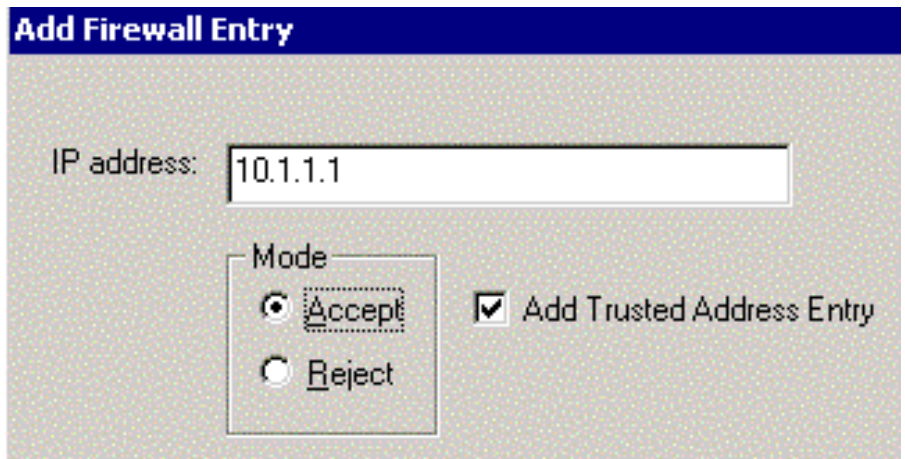
Quick & Dirty BlackIce

- Do a normal install (click/shoot)
- Once running we'll tweak two settings
  - Right-click BlackIce in service tray
  - Bring up properties and set Protection Level to paranoid



Finishing BlackIce Setup

- Using BlackIce to restrict clients
  - Right-click the BlackIce in the system tray
    - Select “Advanced Firewall Settings”
    - Now add specific addresses to allow



    - Once done, simply “ok” all changes

Finished Probe Results

- Snort up and running
- Secure, web based GUI
- Economical firewall protection