# Global Information Assurance Certification Paper

Felix Bakhman
Security Essentials Certification (GSEC) version 1.4b option 1
Building a Simple Honeypot in Windows
30 May 2003

Abstract

This paper is written to demonstrate the construction and implementation of a research Honeypot in a Windows-based environment, with all steps in the construction project documented as they are performed. Since Honeypot is implemented using various tools, those tools will be explained during the building procedure. Best effort is applied to provide explanation of all the tools used, but since this can be very lengthy, appropriate Web links are provided for further reading and research.

Introduction

The first time I encountered the word Honeypot and its explanation was under exciting and at the same time disappointing circumstances. As I was preparing the topic for GIAC (1), I began thinking in terms of security. I needed to reshape my mind and change my way of thinking about security. As I began searching for an original topic, I thought about my past and current visits to Warez (2) and hacking websites, which brought up a question: Who are the people that we are defending against? Moreover, why so little information is available about the attacks that take place in real time and monitored while in action?

I began thinking in terms of firewall technologies in use, as well as their purpose. To keep the "bad guys" out, we would configure our devices and sit back; satisfied with the feeling of safety we thus acquire, only to be burned again and again by an invisible enemy. After reading many reports about break-ins all over the world, it became clear that the enemy is ahead of the game.

Intrusion Detection sounds like an answer to complete our security, but unfortunately, this is far from the truth. We would set up our IDS and our firewall and think of our security measures as complete, the IDS helping to detect the intrusions and allowing for a quick modification of the firewalls and systems against the latest scan or intrusion attempt that the IDS informed about. If the organization was lucky, the administrator patched up the holes, and no damage has been done. However, after all the efforts to protect and detect, the ball was still not in our court; all the action to secure the resources was still taken after the fact.

At this time, the word "trap" became attractive, and I began my search string on Google (3). I came upon an article titled "To Trap a Thief "by Matthew Schwartz (4) in an online version of Computer World, a monthly general PC industry publication put out by IDG Company. While reading it, I stumbled upon the word Honeypot with a brief explanation of the technology and possible use.

Based on my understanding the word, Honeypot has absolutely no

technical meaning but more of a psychological. A pot of honey is placed on a wide-open entrance to a trap to attract dangerous bears. When the bears are lured in, the lid is shut and the predator is trapped. The lid, however, can remain permanently open, and the predators are allowed to explore but their actions are recorded, studied and used against them to defend ourselves against future attacks of the same kind.

## Honeypots Explained

Before the construction can begin, the reader must have an understanding of what Honeypots are and how they came about.

To apply technical meaning to the honeypot is quite simple. A tool is built, with one purpose only—to be compromised by a malicious code, such as a virus, or broken into by a hacker. The goal of the hacker is to do damage to the system itself or to use the unit to stage further attacks over the Web. The catch to this Honeypot tool is that the actions of the damaging party, whether it is a virus code that is running wild on the Internet, or a live hacker who has found the unit by performing blocks of IP scans, are being monitored, logged, and studied. A honeypot can be anything from Windows to UNIX; if it can be written in computer code it can most likely be cracked, and if it can be cracked, it has the potential to run as a honeypot.

"The honeypot technology is not new, the military and government and commercial organizations have studied it and continue to do so, but unfortunately very little of it was public knowledge until 1990" (5-Spitzner) Interested reader is encouraged to read work by Clifford Stoll The Cuckoo's Egg (6) and Bill Cheswick An Evening with Berferd (7), which are the early documents on the honeypot subject. The term Honeypot has not become the buzzword around the Information Security field until Lance Spitzner (8) and his team produced the first detailed book Honeypots: Tracking Hackers, published together with a resource website http://www.tracking-hackers.com (9).

Therefore, with out any further interruptions let us look at how honeypots have been defined. We also will describe their use, value, and finally create a simple Windows-based setup.

## Definitions

"A security resource whose value lies in being probed attacked and compromised" (10-Spitzner). To create such a system is simple: using available hardware resources, we build a system, which can be Windows or any flavor of UNIX. Since there are no rules on how the honeypot box is build, we can be as creative as possible.

For example, we can build a unit that is a default install of any operating system, thus making a compromise a very simple process. Alternatively, we can fully patch the box to make it even more interesting. Then we simply wait for the machine to be compromised. At this time, you might be asking yourself why we

would want our systems to be compromised if we put in so much effort, time, and money to keep the “bad guys” out. This is exactly were the exciting part comes into play.

A honeypot is not a production system, which means that when an organization implements the honeypot tool, there is no business-related traffic coming in or out of the honeypot. If traffic is being detected then the unit is being compromised. Honeypot’s sole purpose is to sit and wait, to monitor inbound and outbound traffic. The information is logged and studied; it is important to understand that a “honeypot does not help us secure any resource or environment; its intent is information based on the incoming traffic, or it can also be used as intrusion avoidance” (11-Spitzner).

At this time, the following question comes up: What is the difference between information used for study and information used to avoid intrusions? Marty Roesch, the creator of Snort IDS, broke down the use of a honeypot to two scenarios, Production and Research. “A Production configuration is used in an organization to help mitigate risk,” Marty Roesch states. “It is a type of configuration that, when the system is compromised, it acts as a border patrol officer” (12-Spitzner). For example, if a hacker enters the area being guarded, a warning will be displayed in the form of a banner, warning the intruder that if any further attempt to proceed is made certain actions will be taken, for example, the intruder will be logged, and possible steps can be taken in the court of law. This type of honeypot configuration can be build to replicate a Web server, a DNS server, or a mail server. There are several commercial and open source simulation honeypots.

A production honeypot setup is concerned with detection and avoidance. If an attempt to compromise is detected, whether a running script or a live hacker, a security administrator would take necessary action and secure previously unnoticed fault. In this case, a honeypot does its job by providing an early warning for the administrator to take action and to avoid possible trouble in the future.

For production honeypot to be effective, the placement location is very important. A good place to deploy a production Honeypot would be with in your DMZ (12), the same location where your web server and your mail server are located. This way if any malicious traffic is passed through the firewall, the honeypot will become the point of interaction and can be used to notify the security authority.


There are certain disadvantages with production honeypot. First, it is essential to understand that a honeypot does not function as IDS; in other words, it will not detect attacks on your network. If an attacker recognizes the honeypot, he can avoid the system and focus on others within your organization. Because no production traffic crosses the honeypot from internal sources, any communication to the honeypot is from outside sources. Therefore, information data that is captured coming into the unit is understood to be with bad intentions. By analyzing this captured data administrator can take appropriate action and investigate if other systems within the organization are vulnerable to the information captured by the honeypot.

For Research purposes, honeypots are implemented for information, namely about a newly discovered virus caught in the wild or with great hopes of actually monitoring a blackhat live in action on the honeypot. The captured data is used to learn techniques and the coded language used to communicate with other hackers. Finally, with the help of honeypot technologies, it becomes possible to fight back with a full view on the battlefield.

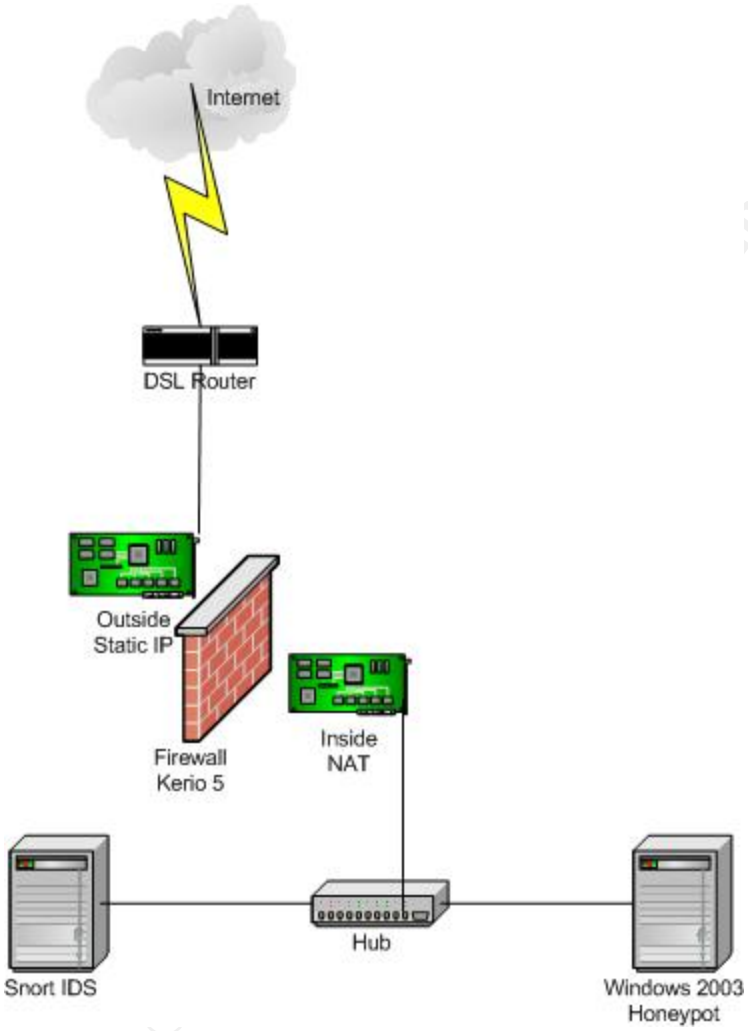
## Building the Honeypot Network

As I began considering ways to put this together, one of the initial steps was to draw out a game plan, a mapping of my new network on paper. Having this initial brain dump of your game plan will keep you on track, that way you can improve the design by adding or removing and not having to concentrate on remembering what your thoughts were about your design after a grueling day in front of your monitor at work.

As I began laying out the groundwork, the first thing I had to realize is I could get as creative as my current available test equipment will permit me, so to begin, this was my hardware list involved in implementation of a simple honeypot network:

1. Firewall -Intel based Pentium 450 with 325MB RAM.
2. IDS -Intel based Pentium 550 with 392MB RAM.
3. Honeypot - an IBM Pentium 300 with 128MB RAM.
4. Hub
5. DSL Router

The plan was to build a simple network where traffic comes in from the Internet through the DSL router into the firewall. The firewall redirects traffic as per Firewall rules in to the honeypot. The permitted traffic is monitored by IDS.




Building a Firewall

The hard drives for all the systems were prepared using two utilities.
1. A small DOS-based utility to erase the hard drive, wipe (13) (when you reach the site, select- support- hard drive information and scroll down to find Wipe).
2. A DOS bootable floppy using DOS 6.22 (14) (after downloading Wipe, extract it in to the DOS boot disk).

Let the system boot with the DOS bootable floppy and proceed following

instructions included with the wipe. After completing the task your data from that HD (up to 8 Gigs) will be erased including the boot sector.

Create a new partition (15) using the DOS bootable floppy. Next, install operating system, Windows 2000 Professional. Next, proceed to install virus scan of choice; McAfee (16) is used in this setup. Next, install Zone Alarm (17) host-based firewall protection (free version of Zone Alarm is used initially so the system can be "safer" connected to the Internet to update and patch up; remove Zone Alarm when installing Firewall of choice). Next, download the latest virus update file.

Fifteen minutes after the unit is connected to the Web, Zone Alarm detected a scan for a Sub Seven Trojan (18). Apparently, no minute is a safe minute when your are online; if it were not for Zone Alarm set to a paranoid level I would have been compromised without any knowledge. Put up a firewall before you proceed and install a virus scanner with the latest signature file. Next, update Windows (18) with the latest service pack and all the patches. After Windows are updated and patched there is an option in the control panel to have Windows automatically download and install updates. Do not select this option—after all, who knows what will be the next vulnerable component or patch (19) in Windows. Instead, do everything manually.

Next step is to remove any components of windows that are not needed. A default install of Windows comes with many different components, for example Windows Media player. Remove all components except for Internet Explorer. To do this, navigate to control panel, double-click Add-Remove programs, and select Add/Remove Windows Components in the left panel.

Next on the list come the unused services.

NOTE: For a detailed explanation on Microsoft services and system components, please visit www.Microsoft.com (20) navigate to the appropriate product for information.

Right-click the icon on the desktop called My Network Places, select properties, right-click on Local Area Connection, navigate to the TCP/IP protocol, and select properties. Hit the advanced tab and select the WINS tab; choose "Disable NetBIOS over TCP" and uncheck Lmhost (21) lookup.

NetBIOS (22) protocol is not used on our network.

The following services have been disabled.

Netlogon
Utility manager
Portable media serial number service
Telephony
Smart card helper
Application management
QosRsvp
DHCP client
ScardSVR
Index service
Automatic updates

NetBIOS Helper
Run-as service
Task schedule
RAS auto
MSDTS
Remote registry service
NetMeeting Remote desktop sharing

NOTE: When you disable the Service, do not forget to stop that service, or reboot, and the service will not start.

To further lock down the OS, permissions on certain folders must be modified, as well as several changes made to the NTFS permissions. For this task, an already established baseline that is developed by several industry and government top Infosec researchers has been consulted. A benchmark called W2k Professional operating system Level 2 Benchmark is selected (23). Implementation of the Benchmark is performed manually; if you choose you can use a baseline template and implement it with the Benchmark Scoring tool (available with the download of the benchmark). The reason the job is performed manually is that the template takes into consideration certain permissions and rights that are needed for a regular user to be able to function without being restricted to everything. This system is not going to have any users so I removed rights even further.

The following steps are the implementation of the baseline PDF manual. The steps are not in any particular order and are implemented with other procedures that are not part of the baseline document.

The first thing I did was change my password. All my passwords are 15 characters long, and it took me some time to develop them. I will explain why I chose the length of 15 characters.

Passwords in W2K can be displayed several ways using different tools, for example pwdump2 (24). “If you set your password to 15 characters or more the string for LM Authentication (LAN Manager used for backward compatibility with Windows) becomes a constant value, which means that the password is null. So when the password travels on the wire it shows as being null” (Urity 25) (another good read on password debate 26).

As to the password’s longevity, change it every 5 days. You cannot be certain who or what your network is up against and what kinds of tools are going to be used with what intent. The last thing you need is to find out later that your firewall has been accessed by using a password cracker. Do not be fooled by what you think is secure. After all, it only takes 5 minutes to come up with one 15-character-long password.

Next step is to implement local policy, located in the Control Panel-Administrative Tools-Local Policy. Begin by setting auditing on the system. The first thing we need to track is successful and failed attempts to create new users or groups and rename, enable, or disable anything related to any administrative or a user’s account. We need to audit these events because the

first thing a hacker does is try to establish or take over an account with most rights.

Open Policy Manager Icon—navigate to Audit Policy.
Audit Account Management—Select to audit Success and Failure.
Audit logon Events—Select Success and Failure (used to track anyone attempting to log on using local machine's credentials). You will also notice an Option to Audit Account logon Events. If you are using a Domain that logs domain credentials, in this setup, this option is not used.
Audit Object Access—Select Failure (object-can be a file or a folder)
Audit Policy Change—Select Failure, any attempt to change the policy will be logged.
Audit System Events—Generates events on a system-wide scale, system start and shut down.

Password Policy

Password history—since passwords are changed every 5 days, password history is set at a low number 3.
Maximum password age—5 days
Password length—14 characters
Password complexity—Enabled

Account Lockout Policy

Set account lockout threshold to four invalid logon attempts.
NOTE: Under User Rights assignment, remove all rights for any one except Administrator.
Rename Guest and Administrative account; make sure both accounts meet password complexity and character length.
In the windows control panel, open Users and Passwords icon to set password properties. Navigate to the advanced tab and on the bottom select the setting to require users to press CTRL+ALT+DEL to logon. (Depending on the physical location of your setup, this might not be necessary, but it is a very good practice to keep the logon procedure enforced.)

Security Option

Additional restrictions for anonymous connection—Select No access without explicit anonymous permission.
Allow system to be shutdown without having to log on—Disable.
Automatically log off users when logon time expires—Disable.
Set the option to clear virtual memory page when system shuts down. (27)
This one might make you blink twice: do not enable the disable CTRL+ALT+DEL requirement to logon.
Do Not Display Last User Name—Enable

Cache the previous logons-select to 0.

Restrict access to CD-ROM and floppy for locally logged-on users only.

Unsigned driver installation behavior—Warn but allow installation. If a driver is not signed by a vendor, you have an option to proceed or cancel driver install.

Unsigned non-driver installation behavior—Do not allow installation.

One of the options that are very useful is the setting to shutdown the computer if unable to log security audits—Set to Enable. Remember if there is a brake-in, the first thing an intruder attempts to do is cover his or her tracks.

Strengthen the default permissions of Global System Objects—Enable

Next step is to secure our Event logs. This step should be performed on all machines. (The honeypot box is not modified). Proceed into the registry and navigate into the following location:

HKEY_LOCAL_MACHINE
SYSTEM
ControlSet001
Services-Evetlog.
+Application
+Security
+System

Next, navigate in to a different partition of choice (other than C :\) and at the root of that partition create three new folders, Application, Security, and System. Go back into the registry and select Application, which now should be highlighted. In the pane on the right side, locate a Key named “File”; double-click to edit and modify the value data to point to a newly created folder “Applications” on the choice partition.

Perform the same task for Security and System.

Securing File and NTFS permissions.

NOTE: All of the settings bellow will have access rights for System and Administrator Group only, granted with full permissions that include folders and files; every other group is removed.

To modify security, right-click on the folder to be modified, select properties and select the security tab.

Proceed to system drive or c:\; perform security change in the following locations, root of c:\ (Found by double-clicking My Computer icon)

c:\WINNT
c:\WINNT\System32
config.nt
config.tmp
autoexec.bat
boot.ini
config.sys
io.sys

msdos.sys
ntdetect.com
Ntldr
pagefile.sys
c:\documents and settings
c:\WINNT\csc
c:\WINNT \debug-inside the debug folder modify “user mode” folder
regedit.exe
c:\WINNT\system32

Inside the system32 folder, modify all listed below:

at.exe
ntbackup.exe
rcp.exe
regedit32
dllcache
rexec.exe
rsh.exe
secedit.exe
setup.exe

Registry Permission

NOTE: in order to modify permissions in the registry use RegEdit32.exe

System and Administrator group has been granted full access to the registry hives; all other groups have been removed.

If, while browsing and viewing security rights, whether at the registry or individual files, you happen to notice that a System group has more rights than Administrator group, do not add equal rights to that location for the Administrator group. If it does not have it by default it does not need it; it is better to take away or add permissions only if needed.

Modify the following locations:

HKLM\Software\microsoft\Windows\CurrentVersion\Policies
HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce
HKLM\Software\Microsoft\Rpc

To test all the security modifications, download Languard (28). Running the application revealed extra security settings that needed to be change. For example, the FTP service came up as active, and since this box has no use for FTP, the service has been disabled.

Next task was to install and configure NIDS (29), Network Intrusion Detection System. This application would run on a separate pc sniffing traffic and reporting the results to a specially configured Web-based interface. This system would run in a promiscuous mode (30). SNORT (31) is selected to perform IDS function.

With great help from Silicon Defense (32) (select Snort-MySQL-IIS-ACID), document by Michael Steel Snort is being set up.

Before proceeding, be aware that this version of Snort does not function

on PPPOE (33). In addition, if connected to a switch, the ports must be Spaned or mirrored (34). Snort will not function on a dual processor box.

The Latest version as of this writing is Snort 1.9.0b227

NOTE: Vulnerability in version 1.9.0 (35) has been discovered. Because this document was written before the discovery, Snort 1.9.0 has been used in the setup, but because of this issue, the installation was updated. If you are currently running Snort 1.9.0, this section of the document can be used to update Snort. All downloads will point to the newest versions of applications available. By the time you read this paper, a new version most likely will be out.

Hardware and Software prerequisites:

1. Fresh install of Windows.
2. Two HD partitions, best if used on 2 hard drives. C:\- minimum 4 GB, and D:\- minimum 10 GB.
3. All service packs and patches applied.

The steps taken to prepare the PC for Snort are the same as the steps taken for the preparation of the firewall.

Install W2K on partition C:\ then perform the same procedure as in previous setup; install virus scan and a personal firewall; update virus scan signatures and update firewall, if any updates are available, as soon as you connect to the Web. All settings on the firewall should be set to maximum protection, only then you can update Windows. (This system needs to be as clean as possible, so perform the updates and do not browse the Web. Uninstall all products after including virus scan when installing Snort.)

This installation of Snort will be using:
MySQL as a database.
IIS 5.0 as a Web Server.
ACID as an Analysis Console for the Intrusion Detection.
Install WinZip (36).
Download all the files below into a new folder created on the desktop.
Folder's name is not important.
Snort 1.9.1 (37)
WinPcap (38)
MySQL (39)
PHP (40)
ADODB (41)
PHPLot (42)
JPGraph (43)
ACID (44)

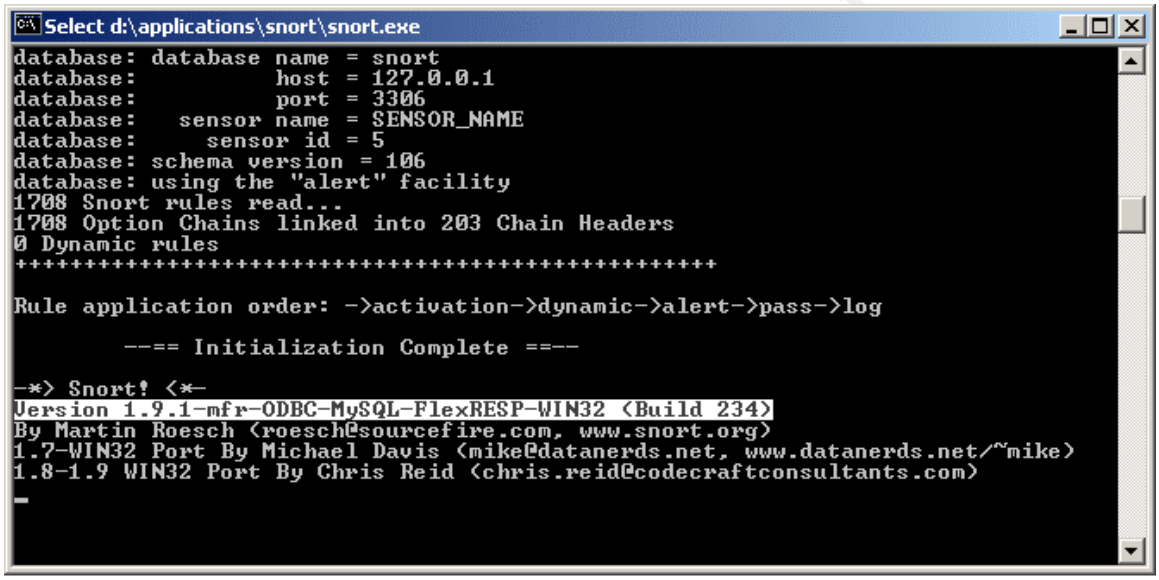
The 1.9.1 version corrects a RPC decoder buffer overflow. Since no documentation or even suggestions in regards to performing the upgrade at this time are available, I decided to experiment and perform installation on top of my existing setup. Before proceeding, make a copy of the snort.conf file and save it in a temporary location.

Stop the Snort service

Double-click the new version of Snort, which includes an automatic installer. Select the options that you need, browse into the directory of the original installation, and proceed to overwrite. The new snort.conf file is the same as the old, so no changes need to be made. Copy and paste the old snort.conf to the location of the new one and proceed to over-write. Navigate in the bin folder located in d:\applications\snort\bin. Inside the bin folder copy the LibnetNT.dll file and the snort.exe file and paste both into the root of the Snort directory.

Reboot the PC.

When the system starts again the new version of snort will be displayed in the cmd prompt at startup.




## New Installations

Because of the new Snort 1.9.1 executable, there is no longer a need to create folders for the installation as in previous versions. The auto installer will create the necessary folders for the Snort package.

Execute the Snort 1.9.1, agree to the license, and on the next screen select the options to install support for FlexResponce. Do not select support for Microsoft SQL. Next, select the list of items to be installed, then select next. On the next screen in the path, type D:\applications\snort. An applications folder will be created and a separate Snort folder inside the applications folder will be the location for all components to be installed for Snort to function.

Open Applications\snort\etc, right-click on the snort.conf and select open. A popup will appear with different program icons. Navigate it to the bottom and select WordPad. Uncheck the Always use this program to open these files (from now on every time you open a configuration file this way always uncheck the box to always open).

Snort.conf is the brains of Snort. This file can be configured to fit your needs, and the language used is simple to understand.

After loading Snort.conf into WordPad, several changes are made to the original.

According text within Snort.conf, it takes four steps to configure your setup:

Step 1 Set the network variables for your network
Step 2 Configure preprocessors
Step 3 Configure your plug-ins
Step 4 Customize your rule set

Note: In the snort.conf, the # symbol is the difference between a statement that will execute or not execute, if # is present, the line is considered for informational purpose only, so if you needed it to work remove the # symbol. In addition, when applying a path to what ever file or directory be careful what slash / \ you use.

Leave default settings for var HOME_NET any—for the internal network, this would cover the range of private IP address.

var EXTERNAL_NET any—this setting covers the rest of the possibilities of network ranges. Snort.conf file has several examples of network address range settings to use.

The next step is to navigate to the var RULE_PATH and point that line to the directory that holds the rules (var RULE_PATH d:\applications\snort\rules)

Find Output database and modify as follows:

log, MySQL, user=snort password=123 dbname=snorthost 127.0.0.1 port-3306 sensor_name=SENSOR_NAME

Find Output database: alert, MySQL, user=snort password=123 dbname=snort host=127.0.0.1 port=3306 sensor_name=SENSOR_NAME

NOTE: When setting up the Output Database files above, make sure the full configuration statement is located on one line only.

Do not separate the statements into two lines in the .conf file
For example, do not do the following 2 lines:

1-log, mysql, user=snort password=123 dbname=snorthost 127.0.0.1
2-port-3306 sensor_name=SENSOR_NAME

If you separate this into two lines, you will receive errors when starting Snort. If you do wish to separate the lines make sure the \ is included at the end of the line.

The SENSOR_NAME can be whatever name you like; this is what will be displayed at the Acid console when viewing alerts.

Next, select Snort to send alerts to the applications log in Windows event viewer by locating the line: Output alert_syslog: LOG_AUTH LOG_ALERT. Remove the # and the line will be active.

Locate Include clasification.config—This allows alerts to be classified and

prioritized. Point the “include” to the location were clasification.config file can be found: D:\applications\snort\etc\clasification.config

Next, search for include reference.config—defines URLs for the references found in the rules. Change the path to the file, after the include statement add D:\applications\snort\etc\reference.config

Save the file and exit.

Next, we install WinPcap; this is a windows packet capture program

When installing WinPcap, accept all defaults.

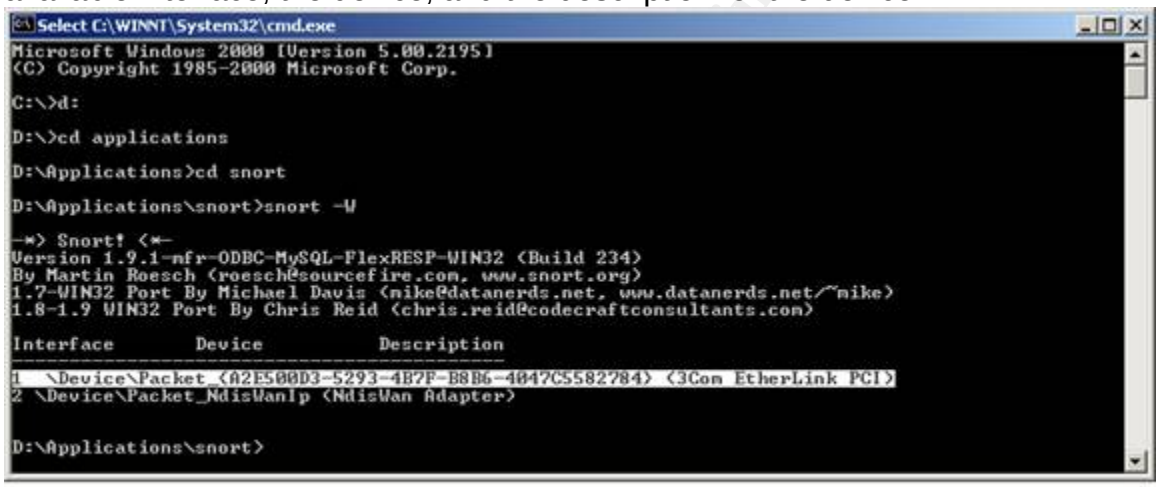
Reboot the PC.

Now let us test the install of Snort.

The following will test Snort in a packet-sniffing mode:

At the cmd change into the directory were Snort is installed (make sure the Snort executable is in the directory) and type the following command: >snort -W (list available interfaces)

After execution of the above command, you should see a selection of available interface, the device, and the description for the device.




To test Snort with a displayed interface, execute the following at the cmd prompt:

In the snort directory type >snort -v (verbose mode) –ix (x stands for the number of the interface that was displayed by the -W switch referencing the prompt above x=1).

To test, execute a webpage and if all goes well you will see data streaming past you on the screen.

To stop, hold down Ctrl and press c. The sniffing will stop and a page with statistics will be displayed.

Configuring Snort to run as a service.

Assuming that this service has never been installed, let us proceed. If it has been previously installed, all traces of this installation must be removed.

If you are experiencing an error, “Snort failed to start the service Erorr:

1067 the process terminated unexpectedly," then a different approach is to be taken.

The installation for Snort to run as a service is derived from a paper written by Christina Neal.

Snort Installation on Win2000/XP with Acid and MySQL for Dummies May 8, 2002 (45)

Download Service Tools (46)
Uncompress to c:\winnt
At the cmd prompt type instsrv srvany c:\winnt\srvany.exe press enter
At the same prompt type>instsrv.exe snort press enter
Open the Registry editor
Navigate to the following location:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Snort
Select the Snort folder. From the Edit menu, select new, select key and name the new folder Parameters
Select the new Parameter key, right click, and select new, select string value and type Application
Right-click the Application, select modify and type D:\applications\snort\snort.exe
Right click on the Paremeter key again; select new, select string value and type AppParameters
Right-click AppParameters, select modify and type -c d:\applications\snort\etc\snort.conf -l d:\applications\snort\log -i1 (the value of 1 is the network device that was displayed when snort -W was executed at the cmd prompt, Also note the – before c)
Right click Parameters, select new, select string value and type AppDirectory
Right click AppDirectory select modify and type D:\applications\snort

After all the steps are completed, navigate into the Windows control panel, Administrative Tools, Services and find the Snort service; right-click the Snort service select properties; select startup time to be automatic and start the service. If all the steps above are followed, you should experience no problems running Snort as a service.

Reboot the system. Proceed to test snort again to verify functionality:

Navigate in to the snort directory at the cmd and type Snort –W to select the interface type Snort –v (verbose) ix (x-is the number of the selected interface that the –W switch displayed).
Execute IE; you should see data scrolling on the screen.

## Installing and Configuring MySQL

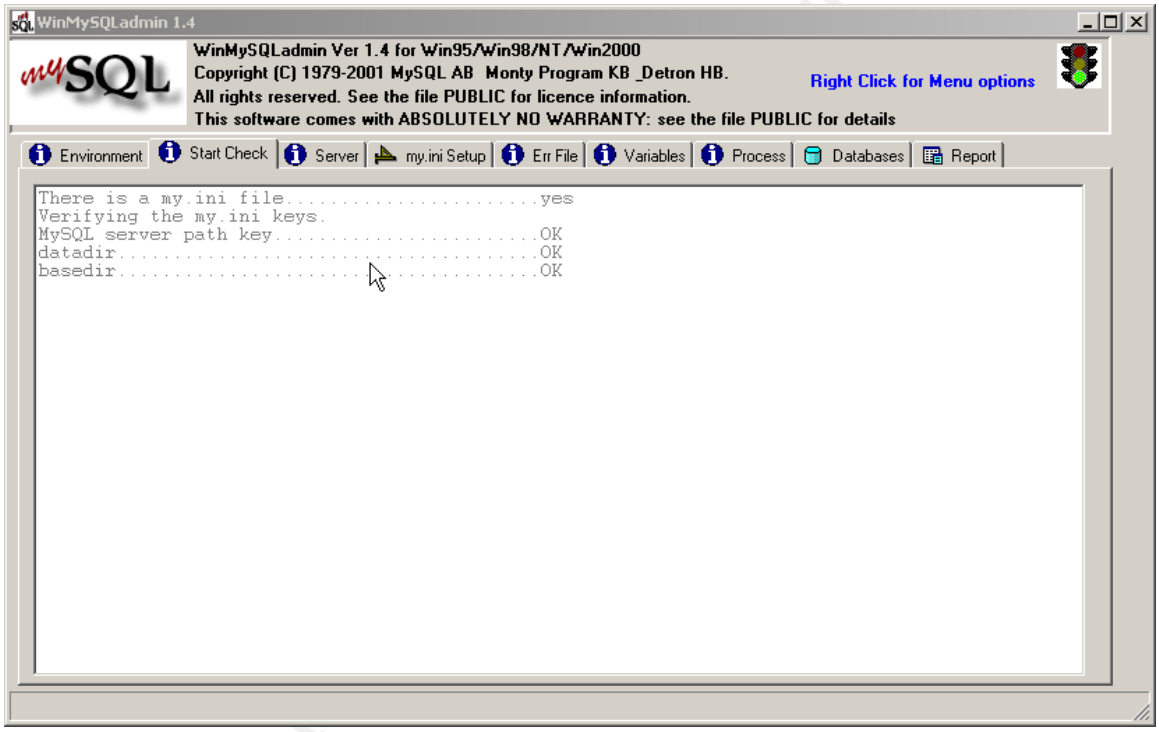
Create a temporary folder and uncompress MySQL into the folder. From the temporary folder install MySQL through setup.exe. On the following screen select next and again next, select browse and type the location of the folder that will hold MySQL, d:\applications\MySQL. For install type select typical, click next

to complete the install, and select finish. Remove the temporary folder. Open the following directory d:\applications\mysql\bin. Inside the bin folder double click the winmysqladmin.exe; this is the administrative console for MySQL.

If all is well, you will see a system indicator for MySQL that resembles a traffic light in the tray at the lower right side on the desktop; at this time, the light will be red.

If you have installed MySQL into any other directory except C:\, attempted to start the service, and failed you will need to perform the following steps:

At this time in the system tray, the MySQL traffic light is red. Right-click on the traffic light and select Show Me. MySQL admin will popup. Click on the Start Check, make sure the ini file is present and all the rest of the options are checked with ok.

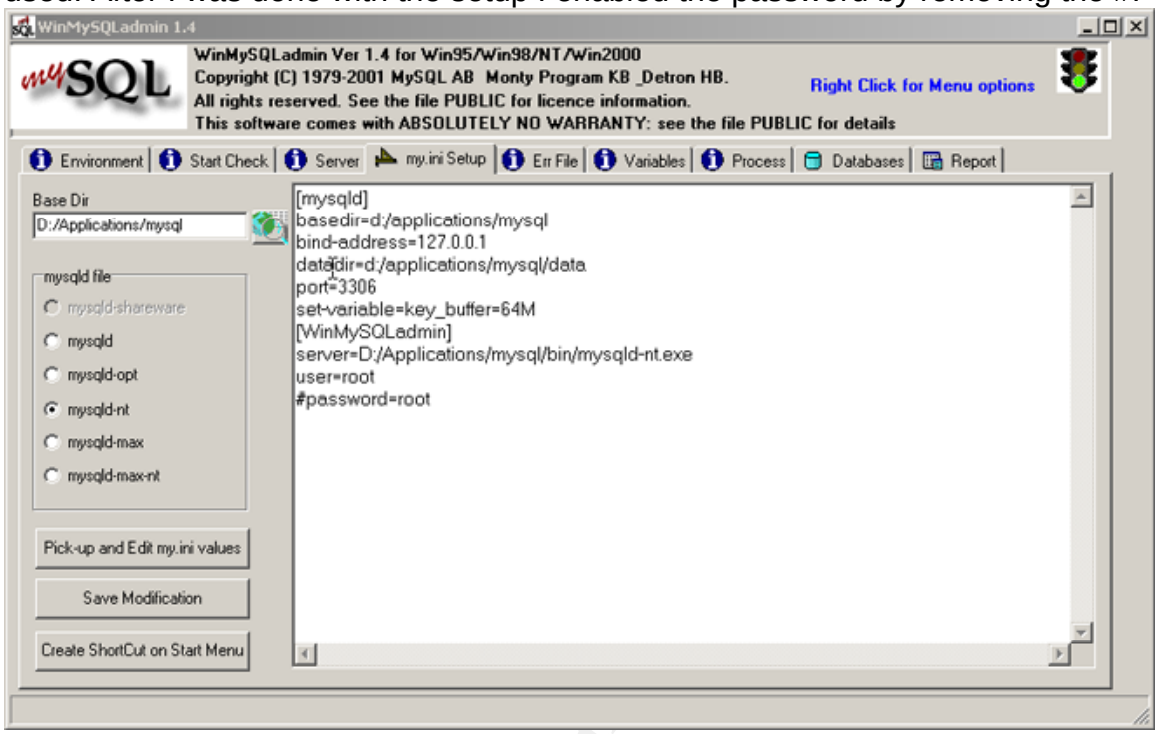



Next, go to my.ini Setup tab, make sure that the MySQL file option is selected as mysqld-nt, and perform the following:

Perform the following changes:

Basedir=(drive of the installation location) :/mysql
The Bind Address=127.0.0.1
DataDir=(drive of the installation location):/mysql/data
Port=3306
set-variable=key_buffer=64M
[WinMySQLadmin]
Server="drive of the installation location":/mysql/bin/mysqld-nt.exe
user=root
password=0100

NOTE: below you will notice that the Password contains #, indicating that it is not used. After I was done with the setup I enabled the password by removing the #.




Click on save this modification
Also, select the option to create Shortcut on start menu
Reboot the box.

If all is OK, the traffic light icon in the system tray should turn green, but if it is still red make sure the following is properly set:

1-my.ini file is located in the WINNT directory of the installation drive and is configured according to specifications. Be careful about which way your slash is pointing / \ and make sure in my.ini you are using the / (forward) slash.

If the service has not started, perform this check in the registry:

Under the Hive HKEY_LOCAL_MACHINE, navigate to the following location:

+System
+CurrentControlSet
+Service
MySQL make sure the string value Labeled ImagePath is pointing to the location of the installation drive and directory of MySQL program.

After verifying, everything is functioning, let us preceded to the next step.

## Removing the Default Databases and Users

Let us start by opening the cmd prompt and navigating to the bin directory in the MySQL folder.

At the bin directory, type the following:

>mysql -u root
You will be in the root of MySQL; proceed to type the following commands:

NOTE: the semicolon (;) is the key sign for the line to be executed, so if some statements are not being performed, first make sure you complete theme with the semicolon.

The following procedures will delete the default anonymous accounts and help secure MySQL (47).

Dropping Default Users

mysql>use mysql;
mysql>delete from user where host = "%";
mysql>flush privileges;
mysql>delete from user where user = '';
mysql>flush privileges;
mysql>select * from user; (after performing this command you should see only one user “Host”).
Mysql>select * from user where password=”; (if any rows come back with accounts, either assign a password to the account or delete the account. You are better off deleting all unnecessary accounts).
To set a password on a selected account perform the following command:
Mysql>set password for user-name@host_name=(new password)

Dropping default DB

Next, let us delete the database Test:
mysql>drop database test;
mysql>show databases; (you should only see one database “mysql”)

Next, we will create several new databases.

At the same prompt in the MySQL program
mysql>create database snort;
mysql>create database archive;
mysql>show databases;
You should see database 'archive', 'mysql', 'snort'.

Next is creating users for the database.

mysql>grant insert,select on snort.* to snort@localhost identified by (select a password);
mysql>show grants for snort@localhost; (you should see what you added

from the previous command)

mysql>grant usage on *.* to acid@localhost identified by (select a password);

mysql>grant select, insert, update, delete, create, alter on snort.* to acid@localhost;

mysql>grant select, insert, update, delete, create on archive.* to acid@localhost;

mysql>show grants for acid@localhost;

mysql>select * from user; this should display three users 'root', 'acid', and 'snort'.

mysql>quite;

This will complete the creation of databases and users.

NOTE: be careful not to get lost on all different passwords that you might create, try to remember what password is used were.

Creating ACID tables in the MySQL DB

Navigate to the bin directory of the MySQL server and at the prompt type the following:

Mysql>mysql -u root snort < D:\applications\snort\contrib\create_mysql
Mysql>mysql -u root archive < D:\applications\snort\contrib\create_mysql
Mysql>mysql -u root
Mysql>use snort;
Mysql>show tables; (you should see table listings)

NOTE: notice the space between the (<) on the left and on the right, make sure the commands are performed with space on both side of the <.

Reboot the box.

Confirm that the Snort.exe mysqld-nt.exe and winmysladmin.exe are running in the processes by opening task manager and selecting processes tab.

Installing the IIS 5.0

If you are using Windows 2000 or XP, the IIS service has been installed by default. If you chose not to install IIS during installation of the OS proceed to perform the following to install IIS 5.0.

To setup IIS, open Control Panel select Add Remove Programs on the side task bar select Add Remove Windows Components.

You will be prompted for the OS CD.

On the popup screen select IIS and proceed with the installation; click on details to see what else is installed by default and deselect the following components:

Documentation

FTP

FrontPage
Visual Interdev RAD
Remote deployment support and SMTP

Proceed to complete the installation.
Reboot the box.

Setting up IIS for ACID

In the applications directory create a folder called ACID. Remove the All Groups from the permissions of the folder and add System account and Administrator Group to have full control.

Start the IIS manager. You can find this icon in the administrative tools in the control panel after installing IIS.

Create a shortcut to the desktop.

At the start of the IIS MMC (Microsoft Management Console) you will see your local computer name; double-click and proceeded to double-click on Default Websites; right-click the Default Websites and select new Virtual Directory; a wizard will take you to the next procedure, Alias name will be Console; select the location of the Acid folder.

This location should be (Drive letter):\applications\ACID. Click next and accept the default access permissions, and finish the install. At this time, you will see the newly created entry under the default website tree called console.

Now let us proceed and secure the IIS 5.0 (48)

1-remove the RDS registry key (Remote Data Service-Allows DOS commands to be “run-as” system).

Remove the following keys and their sub-keys:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\ADCLaunch\RDSServer.DataFactory

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\ADCLaunch\AdvancedDataFactory

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\
Parameters\ADCLaunch\VbBusObj.VbBusobjCls (if present)

This configuration will prevent ODBC from allowing DOS commands.

NOTE: Even though this setup does not use ODBC, you might choose to use a package that does utilize ODBC. Below are the modifications to be performed in the registry.

HKEY_LOCAL_MACHINE\Software\microsoft\Jet

Look for two sub-keys 3.5 or 4.0 and under that key another sub-key called Engines.

Find a DWORD value called SandboxMode and set it to 3.

NOTE: If you are experience trouble with rights in your environment please reference the following http://support.microsoft.com/default.aspx?kbid=239104

(49) for different values for this key.

Next, let us cleanup extensions that will not be used.

Right click on the new Virtual Directory Console, select properties and click on the configuration tab. There you will see support extensions; proceed to remove all except .asp .asa .shtm .shtml; click OK and OK.

NOTE: If you updated your Windows by using Microsoft Windows update site and you downloaded and installed .NET Frame Work, the update created many different extensions automatically in your IIS. Please check your settings, and remove any added extensions.

Remove the IIS Samples-c:\inetpub\iissamples

Remove the Help directory-c:\winnt\help\iishelp

Remove the MSADC-c:\program files\common files\system\msadc

Before attempting to remove the msadc folder, close IIS MMC. If you still have troubles removing the folder, drag it to the desktop. The contents of the folder will be moved to the desktop and you will immediately be able to delete those with only the root folder being left in place.

If you are still unable to delete the root msadc, just lock it down by modifying the security settings, remove every one except administrators group, and assign that group only read permissions.

<u>The process of installing PHP HTML embedded scripting language</u>

Uncompress the PHP downloaded zip into the d:\Applications. You do not need to create the PHP folder; the application will extract into a two-layer folder; rename the second folder to PHP and place it into the d:\Applications.

At the root of the PHP folder locate the php4ts.dll; copy it and place it in the c:\winnt\system32.

In the same PHP folder locate the php.ini-recommended; copy it and place it into the same Winnt folder; rename the php.ini-recomended to php.ini

Proceed to edit the php.ini to make the changes listed bellow:

Change: max_execution_time from 30 to 60

Change: session.save_path = /tmp to session.save_path = c:\Temp (create a Temporary folder especially for this use; anyone who is using Acid needs permissions to access this folder.)

; cgi.force_redirect = 1

change to cgi.force_redirect = 0 (1)

change to extension=php_gd.dll (2)

NOTE: Notice the removal of the semicolon from the beginning of the above two statements.

extension_dir = ./ to extension_dir = d:\applications\php\extensions

Save the file and exit

Configuring PHP extensions for IIS

Open the IIS MMC; navigate to our new creation named Console located under Default websites.

Right-click on Console select properties; click on the virtual directory tab; click the configuration button and click on the application mappings tab.

Select add and insert, d:\applications\php\php.exe in the extension box, type> .php (note the period before php to indicate extension).

Check the script engine checkbox.

Select the “Check that the file exists.” This will check that the script file exists and sort out authentication before starting up php.

Apply and click OK to proceed.

Installing and configuring ADODB

Uncompress the latest version into the d:\applications folder.

Navigate to d:\applications\adodb\adodb.inc.php and open adodb.inc.php using WordPad.

Locate $ADODB_database = ‘’; and insert the following between the quotation marks ‘D:\applications\adadb’

Save and exit.

Installing and Configuring PHPLot

Uncompress latest version in to D:\applications.

Rename the uncompressed folder to phplot.

Installing and configuring JPGraph

Uncompress the latest jpgraph in to D:\applications.

Navigate in to jpgraph folder and open src folder; copy all .php files into the D:\applications\phplot.

There is no longer any use for the jpgraph folder you can delete it.

Installing ACID

Uncompress the latest ACID version into D:\applications.

Edit, acid.conf.php in WordPad, perform changes listed below.

Locate @DBli_path = “” insert between the quotes (D:\applications\adodb)

$alert_dbname = “snort_log”;

$alert_host = “localhost”; (do not change)

$alert_port = “”; (insert port “3306” between quotes)

$alert_user = “root”; (change root to acid)

$alert_password = “mypassword” (replace my password with the same created for Acid user in MySQL setup)

$archive_dbname = “snort archive”;

$archive_host = “localhost”; (do not change)
$archive_port = “”; (insert port “3306” between quotes)
$archive_user = “root”; (replace root with acid)
$archive_password = “mypassword” (replace “mypassword” with the same password as created for Acid user in MySQL setup)
$ChartLib_path = “”; (insert “D:\applications\phplot” between the quotes)

Note: make sure you use quotes for all modifications and all statements are ended with a semicolon (;)

The Acid setup is complete; Save and Exit
Reboot the system.

After reboot, open IE and type in the following into the URL address space: http://localhost/console/index.html
At the first attempt, an error will show that “the underlying database snort@local appears to be invalid.”
To correct the error select the link “Setup page” and select “Create ACID AG” to complete the Acid Alert group configuration.
At the IE enter the same URL again, and the console will open.
Create a shortcut to the desktop by selecting File-Send-Shortcut to the Desktop.
We are finished setting up Snort IDS.
After our firewall is setup, we will test our IDS to see if the traffic is being detected by Snort.

Setting up a Firewall to control traffic to and from the Honeypot

As I began searching for a firewall for my environment, I concluded that the software would have to be from a commercial company on a trial basis because I was unable to locate anything from open source for Win32.
For my firewall, I decided to go with Kerio (50) Firewall 5.x.x because of the simplicity of the setup.
Here is some information about Kerio if you cannot decide on what to use. Firewall 5 is a Stateful network firewall – (Analysis of data within the lowest levels of the protocol stack and comparison of the current session to previous ones in order to detect suspicious activity. Uses business rules (corporate security policy) defined by the user and therefore does not rely on predefined application information. (51)
Internet connection sharing using NAT (Network Address Translation) allows your Intranet to use addresses that are different from what the outside Internet thinks you are using. It permits many users to share a single external IP address at the same time. NAT address range is not routable range. In other words, routing devices are unable to pass the packets from one location to another coming from a NATed address (52).
Internet connection sharing is supported for DSL, Cable, Dial-up and

Wireless. The software also keeps detailed logs; the only thing that is a bit tiresome is the process of sorting out the logs.

Let us begin installing the software and accepting default settings for the location of the installation. You can also change to install into any drive other than c:\. Once the wizard is selected to help with the rules, proceed to select the adapter that is connected to the Internet; select next, and the available adapters will be displayed.

NOTE: To make things less confusing you should rename the connections in the network places icon on the desktop, or in the control panel. On the desktop, right-click the My Network Places icon and select properties and rename the two connections appropriately, one for “Inside” and the other for “Outside.”

Now let us proceed by selecting the Outside connection in the wizard for Network Rules. You should see your IP for the outside source subnet mask and Mac addresses; click on next.

On the next screen, Outbound Policy, you have two options: to allow all outbound access from the inside source, honeypot; or to select several services. Do not select the all services with no limitations option to be allowed to access the Internet.

Check the option to allow access to the following services and select a hand-full to monitor. Kerio has a Time Ranges option, where you can apply different periods to be implemented with specific rules.

Remember: the more services that are open from your honeypot the larger the possibility to inflict damage to other locations on the Internet. So keep the services opened to the limited amount; for example, if you setup your honeypot as a Windows 2000 server you can open the DNS port 53. In addition, if you wish to see busy IDS, configure your honeypot as a Web server and select the firewall to allow access to HTTP port 80.

I want to remind you if you are attempting to replicate my environment, please be very careful with how you allow traffic to exit your honeypot. We do not want to cause damage to others, so monitor your setup carefully and only allow access to the outside on a limited basis and only monitored. I only allow traffic outbound while present at the network.

Next after deciding on what traffic to let out on controlled level, the next screen will ask if you wish to advertise any servers running on your LAN that should be available from the Internet. Click add and select IP address of the server on your internal LAN with a private IP address that is the honeypot box. Select the service you wish to advertise, for example HTTP.

Proceed to the next option; here is the location to select NAT. When you enable NAT option, your Internet connection NIC is able to communicate with private IP address ranges; Internet connection sharing is enabled to provide Internet service to our honeypot configured with a private IP of 192.168.x.x After completing the wizard, you will have all necessary components running on the firewall to begin seeing traffic into your honeypot.

Next, let us see what we have created so far. To do this, we will run a test

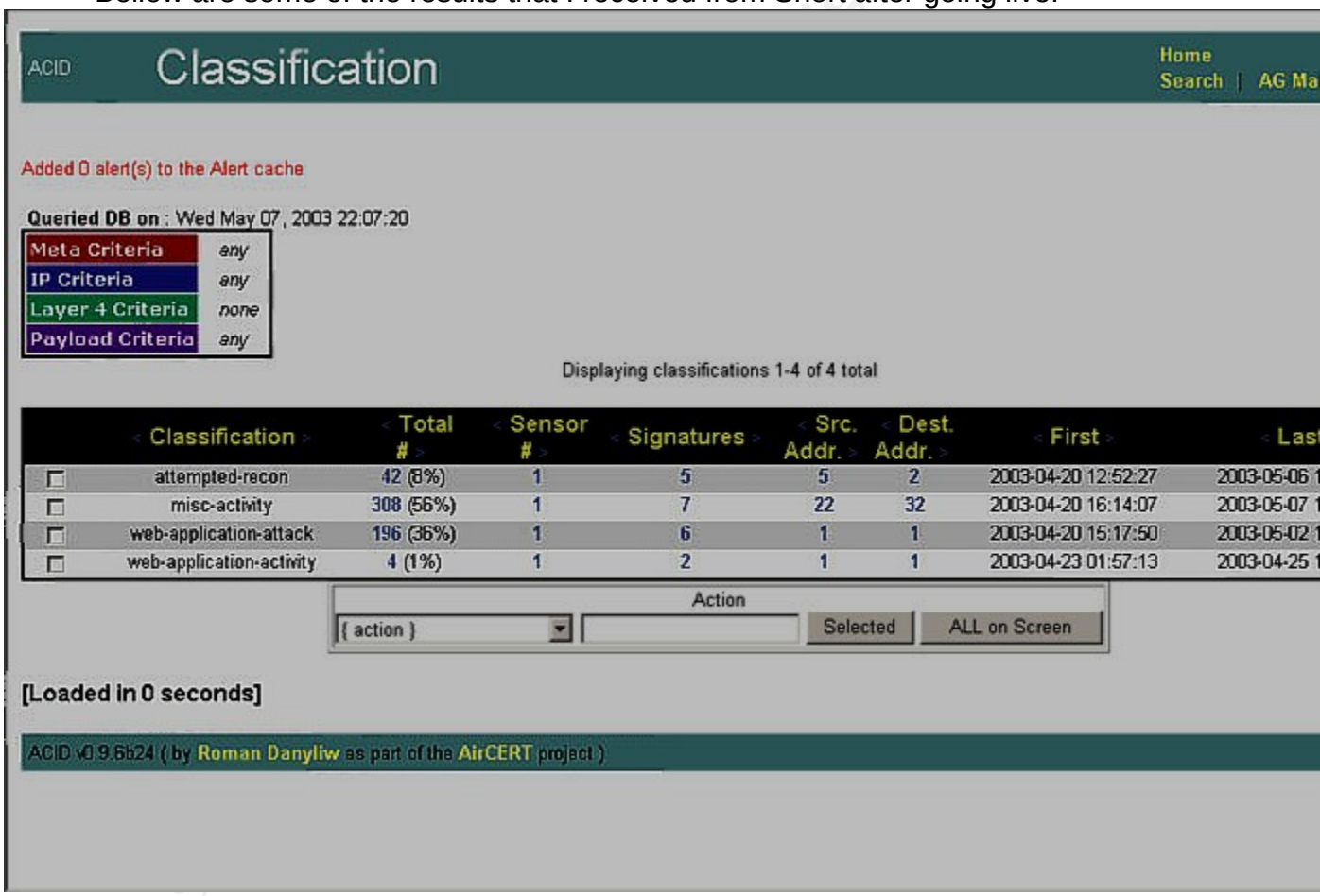
and scan our setup from an outside source just as anyone would, wishing to find an unsecured setup. The following procedure is considered Data Pollution(53), but this is a research environment for learning, and this will test our setup to see if we are functioning as planed.

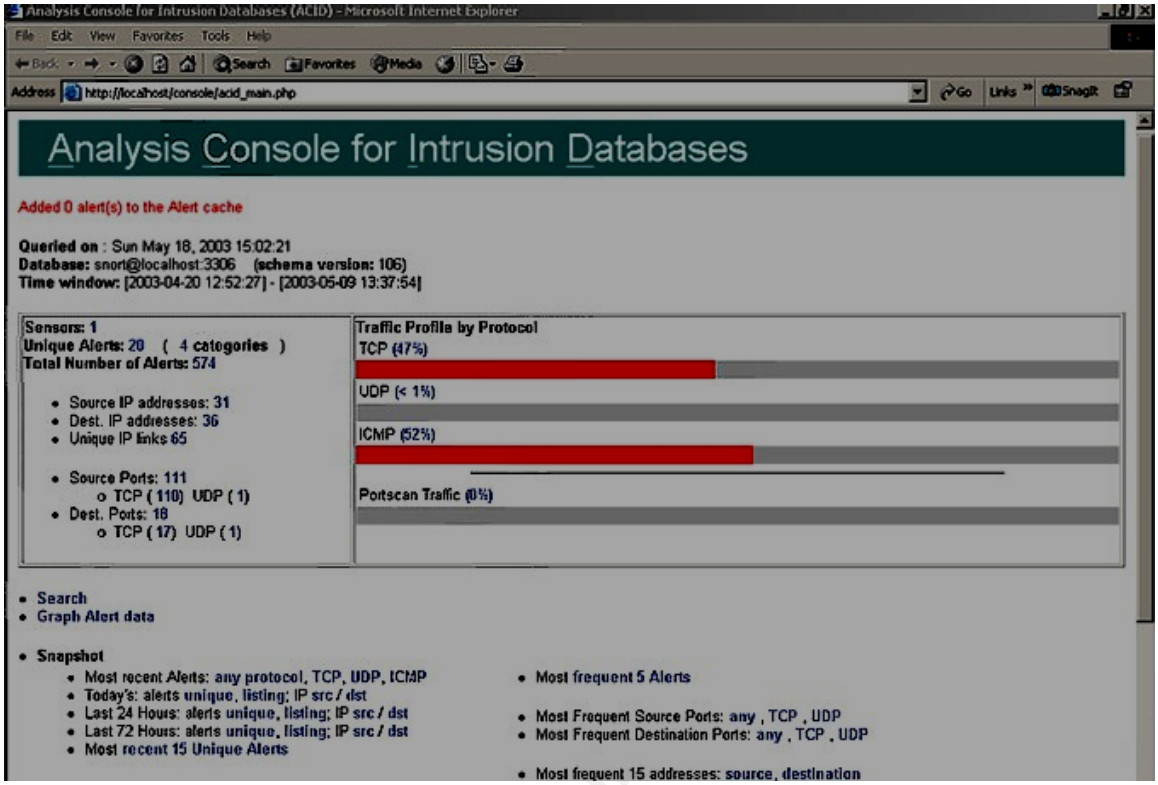
Use a laptop or any other system you can find with a different IP address.

Download a utility called NmapWin(54). NmapWin is a UNIX-based network scanner and auditing tool that has been ported over to Win32 by a team from eEye. The software comes with excellent documentation, so you can proceed and test the environment from outside.

This concludes our honeypot setup

Bellow are some of the results that I received from Snort after going live.






Some of the results that I received from Snort that I chose not to display were attacks on the honeypot from public and private entities that were vulnerable and therefore exploited. The compromised units in the organizations attacked my honeypot. Contact was made with the administrators and logs have been provided upon request. The response has been very interesting; most have been very grateful.

## Conclusion

As mentioned in the beginning of the paper this is a very simple setup, but the procedure to build it is not that simple and takes some steps. It is very important to make sure that all the equipment involved is as secure as possible, so go over your setup several times.

After going live, the results were fascinating. The network was scanned and attacked almost immediately. Most of the attacks on the honeypot came from organizations and personal systems that have been compromised by hackers.

The honeypot that was created is by no means a permanent research honeypot. It lacks many technical important procedures, such as:

1. A more manageable Firewall solution.
2. Separation of administrative and research network using routers.
3. Separate log machine.

The network has been up for a short time, and during that time under supervision. At this time, the honeypot is offline until necessary equipment is available to proceed.

# References


"ADOdb 3.50." PHPEveryWhere. URL: http://www.php.weblogs.com (25 May 2003).

"Analysis Console for Intrusion Databases." Carnegie Mellon Software Engineering Institute. URL: http://www.cert.org/kb/acid/ (25 May 2003).

Burnett, Mark. "Ten Windows Password Myths." Security Focus Magazine. 7 March 2002. URL: http://online.securityfocus.com/infocus/1554 (25 May 2003).

Caswell, Brian, Beale, Jay, Foster, James & Faircloth, Jeremy. Snort 2.0 Intrusion Detection. Rockland, MA: Syngress Media, 2003.

Cheswick, Bill. "An Evening with Berferd." White paper, 1990.

"Configuring the Catalyst Switch Port Analyzer (CSPAN) Feature." Cisco Systems. URL: http://www.cisco.com/en/US/products/hw/switches/ps700/products_tech_note09186a008015c612.shtml (25 May 2003).

Cooper, Russ. "10 Steps to Better IIS Security." Information Security Magazine. (August 2001). URL: http://www.infosecuritymag.com/articles/september01/features_IIS_security.shtml (25 May 2003).

Crapanzano, Jamie. "Deconstructing SubSeven, the Trojan Horse of Choice." SANS InfoSec Reading Room. URL: http://www.sans.org/rr/toppapers/subseven.php (25 May 2003).

DuBois, Paul. "Securing Your MySQL Installation." URL: http://www.kitebird.com/articles/ins-sec.html (25 May 2003).

"Enterprise Vulnerability Assessment and Remediation." eEye Digital Security. URL: http://www.eeye.com (25 May 2003).

"GFI LANguard Network Security Scanner 3.2." GFI Downloads. URL: http://www.gfi.com/downloads/downloads.asp?pid=8&vid=1&lid=1 (25 May 2003).

"GIAC: Global Information Assurance Certification." Official website. URL: http://www.giac.org (25 May 2003).

Google Search Engine. URL: http://www.google.com (25 May 2003).

"Honeynet Definitions, Requirements, and Standards, Version 1.5.2." Honeynet Charter. 12 April 2003. URL: http://www.honeynet.org/alliance/requirements.html (25 May 2003).

"Honeypots Solutions." URL: www.tracking-hackers.com/solutions (25 May 2003).

"Intrusion Detection System." Internet.com's Webopedia. URL: http://www.webopedia.com/TERM/I/Intrusion_detection_system.html (25 May 2003).

"Jet Expression Can Execute Unsafe Visual Basic for Applications Functions." Microsoft Product Support Services. URL: http://support.microsoft.com/default.aspx?kbid=239104 (25 May 2003).

"JpGraph – OO Graph Library for PHP." URL: http://www.aditus.nu/jpgraph (25 May 2003).

"Kerio." Official website. URL: http://www.kerio.com/kerio.html (25 May 2003).

"Lmhost." ComputerHope.com. URL: http://www.computerhope.com/jargon/l/lmhost.htm (25 May 2003).

Magri, Matt. "Jargon Dictionary" URL: http://info.astrian.net/jargon/How_Jargon_Works/Hacker_Writing_Style.html (30 May 2003).

"McAfee Security." Official website. URL: http://www.mcafee.com (25 May 2003).

"Microsoft." Official website. URL: http://www.microsoft.com (25 May 2003).

"Microsoft Windows Update." Official website. URL: http://windowsupdate.microsoft.com (25 May 2003).

"Clear virtual memory page file when system shuts down" URL: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/gp/567.asp (25 May 2003)

"MySQL." Official website. URL: http://www.mysql.com (25 May 2003).

"NetBIOS." Internet.com's Webopedia. URL: http://www.webopedia.com/TERM/N/NetBIOS.html (25 May 2003).

"Nmap – Free Stealth Port Scanner." Insecure.org. URL: http://www.insecure.org/nmap/nmap_download.html (25 May 2003).

"Partitioning and Formatting a Hard Disk for a Windows-Based System." National Instruments. URL: http://digital.ni.com/public.nsf/websearch/e503d0842606377a862569ea006ffd01 (25 May 2003).

"PHP." Official website. URL: http://www.php.net (25 May 2003).

"PPPoE." Internet.com's Webopedia. URL: http://www.webopedia.com/TERM/P/PPPoE.html (25 May 2003).

"Promiscuous Mode." SearchSecurity.com Definitions. URL: http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci518283,00.html (25 May 2003).

"PWDUMP2." Razor Tools. URL: http://razor.bindview.com/tools/desc/pwdump2_readme.html (25 May 2003).

Reed, Brian. "The DMZ Zone Explained." URL: http://www.firewalls.com/document-dmz.asp (25 May 2003).

Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G.J. & Lear, E. "Address Allocation for Private Internets." February 1996. Network Working Group. URL: ftp://ftp.ripe.net/rfc/rfc1918.txt (25 May 2003).

Schwartz, Mathew. "To Trap a Thief." Computerworld Online Magazine. 2 April 2001. URL: http://www.computerworld.com/networkingtopics/networking/lanwan/story/0,10801,59072,00.html (25 May 2003).

Sharick, Paula. "IE Cumulative Update Is Messy." Windows & .Net Magazine. 18 March 2003. URL: http://www.winnetmag.com/Articles/Index.cfm?ArticleID=38372 (25 May 2003).

"Silicon Defense." Official website. URL: http://www.siliconedefense.com (25 May 2003).

"Snort 1.9.1 Final Release." Silicone Defense. URL: http://www.silicondefense.com/support/windows/downloads.php (25 May 2003).

"Snort RPC Preprocessor Fragment Reassembly Buffer Overflow Vulnerability." Security Focus Magazine. URL: http://www.securityfocus.com/bid/6963/info (25 May 2003).

Christina, Neal "Snort Installation on Win2000/XP with Acid and MySQL for Dummies."

URL:http://www.sans.org/rr/paper.php?id=362 (25 May 2003)

Spitzner, Lance. “Honeypots: Definitions and Value.” White paper. URL: http://www.computerworld.com/networkingtopics/networking/lanwan/story/0,10801,59072,00.html (25 May 2003).

Spitzner, Lance. Honeypots: Tracking Hackers. Boston: Addison-Wesley, 2002.

“Stateful Inspection.” Internet.com’s Webopedia. URL: http://www.webopedia.com/TERM/S/stateful_inspection.html (25 May 2003).

Stoll, Clifford. Cuckoo’s Egg: Tracking a Spy Through the Maze of Computer Espionage. New York: Pocket Books, 2000.

“The Center for Internet Security.” Official website. URL: http://www.cisecurity.org (25 May 2003).

“Upgrade Your PC with MicroStorage.” URL: http://www.microstorage.com (25 May 2003).

Urity. “A Wonder of Windows 2000 Password.” Security Friday. June 2001. URL: http://www.securityfriday.com/Topics/win2k_passwd.html (25 May 2003).

“Warez: The Hacking Dictionary.” Official website. URL: http://info.astrian.net/jargon/terms/w.html#warez (25 May 2003).

“Windows Boot Disks.” URL: http://www.bootdisk.com/bootdisk.htm (25 May 2003).

“WinPcap: The Free Packer Capture Architecture for Windows.” Official website. http://winpcap.polito.it (25 May 2003).

“WinZip: The Archive Utility for Windows.” Official website. URL: http://www.winzip.com (25 May 2003).

“Zone Labs: Smarter Security.” Official website. URL: http://www.zonelabs.com (25 May 2003).

Last Updated: May 30th, 2017

# Upcoming Training


| | | | |
|---|---|---|---|
| SANS San Francisco Summer 2017 | San Francisco, CA | Jun 05, 2017 - Jun 10, 2017 | Live Event |
| SANS Houston 2017 | Houston, TX | Jun 05, 2017 - Jun 10, 2017 | Live Event |
| Security Operations Center Summit & Training | Washington, DC | Jun 05, 2017 - Jun 12, 2017 | Live Event |
| Community SANS Ottawa SEC401 | Ottawa, ON | Jun 05, 2017 - Jun 10, 2017 | Community SANS |
| SANS Charlotte 2017 | Charlotte, NC | Jun 12, 2017 - Jun 17, 2017 | Live Event |
| SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style | Denver, CO | Jun 12, 2017 - Jun 17, 2017 | vLive |
| SANS Secure Europe 2017 | Amsterdam, Netherlands | Jun 12, 2017 - Jun 20, 2017 | Live Event |
| Community SANS Portland SEC401 | Portland, OR | Jun 12, 2017 - Jun 17, 2017 | Community SANS |
| SANS Rocky Mountain 2017 | Denver, CO | Jun 12, 2017 - Jun 17, 2017 | Live Event |
| SANS Minneapolis 2017 | Minneapolis, MN | Jun 19, 2017 - Jun 24, 2017 | Live Event |
| SANS Columbia, MD 2017 | Columbia, MD | Jun 26, 2017 - Jul 01, 2017 | Live Event |
| SANS Cyber Defence Canberra 2017 | Canberra, Australia | Jun 26, 2017 - Jul 08, 2017 | Live Event |
| SANS Paris 2017 | Paris, France | Jun 26, 2017 - Jul 01, 2017 | Live Event |
| SANS London July 2017 | London, United Kingdom | Jul 03, 2017 - Jul 08, 2017 | Live Event |
| Cyber Defence Japan 2017 | Tokyo, Japan | Jul 05, 2017 - Jul 15, 2017 | Live Event |
| SANS Cyber Defence Singapore 2017 | Singapore, Singapore | Jul 10, 2017 - Jul 15, 2017 | Live Event |
| Community SANS Minneapolis SEC401 | Minneapolis, MN | Jul 10, 2017 - Jul 15, 2017 | Community SANS |
| SANS Los Angeles - Long Beach 2017 | Long Beach, CA | Jul 10, 2017 - Jul 15, 2017 | Live Event |
| Community SANS Phoenix SEC401 | Phoenix, AZ | Jul 10, 2017 - Jul 15, 2017 | Community SANS |
| SANS Munich Summer 2017 | Munich, Germany | Jul 10, 2017 - Jul 15, 2017 | Live Event |
| Mentor Session - SEC401 | Ventura, CA | Jul 12, 2017 - Sep 13, 2017 | Mentor |
| Mentor Session - SEC401 | Macon, GA | Jul 12, 2017 - Aug 23, 2017 | Mentor |
| Community SANS Atlanta SEC401 | Atlanta, GA | Jul 17, 2017 - Jul 22, 2017 | Community SANS |
| Community SANS Colorado Springs SEC401 | Colorado Springs, CO | Jul 17, 2017 - Jul 22, 2017 | Community SANS |
| SANSFIRE 2017 | Washington, DC | Jul 22, 2017 - Jul 29, 2017 | Live Event |
| SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style | Washington, DC | Jul 24, 2017 - Jul 29, 2017 | vLive |
| Community SANS Charleston SEC401 | Charleston, SC | Jul 24, 2017 - Jul 29, 2017 | Community SANS |
| Community SANS Fort Lauderdale SEC401 | Fort Lauderdale, FL | Jul 31, 2017 - Aug 05, 2017 | Community SANS |
| SANS San Antonio 2017 | San Antonio, TX | Aug 06, 2017 - Aug 11, 2017 | Live Event |
| SANS Prague 2017 | Prague, Czech Republic | Aug 07, 2017 - Aug 12, 2017 | Live Event |
| SANS Boston 2017 | Boston, MA | Aug 07, 2017 - Aug 12, 2017 | Live Event |