GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

SMaK

Smoothwall, **M**ySQL **a**nd **K**iwi Syslog Daemon:
Cost Effective Firewall and Logging with Database
And Analysis



GIAC Essentials Security Essentials Certificate (GSEC)

Practical Assignment
Version 1.4b
Option 2

Russell McRee
Submitted August 2004

© SANS Institute 2004, author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Table of Contents

Abstract ---------- 2
A Typical Pre-SMaK Environment ---------- 3
SMaK Hardware Requirements ---------- 4
SmoothWall Express 2.0 ---------- 4
Kiwi Syslog Daemon ---------- 4
MySQL 4.0 ---------- 5
Package Overviews ---------- 5
SmoothWall Express 2.0 ---------- 5
MySQL 4.0 ---------- 5
Kiwi Syslog Daemon ---------- 5
Prepare for a SMaK - Installation and Configuration ---------- 6
Preliminary Steps ---------- 6
SmoothWall Express 2.0 Installation ---------- 6
SmoothWall Express 2.0 Configuration ---------- 7
MySQL 4.0 Installation and Configuration ---------- 8
MySQL Control Center ---------- 9
Kiwi Syslog Daemon Installation ---------- 10
Configuring Kiwi to Log to MySQL ---------- 10
Configuring SmoothWall to Log to Kiwi Syslog ---------- 11
Configuring SmoothWall to Drop Logging on Noisy Traffic -- 12
You've Been SmaKd - Analyzing the Data ---------- 13
SmoothWall Express 2.0 ---------- 13
Kiwi Syslog Daemon ---------- 13
Querying the MySQL Database ---------- 14
What Does The Data Mean? ---------- 15
Archiving and Maintaining Data ---------- 16
SmoothWall Express 2.0 ---------- 16
Kiwi Syslog Daemon ---------- 17
MySQL 4.0 ---------- 17
Alternative Considerations ---------- 18
Conclusion ---------- 18
References ---------- 19

Abstract

He who is prudent and lies in wait for an enemy who is not, will be victorious.
- Sun Tzu

Consider the typical small business, perpetually cost conscious yet deeply concerned about securing their enterprise. Implementing a functional firewall with the ability to monitor and archive logs can be laborious and expensive, a challenge to manage consistently, and often overwhelming to analyze. While most every organization now utilizes a firewall of some sort and perhaps an associated Intrusion Detection System (IDS), without effective maintenance, trends and attacks become difficult to identify. To provide a firewall, IDS and a

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

logs database with tools for viewing, archiving, and analysis would likely cost an organization thousands of dollars were they to choose typical commercial solutions. Yet, there are inexpensive and open source solutions, that combined, can yield tremendous results towards this cause. Better still, these tools can be gathered and implemented in a relatively straightforward undertaking that will yield invaluable information in defending your enterprise and analyzing the traffic, no matter how small your organization.
This paper intends to identify a package of applications that, properly configured, will provide a firewall with syslog output to a database for queries, ready for analysis and archiving, all on inexpensive hardware at a cost less than $500. Each element in this conglomeration has excellent attributes and is robust and capable in its function. By definition, both Smoothwall and MySQL are open source and thus freely available under the General Public License (GPL). Kiwi Syslog Daemon is not open source but can be downloaded as freeware with limited functionality. Kiwi is exclusive to Windows installations so it will be assumed here that Kiwi and MySQL will be installed on the same Windows 2000 or XP system. It is the goal of this paper to offer a solution to the vast majority of SOHOs (Small Office, Home Office) or SMBs (Small, Medium Business) comfortable with the Windows platform and likely limited in IT resources, however, the concept proposed in this paper could be implemented entirely with no software costs on Linux platforms. See **Alternative Considerations** for more.

A Typical Pre-SMaK Environment

How many businesses fit the following model? Imagine 50 people, 35 PCs, 3 servers, a 48-port switch and a router. Their requirements are simple: email and Internet access are the primary considerations. The servers likely host files, a database of some sort and a mail server. Perhaps the router is configured with ACLs (Access Control Lists) and is hopefully providing NAT (Network Address Translation). Most likely, system administration is provided by an employee with other job functions or is handled part time by a contractor. No matter the possible organizational structure, budget is always a concern, yet no business wants to be vulnerable or unaware of threats and attacks. Are there any devices providing a true firewall service, logging messages from that firewall and archiving the data for potential legal action or forensic analysis? Is there budget available to spend thousands to buy commercial solutions in the form of expensive appliances or application suites with a major licensing obligation?
With two surplus PCs meeting the minimum hardware requirements listed in the next section and a $100 for a Kiwi Syslog Daemon license, an organization can move rapidly towards a more secure environment that will provide numerous ways to review potential attack data. Assume that the two surplus PCs from inventory or purchased from a reseller are valued at $150 or less, and that a Windows 2000 Pro license can be had for $100. Our total cost is less than $500; a small price to pay for vastly improved enterprise security.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

SMaK Hardware Requirements

In a perfect world your IT budget includes enough to put Kiwi Syslog Daemon and MySQL on a stout server with a RAID and Windows 2000 Server or Windows Server 2003. However, this perfect world is not where most of us live. Thus, listed below are minimum requirements.

SmoothWall Express 2.0

An extremely powerful machine is not critical here but at least a 150 MHz or faster processor is recommended. RAM requirements include a minimum 32 Mbytes RAM, ideally 64 Mbytes or more. With less than 64 Mbytes RAM it may not be possible to run all services, especially the Web Proxy Server and the Intrusion Detection System. Additional RAM may be needed for optimal performance if the Proxy Cache and Intrusion Detection features are utilized. An IDE drive of 2GB capacity is recommended. It may be possible to operate on as little as 540 Mbytes of disk, although this may present capacity problems with proxy log files etc. Higher capacity disks allow for more and larger log files to be stored; 2GB or more is advised if there are a large number of users behind the SmoothWall Express, as the more users and activity the quicker the proxy log files grow. An IDE CD-ROM drive is recommended for ease of installation; although SmoothWall can be installed across a network, the installation is more straightforward when using a local CD-ROM drive. Using a bootable CD-ROM drive makes the installation even simpler. See the Hardware Compatibility List for supported CD-ROM drives. Video card, monitor, keyboard and mouse requirements are left unstated as the majority of interaction with this machine will occur over the browser interface.
Network card: At least one supported network card is needed to connect the SmoothWall Express to the protected local network. For the ideal implementation, given a connection to the Internet via a broadband device such as a cable modem, Ethernet-presented ADSL, or another Ethernet-presented connection, a second supported network card will be required. [1]

As one of the goals of this paper is to minimize cost, it is suggested that Kiwi Syslog Daemon and MySQL be installed on the same system to conserve both hardware resources and network use. If the traffic you monitor is high volume there is an obvious argument for separating services but test your configuration with a SmoothWall Express server and a database/logging server first. The following requirements are offered if you intend to separate the services.

Kiwi Syslog Daemon

The system requirement to run Kiwi Syslog Daemon is a minimum of a Pentium 200 with 32MB RAM. Recommended is a Pentium III 850 with 256MB RAM. The Service edition of KIWI as utilized in this document will only run on Windows NT4 (Server or Workstation), Windows 2000 (Server or Professional) and XP Professional. Keep in mind that the recommended installation of these combined applications is to place MySQL and Kiwi on the same server. If you've chosen an

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

acceptable platform to support the database it is likely that it will more than suffice for Kiwi.[2]

MySQL 4.0

Administrator discretion is in order here. A database server's strengths depend on its abilities to support transactions. Syslog output from a SmoothWall implementation protecting an ADSL connection on a common ISP will log no less than 100 transactions an hour, sometimes much more during peak traffic times. Given the capacity of Kiwi Syslog Daemon to log input from multiple devices one can quickly see where the transaction count can climb quickly. Therefore, a more powerful CPU and above average RAM will benefit your organization. Additionally, a RAID 5 drive set for redundancy and larger capacity would bring even more significant gain.[3]

Package Overviews

The Firewall: Smoothwall Express 2.0

SmoothWall Express 2.0 is the latest release from Smoothwall in the UK. It is a 2.4 kernel based Linux distribution optimized for firewall functionality. It includes iptables, SSH access as well as Web interfaces for management over both HTTP and SSL. A tool set including *whois* and *traceroute* are included along with IP blocking, port forwarding, VPN and Snort IDS. SmoothWall maintains logs on the local host, which are accessible for viewing from the browser interface or via a text editor on the actual PC. [4]

The Database: MySQL 4.0

MySQL is an open source SQL database of extraordinary functionality and is fast, reliable and easy to use. It can also be purchased as a supported, enterprise ready application but for the purposes of this paper only the open source distribution will be discussed. MySQL, like Smoothwall is also released under the GPL.
"MySQL Database Software is a client/server system that consists of a multi-threaded SQL server that supports different back ends, several different client programs and libraries, administrative tools, and a wide range of application programming interfaces (APIs)."[5]

The Syslog: Kiwi Syslog Daemon 7.1

Kiwi Syslog Daemon is a Syslog Daemon for Windows. It receives, filters, logs, displays and forwards Syslog messages from hosts such as routers, switches, and for our purposes, SmoothWall Express 2.0.
Kiwi Syslog Daemon, while not open source, is available for a very reasonable fee and worth every dime. While it is available as freeware, the freeware version is limited and will only log to file without ODBC functionality necessary for the purposes of this paper. Widely diverse configuration options exist in Kiwi but this

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

paper will focus exclusively on logging to a MySQL database.

Prepare for a SMaK - Installation and Configuration

Preliminary Steps

Where your SmoothWall lives in your network infrastructure is obviously critical if it is to be successful in its purpose. The simplest configuration places the SmoothWall between your router and your backbone switch. See Figure 1 below. An excellent source of basic firewall information can be found at http://cc.uoregon.edu/cnews/spring2002/firewall.html.

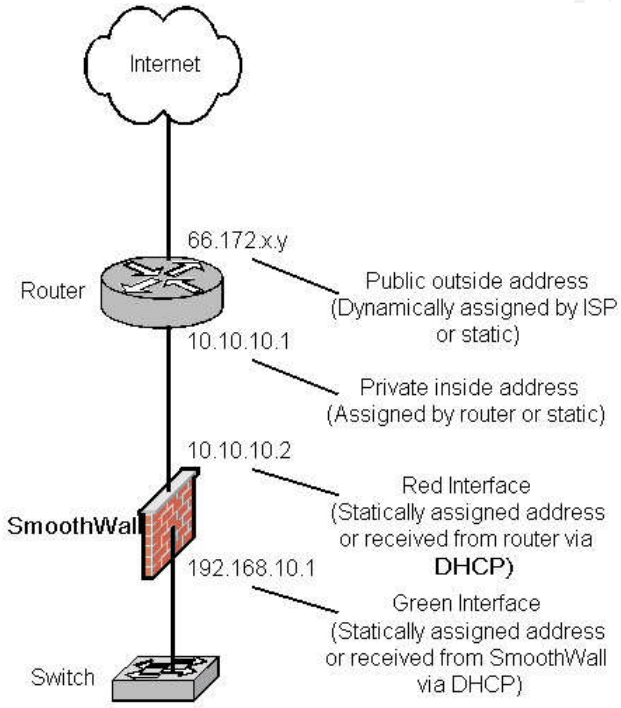


Figure 1

SmoothWall Express 2.0 Installation

The installation begins with Smoothwall as it provides the critical ingredient in the bundle this paper focuses on. Smoothwall maintains remarkably good installation and administration guides on their website so for purposes of this document we'll focus only on an installation overview with relevance to the proposed bundle. See http://smoothwall.org/docs/ for all documentation relevant to installing and administering SmoothWall 2.0.
SmoothWall issues it's installation as an iso available for download also on its website.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

1) Once you have the iso downloaded and burned to CDR, boot to it on the host dedicated to the Smoothwall implementation. The install process is rather direct and simple but requires some planning when arriving at the NIC setup and address scheme. Numerous configuration options exist denoted in color arrangements like modem as RED, inside NIC as GREEN and DMZ NIC as ORANGE. The author's configurations have typically been outside NIC RED and inside NIC GREEN. A three NIC scenario is necessary or recommended when your configuration includes outward facing servers like those offering web or email services.
2) If one's ADSL modem issues inside addresses via DHCP then allow the red NIC to configure dynamically. Typically SmoothWall's inside green NIC can offer protected hosts addresses via an inside DHCP scope as well or they can be assigned statically on each client. A typical ADSL modem might issue Class A private addresses (10.10.10.x) so the inside scope or static scheme should be a Class C private subnet (192.168.10.x).
3) Regardless, be sure to document accordingly to avoid later confusion. After rebooting, the Smoothwall implementation can be further configured via its browser interface. [6]

SmoothWall Express 2.0 Configuration

Once SmoothWall is installed and available on your LAN, access to it occurs via your web browser with a syntax of http://<smoothwall hostname or ip>:81 or https://<smoothwall hostname or ip>:441. Utilizing the Secure Socket Layer (SSL) over port 441 is recommended. SmoothWall modified its default ports to 81 and 441 as opposed to 80 and 443 as an added security measure.
The first step you should take is navigating to Services then Intrusion Detection System, check the box next to Snort and save the configuration. This will allow you to monitor more aggressive attacks in the IDS view under Logs.
The second step you should take is to select the Networking tab then Advanced and check the boxes for the following (See Figure 2): [7]
Block ICMP Ping – Prevents SmoothWall Express from responding to PING messages, from either the Internet or from the local (Green) network. Like SYN attacks described below, Denial of Service attacks can include flooding a box with PING messages.
Block and ignore IGMP packets – If your log files contain lots of spurious messages referring to IGMP packets, then enabling this option will allow SmoothWall to ignore these packets and not log them. This problem is often seen with cable modems.
Enable SYN cookies – Defends SmoothWall against SYN Flood attacks. A SYN Flood attack consists of a huge number of connection requests (SYN packets) to a machine in the hope that it will be overwhelmed trying to make so many connections. SYN cookies are a standard defense mechanism against this attack, the goal being to avoid a Denial of Service (DoS) situation where the machine is too busy to do any real work.
Block and ignore multicast traffic – Certain ISPs configure their users to receive multi-cast messages on network address 224.0.0.0. Checking this option

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

will block multi-cast messages and stop them being logged which can otherwise fill the log files with useless entries.
Don't forget to click the Save button to record any changes.[8]

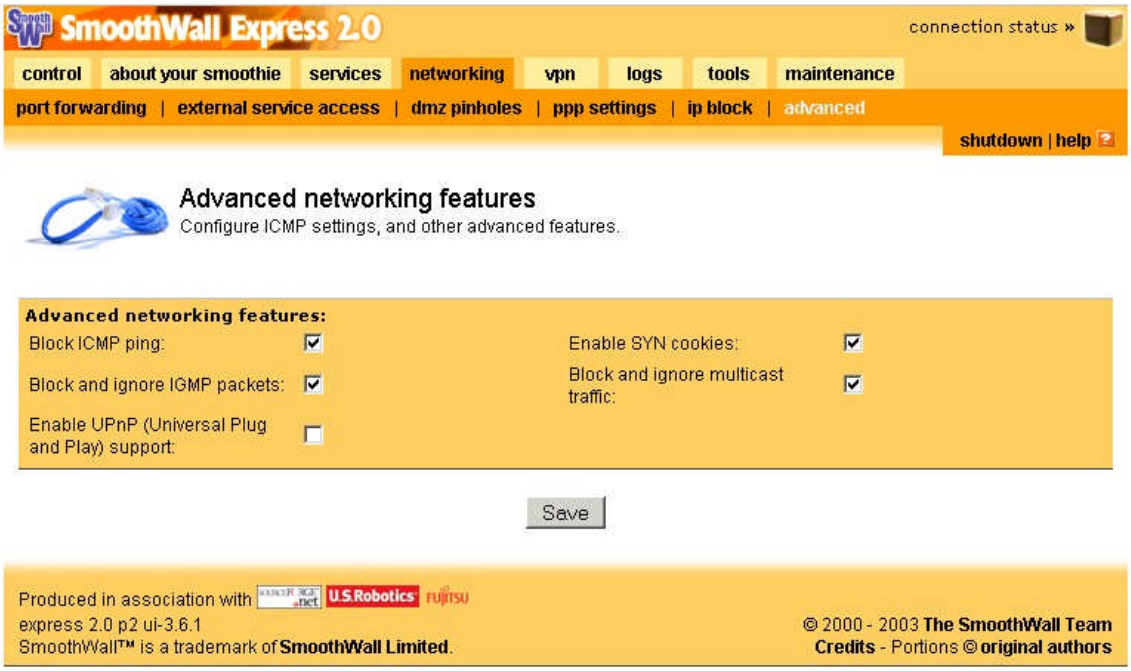


Figure 2

MySQL 4.0 Installation and Configuration

MySQL's installation and administrative manual is a 1276 page behemoth that need not be recited word for word here. Download the pdf at
http://dev.mysql.com/get/Downloads/Manual/manual.pdf/from/pick
A brief installation overview follows with relevance to this package set.

1) Navigate to http://dev.mysql.com/downloads/mysql/4.0.html and download the 4.0 package for Windows. It is recommended for ease of installation that you download the package with the installer.
2) It is imperative that you also download the ODBC driver installer *MyODBC-standard-3.51.07-win.exe*. MySQL is quite useless without it. Go to http://dev.mysql.com/downloads/connector/odbc/3.51.html and download the Driver Installer. Stash the ODBC .exe in the *mysql-bins* directory you will make in the next step.
3) Create a directory called *mysql-bins* and unzip the installer there.
4) Be sure you are logged in to an account with administrator privileges. Navigate to the *mysql-bins* directory and execute the ODBC Driver Installer first. Accept the license, hit next and it will finish. Reboot at this time.
5) Navigate to the *mysql-bins* directory and click the Setup file. Accept defaults unless you're installing to a drive other than C:.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

5) As described earlier in this document it is suggested that MySQL be installed on an NT platform in order to allow installation as a service. After installed drill down to *mysql\bin* and execute *mysqld.exe*

Typically the MySQL installer will create at *x:\mysql* directory (x representing your drive letter of choice). The *bin*, *data* and *lib* subdirectories will also be installed. Often an administrator may wish to change installation methodology i.e. binaries on the system drive and database on the data drive. As an example, after the initial installation move *c:\mysql\data* to *d:\mydata* then modify the *my.ini* file to point MySQL to the correct directory. The *my.ini* entry may look as follows:

```
[mysqld]
# set basedir to your installation path
basedir=D:/mysql
# set datadir to the location of your data directory
datadir=D:/mydata/data
```

Windows pathnames are specified in option files using forward slashes rather than backslashes so if you do use backslashes you must double them.
The WinMySQLAdmin tool will also allow you to modify the *my.ini* file and can be found in the bin directory where you installed MySQL.[9]
It is recommended and may be necessary to add two directories to your path environment in order for executable and libraries to be found easily. In order, click Start-Settings-Control Panel-System-Advanced-Environment Variables. Under System Variables highlight Path and select Edit. Add *x:\mysql\bin* and *x:\mysql\lib\opt* remembering to separate all additions with a semicolon.
Important:
Modify the root password on the new MySQL install immediately. From the command prompt issue **mysqladmin –u root password *new_password***
It is also suggested that you add a user that you use to administer your kiwi_syslog database. Do so by executing the following commands:

1) Login with your newly established root password by typing **mysql -u root –p** and enter your password
2) Type **grant all on kiwi_syslog.* to *newuser*@localhost identified by '*password*';**[10] Exit by entering \q at the mysql> prompt.
3) Type **mysqladmin –u root –p create kiwi_syslog**. After entering your password this will create a MySQL database called “kiwi_syslog" For a full list of commands, type "mysqladmin".

The MySQL Pocket Reference by George Reese from O’Reilly is an excellent guide for instant reference to commands, syntax and examples.

MySQL Control Center

MySQL also offers an excellent GUI for point & click administrative ease. If you seek functionality beyond the command line the Control Center will allow you to execute interactive queries with a syntax-highlighting SQL editor, perform database and table management as well as server management. See http://www.mysql.com/products/mysqlcc/ to download MySQLCC.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Kiwi Syslog Daemon Installation

1) Download the Kiwi Syslog Daemon from http://kiwisyslog.com/software_downloads.htm. Be sure to download the Service version as you will certainly want to run the sylogger as a service. While there, from the same view where you downloaded the installer be sure to Request a Trial Key until you're ready to purchase or upgrade to the full version. Without the Trial Key full functionality will not be available and you will be unable to log to a MySQL database. Also while in the same browser window scroll down and download the Kiwi Log Viewer for easy log viewing. Other tools are also available for free or a reasonable fee.
2) Execute Kiwi_Syslogd_Service.exe and accept all defaults unless you wish to put the daemon on a different drive.

Refer to the next section, **Configuring Kiwi to Log to MySQL** for the next Syslog steps.

Configuring Kiwi to Log to MySQL

The guide below assumes that you already have both MySQL and MyODBC installed on the system. It also assumes that you are logging to the localhost. These details can be found at www.kiwisylog.com. See graphic below.
You created the database to store your table in during the MySQL installation.

- Open Kiwi Syslog Daemon.
- Open the Properties setup window (Ctrl-P)
- Right-click Action and select Add Action
- Create a "Log to ODBC database" action
- From the right hand action settings pane, press "ODBC Control Panel"
- Press the System DSN tab
- Press the "Add" button and select the MySQL ODBC driver from the list and press the "Finish" button.
- Enter a Data Source Name, for example "Syslog"
- Enter the Database Name, "kiwi_syslog"
- Enter the name and password of the user you created and granted permissions to the kiwi_syslog database in the **MySQL 4.0 Installation and Configuration** section
- Press the "Test Data Source" button. You should receive a message stating that it connected correctly.
- Press "OK"
- Press "OK"
- Now back on the Kiwi Syslog Daemon setup page, press the "Browse" button.
- Select "Syslog" from the list and press "OK".
- Select "Kiwi MySQL format ISO yyyy-mm-dd" from the Database

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

type/field format dropdown box. This step is essential or you will see a syntax error message.

- Now press the "Create table" button. This will try to connect to the database and create the table called "Syslog" in the database specified by the DSN string. If that was successful then you now have a table ready to receive the syslog messages.
- Press the "Test" button a few times to log some test messages. This should show the green tick beside the Test button if successful.
- Now press the "Query table" button. This will read the last 5 lines from the database and show you the values as well as the database field format information. You can now press the "OK" button on the properties window to close it and accept the changes. The next time a message is received, it will be logged to the database. If the create table button or test button gives an error, it will mean that the program can't contact the database via the ODBC DSN. You will need to check the specified DSN is correct. A system reboot may also help.[11]

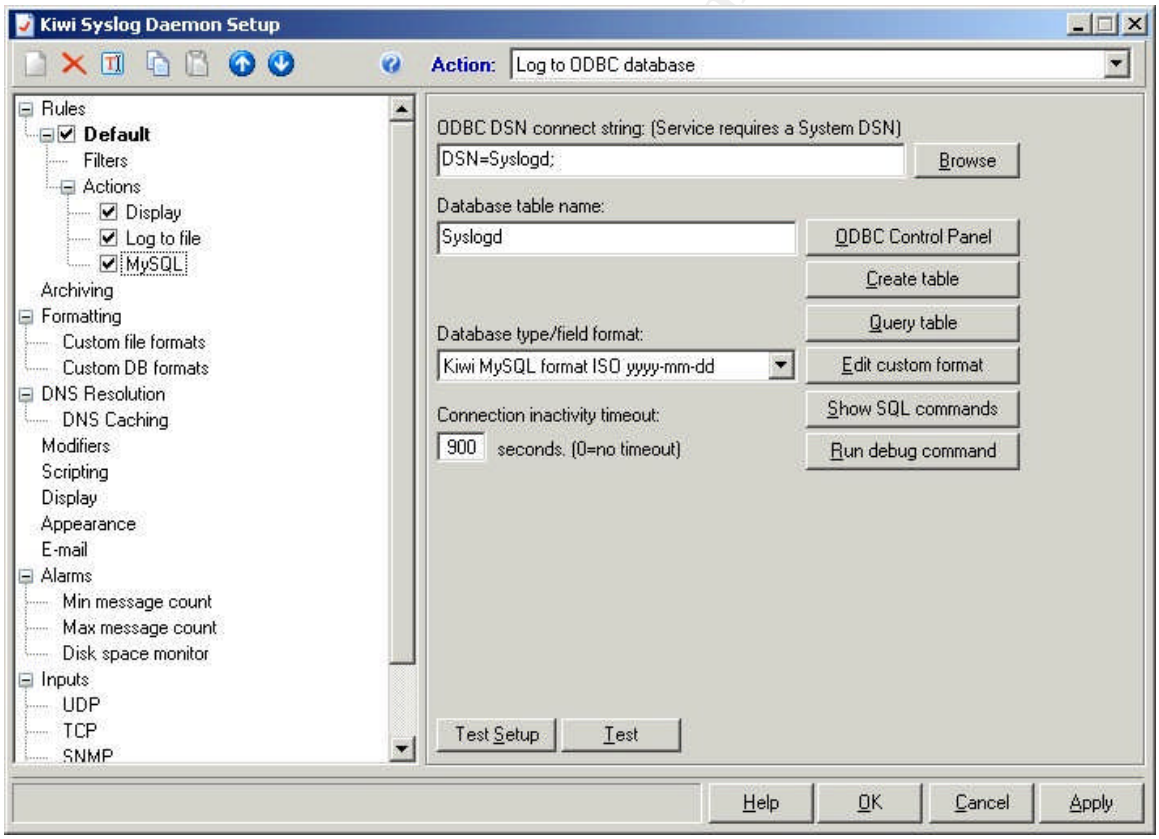


Figure 3

Configuring SmoothWall Express 2.0 to log to Kiwi Syslog Daemon

SmoothWall must be configured so that it logs to your Kiwi Syslog Daemon. To do so, open a shell to your SmoothWall. This can be from the web interface or SSH to your SmoothWall machine using port 222. Change to /etc (cd /etc). Edit syslog.conf (vi syslog.conf) and add

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

kern.* @192.168.1.xxx
to the end of syslog.conf. @192.168.1.xxx is the IP address of the machine that is running Kiwi Syslog Daemon. Be sure to use tabs and not spaces between kern.* and @192.168.1.xxx. Save and exit. Close the shell and restart SmoothWall.[12] See **Configuring Kiwi to Log to MySQL** below for further details on that process.
Keep in mind that once SmoothWall is configured to log to the Kiwi/MySQL server it is important to avoid downtime on the Kiwi/MySQL server. When SmoothWall attempts to log to an unavailable server it can quickly bog down.

Configuring SmoothWall Express to Drop Logging on Noisy Traffic

There a few steps you can take to quiet down some of the chatter logged by SmoothWall with a few additions to the firewall configuration files.
Log in to your SmoothWall locally or via SSH keeping in mind that as you enable changes you may be disconnected. First, stop logging hits on TCP port 135 (likely from the Blaster worm).
Remember that SmoothWall will still block all incoming traffic on port 135 - it's just not logging the hits anymore.

Edit /etc/rc.d/rc.firewall.up and immediately after the line containing

/sbin/iptables -P OUTPUT ACCEPT

Insert the following

 # drop hits from Blaster worm
/sbin/iptables -A INPUT -p TCP -i $RED_DEV --dport 135 -s 0/0 -j DROP

You can stop logging NetBIOS hits on UDP port 137 as well. Again, note that SmoothWall will still block all incoming traffic on port 137 - it's just not logging the hits anymore.

Edit /etc/rc.d/rc.firewall.up and immediately after the line containing

/sbin/iptables -P OUTPUT ACCEPT

Insert the following

 # drop netbios traffic
/sbin/iptables -A INPUT -p UDP -i $RED_DEV --dport 137 -s 0/0 -j DROP

There are further details on blocking additional traffic, particularly outbound, on Martin Pot's website, http://martybugs.net/smoothwall/iptables.cgi as well as other helpful relevant information about modifying SmoothWall. [13] This methodology works quite nicely for any traffic you may wish to no longer log. Simply modify the protocol (TCP or UDP) as well as the dport reference.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

You've Been SmaKd - Analyzing the Data

Smoothwall

Logs can be viewed using the SmoothWall 2.0 interface via https://*smoothwall*:441 with SmoothWall representing the name or IP of your SmoothWall host. From the index page select log and prepare to login with the admin account.
Once at the log page you can view both firewall entries and Intrusion Detection hits.

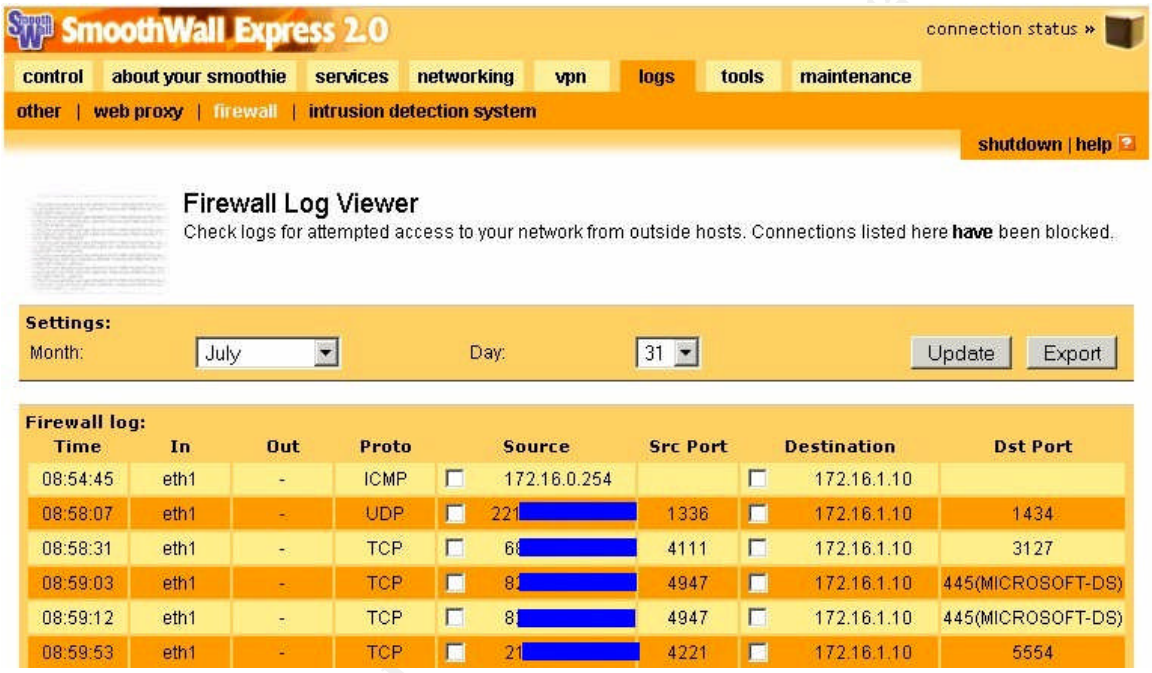


Figure 4

Kiwi Syslog Daemon

Kiwi logs to a text file that by default can be found in C:\Program Files\Syslogd\Logs\SyslogCatchAll.txt

Kiwi offers a useful log file viewer free of charge from its website that you should have downloaded when you retrieved the syslog daemon. For a quick snapshot this tool works nicely but to truly review some data you need to query the database.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

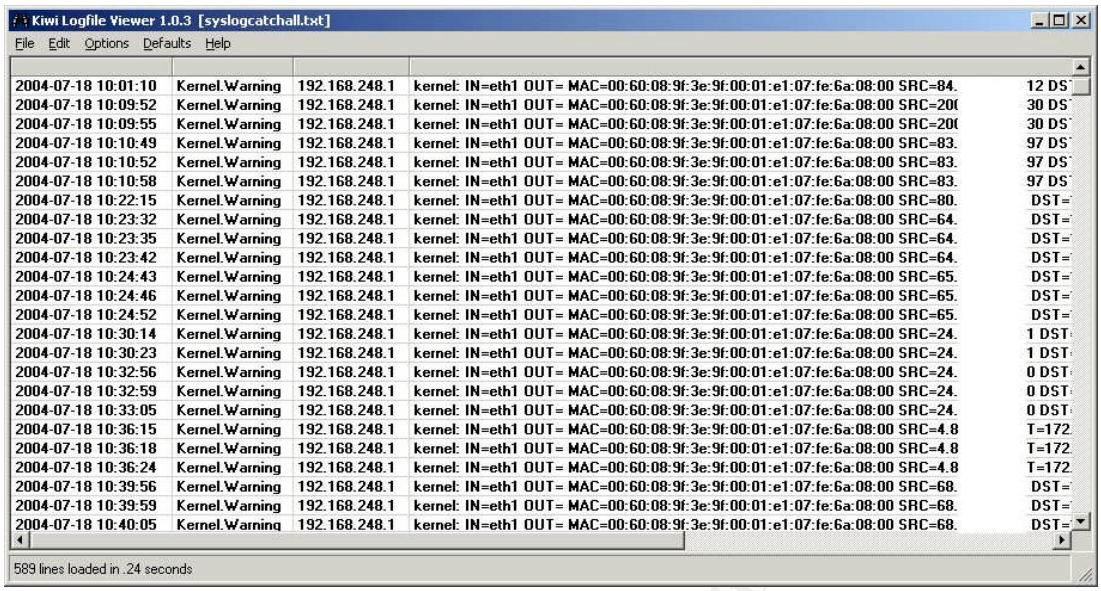


Figure 5

Querying the MySQL Database

Even the most basic query can yield valuable information or sort the data in more discernible lots. The following examples can be executed from the command line after you've typed **mysql –u *username* –p** then **use kiwi_syslog**. Remember to follow all queries with a semicolon. Additionally, refer to http://www.cs.wcupa.edu/~rkline/mysqlEZinfo/basic_commands.html for some basic syntax reference. Remember the MySQL Pocket Reference as well.
a) mysql> **SELECT * FROM syslogd WHERE MsgDate = '2004-05-25';**
This query would then generate all the results logged May 25th.
b) mysql> **SELECT * FROM syslogd WHERE MsgText LIKE '%24.x.y.211%';**
Adding **INTO OUTFILE 'file_name'** will send the query to a text file.
However, if you're more comfortable with a GUI and you've installed MySQL Control Center as described on page 10 you will be also be able to save the results quite easily for additional dissemination or analysis.

Situational example: You've discovered that you are getting extensive hits on different ports from a specific IP address. You run *whois* from SmoothWall and discover that the address belongs to your fiercest competitor. After few more hours of monitoring and data capture you approach your supervisor. As the manager of a competitive financial services company, she, too, is quite concerned. She asks you to give her substantial data exemplifying the probe or attack attempt from the last 24 hours so she can begin legal proceedings to thwart the affront. You open MySQL Control Center and issue a query by typing Ctrl-Q or clicking on the SQL button in the Console Manager. Assuming the date of the bad traffic is July 15th, 2004 you could issue the following:
SELECT * FROM syslogd WHERE MsgDate = '2004-07-15' AND MsgText LIKE '%66.x.y.28%';[14]
This query would report back all logged entries from IP address 66.x.y.28 on July 15th. If you right-click anywhere in the query result and select Save Results you

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

will have generated an instant and legible report for your supervisor.

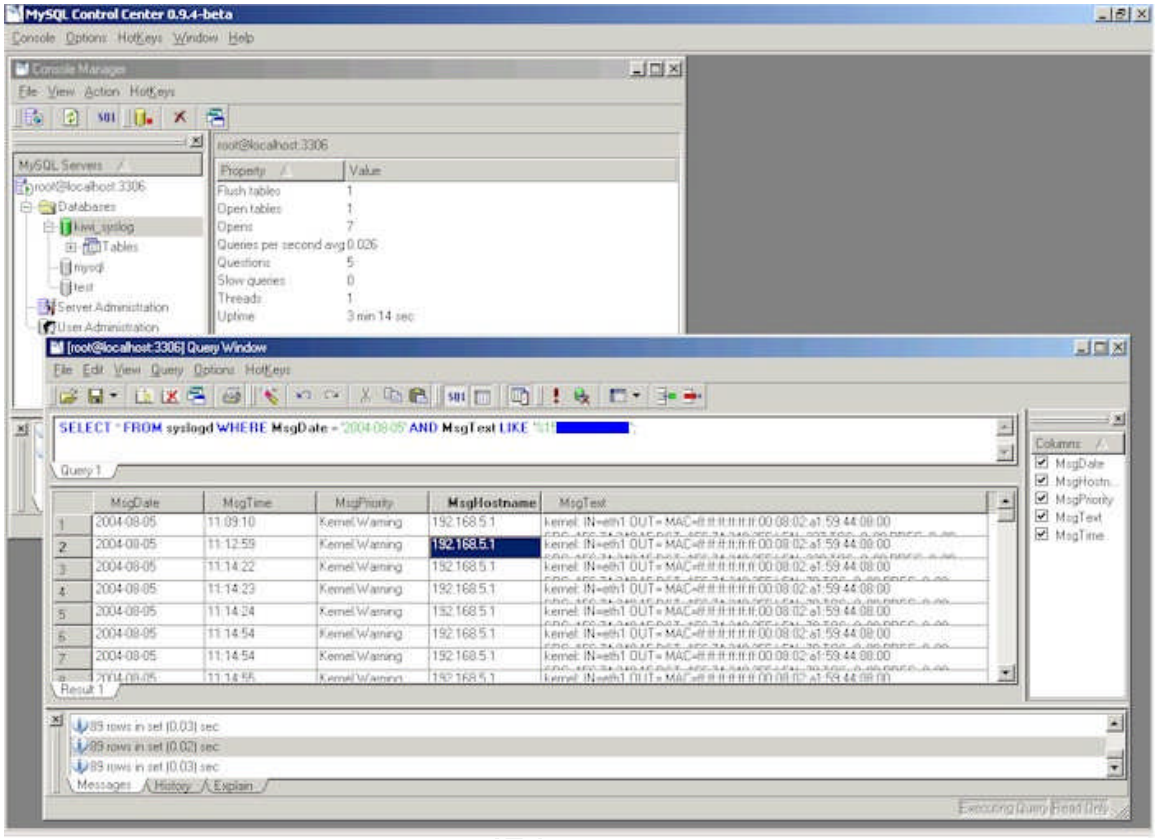


Figure 6

What Does The Data Mean?

Interpreting and analyzing firewall logs can be a full time job unto itself and can be imposing to say the least. The following is a simplified approach to understanding what you're looking at as well as key elements to look for. Each listing provides a link to a relevant website that details matching information.

You will see log entries referring to **UDP port 137** perhaps more than any other.[15] These are NetBIOS hits and are typically so noisy it is suggested to drop logging them as described in the section **Configuring SmoothWall Express to Drop Logging on Noisy Traffic.**
http://www.robertgraham.com/pubs/firewall-seen.html#10

Port 1434 shows up on occasion and likely indicates the MS-SQL Slammer worm. [16]
http://xforce.iss.net/xforce/alerts/id/advise140

ICMP ping type 12 is probably not a friendly visit either. Type 12 typically indicates a fingerprinting attempt, which is an effort to determine what operating system you are running.[17]
http://www.robertgraham.com/pubs/hacking-dict.html#fingerprint

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Sasser will generate traffic on **ports 445, 5554 and 9996**.
A machine infected with **Phatbot/Agobot** has been known to scan some of the following TCP ports in rapid succession (and not necessarily this order): **2745 1025 80 3127 6129 1433 5000 445 443 135**.
The Windows **RPC/LSASS (MS04-011)** remote exploit is an attack against lsasrv.dll. In addition to **TCP 1025**, the following ports are vulnerable to the LSASS exploit: **TCP 135, 139, 445, and 593. UDP 135, 137, 138, and 445**.[18]
http://isc.sans.org/diary.php?date=2004-04-30

You likely get the point by now. Your traffic patterns may show different tendencies but the concern is the same. Firewalls and IDS are employed for a plethora of obvious reasons. There be dragons here!

Probes to ports that have no services running on them: When hackers consider installing backdoor Trojans, they determine which ports you're already using for running services. If you see a lot of probes to ports not in use, look up the port and find out what they're used for and verify that you're protected.
Unsuccessful access attempts to your firewall and/or other high-profile systems: If you notice repeated unsuccessful attempts to access your firewall and other systems from one IP address (or group of IP addresses), then you might want to configure SmoothWall to drop all connections from that IP space (making sure that the IP address isn't being spoofed). Go to Networking then IP Block via the browser interface to terminate the perpetrator.
IP addresses of the connections that are being rejected and dropped: If an IP address is spoofed, you won't be able to find the owner. Otherwise, you should resolve the domain using the *whois* tool on your SmoothWall, contact the owner, and find out why someone from their IP space is trying to attack your systems. To use whois navigate to Tools and the IP Information tab from your browser view.
Suspicious outbound connections: Outbound connections coming from internal servers such as your Web servers could be an indication that a hacker is using your systems to launch attacks against other organizations or individuals.
External packets with internal IP addresses: Packets with a source address internal to your network that originate from outside your network indicate that a hacker is spoofing your internal addresses to attempt to gain access to your internal network. [19]
See Michael Mullins' *Best practices for managing firewall logs* on Zdnet for more.
http://www.zdnet.com.au/insight/0,39023731,20265680,00.htm

Archiving and Maintaining Data

SmoothWall Express 2.0

SmoothWall logs live in */var/log*. Current firewall messages are found in a file called *messages*. Intrusion detection entries are found in the */var/log/snort* directory and are organized in individual directories named for the offending IP as well as in a file called *alert*.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

You may see files like messages.1 as well as messages.2.gz or alert.1.gz. SmoothWall compresses it's logs automatically after they reach a certain size. You can choose to backup the compressed files to whatever storage platform you utilize or delete them after a period. Be sure you are not violating any policies in deleting these files as they could aid you greatly in the forensic analysis of a network compromise.
Keep in mind that if you're logging a lot of traffic these files will grow. If you opted to use an older PC for your SmoothWall instance the hard drive may not be that large and could become cluttered quickly so moving the compressed archive to a storage system may be necessary.

Kiwi Syslog Daemon

Kiwi offers excellent archiving tools to keep captures well organized and maintained.
Hit Ctrl-P to bring up the Kiwi Syslog Daemon Setup. Right click on Archiving and select Add New Archive Schedule. By default this will setup a daily archive under C:\Program Files\Syslogd\Logs in directories named by date following the YYYY-MM-DD convention. All these settings can be modified per your preferences.

MySQL 4.0

Backing up your MySQL database is a straightforward process best done utilizing the **mysqldump** command. As an example, use the following syntax:

> mysqldump -u [username] -p [password] [databasename] > [backupfile.sql]
>
> - [username] - this is your database username
> - [password] - this is the password for your database
> - [databasename] - the name of your database
> - [backupfile.sql] - the file to which the backup should be written.

The resultant dump file will contain all the SQL statements needed to create and populate the table in a new database server. To backup your database 'kiwi_syslog' with the username 'kiwiadmin' and password 'pass21' to a file kiwi_syslog.sql, you would issue the command:

mysqldump -u kiwiadmin -p pass21 kiwi_syslog > kiwi_syslog.sql

Restoring your database is just as easy. Execute the command:

mysqldump -u kiwiadmin -p pass21 kiwi_syslog < kiwi_syslog.sql

An excellent article at http://www.devshed.com/c/a/MySQL/Backing-up-and-restoring-your-MySQL-Database/ will further enlighten you on caring for your MySQL database.[20]

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Alternative Considerations

This package can also be matched on the Linux platform with SmoothWall 2.0 on one host and a distribution like Fedora Core 2 running MySQL, syslog and logwatch or logdog on another. Additionally, an Apache server with PHP enabled will yield excellent web and browser based reporting, properly configured. Your Linux skills need be fairly refined to implement an installation of this nature but the results can be highly rewarding. See discussions on LAMP (Linux, Apache, MYSQL and PHP) at:
http://www.onlamp.com/pub/a/onlamp/2001/01/25/lamp.html.

Conclusion

The premise that a complete enterprise-worthy security solution need be expensive, difficult to maintain and monitor, and beyond reach of the small business is shortsighted. SMaK is intended to provide a budget conscious, security minded SOHO or SMB with all the tools necessary to protect their enterprise, understand their attacker, protect their information, be proactive or react accordingly. No connection to the Internet should ever go unprotected, and as a business grows protecting the internal network becomes all the more essential. According to a UC Davis study by Frank Bernhard in 2000, security gaps cost business 5.7 percent of annual revenue.[21] SMaK is certainly not the only solution; the list of excellent appliance and software possibilities are endless. But with a small investment and the time necessary to implement SMaK your business can begin to seal the “economic leakage” referenced in Bernhard’s study.
What is the cost of compromise to a business?
In some cases it can mean closing the doors.
The lesson?
Don’t leave the wrong door open.

In making tactical dispositions, the highest pitch you can attain is to conceal them.
- Sun Tzu

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

References

[1] The SmoothWall Open Source Project. SmoothWall 2.0 Express Installation Guide, www.smoothwall.org, 2003

[2] Kiwisyslog.com. "System requirements to run Kiwi Syslog Daemon." 2002-2004
URL: http://www.kiwisyslog.com/faq/syslog/syslog_minimum_requirements.htm

[3] MySQL AB. MySQL Reference Manual, Section 1.2, www.mysql.com, 1997-2004

[4] The SmoothWall Open Source Project. SmoothWall 2.0 Express Installation Guide, www.smoothwall.org, 2003

[5] MySQL AB. MySQL Reference Manual, Section 1.2, www.mysql.com, 1997-2004

[6] The SmoothWall Open Source Project. SmoothWall 2.0 Express Installation Guide, www.smoothwall.org, 2003

[7] The SmoothWall Open Source Project. SmoothWall 2.0 Express Administrator's Guide, www.smoothwall.org, 2003

[8] The SmoothWall Open Source Project. SmoothWall 2.0 Express Administrator's Guide, www.smoothwall.org, 2003

[9] MySQL AB. MySQL Reference Manual, Section 2.2.1.3, 77, www.mysql.com, 1977-2004

[10] Reese, George. MySQL Pocket Reference, Sebastopol, O'Reilly 2003, 49

[11] Kiwi Enterprises. "How do I log to an MySQL Database?" 2002-2003
URL: http://www.kiwisyslog.com/faq/syslog/syslog_mysql_logging.htm

[12] Dshield.org. "SmoothWall Using Kiwi Syslog Daemon." 7 August 2004
URL: www.dshield.org/clients/cvtwinfirewalls.php#kiwi_smoothwall

[13] Pot, Martin. "Adding iptables Rules." 4 August 2004
URL: http://martybugs.net/smoothwall/iptables.cgi

[14] Butcher, Anthony. Teach Yourself MySQL in 21 Days, Indianapolis, SAMS, 2003, 128-154

[15] Graham, Robert. "Firewall Signatures." 2004
URL: http://www.robertgraham.com/pubs/firewall-seen.html - 10

[16] Internet Security Systems. "Microsoft SQL Slammer Worm Propagation." 25 January 2003
URL: http://xforce.iss.net/xforce/alerts/id/advise140

[17] Graham, Robert. "Fingerprint defined." 2004
URL: http://www.robertgraham.com/pubs/hacking-dict.html#fingerprint

[18] Sachs, Marcus H. "Handler's Diary April 30th 2004." 1 May 2004
URL: http://isc.sans.org/diary.php?date=2004-04-30

[19] Mullins, Michael. "Best practices for managing firewall logs." 3 June 2002
URL: http://www.zdnet.com.au/insight/0,39023731,20265680,00.htm

[20] Thomas, Vinu. "Backing Up and Restoring Your MySQL Database." 15 June 2004
URL: http://www.devshed.com/c/a/MySQL/Backing-up-and-restoring-your-MySQL-Database

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

---

[21] DeLong, Daniel. “Hackers Said To Cost US Billions.” 8 February 2001
URL: http://www.newsfactor.com/perl/story/7349.html

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.