Global Information Assurance Certification Paper

GIAC Security Essentials Certification (GSEC)
Practical Assignment v1.4c (Option 1)
submitted October 18, 2004
Brian Spindel

Capturing and Analyzing SOHO Router/Firewall Logs

Table of Contents

Abstract

This case study is meant to show home and small office/home office (SOHO) network users that commonly-used security precautions do not completely protect them from malicious activity, and that by capturing and periodically reviewing their router logs, they can understand what's occurring on their network. Using this ability to view the activity occurring on their network then becomes another layer of protection in a defense-in-depth approach to network security, and can help direct additional protective efforts toward design aspects or users of their network that are making them unnecessarily vulnerable to malicious activity. We walk through creating a logging facility, archiving and sorting logs entries, identifying most-commonly seen traffic, and responding where a security incident is identified.

The Problem

More and more home and SOHO users receive broadband Internet access through subscription to cable or DSL (digital subscriber line) providers. The relatively high data transfer rate is the biggest benefit, but the ability to share that high-speed access among multiple users leverages the subscription cost. Adding a SOHO router behind the cable/DSL modem allows one to share high-speed connection with many other users.

However, broadband connectivity is not without drawbacks. Its always-on design increases opportunities for attackers to target a home network. The always-on connection, static or infrequently changing external IP (Internet Protocol) address[1], high connection speed, and lack of any protective measures employed by Internet security providers (ISP) all make your computer a more likely target for malicious activity than it might have been with a dial-up connection.[2]

To help mitigate this exposure, SOHO users can use two basic premises of network security, 'Defense in Depth' and 'Know Your Network.'

The 'defense in depth' premise recommends that to effectively secure information assets, one must deploy countermeasures in multiple locations with multiple layers. Business networks also typically use broadband connections, but are much more likely to be protected by defense-in-depth, i.e., using many layers of security, ranging from network firewalls to encryption. In addition, they usually have support staff who maintain the security and availability of these network connections.[3]

SOHO broadband users, at the very least, should have these protective measures in place:

- Run anti-virus software on every computer, using up-to-date signatures and the software's automatic signature update function.
- Use the most current version of their browser, email client, operating system software on every computer.
- Use a SOHO router with Network Address Translation (NAT)[4] feature to hide the IP addresses of hosts on the SOHO network.

However, even with these measures in place, home/SOHO users are still vulnerable to attackers who use backdoors, malicious code, and crafted packets to gain access to their network.

The 'know your network' premise of network security suggests that one must know what equipment is attached to their network, what services that equipment is providing, and what vulnerabilities are associated with those services. It is very simple, using the tools available today, to run port-scanning and vulnerability assessment tools to better understand your network's vulnerability profile. For example, Symantec and other sites offer free, on-demand security checks to identify open ports.[5]

By adding a practical way to capture and analyze router logs, the SOHO user add yet another layer to their defense-in-depth approach to their network's security. Without such a system, SOHO users also cannot “know their network.” They are blind to what's happening at the interface of their network and the Internet, and are therefore likely have false confidence that

their anti-virus software and router are sufficiently protecting them from malicious activity, and also would not know it when such activity is taking place.

Using some simple log-capturing software installed on a used, under-powered Windows system, SOHO users can take advantage of the logging abilities built in to most routers to produce a fairly sophisticated network traffic analysis and security event notification system. I show how to install such a logging system, review some of the types of traffic the logs could contain, and discuss how to respond should certain types of unexpected traffic be detected. By collecting and analyzing log files, you can glean useful intelligence about the activity on your network:

- whether computers are infected with spyware; if they are, you'll likely see content being regularly retrieved from websites you'd never heard of or without your request,
- which computers are properly updating their anti-virus signatures, as you'll see traffic indicative of your computers getting updates,
- whether computers are infected with a BotNet[6], as you'll see a spike in IRC[7] traffic,
- presence of an e-mail virus, as you'll see spikes in your outgoing mail connections.[8]

A Solution

Some straightforward steps were required to create a logging facility:

1.) Set up a SOHO network using a router (assumed done before this project). The router assigns the 192.168.1.x IP addresses and the cable/DSL Internet service provider (ISP) assigns the router's external IP:

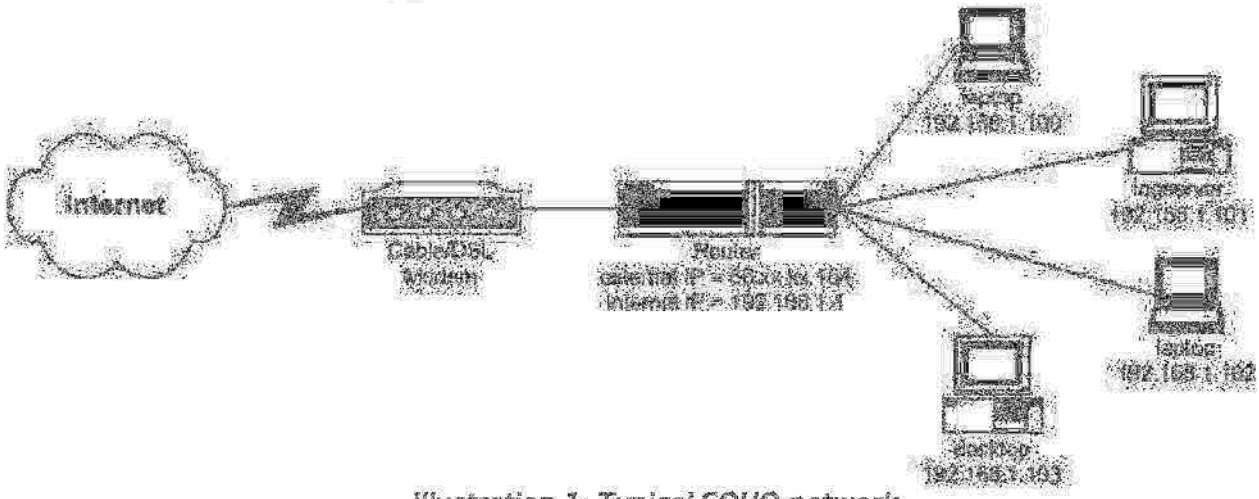

Illustration 1: Typical SOHO network

Note that not all popular SOHO routers can log traffic, and of those that do use different protocols to report logged traffic by broadcasting logs to any log-capturing program listening on the internal network:

router/info	logging protocol
Cisco SOHO 71 Broadband Router[9]	syslog (UDP/514)
D-Link Express EtherNetwork DI-604 Router[10]	NO LOGGING
Linksys BEFSR41EtherFast® Cable/DSL Router[11]	snmp (UDP/162)
Netgear RP611 4-Port Cable/DSL Router[12]	syslog (UDP/514)
SMC7004ABR Barricade 4-Port 10/100Mbps Broadband Router[13]	NO LOGGING

Although most SOHO routers *can* log traffic, logging may be turned off by default.

2.) Obtained hardware to create a log server.

I obtained a used PC. Most any dated hardware would make a good dedicated log server since little processing power or memory is required, but more than two total gigabytes of hard disk space is desirable.

3.) Installed an operating system on the hardware.

I installed Windows 2000 Professional operating system on the hardware. **** The operating system chosen is determined by the log capturing software chosen, which in turn is determined by the log transmission protocol used by the router. ****

I won't cover installing Microsoft Windows 2000 or any other operating system here, but I will take this opportunity to recommend some best practice steps for installing a secure Microsoft Windows operating system:

1. Use a licensed copy of the operating system.
2. Given that the computer is plugged into one of the Ethernet ports of your router, as soon as the operating system is installed, launch Windows Update and download and install all critical updates suggested before accessing any other Internet sites.
3. Install anti-virus software and update its virus signatures.
4. Install Mozilla Firefox browser[14] and, when asked, select to make it your default browser. Delete Internet Explorer icons from the desktop and Quick Launch menus to prevent accidental use of this vulnerable browser.

4.) Install a logging application.

There was also a choice to be made for log management software, and that choice would depend on the protocol the router uses to broadcast the logs and would dictate the operating system installed on the logserver:

logging application	operating system(s)	protocol(s) captured
checksyslog[15]	any system supporting Perl	syslog
Kiwi Syslogd Server[16]	Windows NT4, 2K, XP	syslog, SNMP, TCP
logsurfer[17]	any system supporting Perl	syslog
Somix Logalot[18]	Windows	syslog, SNMP
Swatch[19]	Linux	syslog
Tenshi[20]	any system supporting Perl	syslog
Wallwatcher[21]	Windows 98 and newer	syslog, SNMP

I decided to use the Kiwi Syslog Daemon because of its ability to collect SNMP-based logs[22] from my Linksys BEFW11S4 router/wireless gateway (and later, syslog-based logs from my Windows and Linux client machines). Its full-feature version in inexpensive, but I used the free version as it is quite feature-rich.[23]

5.) Configure the router to send logs to the logserver

Routers (that do log) broadcast their logs to the internal network where they can be captured by any logging application configured to listen for them. On a Linksys router,

1. Open your browser and type http://192.168.1.1 in the address bar.
2. Login as 'Admin' (default password is also 'admin', but we'll assume here that you changed the password when you set up the router for the first time).
3. Click 'Enable' Access Log.
4. In the 'Send Log to:' field, enter
   a) 192.168.1.255 to instruct the Linksys Router to broadcast its logging information to all systems on the LAN. This option is recommended, since most people use the DHCP service within their Linksys Router, which can change the IP address of their logging computer.

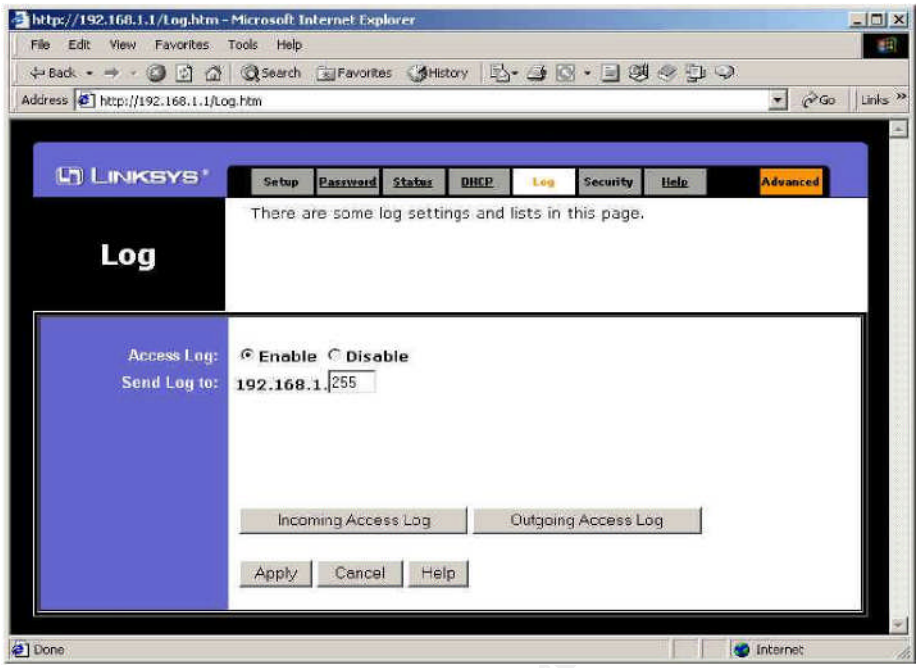

Illustration 2: Linksys BEFW11S4 Log configuration screen

b) the IP of the the system which is running the logging software (192.168.1.100 for example), if you are confident that the IP address isn't go to change. Otherwise the router may send your logging information to the wrong computer.

6.) (Optional: Configure other machines to send their logs to the logserver.)

You can configure your network's client computers to share their own logs with a central logging application. Doing this would better support investigation of questionable traffic because you can correlate what the router sees with what the client computers are doing. This level of investigation is beyond the scope of this case study.

Windows clients:

Purdue's Engineering Computer Network provides Eventlog to Syslog, a utility which simply outputs Microsoft Windows' Event Log messages to a syslog server.[24] It is free, and it is easy to install. You download the pre-compiled executable, unzip it. After unzipping the package:

1. Copy evtsys.dll and evtsys.exe to WINNT\system32.
2. Open a DOS prompt window (Start - Run - cmd.exe).
3. cd to that directory and run: evtsys -i -h [syslogserver], Where [syslogserver] is the name of your syslog server (without the brackets). This installs a registry entry for the service.

4. To start the Eventlog to Syslog service, right-click on My Computer, select Manage - Services. Locate the Eventlog to Syslog service. Start it now and set it to start automatically.[25]

Linux clients:

Linux client computers can also be configured to broadcast their logs to the listening log server. The necessary changes for the clients are within the /etc/syslog.conf file. For each appropriate entry in your syslog.conf (the ones that are writing to files), add an entry that sends them off to syslog server. Be careful with the file, it is sensitive to white space. You must use tabs between the fields. Here's an example:[26]

```
# Log anything (except mail) of level info or higher. #
Don't log private authentication messages!
*.info;mail.none;authpriv.none;cron.none        /var/log/messages
*.info;mail.none;authpriv.none;cron.none        @192.168.1.102
```

7.) Capture logs. Start

Kiwi Syslogd.

8.) Analyze logs.

From the start, some patterns of regular traffic were identifiable (along with some not-so-regular traffic. Both are discussed in the Results section of this case study.

Note that Kiwi Syslogd and other logging software can often be configured to define rules/criteria for filter log entries, send alerts when certain rules are met, and send periodic activity reports to reveal summaries of traffic types and volume. Some routers can also be configured to automatically email activity logs or summary reports to a specified recipient. These features are beyond the scope of this case study.

The Results

As soon as logging was enabled, traffic logs began accumulating in the log viewer interface of Kiwi Syslogd. Unfortunately, even within one day, a SOHO router may produce hundreds or even thousands of log entries. Our mission, now that we're capturing logs, is to search through these entries to differentiate 'noise' entries from those entries that may represent true security issues that require further investigation and response. Sorting the log entries will help us do that.

Log storage and review techniques

1. To enable log archiving, click the **Archiving** option in Kiwi Syslog setup. Saving records by week is recommended, or by day if you have a very

busy network.

2. Determine your internal IP addresses (run ipconfig.exe from a DOS command window on each Windows PC or run ifconfig on each Linux PC).
3. Determine your external IP address by browsing to http://www.whatismyip.com. That site will display your current external IP address.
4. Open any archived log file using Microsoft Excel or other spreadsheet as a tab-delimited file.
5. Sort the log records in that file by traffic direction (inbound/outbound), source IP address, and source port.

Right away, you will be able to see many, many unfamiliar source IP addresses with many source port numbers greater than 1024. You can also see that each of these entries is attempting to connect to YOUR external IP address. These entries represent the thousands of constant, indiscriminate attempts by worms and hackers using scripts and other tools to connect to any accessible PC. Further down the list, you'll begin to see records of the traffic that users on your network generated – the traffic you'd expect to see. The following sections illustrate in more detail how to recognize different types of network traffic.

Inbound traffic

Using the knowledge of your internal IP addresses, external IP address, and well-known TCP port numbers[27], network traffic appears to be either easily-recognized traffic associated with the SOHO network users' activity or with traffic of unknown or potentially malicious nature. I examined and share examples of each, as well as illustrate patterns that might be seen if a computer on my network were infected or if users on my network were doing dangerous things.

With every review of your router's logs, you will see a constant flow of other suspicious, potentially malicious traffic. The following edited excerpts of router logs show inbound traffic, where the log format is:

```
date time reporting_host direction source_host/port destination_host/port
```

Based on inbound traffic direction, destination port of my external IP address, and destination port of TCP port 22, it appeared that someone or some program was trying to connect to my external IP through the SSH service:

```
2004-08-08 18:43:05 192.168.1.1 @in 209.xx.xx.183 19478 66.xx.xx.164 22
```

A similar example, again with inbound direction to my external IP address, but this time to TCP port 23, appears to be someone or some program trying to connect to my network using the telnet service:

```
2004-08-08 18:56:36 192.168.1.1 @in 66.xx.xx.25 43829 66.xx.xx.164 23
```

More examples of similar connection attempts included traffic to TCP 111 (RPC service on *nix systems) and TCP 443 (https).

A different and very common traffic pattern noted can be identified as connection attempts using a spoofed source address. This connection attempt illustrates use of a spoofed source IP (the loopback address) to try to get any machine on my network to respond:

```
2004-08-05 14:56:50 192.168.1.1 @in 127.0.0.1 80 66.xx.xx.164 1379
```

Some flawed implementations of hardware router NAT (Linksys, in particular) will forward packets spoofed like this to a port on a (somewhat random) internal machine for a short time. The hacker could then attempt to open a socket on the port he just opened, but with a valid source address, allowing him to then gain access to that machine on the SOHO network.

There were also many attempts to connect to my external IP through TCP ports 1025 through 1029. Microsoft Windows assigns programs using RPC to these ports as they first available ephemeral ports, hackers/worms try connecting to these ports since they may well be open:

```
2004-08-07 05:03:17 192.168.1.1 @in 66.xx.xx.207 2239 66.xx.xx.164 1025
2004-08-07 05:03:20 192.168.1.1 @in 66.xx.xx.207 2239 66.xx.xx.164 1025
2004-08-07 05:03:26 192.168.1.1 @in 66.xx.xx.207 2239 66.xx.xx.164 1025
```

There were also many, many attempts by known worms[28] to connect to my external IP through these TCP ports that they target:

- 1434 (Microsoft-SQL-Monitor)
- 3127 (W32/MyDoom, W32.Novarg.A backdoor)
- 5554 ([trojan] Sasser Worm FTP Server)
- 6129 (DameWare Mini Remote Control vulnerability)[29]
- 9898 ([trojan] Dabber Worm backdoor).

Note the rapid timing and repeated use of certain port combinations, providing evidence that this is an automated scan:

```
2004-08-05 20:06:51 192.168.1.1 @in 66.xx.xx.97 4445 66.xx.xx.164 1025
2004-08-05 20:06:51 192.168.1.1 @in 66.xx.xx.97 4447 66.xx.xx.164 6129
2004-08-05 20:06:51 192.168.1.1 @in 66.xx.xx.97 4454 66.xx.xx.164 5554
2004-08-05 20:06:54 192.168.1.1 @in 66.xx.xx.97 4447 66.xx.xx.164 6129
2004-08-05 20:06:54 192.168.1.1 @in 66.xx.xx.97 4454 66.xx.xx.164 5554
2004-08-05 20:06:54 192.168.1.1 @in 66.xx.xx.97 4445 66.xx.xx.164 1025
2004-08-05 20:07:00 192.168.1.1 @in 66.xx.xx.97 4447 66.xx.xx.164 6129
2004-08-05 20:07:00 192.168.1.1 @in 66.xx.xx.97 4445 66.xx.xx.164 1025
2004-08-05 20:07:00 192.168.1.1 @in 66.xx.xx.97 4454 66.xx.xx.164 5554
```

All of these inbound connection attempts are indicative of scans to find these ports of interest accessible to the Internet. All of these scans were unsuccessful here as none of these services are running on my network and all of my client computers have non-routable RFC 1918[30] IP addresses.

Outbound traffic

Up to this point, we've focused on inbound connection attempts. Arguably more valuable, however, is review of outbound traffic. Yes, we've identified most of the threats aimed at out SOHO network, but review of outbound traffic could reveal evidence of *successful* exploits. Here are excerpts of router logs for outbound traffic that I initiated:

Surfing the web, where the source IP is that of one of my client machines, the source port is an ephemeral port,[31] the destination is a public website (hostname as resolved by Kiwi Syslogd) and destination port TCP 80 (http) or TCP 443 (https):

```
2004-08-08 21:13:54 192.168.1.1 @out 192.168.1.102 1306 www.google.com 80 2004-
08-08 21:13:54 192.168.1.1 @out 192.168.1.101 1176 engineering.purdue.edu 80
```

Checking email using POP3 protocol, where destination mail.earthlink.net is a mailserver and the destination port is TCP 110 (POP3):

```
2004-08-08 19:25:40 192.168.1.1 @out 192.168.1.100 32795 mail.earthlink.net 110
```

Downloading software from an FTP server, where destination mirror.cs.wisc.edu is an FTP server and destination port is TCP 21 (FTP):

```
2004-08-05 19:18:58 192.168.1.1 @out 192.168.1.100 32795 mirror.cs.wisc.edu 21
```

On the other hand, with my very first review of router logs, I noticed a recurring pattern of traffic that caused me to be concerned. Here is an edited excerpt of the router log. Based on the traffic's destination of port 25, (commonly used by the sendmail program) and a destination host of 'mx.aol.com,' which appeared to be an aol.com mailserver, the pattern looked like repeating attempts by a Linux laptop on my network to mail something to someone:

```
2004-08-05 15:33:56 192.168.1.1 @out 192.168.1.100 33205 mailin-04.mx.aol.com 25
2004-08-05 15:34:56 192.168.1.1 @out 192.168.1.100 33206 mailin-04.mx.aol.com 25
2004-08-05 15:35:56 192.168.1.1 @out 192.168.1.100 33207 mailin-04.mx.aol.com 25
2004-08-05 15:36:56 192.168.1.1 @out 192.168.1.100 33208 mailin-04.mx.aol.com 25
2004-08-05 15:37:56 192.168.1.1 @out 192.168.1.100 33209 mailin-02.mx.aol.com 25
2004-08-05 15:38:56 192.168.1.1 @out 192.168.1.100 33210 mailin-02.mx.aol.com 25
2004-08-05 15:39:56 192.168.1.1 @out 192.168.1.100 33211 mailin-02.mx.aol.com 25
2004-08-05 15:41:56 192.168.1.1 @out 192.168.1.100 33213 mailin-01.mx.aol.com 25
2004-08-05 15:42:56 192.168.1.1 @out 192.168.1.100 33214 mailin-01.mx.aol.com 25
2004-08-05 15:43:56 192.168.1.1 @out 192.168.1.100 33215 64.12.137.89 25
2004-08-05 15:44:56 192.168.1.1 @out 192.168.1.100 33216 64.12.138.57 25
```

```
2004-08-05  15:45:56 192.168.1.1 @out 192.168.1.100 33217 mailin-03.mx.aol.com 25
2004-08-05  15:46:56 192.168.1.1 @out 192.168.1.100 33218 64.12.137.152 25
2004-08-05  15:47:56 192.168.1.1 @out 192.168.1.100 33219 mailin-03.mx.aol.com 25
2004-08-05  15:48:56 192.168.1.1 @out 192.168.1.100 33220 mailin-03.mx.aol.com 25
```

This pattern repeated every minute, every few hours, for several days. After some investigation, I found that there was an undeliverable mail in the laptop's mail queue:

```
[bspindel@localhost bspindel]$ su
[root@localhost bspindel]# /usr/bin/mailq
/var/spool/mqueue (1 request)
 ----Q-ID-------Size -------Q-Time ----
 ----------Sende r/Reci pi ent--------
i721jhuS020381  116 Sun Aug  1 20:45 <bspindel@ISPname>
(Deferred: Connection timed out with mailin-02.mx.aol.com.)
<IntendedRecipient@ISPname>
Total requests: 1
[root@localhost bspindel]#
```

I was relieved that I hadn't so quickly discovered some Trojan at work. Once the mail delivery timed out (5 days), the pattern stopped.

Outbound logs can alert you to backdoored machines trying to connect to their IRC controllers or machines with various adware/spyware trying to phone home. Spyware can be identified by many connects from one or more machine to the same website many, many times per day (to retrieve banner ads, etc.). If I had seen traffic that looked like this:

```
2004-08-12  16:47:24    192.168.1.1 @out 192.168.1.102:1531    66.xx.xx.164:6667
2004-08-12  16:47:30    192.168.1.1 @out 192.168.1.102:1531    66.xx.xx.164:6667
2004-08-12  16:47:44    192.168.1.1 @out 192.168.1.102:1533    66.xx.xx.164:6667
2004-08-12  16:47:47    192.168.1.1 @out 192.168.1.102:1533    66.xx.xx.164:6667
2004-08-12  16:47:53    192.168.1.1 @out 192.168.1.102:1533    66.xx.xx.164:6667
```

I'd have to think that:

a) a user on my network was attempting to connect to an IRC server (TCP port 6667), or

b) a computer on the my network (192.168.1.102) was sending connection attempts generated by some Trojan software such as the aforementioned BotNet, as destination port 6667 is also used by a variety of Trojans:[32]

I would have hoped that, if the traffic was originated by a Trojan, my anti-virus software would have found this software. Even if I found the offending file, just deleting the file may not entirely fix the problem if it's a self-repairing virus/Trojan program, so again I'd rely on inspection of router logs to detect resumption or continuation of this traffic pattern.

If I'd seen outbound traffic to port TCP/6346 and/or UDP/6346 like this,

```
2004-08-12 16:47:53 192.168.1.1 @out 192.168.1.102:1533 66.xx.xx.164:6346
```

I'd have evidence that some user on my network may be downloading music from the Internet, as these these ports are typically associated with use of Gnutella or similar P2P file-sharing software. In a corporate environment, this activity would likely violate an established Appropriate Use Policy (AUP). In the SOHO environment, there wouldn't be a formal AUP, but the security and copyright infringement risks related to file-sharing would still apply.

Conclusion

Setting up a logging facility as I've described was very simple to do, causes no impact on or interference with other resources on the network, and depending on the hardware, operating system, and logging application used, can be implemented for little or no cost beyond what the SOHO user has already invested in broadband connection, modem, and router.

By capturing, reviewing, and analyzing network traffic, a proactive SOHO user can begin to understand what's happening on their network. Although, like use of a router and anti-virus software, log analysis does not in itself completely protect one from malicious activity, log analysis is yet another layer in the 'defense-in-depth' approach to network protection. One cannot protect themselves from something that they do not know exists, so seeing and identifying your network traffic gives one a powerful tool for network control and defense.

Endnotes

[1] Wikipedia, “IP address,” <http://en.wikipedia.org/wiki/IP_address> 2004 (18 OCT 2004)

[2] CERT® Coordination Center, “How are broadband services different from traditional dial-up services?,” *Home Network Security,* 2001 <http://www.cert.org/tech_tips/home_networks.html#II-D> (09 AUG 2004)

[3] CERT® Coordination Center, “How are broadband services different from traditional dial-up services?,” *Home Network Security,* 2001 <http://www.cert.org/tech_tips/home_networks.html#II-E> (09 AUG 2004)

[4] CERT® Coordination Center, “What is NAT?,” *Home Network Security,* 2001 <http://www.cert.org/tech_tips/home_networks.html#II-J> (09 AUG 2004)

[5] Symantec Corporation, “Symantec Security Check,” 2004 <http://www.security.symantec.com/sscv6/home.asp> (13 OCT 2004)

[6] DALnet IRC Network, “Just What Is a BotNet?,” DALnetizen, 2003 <http://zine.dal.net/previousissues/issue22/botnet.php> (03 SEP 2004)

[7] Wikipedia, “Internet Relay Chat,” <http://en.wikipedia.org/wiki/Irc> 2004 (18 OCT 2004)

[8] Ranum, Marcus J., "Untapped Riches," Information Security, 2004 <http://infosecuritymag.techtarget.com/ss/0,295796,sid6_iss407_art816,00.html> (2004-08-09)

[9] Cisco Systems, Inc., *Cisco SOHO 71 Broadband Router,* 2004 <http://www. ci sco.com/en/US/prod ucts/hw/routers/ps2167/prod ucts_data_sheet09186a008 0088740.html> (09 AUG 2004)

[10] D-link Systems, Inc., *D-Link DI-604 4-Port Broadband Router,* 2002 <http://www.dlink.com/products/?model=DI-604> (09 AUG 2004)

[11] Cisco Systems, Inc., *Linksys EtherFast® Cable/DSL Router with 4-Port Switch,* 2003 <http://www.linksys.com/products/product.asp?grid=34&scid=29&prid=561> (09 AUG 2004)

[12] Netgear, *Model RP614 4-Port Cable/DSL Router with 10/100 Mbps Switch,* 2004 <http://www.netgear.com/products/prod_details.php?prodID=131&view=hm> (09 AUG 2004)

[13] SMC Networks, Inc., *SMC7004ABR - Barricade™ 4-Port 10/100Mbps Broadband Router,* 2003 <http://www.smc.com/index.cfm?sec=Products&pg=Product-Details&prod=67&site=c> (09 AUG 2004)

[14] Mozilla.org, *Firefox 0.9,* 2004 <http://www.mozilla.org/products/firefox/> (09 AUG 2004)

[15] checksyslog v1.3, 2001 <http://www.jammed.com/~jwa/hacks/security/checksyslog/checksyslog-doc.html> (09 AUG 2004)

[16] Kiwi Enterprises, *Kiwi Syslog Daemon,* 2004 <http://www.kiwisyslog.com/help/Syslogd/index.html> (09 AUG 2004)

[17] DFN-CERT Services GmbH, “Overview” *Logsurfer Homepage,* 2004 <http://www.cert.dfn.de/eng/logsurf/> (09 AUG 2004)

[18] Somix Technologies, Inc., *Logalot,* 2004 <http://www.somix.com/products/logalot.php> (09 AUG 2004)

[19] Sourceforge.net, *Swatch,* 2004 <http://swatch.sourceforge.net/> (09 AUG 2004) Tenshi

[20] 0.2, 2004 <http://www.gentoo.org/proj/en/infrastructure/tenshi> (09 AUG 2004)

[21] Wallwatcher version 3.0.15, 2004 <http://www.sonic.net/wallwatcher/> (04 OCT 2004)

[22] DShield.org “Distributed Intrusion Detection System, Routers and Firewalls using Kiwi Syslog Daemon”, *How to submit your firewall logs to DShield,* 2004 <http://www.dshield.org/howto.php> (09 AUG 2004)

Endnotes

[23] Kiwi Enterprises, *Kiwi Syslog Daemon,* "Features of the Free version" 2004 <http://www.kiwisyslog.com/info_syslog.htm> (20 AUG 2004)

[24] Purdue University Engineering Computer Network, *Eventlog to Syslog Utility,* 2003 <https://engineering.purdue.edu/ECN/Resources/Documents/UNIX/evtsys> (09 AUG 2004)

[25] Der Ga'had, Urbana, *"Make Windows Talk to Syslog"* 2003 <http://www.netadmintools.com/art284.html> (09 AUG 2004)

[26] Der Ga'had, Urbana,"*Automated Log Monitoring with LogSentry and a Central Syslog Server II, Configuring the Clients"* 2002 <http://www.netadmintools.com/art127.html> (09 AUG 2004)

[27] Internet Assigned Numbers Authority (IANA), *Port Numbers* 2004 <http://www.iana.org/assignments/port-numbers> (04 OCT 2004)

[28] The SANS Institute, *Top 10 Ports,* 2004 <http://isc.incidents.org/top10.php> (19 AUG 2004)

[29] *Beyond Security Ltd., DameWare Mini Remote Control Buffer Overflow,* 2003 <http://www.securiteam.com/windowsntfocus/6N00B1P95I.html> (19 AUG 2004)

[30] RFC 1918, *RFC 1918 - Address Allocation for Private Internets,* 1996 <http://www.faqs.org/rfcs/rfc1918.html> (19 AUG 2004)

[31] Mike Gleason, *NcFTP Software, "The Ephemeral Port Range"* 2001 <http://www.ncftpd.com/ncftpd/doc/misc/ephemeral_ports.html> (20 AUG 2004)

[32] broadbandreports.com/dslreports.com, *Security» 2. Personal Firewalls (general), 2004 <http://www.dslreports.com/faq/8226>* (09 AUG 2004)