Interested in learning more about security?

SANS Institute InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Doing My Part - Sending Data to the Internet Storm Center

Home and small office broadband users MUST take responsibility for tightening their security. There are a number of excellent papers on small office / home office (SOHO) security in the SANS Reading Room that provide clear examples of using a variety of inexpensive firewall devices and/or software-based personal firewalls, which allow even a novice to start at the beginning and slowly work through securing a home or small office network. Following these best practices is an excellent start, but my SANS Security Essenti...

Copyright SANS Institute

Author Retains Full Rights

AD

Sydney Jensen
GSEC Practical version 1.4

DOING MY PART – Sending Data to the Internet Storm Center

Abstract

An increasing number of Americans use a broadband connection to connect their home or small office network to the internet, and in January 2002 broadband use surpassed dial-up time spent online "for the first time ever."[1] Most home and small office users are sadly unprotected and unwittingly aid the "bad guys" in their DoS attacks, worms, internet mail relay, and other unsavory activities.[2] A classic example of this was the Code Red outbreak, when many broadband ISPs (including Qwest, the local DSL provider) had their networks saturated with Code Red-related traffic due in part to unsecured home broadband connections.[3]

Home and small office broadband users MUST take responsibility for tightening their security. There are a number of excellent papers on small office / home office (SOHO) security in the SANS Reading Room that provide clear examples of using a variety of inexpensive firewall devices and/or software-based personal firewalls, which allow even a novice to start at the beginning and slowly work through securing a home or small office network.

Following these best practices is an excellent start, but my SANS Security Essentials instructor, Bob Hillery, made it a point to emphasize that locking the doors is only a part of the answer -- to really be secure on the internet you have to go a step further – you have to do your part to stop hacker activity. [4] This paper documents the procedure that I set up to automate collecting and sending intrusion attempt information to Incidents.org and the Internet Storm Center, then discusses my results and some possible next steps.

Incidents.org and the Internet Storm Center

Incidents.org (http://www.incidents.org) is a global organization that exists in virtual space to help security professionals do their jobs better, faster, and with less effort. Incidents.org has members from many fields such as security analysts, computer forensics experts, and incident handlers, all working together to provide real-time, real world, mission critical threat information. Incidents.org consolidates vulnerability data, attack statistics, and general security news and provides a daily window into security threats and vulnerabilities with extensive "drill down" capability including breaking news, top threats, archives of past threats and breaches, security patches and "how to" information to close vulnerabilities and repair systems.[5] Incidents.org should be in every security professional's internet bookmarks.

Incidents.org sponsors the Internet Storm Center (http://isc.incidents.org/), which consolidates data from thousands of firewalls and intrusion detection systems in

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

over 50 countries. This data is processed with advanced analysis tools and put into a format that allows easy visualization of the type and frequency of Internet threats. The global nature of incidents.org ensures that data is analyzed around the clock. When a threat pattern is identified professionals investigate and gauge the threat's severity and impact. Critical alert information is rapidly disseminated via email and web sites.[6] It is possible to watch attacks move across the globe in near real time! Figure 1 below shows attack patterns and advisories listed at the Internet Storm Center as of July 2, 2002.[7]

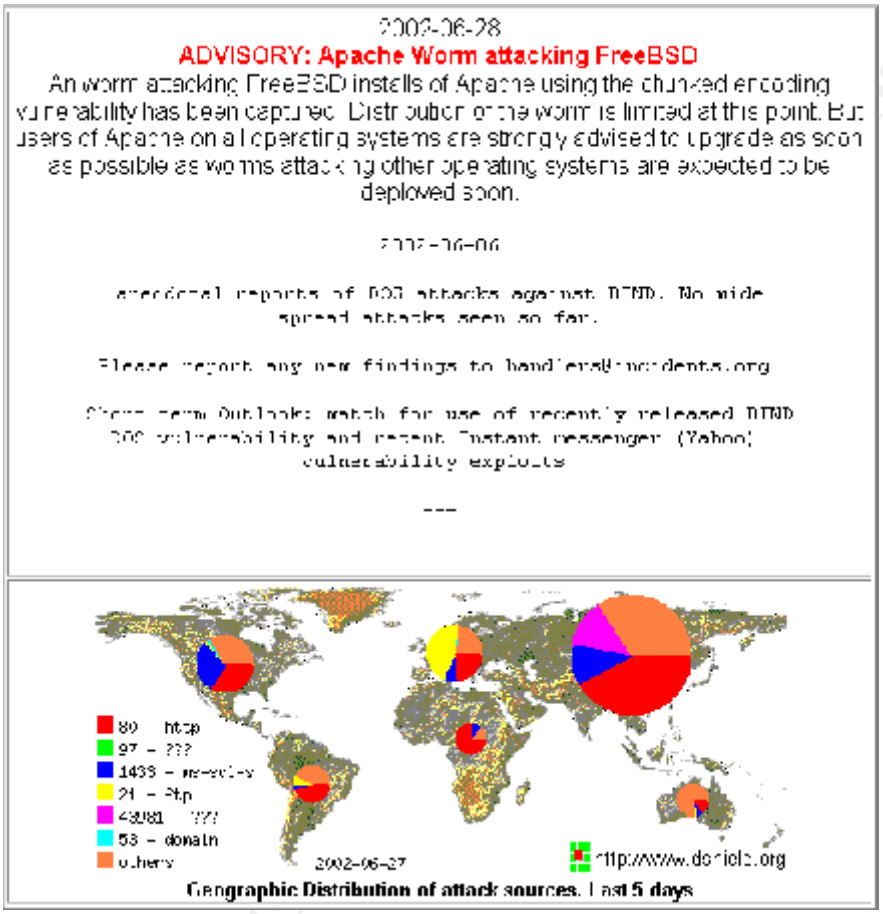

Figure 1 (http://isc.incidents.org)

Dshield – Collecting Data for the Internet Storm Center

The data feeds to Incidents.org come from thousands of individuals and organizations using client software to process and upload intrusion attempt information from firewalls, routers, and other intrusion detection systems. Think of this as a multi-platform, global, distributed intrusion detection system. The client software to let home and small office users participate is available through DShield.org (http://www.dshield.org). Firewall users submit logs to the DShield database using one of the ready to go client programs, their own programs, or the DShield Web Interface (http://www.dshield.org/report.html) to manually submit firewall logs.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

In addition to collecting the data for Internet Storm Center analysts, Dshield also provides some summary reports via the DShield web site. The DShield reports and database summaries (http://www.dshield.org/reports.html) include: Top 10 offenders in the DShield database; Top 10 most probed ports; Thirty day history of a user selected port; information about a user specified IP address; Summary of recent activity from a Subnet; List of IP address ranges you might want to block; and also allows a user to search the DShield database [8]

Fight Back!

DShield has a FightBack! program (http://www.dshield.org/fightback.html) which helps users fight back against attackers by analyzing submitted log reports and selecting strong cases to forward to the ISP from which the attack originated. A copy of the abuse report is also forwarded to the submitting user(s). DShield claims that this is much more effective than having each individual user submit abuse reports, which generally receive an automated reply and are then promptly forgotten. (Who hasn't forwarded email to abuse@SomeISP.com and gotten only an automated response, and never known if anything was done with the report?) DShield has been able to get responses, and action, from many ISPs. This includes things like closing accounts for violation of the ISP's Terms of Service, locating and cleaning infected or compromised systems, and locating and patching systems deployed improperly. Current example responses can be seen online (http://www.dshield.org/fightback_results.html).[9]

Are you convinced now? I was. The following pages document how I configured my home/home office security, selected and configured client software, and automated submission of my logs to DShield and the Internet Storm Center.

Step 1: SOHO Network Configuration & Security

The first thing I needed to do was to make sure that my SOHO network was set up in a secure fashion and would protect my personal and company resources from unauthorized access or use. When I set up the network I did attempt to make sure that it was not wide open, but it is a good idea to periodically audit your own security and make sure that everything is up-to-date and functioning properly. Figure 2 (below) shows my network configuration. Note that I use two LinkSys devices, segregating my Home and Home Office networks. This paper concerns logging and forwarding events to DShield only from the external LinkSys device.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

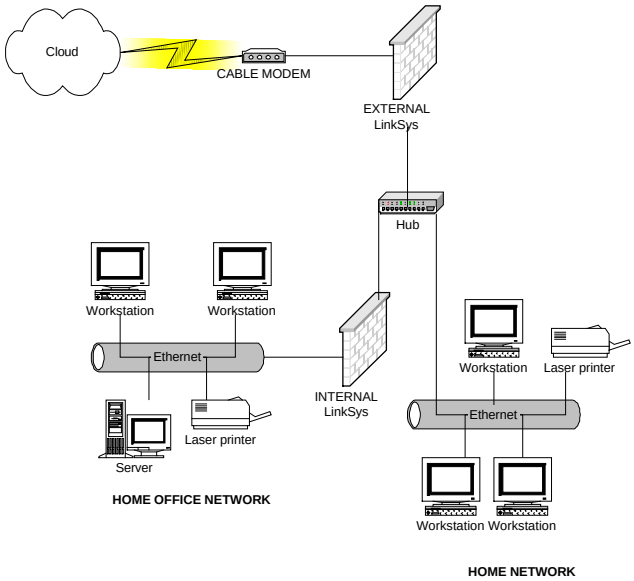

figure 2 – my network

I followed documented security steps to secure my SOHO network, referencing Charnick's excellent paper in the SANS Reading Room (http://rr.sans.org), "Getting the Most Security out of the Linksys ® Cable/DSL Router."[10] This gave me confidence that my external facing LinkSys router was properly configured, documented and verified my network configuration, and ensured that I was running the most current version of the firmware.

I then checked my external security using a simple, publicly accessible website: Gibson Research Corporation's "Shields Up!" test (https://grc.com/x/ne.dll?bh0bkyd2). The ShieldsUp! test attempted to establish standard TCP Internet connections with well-known and often vulnerable Internet service ports on my computer. Successful connections would have revealed ports that were "open" and therefore vulnerable to Internet port scanners. The test took only a few moments and revealed that I was in "stealth" mode – my computer did not even reply back to verify existence of the ports, much less whether or not they were accepting connections.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

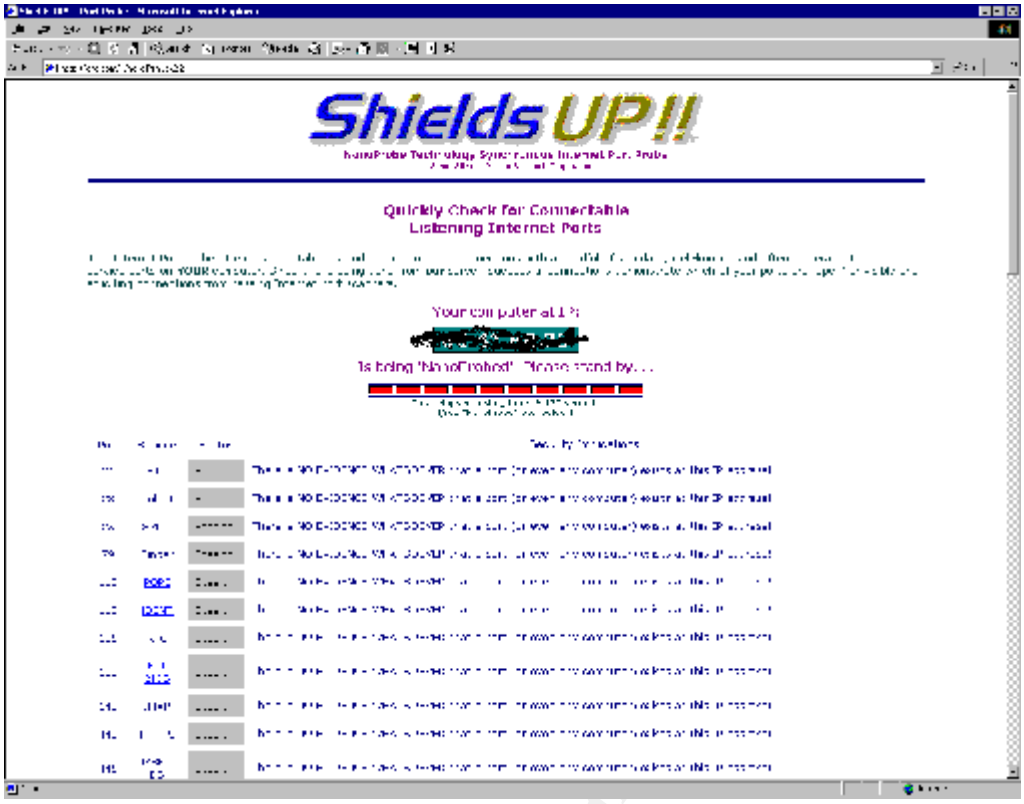

figure 3 – Results of Gibson Research Corp. Port Scan

Step 2 - Configure the LinkSys BEFSR41 Router for Logging

With the prerequisite security setup out of the way, I now moved on to setting up my DShield-friendly environment. The first step was to configure my LinkSys BEFSR41 router for logging and to send the logs to my evaluation workstation (the "logging" computer). This is setup in the LinkSys administration web interface (default is http://192.168.1.1), on the "Logs" tab.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

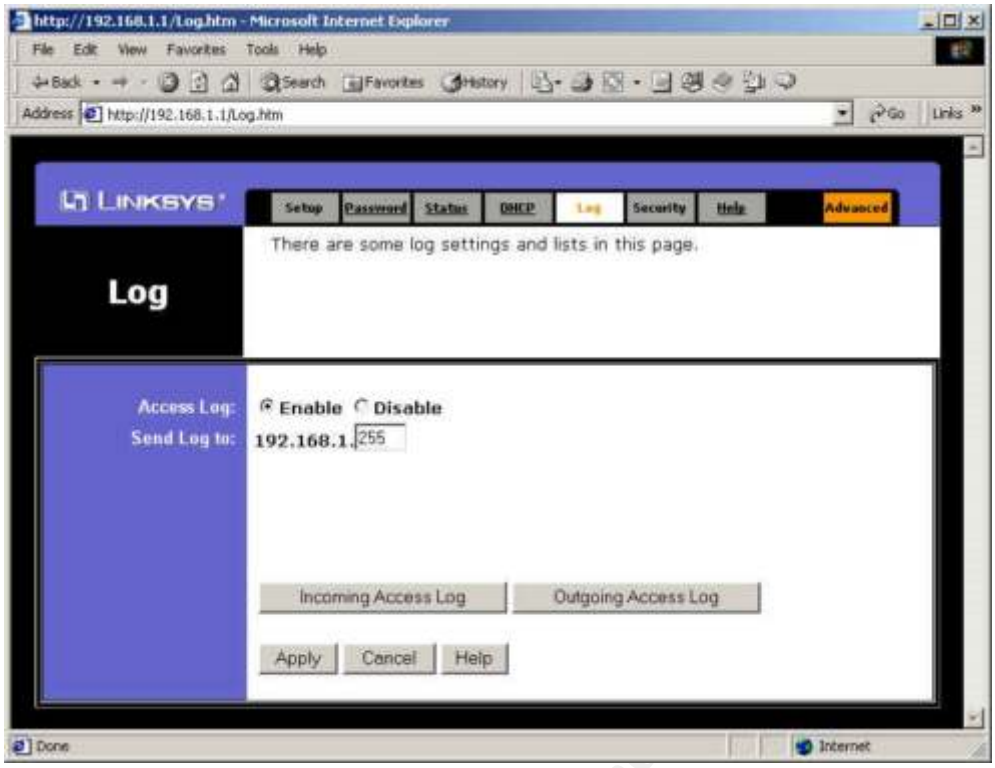

figure 4 – LinkSys administrative web console

Note that the administrative web interface has buttons for “Incoming Access Log” and “Outgoing Access Log.” These options open additional browser windows and show the twenty-five (25) most recent entries in the incoming and outgoing logs, respectively. This data is not saved anywhere unless you configure your LinkSys to send the log to a receiving computer.

Setting the 'Send Log to:' field to 192.168.1.255 will instruct the Linksys Router to broadcast its logging information to all systems on the LAN. Remember that the simplest LinkSys setup uses the DHCP service within the Linksys Router to assign IP addresses to computers on the network. This means that the IP address of the logging computer could change, so set the 'Send Log to:' address to the system which is running logging software (192.168.1.100 for example) only if you are using static IP addresses and know the IP address isn't going to change or otherwise send your logging information to the wrong computer. I only use static IP addresses for my internal servers, not for any workstations, so I elected to use the broadcast address.

Step 3 - Register with DShield

I registered with Dshield (http://www.dshield.org/signup.html) and signed up for the FightBack! program. That gave DShield permission to forward selected

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

reports I might submit to ISPs where attacks originate. You do not need to register with DShield to submit firewall logs. Registration will not clog your email with mass mailings. If you decide not to register, you will not have the option of participating in the FightBack! Program. I elected to register with a personal email address, not my primary business email, so that my submissions would not be mistaken for "official" company submissions.

Step 4 - Client Software

Once the router logging was properly configured, my next step was to install and configure client software. The client software collects, displays, and analyses log information from the router/firewalls. This data is then forwarded to the DShield database. The DShield software page (http://www.dshield.org/windows_clients.html) contains links to client software. My client workstation was running Windows 2000, and my router is a LinkSys BEFSR41, which ruled out using the default DShield software. The list of third party applications showed that I had two choices: LinkLogger (http://www.linklogger.com) and Wallwatcher (http://www.wallwatcher.com/). Wallwatcher is freeware, with a built-in mechanism to forward logs to DShield, while LinkLogger costs $21.95 to register and requires another application to forward logs. I decided to evaluate both.

Step 4a - Client Candidate 1: LinkLogger

LinkLogger is compatible with Linksys, Netgear, ZyXEL Prestige and ZyWall routers and gateways. The firmware version required varies depending on which router you are using, so be sure to consult the requirements list on the web site.[11] LinkLogger also requires that you have the Microsoft Data Access Components installed. PLEASE NOTE: If you install MDAC 2.6 on a clean system, you will need the Microsoft JET Service Pack 3 (http://www.microsoft.com/data/download.htm#Jet4SP3info) for LinkLogger to function.[12]

I did a standard install using default values for install directory and program group, then fired up LinkLogger and began configuration using the online documentation (http://www.linklogger.com/linksys_setup.htm). This was simple enough, requiring only that I point LinkLogger to my LinkSys device. To find this screen select 'Edit' from the main menu and then select the 'Setup...' option and click on the 'Router' tab. The Router Address is the internal LAN IP address of your Linksys Router (192.168.1.1 by default).

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

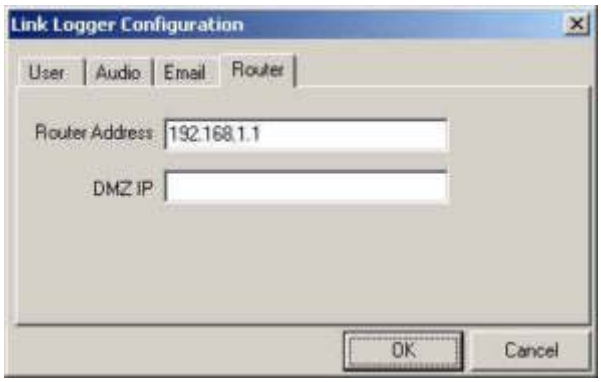

figure 6 – LinkLogger configuration

LinkLogger also has more advanced configuration options, allowing audible and email alerts for probes and scans, connection attempts, active Trojans, and "battle stations" events. I left these fields blank for the time being, then verified that LinkLogger was receiving and collecting the log of my LinkSys activity.

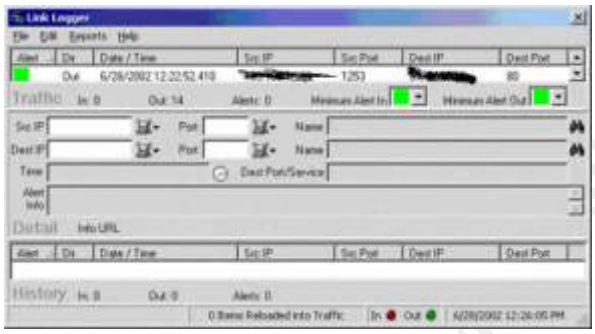
figure 7 – LinkLogger is collecting log information

LinkLogger requires another program to forward data to DShield.org. The recommended solution, from both LinkLogger and DShield, is Dshieldup (http://www.linklogger.com/dshieldup.htm). The file is simply extracted into a folder. I chose the LinkLogger folder.

DShieldup is very easy to configure - enter the SMTP email host from your ISP (check your email setting for the SMTP address). The Author ID is your personal ID from DShield.org, which is assigned when you register. Anonymous users can enter 0 for their Author ID. I suggest using your own email address in the "send to" field while you are testing, and changing it to reports@DShield.org when you know that everything else is properly configured. The DShieldUp documentation also recommends that you turn off descriptions in the drag and drop (user configuration) to speed up drag and drop operations. [13]

Unfortunately DShieldup is a bit tricky to use properly. The documentation says "In Link Logger build a search list of events that you would like to send, then drag and drop them onto DShieldUp (figure 8)."[14] This sounds easy, but is cumbersome to set up. I was also disappointed in the small data window in LinkLogger. There were no instructions to automate sending reports to

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

DShield.org. The LinkLogger/DshieldUp option is functional, but not as well-integrated or as easy to use as I had hoped. Time to evaluate the freeware!

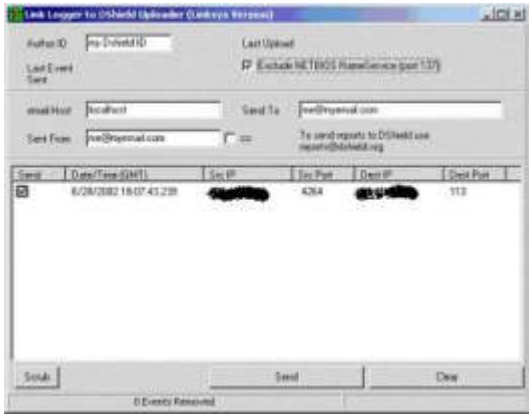

figure 8 - DShieldup

Step 4b - Client Candidate 2: WallWatcher

I uninstalled LinkLogger and DShieldUp, rebooted, then installed WallWatcher. WallWatcher collects, displays, and analyses log information from the Linksys BEFSR11, BEFSR41, BEFSR81, and similar Linksys router/firewalls running Firmware versions 1.36 or later. It runs under Microsoft Windows 98, SE, ME, 2000, NT4.0, and XP. WallWatcher has a very simple installation: download two ZIP files (WallWatcher and its library), extract their contents into a folder and WallWatcher is ready to run. I installed to C:\wallwatcher.

Once installed, I verified that WallWatcher was collecting logs (figure 10).

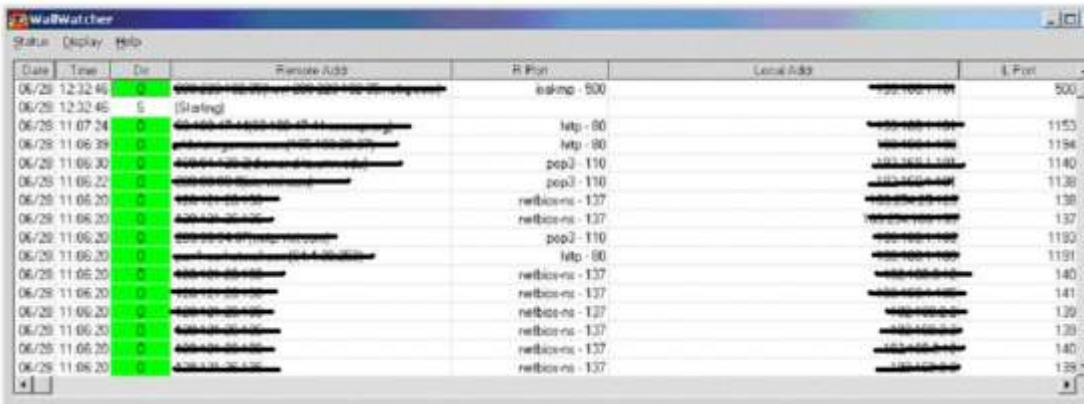

figure 10 – WallWatcher in action

WallWatcher recommends using a plug-in called WW2DShield (http://www.wallwatcher.com/WW2Dshield.html) to prepare and submit reports to DShield. WW2DShield is very easy to install: download and unzip the file

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

(http://www.sonic.net/~sraaii/wallwatcher/WW2Dshield.zip) to the WallWatcher directory. During the one-time setup, you can choose how you want to submit your reports. The preferred method is via e-mail, but you can also use your Browser (it gives you more control and a chance to preview what you're going to submit). After you've done the Setup, you can submit occasional reports when you think there's excessive activity, or schedule automatic daily e-mail reports.

To prevent duplicate submissions, WW2DShield keeps track of the latest timestamp it has successfully sent to DShield and won't send any records with an earlier timestamp. You can temporarily bypass this feature if you need to resend data. NOTE: If you are ever manually sending several log files, be sure to send them in chronological order (oldest to newest), or WW2DShield will tell you that there are no reportable incidents in the older logs. In that case you will have to disable the time checking feature (uncheck the box next to the option "Only use records dated after…"). Figure 11 (below) shows the WW2DShield interface.

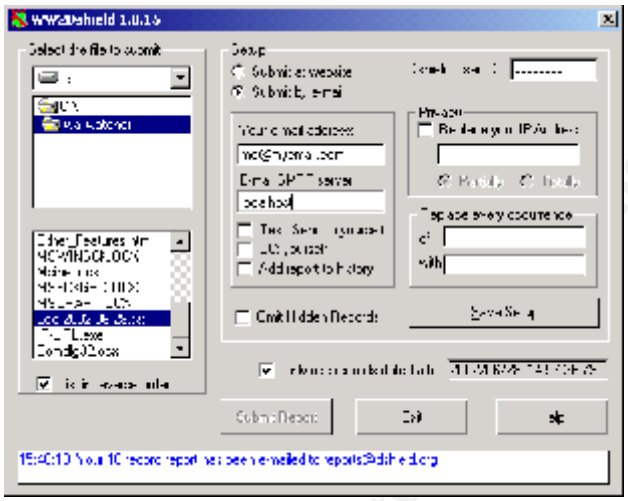

figure 11 – WW2Dshield interface

Once you have WW2DShield configured, make sure that it is working properly. To do this, manually submit a report by selecting the log file that you want to submit to Dshield then click the SUBMIT button. Note that in figure 11 (above) I received the message "Your 10 record report has been e-mailed to reports@DShield.org." If you check the box marked "CC: yourself" a successful submission will also result in an email to you. It should look something like this (figure 12):

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

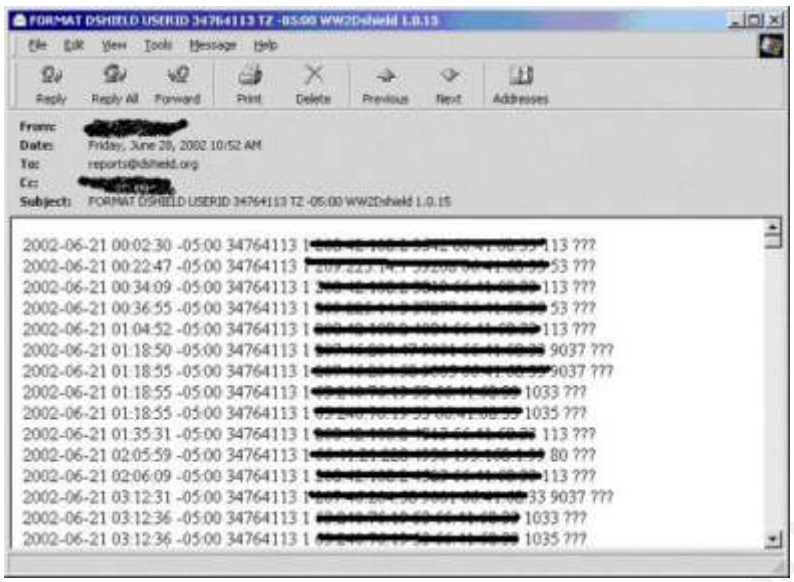

figure 12 – Dshield confirmation email

You may want to turn off this CC: feature once you know the process is working, or to setup an email rule to move these emails to a specific location for archival purposes and to keep your email box a little clearer.

Step 4c - Client Software: Selection

I preferred the WallWatcher/WW2DShield software to the LinkLogger/DshieldUp software. WallWatcher and WW2Dshield installed cleanly, it was easier to configure data to send to Dshield (since it does it automatically), and the software is freeware. Not bad! I added WallWatcher to the Startup group on my logging computer, then rebooted to make sure that WallWatcher started automatically.

Step 5 - Automating Submission

I am a fairly busy person, and I do take the occasional weekend off, and even use a vacation day once in a while. I did not want to have to remember to manually send my logs to DShield every day, I wanted a way to automate that task. It was a trivial task to automate submission of WallWatcher logs to DShield.org.using the Windows task scheduler. I scheduled the task to occur on a daily basis. Remember that this only works if the system is powered up at the scheduled time! Detailed instructions to set up this scheduled job are available online, and are summarized below:[15]

1. Start the Windows Task Manager
2. Select "Add new task"
3. Browse to "WW2DSHIELD.EXE" and select it
4. Schedule it to run daily
5. Click "open advanced properties", then click Finish

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

6. The Task tab of the Settings window will open, highlighting the program path and name;
7. Add parameters to specify the log file to use:

    - **-Y** specifies "yesterday's" log file. This should work from 12:01 AM to 11:58 PM. It is the preferred choice because yesterday's log is complete;
    - **-T** specifies "today's" log file, which will always be incomplete unless you're scheduling the task for just before midnight. (that's why "-Y" is the preferred choice.)

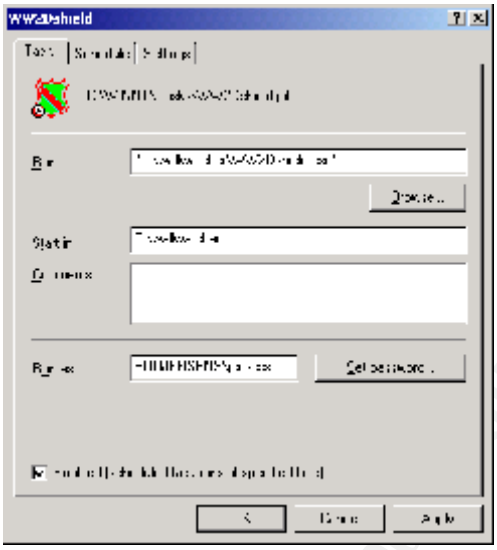

figure 14 – WW2Dshield Log Selection Parameters

8. Click "OK".
9. WW2DSHIELD should appear as a scheduled task in the list;

The reports will be sent in every day until you change the schedule or are no longer running WallWatcher. **NOTE:** If you remove WW2DShield from your system, be sure you also remove it from the Task Scheduler.

Step 6 - Automating Archiving and Directory Cleanup

WallWatcher creates two files for every day it is in operation. The first is the raw data from the firewall log, filename format “Raw yyyy-mm-dd.dat,” and the second is the prepared log file, filename format “Log yyyy-mm-.txt.” These files should be archived over time and moved to a subdirectory in order to keep the WallWatcher directory clean. I automated this task as well.

I created archive directories for the raw data and the log files (c:\wallwatcher\old_raw_data and c:\wallwatcher\old_logs) . Next I wrote a simple batch file that moves all the raw data to the c:\wallwatcher\old_raw_data folder and

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

all the logs to the c:\wallwatcher\old_logs folder (figure 15). I then used Windows task scheduler to automate running this batch file once a week, on Friday at 12:00 AM.

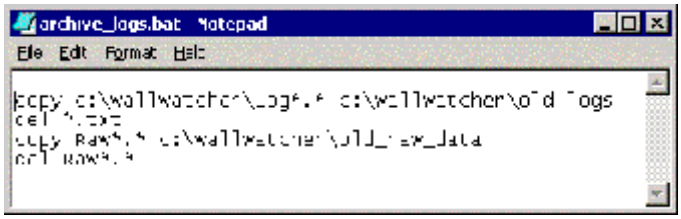

figure 15 – archive and clean up batch file

Step 7 - Verify

I left WallWatcher and WW2DShield running over a weekend to verify that automated submissions were working properly. I could see that the task had run as scheduled by looking in the Task Scheduler (figure 16). Note that the “Last Time Run” now displays.

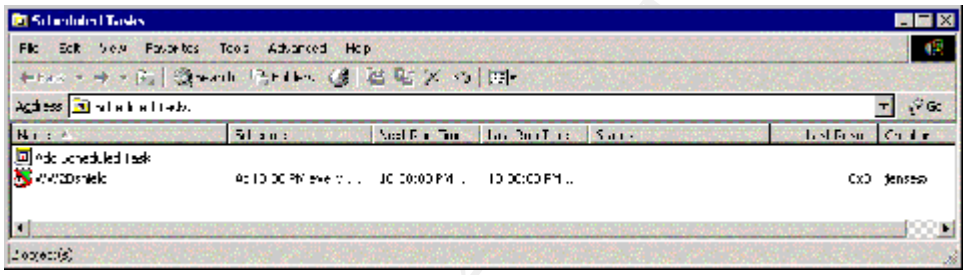

figure 16

I was able to verity that the prepared reports had been submitted by checking "WW2DSHIELD.LOG" (in the WallWatcher directory). All reports that have been successfully submitted are marked “sent.” (figure 17)

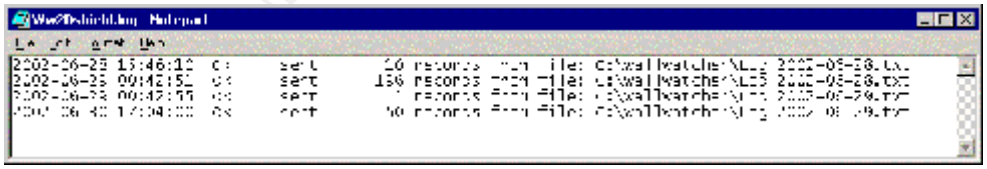

figure 17

Successful submissions also result in confirmation email from DShield (figure 18). I have an email rule to store these confirmations in a specific folder, and take a look at them every few days to see how busy the bad guys are.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

figure 18 – confirmation email from DShield

What My Logs Revealed

I was interested in manually looking through my logs to see what the data looked like. WallWatcher automatically installs a companion piece of software called WallReviewer to allow log sifting. WallReviewer allows you to select the log you want to view from a drop down list of all the logs in the directory, to consolidate logs from more than one day for analysis, to summarize by remote address, local address, local port, remote port, or date. It also displays the count for each intrusion, so you can see at a glance how many times you have been probed. Figure 19 (below) shows my logs for 4 days (June 13-19, as not every day was logged), with outbound traffic filtered, and sorted by count.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

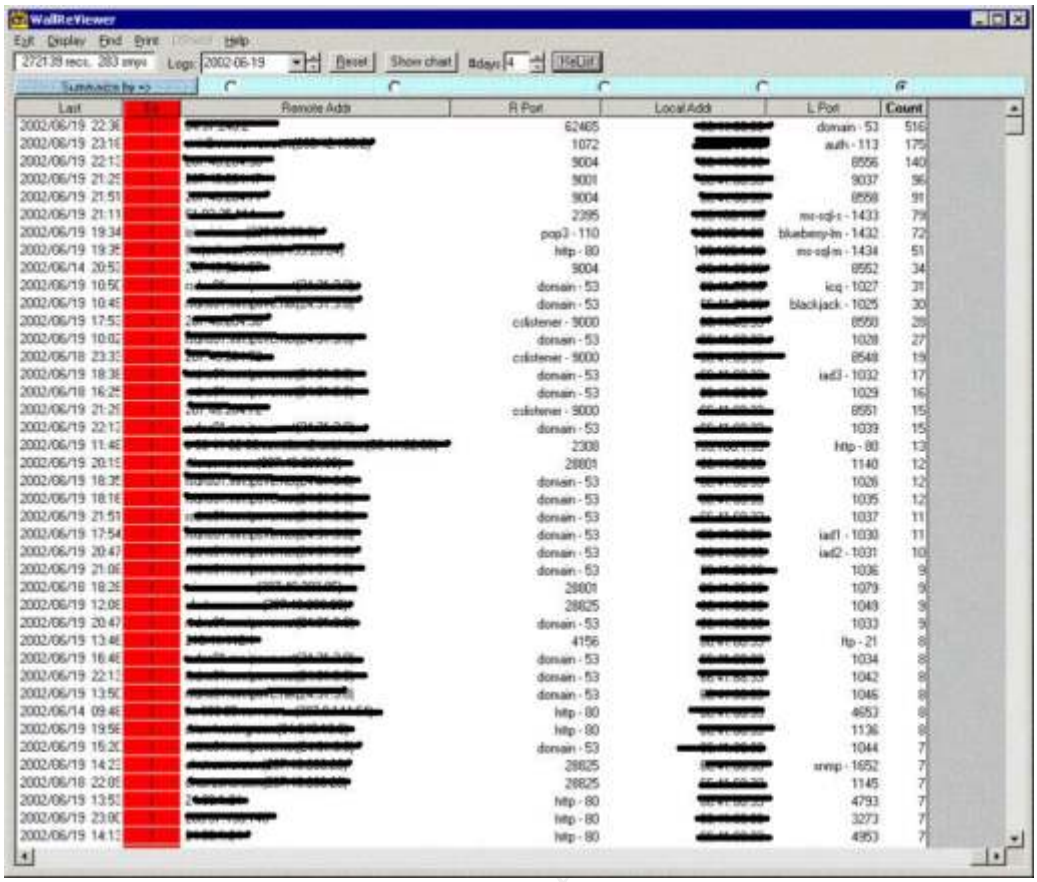

figure 19 – WallReviewer (4 days of data, outbound filtered out)

The logs were not terribly surprising. They showed some probes of Microsoft SQL server ports (1433 and 1434), some port 80 probes looking for a web site, some probes to see if I had an ftp server running (port 21), and other miscellaneous ports. I was intrigued by some of the traffic, such as seventy-two attempts on port 1432. I looked up this port on the Internet Storm Center Port Report (http://isc.incidents.org/port_details.html?port=1027) and found that port 1432 is for the Blueberry Software license manager service.[16] Blueberry Software? A Google search led me to the Blueberry Software page.[17] It looks like legitimate software, not an oddly named trojan. Is someone actually searching for a software license server at my IP address? Or is it just a port scan, and caught my eye because 1432 is adjacent to 1433 and 1434, the Microsoft SQL ports? There's no way to know, but port scanning is quite likely.

My logs also showed some attempts on port 1027, listed as ICQ, and which the Internet Storm Center identifies as a port used by a Trojan called ICQKiller,[18] and port 1025, which is shared by several trojans (among them are blackjack, fragglerock, and NetSpy).[19] At this point I got a bit suspicious, and even though I run up-to-date antivirus software and occasionally run a port scan myself, I quickly checked to see what ports my system was listening on. The simplest way to

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

check this is to open a command prompt and type “netstat –a” (without the quote marks). This quick check did not show that my computer was listening on any suspect ports.

Relevance

The information from my logs is valuable to Incidents.org and the Internet Storm Center, as it helps track how prevalent and/or widespread the use of specific exploits is. Following the publication of the Microsoft SQL “blank SA password’ exploit there was an increase in activity directed at port 1433. It is also possible to track unknown exploits this way. For example, if there is a sudden spike of activity directed at port 21 (ftp), experts at Incidents.org can focus their search for vulnerabilities to ftp servers, and eventually discover the specific vulnerability for which the “bad guys” are looking.

Summary

My small part of “defending the internet” began simply. I knew there were risks associated with an always on broadband connection, and that it was my responsibility to make sure that I was not aiding nefarious online activity. My home and small office network is now much more secure than it was. Charnick’s paper provided a very good walk through of properly configuring my LinkSys device to act as an effective firewall. [20] I verified this using Gibson Research Corp’s online port scan utility.

Contributing to DShield’s work began with configuring my LinkSys router to forward logs to a PC running client software that would collect, analyze and store the logs. I evaluated two possible solutions and elected to use WallWatcher and its plug-in application WW2DShield (both freeware).

WallWatcher is configured to start automatically when my logging computer is rebooted. I registered with DShield and FightBack! so that my logs can be used to work with ISPs to track down and resolve incidents. My logs are now sent to DShield automatically every night, the logs and raw data are archived once a week, and I am able to verify successful submissions.

I am confident that I have begun doing my part to make the Internet a less hospitable playground for crackers and script kiddies. It may sound funny, but I am actually looking forward to a time when I get an email from FightBack telling me that my logs helped an ISP put a cracker out of business. I may undertake additional security projects on my home network, such as logging and forwarding from my internal LinkSys (excluding internal IP addresses from submission), adding a redundant internet connection with proper security, upgrading from the LinkSys to a Cisco PIX device, and/or adding host-based intrusion detection. I will do my best to make sure that I can share the data I gather with Incidents.org.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Thanks to SANS and Bob Hillery, I am no longer a part of the problem; I am now a part of the solution.

FOOTNOTES

[1] "Broadband Hits the Mainstream," NewsFactor Network Report (March 2002).
[2] "Smurf Attack Cripples More Big Sites." OnMagazine.com. (Feb 2000).
[3] Qwest DSL Code Red Virus Alert http://www.qwest.com/dsl/customerservice/coderedvirus.html (July 2002)
[4] Hillery, Bob. At SANS Kansas City, March 2002.
[5] "Frequently Asked Questions," Incidents.org. http://www.incidents.org/faq/index.html (July 2, 2002)
[6] "Frequently Asked Questions," Incidents.org. http://www.incidents.org/faq/index.html (July 2, 2002)
[7] Internet Storm Center. http://isc.incidents.org (July 2, 2002).
[8] DShield "Reports and Database Summaries." http://www.DShield.org/reports.html (July 2002)
[9] FightBack! http://www.dshield.org/fightback.html (July 2, 2002).
[10] Charnick ,Earl. "Getting the Most Security out of the Linksys® Cable/DSL Router." http://rr.sans.org/homeoffice/linksys.php (paper dated November 30, 2001) (retrieved 15 June 2002).
[11] LinkLogger Documentation http://www.linklogger.com/requirements.htm (July 2002) .
[12] LinkLogger documentation, http://www.linklogger.com/download.htm (July 2, 2002).
[13] Dshieldup documentation http://www.linklogger.com/dshieldup.htm (July 2002).
[14] Dshieldup documentation http://www.linklogger.com/dshieldup.htm (July 2002).
[15] WW2Dshield documentation, http://www.wallwatcher.com/WW2Dshield.html (July 2002).
[16] Incidents.org Port Report, Port 1432 (http://isc.incidents.org/port_details.html?port=1432)
[17] Blueberry Software homepage http://www.blueberry.com (July 2, 2002).
[18] Incidents.org Port Report, Port 1027 (http://isc.incidents.org/port_details.html?port=1027)
[19] Incidents.org Port Report, Port 1025 (http://isc.incidents.org/port_details.html?port=1025)
[20] Charnick, http://rr.sans.org/homeoffice/linksys.php.

REFERENCES

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

"Broadband Hits the Mainstream." NewsFactor Network Report. URL http://www.newsfactor.com/perl/story/16629.html (report dated March 6, 2002) (retrieved 1 July 2002).

Blueberry Software http://www.blueberry.com (July 3, 2002).

Charnick, Earl. "Getting the Most Security out of the Linksys® Cable/DSL Router." URL http://rr.sans.org/homeoffice/linksys.php (paper dated November 30, 2001) (retrieved 15 June 2002).

DSHIELD.ORG: http://www.DShield.org (July 2, 2002).

DShieldUp! http://www.linklogger.com/DShieldup.htm (July 2, 2002).

Gibson, Steve. Gibson Research Corporation. http://www.grc.com (July 2002).

Gibson, Steve. ShieldsUp! https://grc.com/x/ne.dll?bh0bkyd2 (July 2, 2002).

Hillery, Bob. SANS Instructor for SANS Kansas City, March 2002. Bio from http://www.sans.org/MotorCity/index.php - hillery .(retrieved 1 July, 2002).

Incidents.org. http://www.incidents.org (July 2, 2002).

Incidents.org. "Port Report." (http://isc.incidents.org/reports.html). (July 2, 2002).

"Instant Broadband series: Cable/DSL Routers. LinkSys Etherfast Cable/DSL Router User Guide." URL: ftp://ftp.linksys.com/pdf/befsr11_befsr41ug.pdf (June 2002) (retrieved 15 June 2002).

Internet Storm Center. http://isc.incidents.org (July 2002).

LinkLogger http://www.linklogger.com/ (July 2, 2002).

Qwest DSL: Code Red Virus Alert. http://www.qwest.com/dsl/customerservice/coderedvirus.html (July 3, 2002).

"Smurf Attack Cripples More Big Sites," OnMagazine.com. URL: http://www.onmagazine.com/on-mag/reviews/article/0,9985,38968,00.html (article dated Feb 2, 2000) (retrieved 1 July 2002).

WallWatcher: http://www.wallwatcher.com/

WW2DShield http://www.wallwatcher.com/WW2DShield.html

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: June 20th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**