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: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

Security Logs and Checkpoint Firewall-1
GSEC Practical Assignment, Version 1.2e
John T. Ryan
June 4, 2001

Introduction

System and Security Logs are tools that are part of the Security Administrators arsenal to defend their network. In far too many instances, log servers are installed and logging activated, only to have the whole system soon forgotten about unless some catastrophic event happens that causes everyone to scramble to the logs to see what happened. Logging systems exist to allow the Security administrator to be proactive to vulnerabilities, not just to perform forensics on. "Security logs are your sentries, your early warning system- and in some cases your packet of money with a dye bomb attached." (Cheswick, p133) One of the first things an attacker will do is turn off logging, install a hacked daemon and erase all traces of themselves in the logs. Daily log inspection should be a task that every company dedicates resources to.

The problem many administrators face is getting those resources allocated. IT organizations are constantly being asked to do more with less people. Procedures and tools need to be put into place to lessen the workload and allow an organization to be proactive. I will attempt to offer some solutions to help with Checkpoint's Firewall-1 product.

Firewall-1 Logging

Checkpoint Firewall-1 is a widely deployed firewall system. According to IDC, Checkpoint has a 41% market share. (Checkpoint Software) Even with the popularity of this product the logging system has not been well developed. There is a huge reliance on OPSEC (Open Platform for Security) products from third party vendors. Because of this, Firewall-1 provides minimal log reporting capabilities in the base product. Weaknesses of the logging system that come in the box include limited logging detail, limited Syslog support, and inconsistent log exporting.

Firewall-1 provides limited logging detail. The software only logs the initial connection, a SYN/ACK. (Welch-Abernathy) This leaves you in the dark about what is happening after that connection is made. Firewall-1 does not give you any information on the data flowing through the connection or the subsequent traffic flowing through after the connection is made.

Another issue with Firewall-1 is its limited Syslog support. The Syslog format is a widely accepted standard for writing system logs to a machine. It is possible to install a server running syslogd that will gather Syslog messages from all other devices that have been told to send log information to it. It then becomes an easy task to run SWATCH for real-time checking of these logs to generate alerts or analysis. Checkpoint relies on add-on products and OPSEC providers to give you these capabilities. This capability comes at an

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

extra monetary cost. With the low priority that logs receive in many organizations it becomes hard to obtain management approval for purchasing these tools.

Firewall-1 writes its logs in a binary format. To obtain the information contained in the logs, you must export them. Firewall-1 has a problem with exporting logs. During the export process, the data is output in a delimited format. The problem that occurs is the fields are not guaranteed to appear in the same order between log exports. It is not uncommon to perform log exports consecutively on different backups and have the fields output in a different order. Fortunately for the security administrator, there are tools that will reformat the output. (Spitzner)

Log Maintenance

Firewall-1 logs can grow very large. If you are using the Checkpoint GUI to view your logs, you will start to experience delays and even crashes if you try to view a log that is too large. The best practice is to write a batch file to perform a fw logswitch and then implement it on a daily basis through a cron job or using the NT scheduler facility.

When a fw logswitch is performed the existing log is written to a new file named in this format, ddmmyyyy-hh:mm:ss.log. As an example, if it is May 23, 2001 at 1:00 am when the *fw logswitch* command is run, the resulting backup log will be named 23May2001-01:00:00.log. These backups can then be moved to another system or written to tape for archival purposes.

The command for performing the fw logswitch is very simple. On a Solaris or IPSO or NT system; from the command line type,

> fw logswitch

To schedule this in the Unix environment, implement the command in a cron job. Cron is the facility for performing commands or scripts at a certain time. A quick way to put this into a cron job is to type "crontab –e" as the root user. This will open up the crontab file for the root user. Add the following line into the file.

0 1 * * * fw logswitch

The format of this cron command is as follows, minute hour day month weekday command. The * stands for ANY. This job will be interpreted by the system as, "Run the command 'fw logswitch' at 1:00 am every day".

To schedule this command in the NT environment you need to create a batch file with the fw logswitch command. Then go to Start:Programs:Accessories:System Tools:Scheduled Tasks, run the Scheduled Task Wizard and enter the batch file.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Once your logs files have been written to a backup file you can begin to export them into an ASCII format so you may begin to analyze them. The command that accomplishes this is the *fw logexport* command. The format of this command is as follows:

> fw logexport –d –i input.file -o output.file –n.

The –d switch specifies a delimiter character with the default being the semi-colon. The –i switch specifies the input file and the –o switch specifies the output file. The –n switch tells the program to not perform any name resolution on the IP addresses. This will greatly speed up the export process. If you have the time and want to see the domain names instead of IP addresses you may omit this switch. One word of caution though, the size of the output files that get created grow an average of 2.5 times the input file. Make sure there is room on the drive. My logs average 20 Megabytes of data a day.

Using the example of the file created above the command to export it would be this,

> fw logexport -d , -i 23May2001-01:00:00.log -o fwlog5-23-01.txt –n

This inputs the backup log file from May 23, 2001, and outputs it to the file "fwlog5-23-01.txt", using a comma to separate the fields.

The first record of the output file will contain the field names to simplify importing this file into other programs. It will be similar to the following though the order may be different.

num, date, time, orig, type, action, alert, i/f_name, i/f_dir, proto, src, dst, service, s_port, len, rule, icmp-type, icmp-code, xlatesrc, xlatedst, xlatesport, xlatedport, message, user, reason, scheme:, methods:, srckeyid, dstkeyid, sys_msgs

The following table defines the fields.

num	Record number
date	Date record was written
time	Time record was written
orig	Which firewall is writing the record
type	Log entry or Alert
action	Accept or Drop
alert	Kind of alert generated, if any
i/f_name	Firewall interface that the traffic was seen on
i/f_dir	In relation to the firewall, inbound or outbound
proto	TCP, UDP, ICMP
src	Source IP address
dst	Destination IP address
service	Destination port

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

s_port	Source port
len	Packet length
rule	Firewall rule that triggered the log Entry
icmp-type	ICMP Type
icmp-code	ICMP Code
xlatesrc	NAT, the source IP that was translated
xlatedst	NAT, the destination IP that was translated
xlatesport	NAT, the translated source port
xlatedport	NAT, the translated destination port
message	Firewall message to explain an action
user	User authenticated by the Firewall
reason	Is Encryption happening, authentication?
scheme:	Encryption Scheme being used
methods:	Encryption protocol being used
srckeyid	Key scheme used by source IP
dstkeyid	Key scheme used by destination IP
sys_msgs	System messages

Log Analysis

Now that the log has been exported into an ASCII format, it is ready to undergo analysis. There are many tools available to manipulate flat file data. They range from spreadsheets to relational databases. MS Access is a nice solution to use for viewing and analyzing the firewall log data. It is easy to learn, deployed in the default image of many organizations and reasonably quick. It also contains an acceptable reporting capability to satisfy management. Because Firewall-1 has a tendency to export the fields in different orders, it is easiest to import the logs into MS Access on an individual basis. Again, there are tools available, to keep the logs in a consistent format. This would be good if you wanted to automate the import process or if you wanted to develop a database to track multiple logs from different firewalls.

Importing the data into MS Access is relatively easy. As you step through the importing process make sure that all fields are set to text format. This will make queries much easier to perform and insure that all data is imported into the database.

Once the data is in your database you can query it to view trends, and produce reports. There is a lot of information and the idea is to zero in on the important information to save time. The queries that are developed can be easily integrated into a report to get a quick view of the activity on your firewall. Some good places to look at for help to develop your queries are:

1) Cert.org, http://www.cert.org/nav/index_red.html, this page shows attack reports and port scan activity.
2) Incidents.org, http://www.incidents.org/cid/index.php, this page shows high malicious activity. It is well organized.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

3) Robert Graham's site, http://www.robertgraham.com/pubs/firewall-seen.html, an excellent tutorial on ports and ICMP as well as other information. This site is highly recommended.
4) Lantz Spitzner's site, http://www.enteract.com/~lspitz/, this site has a lot of good information on firewalls and the Honeynet Project.

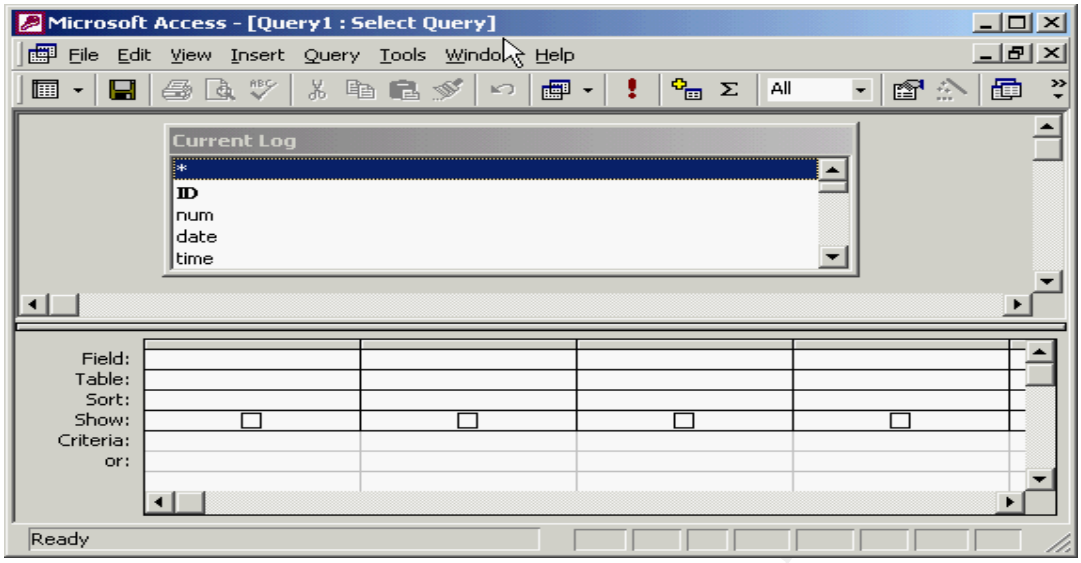
From visiting these sites the following list of queries were formed.

1) The top 5 IP addresses being dropped by my firewall. These addresses may possibly be attempting a scan of my network.
2) The top 10 IP addresses hitting my website.
3) The top 10 websites being viewed by company employees. (Spitzner)
4) Connection attempts from Port 0-5, because these are normally used in OS fingerprinting attacks.
5) Connection attempts from IP 0.0.0.0. This is a common fingerprint technique. (Graham)
6) Attempted connections to ports 21/ FTP, 23/Telnet, 110/POP3, and 143/Imap. These services are not offered on my network and attempts to connect to these indicate a vulnerability probe.
7) Attempts to 111/RPCBind. This is a widespread automated attack and I check for it both incoming and outgoing because of the possibility of internal network machines being used as zombies.
8) ICMP types 0, 8 to the Firewall for Smurf attacks.
9) ICMP types 5, 9, redirect and router advertisement. Could be indicative of a "man in the middle attack".
10) ICMP type 12. This is a parameter error message, which is highly unusual and may be indicative of an attack.
11) Port scans in the range of, 33434 – 33600. This is the range of UNIX Trace Route ports and may indicate a mapping attempt through the Firewall.

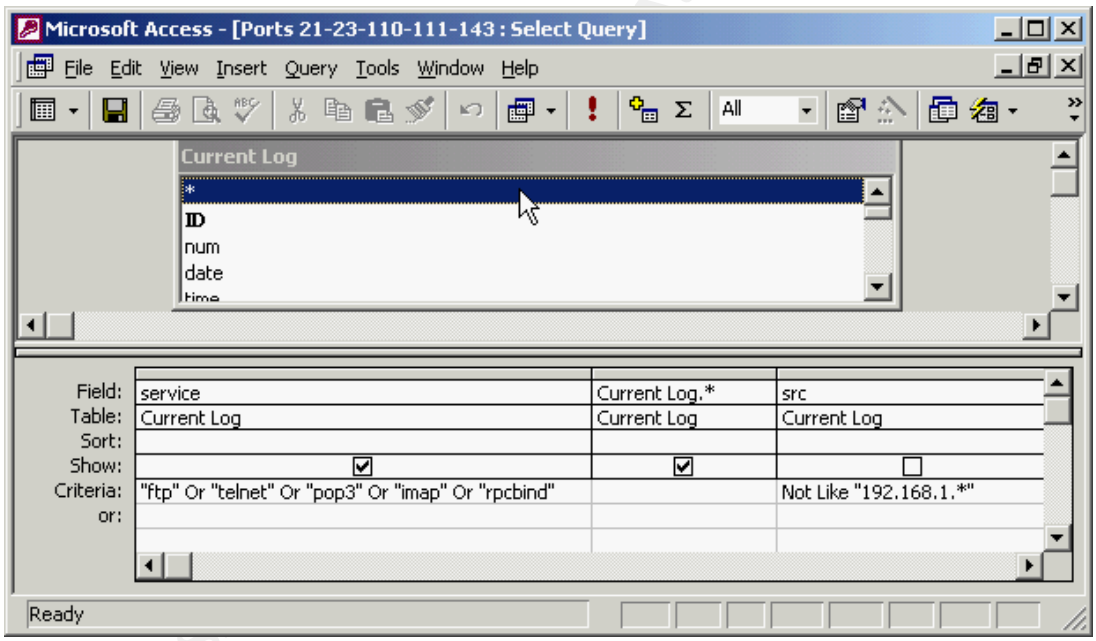
The first thing that must be done is to copy the imported log that you want to analyze to a table called Current-Log. This allows you to develop a set of queries that will work without being changed with every new log analysis. From this list a group of database queries were built to pull the relevant information from the database and output into a daily report.

To develop a query in MS Access, from the main window click on Queries in the Objects Bar on the left side of the window. Then double-click on "Create Query in design view" in the main window. You will then see a screen like this:

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.



You can then point and click to build the query. Using the criteria from list items 6 and 7, the completed query looks like this.



After developing the queries in MS Access you can go to the Report Wizard and develop reports based upon your queries. Using the built in Wizards, this is an extremely simple task.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Summary

Security logs are an important component of an organization's security policy. We activate them and let them gather data; we should take the time to review them. Firewall logs can alert us to ongoing attacks, probes, or even malfunctioning rule sets. Checkpoint Firewall-1 does not come with very good log reporting tools, but by taking a little time and performing some research, we can implement some working tools that let us affordably analyze our logs and produce reports that quickly let us visualize the possible dangers to our networks.

I was surprised at what I discovered by viewing my organization's firewall logs. We had a server that had been compromised and was trying to send rpcbind scans to outside IP addresses. Luckily the rule set was dropping those attempts. I was also surprised at the amount of probes and attempts against my network. The daily reporting has helped to awaken others in the organization and allowed changes to be budgeted for and made.

The database developed during this project is freely available for download and improvements at http://secure-net.hypermart.net/index.htm.

© SANS Institute 2000 - 2002 Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

References

Brandt, Ken and Green, Stu and Zuniga, Enrique. "Battle Plans".
Information Security March 2001: page 86-94.

Cambridge Technology Partners Enterprise Security Services "Firewalk"
<http://www.packetfactory.net/Projects/Firewalk/firewalk-final.html>
(31 May 2001).

CERTCC "CERT Coordination Center: Incidents, Quick Fixes, and Vulnerabilities"
2001. <http://www.cert.org/nav/index_red.html>
(31 May 2001).

Chaswick, William R. and Bellovin, Steven M.
Firewalls and Internet Security - Repelling the Wily Hacker. Boston: Addison-Wesley, 1994. 14th Printing, 2000.

Checkpoint Software "Check Point Software Gains Nearly Ten Percent Additional Market Share in the Worldwide Firewall Market."
<http://www.checkpoint.com/press/2000/idc112800.html>
(30 May 2001).

Graham, Robert "FAQ: Firewall Forensics (What am I seeing?)."
<http://www.robertgraham.com/pubs/firewall-seen.html>
(29 May 2001).

IANA "IANA | Protocol/Number Assignments Directory."
2001. <http://www.iana.org/numbers.htm>
(31 May 2001).

Sans Institute "incidents.org - By The SANS Institute: Consensus Intrusion Database."
2001. <http://www.incidents.org/cid/index.php>
(31 May 2001).

Spitzner, Lance "Lance's Security Papers."
<http://www.enteract.com/~lspitz/>
(2 June 2001).

Welch-Abernathy, Dameon D. "FireWall-1 FAQ: Drop Does Not Always Mean Drop"
1999. <http://www.phoneboy.com/faq/0134.html>
(31 May 2001).

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.