Global Information Assurance Certification Paper

Unix Security Logging
Ray McAlarnen
April 18, 2001

Introduction

Unix operating systems have the ability to log various types of information from process activities to system errors to user activities. This paper will discuss the various types of logs that can be utilized to monitor the system and assist in detecting unauthorized access or the attempt of unauthorized access. The default settings of some Unix logs may not capture all the necessary information one needs to detect unauthorized access or the attempt. Some of the logs have configuration files that may need to be adjusted to capture what is appropriate for your environment.

This paper will not tell you what should be logged or how often to review the logs. That is a determination that must be made based on your environment and the information you are protecting. However, we will discuss the different log files, how to read them, and (if applicable) their configuration file and how to modify it. In particular, we will be discussing the syslog and it's configuration file, the sulog and it's configuration file, the loginlog, and the utmp and wtmp files.

Log files may have different names and different locations depending on the type of Unix that is being used. In this paper, we will be discussing the Solaris 2.6 operating system.

Syslog

The system log facility (i.e., syslog daemon - syslogd) generates notification (i.e., email, logging, paging, etc.) of specific events that occur. The syslog daemon is started at boot time and reads its configuration file (/etc/syslog.conf). The syslog daemon then runs continuously unless purposely stopped (i.e., via HUP).

The syslog file is usually located at /var/adm/messages. A syslog message typically consists of four parts: date/time, server name, program name, and the message. For example,

Mar 17 18:32:42 myhost su: 'su root' failed for ray on /dev/pts/6
Mar 17 18:33:01 myhost su: 'su root' succeeded for ray on /dev/pts/6
Mar 19 08:36:06 myhost login: REPEATED LOGIN FAILURES ON /dev/console
Mar 20 07:00:20 myhost unix: NOTICE: alloc: /var: file system full
Mar 21 22:17:47 myhost snmpdx: error while receiving a pdu from mysite.com.3820: The message has the wrong version (1)
Mar 21 22:17:50 myhost last message repeated 2 times

As can be seen from the above example syslog, the log can record many different types of errors:

su attempts, login failures, and various system messages. Also, if the same information to be logged occurs many times in a row, the syslog will not log each message but will document that it occurred x number of times (i.e., the last line of the example).

Syslog Configuration

The syslog configuration file is located at /etc/syslog.conf and might look like:

```
Mail.debug          /var/adm/mail.log
*.info; mail.none   /var/adm/messages
*.alert             /dev/console
*.alert             root
*.emerg             *
```

The first column is the selector that specifies which kind of messages to log. There are two parts to the selector: a facility (i.e., mail, user, printer, etc.) and a priority (informational, error, critical, emergency, etc.). The second column is the action field that specifies what should be done with the message (i.e., log in a specific file, send to a user's terminal, etc.). A tab character must be used between the selector and the action fields.

Practical Unix & Internet Security describes the syslog facilities and priorities as follows:

Name	**Facility**
kern	Kernel
user	Regular user processes
mail	Mail system
lpr	Line printer system
auth	Authentication system, or programs that ask for user names and passwords (*login*, *su*, *getty*, *ftpd*, etc.)
daemon	Other system daemons
news	News subsystem
uucp	UUCP subsystem
local0..local7	Reserved for site-specific use
mark	A timestamp facility that sends out a message every 20 minutes

Priority	**Meaning**
emerg	Emergency condition, such as an imminent system crash, usually broadcast to all users
alert	Condition that should be correct immediately, such as a corrupted system database
crit	Critical condition, such as a hardware error
err	Ordinary error
warning	Warning

notice	Condition that is not an error, but possibly should be handled in a special way
info	Informational message
debug	Messages that are used when debugging programs
none	Do not send messages from the indicated facility to the selected file. For example, specifying **.debug;mail.none* sends all messages except mail messages to the selected file.

The priorities above are listed from most important down to lowest. The priority of a message is the minimum level that has to occur for the action to be taken. For example, if there is a selector of auth.notice, then action will occur for all authentication messages of priority notice and above while no action will be taken for authentication messages of info and debug.

Therefore from our sample syslog.conf file above, the second line tells us that all informational and above priority messages and no mail messages are to be written to the syslog. The fourth line says that all alert and emergency priority messages are to be shown on root's screen. The last line determines that any emergency messages should be broadcast to every logged in user's screen.

You can even set up various logs to record different types of messages. For example, you could log all authentication attempts (auth.*) to a complete different log than syslog, say /var/adm/auth_log. You could even log directly to a printer (i.e., by having the action set to /dev/ttya).

You may want to have a secure machine that does nothing but receive logs from the other servers in your environment. The syslog daemon can do this by having the action specify a different server, i.e.,

auth.* @loghost

where loghost is defined in the /etc/hosts file.

Syslog is a powerful logging facility that can log a variety of events in many different locations. However, you must take the time to consider how much to log, where you want to log different events, and how long to maintain the logs. Remember, logs that are never reviewed do not do you much good. Also, don't forget to prune the logs, otherwise you may run out of disk space and shut down your server.

Sulog

The 'su' command will allow a user to 'substitute user'. When a user wants to temporarily log into another user's account, they can issue the su command plus the user name (or a blank to attempt to su to root). If that user's password is correctly entered, a new shell process is created

that has the real and effective user ID, group ID, etc. of that user. The sulog tracks all usage of this command. The format of the sulog is:

SU date time result(+/-) port username-attempted username

where,

date	is in the month/day format of MM/DD
time	is in the hour/minute format of HH:MM and HH is in the 24-hour format
result	is in the format of a + or a -. A plus signifies a successful attempt and a – signifies an unsuccessful attempt.
port	is the name of the terminal device that the su was executed (i.e., console, pts/4, etc.).
username	is the user ID of the individual executing the su command
attempted username	is the user ID that the individual is attempting to switch to with su.

An excerpt from a sulog would look like:

SU 03/06 13:09 + pts/9 jsmith-root
SU 03/06 16:18 - pts/9 jsmith-root
SU 03/06 16:18 + pts/9 jsmith-root

The first and third entries would be a successful attempt (identified by the +) by jsmith to su to root. The second entry is an unsuccessful attempt (denoted by the -).

Sulog Configuration

The following is an example of the sulog configuration file located at /etc/default/su:

```
#ident  "@(#)su.dfl     1.6     93/08/14 SMI" /* SVr4.0 1.2   */

# SULOG determines the location of the file used to log all su attempts
#
SULOG=/var/adm/sulog

# CONSOLE determines whether attempts to su to root should be logged
# to the named device
#
#CONSOLE=/dev/console

# PATH sets the initial shell PATH variable
#
#PATH=/usr/bin:
```

```
# SUPATH sets the initial shell PATH variable for root
#
#SUPATH=/usr/sbin:/usr/bin

# SYSLOG determines whether the syslog(3) LOG_AUTH facility should be used
# to log all su attempts.  LOG_NOTICE messages are generated for su's to
# root, LOG_INFO messages are generated for su's to other users, and LOG_CRIT
# messages are generated for failed su attempts.
#
SYSLOG=YES
```

The first section of the configuration file is setting where the log of su attempts should be stored and the name of the file. The next section is determining if we are going to log su attempts to the console in the Data Center (or some other device). In our example, it is commented out and therefore not used. You will have to make a determination if you want su attempts to be logged to your console or not. The next two entries are the initial shell PATH that would be set depending on whether the su was to a regular user or to root. Again, the settings here are commented out and you will have to make a determination if these settings are appropriate or necessary in your environment.

The last section determines if su attempts should be logged in the syslog as well. A caveat here is that even though you say 'YES' your syslog may not capture the information due to your configuration file setup. For example, if you are not logging any of the auth facility messages (auth.*) or any general notice (*.notice), info (*.info), or critical (*.crit) priority messages, you will not log any su attempts to the syslog. See the **Syslog Configuration** section for more information on these settings.

Loginlog

The loginlog resides at /var/adm/loginlog and is utilized to record failed login attempts. This file is in ASCII and the format of the contents is: attempted name, terminal, and date/time. For example,

```
root:/dev/pts/5:Fri Mar 16 18:12:14 2001
root:/dev/pts/5:Fri Mar 16 18:13:01 2001
```

Five (5) consecutive unsuccessful login attempts to a user ID constitutes a failed attempt and is then recorded in the loginlog as one failed attempt. Therefore, from the above example, there have been 10 unsuccessful attempts to enter root's password.

The file does not exist by default and must be created (i.e., via the touch command). According to the Solaris 2.6 Reference AnswerBook man page(4) for loginlog, "To enable logging, the log file must be created with read and write permissions for owner only. Owner must be **root** and

group must be **sys**."

Utmp, utmpx

The /etc/utmp (and the extended version utmpx – which captures all the utmp information as well as inittab ID, session ID, and remote host name) file is a log of all the users currently logged onto the server. This is a binary file. Therefore, you need to read it through the use of various commands (i.e., who, users, finger, etc.), which all have different output formats.

Wtmp, wtmpx

The /etc/wtmp (and the extended version wtmpx– which captures all the wtmp information as well as inittab ID, session ID, and remote host name) file is a log of all logins and logouts that have occurred on the server. This is also a binary file and needs to be read with the last command. Using the last command without any arguments will display all the logins and logouts for every device. To manage the amount of information, you can identify specific users or devices as arguments. This file can grow to be very large; so, you must monitor it's size and prune or transfer the information to another file as necessary.

Conclusion

Unix has many different logs available to assist with security. By default, Unix does not capture everything that may be of importance. Some of the logs (syslog and sulog) may need to have their configuration file modified. Another (loginlog) needs to be created for the operating system to use it. Others (utmp, utmpx, wtmp, and wtmpx) cannot be read directly and have to be accessed through commands. Some of the information recorded may overlap between these logs (i.e., login). The important thing is to understand what these logs can and cannot do, determine what is necessary for your environment, and then implement and review these logs.

References

Garfinkel, Simson and Gene Spafford. Practical Unix & Internet Security, Second Edition. : O'Reilly & Associates, Inc., 1996. 289-318.

Nemeth, Evi, et. al. Unix system Administration Handbook, Second Edition. Upper Saddle River, NJ: Prentice Hall PTR, 1995. 200-217.

CERT Coordination Center. "Understanding system log files on a Solaris 2.x operating system." March 2, 2000.
URL: http://www.cert.org/security-improvement/implementations/i041.12.html (April 12, 2001)

CERT Coordination Center. "Configuring and using syslogd to collect logging messages on systems running Solaris 2.x." January 29, 2001.
URL: http://www.cert.org/security-improvement/implementations/i041.08.html (April 12, 2001)

Solaris 2.6 Reference Manual AnswerBook. "loginlog." Man Pages(4): File Formats.
URL: http://docs.sun.com/ab2/@LegacyPageView?toc=SUNWab_40_4%3A%2Fsafedir%2Fspace3%2Fcoll3%2FSUNWaman%2Ftoc%2FREFMAN4%3A0114_loginlog.4;bt=man+Pages(4)%3A+File+Formats;ps=ps%2FSUNWab_40_4%2FREFMAN4%2F0114_loginlog.4&Ab2Lang=C&Ab2Enc=iso-8859-1 (April 13, 2001)

Solaris 2.6 Reference Manual AnswerBook. "syslog.conf." Man Pages(4): File Formats.
URL: http://docs.sun.com/ab2/@LegacyPageView?toc=SUNWab_40_4%3A%2Fsafedir%2Fspace3%2Fcoll3%2FSUNWaman%2Ftoc%2FREFMAN4%3A0178_syslog.conf.4;bt=man+Pages(4)%3A+File+Formats;ps=ps%2FSUNWab_40_4%2FREFMAN4%2F0178_syslog.conf.4&Ab2Lang=C&Ab2Enc=iso-8859-1 (April 13, 2001)

Solaris 2.6 Reference Manual AnswerBook. "sulog." Man Pages(4): File Formats.
URL: http://docs.sun.com/ab2/@LegacyPageView?toc=SUNWab_40_4%3A%2Fsafedir%2Fspace3%2Fcoll3%2FSUNWaman%2Ftoc%2FREFMAN4%3A0175_sulog.4;bt=man+Pages(4)%3A+File+Formats;ps=ps%2FSUNWab_40_4%2FREFMAN4%2F0175_sulog.4&Ab2Lang=C&Ab2Enc=iso-8859-1 (April 13, 2001)

Solaris 2.6 Reference Manual AnswerBook. "utmp, wtmp." Man Pages(4): File Formats.
URL: http://docs.sun.com/ab2/@LegacyPageView?toc=SUNWab_40_4%3A%2Fsafedir%2Fspace3%2Fcoll3%2FSUNWaman%2Ftoc%2FREFMAN4%3A0201_wtmp.4;bt=man+Pages(4)%3A+File+Formats;ps=ps%2FSUNWab_40_4%2FREFMAN4%2F0195_utmp.4&Ab2Lang=C&Ab2Enc=iso-8859-1 (April 13, 2001)

Solaris 2.6 Reference Manual AnswerBook. "utmpx, wtmpx." Man Pages(4): File Formats.
URL: http://docs.sun.com/ab2/@LegacyPageView?toc=SUNWab_40_4%3A%2Fsafedir%2Fspace3%2Fcoll3%2FSUNWaman%2Ftoc%2FREFMAN4%3A0202_wtmpx.4;bt=man+Pages(4)%3A+File+Formats;ps=ps%2FSUNWab_40_4%2FREFMAN4%2F0196_utmpx.4&Ab2Lang=C&Ab2Enc=iso-8859-1 (April 13, 2001)