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 (Security 401)"
at http://www.giac.org/registration/gsec

Maintaining the Forensic Viability of Logfiles

Tom Ceresini

May 29, 2001

Introduction

Collecting and retaining network and system logfiles has many advantages. There are several good sources of information related to what information should be logged, how best to log it, and in what ways this information can be used (Hunter, 2000; Morton, 2000; Pitts, 2000). However, the requirements for the use of logfile data for technical purposes such as intrusion detection are quite different from, and not always complementary to, the requirements for the use of such data in a legal setting (Sommer, 1999).

A "forensically viable" logfile is one that has been tracked and protected from the time it was created, and which contains entries that relate to the legal issue at hand. In most cases, the requirement to use a particular logfile in a legal investigation comes some time after the log data was collected and stored. Therefore, in order to guarantee that such data will be considered valid and pertinent to an issue presented in a trial, the data collection and storage policies and procedures must be implemented in advance with such use in mind. This paper seeks to explain the legal requirements as they relate specifically to network and computer logfiles, as well as to suggest some technical and procedural methods for achieving those requirements.

There are a number of issues to consider while reading this material. First, I am not a lawyer. I provide this information from my perspective as a computer and network security engineer. I believe, however, that the principles described in this paper can provide a basis for thoughtful consideration of how best to protect your logfiles. Second, the scope of this paper is limited to the legal system within the United States of America. While the general principles may still be useful, it is likely that rules of evidence and prosecution methods in other countries, and even from one state to another within the U.S., will be different. Therefore, you should seek advice from your corporate or institutional legal counsel on issues related to the admissibility of logfile data as evidence in legal proceedings.

Legal Considerations

To be able to prosecute someone for an incident, for example, a system penetration, you must be able to demonstrate why you think a particular individual or group is at fault. That is, you must present evidence to support your conclusion. A variety of network and system logfiles are frequently used to investigate such incidents and, later, to demonstrate to others what you believe you have found. These logfiles, then, will serve as pieces of evidence in the event of a trial or other legal proceedings. What requirements and expectations of the legal system should be considered when dealing with such data?

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

According to an article in SC Magazine (Holley, 2000),

> "…a forensically sound [computer] examination is one conducted under such controlled conditions that it is completely documented, it is repeatable and its results are verifiable…[it] changes no data on the original evidence, preserving it in pristine condition. And regardless of who completes an examination of the media and the specific tools and methods employed, they should get the same results."

A recent paper from Veritect, Inc. states, "Preserving evidence according to Federal Rules of Evidence gives a company or individual choices that otherwise would not exist..." (Veritect, 2001). Even if you don't anticipate use of logfiles in the persuit of legal remedy, other organizations may seek to take action against you or to request your assistance in an action against a third party. Clearly, it is important to implement appropriate procedures and technologies in advance in order to adequately meet these requirements.

There are three basic tasks to be considered when dealing with logfiles as evidence. First, logfiles must be preserved in a way that guarantees they can't be lost, damaged or modified. This is true even before you know that some data in a given logfile can or will be used as evidence, since the potential for intentional or unintentional damage is high. Second, you must find the evidence within the logfiles. Finally, you must prepare the evidence and document everything that is done with the original logfiles, as well as the media on which it is stored, so that it can withstand judicial scrutiny (Veritect, 2001).

There are several principles regarding the admissibility of evidence that must be considered, according to Alan Brill of Kroll Associates (Brill, 1999). First, it must have integrity – in other words, the information must be what you say it is, and you must be able to demonstrate that you collected and handled the information in a way that was both lawful and accurate. Second, it must be probative – that is, it must help the court decide the issue being considered. Both the applicability of the information to the issues and the technical details of the collection and storage procedures may need to be explained to the judge and jury. Third, it must be retrieved by an expert – the individuals involved in the process of obtaining and handling the information must have the knowledge and ability to prevent modification of the data. Otherwise, the reliability of the information itself may be called into question.

Proper handling of evidence requires that a "chain of custody" be established and maintained. The term refers to the ability to demonstrate where the evidence has been and who had access to it from the time the information was collected until its presentation as evidence in court. This can be done by presenting documentation in the form of policies and procedures as well as records showing that those policies and procedures have been adhered to in the case of the specific logfiles to be used as evidence. This includes such details as how the data was collected and stored, how it was copied, and who had access to the data at any point in time.

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

The key to maintaining the forensic viability of logfiles is to be able to answer "yes" to the question, "Can the data be trusted?" In addition to the above points, it is important to show that the various hardware and software components involved in registering, transmitting and storing the data were in proper working order at the time the data was recorded and during subsequent handling of the media on which it is stored.

The consequences of failing to adequately maintain the chain of custody can be significant. Judges have become less tolerant of poor handling of electronic evidence, including the granting of motions for sanctions against companies who fail to maintain a satisfactory chain of evidence for electronic data in their possession (Racich, 1999).

It is important to remember that, in addition to the actual logfiles, any written communication may be required to be made available to the court or opposing counsel in a discovery process. As stated in an article entitled "Computer Forensics" in the magazine Internal Auditor:

> "…all reports of [an] investigation should be prepared with the understanding that they may be read by management, the authorities, opposing counsel, the court, the press, and the general public...only the facts of the investigation should be presented, and opinions should be avoided altogether. If the company's legal counsel is involved, much of the investigative work should be privileged under the 'attorney work product doctrine' and therefore will be protected from disclosure to opposing counsel in a criminal trial…" (Bigler, 2000).

Policies and Procedures

The goal, then, is to ensure that logfiles cannot be tampered with so that you can preserve all potential legal avenues in the future. Toward this end, you must maintain a proper chain of custody over the logfiles, and this requires that you establish and monitor the proper functioning of the hardware, software and operational procedures used in the process.

It is useful for computer security professionals and corporate or institutional counsel to work together in crafting and auditing compliance with policies, procedures and standards related to logfile collection and storage. A recent Computerworld article on this topic stated, "What's needed is a team approach, especially one that involves a corporate legal department that understands the investigative process and can help law enforcement…" (Thibodeau, 2001).

In an article entitled, "In-House Cyber Security: Corporate Counsel Must Plan Ahead to Minimize Risks of Data Security Breaches" in Legal Times (Zwillinger, 2001), Marc J. Zwillinger presented this issue from the perspective of a company's legal counsel:

> Simply put, as in-house counsel, you must become familiar with the network security architecture and technology policies of your organization. Without that knowledge, you may fail to recognize how the organization may be exposed to

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

> serious security breaches, criminal and civil litigation, and the spread of embarrassing and damaging news to shareholders and the public…
>
> Left to their own devices, the IT staff is not likely to configure the corporate network in a way that takes into account the relevant information security and data protection regimes in all the jurisdictions traversed by the network.

Working together, you can establish policies and procedures to support the forensic viability of your logfiles. It is essential that all policies and procedures are presented in written form, and that all affected personnel are educated in the proper execution of the procedures. It is also crucial that complete logs be kept of all activities that related to the execution of those procedures, and that such logs are external to the systems being monitored.

Here is a list of some of the specific areas for which policies and procedures must be established. "Logging infrastructure systems" include all loghost servers plus any supporting systems such as NTP timeservers, etc.

Personnel

- Provide education regarding policies and procedures to all personnel involved with maintenance of logging infrastructure systems. Require that personnel sign these policies to indicate their understanding of and commitment to follow them. Work with your legal counsel and human resources or personnel department to ensure that these signed documents are legally enforceable.
- Require background checks for personnel with significant access authority to logging infrastructure systems.

Hardware, operating system and software events and maintenance

- Clearly document all operational aspects of maintaining your logging infrastructure systems. This includes the performance of normal maintenance activities, system backup, and handling of unusual events such as system error messages and hardware failures.
- Provide clear guidelines regarding the installation or update of hardware and software.
- Dedicate all logging infrastructure systems to their intended task. Install only the hardware, services and client software necessary to perform that task.
- Restrict access to logging infrastructure systems to only those users with direct responsibility for maintaining those systems; ideally, require the use of two-factor authentication. In addition, restrict access to the console only, or, if necessary, require the use of encrypted access from the internal or service network segment (using OpenSSH or similar tools).
- Require that all systems and network components and cabling in your logging infrastructure systems (both clients and servers) be isolated to a single physical

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

security perimeter. In addition, strictly define how network ingress and egress from within that perimeter will be controlled.
- Control and record personnel access to the physical security perimeter housing logging infrastructure systems.
- Require daily checks of all sensor and logging devices and networks to ensure reliability. In addition, require periodic checks of physical systems such as power, UPS (power backup), air conditioning, etc.

Incident response

- Require that each incident investigation maintain a separate log. If a given log must be surrendered to law enforcement officials or opposing counsel, this will limit the release of information to the particular incident required.
- Ensure that exact copies of the original logfiles be used in incident investigation.

Logfile handling

- Write logfiles to write-once media immediately upon receipt by the loghost.
- Require anti-tamper controls to logfile entries be undeletable and unalterable. This will permit your audit capabilities to survive (to the extent possible) both successful and unsuccessful attacks.
- Forbid the alteration of original media in any way. Make write-once copies and file the original as soon as possible. Mark the copies to indicate that they are exact reproductions of the original.
- Restrict any handling of original media to authorized network or computer security personnel only and log such handling on a per-transaction basis.
- Restrict any handling of copied media and logfiles to authorized network or computer security personnel only and log such handling on a per-transaction basis. Restrict access to any reports based on such data to a need-to-know basis.
- Store original media in conditions that will ensure that the media and data are not degraded. Put media in appropriate container (case, envelope, etc.) and seal with a tape signed and dated by the person responsible for copying and filing that media.

Audit controls

- Require regular audits of compliance with all procedures, including review of all procedural logs.

Implementation Considerations

In addition to establishing and ensuring adherence to policies and procedures, there are specific technical issues to consider in the implementation of a logging infrastructure.

Hardware

© SANS Institute 2000 - 2002, Author retains full rights.

- Set up a single centralized loghost or group of loghosts.
- Write log entries directly to write-once media upon receipt by the loghost. For forensic purposes, magneto-optical drives have a number of advantages over CD-R/CD-RW drives (International Journal of Forensic Computing, 1997). One possibility is to write the log entry to the MO drive, and have a second process copy the entries from the MO drive to a CD-R drive; this latter media can be used as a working copy, while the MO media is archived to permanent storage.
- Several vendors have devices or systems based on "gap" (or "air gap") technology to protect previously written data (Bobbit, 2000).
- Make sure your loghost has sufficient resources to operate efficiently. In particular, make sure there is sufficient disk space and that write-once media is replaced as needed.
- Consider using redundant hardware (e.g., dual power supplies, RAID drives).
- Install a local printer as a local log for notable events, especially any significant log entries for the loghost itself (in addition to logging this data to a standard logfile). Date, initial, copy and archive the original output, and use the copies for review and investigation.
- Consider using some non-network channel (e.g., serial or parallel port) to transmit real-time alert messages of critical events on the loghost to your network operations center console or oncall pager.

Operating system

- Use a readily securable operating system. Some alternatives to consider are TCSEC C2 certified systems, OpenBSD, and operating systems that can be tailored to include only the features and services that you require.
- Consider using an open source-style operating system so that you can examine and modify (if necessary) the source code. This will permit you to check the authenticity of the source files, compile the kernel and executable files with exactly the options you need, and include in your system only those services and utilities you require on the system. The use of vetted source code to compile the kernel and executable files is preferable to getting and using binary files, since you can be sure that what you're running is exactly based on the source code you've examined.
- Use system integrity programs such as Tripwire to generate baseline information on important files and regularly rerun and compare the new results to the baseline information. Compare these findings against the system operations log to find undocumented file changes, and investigate to determine the cause of such changes.
- Document and retain all details of the OS installation as well as any upgrades or maintenance that may be done afterwards.
- Use post-installation tools such as Bastille Linux (for Linux systems) to "harden" your system. Bastille Linux can also be used on a regular basis as an auditing tool.
- Gather baseline utilization statistics on your loghost and network, and compare these at regular intervals with current utilization. Investigate any anomalous findings.

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

- Enable and review all appropriate accounting and auditing tools to accurately record operator and other system-level activity.
- Create accounts only for persons who must access the system, and give each account only the required privileges and group access permissions. Don't create any "shared" accounts.
- If the OS supports ipfilter, ipchains or some other kernel-level firewall capability, consider using it to restrict and log system access.
- Consider using separate filesystems for different logfiles to provide some protection against denial-of-service schemes that attempt to fill up the loghost's file system.
- If your OS supports it, set up all logfile filesystems as "append-only."
- Consider setting the system clock to UTC instead of local time. This could simplify correlation of logfiles from systems originating in different time zones.

Software

- While the standard Unix syslog service provides many advantages, it also has some significant limitations in data security and transmission reliability (Hunter, 2000). Use an alternative syslog program (Pitts, 2000) to provide enhanced functions such as TCP connections, encrypted transmission of data across the network, public key signing of log entries for non-repudiation, etc.
- Use an alternative syslog server to enable log entry relay ability without alteration of the original log entry data from the central loghost to downline loghosts. This permits the restriction of interactive access to the central loghost while providing log data for analysis on other systems.
- In addition to logging the original log entries to traditional logfiles, consider setting up a specialized "metadata" logfile. This logfile could record information such as the loghost system date and time of receipt of individual log entries, source IP address of the log entry, and original log entry time stamp converted to UTC (in addition to the log entry as received).
- Carefully filter incoming log entries to separate logfiles, as appropriate, to simplify management and later interpretation of the logfile data.
- Consider use of a tool to convert Windows Event Log entries to syslog format and transmit them to a common loghost system (Gerhards, 2001). This can simplify management of logfiles across your facility.

Network

- Consider using a separate, "out of band" network for all logfile traffic. If you already have an out of band management segment, it may be appropriate to pass your logfile traffic on it. Use of such a network can help avoid spoofed log entries being sent to your loghost.
- Use access controls on firewalls, routers, switches and loghosts to ensure that network traffic is only accepted from known IP addresses and ports. Use ingress/egress filtering to reject spoofed packets.
- Consider the use of VPN-based tunnels to communicate between client and loghost systems (Hunter, 2000).

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

- Gather baseline utilization statistics on your network, and compare these at regular intervals with current utilization.
- Investigate the possibility of using a non-TCP/IP or even a non-Ethernet connection to transfer logfile data from client to loghost or from loghost to write-once media. Consider using serial, parallel or USB ports or specialized SCSI ports for this connection. These would be completely unavailable to the TCP/IP network and could be set up as write-only.
- At least one facility (SANS, 2001) has used a specially modified CAT5 cable to disable the transmit signal from the loghost system back to the network. In order for this to work properly, the cable was also modified to send a heartbeat signal from a second switch port to the loghost switch port. This ensures that the loghost runs in receive-only mode, although it thereby limits you to the use of the UDP protocol (since TCP requires two-way communication).

Supporting Systems

- Use one or more NTP servers to provide a common and consistent time to all systems. This will make the comparison and correlation of logfile entries from different systems much simpler. Ideally, have your primary on-site NTP servers get their time signal directly from an official time authority – in the U.S., NIST and USNO can provide this signal. NTP servers which get their time signals via a radio clock (based on GPS, CDMA or broadcast spectrum radio signals) will provide the most clearly traceable time signal. A reasonable alternative to these is NIST's Automated Computer Time Service (ACTS), which is accessible via a serial dial-out modem. Getting your time signal from an Internet-based NTP stratum 1 or 2 server might not be considered directly traceable to NIST or USNO, but is still preferable to no external standard.

Conclusion

It is important to take proper steps in advance to ensure that all logfile data you collect will be as useful as possible in any potential future legal action. There are specific legal requirements that suggest possible policy, procedures and implementation details to implement within your corporation or institution. Working to ensure the forensic viability of your logfiles will give you the widest range of options in future investigations and prosecution efforts.

References

Sources cited in the text:

Bigler, Mark. "Computer Forensics." Internal Auditors, Vol. 57 No. 1 (2000).

Brill, Alan. "Computer Forensics: Files From the Kroll Casebook." 14 December 1999. URL: http://www.krollworldwide.com/forum_kk01.cfm?199912141118 (11 April 2001).

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

Bobbit, Michael. “(Un)Bridging the Gap.” Information Security Magazine, July 2000. URL: http://www.infosecuritymag.com/articles/july00/cover.shtml (27 March 2001).

Gerhards, Rainer. “How to Monitor Windows NT from Unix.” 11 February 2001. URL: http://www.eventreporter.com/Common/en/Articles/EventReporter-Monitor-Windows-NT-From-Unix.asp (28 May 2001).

Holley, James. "September 2000 Market Survey: Computer Forensics." September 2000. URL: http://www.scmagazine.com/scmagazine/2000_09/survey/survey.html (26 March 2001).

Hunter, James. "Central Logging Security." 25 November 2000. URL: http://www.sans.org/infosecFAQ/unix/logging_sec.htm (2 April 2001).

International Journal of Forensic Computing. "CD-ROM -v- Optical Disks." August 1997. URL: http://www.computer-forensics.com/articles/ (12 April 2001).

Morton, Matt. "Logging and critical logs files: the Decision to Effectively and Proactively Manage System logging and Log Files." 9 December 2000. URL: http://www.sans.org/infosecFAQ/securitybasics/logging.htm (25 March 2001).

Pitts, Donald. "Log Consolidation with syslog." 23 December 2000. URL: http://www.sans.org/infosecFAQ/unix/syslog.htm (2 April 2001).

Racich, J. Christopher. "E-Evidence: Handle With Care." 23 August 1999. URL: http://www.krollworldwide.com/forum_kk01.cfm?199912141118 (11 April 2001).

SANS 2001. Birds of a feather (BOF) discussion entitled “Tamper-proof logs – possible???” 14 May 2001.

Sommer, Peter. “Intrusion Detection Systems as Evidence.” Computer Networks. Vol 31 Num 23-24(1999): 2477-2487. URL: http://www.zurich.ibm.com/~dac/Prog_RAID98/Full_Papers/Sommer_text.pdf (22 April 2001).

Thibodeau, Patrick. "IT Urged to work with corporate legal staff to fight computer crime." 4 April 2001. URL: http://www.computerworld.com/cwi/stories/0,1199,NAV47_STO59238,00.html (13 April 2001).

Veritect Inc. "What Lawyers and Managers Should Know About Computer Forensics." January 2001. URL: http://www.veritect.com/about_veritect/comp_forensics.pdf (22 April 2001).

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

Zwillinger, Marc J. "In-House Cyber Security: Corporate Counsel Must Plan Ahead to Minimize Risks of Data Security Breaches." Legal Times. 21 February 2001 (2001).

Other sources of interest:

Brockman, Belinda. "A Forensic Argument for Network Time Synchronization." 20 November 2000. URL: http://www.sans.org/infosecFAQ/legal/time_sync.htm (23 May 2001).

CERT Coordination Center. "Collect and protect information associated with an intrusion." URL: http://www.cert.org/security-improvements/practices/p048.html (26 March 2001).

CERT Coordination Center. "Configure firewall logging and alert mechanisms." 2 August 1999. URL: http://www.cert.org/security-improvement/practices/p059.html (25 March 2001).

CERT Coordination Center. "Configuring and using syslogd to collect logging messages on systems running Solaris 2.x." 29 January 2001. URL: http://www.cert.org/security-improvements/practices/p048.html (26 March 2001).

CERT Coordination Center. "Manage logging and other data collection mechanisms." 18 October 2000. URL: http://www.cert.org/security-improvements/practices/p048.html (26 March 2001).

DiCarlo, Vincent. "A Summary of the Rules of Evidence: The Essential Tools for Survival in the Courtroom." URL: http://www.dicarlolaw.com/RulesofEvidenceSummary.htm (21 April 2001).

Gottfried, Grant. "Taking a Byte Out of Crime -- From thirteen-year-old perpetrators to rogue nation saboteurs, dangers to your organization abound. Groom your computer forensic watchdogs!" 5 February 2001. URL: http://www.networkmagazine.com/article/NMG20010125S0001 (26 March 2001).

Hines, Eric and Yarochkin, Fyodor. "Complete Reference Guide to Creating a Remote Log Server." 22 August 2000. URL: http://www.linuxsecurity.com/feature_stories/feature_story-64.html (26 March 2001).

Kerr, Orin S. "Computer Records and the Federal Rules of Evidence." USA Bulletin, March 2000. URL: http://www.usdoj.gov/criminal/cybercrime/usamarch2001_4.htm (4 May 2001).

Schneier, Bruce and Kelsey, John. "Cryptographic Support for Secure Logs on Untrusted Machines." URL: http://www.counterpane.com/secure-logs.pdf (4 May 2001).

© SANS Institute 2000 - 2002, Author retains full rights.

Seifried, Kurt. "An Overview of OS Security Features - Part I." 22 March 2000. URL: http://securityportal.com/closet/closet20000426.html (24 March 2001).

Seifried, Kurt. "An Overview of OS Security Features - Part II." 29 March 2000. URL: http://securityportal.com/closet/closet20000426.html (24 March 2001).

Seifried, Kurt. "Electronic Forensics." 8 May 2000. URL: http://www.securityportal.com/cover/coverstory20000508.html (26 March 2001).

Seifried, Kurt. "Securing Your Network with OpenBSD." 21 June 2000. URL: http://securityportal.com/closet/closet20000426.html (24 March 2001).

Sommer, Peter. “Downloads, Logs and Captures: Evidence from Cyberspace.” British Computer Society Legal Affairs Committee, March 2000. URL: http://www.bcs.org.uk/lac/dlc.htm (4.May 2001).

Wenchel, Kevin. "Implementing C2 Auditing in the Solaris Environment." 1 November 2000. URL: http://www.eshaman.com/ (26 March 2001).

© SANS Institute 2000 - 2002, Author retains full rights.