Security Laboratory

The 6 Categories of Critical Log Information

Various
Version 3.01

Top 6 SANS Essential Categories of Log Reports 2013

Version 3.01

Questions?

Email us at info@sans.edu.

Introduction

The SANS Institute published the original “Top 5 Essential Log Reports” at the SANS Log Management Summit in 2006. Even now after more than 7 years, they deliver valuable insight for organizations dealing with logs – which today, in the age of compliance, really means everybody. However, the times are changing and new requirements for log data are emerging for security, compliance and operational reasons. Therefore we offer this update.

In the introduction to version 1.0, the authors stated: “In the spirit of this original consensus, the SANS community has again banded together in order to create the "Top 6 Essential Log Reports" consensus. This list is not intended to be a complete review of all the potentially useful log reports. Rather, the focus is on identifying the five most critical log reports for a wide cross-section of the security community. These are the top reports that should be reviewed on a regular basis. The goal is to include reports that have the highest likelihood of identifying suspect activity, while generating the lowest number of false positive report entries. The log reports may not always clearly indicate the extent of an intrusion, but will at least give sufficient information to the appropriate administrator that suspect activity has been detected and requires further investigation.”

The original Essential Log Reports included:

- ***Attempts to Gain Access*** **through Existing Accounts**
- **Failed File or *Resource Access Attempts***
- **Unauthorized *Changes* to Users, Groups and Services**
- **Systens Most Vulnerable to Attack**
- ***Suspicious or Unauthorized Network*** **Traffic Patterns**

This spirit and goals are even more alive today. Many organizations struggle with PCI DSS and multiple regulatory compliance frameworks (HIPAA/HITECH, FISMA, and many others) as well as with advanced threats (APT, malware, criminal hackers, mobile threats, cloud security challenges, etc). Also, malicious insiders now have new ways to harm or defraud a business. At the same time, the importance of information technology for businesses and government organizations has grown tremendously and will grow even more.

This research document published by the SANS Technology Institute, presents an updated 2013 version of Top 5 Log Reports, expanded to “Top 6 Essential Categories of Log Reports.”

The new reports are organized into six broad categories or report types with specific examples applicable to most organizations. They are designed to be technology agnostic and can be produced with commercial, open source or homegrown log management and analysis tools. More advanced Security Information and Event Management (SIEM) tools can be used as well.

While the focus of this document is log reports, the importance of log management also needs to be mentioned, as these reports are only as good as the data collected from network devices and applications. To ensure the confidentiality and integrity of log messages, logs should be, as a minimum, transferred via an encrypted channel and stored in an encrypted format. Additional best practices might be placing logs on a separate drive or share from the operating system or application, securing them with additional access controls, generating cryptographic hashes to prove integrity and definitely making sure that all log sources are time synchronized.

The new top report categories are:

1. **Authentication and Authorization Reports**
2. **Systems and Data Change Reports**
3. **Network Activity Reports**
4. **Resource Access Reports**
5. **Malware Activity Reports**
6. **Failure and Critical Error Reports**

In the rest of the document, we will cover each category with specific examples.

Authentication and Authorization Reports

These reports identify successful and failed attempts to access various systems at multiple user privilege levels (authentication) as well as specific privileged user activities and attempts to use privileged capabilities (authorization).

Why They Are Important

Authentication is the main barrier and means of controlling access to today's systems. From simple passwords to tokens and cryptographic mechanisms, reviewing authentication activity across the organization is one of the key security activities.

Specific Reports

Key reports in this category are:

- **All login failures and successes by user, system, business unit:** this may be one report or multiple reports showing login successes and login failures across various systems, access methods (local, remote) and users. Note, that to be valuable, this report requires that you track login successes and not just failures
- **Login attempts (successes, failures) to disabled/service/non-existing/default/suspended accounts**: this report group covers attempted access to accounts and services that should not be accessed, ever. Both failures and successes are of interest to security professionals.
- **All logins after office hours / "off" hours**: similar to the above report, such activity is commonly of interest especially if the access attempt is successful. However, such events have to be investigated especially in environments where system administrators work 24/7. Such events have to be investigated, particularly in environments where system administrators work 24/7. One reason this report is valuable is because it is derived from its contrast to baseline data. When we understand what normal looks like for the enterprise, anomalies stand out.
- **User authentication failures by count of unique attempted systems:** this aggregate report has to detect account scans where a single machine checks for the same account or different accounts across many systems. It is a little similar to an old school "host scan".
- **VPN authentication and other remote access logins (success, failure)**: while all login attempts

might be of interest under the right circumstances, remote login attempts such as via VPN or other remote connectivity methods are of escalated interest and should be tracked carefully. Including source IP addresses with this report makes it particularly useful.

- **Privileged account access (successes, failures)**: root logins, su use, Run As use as well as relevant equivalents for other platforms and systems have to be accounted for since a privileged user can typically do much more damage than a normal user.

- **Multiple login failures followed by success by same account:** while rule-based (SIEM-style) correlation is needed to produce this report, tracking for multiple account failures immediately followed by a successful connection is of obvious interest, since it almost always indicates successful attempts to guess login credentials.

Who Can Use These Reports

These reports have universal applicability, depending on the scope of systems covered. A chief security officer (CSO) may review authentication summaries across the entire organization, security analyst may use these reports during daily log review, incident responders may run them while investigating an incident and system administrators can run these reports on their own systems.

Example

An example report below shows login attempts to systems:

System	Account Name	Source IP	Status	Method	Count
Venus	administrator	10.1.1.2	Failure	Local	1
Jupiter	anton	10.11.12.13	Success	Local	1
Mercury	root	10.1.2.3	Failure	SSH	893765

Change Reports

These reports identify various system and critical security changes to various information system and networked assets – configuration files, accounts, regulated and sensitive data and other components of the system or applications.

Why They Are Important

Unauthorized changes to information systems can lead to costly crashes and the loss of data and may indicate security incidents. On top of this, attackers will often modify your systems in order to enable their access in the future. Being diligent with tracking changes will also improve your overall IT operation.

Specific Reports

Key reports in this category are:

- **Additions/changes/deletions to users, groups:** attackers will frequently add new accounts and then sometimes delete them after access. This type of privileged activity if authorized and based on legitimate use should be differentiable from suspicious account management activity.

- **Additions of accounts to administrator / privileged groups**: in particular, changes to the administrator accounts and other privileged users should be at the top of the list of tracked account changes.

- **Password changes and resets – by users and by admins to users**: password changes are often just as important as new account creations. These can be performed by users as well as by administrators, depending on the password change/reset policy in an organization. In addition, this report can be used to ensure that authorized password changes are performed according to policy schedule.

- **Additions/changes/deletions to network services**: new services that allow network connectivity may open your network to additional attacks; they also are frequently performed by attackers. The creation of new services in general is something that should be tracked whether they be network centric or not. Process Logging – on key systems, process auditing, which logs the creation and/or termination of

processes, should be considered. The process creation events contain the process identifier (PID), the parent process identifier (PPID), and the user responsible, invaluable information during an investigation.

- **Changes to system files – binaries, configurations**: changes to system files such as binaries and configuration files whether accidental, planned or malicious need to be carefully tracked.

- **Changes to other key files**: various systems might have broad lists of key files in addition to binary executables and configuration files; track access to these needs to be tracked as well.

- **Changes in file access permissions**: a sneakier variety of a risky change is a change in file permissions; if not accounted for, such changes can lead to sensitive data compromise.

- **Application installs and updates (success, failure) by system, application, user**: all application installs and updates need to be logged across all systems; at the very least, these logs will be incredibly useful during incident.

Who Can Use These Reports

These reports have universal applicability, depending on scope of systems covered. A chief security officer (CSO) may review change summaries across the entire organization, security analyst may use these reports during daily log review, incident responders may run them while investigating an incident and system administrators can run these reports on their own systems.

Example

An example report below shows all account and group additions on a Linux system:

Date	System	Account Name	Operation	Object	Status
1/10/11 11:11AM PST	Venus	root	Account Added	anton	Success
1/11/11 11:11AM PST	Jupiter	anton	Group Added	sudoers	Success
1/10/11 11:11AM PST	Venus	root	Account Added	root1	Failure

Network Activity Reports

These reports identify system suspicious events and potentially dangerous network activities as well as activities that need to be tracked for regulatory and/or PCI compliance.

Why They Are Important

The network is the main vector for threats to arrive at information assets. Obviously, the network is also the main way to steal information assets from today's organizations.

Specifics Reports

Key reports in this category are:

- **All outbound connections from internal and DMZ systems by system, connection count, user, bandwidth, count of unique destinations**: there are multiple ways to slice the information on outbound connections from your environment, but the principle remains the same: tracking who is connecting from your network outside is the way to detect intrusions and compromises and malicious software – as well as users abusing network access. Be prepared, that this can generate an extreme amount of log material and logs, especially for larger organizations.

- **All outbound connections from internal and DMZ systems during "off" hours:** using firewall and web proxy logs, one can use a more targeted version of the above report and only track outbound access doing

unusual hours, but also lessens the chances of finding a compromise, as many of these happen as a result of opening a document, etc. during normal business hours.

- **Top largest file transfers (inbound, outbound) OR Top largest sessions by bytes transferred**: either of the two reports allows organizations to track blatant data theft and bandwidth abuse.

- **Web file uploads to external sites:** based on proxy logs, one can track what files are being uploaded to external sites as well as being attached to web mail

- **All file downloads with by content type (exe, dll, scr, upx, etc) and protocol (HTTP, IM, e-mail, etc)**: tracking what files enter your environment from the web is also important and can be done by a tracking files across protocols and methods. Please note, executables are not the suspicious files. Exploits can be packaged into PDFs, Excel spreadsheets as well as other file types.

- **Internal systems using many different protocols/ports**: while there is no reliable way to always distinguish malware activity from legitimate, internal systems suddenly starting to “talk” over many new ports and protocols are a known tell-tale sign of malicious activity.

- **Top internal systems as sources of multiple types of NIDS, NIPS or WAF Alerts**: one of the most useful reports, tracking internal information assets that trigger many alerts from multiple sources.

- **VPN network activity by user name, total session bytes, count of sessions, usage of internal resources**: we highlighted the need to track VPN logins in the above section, but VPN usage should also be tracked in order to spot the VPN access and traffic anomalies. This report should include the source IP address.

- **P2P use by internal systems**: while user breaking the organization's Acceptable Use Policy (AUP) might be HR's focus for this activity; P2P software can also be a vector for accidental and malicious data theft and loss

- **Wireless network activity:** wireless network devices can record many different events but it is useful to treat them as VPNs and other remote access network mechanisms above and track access (with username or Windows name); another useful report on wireless data will include rogue AP presence detection and rogue AP association logs.

- **Log volume trend over days**: while not strictly an example of network activity report, reviewing of a raw log volume produced on your network is extremely useful as a big picture view across the entire pool of log data.

Who Can Use These Reports

These reports have universal applicability, depending on scope of systems covered. A chief security officer (CSO) may review network activity summaries across the entire organization, security analyst may use these reports during daily log review, incident responders may run them while investigating an incident. System administrators can use these reports in the management of their own systems.

Example

An example report below shows all account VPN access and activities across the organization network:

Date	VPN	User Name	System	Action	Status	Count
1/11/11	VPN1	anton	antonlaptop	Login	Success	2
1/12/11	VPN1	anton	antonlaptop	Login	Failure	1
1/13/11	VPN2	root	Lapt19847	Login	Failure	77

Resource Access Reports

These reports identify various system, application and database resource access patterns across the organization and can be used for both activity audit, trending and incident detection.

Why They Are Important

Tracking resource access can be used to reveal insider abuse and even fraud. They are valuable during

incident response for determining which resources the attacker has accessed and possibly corrupted or modified (see Change Reports above). In addition, resource access can be used for purposes outside of security, such as capacity planning and other purposes

Specific Reports

Key reports in this category are:

- **Access to resources on critical systems after office hours / "off" hours:** similar to the above "off" hours network access and logins, this report can be used to track access and activities on critical and regulated systems during unusual times.
- **Top internal users blocked by proxy from accessing prohibited sites, malware sources, etc**: this versatile web access report can be used for multiple purposes from tracking compromised systems to the data leakage tracking to improved productivity.
- **File, network share or resource access (success, failure)**: this report can be useful if run for specific audited resources; enabling logging of file access and system calls.
- **Top database users**: to be useful for security activity tracking it must exclude known application access to the database; ideally, a production database should have no direct access from users or developers.
- **Summary of query types**: excluding known application queries allow this report to serve as anomaly detection tool that can show anomalous data base access.
- **All privileged database user access:** as with servers and applications, all privileged user activities should be recorded and analyzed periodically.
- **All users executing INSERT, DELETE database commands**: in addition to tracking application and user access, it makes sense to separately track more damaging commands that can destroy data. Excluding known application queries is a useful practice here.
- **All users executing CREATE, GRANT, schema changes on a database**: in addition to tracking application and user access, it makes sense to separately track more damaging commands that can destroy data and change the database instance itself.
- **Summary of database backups**: backups present a clean way to extract massive quantities of data from a database and thus commit data theft; this report will allow you to review who performed database backups and catch those performed without authorization.
- **Top internal email addresses sending attachments to outside**: across many email access reports, this stands out in its usefulness for both detecting and investigating insider abuse and data theft.
- **All emailed attachment content types, sizes, names**: similar to the above report, this can be used to track information leakage as well as detect users emailing potentially sensitive information.
- **All internal systems sending mail excluding known mail servers**: a basic way to find systems infected with spam-sending bots across your environment.
- **Log access summary**: logging and then reviewing access to logs is good practice and is commonly required by regulatory guidance. This basic report may be designed to allow you to exclude your own viewing of log data.

Who Can Use These Reports

These reports have universal applicability, depending on scope of systems covered. A chief security officer (CSO) may review resource access summaries across the entire organization, a security analyst may use these reports during daily log review, and incident responders may need them while investigating an incident. Resource owners and resource managers can use these reports to plan capacity and make other business decisions.

Example

An example report below shows all file access across multiple servers:

Date	Server	User Name	File Name	Access Type	Status	Count
1/11/11	Win1	anton	Expenses.xlsx	Read	Success	1
1/12/11	Win2	anton	Roadmap.ppt	Read	Success	1
1/13/11	NFS	anton	Blank.docx	Write	Failure	37

Malware Activity Reports

These reports summarize various malicious software activities and events likely related to malicious software.

Why They Are Important

Malicious software in various forms remains one of the key threat vectors for today's organizations, large and small. Anti-virus tools have been losing efficiency for detecting and stopping malware over the last few years. Therefore other information sources such as logs must be used in the fight against malware.

Specific Reports

Key reports in this category are:

- **Malware detection trends with outcomes**: a basic report with a summary or a trend of malicious software detection, also showing the system and the outcome (cleaned or left alone) is a good starting point.
- **Detect-only events from anti-virus tools**: all anti-malware tools log the cases where malicious software was detected but not cleaned (for various reasons); these logged "leave-alones" have helped many organization avoid massive damage.
- **All anti-virus protection failures**: given that today's malicious software is well equipped for fighting anti virus tools, all crashes, protecting engine unloads, update failures, etc must be logged and reviewed.
- **Internal connections to known malware IP addresses**: this incredibly useful report uses logs (such firewall or other) and a public blacklist of IP address; this simple approach can stop the organization from losing valuable data to malware operators.
- **Least common malware types**: along with other "Bottom 10" (as opposed to "Top 10") reports, this presents a useful insight into unusual and thus possibly damaging malicious software in your organization.

Who Can Use These Reports

These reports are useful for all security professionals, from a junior administrator in charge of desktop antivirus to a CSO in charge all entire organization security. Such reports are also useful for incident response and malware infection investigations.

Example

An example report shows virus types detected by any means across the enterprise. In this case the span is a week of log data.

Malware type	Status	Infected System Count
VirusX	Detected	1
VirusY	Detected	1
Botz	Quarantined	2

Critical Errors and Failures Reports

These reports summarize various significant errors and failure indications, often with direct security significance.

Why They Are Important

Errors and failure log messages often present valuable early indication of security threats, including advanced threats not captured by security-specific devices, such as IDS and IPS systems. Paying diligent attention to unusual error messages often pays off when a possibly damaging new threat factor manifests on your network.

Specific Reports

Key reports in this category are:

- **Critical errors by system, application, business unit**: while on the surface not security significant, various error messages appearing in logs (especially for the first time) should be investigated as they often present a very early indication of malicious activities.

- **System and application crashes, shutdowns, restarts**: whenever applications crash – due to failed attacks or other reasons – business functioning is likely to be affected; these events should not only be taken as having impact on availability but investigated as possible early indirect indication of attacks.

- **Backup failures** are critical events affecting business continuity and possibly regulatory compliance, in addition, unauthorized backups, (failed, in this case), may be triggered by attacker's attempts to steal data.

- **Capacity / limit exhaustion events for memory, disk, CPU and other system resources** often stem from attacker's or other unauthorized use of business systems, high resource usage may also be caused by attack floods, denial of service or brute force attacks.

Who Can Use These Reports

These reports are useful for all security professionals, from a junior administrator in charge of desktop anti-virus to a CSO in charge all entire organization security. These reports are also useful for incident response and malware infection investigations. Other IT personnel can benefit from them as well.

Example

An example report shows disk full and high CPU usage messages across a pull of Unix/Linux servers

Server	Event Type	Date
Serv1	Disk Full	10/1/11
Sirius	Disk Full	1/1/11
VenusX	CPU Load 100%	1/2/11

Acknowledgements

V1 authors: Chris Brenton, Marcus Ranum, Tina Bird and others

V2 author Dr. Anton Chuvakin with valuable contributions from Marcus Ranum and many people from SANS community – sorry for not naming all of you here!

V3 author: Peter Czanik, BalaBit

V3.01 technical review: John Allison, Jake Evans, Barbara Filkens, Orhan Moye, Stephen Northcutt, Jeff Read, Alissa Torres, Mark Wityszyn

Featured Research

Security Development Lifecycle Awareness
By Russ McRee | Aug 2013 | 75 KB

Develop a Security Response Plan
By Russ McRee | Aug 2013 | 877 KB

Customized Security Awareness Program
By Mason Pokladnik | Aug 2013 | 57 KB

View More Student Presentations / Projects

Featured Student/Alumni

Russell Eubanks

Russell Eubanks leads the Security Architecture, Risk and Compliance teams at Cox Communications. He has developed information security programs from the ground up and actively seeks opportunities to measurably increase their overall security posture. Read More →

View our Site Directory

Cyber Security Degrees

Contact Us

Questions: info@sans.edu
Web: webmaster@sans.edu

"After starting the program, I was promoted to Information Security Officer. I believe my involvement in the program was a contributing factor in that happening. - John Brozycki, Alumni of SANS Technology Institute"

"The experiences gained in the SANS Technology Institute program have helped me advance in IBM, taking a more public facing role. - Jerome Radcliffe, SANS Technology Institute Student"