Everything You Always Wanted to Know About Log Management But Were Afraid to Ask

August 21, 2013
Logging and Log Management

About the Author

• **Christopher Phillips**
  – Manager and senior software developer at Dell SecureWorks.
  – Responsible for the design and development of the company’s Threat Intelligence service platform.
  – Previously was responsible for the Log Retention service line
  – Prior to Dell SecureWorks, Christopher worked for McKesson and Allscripts, helping clients with healthcare systems integration secure healthcare transactions and communication, and meet HIPAA compliance in their information systems environment.
  – More than 18 years of experience in software development and design
What are Logs?

- Logs provide evidence of actions taken by the system or individuals using the system.
- Logs have a defined meaning and categorization based on the system that generating the log
- Allows IT to trace what has occurred in the past
Where to Find Logs

- Servers
- Firewalls
- Databases
- Routers
- Point of Sale Devices
- USB Drives
- Kiosks
- Etc.
Types of Logs

- Audit Logs
- Transaction Logs
- Intrusion Logs
- Connection Logs
- System Performance
- Activity Logs
- Application specific logs
- OS Specific Logs
Why is log data important?

- System Monitoring
- Troubleshooting
- Forensics and Analysis
- Incident Response
- Measurement of System Utilization and Resource Planning
- Regulatory Compliance
- Public Disclosure Requirements
Key items in Logging

- Log Transport
- Log Syntax and Format
- Log Taxonomy and components
- Log Settings and Configuration
Well Known Log Formats

- W3C Extended Log File Format (ELF) - Improved format for Web server log files
- Apache Access Logs
- Cisco SDEE/CIDEE
- ArcSight common event format (CEF)
- Syslog
- Windows Event Logs

Syslog is closest thing to a standard in logging!!
Log Taxonomy and Components

Common Set of Log Fields

- Date/Time (hopefully including Timezone)
- Type of Log Entry (Debug, Info, Fatal, ... )
- System that produced the log
- Application or component that produced the log
- Severity, priority, or importance of the message
- User or username involve in the activity
- Description of the event that occurred
Log Transport

• Syslog UDP
• Syslog TCP
• Encrypted Syslog
• HTTP
• HTTPS
• SNMP
• File transfer protocols such as FTP or SCP
Log Settings and Configuration

Key items on configuration:
• System Specific
• Many systems require configuration
• Time and retention policy
• Transport options
• Compliance needs

Figure 1—Compliance Requirements Set the Stage for Log Management

- **PCI DSS**
  - Automation of audit trails
  - Unauthorized modification
  - Retention of log data
  - Loss of credit card privileges

- **HIPAA**
  - Regular audits
  - Retention of log data for up to seven years
  - Imprisonment to 10 years

- **SARNAES-OXLEY**
  - System and user activity monitoring
  - Identification and investigation of security breaches
  - Retention of log data for up to five years
  - Login and logoff monitoring

- **GLBA**
  - Activity monitoring and system condition monitoring
  - Incident activity and response reporting
Problems with Log Records

- Different Log Formats
  - Logs from similar systems like web servers are formatted differently and different levels of information
  - Syslog closest thing to a standard nowadays
- Log criticality and difference in meaning
  - Error, alert, and information events can be different across the enterprise
- Log transport and protocol differences
  - Flat files, TCP versus UDP, unencrypted and encrypted logs
- Log configuration settings
  - Most applications are configured for minimal log information by default and each application has its own configuration settings and methods
- No standard log API used by applications
  - Applications and in house developed solutions can use different logging APIs and log different types of information. No standard API for meeting HIPAA or other compliance framework requirements
What is Log Analysis?

• Log analysis is an art and science seeking to make sense out of computer-generated records (also called log or audit trail records).
  - Wikipedia

• Can Involve:
  – Knowing the “bad” things to look for
  – Data Correlation and Normalization to perform system wide analysis
  – Knowledge of specialized and system specific tools
  – Dealing with the challenges of “time”
Why Perform Log Analysis

• Compliance and regulations
  – HIPAA, HITECH, SOX, PCI-DSS, others

• Proactive alerting of potential issues
  – Correcting issues and stopping a breach in progress

• Early detection of security/privacy breaches
  – Limiting risk to the organization and data loss prevention

• Finding and eliminating internal and external threats

• Finding and eliminating sources of data loss
  – E-mailing business critical information, storage of patient data on personal devices, client lists and sales forecasts, etc.
Needle In a Haystack Problem

“With so many logs, how do I make sense of it all?”

Making Sense of it all:
• Filtering – Keeping or discarding data you care about
• Normalization – Break logs down to their key components, discovering how systems can be uniquely identified, and creating common comparisons between log messages
  – Vendor ID 6856 – Fatal Error
  – Other system - FATAL
• Correlation – finding connections in logs and events
• Alert – Using systems and tools to get notified on anomalies
Notables About Log Filtering

• Common Filtering Techniques
  – Show me the “bad stuff” – Positive Filtering
  – Show me the “good stuff” – Negative Filtering

• Pros:
  – Easy to interpret
  – Most tools allow for this type of filtering

• Cons:
  – May lose context of what occurred before and after an event
  – Assumes you know what bad is and that you can trace the “good” messages from other systems
Log Analysis Options

• Do It Yourself
• Buy a Tool
• Hire the Experts
Do it yourself - Manual Log Analysis

• Use tools like grep, awk, Microsoft Excel to find “interesting” data

• Pros
  – Can be cheap – uses tools and technologies in use or available today in an organization
  – Immediately available

• Cons
  – Time consuming – searching terabytes and petabytes of information can take a very long time
  – Assumes you know what you are looking for
  – Difficult to correlate logs across systems
Buy a tool – Specialized Log Analysis tools

• There are a number of special built systems from vendors like LogLogic and Splunk specially designed for log analysis

• Pros
  – Centralize log data
  – Many tools have options for real time alerting and log forensics designed and developed for working with large volumes of data
  – Reporting and auditing tools to meet compliance reporting needs
  – Support for many log formats and correlation of log data across the organization

• Cons
  – Requires specialized security knowledge and training
  – Training and system acquisition costs
  – Security team member hiring and staffing
Hire the experts – Security Outsourcing

• Allows organizations to rely on specialized providers to help perform the analysis, tuning, and alerting on the organization’s log data
• Managed Security Service Providers (MSSP) organizations like Dell Secureworks have years of security knowledge and experience working with and protecting organizations

• Pros
  – Can have lower cost of ownership with many MSSP organizations operating on a subscription based model
  – Lower security staffing and training costs
  – Reporting and auditing tools to meet compliance reporting needs
  – Support for many log formats and correlation of log data across the organization

• Cons
  – Loss of control and vendor dependence
  – Vendor financial stability and costs of changing vendors
Log Retention?

“How long do I need to keep logs around?”

- Organizations need to develop a log retention policy
- Key criteria in the policy are:
  - Assess applicable compliance requirements
  - Review the organization’s risk posture
  - Look at various log sources and the size of the logs generated
  - Review available storage options
Log Storage Technologies

Online
- Host System
- Central Repository
- Database
- Hadoop
- The Cloud

Near-Line or Offline
- Tape
- CD/DVD/Blu-ray
- Cloud Options like Amazon Glacier
Log Management Lifecycle

• Phases of Log Management
  – Collect – securely and encrypted
  – Alert – get notifications on key issues
  – Store – should be immutable
  – Search – tools and utilities to find key items in the logs
  – Analyze – make conclusions from logs across systems
  – Act – take actions to protect your network

Repeat! – Tune logging policies and needs and review regularly to make sure your strategy still meets your organizations needs!
Problems with Log Management

• Logging not turned on!
  – Many tools and applications need logging enabled and tuned to be useful to an organization

• Not enough data logged
  – Typical default settings are optimized to only log errors or warnings to optimize system performance or limit disk space requirements

• Log message diversity and diversity in meaning
  – Without specialized knowledge or understanding of systems, it can be difficult to find the “interesting” information in log files

• Inconsistent times or times out of sync
  – Correlating log events across systems can be difficult with multiple time zones and different system times

• Difficulty in retrieving logs from systems
  – Logs can be locked up in flat files and proprietary formats that require additional tools and software to retrieve and centralize
Common Issues or Mistakes

- Gaps in tools to address regulatory needs
- Not turning on or tuning logging on all systems in an organization
- Not looking at and analyzing logs until a breach, event, or the auditors inquire about them
- Storing logs for too short a period of time or having different retention times on different systems
- Only storing the "interesting" log information or limiting log information
- Ignoring logs from key systems in the organization
- Only looking at known bad messages and ignoring the rest
- No security controls or protections on log data
- Limited planning and analysis to address log growth and storage needs
- Lack of updates to log retention tools and strategy to meet new regulations – HIPAA passed in 1996 - HITECH passed in 2009
Tools to Help

• Basic Analysis Tools
  – Grep, Awk, Microsoft Excel, Open Source

• Log Centralization
  – Syslog, Rsyslog, Snare

• Advanced Analysis Tools
  – OSSEC, OSSIM, Others

• Commercial Tools
  – Splunk, NetIQ Sentinel, IBM q1Labs, Loggly

• Managed Security Service Provider
  – Dell Secureworks
Trends in Logging

• Cloud based systems need log analysis too
• Regulations becoming more prescriptive on log retention
• Regulatory and Legal changes specifying limits for public disclosure
Dell SecureWorks Security Services

Managed Security
- 24/7 security monitoring
- Security device mgmt.
  - IPS/IDS
  - Firewalls
  - Next Generation Firewalls
  - Web Application Firewalls
- Log Management
- SIM On-demand
- Vulnerability management
- Web application scanning
- Managed SIEM
- Managed Advanced Malware Protection

Security and Risk Consulting
- Testing & assessments
- Mobile & cloud security
- Compliance and certification
- Program development & governance
- Architecture design and implementation
- Expert residency
- Physical Security Assessments
- Wireless security testing
- Social engineering

Threat Intelligence
- Threat, vulnerability & advisory feeds
- Emerging threat bulletins
- Targeted Threat Intelligence
- Microsoft update analysis
- Weekly intelligence summary
- Cybersecurity news roundup
- Live intelligence briefings
- CTU support
- Attacker database feed

Incident Response
- CIRP development
- CIRP Gap Analysis
- CIRP training
- Tabletop exercises & "War Gaming"
- Incident handling
- Digital forensics investigation
- Incident management
- Malware analysis
- Eradication & recovery
- Postmortem analysis
- Documentation
Questions?

Chris Phillips
Contact: c_phillips@dell.com