Project Proposal: Compact Log Management and File Integrity Solution for Small Businesses

Brittany Wilbert
Sam Houston State University
10/22/2012

Background

- From 2005-2012 over 560,000,000 data breaches have occurred [1].
- As a result of compromises, many small businesses risk substantial losses and potential shut down if they do not follow laws and regulations which demand complete and accurate audit trails.
- According to research, small businesses are more likely to become victims of cyber attacks [2][3][4][5].
- Approximately 36% of cyber attacks were made against small businesses between Jan 2012 and June 2012 [6].
- However the cost to deploy and monitor an effective log management and file integrity monitoring solution frequent outweigh the requirements to deploy.

Problem Statement

- Small businesses frequently do not deploy log management solutions until their systems have been compromised [7].
- Log management solutions must be affordable, compact, and contain both access to file integrity monitoring and log management capabilities.
- How does a small business minimize the cost of log management and file integrity monitoring without significantly reducing the quality of their management solution?
- How can small businesses integrate their log management solution to a multiple operating system environment?
- What solutions will produce the most viable data retention and log management capability while minimizing the cost associated with deployment of the solution?
- How can analytics and metrics be used to allow a low number of security staff members to understand and interpret results regularly?

Project Plan

- To utilize freeware/shareware log management solutions to construct a File Integrity/Log Management Solution.
- To focus features specifically centered for small business environment while focuses on
- To deploy solution to a virtual machine cluster equivalent of a small business (10-20 virtual machines instances)
- Analyze results based on following criteria:
  - Performance capability: How much impact software has on system performance?
  - Software availability: How the deployment response to stress? Does it frequently crash?
  - Log message compression: How are log messages stored if not in use?
  - Log message integrity: How does deployment protect what it receives?
  - FIM integration: Does deployment optimally integrate FIM with log management service
  - Size of log solution: How large is the deployment? Does deployment use too many resources?

Hardware/Software Tools

Hardware

- Log Management Server:
  - Custom Built
  - AMD Phenom II X2 560 Processor 4.12 GHz
  - 4 GB Memory
  - 1 TB Hard Drive
- Desktop Workstation (Currently being obtained)
  - HP Pavillion or Dell Vostro Desktop Computer
  - 4 GB Memory
  - 500 GB Internal Hard Drive
  - Intel Core i3 (or equivalent minimum)
- Laptop Workstation
  - Dell Studio 1555
  - 4 GB memory
  - Intel Core 2 DUO CPU
  - 500 GB Hard drive

Software

- VMWare Workstation/Player
- Virtual Machine Images:
  - Windows Server 2008
  - Windows Server 2003
  - Windows XP
  - Windows 7
  - Linux distributions (Red Hat, Ubuntu, CentOS)
- OSSEC (file integrity monitoring/log management) - http://www.ossec.net/
- Lasso (remote Windows log collection) – http://sourceforge.net/projects/lassolog/
- Syslog-ng (Windows/Linux) - http://www.balabit.com/network-security/syslog-ng
- LogWatch (Analytics Engine) – Perl: http://sourceforge.net/projects/logwatch/

Project Timeline

Task	Start Date	Finish Date	Vital Deadlines
Research Compilation and Review	10/01/2012	10/15/2012	
Completion of Master's Project PowerPoint	10/16/2012	10/22/2012	
Master's Project Proposal (at Sam Houston State University)	10/22/2012	10/22/2012	
File Integrity Monitoring and Log Management Integration	11/01/2012	03/02/2013	
Master's Paper Outline and First Draft	12/01/2012	03/20/2013	Outline – 01/05/2012, 1st Draft - 03/20/2013
Master's Paper Revisions and Final Draft	03/20/2012	04/05/2013	1st Revision – 03/25/2013. 2nd Revision – 04/01/2013. Final Draft – 04/06/2013
Project Documentation And Paper Submission	03/15/2013	04/17/2013	Documents to Committee – 04/12/2013. Documents to Graduate Advisor 04/19/2013
Submit Paper to Conference	04/05/2013	04/19/2013	TBA. Deadline flexible depending on conference deadlines.
Project Presentation	04/19/2013	04/26/2013	Sign-up: 04/19/2013. Presentation: 04/26/2013 (Tentatively)

File Integrity Monitoring (FIM) and Log Management Solution Integration Timeline

Task	Purpose	Start Date	End Date
Initial Specifications Gathering.	Identify key metrics for operating systems and software limitations.	11/01/2012	11/30/2012
Analytics Software Updating and Modifying.	Modifying and updating analytics software for deployment.	11/01/2012	12/25/2012
Operating System Deployment and Configuration	Complete installation of operating systems and complete configuration	12/01/2012	12/25/2012
Initial Log Management/FIM Software and Analytics Deployment.	Complete initial deployment of software solutions for initial review	12/01/2012	01/04/2013
Initial Deployment Review	Complete review of deployment based defined criteria	01/04/2012	01/20/2013
Testing and Optimization Phase	Update software solutions based on initial deployment.	01/21/2013	02/01/2013
Final Deployment Update and Modifications	Update deployment and make final modifications before final analysis.	02/02/2013	02/10/2013
Final Analysis and Documentation Write-up	Obtain final metrics based on solution and complete documentation	02/10/2013	03/02/2013

Presentation References

1. Privacy Rights Clearinghouse, “Chronology of Data Breaches,” April 2011. Updated May 6th, 2011. Available: http://www. privacyrights.org/data-breach.
2. B. Krebs, "Uptick in Cyber Attacks on Small Businesses." August 2012. Available: http://krebsonsecurity.com/2012/08/uptick-in-cyber-attacks-on-small-businesses/.
3. J. Cloona, "Cyber Attacks Increasingly Target Small Businesses." Aug 2012. Available: http://www.infosecisland.com/blogview/22129-Cyber-Attacks-Increasingly-Target-Small-Companies.html.
4. J. Fontana, "On Cybersecurity, small businesses flirting with disaster, survey finds." October 2012. Available: http://www.zdnet.com/on-cybersecurity-small-businesses-flirting-with-disaster-survey-finds-7000005891/.
5. M. Rockwell, "FCC unveils new version of Cyber protection planner for small businesses." October 2012. Available: http://www.gsnmagazine.com/node/27633?c=cyber_security.
6. Symantec. "Symantec report finds that more than a third of global targeted attacks are aimed against small businesses." July 2012. Available: http://www.symantec.com/about/news/release/article.jsp?prid=20120710_01 .
7. R. Faustus, “Security Log Management for Small Businesses.” February 2011. Available: http://www.brighthub.com/computing/smb-security/articles/24328.aspx.

Prior Work

- J. Purcell, “Log Analyzer for Dummies,” December 2007. Available: http://www.sans.org/reading_room/whitepapers/logging/log-analyzer-dummies_2031.
- K. Nawyn, “A Security Analysis of System Event Logging with Syslog,” May 2003. Available: http://www.sans.org/reading_room/whitepapers/logging/security-analysis-system-event-logging-Syslog_1101.
- R. F. Smith, “Bridging the Gap Between Native Active Directory Auditing & Successful Compliance,” 2011. Available: http:// www.ultimatewindowssecurity.com/tools/ondemandlm/BridgingTheGap.pdf.
- I. Eaton, “The ins and outs of system logging using Syslog”, October 2003, Available: http://www.sans.org/reading_room/whitepapers/ logging/ins-outs-system-logging-syslog_1168.
- K. Kent and M. Souppaya, “Guide to computer security log management,” September 2006. Available: http://csrc.nist.gov/ publications/PubsSPs.html.
- Johnson, R., I. Pandis, R.Stoica, M. Athanassoulis, and A. Ailamaki. “Aether: a scalable approach to logging.” 2010. *Proc. VLDB Endow.* 3, 1-2 (September 2010), 681-692.
- Huemer, D., and A. M. Tjoa, “*A Stepwise Approach Towards an Interoperable and Flexible Logging Principle for Audit Trails*,” *3rd Int. Conf. on New Generations*, pp. 114-119, © Apr 2010 IEEE. doi: 10.1109/ITNG.2010.33.
- Vaughan, J. A., L. Jia, K. Mazurak, and S. Zdancewic, “*Evidence-based audit*,” *IEEE Computer Security Foundations Symposium*, pp. 177-191, © Jun 20088 IEEE. doi: 10.1109/CSF.2008.24.
- Fabbri, D., and K. LeFevre, “*Explanation-based auditing*,” *Proc. VLDB Endow,* Vol 5, Issue 1, pp. 1-12, Sept 2011.
- Fu, Q. J. Lou, Y. Wang, and J. Li, “*Execution Anomaly Detection in Distributed Systems through Unstructured Log Analysis*,” *Int. Conf. on Data Mining*, pp. 149-158, © Dec 2009 IEEE. doi: 10.1109/ICDM.2009.60.
- Zhou, W., F. Qiong, A. Narayan, A. Haeberlen, B. T. Loo, and M. Sherr, “*Secure network provenance*,” *Proceedings of the 23rd ACM Symp. on Operating Systems Principles,* pp. 295-310, © 2011 ACM. doi: 10.1145/2043556.2043584.
- Chen, Y. and B. Malin, “*Detection of anomalous insiders in collaborative environments via relational analysis of access logs*,” *Proceedings of 1st ACM conference on Data and application security and privacy,* pp. 63-74, © 2011 ACM. doi: .1145/1943513.1943524.