Building a Logging Infrastructure

Abe Singer and Tina Bird
© Copyright 2004 by the USENIX Association. All rights reserved.
ISBN 1-931971-25-0

To purchase additional copies and for membership information, contact:

The USENIX Association
2560 Ninth Street, Suite 215
Berkeley, CA USA 94710
orders@sage.org
http://www.sage.org/

First Printing 2004

USENIX and SAGE are registered trademarks of the USENIX Association.
USENIX acknowledges all trademarks herein.
Contents

Foreword by Rik Farrow v

Introduction 1

1. Why Logs Are Important 3
   The Log Problem 4
   Second-level head

2. Getting Started 7
   What Does It Take? 7
   Basic Logging 7
   Spelling “login” in Many Languages 10

3. Sources of Log Information 16
   TCP Wrappers 18
   Iptables 18
   Other Open Source Security Alarms 19
   Generating Your Own Messages 20
   Identifying Devices and Services on Your Network 20
   Recording Facility and Level 23

4. Centralized Logging 25
   Architectures 25
   Building a Loghost 25
   Central Loghost 26
   Relay Architecture 27
   Stealth Loghost 29
   Non-UNIX syslog Servers 30
   Protecting the loghost . . . 31
   Have a Good Time 32
   Log Data Management 32
   UNIX Log Rotation 33
   Archiving 33
   Getting Data to the Loghost 34

5. The Gory Details 37
   syslog and Its Relatives 37
   syslog: The Protocol 40
   Real-World Secure Transmission 41
   syslog Output 42

6. Log Reduction, Parsing, and Analysis 43
   Data Reduction 43
7. **Windows Logging** 62
   - The Windows Event Log 62
   - Configuring Windows Audit Policy 64
   - Logger Equivalents for the Windows Event Log 67
   - Managing the Windows Event Log 68
   - Windows to Loghost 68

8. **Conclusion** 70

Appendix 1: Events to Record 72
Appendix 2: Sources of Log Information 74
Appendix 3: A Perl Script to Test Regular Expressions 76
Managing logging has often been an ignored task. Operating system vendors have learned to include provisions for rotating or even overwriting logs so that the logfiles do not grow to fill up entire disks. Sometimes, logging is just left disabled for most events.

Yet logging is an important part of proactive system administration. While waiting for phone calls from frantic (and annoyed) clients will eventually produce similar information, even if it is stunningly lacking in accurate detail, effective use of logging allows a system administrator to appear omniscient. At the very least, the sysadmin can be ahead of the game by collecting nuggets of data about interesting events.

This booklet provides the information needed to begin collecting and analyzing logging messages. Tina Bird began this project as an outgrowth of her work with a company that focused on the collection and analysis of logging and IDS information. She later took that information and turned it into a tutorial that formed the initial basis for this booklet. Abe Singer, a security analyst for San Diego Supercomputer Center, has shared his own experience in working with both security and logs. Together, the authors provide many years of experience, much of it focused specifically on the problems of logging, with an emphasis on security.

Even if your primary interest in logging is not security, the advice and information in this booklet will guide you in setting up and maintaining an effective logging infrastructure. The fruits of logging include the ability to detect problems before they get out of hand, to understand how the systems under your control normally work, and to recognize when things go wrong—before the phone starts ringing.

Logging is not a task that you can safely ignore.

Rik Farrow
Series Editor