Hardening Windows

JONATHAN HASSELL

Apress™

ISBN (pbk): 1-59059-266-2

Printed and bound in the United States of America 10987654321

Lead Editor: Jim Sumser

Technical Reviewer: Oris Orlando

Editorial Board: Steve Anglin, Dan Appleman, Gary Cornell, James Cox, Tony Davis, John Franklin, Chris Mills, Steve Rycroft, Dominic Shakeshaft, Julian Skinner, Jim Sumser, Karen Watterson, Gavin Wray, John Zukowski

Project Manager: Tracy Brown Collins

Copy Manager: Nicole LeClerc

Copy Editor: Mark Nigara

Production Manager: Kari Brooks

Production Editor: Janet Vail

Compositor: Dina Quan

Proofreader: Liz Welch

Indexer: Carol Burbo

Artist: April Milne

Cover Designer: Kurt Krames

Manufacturing Manager: Tom Debolski

Distributed to the book trade in the United States by Springer-Verlag New York, Inc., 175 Fifth Avenue, New York, NY 10010 and outside the United States by Springer-Verlag GmbH & Co. KG, Tiergartenstr. 17, 69112 Heidelberg, Germany.

In the United States: phone 1-800-SPRINGER, e-mail orders@springer-ny.com, or visit http://www.springer-ny.com. Outside the United States: fax +49 6221 345229, e-mail orders@springer.de, or visit http://www.springer.de.

For information on translations, please contact Apress directly at 2560 Ninth Street, Suite 219, Berkeley, CA 94710. Phone 510-549-5930, fax 510-549-5939, e-mail info@apress.com, or visit http://www.apress.com.

The source code for this book is available to readers at http://www.apress.com in the Downloads section.

CHAPTER 10

Security Auditing and Event Logs

You've come to the final chapter in this book, which is no small feat—congratulations! This part of the book focuses mainly on how you can discern if your hardening efforts, fine-tuned with what you've learned in the first nine chapters, were successful at thwarting attacks. Event logs and security auditing policies are an astute administrator's best friend, but most IT personnel overlook logs, as if logs were there for no other purpose than to simply take up valuable hard disk space.

Auditing and event-viewing procedures are different on Windows NT, 2000, XP, and Server 2003, so I'll group each platform and tackle different approaches independently. At the close of the chapter, I'll look at ways to decipher events and make log searching and checking easier.

For Windows 2000, XP, and Server 2003

Auditing controls and properties for versions of Windows later than NT are modified through Group Policy objects (GPOs) in Windows 2000, XP, and Server 2003. Assuming your computer is participating in an Active Directory domain, you can find the domain auditing policy inside the Default Domain Policy, by selecting Computer Configuration ➢ Windows Settings ➢ Security Settings ➢ Local Policies ➢ Audit Policies. Otherwise, you can view the Local Security Policy through the Administrative Tools applet in Control Panel.

The settings for each Group Policy object indicate on what type of events and on what type of result a log entry will be written. The options for auditing policies are outlined here:

- Audit account logon events
- Audit account management
- Audit directory service access
- Audit logon events

- Audit object access
- Audit policy change
- Audit privilege use
- Audit process tracking
- Audit system events

You can configure individual objects to be audited by editing the System Access Control List (SACL) for any given object, which is much like assigning permissions, except that it's indicating to Windows on what type of access an event log entry should be writing. You can access the SACL for an object by clicking the Advanced button on the Security tab of its properties sheet. On the Auditing tab, you can click Add to include new auditing events for an object, or click View ➢ Edit to modify an existing auditing event. Figure 10-1 shows the SACL for an object.

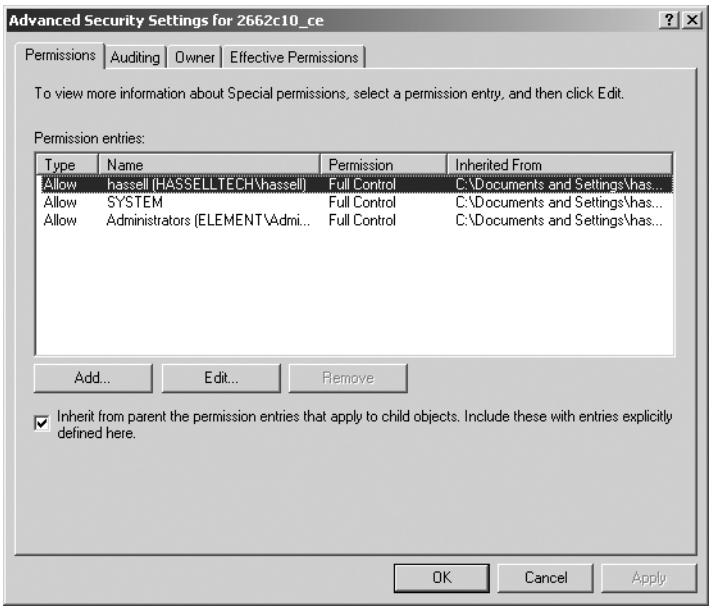

Figure 10-1. The SACL for an object

NOTE *Only NTFS files and folders can be audited. FAT partitions don't support auditing events because they don't contain the necessary permission information.*

Recommended Items to Audit

You'll want to take particular note of the following items from your event logs:

- Logon and logoff events, which can indicate repeated logon failures and point to a particular user account that's being used for an attack
- Account management, which indicates users who have tried to use or have used their granted user- and computer-administration power
- Startup and shutdown, which shows both the user who has tried to shut down a system and what services may not have started up properly upon the reboot
- Policy changes, which can indicate the users who are tampering with security settings
- Privilege use, which can show any attempts to change permissions to certain objects

Event Logs

Similarly to auditing policies, the policies for configuring the event logs are found inside the Default Domain Policy, by selecting Computer Configuration ➢ Windows Settings ➢ Security Settings ➢ Local Policies ➢ Event Log.

The settings for each of these GPOs indicate the amount of disk space dedicated to storing log events as well as the permissions granted to view the event logs, how long their contents are retained before rolling over to new logs, and how those event logs are supposed to be retained during that time. The options for event-log policies are described here:

- Maximum application log size
- Maximum security log size
- Maximum system log size
- Restrict guest access to application log
- Restrict guest access to security log
- Restrict guest access to system log

- Retain application log
- Retain security log
- Retain system log
- Retention method for application log
- Retention method for security log
- Retention method for system log
- Shut down the computer when the security audit log is full

The Event Viewer

The Event Viewer allows you to look at events in three event logs. Figure 10-2 shows a typical Event Viewer console.

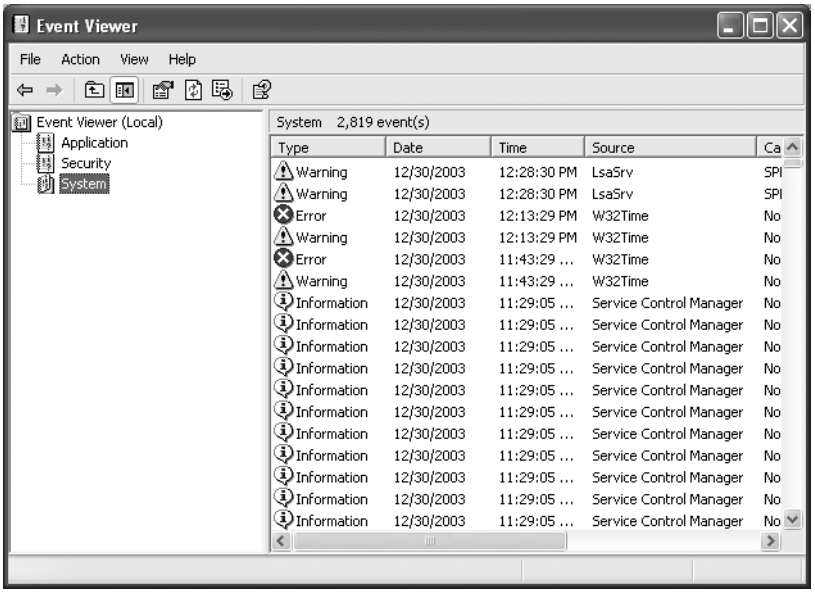

Figure 10-2. An Event Viewer console

First, the security log displays successes and failures with regard to privilege use, and classifies them into categories such as object access, account logon, policy change, privilege use, directory service access, and account management. The remaining event logs have three different classes of entries: errors, informational events, and warnings. The application log consists of information reported from programs running on the system. The system log consists of events and exceptions thrown by Windows itself. All users can see the system and application logs, but only members of the administrators group can see the security log.

To clear all events from your Event Viewer console, choose Clear All Events from the Action menu.

For Windows NT 4.0

Auditing is a necessary part of Windows NT's C2 security certification, but it's not enabled by default. You'll need to enable it on each NT machine by opening the User Manager and selecting Audit from the Policies menu. You'll be presented with an Audit Policy dialog box, as shown in Figure 10-3.

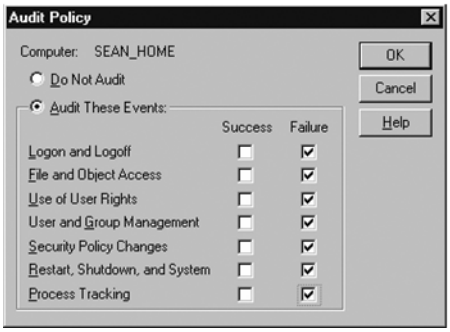

Figure 10-3. The NT Audit Policy dialog box

How you configure the auditing policy depends on how detailed you want to get in your log reviews. If you're simply interested in looking out for suspicious and possibly nefarious activity, then you should restrict your auditing events to a few serious classes of events and of those, only failure events. If, however, forensic analysis is your hobby, you may want to log everything possible, so you can extract as complete a picture as possible of a sequence of events that may require later investigation.

To turn on auditing of specific objects, you can click the Auditing button on the Security tab of their properties sheet, as depicted in Figure 10-4.

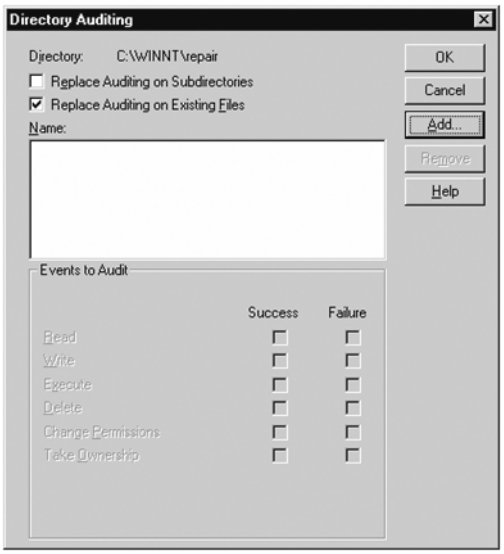

Figure 10-4. Enabling auditing for a specific object

Recommended Items to Audit

You'll want to take particular note of the following items from your event logs:

- Audit failures for logon and logoff events
- Audit all file and object-access events for files and directories of special interest or particular concern
- Audit failures of user rights
- Audit both successes and failures of user- and group-management privileges
- Audit both successes and failures of security policy changes—especially successes, because they would occur rarely in legitimate practice
- Audit failures in restart, shutdown, and system events
- Audit failures of process-tracking events

The Event Log

You can specify the retention policy, maximum log size, and rollover functions for each log from the Event Viewer application by selecting Start ➢ Programs and navigating to the Administrative Tools folder. From the Log menu, choose Log Settings. Select the log to configure in the Change settings for drop-down list, and then specify a maximum size for that particular log in kilobytes. You can also choose to overwrite older events when the maximum size is reached, overwrite events at Windows' discretion, or not to overwrite at all, which requires manual administrator intervention.

You can clear all events in a particular log by choosing Clear All Events from the Log menu of Event Viewer.

Filtering Events

In all versions of Windows, it's quite easy to limit the display of event items within Event Viewer to only those that match certain criteria. In Windows NT, select Filter Events from the View menu. In all other version of Windows, select Filter from the View menu. You'll see a dialog box much like Figure 10-5.

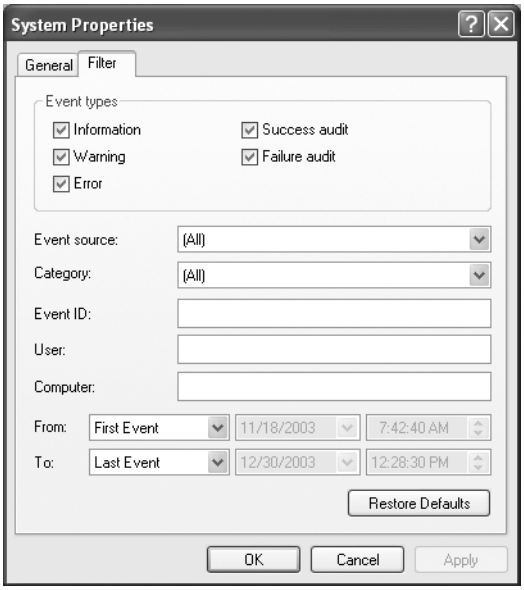

Figure 10-5. Filtering in the Event Viewer application

From this dialog box, you can indicate the events that interest you in a variety of ways, including by date (the From and To fields), success or failure (the checkboxes in the Event Types area), the class of the event (the Category drop-down list), the affected user, the system where the event originates, and the event type.

TIP *You can obtain a translation of a specific event ID number at* `http://www.eventid.net`. *You can enter the ID number and obtain a helpful explanation of the event, what it might mean, and the operating systems that it affects.*

What Might Be Missing

If you're reconstructing an occurrence through event logs, you might scratch your head at the absence of some events from any of your logs. This section offers a bit of explanation as to why that might be.

First, no audit events will be generated for unsuccessful attempts to access and modify a file or directory of interest if you haven't enabled security auditing for that item. To record such events, you have to enable auditing for the item. Also, I'll note once more that you can only audit items on NTFS file systems.

Second, failed login events in which the user has entered an invalid password aren't recorded in the audit logs for domain controllers in Active Directory or the primary domain controller in an NT 4 domain. Instead, those failed attempts are logged in the security log for the computer at which the failure occurred. Additionally, you must enable auditing on that system for the recording to occur.

TIP *There are some third-party software products that can help you manage auditing and event logs, including AuditPro from Network Intelligence India, at* `http://www.nii.co.in/software/apwin.html`, *and Informant from RippleTech, at* `http://www.rippletech.com/products/Informant/Prod_INF_Overview.htm`.

Checkpoints

In this final chapter you've learned how to use security auditing and event logs for various versions of Windows; these will support your hardening efforts. The

key auditing strategies for this chapter for Windows 2000, XP, and Server 2003 users are as follows:

- Logon and logoff events, which can indicate repeated logon failures and point to a particular user account that's being used for an attack.
- Account management, which indicates users who have tried to use or used their granted-user and computer-administration power.
- Startup and shutdown, which displays both the user who has tried to shut down a system and what services may not have started up properly upon the reboot.
- Policy changes, which can indicate users tampering with security settings.
- Privilege use, which can show attempts to change permissions to certain objects.

For Windows NT users, the chief auditing points include the following:

- Audit failures for logon and logoff events.
- Audit all file and object access events for files and directories of special interest or particular concern.
- Audit failures of user rights.
- Audit both successes and failures of user- and group-management privileges.
- Audit both successes and failures of security policy changes—especially successes, because they would occur rarely in legitimate practice.
- Audit failures in restart, shutdown, and system events.
- Audit failures of process-tracking events.

For all versions of Windows, the following items apply:

- Make searching easier by filtering events inside Event Viewer.
- Search on events that interest you at `http://www.eventid.net` to learn more about them.
- Understand why some events might not be recorded in certain error logs.