Security Log Secrets

Security Log Secrets illuminates the cryptic Windows security log and gives you the knowledge to effectively monitor, report, and investigate activity throughout your Windows and Active Directory environment. Security log expert Randy Franklin Smith, uses the most innovative methodologies to teach you monitoring, reporting and analyzing the Window security logs in your network.

Randall Franklin Smith
CISA, SSCP, Security MVP

You'll master how to leverage the security log to aid Sarbanes-Oxley compliance. You'll learn how to monitor end-users as well as administrators and how to detect intrusions and system changes.

Seminar Outline

- Audit Policies and Event Viewer
- Understanding Authentication and Logon
- Account Logon Events
- Logon/Logoff Events
- Detailed Tracking Events
- Object Access Events
- Account Management Events
- Directory Service Access Events
- Privilege Use Events
- Policy Change Events
- System Events
- Getting the Most from the Windows Security Log

What You Will Learn

- Audit changes in access control to privileged financial, cutomer and patient data
- Detect and report changes in administrator authority
- Find out how to centally monitor logons
- Track changes in system policy including group policy objects and organizational units
- Audit file system activity such as changes to critical files
- Learn which events are worth monitoring and what is just "noise"
- Understand the security log, its arcane codes, and event ID's

Benefits

- Finally get real ROI from your security log management solution
- Comply with SOX, HIPPA, GLBA (et al.) monitoring and reporting requirements
- Establish audit trails for change control
- Detect suspicious behavior and intrusion attempts
- Enforce accountability over administrators
- Conduct better investigations and forensic analysis
- Save time by knowing which events are safe to ignore

Security Log Resource Kits

Unlock the cryptic and arcane Windows Security log with Randy's Security Log Revealed books; master the Security log event-by-event with Randy's Security Log Encyclopedia; focus in on the key areas of the Security log with Randy's Mini-Seminar Series on DVD – all are available for Windows Server 2003 and Windows Server 2008, or get both in Randy's Security Log Resource Kit Combo Edition. For more details visit our Security Log page at:

www.UltimateWindowsSecurity.com/securitylog/resourcekits

Rosetta Audit Logging Kit

- Best practice guidance on which events to alert and report on
- Report designs you can implement in your existing log management solution
- Alert specifications that include event criteria, alert text and suggested recipients
- Deep mappings to specific compliance requirements
- Recommended courses of action to each alert and report
- Filter specifications so you can get rid of the noise
- Help from the authority in Windows security logging

www.UltimateWindowsSecurity.com/securitylog/rosetta

Ultimate Windows Security is a division of Monterey Technology Group, Inc.
www.UltimateWindowsSecurity.com

Randy Franklin Smith's ULTIMATE WINDOWS SECURITY .COM™

Security Log Quick Reference

Important Windows Security Events (Domain Controllers)

Event ID	Category	Explanation
675 or 4771	Audit account logon events	Event 657/4771 on a domain controller indicates a failed initial attempt to login via Kerberos at a workstation with a domain account usually due to a bad password but the failure code indicates exactly why authentication failed. See Kerberos failure codes below.
676, or Failed 672 or 4768	Audit account logon events	Event 676/4768 gets logged for other types of failed authentication. See Kerberos failure codes below. NOTE: Windows 2003 Server logs a failure event 672 instead of 676.
681 or Failed 680 or 4776	Audit account logon events	Event 675/4776 on a domain controller indicates a failed logon via NTLM with a domain account. Error code indicates exactly why authentication failed. See NTLM error codes below. NOTE: Windows 2003 Server logs a failed event 680 instead of 681.
642 or 4738	Audit account management	Event 642/4738 indicates a change to the specified user account such as a reset password or a disabled account being re-enabled. The event's description specifies the type of change.
632 or 4728 636 or 4732 660 or 4756	Audit account management	All 3 events indicate the specified user was added to the specified group. Group scopes Global, Local and Universal correspond to the 3 event IDs.
624 or 4720	Audit account management	New user account was created.
644 or 4740	Audit account management	Specified user account was locked out after repeated logon failures.
517 or 1102	Audit system events	The specified user cleared the security log.

Logon/Logoff

Event ID	Title
528 or 4624	Successful Logon
529 or 4625	Logon Failure - Unknown user name or bad password
530 or 4625	Logon Failure - Account logon time restriction violation
531 or 4625	Logon Failure - Account currently disabled
532 or 4625	Logon Failure - The specified user account has expired
533 or 4625	Logon Failure - User not allowed to logon at this computer
534 or 4625 or 5461	Logon Failure - The user has not been granted the requested logon type at this machine
535 or 4625	Logon Failure - The specified account's password has expired
539 or 4625	Logon Failure - Account locked out
540 or 4624	Successful Network Logon (Windows 2000, XP, 2003 Only)

Kerberos Failure Codes

Error Code	Cause
6	The username doesn't exist.
12	Workstation restriction; logon time restriction.
18	Account disabled, expired, or locked out.
23	The user's password has expired.
24	Pre-authentication failed; usually means bad password
32	Ticket expired. This is a normal event that get frequently logged by computer accounts.
37	The workstation's clock is too far out of synchronization with the DC's clock.
For other Kerberos Codes see http://www.ietf.org/rfc/rfc1510.txt	

NTLM Error Codes

Error Code (Decimal)	Error Code (Hex)	Explanation
3221225572	C0000064	user name does not exist
3221225578	C000006A	user name is correct but the password is wrong
3221226036	C0000234	user is currently locked out
3221225586	C0000072	account is currently disabled
3221225583	C000006F	user tried to logon outside his day of week or time of day restrictions
3221225584	C0000070	workstation restriction
3221225875	C0000193	account expiration
3221225585	C0000071	expired password
3221226020	C0000224	user is required to change password at next logon

Logon Types

Logon Type	Description
2	Interactive (logon at keyboard and screen of system)
3	Network (i.e. connection to shared folder on this computer from elsewhere on network or IIS logon - Never logged by 528 on W2k and forward. See event 540)
4	Batch (i.e. scheduled task)
5	Service (Service startup)
7	Unlock (i.e. unnattended workstation with password protected screen saver)
8	NetworkCleartext (Logon with credentials sent in the clear text. Most often indicates a logon to IIS with "basic authenti - cation") See this article for more information.
9	NewCredentials
10	RemoteInteractive (Terminal Services, Remote Desktop or Remote Assistance)
11	CachedInteractive (logon with cached domain credentials such as when logging on to a laptop when away from the network)