



Andrei Miroshnikov

Windows[®] Security Monitoring

| Scenarios and Patterns

WILEY

Windows® Security Monitoring



Windows® Security Monitoring

Scenarios and Patterns

Andrei Miroshnikov

WILEY

Windows® Security Monitoring: Scenarios and Patterns

Published by
John Wiley & Sons, Inc.
10475 Crosspoint Boulevard
Indianapolis, IN 46256
www.wiley.com

Copyright © 2018 by John Wiley & Sons, Inc., Indianapolis, Indiana
Published simultaneously in Canada

ISBN: 978-1-119-39064-0
ISBN: 978-1-119-39089-3 (ebk)
ISBN: 978-1-119-39087-9 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 646-8600. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at <http://www.wiley.com/go/permissions>.

Limit of Liability/Disclaimer of Warranty: The publisher and the author make no representations or warranties with respect to the accuracy or completeness of the contents of this work and specifically disclaim all warranties, including without limitation warranties of fitness for a particular purpose. No warranty may be created or extended by sales or promotional materials. The advice and strategies contained herein may not be suitable for every situation. This work is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If professional assistance is required, the services of a competent professional person should be sought. Neither the publisher nor the author shall be liable for damages arising herefrom. The fact that an organization or Web site is referred to in this work as a citation and/or a potential source of further information does not mean that the author or the publisher endorses the information the organization or website may provide or recommendations it may make. Further, readers should be aware that Internet websites listed in this work may have changed or disappeared between when this work was written and when it is read.

For general information on our other products and services please contact our Customer Care Department within the United States at (877) 762-2974, outside the United States at (317) 572-3993 or fax (317) 572-4002.

Wiley publishes in a variety of print and electronic formats and by print-on-demand. Some material included with standard print versions of this book may not be included in e-books or in print-on-demand. If this book refers to media such as a CD or DVD that is not included in the version you purchased, you may download this material at <http://booksupport.wiley.com>. For more information about Wiley products, visit www.wiley.com.

Library of Congress Control Number: 2017962214

Trademarks: Wiley and the Wiley logo are trademarks or registered trademarks of John Wiley & Sons, Inc. and/or its affiliates, in the United States and other countries, and may not be used without written permission. Windows is a registered trademark of Microsoft Corporation. All other trademarks are the property of their respective owners. John Wiley & Sons, Inc. is not associated with any product or vendor mentioned in this book.

I dedicate this book to those who always wants to know more and seek new information and experience every day.

—Andrei



About the Author

Andrei Miroshnikov graduated at Irkutsk State University (Russia) with a Master Degree in Computer Science. With more than 9 years of experience in the Information Security field, he is an author and organizer for Forensics CTF for the DEFCON 24 conference. He authored “Windows 10 and Windows Server 2016 security auditing and monitoring reference,” which is a part of Microsoft TechNet. Andrei is a speaker for Microsoft BlueHat and Positive Hack Days conferences.

About the Technical Editor

Roger A. Grimes, Microsoft, Principal Security Architect, is a 30-year computer security consultant specializing in host security, advanced persistent threat, IdM, and other defenses. Roger has written 9 books and over 1,000 magazine articles on computer security. He is a frequent guest speaker at national security conferences.



Project Editor

Tom Dinse

Technical Editor

Roger A. Grimes

Production Editor

Barath Kumar Rajasekaran

Copy Editor

Kimberly A. Cofer

Production Manager

Katie Wisor

**Manager of Content Development
and Assembly**

Pete Gaughan

Marketing Manager

Christie Hilbrich

Business Manager

Amy Knies

Executive Editor

Jim Minatel

Project Coordinator, Cover

Brent Savage

Proofreader

Nancy Bell

Indexer

Johnna VanHoose Dinse

Cover Designer

Wiley

Cover Image

©traffic_analyzer/Getty Images



Acknowledgments

I would like to say thank you to my wife, Anna, for supporting me during the year I spent working on this book. She was taking care of our home and kids to give me more time to spend on the book.

Thank you to my mother, Natalia Miroshnikova, and father, Sergey Miroshnikov, who invested their time in me from the moment I was born. I owe them a lot.

Thank you to my technical editor, Roger A. Grimes, who supported me from the beginning of this process till the end.

Thank you to my friends Lucine Wang and Jon DeHart for a good time we spent together; this helped me to get some small breaks during my tight schedule.

Thank you to John Wiley & Sons for giving me the opportunity to write my own book. It is a great company to work with. I would like to also say a personal thank you to Tom Dinse, Jim Minatel, and Kim Cofer for their help editing the book and coordinating all work related to its creation.



Contents at a glance

Introduction		xxix
Part I	Introduction to Windows Security Monitoring	1
Chapter 1	Windows Security Logging and Monitoring Policy	3
Part II	Windows Auditing Subsystem	11
Chapter 2	Auditing Subsystem Architecture	13
Chapter 3	Auditing Subcategories and Recommendations	47
Part III	Security Monitoring Scenarios	81
Chapter 4	Account Logon	83
Chapter 5	Local User Accounts	141
Chapter 6	Local Security Groups	201
Chapter 7	Microsoft Active Directory	237
Chapter 8	Active Directory Objects	285
Chapter 9	Authentication Protocols	323
Chapter 10	Operating System Events	367
Chapter 11	Logon Rights and User Privileges	419
Chapter 12	Windows Applications	437
Chapter 13	Filesystem and Removable Storage	485
Chapter 14	Windows Registry	523
Chapter 15	Network File Shares and Named Pipes	559

Appendix A	Kerberos AS_REQ, TGS_REQ, and AP_REQ Messages Ticket Options	585
Appendix B	Kerberos AS_REQ, TGS_REQ, and AP_REQ Messages Result Codes	589
Appendix C	SDDL Access Rights	597
Index		603



Contents

Introduction	xxix
Part I Introduction to Windows Security Monitoring	1
Chapter 1 Windows Security Logging and Monitoring Policy	3
Security Logging	3
Security Logs	4
System Requirements	5
PII and PHI	5
Availability and Protection	5
Configuration Changes	6
Secure Storage	6
Centralized Collection	6
Backup and Retention	7
Periodic Review	7
Security Monitoring	7
Communications	8
Audit Tool and Technologies	8
Network Intrusion Detection Systems	8
Host-based Intrusion Detection Systems	8
System Reviews	9
Reporting	9
Part II Windows Auditing Subsystem	11
Chapter 2 Auditing Subsystem Architecture	13
Legacy Auditing Settings	13
Advanced Auditing Settings	16

Set Advanced Audit Settings via Local Group Policy	18
Set Advanced Audit Settings via Domain Group Policy	19
Set Advanced Audit Settings in the Local Security Authority (LSA) Policy Database	19
Read Current LSA Policy Database Advanced Audit Policy Settings	20
Advanced Audit Policies Enforcement and Legacy Policies Rollback	20
Switch from Advanced Audit Settings to Legacy Settings	21
Switch from Legacy Audit Settings to Advanced Settings	22
Windows Auditing Group Policy Settings	22
Manage Auditing and Security Log	22
Generate Security Audits	23
Security Auditing Policy Security Descriptor	23
Group Policy: "Audit: Shut Down System Immediately If Unable to Log Security Audits"	24
Group Policy: Protected Event Logging	25
Group Policy: "Audit: Audit the Use of Backup and Restore Privilege"	25
Group Policy: "Audit: Audit the Access of Global System Objects"	26
Audit the Access of Global System Container Objects	26
Windows Event Log Service: Security Event Log Settings	27
Changing the Maximum Security Event Log File Size	28
Group Policy: Control Event Log Behavior When the Log File Reaches Its Maximum Size	29
Group Policy: Back Up Log Automatically When Full	29
Group Policy: Control the Location of the Log File	30
Security Event Log Security Descriptor	31
Guest and Anonymous Access to the Security Event Log	33
Windows Auditing Architecture	33
Windows Auditing Policy Flow	34
LsaSetInformationPolicy and LsaQueryInformationPolicy Functions Route	35
Windows Auditing Event Flow	36
LSASS.EXE Security Event Flow	37
NTOSKRNL.EXE Security Event Flow	37
Security Event Structure	38
Chapter 3 Auditing Subcategories and Recommendations	47
Account Logon	47
Audit Credential Validation	47
Audit Kerberos Authentication Service	50
Audit Kerberos Service Ticket Operations	53
Audit Other Account Logon Events	54
Account Management	54
Audit Application Group Management	54
Audit Computer Account Management	54

Audit Distribution Group Management	55
Audit Other Account Management Events	56
Audit Security Group Management	57
Audit User Account Management	57
Detailed Tracking	58
Audit DPAPI Activity	58
Audit PNP Activity	58
Audit Process Creation	58
Audit Process Termination	59
Audit RPC Events	59
DS Access	60
Audit Detailed Directory Service Replication	60
Audit Directory Service Access	60
Audit Directory Service Changes	61
Audit Directory Service Replication	61
Logon and Logoff	61
Audit Account Lockout	61
Audit User/Device Claims	62
Audit Group Membership	62
Audit IPsec Extended Mode/Audit IPsec Main Mode/ Audit IPsec Quick Mode	63
Audit Logoff	63
Audit Logon	64
Audit Network Policy Server	65
Audit Other Logon/Logoff Events	65
Audit Special Logon	66
Object Access	66
Audit Application Generated	67
Audit Certification Services	67
Audit Detailed File Share	67
Audit File Share	67
Audit File System	68
Audit Filtering Platform Connection	68
Audit Filtering Platform Packet Drop	69
Audit Handle Manipulation	69
Audit Kernel Object	70
Audit Other Object Access Events	71
Audit Registry	71
Audit Removable Storage	72
Audit SAM	72
Audit Central Policy Staging	73
Policy Change	73
Audit Policy Change	73
Audit Authentication Policy Change	74
Audit Authorization Policy Change	74
Audit Filtering Platform Policy Change	75
Audit MPSSVC Rule-Level Policy Change	75

	Audit Other Policy Change Events	75
	Privilege Use	76
	Audit Non Sensitive Privilege Use	76
	Audit Other Privilege Use Events	77
	Audit Sensitive Privilege Use	77
	System	77
	Audit IPsec Driver	78
	Audit Other System Events	78
	Audit Security State Change	78
	Audit Security System Extension	79
	Audit System Integrity	79
Part III	Security Monitoring Scenarios	81
Chapter 4	Account Logon	83
	Interactive Logon	85
	Successful Local User Account Interactive Logon	85
	Step 1: Winlogon Process Initialization	85
	Step 1: LSASS Initialization	87
	Step 2: Local System Account Logon	88
	Step 3: ALPC Communications between Winlogon and LSASS	92
	Step 4: Secure Desktop and SAS	92
	Step 5: Authentication Data Gathering	92
	Step 6: Send Credentials from Winlogon to LSASS	94
	Step 7: LSA Server Credentials Flow	95
	Step 8: Local User Scenario	96
	Step 9: Local User Logon: MSV1_0 Answer	99
	Step 10: User Logon Rights Verification	104
	Step 11: Security Token Generation	105
	Step 12: SSPI Call	105
	Step 13: LSASS Replies to Winlogon	105
	Step 14: Userinit and Explorer.exe	105
	Unsuccessful Local User Account Interactive Logon	106
	Successful Domain User Account Interactive Logon	110
	Steps 1–7: User Logon Process	110
	Step 8: Authentication Package Negotiation	110
	Step 9: LSA Cache	111
	Step 10: Credentials Validation on the Domain Controller	112
	Steps 11–16: Logon Process	112
	Unsuccessful Domain User Account Interactive Logon	112
	RemoteInteractive Logon	112
	Successful User Account RemoteInteractive Logon	112
	Successful User Account RemoteInteractive Logon Using Cached Credentials	114
	Unsuccessful User Account RemoteInteractive Logon - NLA Enabled	115

Unsuccessful User Account RemoteInteractive Logon - NLA Disabled	117
Network Logon	118
Successful User Account Network Logon	118
Unsuccessful User Account Network Logon	120
Unsuccessful User Account Network Logon - NTLM	121
Unsuccessful User Account Network Logon - Kerberos	122
Batch and Service Logon	123
Successful Service / Batch Logon	123
Unsuccessful Service / Batch Logon	125
NetworkCleartext Logon	127
Successful User Account NetworkCleartext Logon - IIS Basic Authentication	127
Unsuccessful User Account NetworkCleartext Logon - IIS Basic Authentication	129
NewCredentials Logon	129
Interactive and RemoteInteractive Session Lock Operations and Unlock Logon Type	132
Account Logoff and Session Disconnect	133
Terminal Session Disconnect	134
Special Groups	135
Anonymous Logon	136
Default ANONYMOUS LOGON Logon Session	136
Explicit Use of Anonymous Credentials	138
Use of Account That Has No Network Credentials	139
Computer Account Activity from Non-Domain-Joined Machine	139
Allow Local System to Use Computer Identity for NTLM	140
Chapter 5 Local User Accounts	141
Built-in Local User Accounts	142
Administrator	142
Guest	144
Custom User Account	145
HomeGroupUser\$	145
DefaultAccount	146
Built-in Local User Accounts Monitoring Scenarios	146
New Local User Account Creation	146
Successful Local User Account Creation	147
Unsuccessful Local User Account Creation: Access Denied	164
Unsuccessful Local User Account Creation: Other	165
Monitoring Scenarios: Local User Account Creation	166
Local User Account Deletion	168
Successful Local User Account Deletion	169
Unsuccessful Local User Account Deletion - Access Denied	173
Unsuccessful Local User Account Deletion - Other	175
Monitoring Scenarios: Local User Account Deletion	176

Local User Account Password Modification	177
Successful Local User Account Password Reset	178
Unsuccessful Local User Account Password Reset - Access Denied	179
Unsuccessful Local User Account Password Reset - Other	180
Monitoring Scenarios: Password Reset	181
Successful Local User Account Password Change	182
Unsuccessful Local User Account Password Change	183
Monitoring Scenarios: Password Change	184
Local User Account Enabled/Disabled	184
Local User Account Was Enabled	184
Local User Account Was Disabled	186
Monitoring Scenarios: Account Enabled/Disabled	186
Local User Account Lockout Events	187
Local User Account Lockout	188
Local User Account Unlock	190
Monitoring Scenarios: Account Enabled/Disabled	191
Local User Account Change Events	191
Local User Account Change Event	192
Local User Account Name Change Event	196
Monitoring Scenarios: Account Changes	198
Blank Password Existence Validation	199
Chapter 6 Local Security Groups	201
Built-in Local Security Groups	203
Access Control Assistance Operators	205
Administrators	205
Backup Operators	205
Certificate Service DCOM Access	205
Cryptographic Operators	205
Distributed COM Users	206
Event Log Readers	207
Guests	207
Hyper-V Administrators	207
IIS_IUSRS	208
Network Configuration Operators	208
Performance Log Users	209
Performance Monitor Users	209
Power Users	209
Print Operators	209
Remote Desktop Users	209
Remote Management Users	210
Replicator	210
Storage Replica Administrators	210
System Managed Accounts Group	210
Users	210
WinRMRemoteWMIUsers__	211

Built-in Local Security Groups Monitoring Scenarios	211
Local Security Group Creation	212
Successful Local Security Group Creation	212
Unsuccessful Local Security Group Creation - Access Denied	217
Monitoring Scenarios: Local Security Group Creation	218
Local Security Group Deletion	218
Successful Local Security Group Deletion	219
Unsuccessful Local Security Group Deletion - Access Denied	221
Unsuccessful Local Security Group Deletion - Other	222
Monitoring Scenarios: Local Security Group Deletion	223
Local Security Group Change	223
Successful Local Security Group Change	224
Unsuccessful Local Security Group Change - Access Denied	226
Monitoring Scenarios: Local Security Group Change	227
Local Security Group Membership Operations	227
Successful New Local Group Member Add Operation	228
Successful Local Group Member Remove Operation	231
Unsuccessful Local Group Member Remove/ Add Operation - Access Denied	232
Monitoring Scenarios: Local Security Group Members Changes	233
Local Security Group Membership Enumeration	234
Monitoring Scenarios: Local Security Group Membership Enumeration	235
Chapter 7	
Microsoft Active Directory	237
Active Directory Built-in Security Groups	237
Administrators	238
Account Operators	238
Incoming Forest Trust Builders	238
Pre-Windows 2000 Compatible Access	238
Server Operators	239
Terminal Server License Servers	239
Windows Authorization Access	239
Allowed RODC Password Replication Group	240
Denied RODC Password Replication Group	240
Cert Publishers	240
DnsAdmins	240
RAS and IAS Servers	241
Cloneable Domain Controllers	241
DnsUpdateProxy	241
Domain Admins	241
Domain Computers	241
Domain Controllers	242

Domain Users	242
Group Policy Creator Owners	242
Protected Users	242
Read-Only Domain Controllers	242
Enterprise Read-Only Domain Controllers	242
Enterprise Admins	243
Schema Admins	243
Built-in Active Directory Accounts	243
Administrator	243
Krbtgt	244
Directory Services Restore Mode (DSRM) Account	244
Active Directory Accounts Operations	245
Active Directory User Accounts Operations	245
Successful Active Directory User Creation	245
Unsuccessful Active Directory User Creation	250
Successful Active Directory User Deletion	251
Unsuccessful Active Directory User Deletion	252
Other Active Directory User Account Operations	252
Successful Active Directory User SID History Addition	252
Active Directory Computer Account Operations	253
Successful Computer Account Creation - Joining a Domain	253
Successful Computer Account Creation - Manual Creation	255
Unsuccessful Computer Account Creation	256
Successful Computer Account Deletion	257
Unsuccessful Computer Account Deletion	257
Successful Computer Account Modification	257
Unsuccessful Computer Account Modification	259
Active Directory Group Operations	259
Active Directory Group Creation	260
Active Directory Group Deletion	261
Active Directory Group Modification	262
Active Directory Group New Member Added	263
Active Directory Group Member Removed	265
Group Type and Scope Type Changes	266
Active Directory Trust Operations	267
Active Directory Trust Creation Operations	267
Active Directory Trust Modification Operations	272
Active Directory Trust Deletion Operations	273
Operations with Forest Trust Records	274
Active Directory Forest Trust Record Creation Operations	274
Active Directory Forest Trust Record Modification Operations	277
Active Directory Forest Trust Record Remove Operations	278
Domain Policy Changes	279
Password and Account Lockout Policies	279
Kerberos Policy	280
Account Password Migration	282

Chapter 8	Active Directory Objects	285
	Active Directory Object SACL	286
	Child Object Creation and Deletion Permissions	291
	Extended Rights	292
	Validated Writes	294
	Properties	295
	Default SACLs	296
	Active Directory Object Change Auditing	304
	Active Directory Object Creation	305
	Active Directory Object Deletion	306
	Active Directory Object Undeletion	307
	Active Directory Object Movement	309
	Active Directory Object Modification	310
	Add Value Operation	310
	Delete Value Operation	313
	Active Directory Object Operation Attempts	313
	Successful Active Directory Object Operation Attempts	313
	Unsuccessful Active Directory Object Operation Attempts	318
	Active Directory Objects Auditing Examples	320
	Organizational Unit Creation/Deletion	320
	Organizational Unit Child Object Creation/Deletion	320
	adminCount Attribute Modification for User Accounts	320
	Group Policy Link/Unlink Operations	321
Chapter 9	Authentication Protocols	323
	NTLM-family Protocols	323
	Challenge-Response Basics	323
	LAN Manager	325
	LM Hash	325
	LM Challenge-Response Mechanism	327
	NT LAN Manager	329
	NTLM Hash	329
	NTLM Challenge-Response Mechanism	330
	NT LAN Manager V2	330
	NTLMv2 Challenge-Response Mechanism	330
	NTLMSSP and Anonymous Authentication	333
	NTLMv1 Session Security and NTLMv2 Session Security	333
	NTLMv2 Session Response	334
	Anonymous Authentication	335
	NTLM-family Protocols Monitoring	335
	Network Security: Restrict NTLM Security Group Policy	
	Settings	335
	Local Account Authentication	336
	Domain Account Authentication	344
	Cross-Domain Challenge-Response	347
	Kerberos	348
	Ticket-Granting Ticket (TGT)	348

Successful AS_REQ Message	352
Unsuccessful AS_REQ Message - Password Expired, Wrong Password, Smart Card Logon Issues	354
Unsuccessful AS_REQ Message - Other Scenarios	356
TGT Renewal	357
Ticket-Granting Service (TGS) Ticket	358
Successful TGS_REQ Message	362
Unsuccessful TGS_REQ and AP_REQ Messages	364
Chapter 10 Operating System Events	367
System Startup/Shutdown	368
Successful Normal System Shutdown	368
Unsuccessful Normal System Shutdown - Access Denied	370
Successful System Startup	371
Monitoring Scenarios: System Startup/Shutdown	371
System Time Changes	372
Successful System Time Zone Change	373
Unsuccessful System Time Zone Change	374
Successful System Clock Settings Change	374
Unsuccessful System Clock Settings Change	376
Monitoring Scenarios: System Time Changes	376
System Services Operations	376
Successful Service Installation - Prior to Windows 10/2016	377
Successful Service Installation - Windows 10/2016	379
Unsuccessful Service Installation - Access Denied	380
System Service State Changes	382
Unsuccessful Service Stop Operation - Access Denied	383
Monitoring Scenarios: System Services Operations	384
Security Event Log Operations	386
Successful Security Event Log Erase Operation	386
Unsuccessful Security Event Log Erase Operation	387
Successful Security Event Log Service Shutdown	387
Unsuccessful Security Event Log Service Shutdown	388
Monitoring Scenarios: Security Event Log Operations	388
Changes in Auditing Subsystem Settings	388
Successful Auditing Subsystem Security Descriptor Change	388
Unsuccessful Auditing Subsystem Security Descriptor Change	394
Successful System Audit Policy Changes	395
Unsuccessful System Audit Policy Changes	400
Monitoring Scenarios: Changes in Auditing Subsystem Settings	400
Per-User Auditing Operations	401
Successful Per-User Auditing Policy Changes	402
Unsuccessful Per-User Auditing Policy Changes	404
Per-User Auditing Database Initialization	404
Monitoring Scenarios: Per-User Auditing Operations	404

Scheduled Tasks	405
Successful Scheduled Task Creation	406
Unsuccessful Scheduled Task Creation - Access Denied	408
Successful Scheduled Task Deletion	410
Unsuccessful Scheduled Task Deletion	410
Successful Scheduled Task Change	410
Unsuccessful Scheduled Task Change	411
Successful Scheduled Task Enable/Disable Operations	411
Monitoring Scenarios: Scheduled Tasks	413
Boot Configuration Data Changes	413
Monitoring Scenarios: Boot Configuration Data	417
Chapter 11 Logon Rights and User Privileges	419
Logon Rights	419
Logon Rights Policy Modification	420
Logon Rights Policy Settings - Member Added	421
Logon Rights Policy Settings - Member Removed	421
Unsuccessful Logons Due to Lack of Logon Rights	422
User Privileges	422
User Privileges Policy Modification	427
User Privileges Policy Settings - Member Added	427
User Privileges Policy Settings - Member Removed	428
Special User Privileges Assigned at Logon Time	429
Logon Session User Privileges Operations	430
Privilege Use	431
Successful Call of a Privileged Service	431
Unsuccessful Call of a Privileged Service	432
Successful Operation with a Privileged Object	433
Unsuccessful Operation with a Privileged Object	435
Backup and Restore Privilege Use Auditing	435
Chapter 12 Windows Applications	437
New Application Installation	437
Application Installation Using Windows Installer	440
Application Removal Using Windows Installer	443
Application Installation Using Other Methods	444
Application Installation - Process Creation	444
Application Installation - Software Registry Keys	445
Application Installation - New Folders in Program Files and Program Files (x86) Folders	448
Application Removal Using Other Methods	448
Application Removal - Process Creation	448
Application Removal - Software Registry Keys	449
Application Removal - Folder Removal in the Program Files and Program Files (x86) Folders	451
Application Execution and Termination	453
Successful Process Creation	455

Successful Process Creation - CreateProcessWithLogonW initiated	460
Unsuccessful Process Creation	461
Process Termination	463
Application Crash Monitoring	464
Windows Error Reporting	467
WER Report	471
Windows AppLocker Auditing	471
AppLocker Policy	471
AppLocker Monitoring	472
EXE and DLL	474
MSI and Script	479
Packaged app-Execution and Packaged app-Deployment	480
Process Permissions and LSASS.exe Access Auditing	480
LSASS's Process Default SACL	482
Chapter 13 Filesystem and Removable Storage	485
Windows Filesystem	486
NTFS Security Descriptors	487
Inheritance	493
SACL	494
File and Folder Operations	495
File/Folder Creation	495
Successful File Creation	495
Unsuccessful File Creation	498
Successful Folder Creation	501
Unsuccessful Folder Creation	502
File/Folder Deletion	503
Successful File Deletion	503
Unsuccessful File Deletion	504
Successful Folder Deletion	504
Unsuccessful Folder Deletion	505
File Content Modification	505
Successful File Content Modification	505
Unsuccessful File Content Modification	506
File Read Data	506
Successful File Read Data Operations	506
Unsuccessful File Read Data Operations	507
File/Folder Attribute Changes	507
Successful File/Folder Attribute Changes	507
Unsuccessful File/Folder Attribute Changes	508
File/Folder Owner Change	508
Successful File/Folder Owner Change	508
Unsuccessful File/Folder Owner Change	509
File/Folder Access Permissions Change	510
Successful Access Permissions Changes	510

Unsuccessful Access Permissions Changes	511
File/Folder SACL Changes	511
Successful Auditing Settings (SACL) Change	511
Unsuccessful Auditing Settings Change	514
Removable Storage	515
Global Object Access Auditing: Filesystem	516
File System Object Integrity Levels	517
File System Object Integrity Level Modification	518
File System Object Access Attempt - Access Denied by Integrity Policy Check	520
Monitoring Recommendations	520
Monitoring Scenarios	521
Chapter 14 Windows Registry	523
Windows Registry Basics	523
Registry Key Permissions	526
Registry Operations Auditing	528
Registry Key Creation	528
Successful Registry Key Creation	528
Unsuccessful Registry Key Creation	531
Registry Key Deletion	532
Successful Registry Key Deletion	532
Unsuccessful Registry Key Deletion	533
Operations with Registry Key Values	533
Successful Registry Value Creation	534
Unsuccessful Registry Key Value Creation	535
Successful Registry Key Value Deletion	536
Unsuccessful Registry Key Value Deletion	538
Successful Registry Key Value Modification	538
Unsuccessful Registry Value Modification	539
Registry Key Read and Enumerate Operations	539
Successful Registry Key Read Operation	539
Unsuccessful Registry Key Read Operation	540
Successful Registry Key Subkeys Enumeration	541
Unsuccessful Registry Key Subkeys Enumeration	542
Successful Registry Key Access Permissions Read	542
Unsuccessful Registry Key Access Permissions Read	543
Successful Registry Key Audit Permissions Read	543
Unsuccessful Registry Key Audit Permissions Read	545
DACL, SACL, and Ownership Change Operations	545
Successful Registry Key Access Permissions Change	546
Unsuccessful Registry Key Access Permissions Change	547
Successful Registry Key Audit Permissions Change	548
Unsuccessful Registry Key Audit Permissions Change	551
Successful Registry Key Owner Change	551

Global Object Access Auditing: Registry	553
Registry Key Integrity Levels	554
Registry Key Integrity Level Modification	554
Monitoring Recommendations	556
Monitoring Scenarios	557
Chapter 15 Network File Shares and Named Pipes	559
Network File Shares	559
Network File Share Access Permissions	563
File Share Creation	564
Successful File Share Creation	564
Monitoring Recommendations	565
File Share Deletion	566
Successful File Share Deletion	566
Unsuccessful File Share Deletion	567
Monitoring Recommendations	567
File Share Modification	567
Successful File Share Modification	568
Unsuccessful File Share Deletion	570
Monitoring Recommendations	570
File Share Access	570
Successful File Share Session Creation	570
Successful File Share File/Folder Operations	572
Unsuccessful Admin File Share Session Creation	574
Unsuccessful File Share Access - File Share Permissions	574
Unsuccessful File Share Access - File System Permissions	575
Monitoring Recommendations	576
Named Pipes	577
Successful Named Pipe Auditing Settings Changes	578
Unsuccessful Named Pipe Auditing Settings Changes	580
Successful Named Pipe Access Permissions Changes	581
Named Pipe Access Attempts	582
IPC\$ Share Access Attempts	582
Monitoring Recommendations	584
Appendix A Kerberos AS_REQ, TGS_REQ, and AP_REQ Messages Ticket Options	585
Appendix B Kerberos AS_REQ, TGS_REQ, and AP_REQ Messages Result Codes	589
Appendix C SDDL Access Rights	597
Object-Specific Access Rights	598
Index	603



Introduction

In this book I share my experience and the results of my research about the Microsoft Windows security auditing subsystem and event patterns. This book covers the Windows Security auditing subsystem and event logs for Windows systems starting from Windows 7 through the most recent Windows 10 and Windows Server 2016 versions.

Many IT Security/Infrastructure professionals understand that they should know what is going on in their company's infrastructure—for example, is someone using privileged accounts during nonworking hours or trying to get access to resources he or she shouldn't have access to? Looking for activities like these is critical to all organizations. To help with this, this book provides technical details about the most common event patterns for Microsoft Windows operating systems. It is a great source of information for building new detection methods and improving a company's Security Logging and Monitoring policy.

The primary goal of this book is to explain Windows security monitoring scenarios and patterns in as much detail as possible. A basic understanding of Microsoft Active Directory Services and Microsoft Windows operational systems will be helpful as you read through the book.

The following areas are covered:

- Implementation of the Security Logging and Monitoring policy
- Technical details about the Windows security event log subsystem
- Information about most common monitoring event patterns related to operations and changes in Microsoft Windows operating systems

The following software and technologies are covered:

- Microsoft Windows security event logs
- Microsoft Windows security auditing subsystem

- Microsoft Windows Active Directory Services
- Microsoft AppLocker
- Microsoft Windows event logs (Application, System, NTLM, and others)
- Microsoft Windows 7, 8, 8.1, 10
- Microsoft Windows Server 2008 R2, 2012, 2012 R2, 2016
- Microsoft PowerShell
- Microsoft Windows Sysinternals tools
- Third-party tools

You will find detailed explanations for many event patterns, scenarios, technologies, and methods, and it is my hope that you will find that you've learned a lot, and will start using this book every day. This book is intended as a reference that you will return to many times in your career.

Who This Book Is For

This book is best suited for IT security professionals and IT system administrators. It will be most valuable for IT security monitoring teams, incident response teams, data analytics teams, and threat intelligence experts.

The best way to use this book is as a reference and source of detailed information for specific Windows auditing scenarios.

What This Book Covers

One of the main goals of this book is to help you create a Security Logging and Monitoring (SL&M) standard for your company. At the beginning of the book I cover what this standard is about, which sections it has, and discuss best practices for creating this document.

Before jumping into the world of event logs, you need to understand how the Windows Auditing Subsystem works and which components and settings belong to this system. I cover security best practices for the Windows security auditing subsystem, its components, and internal data flows.

There are multiple event logs in Windows systems besides the Security log, and many of these logs contain very useful information. It's important to know which subsystems have which event logs, the purpose of these event logs, and the type of information collected in these logs. This information is also present in this book.

I think the most interesting part of the book deals with security monitoring scenarios and patterns. Based on these scenarios, security managers, analysts, engineers, and administrators will be able to improve security monitoring policies and build new or improve existing detection methods.

How This Book Is Structured

This book consists of 15 chapters and three appendixes. The first three chapters cover general information about the Windows auditing subsystem and security monitoring policy. The remaining chapters go deeper in to different monitoring scenarios and event patterns.

Chapter by chapter, this book covers:

- **Windows Security Logging and Monitoring Policy (Chapter 1)**—This chapter guides you through the sections of the Security Logging and Monitoring (SL&M) standard and provides the basic information you need to create your own version of it.
- **Auditing Subsystem Architecture (Chapter 2)**—In this chapter you will find information about Legacy Auditing and Advanced Auditing settings, Windows auditing group policy settings, auditing subsystem architecture, and security event structure.
- **Auditing Subcategories and Recommendations (Chapter 3)**—In this chapter you will find descriptions for each Advanced Auditing subcategory and recommended settings for domain controllers, member servers, and workstations.
- **Account Logon (Chapter 4)**—This chapter contains information about Windows logon types and the events generated during each of them.
- **Local User Accounts (Chapter 5)**—In this chapter you will find information about different built-in local user accounts on Microsoft Windows operating systems and specific monitoring scenarios for the most important operations/changes done to local user accounts.
- **Local Security Groups (Chapter 6)**—In this chapter you will learn about different scenarios related to local security groups, such as security group creation, deletion, and modification, and so on.
- **Microsoft Active Directory (Chapter 7)**—In this chapter you will find information about the most common monitoring scenarios for Active Directory, such as user or computer account creation, operations with groups, operations with trusts, and so on.

- **Active Directory Objects (Chapter 8)**—This chapter contains detailed information about monitoring Active Directory changes and operations with objects, such as group policy creation, organization unit modification, and so on.
- **Authentication Protocols (Chapter 9)**—In this chapter you will find information about how the LM, NTLM, NTLMv2, and Kerberos protocols work and how to monitor the most common scenarios involving these protocols.
- **Operating System Events (Chapter 10)**—This chapter contains information about the different system events that might indicate malicious activity performed on the system.
- **Logon Rights and User Privileges (Chapter 11)**—In this chapter you will find detailed information about how to monitor logon rights and user privileges policy changes, user privileges use, and use of backup and restore privileges.
- **Windows Applications (Chapter 12)**—It is important to monitor the use of applications on the host, activities such as application installation, removal, execution, application crashes, application block events by the AppLocker component, and so on. In this chapter you will find detailed information about monitoring these scenarios and more.
- **Filesystem and Removable Storage (Chapter 13)**—This chapter is probably one of the most interesting chapters in the book, because it covers some of the most common questions you'll have or hear during incident investigation procedures: Who deleted the file? Who created the file? How this file was accessed? Using which tool/application?

Some of these questions are easy to answer, but some of them are not. In this chapter you will find information about monitoring recommendations for the most common scenarios related to Windows filesystem and removable storage objects.
- **Windows Registry (Chapter 14)**—This chapter contains information about Windows registry operations and monitoring scenarios.
- **Network File Shares and Named Pipes (Chapter 15)**—In this chapter you will find information about monitoring scenarios for actions related to network file shares and named pipes.

What You Need to Use This Book

This book requires that you have Windows 10 (build 1511 or higher) installed to open the `.evtx` files included in this book's download materials.

Conventions

To help you get the most from the text and keep track of what's happening, we've used a number of conventions throughout the book.

NOTE Notes, tips, hints, tricks, and asides to the current discussion look like this.

As for styles in the text:

- We *italicize* new terms and important words when we introduce them.
- We show keyboard strokes like this: Ctrl+A.
- We show filenames, URLs, and code within the text like so: `persistence.properties`.

We present code and event listings in two different ways:

We use a monofont type with no highlighting for most code and event examples.

We use bold type to emphasize code or events of particularly importance in the present context.

What's on the Website

All of the event examples used in this book are available for download at www.wiley.com/go/winsecuritymonitoring as `.evtx` files. These files can be opened by the built-in Windows 10 or Windows Server 2016 Event Viewer application. You will find references to these event log files in each section of every chapter that has event samples in it.

Part

I

Introduction to Windows Security Monitoring

In This Part

Chapter 1: Windows Security Logging and Monitoring Policy

Windows Security Logging and Monitoring Policy

The purpose of the Security Logging and Monitoring (SL&M) policy is to ensure the confidentiality, integrity, and availability of information by specifying the minimum requirements for security logging and monitoring of company systems.

It is recommended to have such a policy defined and published in order to standardize security logging and monitoring requirements.

This chapter guides you through the sections of the SL&M policy and provides basic information for creating your own version.

Security Logging

This section outlines the requirements for what needs to be logged and how logs need to be managed.

Security logs provide vital information about system events that may, when correlated with other events or used independently, indicate a breach or misuse of resources. When configured and managed properly, logs are key in establishing accountability and attribution for any event. They provide answers to the critical questions about security events: who is involved, what happened, when and where it happened, and how it happened.

Companies should ensure that information passing through their systems, including user activities such as web sites visited and servers accessed, is logged, reviewed, and otherwise utilized.

Implementing the recommendations in this section can mitigate the risk of an attacker's activities going unnoticed and enhance a company's ability to conclude whether an attack led to a breach.

Security Logs

Information systems should enable and implement logging, also referred to as audit logging. Activities that should be logged may include the following:

- All successful and unsuccessful logon attempts
- Additions, deletions, and modifications of local and domain accounts/privileges
- Users switching accounts during an active session
- Attempts to clear audit logs
- Activity performed by privileged accounts, including modifications to system settings
- Access to restricted data additions, deletions, and modifications to security/audit log parameters
- User account management activities
- System shutdown/reboot
- System errors
- New system service creation
- Application shutdown/restart
- Application errors/crashes
- Process creation/termination
- Registry modification(s)
- Local security policy modifications
- GPO-based security policy modifications
- Use of administrator privileges
- File access
- Critical process manipulation (*LSASS.exe*)
- System corruption (for example, audit pipeline failure, LPC impersonation, and so on)

All of these items are discussed in more detail in this book.

You should also think about where and how to store system events that are used to detect system attack attempts. These events also represent evidence for incident follow-up.