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

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

Library of Congress Control Number: 2017962214

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.

Credits

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

Contents

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 crushes, 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`.

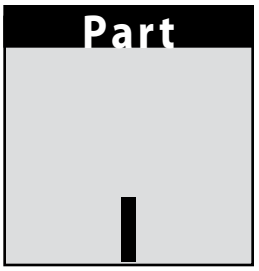
We present code and event listings in two different ways:

```
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.



Introduction to Windows Security Monitoring

In This Part

CHAPTER 1

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.