



TIMELY. PRACTICAL. RELIABLE.

Incident Response

Incident Response: Computer Forensics Toolkit

By Douglas Schweitzer

Paperback / April 2003 / 0764526367

[Link to Publisher](#)

[Link to Amazon](#)

Computer
Forensics
Toolkit



Douglas Schweitzer

Contents at a Glance

Acknowledgments

Introduction

Chapter 1 Computer Forensics and Incident Response Essentials

Chapter 2 Addressing Law Enforcement Considerations

Chapter 3 Forensic Preparation and Preliminary Response

Chapter 4 Windows Registry, Recycle Bin, and Data Storage

Chapter 5 Analyzing and Detecting Malicious Code and Intruders

Chapter 6 Retrieving and Analyzing Clues

Chapter 7 Procedures for Collecting and Preserving Evidence

Chapter 8 Incident Containment and Eradication of Vulnerabilities

Chapter 9 Disaster Recovery and Follow-Up

Chapter 10 Responding to Different Types of Incidents

Chapter 11 Assessing System Security to Prevent Further Attacks

Chapter 12 Pulling It All Together

Appendix A What's on the CD-ROM

Appendix B Commonly Attacked Ports

Appendix C Field Guidance on USA Patriot Act 2001

Appendix D Computer Records and the Federal Rules of Evidence

Appendix E Glossary

Index

Contents

Acknowledgments

Introduction

Chapter 1 Computer Forensics and Incident Response Essentials

Catching the Criminal: The Basics of Computer Forensics

- Recognizing the Signs of an Incident
- Preparing for Incidents
- Developing a Computer Security Incident Response Capability
- The Computer Security Incident Response Team
- The Incident Reporting Process
- Assessment and Containment
- Recovery Operations
- Damage Analysis and Determination
- Shutdown Procedures while Preserving Evidence
- NIPC Recommendations for Victims
- Building an Incident Response/Forensic Toolkit
- Chapter Summary

- Chapter 2 Addressing Law Enforcement Considerations
 - A Look at the Fourth Amendment
 - A Brief Primer on the Freedom of Information Act
 - Reporting Security Breaches to Law Enforcement
 - Information Sharing Issues in Computer Crime Investigations
 - The Role of the National Infrastructure Protection Center
 - Understanding Disclosure and Discovery
 - Disclosure of Contents
 - Federal Computer Crimes and Laws
 - The Computer Fraud and Abuse Act of 1986
 - Computer Fraud and Abuse Act of 1986 (US) 18 USC 1030
 - The Computer Abuse Amendments Act of 1994
 - The USA Patriot Act of 2001
 - Chapter Summary

- Chapter 3 Forensic Preparation and Preliminary Response
 - Preparing Operating Systems for Data Collection
 - The Significance of Log Files
 - Auditing and Logging Procedures
 - Enabling Auditing and Logging on Windows NT
 - A Quick Note about Auditing, Logging, and Log File Size
 - Centralized Logging
 - Time Synchronization
 - Time-Stamping
 - Identifying Network Devices
 - Collecting Data from Memory
 - Selecting the Appropriate Memory Dump Options
 - Using Dumpchk.exe to View the Windows memory.dmp File
 - Performing Memory Dump on Unix Systems
 - Imaging Hard Drives
 - Following the Chain-of-Custody for Evidence Collection
 - Business Continuity and Contingency Planning
 - The IT Contingency-Planning Process
 - Chapter Summary

- Chapter 4 Windows Registry, Recycle Bin, and Data Storage
 - The Windows Registry
 - Registry Structure

- Viewing and Editing the Registry
- Collecting Registry Data
- Registry Backup and Restore Procedures
- Registry Backup Programs (Shareware and Freeware)
- Understanding Data Storage
- The Hard Disk
- The Floppy Disk
- The CD-ROM
- The Windows File Allocation Table
- The Windows New Technology File System
- The Windows Recycle Bin
- The Bin Is Empty, yet the Evidence Remains
- Tracking Deleted Files Through the Windows Recycle Bin
- Recovering Deleted Data in Windows
- Industrial-Strength Recovery Utility
- Unix/Linux Data Storage Using the ext2 File System
- File Deletion in ext2
- File Recovery in ext2
- Using e2undel
- Chapter Summary

- Chapter 5 Analyzing and Detecting Malicious Code and Intruders
- System Processes
- Detecting Abnormal System Processes
- Using the Windows Task Manager to View Running Processes
- Default Processes in Windows NT, 2000, and XP
- Process-Monitoring Programs
- Unusual or Hidden Files
- Viewing Hidden Files in Windows
- Viewing Hidden Files under Unix/Linux
- Rootkits and Backdoors
- Detecting the Presence of a Rootkit
- Detecting the Presence of a Backdoor
- Removing Rootkits and Trojans
- Detecting and Defending Against Network Sniffers
- Chapter Summary

- Chapter 6 Retrieving and Analyzing Clues
- Performing Keyword Searches
- Industrial Strength Keyword-Searching Programs
- Freeware Keyword Search Tools
- Using SectorSpyXP to Perform a Keyword Search
- General Guidelines for Hard Drive Examination
- Examining the Windows Swap File
- Locating the Windows Swap File
- Viewing the Contents of the Swap/Page File
- E-Mail as Evidence
- Locating E-Mail
- Retrieving Deleted E-Mail
- Recovering Evidence from the Web Browser
- Locating Browser History Evidence
- Locating Web Cache Evidence

Print Spooler Files
Locating Hidden Data
Steganography
Password-Protected Compressed Data
Example Using Ultimate ZIP Cracker
Chapter Summary

Chapter 7 Procedures for Collecting and Preserving Evidence
Postcompromise Evidence Collection
Legal Requirements for Collecting Electronic Evidence
Unix/Linux Login Banners
The Order of Collection
Understanding Volatility of Evidence
Creating a Real-Mode Forensics Boot Disk
The Skinny on the FAT
Creating a Windows Real-Mode Boot Disk
Creating a Linux Boot Disk
Using Packet Sniffers to Gather Evidence
Building a Forensic Toolkit
The Coroner's Toolkit (TCT)
Using Grave-robber
Running Grave-robber
Following the Chain-of-Custody
The Admissibility of Evidence
Authentication
The Frye Test
The Best Evidence Rule
The Permissible Time Period for Examining Seized Computers
Evidence Preservation
Chapter Summary

Chapter 8 Incident Containment and Eradication of Vulnerabilities
Quarantine and Containment
Determine the Risk of Continuing Operations
Preserving Integrity
Audit Mechanisms
User-Detected Technical Vulnerabilities
Vulnerability Reporting Form
Severing Network and Internet Connections
Network and File-Sharing Issues
Configuring Windows File Sharing for Maximum Security
Windows XP File Sharing
Windows XP Simple File Sharing
Creating Access Control Lists
Disabling File and Print Sharing under Windows 95/98/Me
Recognizing the Trust Model
The Trust Model in Computer Operations
User ID and Password Trust
Operating System Trust
The Trust Model and Identity Theft
Computer Security Awareness
Multimedia Documentation Strategies

The Eradication Phase
Harden Your Defenses
Perform Analysis of Vulnerabilities
Chapter Summary

Chapter 9 Disaster Recovery and Follow-Up
Disaster Recovery Planning
Developing a Disaster Recovery Plan
Sample Contingency Disaster Recovery Plan
Electronic Recordkeeping
Authentication of Electronic Records
Electronic Records as Evidence
Records Security
The Uninterruptible Power Supply
How UPS Works
UPS Benefits
Purchasing a UPS
Understanding Data Backup Procedures
Creating a Backup Plan
Data Backup Tools
Post-Incident Monitoring and Analysis
Anticipating Future Attacks
Chapter Summary

Chapter 10 Responding to Different Types of Incidents
Responding to Hacker Incidents
Identify the Hacker
Active Hacker Incidents
Monitoring Hacker Activity
Previous Incidents
Follow-Up
Responding to Malicious Code Incidents
Trojan Horses
Internet Worms
Isolate the System and Notify Appropriate Staff
Contain the Virus, Worm, or Trojan Horse
Inoculate the System
Return Systems to Normal Operating Mode
Handling Inappropriate Use
Types of Harassment
Incidents Involving Sexual Harassment
Avoiding Sexual Harassment Lawsuits
Guidelines for Developing a Sexual Harassment Policy
Preventing Workers from Viewing Inappropriate Material
Industrial Espionage
Defending Against Insider Attacks
Chapter Summary

Chapter 11 Assessing System Security to Prevent Further Attacks
Assessment of Security Policies and Procedures
Developing Security Policy Checklists
Policy Audit Checklist — Sample

- An Overview of the Computer Security Audit Process
- Auditing Workstations and Servers
- Analyzing Workstations
- Analyzing Network Servers
- How to Disable NetBIOS Null Sessions
- Penetration Testing
- In-House vs. Outsourcing
- Penetration-Testing Software for In-House Audits
- Third-Party Penetration Testing
- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- HIPAA Compliance
- The HoneyNet Project
- Chapter Summary

- Chapter 12 Pulling It All Together
- Analyzing Real-World Attacks
- Security Lessons Learned from Others
- Lessons Learned from the Code Red Worm
- Lessons Learned from Hackers
- Where to Go for Up-to-Date Information
- Future Trends in Security Technology
- Chapter Summary

- Appendix A What's on the CD-ROM
- Appendix B Commonly Attacked Ports
- Appendix C Field Guidance on USA Patriot Act 2001
- Appendix D Computer Records and the Federal Rules of Evidence
- Appendix E Glossary
- Index