CONTENTS IN DETAIL

FOREWORD **xix**

ACKNOWLEDGMENTS **xxi**

INTRODUCTION **xxiii**

Who Is This Book For? xxiv
What Is in This Book? xxiv
PowerShell Conventions Used in This Book xxvii
Getting in Touch. xxviii

PART I: AN OVERVIEW OF THE WINDOWS OPERATING SYSTEM **1**

1
SETTING UP A POWERSHELL TESTING ENVIRONMENT **3**

Choosing a PowerShell Version 3
Configuring PowerShell. 4
An Overview of the PowerShell Language. 5
Understanding Types, Variables, and Expressions 5
Executing Commands 9
Discovering Commands and Getting Help 10
Defining Functions. 13
Displaying and Manipulating Objects 14
Filtering, Ordering, and Grouping Objects. 17
Exporting Data 20
Wrapping Up 21

2
THE WINDOWS KERNEL **23**

The Windows Kernel Executive 24
The Security Reference Monitor 25
The Object Manager 27
Object Types 27
The Object Manager Namespace. 28
System Calls. 29
NTSTATUS Codes 32
Object Handles. 35
Query and Set Information System Calls 42
The Input/Output Manager 45
The Process and Thread Manager 47
The Memory Manager 49
NtVirtualMemory Commands 49
Section Objects. 51

Code Integrity 54
Advanced Local Procedure Call 55
The Configuration Manager 55
Worked Examples 56
Finding Open Handles by Name 57
Finding Shared Objects 57
Modifying a Mapped Section 59
Finding Writable and Executable Memory 60
Wrapping Up 61

3
USER-MODE APPLICATIONS 63

Win32 and the User-Mode Windows APIs 64
Loading a New Library 65
Viewing Imported APIs 66
Searching for DLLs 68
The Win32 GUI 70
GUI Kernel Resources 71
Window Messages 73
Console Sessions 74
Comparing Win32 APIs and System Calls 77
Win32 Registry Paths 80
Opening Keys 81
Listing the Registry's Contents 81
DOS Device Paths 83
Path Types 84
Maximum Path Lengths 85
Process Creation 87
Command Line Parsing 88
Shell APIs 89
System Processes 91
The Session Manager 92
The Windows Logon Process 92
The Local Security Authority Subsystem 92
The Service Control Manager 92
Worked Examples 94
Finding Executables That Import Specific APIs 94
Finding Hidden Registry Keys or Values 94
Wrapping Up 96

PART II: THE WINDOWS SECURITY REFERENCE MONITOR 97

4
SECURITY ACCESS TOKENS 99

Primary Tokens 100
Impersonation Tokens 104
Security Quality of Service 104
Explicit Token Impersonation 107

Converting Between Token Types 107
Pseudo Token Handles 108
Token Groups 109
Enabled, EnabledByDefault, and Mandatory 110
LogonId 111
Owner 111
UseForDenyOnly 111
Integrity and IntegrityEnabled 112
Resource 113
Device Groups 113
Privileges 113
Sandbox Tokens 117
Restricted Tokens 117
Write-Restricted Tokens 119
AppContainer and Lowbox Tokens 120
What Makes an Administrator User? 122
User Account Control 124
Linked Tokens and Elevation Type 126
UI Access 129
Virtualization 129
Security Attributes 130
Creating Tokens 131
Token Assignment 133
Assigning a Primary Token 133
Assigning an Impersonation Token 136
Worked Examples 138
Finding UI Access Processes 138
Finding Token Handles to Impersonate 139
Removing Administrator Privileges 140
Wrapping Up 141

5
SECURITY DESCRIPTORS 143

The Structure of a Security Descriptor 144
The Structure of a SID 146
Absolute and Relative Security Descriptors 149
Access Control List Headers and Entries 151
The Header 152
The ACE List 153
Constructing and Manipulating Security Descriptors 156
Creating a New Security Descriptor 157
Ordering the ACEs 158
Formatting Security Descriptors 159
Converting to and from a Relative Security Descriptor 163
The Security Descriptor Definition Language 165
Worked Examples 173
Manually Parsing a Binary SID 173
Enumerating SIDs 175
Wrapping Up 176

6
READING AND ASSIGNING SECURITY DESCRIPTORS 177

Reading Security Descriptors 178
Assigning Security Descriptors 180
Assigning a Security Descriptor During Resource Creation 180
Assigning a Security Descriptor to an Existing Resource 205
Win32 Security APIs 208
Server Security Descriptors and Compound ACEs 213
A Summary of Inheritance Behavior 214
Worked Examples 216
Finding Object Manager Resource Owners 216
Changing the Ownership of a Resource 218
Wrapping Up 219

7
THE ACCESS CHECK PROCESS 221

Running an Access Check 222
Kernel-Mode Access Checks 222
User-Mode Access Checks 225
The Get-NtGrantedAccess PowerShell Command 226
The Access Check Process in PowerShell 227
Defining the Access Check Function 228
Performing the Mandatory Access Check 230
Performing the Token Access Check 237
Performing the Discretionary Access Check 241
Sandboxing 244
Restricted Tokens 244
Lowbox Tokens 246
Enterprise Access Checks 249
The Object Type Access Check 249
The Central Access Policy 255
Worked Examples 261
Using the Get-PSGrantedAccess Command 261
Calculating Granted Access for Resources 262
Wrapping Up 263

8
OTHER ACCESS CHECKING USE CASES 265

Traversal Checking 266
The SeChangeNotifyPrivilege Privilege 267
Limited Checks 267
Handle Duplication Access Checks 269
Sandbox Token Checks 272
Automating Access Checks 275
Worked Examples 277
Simplifying an Access Check for an Object 277
Finding Writable Section Objects 278
Wrapping Up 279

9
SECURITY AUDITING **281**

The Security Event Log 282
Configuring the System Audit Policy 282
Configuring the Per-User Audit Policy 285
Audit Policy Security 287
Configuring the Resource SACL 288
Configuring the Global SACL 292
Worked Examples 293
Verifying Audit Access Security 293
Finding Resources with Audit ACEs 294
Wrapping Up 295

PART III: THE LOCAL SECURITY AUTHORITY AND AUTHENTICATION **297**

10
WINDOWS AUTHENTICATION **299**

Domain Authentication 300
Local Authentication 300
Enterprise Network Domains 301
Domain Forests 302
Local Domain Configuration 305
The User Database 305
The LSA Policy Database 309
Remote LSA Services 311
The SAM Remote Service 312
The Domain Policy Remote Service 318
The SAM and SECURITY Databases 324
Accessing the SAM Database Through the Registry 325
Inspecting the SECURITY Database 334
Worked Examples 336
RID Cycling 336
Forcing a User's Password Change 337
Extracting All Local User Hashes 338
Wrapping Up 339

11
ACTIVE DIRECTORY **341**

A Brief History of Active Directory 342
Exploring an Active Directory Domain with PowerShell 342
The Remote Server Administration Tools 343
Basic Forest and Domain Information 344
The Users 345
The Groups 346
The Computers 348

Objects and Distinguished Names 349
Enumerating Directory Objects 350
Accessing Objects in Other Domains 352
The Schema 353
Inspecting the Schema 354
Accessing the Security Attributes 356
Security Descriptors 358
Querying Security Descriptors of Directory Objects 358
Assigning Security Descriptors to New Directory Objects 360
Assigning Security Descriptors to Existing Objects 363
Inspecting a Security Descriptor's Inherited Security 365
Access Checks 366
Creating Objects 366
Deleting Objects 369
Listing Objects 369
Reading and Writing Attributes 370
Checking Multiple Attributes 371
Analyzing Property Sets 373
Inspecting Control Access Rights 376
Analyzing Write-Validated Access Rights 378
Accessing the SELF SID 379
Performing Additional Security Checks 380
Claims and Central Access Policies 382
Group Policies 384
Worked Example 387
Building the Authorization Context 387
Gathering Object Information 390
Running the Access Check 391
Wrapping Up 395

12
INTERACTIVE AUTHENTICATION **397**

Creating a User's Desktop 398
The LsaLogonUser API 399
Local Authentication 401
Domain Authentication 403
Logon and Console Sessions 404
Token Creation 407
Using the LsaLogonUser API from PowerShell 410
Creating a New Process with a Token 412
The Service Logon Type 413
Worked Examples 414
Testing Privileges and Logon Account Rights 415
Creating a Process in a Different Console Session 416
Authenticating Virtual Accounts 417
Wrapping Up 419

13
NETWORK AUTHENTICATION **421**

NTLM Network Authentication 422
NTLM Authentication Using PowerShell 423
The Cryptographic Derivation Process 431

Pass-Through Authentication 434
Local Loopback Authentication 435
Alternative Client Credentials 436
The NTLM Relay Attack 438
Attack Overview 438
Active Server Challenges 440
Signing and Sealing 440
Target Names 443
Channel Binding 444
Worked Example 445
Overview 445
The Code Module 446
The Server Implementation 449
The Client Implementation 451
The NTLM Authentication Test 453
Wrapping Up 454

14
KERBEROS **457**

Interactive Authentication with Kerberos 458
Initial User Authentication 458
Network Service Authentication 463
Performing Kerberos Authentication in PowerShell 465
Decrypting the AP-REQ Message 469
Decrypting the AP-REP Message 476
Cross-Domain Authentication 477
Kerberos Delegation 479
Unconstrained Delegation 481
Constrained Delegation 484
User-to-User Kerberos Authentication 491
Worked Examples 493
Querying the Kerberos Ticket Cache 494
Simple Kerberoasting 495
Wrapping Up 496

15
NEGOTIATE AUTHENTICATION AND OTHER SECURITY PACKAGES **499**

Security Buffers 500
Using Buffers with an Authentication Context 501
Using Buffers with Signing and Sealing 502
The Negotiate Protocol 503
Less Common Security Packages 505
Secure Channel 506
CredSSP 510
Remote Credential Guard and Restricted Admin Mode 513
The Credential Manager 514
Additional Request Attribute Flags 517
Anonymous Sessions 518
Identity Tokens 519

Network Authentication with a Lowbox Token 520
Authentication with the Enterprise Authentication Capability 520
Authentication to a Known Web Proxy 521
Authentication with Explicit Credentials 522
The Authentication Audit Event Log 524
Worked Examples 527
Identifying the Reason for an Authentication Failure 527
Using a Secure Channel to Extract a Server's TLS Certificate 530
Wrapping Up 533
Final Thoughts 533

A
BUILDING A WINDOWS DOMAIN NETWORK FOR TESTING 535

The Domain Network 536
Installing and Configuring Windows Hyper-V 537
Creating the Virtual Machines 538
The PRIMARYDC Server 539
The GRAPHITE Workstation 542
The SALESDC Server 544

B
SDDL SID ALIAS MAPPING 547

INDEX 551