



Contents

Foreword	xxvii
Acknowledgments	xxxix
Introduction	xxxiii
Part I Introducing Windows Vista	1
Chapter 1 New Security Features	3
Security Development Lifecycle	3
Improved C++ Security	4
Address Space Layout Randomization	5
Data Execution Protection	6
Protected Processes	7
Windows Vista User Experience	7
Host-Based Security	8
Boot Changes	8
Boot Configuration Data	8
System Recovery	10
Startup Repair Tool	11
BitLocker Drive Encryption and TPM	11
Security Defaults	12
Windows Defender	13
Malicious Software Removal Tool	13
Improved Logon Architecture	14
LAN Manager Disabled	14
Better Support for Additional Authentication Methods	14
Session Isolation	16
Service Hardening	17
Enhanced Device Driver Experience	18
User-Mode Driver Framework	19
Portable Media Device Control	19
ReadyBoost Memory	19

xii Contents

User Account Control	20
Secure Desktop	21
Mandatory Integrity Control	22
Improved File, Folder, and Registry Protection	23
NTFS Changes	23
Creator Owners Can Be Prevented from	
Having Full Control	24
Per Socket Permissions	24
New Built-in Users and Groups	24
File and Registry Virtualization	25
Windows Resource Protection	25
Encryption Enhancements	26
EFS Enhancements	27
RMS-Integrated Client	27
Unix on Windows	28
Improved Patch Management	28
Hot Patching and Restart Manager	28
Improved Event Logs	28
Subscription and Forwarded Events	29
Task Manager	30
Increased Emphasis on Backup	31
Securing E-mail and the Internet	31
Windows Mail	31
Internet Explorer	32
IIS 7	34
Securing Windows Networks	34
Enhanced Network Location Awareness	35
Network Map	35
The Rebuilt TCP/IP Stack with IPv6	36
Routing Compartmentalization	36
Windows Firewall	36
Domain Isolation	36
Improved Wireless Security	37
New Peer-to-Peer Networking	37
SMB 2.0	38
Group Policy	38
64-bit Only Improvements	39
Future Improvements	40
Summary	40
Best Practices	42
Chapter 2 How Hackers Attack	43
Malicious Exploitation	43
Eight Exploitation Techniques	43
Logon Credential Guessing/Cracking	44
Password Guessing	44
Buffer Overflow	51

Metasploit Framework	53
OS or Application Vulnerability	54
Privilege Escalation	54
Information Disclosure	55
Data Malformation	55
Unintended Consequences	56
OS or Application Misconfiguration	56
Eavesdropping/Man-in-the-Middle Attack	57
Denial of Service Attack	57
Client-Side Attack	58
Social Engineering	59
Dedicated Hacker Methodology	60
Automated Malware	62
Computer Virus	62
Computer Worm	62
Trojan Horse Program	62
Bot	63
Spyware	64
Adware	64
Where Windows Malware Hides	65
Why Malicious Hackers Hack	70
Summary	71
Chapter 3 Windows Infrastructure	73
Boot Sequence	74
Boot Viruses No Longer a Threat	76
BitLocker Volume Encryption	76
Enabling TPM and BitLocker	80
Post-Boot Startup	87
Applying Security Policy	88
Name Resolution	89
NetBIOS Name Resolution Is Often Required	90
User Profiles	90
Services	92
Services You Need To Understand	94
Svchost	94
RPC	95
SMB/CIFS	97
Computer Browser, Workstation, and Server Service	98
Autorun Programs	99
Registry	101
Registry Structure	101
HKey_Local_Machine Hive	102
HKey_Classes_Root	103
HKey_Current_Users	107
HKey_Users	107
HK_Current Config	107

xiv Contents

Logon Authentication	108
Identity	108
Authentication	109
Computer Accounts	109
Password Storage	110
Authentication Protocols	110
SAM Versus Active Directory	112
Cache Credentials	113
Access Control	114
Share Versus NTFS Permissions	115
Impersonation Versus Delegation	115
Integrity Controls	116
Summary	117
Part II	Host-Based Security
	119
Chapter 4	User Account Control
	121
Introduction	121
Basics	123
Security Identifiers	124
Security Token	125
The Case for Least Privilege	128
Admins Are Omnipotent	129
User Account Control Is More Than You Think	129
Elevation	130
Non-Admin Elevation	137
Special Topics in Elevation	139
New Privileges to Delegate Common Tasks	140
Application Factoring	143
Virtualization	145
Integrity Labels and Low Rights Apps	146
Special Treatment of Built-in Administrator	146
No More Power Users	147
UAC and Remote Access	148
SMB Access	148
Remote Desktop and Remote Assistance	148
UAC Policy Configuration	150
User Account Control: AdminApproval Mode for the Built-in Administrator Account	150
User Account Control: Behavior of the Elevation Prompt for Administrators in Admin Approval Mode	150
User Account Control: Behavior of the Elevation Prompt for Standard Users	150
User Account Control: Detect Application Installations and Prompt for Elevation	151
User Account Control: Only Elevate Executables that Are Signed and Validated	151
User Account Control: Only Elevate UIAccess Applications that Are Installed in Secure Locations	152

User Account Control: Run All Administrators in Admin Approval Mode	152
User Account Control: Switch to the Secure Desktop when Prompting for Elevation	152
User Account Control: Virtualize File and Registry Write Failures to Per-User Locations	152
Frequently Asked Questions About UAC	153
Why Can't I Access My Files?	153
Why Can't I Delete Stuff If I Elevate Windows Explorer?	154
How Do I Disable UAC?	156
What Happens If I Turn Off UAC?	157
What Access Do Low Processes Have to High Processes?	157
Why Does the Screen Have to Go Black?	158
I Don't Need UAC; Can I Just Enable It for Other Users?	159
What About Remote Access?	160
Why Isn't UAC More Like Sudo?	160
How Do I Audit Elevation?	162
Leveraging User Account Control in Applications	164
Application Manifests	165
Elevating Installers	166
Elevating in Scripts	166
The Elevate Tool	166
Elevated Command Prompt	166
Summary	168
Best Practices	168
Chapter 5 Managing Access Control	171
Access Control Terminology	172
Securable Object	172
Access Control List	173
Security Descriptor	173
Access Control List Entry	174
ACL Representations	174
Inheritance	174
How an Access Control List Is Used	175
Major Access Control List Changes in Vista	178
Least Privilege	179
New and Modified Users and Groups	179
Administrator — Disabled By Default	180
Power Users Permissions Removed	180
Trusted Installer	181
Help and Support Accounts Removed	181
New Network Location SIDs	181
OWNER_RIGHT and Owner Rights	182
Default ACLs	183
Trusted Installer	184
Deny ACEs	184
Default Permissions	186

xvi Contents

Share Security	189
Changes to Token	189
Integrity Levels	190
Tools to Manage Access Control Lists	190
Cacls and Icacls	191
Save ACLs	191
Restore ACLs	192
Substitute SIDs	193
Change Owner	194
Find All Aces Granted to a Particular User	195
Resetting ACLs	195
Grant/Deny/Remove	195
Set Integrity Level	196
ACL UI	197
Other Tools	199
Registry ACLs	199
Summary	201
Best Practices	201
Chapter 6 Application Security	203
Client Security	203
Service Hardening	204
Service SID	204
Services Running with Less Privilege	205
Reduction of Privileges in Services	205
Write Restricted Tokens	207
Firewall Policies Restricting Services	207
Named Pipes Hardening	207
Windows Resource Protection	209
Session 0 Isolation	210
Sessions	210
Window Stations	211
Desktops	211
Why Session Isolation Is Needed	211
How Session 0 Isolation Works	212
Reducing the Footprint	213
No Longer Installed by Default	214
Gone Altogether	214
Added Instead	215
It Should Have Been Gone	215
Restart Manager	216
ActiveX Installer Service	218
Antivirus	220
Desktop Optimization Pack	221
Summary	222
Best Practices	222

Chapter 7	Vista Client Protection	225
	Popularity of Client-Side Attacks	225
	Malicious Software Removal Tool	226
	Security Center	230
	Windows Defender	231
	Windows Live OneCare	238
	Microsoft Forefront Client Security	239
	Should Microsoft Be in the Anti-Malware Business?	239
	Summary	241
	Best Practices	241
Part III	Securing Internet and E-mail Access	243
Chapter 8	Securing Internet Explorer	245
	Should You Use Another Browser?	245
	New IE 7.0 Security Features	248
	Protected Mode	248
	New Low Integrity Folders and Registry Keys	250
	IE Compatibility Shims	251
	Protected Mode's Impact on Malware and Hackers	253
	Anti-Phishing Filter	254
	Add-on Management	256
	Improved ActiveX Control Handling	257
	Improved Digital Certificate Handling and Encryption	257
	Improved URL Handling Protections	258
	CardSpace	259
	Internet Explorer Security Settings	260
	Security Zones	260
	Local Computer Zone	260
	Internet Site Zone	261
	Local Intranet Zone	262
	Trusted Sites Zone	263
	Restricted Sites Zone	263
	Zone Security Settings	264
	.NET Framework — Loose XAML	264
	.NET Framework — XAML Browser Applications	264
	.NET Framework — XPS Documents	264
	.NET Framework-Reliant Components — Run	
	Components Not Signed with Authenticode	265
	.NET Framework-Reliant Components — Run	
	Components Signed with Authenticode	265
	ActiveX Controls and Plug-Ins — Allow Previously	
	Unused ActiveX Controls to Run Without Prompting	265
	ActiveX Controls and Plug-Ins — Allow Scriptlets	266
	ActiveX Controls and Plug-Ins — Automatic Prompting	
	for ActiveX Controls	266
	ActiveX Controls and Plug-Ins — Binary and	
	Script Behaviors	266

xviii Contents

ActiveX Controls and Plug-Ins — Display Video and Animation on a Web Page That Does Not Use External Media Player	267
ActiveX Controls and Plug-Ins — Download Signed ActiveX Controls	267
ActiveX Controls and Plug-Ins — Download Unsigned ActiveX Controls	267
ActiveX Controls and Plug-Ins — Initialize and Script ActiveX Controls Not Marked as Safe for Scripting	267
ActiveX Controls and Plug-Ins — Run ActiveX Controls and Plug-Ins	268
ActiveX Controls and Plug-Ins — Script ActiveX Controls Marked Safe for Scripting	268
Downloads — Automatic Prompting for File Downloads	268
Downloads — File Download	269
Downloads — Font Download	270
Enable .Net Framework Setup	270
Java VM-Java Permissions	270
Miscellaneous — Access Data Sources Across Domains	270
Miscellaneous — Allow META REFRESH	270
Miscellaneous — Allow Scripting of Internet Explorer Web Browser Control	270
Miscellaneous — Allow Script-Initiated Windows Without Size or Position Constraints	271
Miscellaneous — Allow Web Pages to Use Restricted Protocols for Active Content	271
Miscellaneous — Allow Websites to Open Windows Without Address or Status Bars	271
Miscellaneous — Display Mixed Content	271
Miscellaneous — Don't Prompt for Client Certificate Selection When No Certificates or Only One Certificate Exists	272
Miscellaneous — Drag and Drop or Copy and Paste Files	272
Miscellaneous — Include Local Directory Path When Uploading Files to a Server	273
Miscellaneous — Installation of Desktop Items	273
Miscellaneous — Launching Applications and Unsafe Files	273
Miscellaneous — Launching Programs and Files in an Iframe	273
Miscellaneous — Navigate Sub-Frames Across Different Domains	273
Miscellaneous — Open Files Based on Content, Not File Extension	274
Miscellaneous — Software Channel Permissions	274
Miscellaneous — Submit Non-Encrypted Form Data	274

Miscellaneous — Use Phishing Filter	274
Miscellaneous — Use Pop-Up Blocker	275
Miscellaneous — Userdata Persistence	275
Miscellaneous — Web Sites in Less Privileged Web Content Zone Can Navigate into This Zone	275
Scripting — Active Scripting	275
Scripting — Allow Programmatic Clipboard Access	275
Scripting — Allow Status Bar Updates Via Script	276
Scripting — Allow Websites to Prompt for Information Using Scripted Window	276
Scripting — Scripting of Java Applets	277
User Authentication	277
IE Advanced Settings	282
Browsing — Disable Script Debugging (Internet Explorer or Other)	282
Browsing — Display a Notification About Every Script Error	282
Browsing — Enable Third-Party Extensions	282
Browsing — Use Inline Autocomplete	282
International — Send UTF-8 URLs	283
Java (or Java-Sun) — Use JRE x.x for <applet>	283
Security — Allow Active Content from CDs to Run on My Computer	283
Security — Allow Active Content to Run in Files on My Computer	283
Security — Allow Software to Run or Install Even If the Signature Is Invalid	283
Security — Check for Publisher's Certificate Revocation	283
Security — Check for Server Certificate Revocation	284
Security — Check for Signatures on Downloaded Programs	284
Security — Do Not Save Encrypted Pages to Disk	284
Security — Empty Temporary Internet Files Folder When Browser Is Closed	284
Enable Memory Protection to Help Mitigate Online Attacks	285
Security — Enable Integrated Windows Authentication	285
Security — Phishing Filter Settings	286
Security — Use SSL 2.0, SSL 3.0, TLS 1.0	286
Security — Warn About Invalid Site Certificates	287
Security — Warn If Changing Between Secure and Not Secure Mode	287
Security — Warn If Forms Submittal Is Being Redirected	287
Other Browser Recommendations	288
Don't Browse Untrusted Web Sites	288
Keep IE Patches Updated	289
Will Internet Explorer 7 Be Hacked A Lot?	289
Summary	290
Best Practices	290

xx Contents

Chapter 9	Introducing IIS 7	293
	Web Server Threats	293
	Application Vulnerabilities	294
	OS Vulnerabilities	295
	Back-End Database Issues	295
	Protocol Vulnerabilities	295
	Buffer Overflows	296
	Directory Traversal Attacks	296
	Sniffing Attacks	297
	Denial of Service	298
	Password Guessing Attacks	299
	Introduction to IIS	299
	New IIS Features	300
	Installing IIS 7	301
	IIS Components	302
	IIS Protocol Listeners	307
	HTTP.SYS	308
	Net.TCP	308
	Net.Pipe	308
	Net.P2P	308
	Net.MSMQ	309
	Worker Processes, Application Pools, and Identities	309
	Worker Processes	309
	Application Pools	309
	Application Pool Identities	311
	IUSR and IIS_USRS	314
	IIS Administration	315
	Feature Delegation	316
	IIS Authentication	318
	Anonymous Authentication	320
	ASP.NET Impersonation	320
	Basic Authentication	322
	Digest Authentication	322
	Forms Authentication	322
	Windows Authentication	322
	Client Side Mapping	323
	Web Server Access Control Permissions	326
	IIS Handler Permissions	326
	NTFS Permissions	332
	Defending IIS	332
	Step Summary	333
	Configuring Network/Perimeter Security	333
	Ensuring Physical Security	334
	Installing Updated Hardware Drivers	334
	Installing an Operating System	334

Configuring a Host Firewall	335
Configuring Remote Administration	335
Installing IIS in a Minimal Configuration	336
Installing Patches	336
Hardening the Operating System	337
Configuring and Tightening IIS	339
Installing Additional IIS Features	340
IIS 7 Modules	340
Minimizing Web Components Even Further	342
Feature Delegation	342
Strengthening NTFS Permissions	342
Configuring Request Filtering	343
Securing Web Sites	344
Hardening NTFS Permissions	344
Web Site IP Settings	346
Application Pool Changes	346
Cleaning and Testing	347
Installing and Securing Applications	347
Conducting Penetration Tests	347
Deploying to Production	347
Monitoring Log Files	348
Summary	348
Chapter 10 Protecting E-mail	351
E-mail Threats	351
Malicious File Attachments	351
File Extension Tricks	380
Embedded Content	381
Embedded Links	382
Leaked Passwords	383
Other Miscellaneous E-mail Threats	383
Introducing Windows Mail	384
Phishing Detection	385
Improved Junk Mail Detection	386
Sender White Lists and Black Lists	387
Top-Level Domain Blocking	387
Simplified E-mail Storage	390
E-mail Defenses	390
Convert All E-mail to Plain-text	391
Execute All HTML Content in the Restricted Zone	393
Disable Automatic Downloading of HTML Content	394
Filter Out Dangerous File Attachments	395
Install Anti-Malware Software	398
Disable Plain-Text Passwords	398
Summary	398
Best Practices	399

xxii Contents

Part IV	Securing Windows Networks	401
Chapter 11	Managing Windows Firewall	403
	New Features	405
	Windows Filtering Platform	405
	IPv6	406
	Integration with IPsec	407
	Stealth	408
	Boot Time Filtering	409
	Strict Source Mapping	410
	Service Hardening and the Firewall	411
	IPv6	412
	Outbound Filtering	412
	How Much Security Can Outbound Filtering Provide?	413
	Firewall Management	417
	Firewall Profiles	417
	Management Interfaces	419
	Windows Firewall Control Panel	419
	Security Center	421
	Windows Firewall with Advanced Security	422
	Group Policy Editor	422
	Netsh	423
	Application Programming Interfaces	424
	Rule Types	426
	Directional Rules	427
	Connection Security Rules	427
	When to Use Which Rules	428
	Rule Precedence	428
	Firewall Scenarios	429
	Restricting Access Based on End-Point	429
	Blocking Outbound SMB in Public Profile	436
	Allowing Management Traffic via VPN	437
	Managing Firewall in a Mixed or Down-Level Environment	438
	RPC	442
	Summary	443
	Best Practices	444
Chapter 12	Server and Domain Isolation	445
	Server and Domain Isolation Overview	445
	Domain Isolation	446
	Server Isolation	447
	Forget About the Perimeter	448
	Network Threat Modeling	450
	Changes in Windows Vista Affecting SDI	451
	AuthIP	451
	Client-to-DC IPsec	451
	Authentication with Multiple Credentials	451

Improved Negotiation Flow	452
Vastly Improved Configuration User Interface	453
Domain Isolation Rules	454
Server Isolation Rules	457
Summary	458
Best Practices	459
Chapter 13 Wireless Security	461
Wi-Fi Terminology and Technologies	461
Wi-Fi Standards	462
Infrastructure versus Ad-Hoc Mode	462
Wi-Fi Standards	463
Wi-Fi Security Standards	464
Wired Equivalent Privacy	465
Wi-Fi Protected Access/802.11i	466
Wireless Threats	471
Eavesdropping	472
Unauthorized Access	474
Bypassing of Traditional Defenses	474
Malware Injection	474
Denial of Service Attacks	475
New Wireless Improvements in Vista	476
Securing Wireless Networks	477
802.11 Legacy Wireless Security Recommendations	477
Changing Access Point's Default SSID	478
Enabling MAC Filtering	478
Disabling DHCP on the Access Point	478
Requiring User Authentication Passwords	479
Turning Off SSID Broadcasting	479
Changing an Access Point's Default Administrator Password	480
WEP	480
VPN Protocols	481
Using WPA	481
Using WPA2/802.11i	481
Summary	482
Best Practices	482
Part V Group Policy and Best Practices	483
Chapter 14 Using Group Policy	485
New Group Policy Features	486
Multiple Local Group Policies	486
Group Policy Precedence	489
Using MLGPOs in a Domain Environment	491
Difference between Local GPOs and Domain GPOs	491

xxiv Contents

New Administrative Template Format	492
Template Embedding	493
Migrating to ADMX	493
Client-Side Pulling and Network Location Awareness	493
Updated Group Policy Features	494
Group Policy Management Console v. 2.0	494
Internet Explorer Management Without IEAK	495
Group Policy Application Factored from Winlogon	496
Group Policy Logging Moved to System Event Log	497
New or Updated Group Policy Settings	498
New Security Options	498
Security Options with Modified Defaults	498
Removed Security Options	504
New Administrative Template Settings	504
Settings That Require Reboot or Logon	510
Windows Vista Security Guide	510
Do You Need the Vista Security Guide?	511
What Is Good in the Vista Security Guide	511
What Could Have Been Better in the Vista Security Guide	511
Importance of the Guide	513
Active Directory Schema Updates	514
Managing Group Policy in a Mixed Environment	514
Rollout Strategy	515
Logon Scripts Fail Because of UAC	516
Using Group Policy in a NAP Environment	516
Summary	517
Best Practices	518
Chapter 15 Thinking about Security	519
It Still Comes Down to Risk Management	520
Jesper's Position	520
Roger's Position	520
Enterprise Risk Management.	521
The Three-Step Approach to Security	523
Keep 'em Off the Box	524
Keep 'em from Running	524
Keep 'em from Communicating	525
Thinking Differently about Security	526
The Top 2 (+ or - 1, or so) Client Security Hacks	526
Jesper's Thoughts	526
Roger's Thoughts	528
Anti-Malware Is Not a Panacea	530
Jesper's Thoughts	530
Roger's Thoughts	532

Tweaking It	532
Security Tweaks You Should Make	533
Turn on DEP for Internet Explorer	536
Security Tweaks You Shouldn't Make	536
Agreeing to Disagree	539
Jesper's Position	541
Roger's Position	545
Wetware	546
Summary	547
Best Practices	547
Appendix A Building a Windows PE Boot Disk	549
Building a WinPE Bootable USB Flash Drive	549
Downloading WAIK	550
Building the WinPE Image	550
Appendix B References	555
Index	561