

# Contents

<b>Acknowledgments</b>	<b>vi</b>
<b>Introduction</b>	<b>xix</b>
<b>Part I: The Basics in Depth</b>	<b>1</b>
<b>Chapter 1: Windows Attacks</b>	<b>3</b>
<b>Attack Classes</b>	<b>3</b>
Automated versus Dedicated Attacker	4
Remote versus Local	7
<b>Types of Attacks</b>	<b>8</b>
Dedicated Manual Attacker Methodology	8
Automated Malware	11
Remote	14
Other Types of Attacks	17
Malware Trends	19
<b>Where Malware Hides</b>	<b>20</b>
<b>Summary</b>	<b>49</b>
<b>Chapter 2: Conventional and Unconventional Defenses</b>	<b>51</b>
<b>Overall Defense Strategy</b>	<b>51</b>
We Will Never Defeat Hackers and Malware	52
Whatever Is Popular Gets Hacked	52
There Is No Perfect Security Solution	53
Focus on the Right Problem of Automated Malware, Not Hackers	53
If a User Can Be Tricked into Running a Malicious Program, It Is Game Over	54
Security-by-Obscurity Works!	54
Don't Let End Users Make Security Decisions	54
Assume Firewalls and Antivirus Software Will Fail	55
Protection Should Be Host-Based	55
Practice Defense-in-Depth	56
Prevent Malware from Hiding Where It Likes to Hide	57
Minimize Potential Attack Vectors, Decrease Attack Space	57
Security Must Be Automated	58
<b>Conventional Defenses</b>	<b>58</b>
Don't Give Users Admin Access	58
Keep Patches Updated	63

# Contents

---

Use a Host-Based Firewall	65
Use Antivirus Software	68
Use Anti-Spam Software	69
Use Anti-Spyware Software	70
Physical Security	70
Harden the TCP/IP Stack	71
<b>Unconventional Defenses</b>	<b>73</b>
Rename Admin and Highly Privileged Accounts	73
Run Services on Non-Default Ports!	75
Install High-Risk Software (i.e., IIS) to Non-Default Folders	76
<b>Summary</b>	<b>77</b>
<b>Chapter 3: NTFS Permissions 101</b>	<b>79</b>
<b>Common Misconceptions</b>	<b>79</b>
<b>How Windows Security Works</b>	<b>80</b>
Access Control Phases	80
GUIDs and SIDs	82
Delegation and Impersonation	90
Groups	95
Computer Accounts	115
Windows Trusts	116
Security Token	117
<b>Share and NTFS Permissions</b>	<b>119</b>
Share Permissions	119
NTFS Permissions	122
Interesting Permission Interactions	127
<b>Current Permission Settings</b>	<b>132</b>
Interesting Points About Information in Tables 3-8 through 3-10	134
<b>Other Best Practice Recommendations</b>	<b>135</b>
Give Security to Groups, Not Users	135
Don't Overuse Everyone Full Control	136
Set Security Using Special Permissions	136
<b>Summary</b>	<b>136</b>
<b>Part II: OS Hardening</b>	<b>139</b>
<b>Chapter 4: Preventing Password Crackers</b>	<b>141</b>
<b>Windows Password Authentication</b>	<b>141</b>
Unicode Passwords	142
Password Complexity	144
Are Complex Passwords Complex?	145
Using a Strong Password	146

---

Windows Password Hashes	146
Windows Authentication	152
Logon Process	159
<b>Passwords Attacks, Tools, and Techniques</b>	<b>160</b>
Password Resetting	160
Password Guessing	163
Password Capturing	165
Password Cracking	166
Guessing and Cracking Methods	171
<b>Other Types of Password Attacks</b>	<b>175</b>
Cached Credentials	176
Computer Accounts	177
Credential Manager	179
RDP Connection Objects	181
Other Common Windows Authentication Mechanisms	182
Island Hopping	183
<b>Defending Against Password Attacks</b>	<b>183</b>
Disable LM Password Hashes	183
Require Long, Complex Passwords	184
Disable LM and NTLM Authentication	184
Enable Account Lockouts	185
Force Moderately Frequent Password Changes	186
Rename Highly Privileged Accounts	186
Give Additional Protections to Highly Privileged Accounts	186
Enable Logon Screen Warning Messages	187
Audit Passwords on a Regular Basis	187
Consider Using Random Password Generators	187
Don't Use a Password	187
<b>Summary</b>	<b>188</b>
<b>Chapter 5: Protecting High-Risk Files</b>	<b>189</b>
<b>What Is a High-Risk File?</b>	<b>189</b>
File Flaws	191
<b>High-Risk File and Program Examples</b>	<b>193</b>
List of Potentially Malicious File Types	193
<b>High-Risk Windows Files</b>	<b>204</b>
Other Windows Files Needing Protection	209
Malicious File Tricks	211
Dangerous Unused Applications	217
Buffer Overflows	217
<b>File Defenses</b>	<b>218</b>
Uninstall, Remove, Delete, and Rename	218
Use NTFS Permissions	218

# Contents

---

Software Restriction Policies	221
Enable Auditing	224
Keep Patches Updated	225
Other Defenses	225
<b>Summary</b>	<b>225</b>
<b>Chapter 6: Protecting High-Risk Registry Entries</b>	<b>227</b>
<b>Registry Introduction</b>	<b>227</b>
Registry Structure	228
Alternate Registry Storage Locations	237
Registry Tools	238
Registry Permissions	241
<b>High-Risk Registry Entries</b>	<b>243</b>
What Is a High-Risk Registry Entry?	243
<b>Defenses</b>	<b>246</b>
Don't Let Non-Admin Users Be Logged On As Administrators	246
Harden HKCU Registry Permissions	247
Block High-Risk File Associations	247
Block High-Risk URI Handlers	249
Remove High-Risk NeverShowExt Values	250
Block File Association Changes	250
Use Group Policy or Security Templates to Automate Registry Permission Changes	251
<b>Summary</b>	<b>251</b>
<b>Chapter 7: Tightening Services</b>	<b>253</b>
<b>Why Tighten Services?</b>	<b>253</b>
Less Attack Surface	253
<b>Reduce Buffer Overflow Risks</b>	<b>254</b>
Reduce Risk of Denial-of-Service Attacks	254
Reduce Management Overhead	254
<b>Services Introduction</b>	<b>254</b>
Identifying Unknown Services	255
Service Details	256
<b>SC</b>	<b>265</b>
RPC Services	267
<b>Common Windows Services and Recommendations</b>	<b>267</b>
Nondefault Windows Services	283
Differences between Windows Platforms	287
<b>Securing Services</b>	<b>288</b>
High-Security Minimal Services	288
Normal Security Environments	288

---

How to Tighten Remaining Services	290
<b>Summary</b>	<b>294</b>
<b>Chapter 8: Using IPSec</b>	<b>295</b>
<b>Introduction to IPSec</b>	<b>295</b>
An Open Standard	296
IPSec Basics	296
Tunnel versus Transport Mode	297
IPSec Security Protocols — AH versus ESP	298
Security Associations	300
Key Management	300
IKE Modes — Main, Aggressive, and Quick	300
NAT versus NAT-T	301
Performance Issues	301
<b>Windows IPSec</b>	<b>302</b>
IPSec Console	302
IPSec at the Command Line	302
IPSec Monitor Tools	303
Default IPSec Policies	305
Setting Up Windows IPSec	306
Creating an IPSec Policy	306
IPSec Exemptions	315
Firewall Ports Needed	318
<b>Using IPSec Security</b>	<b>319</b>
Setup Planning	319
When to Use IPSec	319
<b>IPSec Attacks and Defenses</b>	<b>321</b>
Bypassing Firewall Defenses	321
Trusted Man-in-the-Middle Attack	322
Denial-of-Service Attacks	322
<b>Other IPSec Links</b>	<b>322</b>
<b>Summary</b>	<b>322</b>
<b>Part III: Application Security</b>	<b>323</b>
<b>Chapter 9: Stopping Unauthorized Execution</b>	<b>325</b>
<b>Deny-by-Default Software Execution</b>	<b>325</b>
Scope of Deny-by-Default Software Execution	325
Benefits of Preventing Unauthorized Software Execution	326
Disadvantages of Preventing Unauthorized Software Execution	327
<b>Developing a Software Restriction Policy</b>	<b>327</b>

# Contents

---

<b>Methods to Prevent Unauthorized Execution</b>	<b>329</b>
Don't Let End Users Be Logged In As Admin	329
Remove or Delete Software	330
Use NTFS Permissions	330
Unregister DLLs	332
Use the Kill Bit	335
Software Restriction Policies	336
<b>Summary</b>	<b>346</b>
<b>Chapter 10: Securing Internet Explorer</b>	<b>347</b>
<b>Internet Explorer</b>	<b>347</b>
IE Features	347
IE Competitors	350
IE Security Statistics	351
How IE Works	352
<b>Internet Explorer Attacks</b>	<b>354</b>
URL Spoofing	354
Buffer Overflow	357
Cross-Site Scripting	357
Zone Manipulation	358
File Execution	361
Directory Traversal	362
Malicious Content	363
Cookie Manipulation	363
Browser Interface Manipulation	364
Plug-In Exploits	364
Browser Tests	365
<b>Internet Explorer Defenses</b>	<b>366</b>
Don't Browse Untrusted Web Sites	366
Don't Let Non-Admin Users Be Logged in as Administrators	366
Use IE 6 XP SP2 or IE 7	366
Keep IE Patches Updated	367
Customize Default Internet Explorer Security Zones	367
Advanced Settings	378
IE Enhanced Security Configuration	385
Third-Party Tools	387
<b>Summary</b>	<b>387</b>

---

<b>Chapter 11: Protecting E-mail</b>	<b>389</b>
<b>E-mail Threats</b>	<b>389</b>
Main E-mail Problems	389
Malicious File Attachments	391
Devious Embedded Links	392
Cross-Site Scripting	393
Spam	393
Phishing	396
Unauthorized Reading of E-mail	397
<b>Securing E-mail</b>	<b>398</b>
Block Malicious File Attachments	398
Disable HTML Content	401
Securely Configure E-mail Client	403
Turn Off Reading/AutoPreview Pane	404
Consider Blocking Unauthorized E-mail	405
Authenticating E-mail Links	405
Antivirus Scanning	406
Block Spam	407
Authenticate It	417
Secure DNS	418
End-User Training	418
<b>Summary</b>	<b>418</b>
<b>Chapter 12: IIS Security</b>	<b>419</b>
<b>IIS Basics</b>	<b>420</b>
Http.sys	421
Worker Processes, Application Pools, and Identities	422
IUSR and IWAM	425
IIS Administration	427
IIS Authentication	428
Permissions	433
Web Service Extensions	436
<b>Step Summary</b>	<b>437</b>
<b>Securing IIS</b>	<b>437</b>
Configure Network/Perimeter Security	437
Ensure Physical Security	438
Install Updated Hardware Drivers	438

# Contents

---

Install the Operating System	438
Configure the Host Firewall	439
Configure Remote Administration	439
Install IIS In Minimal Configuration	440
Install Patches	440
Harden the Operating System	441
Configure and Tighten IIS	443
Secure Web Site(s)	452
Configure Logging	455
Clean and Test	455
Install and Tighten Applications	456
Conduct Penetration Tests	456
Deploy to Production	456
Monitor Log Files	456
More Resources	456
<b>Summary</b>	<b>457</b>
<b>Chapter 13: Using Encrypting File System</b>	<b>459</b>
<b>How EFS Works</b>	<b>459</b>
Encrypting a File	459
Alternative EFS Methods	461
Decrypting Files	461
File Security and EFS	462
EFS Certificate	462
File Encryption Key	464
DDF and DRF	465
New EFS Options in XP and XP SP2	465
Using EFS on Servers	469
Setting Up an EFS Recovery Policy	471
<b>Setting Up EFS</b>	<b>476</b>
<b>EFS Caveats</b>	<b>477</b>
<b>EFS Best Practices</b>	<b>477</b>
<b>Other Links</b>	<b>478</b>
<b>Summary</b>	<b>478</b>
<b>Part IV: Automating Security</b>	<b>479</b>
<b>Chapter 14: Group Policy Explained</b>	<b>481</b>
<b>How Group Policy Works</b>	<b>481</b>
Accessing Group Policy	482
GPO Internals	485

---

<b>Group Policy Settings</b>	<b>487</b>
General Observations	487
Main Setting Categories	487
Software Settings	488
GPO Windows Settings	490
Administrative Templates	515
GPO Notes/Recommendations	517
<b>Summary</b>	<b>518</b>
<b>Chapter 15: Designing a Secure Active Directory Infrastructure</b>	<b>519</b>
<b>Active Directory Introduction</b>	<b>519</b>
Top Active Directory Containers	521
LDAP	525
<b>Parts of Active Directory Security Policies</b>	<b>525</b>
History of Group Policy	525
Security Templates	527
Local Computer Policy	528
Group Policy Objects	528
<b>Efficient Active Directory Security Design</b>	<b>536</b>
Use Role-Based Security	537
Create a Role-Based OU Structure	537
Create and Use a One-Time Security Template on All Computers	538
Create and Use a Local Computer Policy	539
Create and Use a Baseline Security Policy for the Domain	539
Create and Use a Role-Based Incremental Security Policy	539
Name GPOs with Version Numbers	539
Design Summary	540
<b>Summary</b>	<b>542</b>
<b>Book Summary</b>	<b>542</b>
<b>Index</b>	<b>543</b>

