

# Inhaltsverzeichnis

<b>Vorwort</b>	<b>13</b>
<b>Danksagungen</b>	<b>15</b>
<b>Einleitung</b>	<b>17</b>
<b>Teil I Ein Überblick über das Windows-Betriebssystem</b>	
<b>1 PowerShell-Testumgebung einrichten</b>	<b>27</b>
1.1 PowerShell-Version auswählen.....	27
1.2 PowerShell konfigurieren .....	27
1.3 Ein Überblick über die PowerShell-Sprache .....	29
1.4 Zusammenfassung .....	46
<b>2 Der Windows-Kernel</b>	<b>47</b>
2.1 Die Windows Kernel Executive .....	47
2.2 Der Sicherheitsreferenzmonitor .....	48
2.3 Der Objekt-Manager .....	51
2.4 Der Eingabe/Ausgabe-Manager .....	71
2.5 Der Prozess- und Thread-Manager.....	73
2.6 Der Speichermanager .....	74
2.7 Codeintegrität .....	80
2.8 Erweiterter lokaler Prozeduraufruf.....	81
2.9 Der Konfigurationsmanager.....	82
2.10 Beispillösungen.....	83
2.11 Zusammenfassung .....	88

<b>3</b>	<b>Anwendungen im Benutzermodus</b>	<b>91</b>
3.1	Win32 und die Windows-APIs im Benutzermodus .....	91
3.2	Die Win32-GUI .....	98
3.3	Win32-APIs und Systemaufrufe vergleichen .....	106
3.4	Win32-Registrierungspfade .....	109
3.5	DOS-Gerätepfade .....	112
3.6	Prozesse erstellen .....	118
3.7	Systemprozesse .....	122
3.8	Beispillösungen .....	125
3.9	Zusammenfassung .....	127
 <b>Teil II Der Sicherheitsreferenzmonitor</b>		
<b>4</b>	<b>Zugriffstoken</b>	<b>131</b>
4.1	Primäre Token .....	131
4.2	Identitätswechseltoken .....	136
4.3	Typ des Tokens konvertieren .....	140
4.4	Pseudo-Token-Handle .....	141
4.5	Token-Gruppen .....	143
4.6	Privilegien .....	147
4.7	Sandbox-Token .....	151
4.8	Was zeichnet einen Administrator-Benutzer aus? .....	157
4.9	Benutzerkontensteuerung .....	159
4.10	Sicherheitsattribute .....	166
4.11	Token erstellen .....	167
4.12	Token zuweisen .....	169
4.13	Beispillösungen .....	175
4.14	Zusammenfassung .....	178
<b>5</b>	<b>Sicherheitsdeskriptoren</b>	<b>179</b>
5.1	Der Aufbau eines Sicherheitsdeskriptors .....	179
5.2	Die Struktur einer Sicherheitskennung (SID) .....	182
5.3	Absolute und relative Sicherheitsdeskriptoren .....	185
5.4	Header und Einträge in Zugriffssteuerungslisten .....	188
5.5	Sicherheitsdeskriptoren erstellen und verändern .....	193
5.6	Die Security Descriptor Definition Language .....	202
5.7	Beispillösungen .....	211
5.8	Zusammenfassung .....	214

<b>6</b>	<b>Sicherheitsdeskriptoren lesen und zuweisen</b>	<b>217</b>
6.1	Sicherheitsdeskriptoren lesen .....	217
6.2	Sicherheitsdeskriptoren zuweisen .....	219
6.3	Win32-Sicherheits-APIs .....	251
6.4	Server-Sicherheitsdeskriptoren und zusammengesetzte Zugriffssteuerungseinträge .....	257
6.5	Zusammenfassung des Vererbungsverhaltens .....	259
6.6	Beispillösungen .....	260
6.7	Zusammenfassung .....	264
<b>7</b>	<b>Der Prozess der Zugriffsprüfung</b>	<b>265</b>
7.1	Zugriffsprüfung durchführen .....	265
7.2	Der Zugriffsprüfungsprozess in PowerShell .....	271
7.3	Sandboxing .....	290
7.4	Zugriffsprüfungen in Unternehmen .....	296
7.5	Beispillösungen .....	309
7.6	Zusammenfassung .....	312
<b>8</b>	<b>Weitere Anwendungsfälle für die Zugriffsprüfung</b>	<b>313</b>
8.1	Traversal-Prüfung .....	313
8.2	Zugriffsprüfung bei Handle-Duplikaten .....	318
8.3	Zugriffsprüfung für Sandbox-Token .....	321
8.4	Zugriffsprüfungen automatisieren .....	324
8.5	Beispillösungen .....	327
8.6	Zusammenfassung .....	329
<b>9</b>	<b>Sicherheitsüberwachung</b>	<b>331</b>
9.1	Das Sicherheitsprotokoll .....	331
9.2	Sicherheit und Überwachungsrichtlinien .....	336
9.3	Beispillösungen .....	344
9.4	Zusammenfassung .....	346

## Teil III Die lokale Sicherheitsautorität und die Authentifizierung

<b>10</b>	<b>Windows-Authentifizierung</b>	<b>349</b>
10.1	Domänenauthentifizierung .....	350
10.2	Lokale Domänenkonfiguration .....	355
10.3	LSA-Remotedienste .....	362
10.4	Die Datenbanken SAM und SECURITY .....	378

10.5	Beispiellösungen . . . . .	391
10.6	Zusammenfassung. . . . .	395
<b>11</b>	<b>Active Directory</b>	<b>397</b>
11.1	Der Werdegang von Active Directory . . . . .	397
11.2	Eine Active-Directory-Domäne mit PowerShell untersuchen .	398
11.3	Objekte und definierte Namen . . . . .	405
11.4	Das Schema. . . . .	410
11.5	Sicherheitsdeskriptoren . . . . .	415
11.6	Zugriffsprüfungen. . . . .	424
11.7	Ansprüche und zentrale Zugriffsrichtlinien . . . . .	442
11.8	Gruppenrichtlinien . . . . .	444
11.9	Beispiellösung . . . . .	447
11.10	Zusammenfassung. . . . .	456
<b>12</b>	<b>Interaktive Authentifizierung</b>	<b>459</b>
12.1	Desktop eines Benutzers erstellen . . . . .	459
12.2	Die LsaLogonUser-API . . . . .	461
12.3	Die API LsaLogonUser von PowerShell aus verwenden . . .	473
12.4	Einen neuen Prozess mit einem Token erstellen . . . . .	475
12.5	Der Anmeldetyp Service . . . . .	477
12.6	Beispiellösungen . . . . .	478
12.7	Zusammenfassung. . . . .	483
<b>13</b>	<b>Netzwerkauthentifizierung</b>	<b>485</b>
13.1	NTLM-Netzwerkauthentifizierung . . . . .	486
13.2	Der NTLM-Relay-Angriff . . . . .	503
13.3	Beispiellösung . . . . .	511
13.4	Zusammenfassung. . . . .	521
<b>14</b>	<b>Kerberos</b>	<b>523</b>
14.1	Interaktive Authentifizierung mit Kerberos . . . . .	523
14.2	Kerberos-Authentifizierung mit PowerShell durchführen. . .	532
14.3	Die AP-REQ-Nachricht entschlüsseln . . . . .	536
14.4	Die AP-REP-Nachricht entschlüsseln. . . . .	544
14.5	Domänenübergreifende Authentifizierung. . . . .	546
14.6	Kerberos-Delegierung . . . . .	548
14.7	Benutzer-zu-Benutzer-Authentifizierung in Kerberos. . . .	560
14.8	Beispiellösungen . . . . .	563
14.9	Zusammenfassung. . . . .	567

<b>15</b>	<b>Negotiate-Authentifizierung und andere Sicherheitspakete</b>	<b>569</b>
15.1	Sicherheitspuffer . . . . .	569
15.2	Das Negotiate-Protokoll . . . . .	573
15.3	Weniger verbreitete Sicherheitspakete . . . . .	576
15.4	Remote Credential Guard und eingeschränkter Administratormodus . . . . .	584
15.5	Anmeldeinformationsverwaltung . . . . .	585
15.6	Weitere Attributflags für Requests . . . . .	589
15.7	Netzwerkauthentifizierung mit einem LowBox-Token . . . . .	591
15.8	Das Ereignisprotokoll der Authentifizierungsereignisse . . . . .	596
15.9	Beispielelösungen . . . . .	600
15.10	Zusammenfassung . . . . .	606
15.11	Ein paar Gedanken zum Schluss . . . . .	606

## Teil IV Anhänge

<b>A</b>	<b>Ein Windows-Domänenetzwerk für Testzwecke aufbauen</b>	<b>609</b>
A.1	Das Domänenetzwerk . . . . .	609
A.2	Windows Hyper-V installieren und konfigurieren . . . . .	610
A.3	Die virtuellen Maschinen erstellen . . . . .	611
<b>B</b>	<b>Zuordnung zwischen SID-Alias und SDDL-SID</b>	<b>621</b>
	<b>Index</b>	<b>625</b>