Obsah

Úvod 7

O autorovi 7

Předmluva autora 7

O této knize 7

Co se v knize dozvíte 8

Popis nástrojů 9

Porozumění zápisu příkazů 9

Co je Sysinternals 9

FAQ o Sysinternals 10

Volný překlad EULA 11

Sysinternals Forum 13

Balík Sysinternals 14

Systémové proměnné 15

Sysinternals Live 16

Další informace o Sysinternals 16

Využití nástrojů Sysinternals 17

Troubleshooting 17

KAPITOLA 1

Souborové a diskové nástroje 19

Contig 20

Disk Usage (DU) 23

DiskView 24

NTFSInfo 25

FindLinks 26

Junction 29

Streams 30

Sync 33

Disk2vhd 34

PageDefrag 35

MoveFile a PendMoves 37

DiskMon 38

DiskExt 39

EFSDump 41
VolumeID 42
LDMDump 43
CacheSet 45
Chkdsk 46
BCDboot 48
BCDedit 49

KAPITOLA 2
Síťové utility 51

AdExplorer 52
AdInsight 54
AdRestore 55
Nltest 56
PipeList 57
PsFile 59
TCPView 60
Netstat 62
Whois 65
Netsh 67
Ping, Tracert, PathPing 70
Route a ARP 74
Mrinfo 78
Nslookup 79

KAPITOLA 3
Procesní nástroje 83

Handle 84
ListDLLs 87
PortMon 89
ProcDump 91
Process Explorer 94
Shutdown 112
Process Monitor 115
PsGetSid 128
PsList 129
TaskList 132

PsKill 133
TaskKill 134
PsService 136
PsSuspend 138
VMMap 139
Mem 142

KAPITOLA 4
Bezpečnostní nástroje 143

AccessChk 144
AccessEnum 146
Autologon 149
Autoruns 150
Msconfig 154
LogonSessions 155
PsExec 157
PsLoggedOn 159
PsLogList 161
RootkitRevealer 165
SDelete 168
ShareEnum 169
ShellRunas 170
Runas 172
SigCheck 173
SigVerif 175
Verifier 176

KAPITOLA 5
Systémové nástroje 179

Coreinfo 180
ProcFeatures 181
PsInfo 181
RAMMap 183
WinObj 184
LoadOrder 186
ClockRes 187
LiveKd 187

Msinfo32 190
GetMac 191
IPconfig 191
Systeminfo 194

KAPITOLA 6
Ostatní nástroje 197

PsTools 198
Hex2Dec 199
Desktops 200
ZoomIt 201
Strings 202
BgInfo 204
Reg a Regedit 206
RegJump 218
RegDelNull 219
DebugView 220
Ctrl2Cap 221
BlueScreen 222
Clip 222
RecDisk 223
Mrt (Malicious Removal Tool) 223
Choice 224
Makecab 224
Cmdkey 227
Winsat 228
Wusa 230

PŘÍLOHY 231
Slovník 231
Klávesové zkratky 236
Systémové konzole 236
Ovládací panely 238
Systémové proměnné 240

REJSTŘÍK 243