

Contents

Introduction	xv
Chapter 1: Tools	1
How Do I Build a Rootkit?	1
The Microsoft Driver Development Kit	4
Microsoft Visual VC++ 2005 Express	5
Microsoft Software Developers Kit	5
Sysinternals Freeware	5
IDA	6
Debugging Tools for Windows	6
Verification	6
VCVARS32.BAT	7
Other Tools to Consider	7
What to Keep Out	7
Summary	8
Chapter 2: A Basic Rootkit	9
Ghost	9
Ghost.h	9
Ghost.c	10
configManager.h	13
configManager.c	14
Alternate Data Streams	15
fileManager.h	16
fileManager.c	17
Installing Your Rootkit	21
SCMLoader.c	22
SCMUnloader.c	25
Testing Your Rootkit	26
Summary	26
Chapter 3: Kernel Hooks	27
The System Call Table	27
Kernel Memory Protection	28

Contents

Defining a Hook Function	31
An Example	33
SOURCES	33
Ghost.c	33
hookManager.c	36
hookManager.h	37
What to Hook?	39
Csr — Client Server Run Time	39
Dbg — Debug Manager	39
Etw — Event Tracing for Windows	40
Ki — Kernel (must be called from Kernel)	40
Ldr — Loader Manager	40
Pfx — ANSI Prefix Manager	40
Rtl — Runtime Library	41
Zw — File and Registry	41
The Problem with Hooking	42
Summary	42
Chapter 4: User Hooks	43
<hr/>	
Process Injection	43
Finding a Specific Dynamic Link Library	44
Defining a Hook Function	47
The Trampoline Function	48
An Example	50
SOURCES	50
Ghost.h	50
Ghost.c	51
hookManager.h	52
hookManager.c	54
injectManager.h	63
injectManager.c	66
parse86.h	78
parse86.c	78
peFormat.h	97
Using Ghost to Block PGP Encoding	99
Summary	100
Chapter 5: I/O Processing	103
<hr/>	
Using DeviceIoControl	103
The Console Application	105
Controller.c	105

IoManager.h	106
buildController.bat	107
Handling IO within the Device Driver	107
IoManager.c	110
SOURCES	112
Injected Function Programming	114
Testing I/O Control	114
Summary	117
Chapter 6: Communications	119
<hr/>	
The Transport Driver Interface	119
Initiating the Connection	120
An Example	120
commManager.h	121
commManager.c	122
SOURCES	130
Running the Example	133
Summary	135
Chapter 7: Filter Drivers	137
<hr/>	
Inserting a Filter Driver	137
File Filtering	138
Network Filtering	139
Combined Filtering	140
An Example	141
filterManager.h	142
filterManager.c	142
Ghost.c	146
IoManager.h	150
IoManager.c	154
SOURCES	166
Summary	166
Chapter 8: Key Logging	167
<hr/>	
Processing Levels	167
IRQL = PASSIVE_LEVEL	168
IRQL = APC_LEVEL	168
IRQL = DISPATCH_LEVEL	168
IRQL = DIRQL	168

Contents

A Keyboard Filter	168
Threading and Synchronization	170
Interpreting Key Codes	170
An Example	171
SOURCES	172
Ghost.c	172
filterManager.c	173
filterManager.h	174
IoManager.c	174
keyManager.h	174
keyManager.c	176
OnKeyboardRead	184
OnReadCompletion	184
GetKey	184
InitializeLogThread	184
KeyLoggerThread	185
StartKeylogger	185
StopKeylogger	185
OnCancel	185
Testing the Example	185
Summary	186
Chapter 9: Concealment	187
<hr/>	
Registry Key Hiding	187
registryManager.h	188
registryManager.c	189
Ghost.c	198
hookManager.h	198
hookManager.c	199
Directory Hiding	203
Process Hiding	205
HideMe.c	206
Testing Concealment	211
Summary	212
Chapter 10: E-mail Filtering	215
<hr/>	
Microsoft Outlook E-mail Filtering	215
OutlookExtension.h	216
OutlookExtension.cpp	218

Installing an Outlook Client Filter	231
Testing the Outlook Client Extension	231
Lotus Notes E-mail Filtering	232
LotusExtension.h	234
LotusExtension.c	234
LotusExtension.def	240
LotusExtension.mak	240
readme.txt	241
Installing a Lotus Notes Client Filter	241
Testing the Lotus Notes Client Extension	242
Summary	242
Chapter 11: Installation Considerations	243
<hr/>	
Intended Installation	243
Intended Installation Software	244
End User License Agreements (EULAs)	244
Unintended Installation	245
Privilege Escalation	245
Persistence	245
ZwSetSystemInformation with SystemLoadAndCallImage	246
Registry Possibilities	247
Initialization Files	248
Installing onto Machines That Visit Your Website	249
Removing the Traces of an Installation	251
Testing Your Installation Techniques	254
Summary	254
Chapter 12: Ghost Tracker	255
<hr/>	
The Controller	255
The Connection	257
Tamper Detection	257
An Example	258
GhostTracker.cs	260
ControlForm.cs	262
TargetController.cs	268
Listen.cs	270
GhostTracker	273
ControlForm	273
Summary	274

Chapter 13: Detecting Rootkits	275
Detection Methods	275
Detection Software	279
Strider GhostBuster	280
RootkitRevealer	280
F-Secure Blacklight	281
RootKit Hook Analyzer	282
IceSword	283
Sophos Anti-Rootkit	286
What to Do with a Detected Rootkit	287
Safe Mode	289
Summary	290
Chapter 14: Preventing Rootkits	291
Operating System Updates	292
Automatic Updates	292
Personal Firewalls	293
Free Personal Firewalls	294
Tiny Personal Firewall	294
Zone Alarm Firewall	294
Sygate Personal Firewall	294
Other Personal Firewalls	294
Kerio Personal Firewall	294
Symantec/Norton Firewall	295
Zone Alarm Professional Firewall	295
Host-based Intrusion Prevention Systems	295
Hardening	295
Virtualizing	297
Blocking Unexpected Operations	298
Rootkit Prevention Techniques	298
Kernel Hook Prevention	298
Service Load Prevention	298
Driver Load Prevention	298
Code in Data Segment Prevention	299
Stack Execution Prevention	299
Summary	299
Appendix A: Freeware	301
Index	317