

Honeypots for Windows

ROGER A. GRIMES

Apress®

Honeypots for Windows

Copyright © 2005 by Roger A. Grimes

All rights reserved. No part of this work may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage or retrieval system, without the prior written permission of the copyright owner and the publisher.

ISBN (pbk): 1-59059-335-9

Printed and bound in the United States of America 9 8 7 6 5 4 3 2 1

Trademarked names may appear in this book. Rather than use a trademark symbol with every occurrence of a trademarked name, we use the names only in an editorial fashion and to the benefit of the trademark owner, with no intention of infringement of the trademark.

Lead Editor: Jim Sumser

Technical Reviewers: Alexzander Nepomnjashiy, Jacco Tunnissen

Editorial Board: Steve Anglin, Dan Appleman, Ewan Buckingham, Gary Cornell, Tony Davis, Jason Gilmore, Chris Mills, Dominic Shakeshaft, Jim Sumser

Assistant Publisher: Grace Wong

Project Manager: Sofia Marchant

Copy Manager: Nicole LeClerc

Copy Editor: Marilyn Smith

Production Manager: Kari Brooks-Copony

Production Editor: Kelly Winquist

Compositors: Kinetic Publishing Services, LLC; Dina Quan

Proofreader: Katie Stence

Indexer: Carol Burbo

Artist: Kinetic Publishing Services, LLC; Dina Quan

Cover Designer: Kurt Krames

Manufacturing Manager: Tom Debolski

Distributed to the book trade in the United States by Springer-Verlag New York, Inc., 233 Spring Street, 6th Floor, New York, NY 10013, and outside the United States by Springer-Verlag GmbH & Co. KG, Tiergartenstr. 17, 69112 Heidelberg, Germany.

In the United States: phone 1-800-SPRINGER, fax 201-348-4505, e-mail orders@springer-ny.com, or visit <http://www.springer-ny.com>. Outside the United States: fax +49 6221 345229, e-mail orders@springer.de, or visit <http://www.springer.de>.

For information on translations, please contact Apress directly at 2560 Ninth Street, Suite 219, Berkeley, CA 94710. Phone 510-549-5930, fax 510-549-5939, e-mail info@apress.com, or visit <http://www.apress.com>.

The information in this book is distributed on an "as is" basis, without warranty. Although every precaution has been taken in the preparation of this work, neither the author(s) nor Apress shall have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused directly or indirectly by the information contained in this work.

The source code for this book is available to readers at <http://www.apress.com> in the Downloads section. You will need to answer questions pertaining to this book in order to successfully download the code.

To those who fight the good fight with constant vigilance.

Contents at a Glance

About the Author	xv
About the Technical Reviewers	xvii
Acknowledgments	xix
Introduction	xxi

PART 1 ■ ■ ■ Honeypots in General

Chapter 1	An Introduction to Honeypots	3
Chapter 2	A Honeypot Deployment Plan	35

PART 2 ■ ■ ■ Windows Honeypots

Chapter 3	Windows Honeypot Modeling	63
Chapter 4	Windows Honeypot Deployment	89
Chapter 5	Honeyd Installation	121
Chapter 6	Honeyd Configuration	151
Chapter 7	Honeyd Service Scripts	167
Chapter 8	Other Windows-Based Honeypots	189

PART 3 ■ ■ ■ Honeypot Operations

Chapter 9	Network Traffic Analysis	223
Chapter 10	Honeypot Monitoring	269
Chapter 11	Honeypot Data Analysis	301
Chapter 12	Malware Code Analysis	337

INDEX	363
--------------------	------------

Contents

About the Author	xv
About the Technical Reviewers	xvii
Acknowledgments	xix
Introduction	xxi

PART 1 ■ ■ ■ Honeypots in General

■ CHAPTER 1	An Introduction to Honeypots	3
	What Is a Honeypot?	3
	What Is a HoneyNet?	5
	Why Use a Honeypot?	5
	Low False-Positives	5
	Early Detection	7
	New Threat Detection	7
	Know Your Enemy	8
	Defense in Depth	8
	Hacking Prevention	8
	Internet Simulation Environment	10
	Basic Honeypot Components	11
	Honeypot Types	13
	Honeypot Layers	13
	Honeypot Interaction Levels	14
	Real Operating System Honeypot	15
	Virtual Honeypots	16
	Summary of Honeypot Types	20
	History of Honeypots	20
	GenI Honeypots	21
	The GenII Model	24
	Future Generations	26

Attack Models	26
Manual Attacks	26
Automated Attack Programs	30
Blended Attacks	31
Summary of Attack Models	32
Risks of Using Honeyspots	32
Summary	34

CHAPTER 2 A Honeypot Deployment Plan 35

Honeypot Deployment Steps	35
Honeypot Design Tenets	36
Attracting Hackers	37
Defining Goals	37
Production or Research?	37
Real or Virtual?	39
Hardening a Virtual Honeypot Host	40
Honeypot System Network Devices	41
Hub	41
Bridge	46
Switch	46
Router	47
Firewall	51
Honeywall	51
Honeypot Network Devices Summary	52
Honeypot System Placement	54
External Placement	55
Internal Placement	56
DMZ Placement	57
Honeypot Placement Summary	58
Summary	59

PART 2 ■ ■ ■ Windows Honeybots

CHAPTER 3 Windows Honeybot Modeling 63

What You Need to Know	63
Common Ports and Services	65

Computer Roles	68
Generic Windows Server	68
IIS Server	69
Windows 2000 Domain Controller	69
Windows Workstation	70
SQL Server	70
Exchange Server	71
Services in More Detail	72
RPC	72
NetBIOS	73
RDP	78
Simple TCP/IP Services	78
FTP	79
Telnet Server	80
IIS	80
Exchange Server	83
Common Ports by Platform	83
Common Windows Applications	86
Putting It All Together	87
Summary	88
CHAPTER 4 Windows Honeypot Deployment	89
Decisions to Make	89
Do You Really Need a High-Interaction Honeypot?	90
Real Operating System or Virtual Machine?	90
Which Microsoft Operating System to Choose?	90
Client or Server?	93
Patched or Unpatched?	93
What Support Tools Are Available?	93
Which Services and Applications to Install?	94
SAM or Active Directory?	94
Hacker's Choice?	94
What Hardware Is Required?	95
Installation Guidance	96
Installation Steps	97
Honeypot Installation Tips	99

Hardening Microsoft Windows	100
Physically Securing the Honeypot	100
Installing Necessary Patches	101
Rejecting Defaults	103
Hardening the TCP/IP Stack	104
Removing or Securing Network Shares	104
Filtering Network Traffic	105
Restricting Unauthorized Software Execution	106
Protecting User Accounts	117
Securing Authentication Protocols	118
Automating Security	119
Summary	120
CHAPTER 5 Honeyd Installation	121
What Is Honeyd?	121
Why Use Honeyd?	122
Honeyd Features	123
IP Stack Emulation	123
TCP/IP Port Emulation	131
Honeyd Logging	134
Honeyd Installation	136
Deciding Logistics	137
Hardening the Host	139
Installing WinPcap	140
Installing Cygwin	142
Installing Honeyd	145
Downloading Scripts	146
Installing Snort	146
Installing Ethereal	147
Reviewing the Honeyd Directory Structure	148
Summary	149
CHAPTER 6 Honeyd Configuration	151
Using Honeyd Command-Line Options	151
Creating a Honeyd Runtime Batch File	152
Setting Up Honeyd Configuration Files	154
Configuring Honeyd Templates	154
Assembling Templates in a Honeyd Configuration File	161

Testing Your Honeyd Configuration	165
Summary	166
CHAPTER 7 Honeyd Service Scripts	167
Honeyd Script Basics	167
Common Script Languages	168
Script Input/Output Routines	170
Honeyd Variables	171
Honeyd Configuration File Syntax	171
Default Honeyd Scripts	172
SSH Test Script	172
Cisco Telnet Session Script	173
IIS Web Emulation	176
Downloadable Scripts	178
Custom Scripts	180
A Worm Catcher Script	180
An Offensive Response Script	181
Microsoft FTP Server	183
Summary	188
CHAPTER 8 Other Windows-Based Honeypots	189
Back Officer Friendly	189
LaBrea	190
Installing and Running LaBrea	191
Using LaBrea	191
SPECTER	192
Setting Up SPECTER	193
Logging and Alerting with SPECTER	194
KFSensor	196
Installing and Running KFSensor	197
Emulating Services with KFSensor	198
Logging and Alerting with KFSensor	208
Configuring KFSensor Listeners and Anti-DoS Settings	210
PatriotBox	212
Emulating Services with PatriotBox	212
Creating Custom PatriotBox Port Listeners	214
Logging and Alerting with PatriotBox	214

Jackpot SMTP Tarpit	214
Installing Jackpot	216
Configuring Jackpot	216
Running Jackpot	218
More Honeypots	219
Summary	219

PART 3 ■ ■ ■ Honeypot Operations

■ CHAPTER 9 Network Traffic Analysis	223
Why Use a Sniffer and an IDS?	223
Sniffer Benefits	223
IDS Benefits	225
How a Sniffer and IDS Complement Each Other	226
Where to Place the Sniffer and IDS	226
Network Protocol Basics	227
The OSI Model	227
TCP/IP Suite Basics	230
Windows Protocols	237
Network Protocol Capturing Basics	239
Ethereal	240
Viewing Packet Information	241
Using Ethereal Features	244
Using Tcpdump or WinDump with Ethereal	249
Using Built-in Ethereal Command-Line Tools	249
Snort	250
Understanding How Snort Works	250
Installing Snort	252
Configuring Snort	252
Using Snort Click-and-Point	268
Summary	268
■ CHAPTER 10 Honeypot Monitoring	269
Taking Baselines	269
Host Baselines	272
Network Baselines	275

- Monitoring 276
 - In-Band vs. Out-of-Band Monitoring 276
 - Monitoring Programs 277
 - Protection for Monitoring Communications 284
- Logging 284
 - Time Synchronization 285
 - Logging of Security Events 285
 - Centralized Data Collection 287
 - Log File Formats 290
 - Data Filtering 291
 - Data Correlation 293
 - A Honeynet Security Console 294
 - Useful Information Extraction 294
 - Log Protection 295
- Alerting 295
 - Alert Considerations 295
 - Alerting Programs 296
- Summary 300

CHAPTER 11 Honeypot Data Analysis 301

- Why Analyze? 301
- Honeypot Analysis Investigations 302
 - Automated vs. Manual 302
 - Initial Compromise 303
 - After the Initial Compromise 303
- A Structured Forensic Analysis Approach 304
 - Taking the Honeypot Offline 305
 - Recovering RAM Data 305
 - Making Copies of the Hard Drive 306
 - Analyzing Network Traffic 309
 - Analyzing the File System 311
 - Analyzing Malicious Code 317
 - Analyzing the Operating System 318
 - Analyzing Logs 319
 - Drawing Conclusions 324
 - Modifying and Redeploying the Honeypot System 324
- Forensic Analysis in Action 325
 - A KFSensor Honeypot 325
 - The WhiteDoe Real Honeypot 332

Forensic Tool Web Sites	335
Summary	336
CHAPTER 12 Malware Code Analysis	337
An Overview of Code Disassembly	337
Assembly Language	339
Programming Interfaces	340
Assembly Language Instructions on Computer Platforms	345
Assembler and Disassembler Programs	349
Assemblers	350
Disassemblers	353
Text Editors	357
Malicious Programming Techniques	358
Stealth Mechanisms	358
Encryption	358
Packing	358
Debugger Tricks	359
Disassembly Environment	360
Disassembly Practice	360
Summary	361
INDEX	363

About the Author

■ **ROGER A. GRIMES** is a 17-year computer security industry veteran, full-time teacher, author, and consultant. He is the author of 4 books and more than 150 magazine articles on computer security, specializing in Microsoft Windows security and malware defenses. He is a contributing editor for *Windows IT Pro* and *InfoWorld* magazines. His certifications include CPA, CISSP, CEH, CHFI, TICSAs, MCT, MCSE: Security (NT/2000/2003/MVP), Security+, A+, and others. Roger is a frequent presenter at national conferences, including MCP TechMentor, Windows Connections, and SANS, where he is always among the highest rated presenters. Roger has created several courses on advanced Windows security for Microsoft, *Windows IT Pro* magazine, and SANS. His clients have included every branch of the armed forces, Microsoft, VeriSign, Fortune 500 companies, cities, and large public school systems and universities.

About the Technical Reviewers



■ **ALEXZANDER NEPOMJASHIY** is a Microsoft SQL Server database designer for NeoSystems NorthWest, a security services, consulting, and training company. He has more than 11 years of experience in the IT field. His work involves extending and improving clients' corporate ERP systems to manage retail sales data, predict market changes, and calculate trends for future market situations.

■ **JACCO TUNNISSEN** has been working in the ISP and security fields since the mid-1990s, mainly focusing on FreeBSD and OpenBSD implementations. Currently, he is “educating the masses” using his web sites, where you can find out all about intrusion detection, honeypots (<http://www.honeypots.net>), incident handling, wireless security, computer forensics, DNS, and BGP routing. In his spare time, he enjoys good food and biking in Rotterdam. Jacco likes working as a technical reviewer for several authors.

Acknowledgments

I wish to thank Apress and my editor Jim Sumser, Sofia Marchant, Marilyn Smith, and StudioB's Neil J. Salkind for seeing the vision for a book like this and putting up with my moving deadlines.

I also want to thank Lance Spitzner, Michael Davis, and Niels Provos, for evangelizing honeypot technology, and answering my many questions. Thanks to Alexander Nepomnjashiy and Jacco Tunnissen for the excellent technical editing.

Much of this book could not have been written without the previous contributions of The Honeynet Project (<http://project.honeynet.org>), Honeypot: Tracking Hackers (<http://www.tracking-hackers.com>), SANS (<http://www.sans.org>), and the Honeypot mailing list (<http://www.securityfocus.com>).

On a personal note, I would especially like to thank my wife, Tricia, who took care of my every need while I was writing and neglecting her. I could not ask for a better friend and partner.

Introduction

Welcome to the world of honeypots! By reading this book, you are joining a friendly community of like-minded individuals who see honeypots as an important step in preventing and learning about malicious hacking activity.

If you were to ask a honeypot administrator why he uses a honeypot, the first response you would likely get is one or more legitimate business reasons explaining why honeypots are the best tool for the job. We've been trained to respond that way, so we can defend all our time spent managing and learning about honeypots to our bosses and loved ones. But underlying all the official logic is the real reason why most of us get interested in honeypots: the thrill of watching the bad guys expose themselves and their techniques, in an environment explicitly built to exploit them. It's videotaping the thief. It's taking the hacker's favorite tool of social engineering and using it against him. It's hacking the hacker.

For once, the good guys are in control and winning. With honeypots, we can track the hackers back to their lairs, identify them, and learn and defend against their techniques before they really get a chance to use them. Honeypots can stop hacker attacks, Internet worms, spam, and other acts of maliciousness. Honeypots remove the implicit veil of privacy most hackers think they have when they exploit a computer. If honeypots become as big and mature as most security experts expect them to be, they could put an end to the random, no consequence, hacking that so proliferates our Internet experience today. Honeypots are one of the few offensive plays in the computer security world.

Honeypots no longer need to prove their value. They have been responsible for discovering many new threats (called *zero-day exploits*) before they were widely known and used, including a Samba buffer overflow. Honeypots have been essential in capturing encrypted hacker traffic and instrumental in learning that hackers are using version 6 of the Internet Protocol (IPv6) to tunnel their communications under the very noses of network administrators. But perhaps, the greatest demonstration of a honeypot's value was the recent profiling of an extensive credit card fraud operation (<http://www.honeynet.org/papers/profiles/cc-fraud.pdf>).

Researchers followed the online activities and communications of individuals involved with credit card fraud, also known as *carders*. The honeynet was able to capture an incredibly automated Internet Relay Chat (IRC) network that allowed credit card numbers and identifying information to be stolen by simply typing a few keystrokes. Members of the ring could type in !cc to receive one random stolen credit card number. Other commands returned credit card account limits and provided web site links to vulnerable online merchant sites. The honeynet tracked key individuals, mostly located in South Asia and Pacific Rim countries, as they bought credit card numbers from legitimate businesses, hacked credit card security systems, and taught newcomers the ins and outs of carding. The credit card ring, by plying its trade online and out in the open, made their illegal activities appear more as a subculture than a crime. This attracted new participants. Honeypots allowed evidence to be recorded that after-the-fact affidavits, search warrants, and bugged phone conversations couldn't provide. The honeypot has solidified its place as a legitimate computer security defense tool.

Why Another Book on Honeypots?

There are already some excellent books, papers, and web sites on honeypots, so why did I feel compelled to write a book on the subject? In one sentence, it's because the world of computer security, and honeypots in particular, is largely Unix-based. Most of the literature about firewalls, intrusion detection systems (IDSs), and honeypots was written by Unix gurus. Most of the tools are Unix-based and work only on Unix platforms. Even when the tools are ported to Windows, they may talk about Windows and give a few Windows examples, but most of the text and examples are for Unix-based users. It can be very frustrating when you are not a Unix person but still want to learn about computer security and use all the cool tools.

The majority of the world's PCs run one of Microsoft's Windows operation systems. This book was written to fill the large gap for Windows administrators trying to learn about honeypots outside the Unix subculture. I don't give examples of software and exploits that do not occur in the typical Windows environment. When the book discusses mail servers, it will be referring to Microsoft Exchange, not Sendmail. When it refers to web servers, it will be talking about Microsoft Internet Information Services (IIS), not Apache. Yes, I know both of those programs have Windows-based counterparts, but they aren't the norm in a Windows network. This doesn't mean that the knowledge and lessons learned in this book cannot be applied to non-Microsoft environments. The opposite is true. You can take anything covered in this book and easily apply it to Unix, Linux, Macintosh, or any other computer environment. But for once, this is a honeypot resource that targets the Windows administrator. It means the following:

- Honeypot planning and setup will target Windows systems.
- Security tools will be Windows versions.
- Hacking examples will be Windows examples.
- When TCP/IP is discussed, it will be as it applies in Windows.
- When TCP/IP ports are discussed, they will be ports common to Windows.

Honeypots for Windows is a book for Windows-based users and administrators.

Who Is This Book For?

This book is for administrators and users with an intermediate understanding of the Windows operating system and computer security. Readers should have experience with the Windows operating system, the Internet, and Windows-based networking; be able to install and troubleshoot network-related software; and have general understanding of the OSI model. It helps if you're familiar with basic computer security concepts, such as computer worms, buffer overflows, and password cracking. An understanding of Windows security mechanisms will make the book more enjoyable.

A strong understanding of TCP/IP network protocol basics is essential for most honeypot administrators. Although this book will cover the fundamentals needed to understand the material presented, readers should understand the following terms prior to beginning this journey: TCP, UDP, ICMP, stateful, stateless, flags, TCP/IP handshake, packet header, and packet payload.

But even if you're not familiar with the details of all these topics, you should still be able to understand every concept discussed in this book. So, don't panic if you can't name all the TCP header flags off the top of your head, or if you don't know the exact meaning of stateful inspection. This book will be of value to people newly interested in computer security and honeypots, as well as to experienced security experts.

Readers without a firm foundation in these fundamentals should consider a quick refresher with a TCP/IP protocol reference. There are several good books on the TCP/IP protocol, and here are some online references:

- Webopedia's TCP/IP page: http://www.webopedia.com/TERM/T/TCP_IP.html
- An excellent TCP/IP Reference by Cisco: http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/ip.pdf
- About.com's Computer Networking Guide to TCP/IP: <http://compnetworking.about.com/cs/basictcpip>
- Wikipedia Internet Protocol Suite reference: http://www.wikipedia.org/wiki/Internet_protocol_suite
- Internet Engineering Task Force (IETF) references: <http://www.ietf.org>

■ **Note** On the IETF web site, at a minimum, read the following Request For Comments (RFCs): 791-IP, 792-ICMP, 768-UDP, and 793-TCP. RFCs are very wordy and long, and a bit like reading IRS tax code, but taking the time to read them will allow you to understand the TCP/IP protocol suite in detail.

What's In This Book?

The book has twelve chapters organized into three main parts.

By the time you get through reading this book, you should have an excellent understanding of honeypots in a Windows environment.

■ **Note** Many of the tools covered in this book are Windows ports of open-source Unix tools, like Honeyd, WinPcap, and Snort. All of these tools have been tested on Windows 98 and later Microsoft platforms, but most have been optimized for Windows 2000 and above. Menu options and screenshots were done on Windows 2000 and XP Professional computers, but most commands and screens are identical, no matter which Microsoft operating system you use. Every effort has been made to verify that all commands and utilities work across all current versions of Windows. Exceptions are noted when known.

Part One: Honey pots in General

Part One covers honey pot theory and topics common to all honey pots, along with the particular configuration requirements of a Windows-based environment.

Chapter 1 explains general honey pot theory and reasons to use honey pots. It discusses the main honey pot types, along with advantages and disadvantages of each choice. The chapter also covers hacking basics, such as attack model types and fingerprinting. Understanding the different hacking threats is essential to setting up and using a honey pot.

Chapter 2 describes the general setup and deployment of a honey pot, as well as how to attract hackers to it. Topics include how to decide where to place a honey pot and why. It covers the physical deployment issues involved in placing a honey pot, including hardening the host and configuring your network to route hacking traffic to your honey pot. It includes details on the problems introduced on switched networks and how to correctly configure your routing tables.

Part Two: Windows Honey pots

Part Two provides a detailed lesson in configuring and using Windows-based honey pots. Using an emulated honey pot in a Windows environment takes special consideration to make it appear as a Windows-based host. This means it should have the normal Windows ports open, run the normal Windows services, and respond in a predictable way. Chapter 3 defines normal behaviors, ports, and services on a Windows host, and tells you how to emulate them on a honey pot.

Chapter 4 describes using a real Windows operating system as a honey pot. It reveals what is the best Windows version to attract malicious hackers and presents hardening tips you can use to minimize compromise damage.

Chapters 5 through 7 focus on Honeyd, the most popular honey pot software in use today. Chapter 5 covers how to download and install Honeyd. Honeyd is a fantastic free tool, but like many other open-source programs, not particularly easy to configure. Chapter 6 begins deciphering the Honeyd configuration and provides several sample configuration files that you can adapt for your own needs. Chapter 7 explains how to use service scripts, which allow Honeyd to mimic basic applications, such as FTP, telnet, and IIS. Service scripts are very important in making a honey pot look like a real system.

Honeyd is the most popular and versatile honey pot software in use today, but it isn't the easiest to use. In Chapter 8, we explore six other Windows-based honey pots with front-end graphical user interfaces that make for a more pleasant user experience. Each of these honey pots excels at different goals. The honey pots are Back Officer Friendly, LaBrea, SPECTER, KFSensor, PatriotBox, and Jackpot.

Part Three: Honey pot Operations

Part Three discusses a range of topics related to getting the most out of your honey pot.

Using a network traffic analyzer and understanding how to recognize and decode malicious network traffic is essential to honey pot operations. Chapter 9 discusses how to install and use various tools for analyzing network traffic. It begins with network protocol basics, reviewing the OSI model and TCP/IP suite, and then focuses on using Snort and Ethereal.

Chapter 10 covers the very important issues of monitoring, logging, alerting, and reporting. It discusses how to set up an alert system, how and what to log, and what reports you need to generate.

Honeypots can quickly gather copious amounts of information—sometimes an overwhelming amount. The ultimate success of your honeypot is determined by how well you interpret the attack evidence. Chapter 11 discusses techniques to use in the forensics analysis of your honeypot data.

Chapter 12 discusses analyzing malicious code by disassembling it. For new programmers, this involves learning assembly language, learning how to disassemble executables, and learning about malicious coding in general. Becoming a disassembler is not for the faint of heart, but with a moderate amount of effort and practice, it can reveal malware functions that cannot be found any other way.

The sample files presented in this book, as well as other related files, are available from the Downloads area of the Apress web site (<http://www.apress.com>). You can direct any technical questions or concerns to me at roger@banneretcs.com.