

Honeypots for Windows

ROGER A. GRIMES

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.

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
-------------	-----