The Basics of Hacking and Penetration Testing

Ethical Hacking and Penetration Testing Made Easy

Second Edition

Dr. Patrick Engebretson

David Kennedy, Technical Editor

ELSEVIER

AMSTERDAM • BOSTON • HEIDELBERG • LONDON • NEW YORK
OXFORD • PARIS • SAN DIEGO • SAN FRANCISCO • SYDNEY • TOKYO
Syngress is an imprint of Elsevier

SYNGRESS

Acquiring Editor: *Chris Katsaropoulos*
Editorial Project Manager: *Benjamin Rearick*
Project Manager: *Priya Kumaraguruparan*
Designer: *Mark Rogers*

Syngress is an imprint of Elsevier
225 Wyman Street, Waltham, MA 02451, USA

Notices
Knowledge and best practice in this field are constantly changing. As new research and experience broaden our understanding, changes in research methods or professional practices, may become necessary. Practitioners and researchers must always rely on their own experience and knowledge in evaluating and using any information or methods described herein. In using such information or methods they should be mindful of their own safety and the safety of others, including parties for whom they have a professional responsibility.

To the fullest extent of the law, neither the Publisher nor the authors, contributors, or editors, assume any liability for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions, or ideas contained in the material herein.

Library of Congress Cataloging-in-Publication Data
Engebretson, Pat (Patrick Henry), 1974-
The basics of hacking and penetration testing : ethical hacking and penetration testing made easy / Patrick Engebretson. — Second edition.
pages cm
Includes bibliographical references and index.
ISBN 978-0-12-411644-3
1. Penetration testing (Computer security) 2. Computer hackers. 3. Computer software—Testing. 4. Computer crimes—Prevention. I. Title.
QA76.9.A25E5443 2013
005.8—dc23
2013017241

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library.

ISBN: 978-0-12-411644-3

For information on all Syngress publications, visit our website at www.syngress.com.

Printed in the United States of America
13 14 15 10 9 8 7 6 5 4 3 2 1

Dedication

This book is dedicated to God and my family. Time to make like Zac Brown and get Knee Deep.

Contents

Acknowledgments

Thank you to everyone involved in making this second edition possible. Publishing a book is a team effort and I have been blessed to be surrounded by great teammates. The list below is woefully inadequate, so I apologize in advance and thank everyone who had a hand in making this book a reality. Special thanks to:

MY WIFE

My rock, my lighthouse, my steel cables. Thank you for the encouragement, belief, support, and willingness to become a "single mother" again while I disappeared for hours and days to work on this second edition. As with so many things in my life, I am certain that without you, this book would not have been. More than anyone else, I owe this work to you. I love you.

MY GIRLS

I know that in many ways, this edition was harder for you than the first because you are now old enough to miss me when I am gone, but still too young to understand why I do it. Someday, when you are older, I hope you pick up this book and know that all that I do in my life is for you.

MY FAMILY

Thank you to my extended family for your love and support. An extra special thank you to my mother Joyce, who once again served as my unofficial editor and has probably read this book more times than anyone else. Your quick turnaround time and insights were invaluable.

DAVE KENNEDY

It has been a real honor to have you contribute to the book. I know how busy you are between family, TrustedSec, the CON circuit, SET, and every other crazy project you run, but you always made time for this project and your insights have made this edition much better than I could have hoped for. Thank you my friend. #hugs. I would be remiss not to give some additional credit to Dave, not only did he contribute through the technical editing process but he also worked tirelessly to ensure the book was Kali compliant and (naturally) single-handedly owned Chapter 5 (SET).

JARED DEMOTT

What can I say to the last man who made me feel like an absolute idiot around a computer? Thanks for taking the time and supporting my work. You have become a great friend and I appreciate your help.

TO THE SYNGRESS TEAM

Thanks again for the opportunity! Thanks to the editing team, I appreciate all of the hard work and dedication you gave this project. A special thanks to Chris Katsaropoulos for all your efforts.

About the Author

Dr Patrick Engebretson obtained his Doctor of Science degree with a specialization in Information Assurance from Dakota State University. He currently serves as an Assistant Professor of Computer and Network Security and also works as a Senior Penetration Tester for security firm in the Midwest. His research interests include penetration testing, hacking, exploitation, and malware. Dr Engebretson has been a speaker at both DEFCON and Black Hat in Las Vegas. He has also been invited by the Department of Homeland Security to share his research at the Software Assurance Forum in Washington, DC. He regularly attends advanced exploitation and penetration testing trainings from industry-recognized professionals and holds several certifications. He teaches graduate and undergraduate courses in penetration testing, malware analysis, and advanced exploitation.