



Advanced Penetration Testing

Hacking the World's Most Secure
Networks

Wil Allsopp

WILEY

Advanced Penetration Testing: Hacking the World's Most Secure Networks

Published by
John Wiley & Sons, Inc.
10475 Crosspoint Boulevard
Indianapolis, IN 46256
www.wiley.com

Copyright © 2017 by John Wiley & Sons, Inc., Indianapolis, Indiana

Published simultaneously in Canada

ISBN: 978-1-119-36768-0
ISBN: 978-1-119-36771-0 (ebk)
ISBN: 978-1-119-36766-6 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 646-8600. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at <http://www.wiley.com/go/permissions>.

Limit of Liability/Disclaimer of Warranty: The publisher and the author make no representations or warranties with respect to the accuracy or completeness of the contents of this work and specifically disclaim all warranties, including without limitation warranties of fitness for a particular purpose. No warranty may be created or extended by sales or promotional materials. The advice and strategies contained herein may not be suitable for every situation. This work is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If professional assistance is required, the services of a competent professional person should be sought. Neither the publisher nor the author shall be liable for damages arising herefrom. The fact that an organization or Web site is referred to in this work as a citation and/or a potential source of further information does not mean that the author or the publisher endorses the information the organization or website may provide or recommendations it may make. Further, readers should be aware that Internet websites listed in this work may have changed or disappeared between when this work was written and when it is read.

For general information on our other products and services please contact our Customer Care Department within the United States at (877) 762-2974, outside the United States at (317) 572-3993 or fax (317) 572-4002.

Wiley publishes in a variety of print and electronic formats and by print-on-demand. Some material included with standard print versions of this book may not be included in e-books or in print-on-demand. If this book refers to media such as a CD or DVD that is not included in the version you purchased, you may download this material at <http://booksupport.wiley.com>. For more information about Wiley products, visit www.wiley.com.

Library of Congress Control Number: 2017931255

Trademarks: Wiley and the Wiley logo are trademarks or registered trademarks of John Wiley & Sons, Inc. and/or its affiliates, in the United States and other countries, and may not be used without written permission. All other trademarks are the property of their respective owners. John Wiley & Sons, Inc. is not associated with any product or vendor mentioned in this book.

This work is dedicated to the memory of Sir Terry Pratchett, OBE (1948–2015), for teaching me comedy and satire and the wisdom to know the difference.

“Do you not know that a man is not dead while his name is still spoken?”

—Going Postal



About the Author

Wil Allsopp always liked taking things apart. Sometimes he was able to put them back together again. He wandered into penetration testing like some people wander into bars (another activity close to his heart). A chance encounter with a like-minded individual in the 't Stadscafe Zaltbommel in 1999 led to him resigning his IBM software development contract and forming his first company, called Tigerteam Security NV, which for reasons lost to time was incorporated in Curaçao. At least that's how he remembers it.

Nearly 20 years later, he's still breaking things, with the important difference that some of the most prestigious companies in the world are paying him to do so.

He lives in The Netherlands with his wife and a large menagerie of cats, dogs, chickens, and a toad named Malcolm.

"We work in the dark—we do what we can—we give what we have. Our doubt is our passion, and our passion is our task. The rest is the madness of art."

—Henry James



About the Technical Editor

Elias Bachaalany has been a computer programmer and a software reverse engineer for more than 14 years. Elias is also the co-author of two books published by Wiley, *Practical Reverse Engineering* and *The Antivirus Hacker's Handbook*, and the author of *Batchography: The Art of Batch Files Programming*. He worked with various technologies and programming languages such as web programming, database programming, and Windows device drivers programming (boot loaders and minimal operating systems), and wrote .NET and managed code, wrote scripts, assessed software protections, and wrote reverse engineering and desktop security tools.



Credits

Project Editor

Adaobi Obi Tulton

Technical Editor

Elias Bachaalany

Production Editor

Barath Kumar Rajasekaran

Copy Editor

Kezia Endsley

Manager of Content**Development & Assembly**

Mary Beth Wakefield

Production Manager

Kathleen Wisor

Marketing Manager

Carrie Sherrill

**Professional Technology &
Strategy Director**

Barry Pruett

Business Manager

Amy Knies

Executive Editor

Jim Minatel

Project Coordinator, Cover

Brent Savage

Proofreader

Nancy Bell

Indexer

Johnna VanHoose Dinse

Cover Designer

Wiley

Cover Image

Bullet © Ejla/istock.com; card

© zlisjak/istock.com; torn edges ©

hudiemm/istock.com



Acknowledgments

Far too many to name (and they know who they are), but special thanks to Tim and Courtney without whom this work would not be possible in its current format; D. Kerry Davies, for being the yardstick by which the rest of are measured; GCHQ, for their helpful suggestions; and last but not least, Gary McGath, one of the most underrated musicians of our age.

Also, thanks to every pen tester, hacker, and security evangelist I've toiled with over the years. You are this book.



Contents at a glance

Foreword	xxiii
Introduction	xxvii
Chapter 1 Medical Records (In)security	1
Chapter 2 Stealing Research	29
Chapter 3 Twenty-First Century Heist	57
Chapter 4 Pharma Karma	77
Chapter 5 Guns and Ammo	103
Chapter 6 Criminal Intelligence	137
Chapter 7 War Games	175
Chapter 8 Hack Journalists	193
Chapter 9 Northern Exposure	213
Index	235

This page intentionally left blank



Contents

Foreword	xxiii
Introduction	xxvii
Chapter 1 Medical Records (In)security	1
An Introduction to Simulating Advanced Persistent Threat	2
Background and Mission Briefing	2
Payload Delivery Part 1: Learning How to Use the VBA Macro	5
How NOT to Stage a VBA Attack	6
Examining the VBA Code	11
Avoid Using Shellcode	11
Automatic Code Execution	13
Using a VBA/VBS Dual Stager	13
Keep Code Generic Whenever Possible	14
Code Obfuscation	15
Enticing Users	16
Command and Control Part 1: Basics and Essentials	19
The Attack	23
Bypassing Authentication	23
Summary	27
Exercises	28
Chapter 2 Stealing Research	29
Background and Mission Briefing	30
Payload Delivery Part 2: Using the	
Java Applet for Payload Delivery	31
Java Code Signing for Fun and Profit	32
Writing a Java Applet Stager	36
Create a Convincing Pretext	39
Signing the Stager	40

Notes on Payload Persistence	41
Microsoft Windows	41
Linux	42
OSX	45
Command and Control Part 2: Advanced Attack Management	45
Adding Stealth and Multiple System Management	45
Implementing a Command Structure	47
Building a Management Interface	48
The Attack	49
Situational Awareness	50
Using AD to Gather Intelligence	50
Analyzing AD Output	51
Attack Against Vulnerable Secondary System	52
Credential Reuse Against Primary Target System	53
Summary	54
Exercises	55
Chapter 3 Twenty-First Century Heist	57
What Might Work?	57
Nothing Is Secure	58
Organizational Politics	58
APT Modeling versus Traditional Penetration Testing	59
Background and Mission Briefing	59
Command and Control Part III: Advanced	
Channels and Data Exfiltration	60
Notes on Intrusion Detection and the Security	
Operations Center	64
The SOC Team	65
How the SOC Works	65
SOC Reaction Time and Disruption	66
IDS Evasion	67
False Positives	67
Payload Delivery Part III: Physical Media	68
A Whole New Kind of Social Engineering	68
Target Location Profiling	69
Gathering Targets	69
The Attack	72
Summary	75
Exercises	75
Chapter 4 Pharma Karma	77
Background and Mission Briefing	78
Payload Delivery Part IV: Client-Side Exploits 1	79
The Curse That Is Flash	79
At Least You Can Live Without It	81
Memory Corruption Bugs: Dos and Don'ts	81
Reeling in the Target	83

Command and Control Part IV: Metasploit Integration	86
Metasploit Integration Basics	86
Server Configuration	86
Black Hats/White Hats	87
What Have I Said About AV?	88
Pivoting	89
The Attack	89
The Hard Disk Firewall Fail	90
Metasploit Demonstration	90
Under the Hood	91
The Benefits of Admin	92
Typical Subnet Cloning	96
Recovering Passwords	96
Making a Shopping List	99
Summary	101
Exercises	101
Chapter 5 Guns and Ammo	103
Background and Mission Briefing	104
Payload Delivery Part V: Simulating a Ransomware Attack	106
What Is Ransomware?	106
Why Simulate a Ransomware Attack?	107
A Model for Ransomware Simulation	107
Asymmetric Cryptography	108
Remote Key Generation	109
Targeting Files	110
Requesting the Ransom	111
Maintaining C2	111
Final Thoughts	112
Command and Control Part V: Creating a Covert C2 Solution	112
Introducing the Onion Router	112
The Torrc File	113
Configuring a C2 Agent to Use the Tor Network	115
Bridges	115
New Strategies in Stealth and Deployment	116
VBA Redux: Alternative Command-Line Attack Vectors	116
PowerShell	117
FTP	117
Windows Scripting Host (WSH)	118
BITSadmin	118
Simple Payload Obfuscation	119
Alternative Strategies in Antivirus Evasion	121
The Attack	125
Gun Design Engineer Answers Your Questions	126

	Identifying the Players	127
	Smart(er) VBA Document Deployment	128
	Email and Saved Passwords	131
	Keyloggers and Cookies	132
	Bringing It All Together	133
	Summary	134
	Exercises	135
Chapter 6	Criminal Intelligence	137
	Payload Delivery Part VI: Deploying with HTA	138
	Malware Detection	140
	Privilege Escalation in Microsoft Windows	141
	Escalating Privileges with Local Exploits	143
	Exploiting Automated OS Installations	147
	Exploiting the Task Scheduler	147
	Exploiting Vulnerable Services	149
	Hijacking DLLs	151
	Mining the Windows Registry	154
	Command and Control Part VI: The Creeper Box	155
	Creeper Box Specification	155
	Introducing the Raspberry Pi and Its Components	156
	GPIO	157
	Choosing an OS	157
	Configuring Full-Disk Encryption	158
	A Word on Stealth	163
	Configuring Out-of-Band Command and Control	
	Using 3G/4G	164
	Creating a Transparent Bridge	168
	Using a Pi as a Wireless AP to Provision Access by Remote	
	Keyloggers	169
	The Attack	171
	Spoofing Caller ID and SMS Messages	172
	Summary	174
	Exercises	174
Chapter 7	War Games	175
	Background and Mission Briefing	176
	Payload Delivery Part VII: USB Shotgun Attack	178
	USB Media	178
	A Little Social Engineering	179
	Command and Control Part VII: Advanced Autonomous Data	
	Exfiltration	180
	What We Mean When We Talk About “Autonomy”	180
	Means of Egress	181
	The Attack	185
	Constructing a Payload to Attack a Classified Network	187
	Stealthy 3G/4G Software Install	188

	Attacking the Target and Deploying the Payload	189
	Efficient “Burst-Rate” Data Exfiltration	190
	Summary	191
	Exercises	191
Chapter 8	Hack Journalists	193
	Briefing	193
	Advanced Concepts in Social Engineering	194
	Cold Reading	194
	C2 Part VIII: Experimental Concepts in Command and Control	199
	Scenario 1: C2 Server Guided Agent Management	199
	Scenario 2: Semi-Autonomous C2 Agent Management	202
	Payload Delivery Part VIII: Miscellaneous Rich Web Content	205
	Java Web Start	205
	Adobe AIR	206
	A Word on HTML5	207
	The Attack	207
	Summary	211
	Exercises	211
Chapter 9	Northern Exposure	213
	Overview	214
	Operating Systems	214
	Red Star Desktop 3.0	215
	Red Star Server 3.0	219
	North Korean Public IP Space	221
	The North Korean Telephone System	224
	Approved Mobile Devices	228
	The “Walled Garden”: The Kwangmyong Intranet	230
	Audio and Video Eavesdropping	231
	Summary	233
	Exercises	234
Index		235