

WIL ALLSOPP

FOREWORD BY  
HANS VAN DE LOOY

# ADVANCED PENETRATION TESTING



HACKING THE  
WORLD'S  
MOST SECURE  
NETWORKS

WILEY



# **Advanced Penetration Testing**





# 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](http://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](http://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.





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





# Contents

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







## Foreword

Ever since I came first into contact with computers, the security (or insecurity if you want) of these very powerful systems has intrigued me. Living in The Netherlands, I was fortunate to be able to use a Philips P9200 system of the Technical University Eindhoven by dialing into it using a 300 baud modem when I attended high school to learn programming in ALGOL 60. Personal computers were virtually nonexistent at that time and computer systems like this cost a small fortune. Using a modem to connect to a system that you could program to solve lots of computational problems was already something magical, but gaining access to the machine itself became something of a quest. Since it was located on the university's campus, this was not that problematic. At that time, security was not really a big issue, and walking onto the premises as a young scholar asking for a tour of the facility was all it took.

There I learned that the P9200 was just a "small mini computer." The real deal was the Burroughs B7700 mainframe. It took some snooping around to find the dial-in number for that system, and a lot of persuading to get an account on that system, but eventually I succeeded. I did not hack the system at that time, but social engineering (being able to tell a persuading enough story to gain trust and/or information) proved to be a very valuable trait to have.

While I studied computing science, we eventually had to use Prime computers. Let me just state that computer security at that time was not considered important. The number of bugs in the operating system (PrimeOS) were numerous, and even fixes for security problems we uncovered would contain new security bugs. At that time, information security really caught my attention and it has not faded since. Just before graduating, I started working for a small company called Positronika, developing systems for the nuclear industry, ranging from a small pocket dosimeter (based on a 6502 processor) to large automated measurement

systems. They used PDP-11 systems for fuel rods after they were used in a nuclear reactor. I not only learned the importance of safety, but also learned how to write secure computer code. You just could not risk the various rod handling routines and drop some very highly radioactive material. It could be fatal.

In 1989, I came into contact with an underground and obscure publication called *Hack-Tic*, which was a so-called hacker magazine published irregularly. It opened up a whole new world to me. I suddenly noticed there were many more people interested in IT security and they published lots of other information as well. This included information on the phone system, which the Dutch telecom provider—at that time called PTT—was not too pleased with (they still did not understand that security through obscurity is a fundamentally bad idea!), as well as information about picking locks, to name but a few tricks. Discussing subjects like these with like-minded people eventually grew to monthly gatherings, random parties, and hacker events (in hotels and on campgrounds—always including high-speed Internet connectivity). Nowadays, there are even hacker spaces where people not only are building or breaking software, but are using all kinds of modern technology in new ways. So what once started as an underground movement is currently very well connected in modern society.

Fast forward to the year 2000. After several positions at various companies, eventually resulting in a lead role in a pentest group at one of the largest computer centers in The Netherlands, two friends and I decided we would start a business ourselves. The Internet bubble had just busted and we thought it a good idea to start a consultancy company focusing on information security. Luckily, we always had the credo, “If we do not succeed, we should at least be able to tell ourselves we had a blast.” Little did we know.

The first assignment came when I was visiting Scandinavia and I had to draft a contract for this penetration test in a room of a hotel I walked by while talking to the prospect and used their fax machine to send it out. We did not even have a name for this venture of ours.

Even though the bubble busted and various Internet companies were forced to close shop, we continued, eventually choosing the name Madison Gurkha since we could not find any domain name containing something that came close to the service we tried to provide. The advantages of this exotic name were numerous, ranging from the fact you had to spell it at least three times (so it would really be burned into the brains of those who had to deal with us), to the assumption people made (and still make) that we were an international conglomerate with an HQ somewhere outside of The Netherlands.

At that time we had no need for a sales and marketing department. Our personal network was expanding and there were not many businesses providing our services, so verbal recommendations brought the opportunities to our door. At that time we basically only did vulnerability assessments of web

applications and ICT infrastructures, and some pentesting when our customers were really interested in the impact of real-live attacks on their ICT environments. Since there were hardly any tools available, we had to create our own exploits and scripts to make our lives easier. Exploits were sometimes also published on the Internet (mostly in newsgroups), but you had to compile them yourself and they always contained some flaw so that script kiddies who just compiled the thing, but did not understand the actual problem, could not use the code (you had to make some minor modifications to be able to use it). At the time of this writing, tools like Metasploit and Nessus are widely available and popular TV shows like *Mr. Robot* show these tools at work.

But IT security advances. It always has been, and will probably always be, a precarious balance between attacks and defenses. The available tools will be enhanced and become more powerful and more advanced tools will become available. But only in the hands of a well-educated specialist will they add real value. That person not only understands the benefits of the tools but also knows their limitations and how to interpret the results.

Wil Allsopp is one such specialist. I have been fortunate to work with Wil when he joined Madison Gurkha in 2006. At that time we were a couple of years old and expanding from the three-person start-up to the well-established dedicated IT security consultancy firm we are today. Wil helped us push the bounds of the security testing envelope even further and has done so ever since. He has always looked for new vulnerabilities and wants corporations and institutions to be aware of the latest threats. This book contains various valuable examples of those advanced threats.

When your organization not only is looking for a positive score on the “in control” checklist, but really wants to know if it is capable of withstanding the kind of very advanced attacks that currently take place on a global scale, you should read this book. Ensure that the company you hire to perform IT security assessments can actually execute attacks like these. Once again, Wil shows that a real IT security specialist not only does know how to use available tools, but is also able to think outside of the box and develop additional and advanced attacks when needed. Regular vulnerability scans are helpful to keep your infrastructure on par; actual penetration testing using advanced techniques like those described in this book will provide your organization with the needed insight on whether you are actually in control of your IT security or have been shutting your eyes to the real dangers out there while adding ticks to your checklists.

Amsterdam, October 5, 2016  
Hans Van de Looy  
Founder of Madison Gurkha BV





# Introduction

There is an old yet erroneous belief that fortune favors the brave. Fortune has and always will favor the prepared. When your organization experiences a serious security incident (and it will), it's your level of preparedness based on the understanding of the inevitability of such an event that will guide a successful recovery. It doesn't matter if you're responsible for the security of a local community college or if you're the CISO of an international bank—this fact will always remain true.

To quote Howard Ruff, “It wasn't raining when Noah built the ark.”  
The first step to being prepared is being aware.

## Coming Full Circle

---

There has always been the impression that you have to patch your systems and secure your networks because hackers are scanning vast address ranges looking for victims who haven't done these things and they'll take whatever vulnerable systems they can get. In a sense that's true—there have always been those who are satisfied with low hanging fruit. It was true back in the 80s as well—war dialing on the PSTN and such attacks are usually trivial to guard against if you know what you're up against. However, if you are specifically targeted by someone with time and resources, you have a problem of an altogether different magnitude. Put simply, gaining access to corporate systems by patiently targeting the users was usually the best way to go in the 80s and it's usually the best way now. However, the security industry, like any other, is constantly looking to sell “new” products and services with different names and to do that, a buzzword is required. The one that stuck was *advanced persistent threat*.