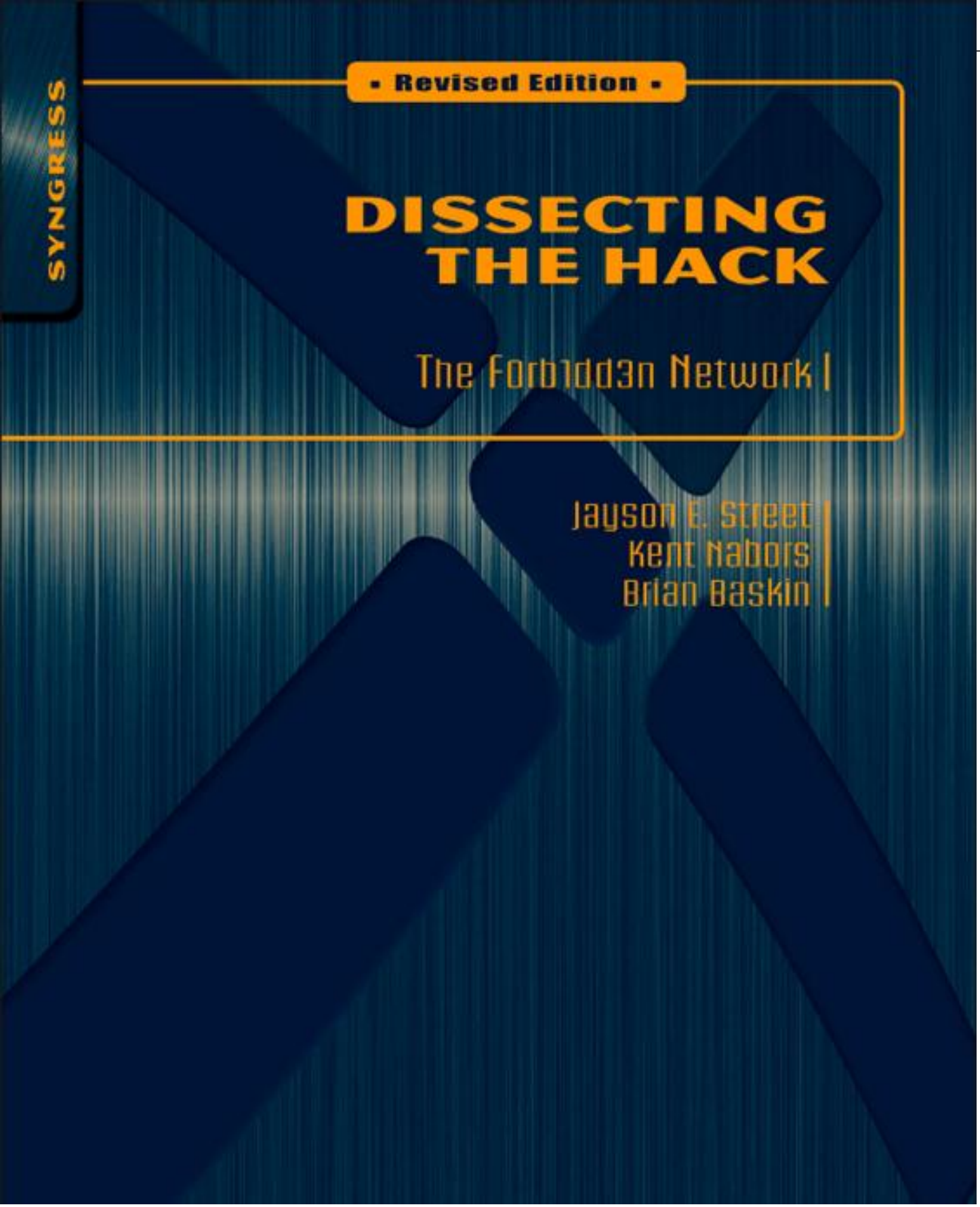
SYNGRESS
• Revised Edition •
DISSECTING THE HACK
The Forb1dd3n Network
Jayson E. Street
Kent Nabors
Brian Baskin

Dissecting the Hack

Revised Edition

This page intentionally left blank

Dissecting the Hack

The F0rb1dd3n Network

Revised Edition

Jayson E. Street

Kent Nabors

Brian Baskin

Marcus Carey

Technical Editor

Dustin D. Trammell

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

SYNGRESS®

Acquiring Editor: Rachel Roumeliotis
Development Editor: Matthew Cater; David Bevans
Project Manager: Julie Ochs
Designer: Alisa Andreola

Syngress is an imprint of Elsevier
30 Corporate Drive, Suite 400, Burlington, MA 01803, USA

Library of Congress Cataloging-in-Publication Data
Application submitted

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

ISBN: 978-1-59749-568-4

Printed in the United States of America
10 11 12 13 14 10 9 8 7 6 5 4 3 2 1

Typeset by: diacriTech, Chennai, India

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

To Earl L. Street
All that I am and part of what my children will become is because of who you were. Thank you and I miss and think of you everyday.

To Dee Drake and Aliera
For all the love you give me thank you. Also for putting up with me when I am there and missing me when I am away.

This page intentionally left blank

Contents

Foreword

The world of hacking is a world of pain and frustration. Frustration for the hacker as he tries to figure out how to break the latest and greatest security device, and pain for the manufacturer or corporation that made or was relying on that device.

At least, that is the layman's view – the hacker is the "bad guy," set on doing evil and causing pain to those he comes up against, and interested only in one thing: destroying the security of the systems in front of him. The manufacturer is the innocent victim, trying to go about its business, but suffering unprovoked attacks. But it's not as simple as that. Hackers come in all shapes and sizes, some good and some bad, and they hack for all kinds of reasons, some benign and some selfish. Manufacturers also come in all shapes and sizes, and of course, the pain and frustration definitely comes in all shapes and sizes:

- The frustration of not getting your message across – trying and failing to make people understand not only what is wrong with their product but why it's important that they get it right.
- The pain of seeing your research buried under threats of lawsuits, even though you are right and the issue you've uncovered is there to be exploited.
- The frustration of dealing with manufacturers or commercial businesses that put profit or expedience over end-user safety and security.
- The pain of losing data or suffering an intrusion through an unpatched system...

The list goes on.

When I met Jayson, he didn't know it then, but he was going to experience pain and frustration in spades. He had come up with a brilliant scheme for overcoming all these obstacles, and it should have been a "no-brainer." Not only that, but he was enthusiastic, intelligent, personable, committed, and, most importantly, *on the right side*. He was one of us, one of the good guys, with something that was going to help solve the everlasting problem of how you get those with the power to make things change understand not only *what* needs to happen but *why* it needs to happen. In other words, how to engage them. Talk to me about marketing and my eyes will glaze over and I'll be a million miles away in a world of my own. Talk to most management about technical or security problems, and you'll have the same effect – they are off with the fairies and your wise words are going in one ear and out of the other.

However, Jayson had a plan. What do people like better than technical manuals and lectures on threat management or risk assessments? Stories, of course. Thrillers! Action! Secret agents taking on the forces of evil and winning!

Jayson and I meet about once a year in, of all places, Las Vegas. We both go there for the world's largest "hacker" conference, DEFCON. When I first met him, Jayson was excited. He had a book. This book. As soon as he explained the concept to me, I was sold. The idea that you could read a good book that not only entertained you but

could then be flipped into a technical reference that showed you exactly how each of those neat hacks worked was a sure winner. Maybe this would be the way to get the "suits" to understand that this is not the stuff of fiction. This is real and it's happening to them, *right now*.

When I met him again the following year, he was still excited. Ideas were flowing, research was pouring in, and his book was progressing. He was now looking for a publisher. Things were looking good.

The year after that, he was still excited, but he was feeling the pain of rejection, and frustration as finding a publisher wasn't as easy as he'd first thought. But he was upbeat. He was a man on a mission. He had loads of new ideas so that just meant the book would be even better by the time it came out, so no problem... soldier on!

Three years on, and here he is again – still smiling and determined, but still frustrated and in pain. They just don't get it. The book gets better and better, but he's hitting a brick wall.

It could have ended there, but Jayson is no quitter. The other thing that impressed me about him when we first met was his determination to follow things through. He's never made me a promise that he hasn't kept (and we all know those are ten a penny at conferences... "Sure, I'll send you that stuff as soon as I get home..."), and he's always looking out for something he can do to benefit those around him. This book is all about sharing and learning, and that encapsulates the hacker ethos and, in particular, the DEFCON ethos. If you know something, share it. If you learn something, learn more. When you really know your stuff, teach it.

The publication of this book was a hard-won victory, and I hope you learn as much from it as Jayson did researching it, but most of all, I hope you enjoy it as much as I have and as much as it deserves to be enjoyed.

Adam Laurie
Dorset, UK, June 2009.

Acknowledgments

Thanks to Haki Berkeri for the pizza, Pepsi, and the good advice that kept me going when nothing else was.

I also owe thanks to Weldon for Wednesday, and Dee for all the days in between. I thank Rudy for the rides and for sticking with Hanzo. Big thanks to Marcus J. Carey for helping me off the ledge and introducing me to Brian. Thanks to Brian Baskin who created what should have been there in the first place, Jeff R. for helping out the iPhone guy, and David Letterman for letting me be on his show (and to Stephen Colbert for letting me on his I hope). Thanks to Del Rhea and Lee for their love of rodents who hang out at the mall. I thank Leon for being my first official fan, Rafe for his patience and tolerance of a wild and loud crazy roommate, Laura (she knows why), and Pam for leaving. I thank Crystal, Jason, and Sean for being good students, Marco for the experience in warehouse living, Leslie's mom for giving me Jackie (I'm taking good care of her), Capt. Tom Johnson for the loan of the gun (I was glad to give it back), Mrs. F. Collins for being the only teacher who encouraged me in learning and poetry, Stone for sweetly shipping me the sword from Shanghai (that was swell), and Sherry, Andrea, and Kris for all the help in the background with the book. Of course, thanks to Rachel for taking a chance on some geek on Twitter ☺. Also thanks to Syngress for making my dream a reality again (stay tuned – more to follow). Thanks to Ming and the Wuxi PWNAGE team for … well you figure it out ;-). Thanks to my family, whose fault it is that I am such a creative and unique individual. Oh yeah! And thanks to that person for that thing (yeah, you know who I'm talking about) – that was great.

A special shout out to Bastiaan de Boer from BRUCON, I can't wait to blow you up in the next book, thanks for supporting Hackers for Charity.

To Dan K., Johnny L., Jeff M., and Marcus R., thanks for believing in me and contributing to this revised version it means more to me than you know.

Last and by no means the least thanks to the INFOSEC and hacking communities, especially Tim Smith and all the great friends I have found on Twitter who have made my life a lot more interesting than it would have been if I had become a lawyer.

– Jayson

Lisa, Christina, and Margaret – thank you for giving me the time and inspiration to write. Mrs. Coffin, thank you for teaching me brevity.

– Kent

Thank you to my family and children for the time, freedom, and motivation to do what needed to be done. Thank you to all law enforcement agencies who work tirelessly every day to make this world a better place, and to the hackers who make

their jobs more fun and interesting. Thanks for Jayson and Kent for putting together an excellent story. Thank you to Jayson for fighting through a major uphill battle, while learning of and climbing additional mountains along the way, and staying cheerful about it all, and to everyone who put it all on the line to make this book a success.

– Brian

H0w t0 R34d *Dissecting the Hack: The F0rb1dd3n Network*

Both sections of this book tell a single story. The adventures of Bob and Leon are more than just a fun read. They illustrate many very real threats to individuals, businesses, organizations, and even countries. The networked world is so interconnected; many don't realize how valuable a target they really are. The best and worst of humanity connected with the speed and power of modern technology comes together in a world of our own making that we do not yet understand.

"The F0rb1dd3n Network" tells the story of two kids caught up in an adventure they did not expect. Bob and Leon are most comfortable in a digital world but soon find that digital actions have physical consequences. Throughout their fictional story are real-world lessons.

"Security Threats Are Real" or STAR focuses on those real-world lessons. The hacks and tools in the fictional story are very real. STAR provides the details, sources, and references to learn more about the threats, defensive techniques, attacker techniques, and even cool toys of the fictional story.

"The F0rb1dd3n Network" can be read by itself as a story. It can also be read as an illustration of the issues described in STAR. Throughout "The F0rb1dd3n Network," you will find links that point to specific references in STAR where you can get more information about key concepts. Or if you read STAR, you will find links to "The F0rb1dd3n Network" where the story illustrates a scenario where very real tools and techniques are applied. Each section leans on the other. How you read them is entirely up to you.

For the more adventurous reader, "The F0rb1dd3n Network" contains "Easter eggs" as well. Woven throughout are references, hints, phrases, and more that will lead you to significant or trivial insights into hacker culture. Again, STAR will help you find out more about the Easter eggs. But not all the answers are given away. There must be some unsolved mystery to make hacking worth the time.

So read "The F0rb1dd3n Network" as a story. Read STAR as a reference work. Dig for Easter eggs in "The F0rb1dd3n Network." Or put it all together to learn more about the very real threats of the digital world we all live in.

Dissecting the Hack: The F0rb1dd3n Network can happen IRL.

This page intentionally left blank

About the Authors

Jayson E. Street Jayson is not just an author of the book *Dissecting the Hack: The F0rb1dd3n Network*. His consultation with the FBI and Secret Service on attempted network breaches resulted in the capture and successful prosecution of the criminals involved. In 2007 he consulted with the Secret Service on the Wi-Fi security posture at the White House.

He has also spoken at DEFCON, BRUCON, UCON, and at several other 'CONs and colleges all over the world on a variety of Information Security subjects. He also was the co-founder and speaker of ExcaliburCon held in Wuxi China. He has also been a witness in civil & criminal cases.

He is a current member on the Board of Directors for the Oklahoma "InfraGard". He is also Vice President for ISSA OKC. Jayson has been a longtime member of the Netragard "SNOsoft" research team.

If you would like to find out more about him than even he cares to admit feel free to visit http://f0rb1dd3n.com/. Also note he is a highly carbonated speaker who has partaken of Pizza from Beijing to Brazil. He does not expect anybody to still be reading this far but if they are please be aware he was chosen as one of Time's persons of the year for 2006 FTW!

Kent Nabors Kent Nabors serves as a Vice President of Information Security for a multibillion dollar financial institution. He has significant experience in both the banking and the IT industries. He has worked in bank examinations with the Federal Deposit Insurance Corporation and the Federal Reserve Bank.

Kent's background includes security policy development, systems implementation, incident response, and training development.

Kent is a graduate of the University of Oklahoma and Southern Nazarene University.

When he isn't thinking about locking down bits and bytes, he is usually trying to keep up with his wife and two daughters. Quiet time usually involves power tools or an eclectic reading list.

Brian Baskin is a digital forensics professional employed by CSC and serves as the Deputy Lead Technical Engineer with the Defense Cyber Investigations Training Academy (DCITA), part of the Department of Defense Cyber Crime Center (DC3). For more than 10 years, Brian has worked with DCITA to research, develop, and teach forensic responses to growing cyber threats. Brian devotes much of his time to researching the evolving Internet crimes, network protocol analysis, and Linux and UNIX intrusion responses.

Brian also serves as a technical reviewer for DCITA. He helps to analyze content and procedures for more than two dozen cyber security courses for technical validity and relevance. For fun, he manages a content creation team that develops online Web-based incident response training that provides hands-on experience to military units stationed overseas. His team works with the various federal and military law

enforcement groups for information sharing and collaboration on ongoing threats and best practices.

Brian has been involved with multiple book projects with Syngress Publishing, and he has also served as a subject matter expert for content development for the National White Collar Crime Center (NW3C) and the Federal Law Enforcement Training Center (FLETC).

Marcus J. Carey is well known for being a compulsive mentor in the information security community. Marcus has more than 17 years of experience in the information security field, working in the military, federal, and private sectors. Marcus served more than 8 years active duty in the U.S. Navy Cryptologic Security Group. Marcus ended his naval service by being assigned to the National Security Agency (NSA) where he engineered, monitored, and defended the Department of Defense's secure networks. Marcus earned a Master of Science in Network Security from Capitol College in Laurel, Maryland.

Technical Editor

Dustin D. Trammell is the founder of the Computer Academic Underground and cofounder of the Austin Hackers Association (AHA!). He has more than a decade of experience in various areas of information security including vulnerability assessment, penetration testing, secure network architecture, vulnerability research and exploit development, and security research in specific areas related to network protocols, network applications, steganography, and Voice over Internet Protocol (VoIP).

Over the years, Dustin has been involved with many security community projects such as the design and development of Sender Policy Framework (SPF) for e-mail (RFC 4408) and contributing as a core developer for the Metasploit Project. Dustin has also released numerous security tools such as the infamous PageIt! mass-paging application, the hcraft HTTP exploit-crafting framework, and the SteganRTP VoIP steganography tool.

He regularly releases vulnerability and exploit advisories, speaks at security-related events and conferences, and is on the Technical Advisory Board of the Voice over IP Security Alliance (VoIPSA).

Throughout Dustin's career, he has performed security research and development focused on attack vectors and exploitation methods for BreakingPoint Systems, VoIP security research for TippingPoint, and founded the VIPER Lab VoIP vulnerability research group at Sipera Systems. Before Sipera, Dustin was a Security Research Scientist for Citadel Security Software (acquired by McAfee) responsible for vulnerability analysis, research, and remediation within the scope of the Linux, Solaris, AIX, and HP/UX platforms.

PART

F0rb1dd3n

1

This page intentionally left blank

A NEW ASSIGNMENT

Thursday, 9:24 a.m.

Stepan Senn looked up at the clear, blue sky of a fall morning. He could hear the crunch of dry grass beneath him as he turned his head slightly. The cool air on his face felt sharp against the hot blood that trickled from the corner of his mouth that was quickly swelling. He tried to sit up, but his body wouldn't obey. There was a sharp sound of metal on metal. The sound was familiar, but his mind wasn't working fast enough to recognize his situation. He craned his neck as he struggled to look above him. He saw legs, a hard face looking down at him, and a gun. The shape of the gun seemed to grow large enough to fill all he could see.

Everything began to spin in his mind. He closed his eyes hard against the image.

◖◗◖◗◖◗

"Sir? Excuse me, sir?" A hand touched Stepan on the shoulder and he jolted awake. "I'm sorry, I didn't mean to startle you."

"No problem." Stepan replied automatically as he picked up the briefcase he had just kicked over. He hadn't realized how tired he was after staying up late the last couple of nights.

"Sir, I believe your flight is boarding."

Stepan looked blearily at the Aeroflot gate agent. As his brain came back into focus, he stood.

"Thank you," he replied as he gathered his briefcase and coat. He made his way down the gangway and onto the plane in a mental fog. His clouded mind began to clear as it processed the surroundings he had awakened to find.

Stepan Senn's job had taken him all over the world. He had flown in many types of aircraft, but the Russian Tupolev 154 was not his favorite. He had flown on Aeroflot a couple of years after the collapse of the U.S.S.R. He remembered back then all the staff put on a good show, but the aircraft itself had looked tired. The exterior paint was faded and chipped. The interior was worn. Seats were dirty. Even the crew's