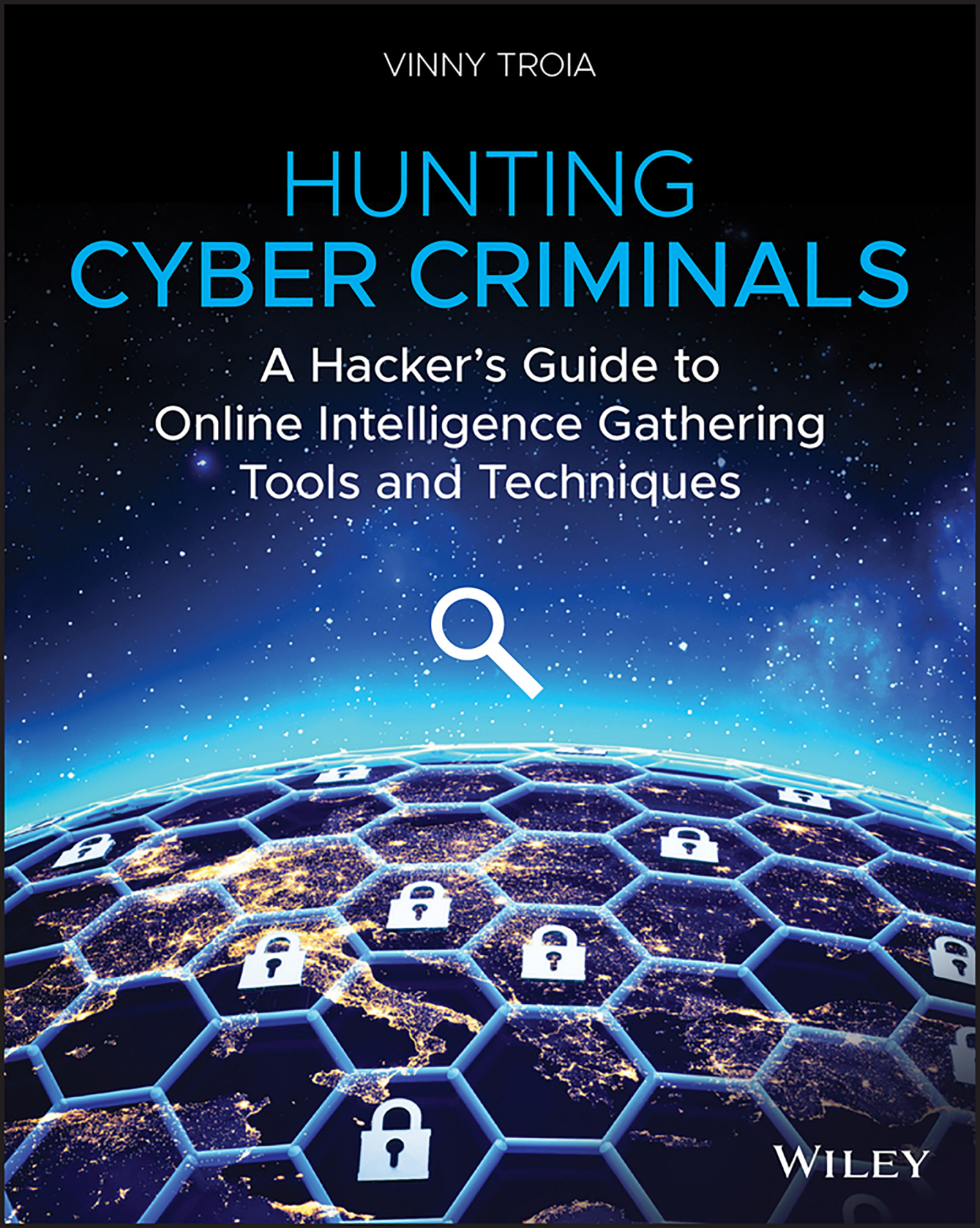
VINNY TROIA

HUNTING CYBER CRIMINALS

A Hacker's Guide to Online Intelligence Gathering Tools and Techniques



WILEY

Hunting Cyber Criminals

Hunting Cyber Criminals

A Hacker's Guide to Online Intelligence Gathering Tools and Techniques

Vinny Troia, PhD

WILEY

ISBN: 978-1-119-54092-2
ISBN: 978-1-119-54089-2 (ebk)
ISBN: 978-1-119-54099-1 (ebk)

Manufactured in the United States of America

Library of Congress Control Number: 2019940773

To my beautiful daughter, Aria, and my incredible wife, Jess. I never realized what a joy it would be to become a father, and I am thankful every day that you have both given me the most amazing gift of my life.

About the Author

Vinny Troia, PhD, CEH, CHFI, currently serves as head of Night Lion Security, a St. Louis–based cybersecurity consulting firm dedicated to providing top-tier ethical hacking and risk management services.

Troia has been recognized as a thought leader in cybersecurity and has become a go-to media expert for security-related discussions about major corporate data breaches, cyber law and legislation, airline and automobile hacking, and cyber-related scandals.

His experience in IT security stems from a lifetime of coding, complex problem solving, and self-taught computer skills. Troia now travels the globe speaking at conferences and security-related events and spends most of his free time hunting for data breaches and infiltrating private criminal circles on the darkweb.

With each new breach, valuable clues are left behind as to the evolution of an attacker's methods. During his speeches, Troia uses that information to teach and inform others on ways to increase their defenses and put necessary response strategies in place for when incidents do occur.

Prior to starting Night Lion Security, Troia spent nearly a decade working on security- and risk-related projects for the U.S. Department of Defense.

Troia holds a PhD from Capella University and is a Certified Ethical Hacker and Certified Hacking Forensic Investigator.

For more information, including samples of Troia's talks, please visit `www.vinnytroia.com`.

You can also connect with Vinny on LinkedIn at `https://linkedin.com/in/vinnytroia` or via Twitter at `http://www.twitter.com/vinnytroia`.

About the Technical Editor

Rhia Dancel conducts information security assessments throughout the United States, focusing on OSINT and risk-based management platforms with key engagements within the DoD and private sector space.

Rhia's technical and analytical background originated from a chemistry degree applied within the pharmaceutical industry for over 15 years. Rhia now supports organizations in their effort to implement security controls and achieve information security objectives across multiple security programs. Rhia also continues to provide technical input on risk- and security-based projects.

Acknowledgments

I would like to acknowledge and graciously thank the following people:

My Wife, for putting up with my countless sleepless nights and non-stop obsessing while I worked to crack this puzzle.

Bev Robb, without you, I don't think I would have been able to solve the mystery of TDO. Sometimes the most random connections and pieces of information can lead to the most significant discoveries, and that is exactly what happened. Thank you so much for putting up with my millions of questions and late-night text messages. I am eternally grateful to you and hope I can one day repay the favor.

Christopher Meunier, for never letting go of that easily identifiable chip on your shoulder that relentlessly muttered statements like this, giving me all the motivation I needed to keep pressing on:

> *whitepacket@xmpp.is: I'm sorry man but you sound like you're either LE or a f***ing retard, probably the latter.*

Dennis Karvouniaris, Thanks for all the info and help you gave me along the way. I'm sorry things had to work out this way. I always enjoy our chats and hope that by the time you read this you will have taken my advice.

Chris "The Human Hacker" Hadnagy, for believing in me enough to connect me with the fine folks at Wiley, ultimately landing me this book deal.

Alex Heid and Jesse Burke, for all the back and forth and continued help pulling some of these pieces together.

And to all of this book's guest experts, I can't thank you enough for volunteering your time to contribute your stories and opinions for this book. I will be giving you all proper credits in the first chapter, but I had to give you all an extra shout-out here as well.

Contents at a Glance

Contents

Prologue

One of the more recent investigations I worked on involved the hack of a multi-billion dollar organization. Their stolen data was posted for sale in private circles, and upon finding this out, I immediately contacted the organization. The organization had many questions, and given my prior investigative work, I was able to reach out to the threat actor on their behalf and obtain information on how the breach occurred.

The following text is a portion of the writeup provided by NSFW, *a threat actor we will be covering in much greater detail throughout this book*, where he describes, in detail, how he was able to hack this organization's network. The process he used was sophisticated, and by no means a run-of-the-mill drive-by hack.

This was very well planned and executed.

All identifying information has been changed.

HACK WRITEUP: NSFW

Firstly I realised that GitHub is adding new device verification within the week, therefore I tried to identify as many developers as possible and sign into their GitHub account to access organisation private repo's.

I then identified software developers working for Company using LinkedIn. Partially doxing each one to obtain Gmail accounts, I found Bob.

Performing database lookups in hope for password reuse (or rules to be applied to their previous password) in order to login with valid credentials.

The way I got into the GitHub was due to Bob, who reused the password "BobsTiger66" (Which GitHub had told was insecure with a red banner, yet he chose to ignore it), and was reused on multiple private databases and one public database (ArmorGames).

Once logged in I had to act quick to avoid GitHub's new ML algorithm to lock accounts out of using new IPs, so I immediately used ssh-keygen to add a new public SSH key to the user profile, I had realised you had added Okta SSO preventing the clone of private repos, in order to bypass this I looked at potential integrations.

CircleCI is a popular CI/CD tool which is inherently linked to organisations via either SSH key linkage or PAT's, therefore I realised the build processes could be exploited in order to obtain private repos, however this was not needed. You guys had added a weird implementation of Okta STS with AWS, producing time-limited tokens, I realised these were spawned everytime a new build process was triggered, therefore I accessed Circle debug mode and managed to extract these time limited tokens, and used them to download your internal datalakes.

Unfortunately these tokens were not given any further privileges, therefore you got lucky or else I would have gained access to RDS via CLI and cloned a snapshot.

When I read this, I was immediately impressed by the level of effort he put into the hack. And despite the outcome, the client was, too.

In the end, this breach had a happy ending, because I was able to provide useful intel to the customer that allowed them to identify how the breach happened, and to also put in proper safeguards to ensure that this did not happen again.

That's ultimately the point, right?

Not to provide customers with a useless writeup of generic TTPs (tactics, techniques, and procedures) regarding assumed threat actors—which is what so many threat intelligence companies do—but to actually provide useful context for how a threat actor breaches their systems.

So many companies just rely on providing existing reports on threat actor groups and never actually get to the core of how an attack happened. Sometimes it takes actually hunting down the threat actors and speaking to them directly. They are usually pretty open and willing to brag about how they did it, because on some level all hackers want to be famous; and as we will see in future chapters, *vanity always trumps OPSEC* (operational security).

In this particular case, I was already speaking to NSFW about several other hacks he is associated with, so it was no issue to ask how he was able to pull this off.

And if you are paying close attention, you will have noticed several misspellings and important "tells" associated with his writeup. Common misspellings or even regional differences in spelling (e.g., organisation vs. organization) can be very important investigative clues that we will discuss in future chapters.

But before we dive into all that, I feel it is important to shed some light on who I am, so you can get to know me a little better, understand what makes me tick, and maybe get accustomed to some of the dry humor and sarcasm that you will find sprinkled throughout this book.

My Story

When I started writing this book, I asked myself a simple question: Am I qualified to write this book? To this day, my answer is still "probably not." I don't believe one person can know everything there is to know about a topic, which is why you will find tips and stories from other industry experts throughout this book.

I admire and respect each of the people that I have asked to contribute to this book. I know their work firsthand, which is why I feel they each bring their own unique perspective that complements and reinforces the topics I will be putting forward.

But before we get to that, here is some insight into who I am and what makes me tick.

History

I was about 10 years old when my dad brought home an IBM PS/2. I had no idea what it was or what it could do, but I was mesmerized. This was before the Windows 3.1 days. I remember turning it on and staring at a DOS prompt and just hacking my way through it. The whole thing was like a giant puzzle, which is probably why it sucked me in.

I am a huge puzzle junkie. The more complex, the better. One of my strengths (and also admittedly a weakness) is that I can be relentless when I am trying to find a solution to a complex problem. Some have referred to this behavior as "obsessive." I get it, and I acknowledge the behavior.

There are nights where I am still cranking away at 4 a.m. because I just can't stop. It's part of who I am, and it is a big part of why I feel that I am very good at what I do—whether that be trying to hack into a system or assembling the story behind a criminal investigation.

Roots and Raves

In case you are wondering, I started out my career as a web developer writing HTML and JavaScript in the late '90s. I grew up in New Jersey and was always into electronic music. Naturally, I was also entranced with the rave culture. Nightclubs like Limelight and Tunnel were the big thing, and I wanted to be a part of it.

Unfortunately these clubs had a 21+ age requirement, which was a problem because I was 16. So I taught myself HTML and offered to build a free website for one of the club's resident DJs. From then on, I could just walk in with him because I was his "web guy." Problem solved.

Penetration testing is not much different, which is why I have been doing it (in one form or another) all my life. It's all a matter of understanding what the rules are, then figuring out a way to circumvent them.

I have always been good at finding ways to get around the rules, which I think is a trait shared by most penetration testers.

Don't get me wrong, rules are important. Some people like living their lives in a well-defined sandbox, while others enjoy the challenge of trying to find ways to break out of it. I am the latter.

Developing a Business Model (with Lasers!!)

One evening circa 2011, I was browsing the Internet the same way most people do: with Burp suite active and running passive recon on all sites that I visited.

I was telling my wife about an awesome site that sells high-powered lasers in different colors, hoping she would let me buy one. That was a hard no, but much to my surprise, Burp suite found a passive SQL injection vulnerability in the site.

I had to check it out, and before I knew it, I was able to see the site's user accounts with hashed passwords. Logging in to the site with one of the admin accounts meant having to crack the admin's password hash, which wasn't difficult using any number of online hash crackers given that the password was some variation of Admin123.

I logged in to the site and voilà! I had full access to everything. System records, user accounts, order information, and all.

NOTE **Yes, I now realize this action was not exactly "legal," but don't judge. We all have to start somewhere. Plus, this story has a happy ending.**

It was that exact moment that I felt the entrepreneurial spark. What if I could take this information and give it to the site's owners so they could fix the injection bug, preventing others from accessing the site in the same way? Surely they would repay this random act of kindness with some of their badass high-power lasers?

I am now the proud owner of a 2,000mW blue laser, and a 1,000mW green laser! Nice, right? The lasers actually burn stuff. They are pretty bad-ass.

More importantly, the site closed the SQL injection vulnerability, and I had a model for a business to provide services that could actually help people.

In the process, I also learned an extremely valuable lesson: If you hack into a website first, *then* try to offer the solution to the customer and ask for a "tip" in the form of a product from their website, it could be interpreted as extortion.

Oops. That clearly wasn't my intent, which I think came off in my email with the CEO, but looking back, I am sure I could have been in some trouble. So while this particular exercise worked out well for everyone, I clearly had to do some work in refining the business model.