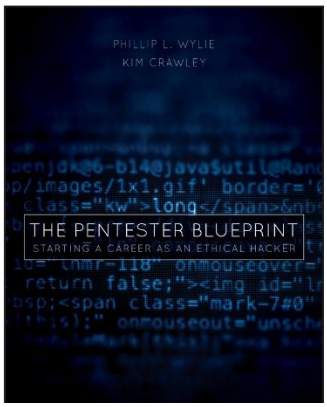

The Pentester BluePrint:
Starting a Career as an Ethical Hacker

By Phillip L. Wylie, Kim Crawley
https://www.wiley.com/en-us/The+Pentester+BluePrint%3A+Starting+a+Career+as+an+Ethical+Hacker-p-9781119684374

If you've ever considered pursuing a career in cyber security, especially penetration testing (or pentesting), ethical hacking, or whatever the kids are calling it these days, *The Pentester BluePrint: Starting a Career as an Ethical Hacker* is the perfect place to begin. Reading this book won't get you a job. However, what it will do is give you direction. It's a roadmap (er…blueprint) for getting started.

My first job in cyber security was as a technical writer with a team of pentesters. As a technical writer, I was never required to be trained in the field in which I was working. Solid communication skills and an aptitude for learning have opened plenty of doors for me. During my time with the security team, I was continually blown away by the work they did. It was really amazing watching them in action. I knew then that I wanted to be a pentester. How to get started, though? It seemed like all of the job openings required experience, and no one was offering training. I kept wondering how I could get experience. You can't get a job without experience, and you can't get experience without a job. What a conundrum!

How could I learn to do all of the amazing (and honestly, really cool!) things the testers were doing? There was really no guide that I could find. There were of course plenty of hacking and security tool reference guides. But all of those assumed that the reader was already skilled. There was no guide on how to get started. After earning some security certifications and gaining experience in incident handling, GRC, and other aspects of security (while still employed as a technical writer), I found a great entry-level security analyst position. My new boss paid for beginner penetration testing training through eLearnSecurity. I got my first real hands-on penetration testing training there. When my employer needed someone to start testing our web applications, I jumped on the opportunity and have since tested dozens of applications.

I may have taken the long way to get where I am. Honestly, I feel like I've been making this (my security career) up as I went along, always learning, listening, making plenty of mistakes, and growing. Had I had a book like *The Pentester BluePrint* to follow, I might have been able to start learning sooner, stay focused, and start my pentesting career earlier. I just didn't know where or how to start.

I met Phillip Wylie in 2019 at the BSides security conference in San Antonio, TX. Phillip was hosting a workshop on web application penetration testing. I was excited about getting some hands-on training from a professional, even if only for a few hours. Later, I watched several of Phillip's webinars, one being *The Pentester BluePrint*, for which this book is named. For the webinar, Phillip outlined the high-level steps required to prepare for a career as a pentester. I really learned a lot from that talk. Later, I took

Phillip's *Web Application Penetration Testing* course at Richland College (now Dallas College). Phillip knows his material, and he knows how to communicate it.

Earlier in 2020, Phillip announced that he was writing a book based on his *The Pentester BluePrint* conference talk. This was a great idea, because it allowed him to move beyond the confines of a one-hour discussion and go into greater detail. And through collaboration with cyber security journalist Kim Crawley, they did just that. They expanded Phillip's one-hour talk into a full 172-page book. I was already familiar with Kim's work, having read several of her articles. Her writing style is very clear, concise, and on point, and it shows in this book. It's not just a checklist, however. It feels like the authors are speaking directly to the reader and sharing their knowledge and experience one-on-one the way a mentor would.

The Pentester BluePrint: Starting a Career as an Ethical Hacker opens with a wonderful forward by half of the team behind the *Tribe of Hackers* series, Marcus Carey, followed by a summary of Phillip's own experiences in the world of IT and pentesting. The book is divided into nine logically ordered chapters:

- Chapter 1: What Is a Pentester?
- Chapter 2: Prerequisite Skills
- Chapter 3: Education of a Hacker
- Chapter 4: Education Resources
- Chapter 5: Building a Pentesting Lab
- Chapter 6: Certifications and Degrees
- Chapter 7: Developing a Plan
- Chapter 8: Gaining Experience
- Chapter 9: Getting Employed as a Pentester

In reading this book, you'll gain a solid understanding of what penetration testing is and why penetration tests are important and necessary. You'll learn about different types of security testing (e.g., vulnerability scanning, web apps, IoT, physical, Red Team, etc.). You'll also get a good general cyber security education. You'll learn about the types of skills (e.g., networking, operating systems, social engineering, etc.) you'll need to acquire if you want to work in this profession.

They discuss other educational resources including certifications, penetration testing guides, and blogs. And of course, there's a lengthy discussion about setting up your own lab including descriptions of some of the more popular pentesting tools. Rounding out the book are chapters on how to create your plan to become a penetration tester, how to gain real world experience, and finally how to get an actual paying job.

This book is very well organized, well written, and easy to follow. What puts it over the top is that the authors interviewed and quoted many working cyber security professionals to learn which tools they use and how they use them, how they gained experience, how they built their pentesting labs, and how they actually got hired as either full-time penetration testers or as security practitioners who perform penetration testing as part of their job. The interviews are not just interesting; they also express the idea that no one way is the right way. If you're interested in pursuing a career as a penetration tester, use *The Pentester BluePrint: Starting a Career as an Ethical Hacker* as your guide, but then choose the right

direction for you. As you learn more and get exposed to new technologies and ideas (or happen to witness a cool hack at BSides or on YouTube), you may realize that you want to focus on one aspect of penetration testing, such as web application or mobile penetration testing, over all of the others. You may also become more of a generalist who conducts several types of tests. But you'll have to get exposed to as many facets of the profession as possible before you can know.

Note: I'm especially excited about the interviews part, because Kim and Phillip interviewed and quoted me. I'm very proud and honored to have been a part of this excellent book.

You may look at all of this and feel overwhelmed. That's why *The Pentester BluePrint: Starting a Career as an Ethical Hacker* was written in such a logical sequence. If you're new, just start at the beginning and work your way through at your own pace. And don't be afraid to ask questions. If you already have experience, take what you need and fill in the gaps.

I hope that Kim and Phillip follow up with a second book that covers the more advanced aspects of the profession.