I'm not robot
reCAPTCHA
Continue

Black hat python: python programming for hackers and pentesters

Python hacker. These are two words you could really use to describe me. At immunity, I have the chance to work with people who, in fact, really know how to code Python. I'm not one of those people. I spend much of my time testing penetration, which requires rapid development of the Python tool, with a focus on execution and delivering results (not necessarily on beauty, optimization, or even stability). Throughout this book, you will learn that this is how I code, but I also feel that this is part of what makes me a strong Pentecostal. I hope this philosophy and style help you too. As you progress through the book, you will also realize that I don't take deep dives on a single subject. It's by design. I want to give you the bare minimum, with a little flavor, so you have some basic knowledge. With this in mind, I sprinkled ideas and homework throughout the book to launch you in your own direction. I encourage you to explore these ideas, and I would like to hear in return one of your own implementations, tools or duties that you have done. As with any technical book, readers at different levels of skill with Python (or information security in general) will experience this book differently. Some of you may just catch it and nab chapters that are relevant to a consultation concert that you are on, while others may read it cover to cover. I recommend that if you are a novice intermediate Python programmer you start at the beginning of the book and read it directly in order. You will pick up some good building blocks along the way. To begin with, I lay down some basic networking principles in Chapter 2 and slowly work our way through the raw takes in Chapter 3 and using Scapy in Chapter 4 for some more interesting network tools. The next section of the book deals with web application piracy, starting with your own custom tooling in Chapter 5, and then extending the popular burp suite in Chapter 6. From there we'll spend a lot of time talking about Trojans, starting with the GitHub command and control in Chapter 7, throughout Chapter 10 where we'll cover some Windows privilege climbing tours. The final chapter deals with the use of Volatility to automate certain offensive techniques of memory forensics. I try to keep the code samples short and in focus, and so do the explanations. If you're relatively new to Python, I encourages you to hit each line to get that muscle memory coding going. All the source code examples in this book are available at. ''' ' '