Python for Cybersecurity Cookbook

80+ practical recipes for detecting, defending, and responding to Cyber threats

Nishant Krishna

www.bpbonline.com

First published: 2024

Published by BPB Online
WeWork
119 Marylebone Road
London NW1 5PU

UK | UAE | INDIA | SINGAPORE

ISBN 978-93-55513-809

www.bpbonline.com

Dedicated to

My late father:

Dr. K. P. Krishna

who was my lifelong mentor and guide

About the Author

Nishant Krishna is an entrepreneur, writer, and inventor who loves exploring and using new ways to solve complex problems in cybersecurity, system programming, cognitive computing, computer vision, and product scaling to hyper-scale levels. He is a co-founder and CTO of a technology startup, TechMachinery Labs. He is also a co-author for *IEEE P1931.1 - Standard for an Architectural Framework for Realtime Onsite Operations Facilitation (ROOF) for IoT*, focusing on IoT security and interoperability.

In his software development career of 23 years, he has created many products from scratch, working in various technical roles in the areas of Architecture, Cybersecurity, API Development, Anti- Counterfeiting Technologies, Cloud and Virtualization, Internet of Things (IoT), and Machine Learning. Apart from his day-to-day work, he also works on core research in the areas of cybersecurity and cognitive computing. In cybersecurity, his focus is on cyber forensics and vulnerability assessment.

In his consulting role, he advises many companies in product development, threat surface reduction, database and application scalability, and using standard processes for delivering high-quality products.

Nishant is also a guest professor, teaching cybersecurity and cognitive computing to students and faculties in multiple prestigious institutions. As a part of his teaching assignments, he tries to find innovative and hands-on ways to teach complex concepts.

Nishant has a Master of Science (MS) in Software Engineering from BITS, Pilani, along with many technical certifications.

About the Reviewers

Bollepelly Arjun Goud is a hands-on cybersecurity expert with extensive experience in reconnaissance, threat hunting, and penetration testing. His exceptional skills in using complex attack vectors during penetration testing activities demonstrate a deep understanding of cybersecurity methodologies. Arjun's proactive approach to threat hunting allows him to identify vulnerabilities before they can be exploited, while his expertise in cyber forensics aids in precise digital evidence analysis. Beyond his technical prowess, Arjun's love for reading comics, non-fiction, and IT-related books fuels continuous learning, enabling him to stay at the forefront of the ever-evolving cybersecurity landscape. With a passion for knowledge and a dedication to his craft, Arjun is a valuable asset to any team focused on cybersecurity defense, making him an excellent fit for penetration testing, threat hunting, cyber forensics, and reconnaissance endeavors.

Sowjanya Kotha is an experienced engineer with a rich background in security and platform domains. Her primary expertise lies in designing robust and reliable user identity verification and access control methods. She is also skilled in platform development, including frameworks, utilizing her solid problem-solving abilities to create efficient and user-friendly solutions. Her primary focus is designing secure on-prem and cloud solutions using Kubernetes and Golang, complementing her foundation in the networking domain. Beyond her professional pursuits, Sowjanya nurtures a fervent passion for art and craftworks, showcasing her creative talents.

Acknowledgements

I want to express my deepest gratitude to my family and friends for their unwavering support and encouragement throughout this book's writing, especially my wife, Parimita, and my brother Prashant. I will always be thankful to my late father, who, as a prolific writer himself, inspired me in considering writing this book.

I am also grateful to BPB Publications for their guidance and expertise in bringing this book to fruition. It was a long journey of revising this book, with valuable participation and collaboration of reviewers, technical experts, and editors.

I would like to acknowledge the valuable contributions of my colleagues and co-worker during many years working in the tech industry, who have taught me so much and provided valuable feedback on my work.

I would also like to acknowledge the valuable contribution of the technical reviewers of this book, Sowjanya Kotha and Arjun Bollepelly. They have reviewed the book for technical errors and have given important suggestions to improve the quality of the book

Finally, I would like to thank all the readers who have taken an interest in my book and for their support in making it a reality. Your encouragement has been invaluable.

Preface

Python is a versatile language and is used in general-purpose applications as well as in specific use cases. Since the creation of Python, it has been used in various applications and use cases by software developers and researchers alike. These applications include system-level applications, APIs (Application Programming Interfaces), e-commerce applications, database applications, and, more recently, data science and cybersecurity applications.

In this book, you will get an in-depth understanding of writing Python code for solving simple to moderate complexity problems in cybersecurity. We will start with simple problems in reconnaissance and then slowly experiment with advanced cybersecurity techniques in forensics analysis or cyber forensics, penetration testing, malware analysis, and many more such areas.

After completing this book, the readers will be confident in solving problems and creating solutions. They should also be able to work as cybersecurity professionals. The readers will benefit from this book's hands-on knowledge and activities, irrespective of their current level. Parte superior do formulárioParte inferior do formulário

Chapter 1: Getting Started - briefly covers the important cybersecurity concepts relevant to this book. This chapers covers setting up the development environment so you can perform all the hands-on activities and assignments in this book.

Chapter 2: Passive Reconnaissance – presents a detailed overview of passive reconnaissance that is used to gain as much information as possible for the target systems and devices without active engagement. The information is mainly aggregated from what is available to the public. This chapter will examine simple techniques for such passive reconnaissance operations, followed by more advanced techniques to gain additional information about the target system.

Chapter 3: Active Reconnaissance - presents a detailed overview of active reconnaissance that is used to gain as much information as possible for the target systems and devices using active engagement, like port scans. This information is aggregated by actively working with the target system. This chapter will look at simple techniques for such active reconnaissance operations, followed by more advanced techniques to gain additional information about the target system.

Chapter 4: Development Environment for Advanced Techniques - covers setting up the development environment so that you can perform all the hands-on activities and assignments for the advanced cybersecurity techniques.

Chapter 5: Forensic Analysis – looks at various aspects of forensic analysis that can be used to look for and analyze digital evidence for exposure or compromise using various techniques like log analysis, event/incident analysis, dumping memory, CPU, process, and so on. Forensic analysis plays a major role while dealing with cybercrime. This chapter covers how Python can be used to write forensic analysis modules and interface with forensic analysis tools.

Chapter 6: Metadata Extraction and Parsing – is dedicated to discussing metadata that is "data about data" and can give much more information about a file or wired/wireless communication. Metadata extraction and parsing give any cybersecurity professional many "hidden" insights, which can then be applied in passive and active reconnaissance techniques. This chapter discusses the important aspects and techniques for metadata extraction and parsing.

Chapter 7: Malware and Phishing Analysis – explains in detail malware and phishing as hidden threats that can compromise a target system with a supposedly harmless operation done by the owner. This chapter covers how to analyze Malware and Phishing based compromise techniques.

Chapter 8: Working with Wireless Devices - discusses how common wireless devices like phones, tablets, and laptops can be at risk when good security practices are not followed. In this chapter, we analyze various ways a malicious actor can gather information about wireless devices and compromise them.

Chapter 9: Working with Network Utilities – is dedicated to network utilities that are tools of the trade for cybersecurity professionals. They can make complex tasks like traffic analysis and sniffing easy for a cybersecurity professional. This chapter covers network utilities that are important for anyone to know.

Chapter 10: Source Code Review and Reverse Engineering – discusses the importance of code review to help cybersecurity professionals understand open source tools and hence create his/her own techniques, including new utilities using the source code. Reverse engineering helps get insights into tools and files for which source code is unavailable. Both of these are essential approaches. We cover how to use these approaches during analysis and testing.

Chapter 11: System Hardening, Discovery, and Implementation – covers system hardening as the method of removing unused and weak processes, ports, and

modules from the system. A hardened system is one of the simplest ways to deter malicious actors from attacking a system. This chapter covers the techniques for discovering the current state of system hardening and implementation techniques for various hardening-related controls.

Chapter 12: Defensive Security Techniques – covers defensive security techniques essential for implementing proactive and preventive security measures. Starting from controls for checking malicious and repeated logins to throttling a DoS attack to logging essential events, they go a long way in fulfilling the security goals of an organization. This chapter covers such techniques and their importance in overall security posture.

Chapter 13: Offensive Security Techniques and Pen Testing – covers offensive security techniques and pen testing (short for penetration testing) methods for cybersecurity professionals to mimic the behavior of an attacker. This helps them to bring out the shortcoming and vulnerabilities in a controlled environment well in advance where there is no real damage done and the product teams can fix them. This chapter covers the basic techniques for offensive security and pen testing, followed by more advanced techniques.

Code Bundle and Coloured Images

Please follow the link to download the
Code Bundle and the ***Coloured Images*** of the book:

https://rebrand.ly/p7nhx5s

The code bundle for the book is also hosted on GitHub at **https://github.com/bpbpublications/Python-for-Cybersecurity-Cookbook**. In case there's an update to the code, it will be updated on the existing GitHub repository.

We have code bundles from our rich catalogue of books and videos available at **https://github.com/bpbpublications**. Check them out!

Errata

We take immense pride in our work at BPB Publications and follow best practices to ensure the accuracy of our content to provide with an indulging reading experience to our subscribers. Our readers are our mirrors, and we use their inputs to reflect and improve upon human errors, if any, that may have occurred during the publishing processes involved. To let us maintain the quality and help us reach out to any readers who might be having difficulties due to any unforeseen errors, please write to us at :

errata@bpbonline.com

Your support, suggestions and feedbacks are highly appreciated by the BPB Publications' Family.

Piracy

If you come across any illegal copies of our works in any form on the internet, we would be grateful if you would provide us with the location address or website name. Please contact us at **business@bpbonline.com** with a link to the material.

If you are interested in becoming an author

If there is a topic that you have expertise in, and you are interested in either writing or contributingd to a book, please visit **www.bpbonline.com**. We have worked with thousands of developers and tech professionals, just like you, to help them share their insights with the global tech community. You can make a general application, apply for a specific hot topic that we are recruiting an author for, or submit your own idea.

Reviews

Please leave a review. Once you have read and used this book, why not leave a review on the site that you purchased it from? Potential readers can then see and use your unbiased opinion to make purchase decisions. We at BPB can understand what you think about our products, and our authors can see your feedback on their book. Thank you!

For more information about BPB, please visit **www.bpbonline.com**.

Join our book's Discord space

Join the book's Discord Workspace for Latest updates, Offers, Tech happenings around the world, New Release and Sessions with the Authors:

https://discord.bpbonline.com

Table of Contents

Chapter 1
Getting Started

Introduction

Python is a versatile language which is used in general-purpose applications and in specific use cases. Since the creation of Python language, it has been used in a wide array of applications and use cases by software developers and researchers. These applications include system-level applications, **Application Programming Interfaces** (**APIs**), e-commerce applications, database applications, and, more recently, data science and cybersecurity applications.

In this book, you will get an in-depth understanding of writing Python code for solving simple to moderate complexity problems in cybersecurity. We will start with simple reconnaissance problems and slowly experiment with advanced cybersecurity techniques in forensics, penetration testing, malware analysis, and many more.

This chapter introduces you to essential concepts of cybersecurity. You will find them useful irrespective of your current level of knowledge in this area.

Structure

In this chapter, we will discuss the following topics:

- Why read this book
- How to make the best use of this book
- Basic cybersecurity concepts and techniques
- Setting up your Python development environment
- Installing Python
- Ethics for a cybersecurity professional
- Licensing considerations for cybersecurity tools

Objectives

This chapter will briefly cover the essential cybersecurity concepts relevant to this book. We will also cover setting up the development environment so you can perform all the hands-on activities and assignments in this book.

Why read this book?

Working in various areas of cybersecurity for around 15+ years now. One of the things realized is that Cybersecurity professionals do not have access to a structured way to learn new concepts, including hands-on examples that can be used right away.

Most cybersecurity professionals have a lot of information and know-how scribbled, typed, or towed away in various digital and paper notes and our brains. This information can be beneficial for anyone, either starting in the cybersecurity field or looking for a structured way to learn new concepts without getting into complex explanations. This book provides a structured way to learn the concepts indispensable for any cybersecurity professional. Moreover, as a cybersecurity professional, you will be able to use the code examples given in this book to perform manual security testing on your target system. Finishing the activities after each of the recipes can help you go one step further and enhance the recipe to something you can use as part of your job function.

This book will give you an in-depth understanding of writing Python code for solving simple to moderate complexity problems in cybersecurity. We will start with simple problems in reconnaissance and slowly experiment with advanced cybersecurity techniques in forensics, penetration testing, malware analysis, and many more such

areas. We will also look at a wide array of techniques a cybersecurity professional, or a researcher will generally use in their day-to-day work. Due to the book's structure, faculties who teach cybersecurity at the entry level and students learning cybersecurity will also benefit from this book.

This book focuses on hands-on with 100+ recipes in a cookbook style. An explanation for each of these recipes is given as inline documentation in the Python code and part of the recipe.

How to make the best use of this book?

Cybersecurity is just like any other area that requires regular practice to become an expert.

Following are some of the important points to keep in mind while using this book as a tool toward expertise in cybersecurity:

- Read the introduction to each of the recipes to understand the problem we are trying to solve or the insight we are trying to get.
- Try out all the programs in the recipe using your favorite Integrated Development Environment (IDE), as discussed later in this chapter.
- Try to relate one recipe with other recipes in the book and visualize how you can put them together to solve a complex problem.

All the code in this book is also available in the Git repository of BPB Publications and is under MIT License. You can use them to learn and create something useful without worrying about any licensing implications.

Basic cybersecurity concepts

Let us discuss about the basic Cybersecurity concepts that are essential to working with the subsequent chapters, where we discuss specific concepts in detail.

What is cybersecurity

Cybersecurity is the practice of securing, protecting, and defending computer systems, electronic systems, networks, network devices, mobile devices, applications, and sensitive data from cyberattacks by malicious actors. The attackers or malicious actors take advantage of the design flaws of the system or network or else try to brute force their way into it. Such attacks aim to compromise security and privacy by unauthorized access to sensitive information, tampering with or destroying the system, or even blocking access to the system and its contents. Cybersecurity mainly deals with digital data.

Difference between cybersecurity and information security

Information Security (or InfoSec) is synonymous in most contexts. However, it focuses on protecting any type of data, not just digital data. Information Security also deals with compliance and policies to protect the data and not just the techniques.

Hence, cybersecurity can be thought of as a subset of Information Security. Information Security is the overarching area covering a wide array of security-related considerations, including Cybersecurity, Encryption, Disaster Recovery, and so on.

Reconnaissance

Reconnaissance is the process or operation of gathering or collecting as much information as possible about the target system.

Passive reconnaissance is done without active engagement or interaction with the target system. That means the information (or intelligence) is gathered from open, public, and passive sources. The owners of the system may never know if someone (a person) or something (a program) is collecting data about their system. Since the data is collected from public and passive sources, it may be outdated or obsolete, and a lot has changed since the time the information was collected and made available publicly. Sometimes the information about the target system is made available intentionally or unintentionally by the parent company.

In active reconnaissance, active engagement with the target system is done to gather information. This may include port scanning, performing HTTP requests, performing handshakes using proprietary protocols, and so on. Since this type of reconnaissance operation is done with direct interaction with the system, the system owners may detect these operations and take severe actions against you. Thus, active reconnaissance should be performed only on those systems which is either set up by you in your lab or the target systems for which you have received permissions from their owners.

We will discuss these in detail in *Chapter 2: Passive Reconnaissance* and in *Chapter 3: Active Reconnaissance.*

Forensic analysis

Forensic analysis (also known as forensics) is a science in itself in the area of cybersecurity. Many of us know about it from the inaccurate dramatization in thriller and science fiction movies.