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

1. Getting Started **1**
Introduction 1
Structure 2
Objectives 2
Why read this book? 2
How to make the best use of this book? 3
Basic cybersecurity concepts 3
What is cybersecurity *3*
Difference between cybersecurity and information security *4*
Reconnaissance *4*
Forensic analysis *4*
Metadata *5*
Malware *5*
Phishing *6*
System hardening *6*
Defensive security *7*
Offensive security *7*
Pen testing or penetration testing *7*
Why cybersecurity? 8
Operating system considerations for your Python development environment 9
Configuring your Python development environment 10
Installing Python 10
Installing a distribution like Anaconda *12*
Configuring your IDE *13*
Using Python virtual environment (venv) *14*
Configuring important libraries *14*
Testing sample programs to confirm that everything is configured well *15*
Ethics for cybersecurity professionals 16
Licensing considerations for cybersecurity tools 17
Conclusion 17
Questions 17

2. Passive Reconnaissance 19
Introduction 19
Structure 19
Objectives 20
A note on using passive reconnaissance to access target system information 20
Using "whois" to get information about an IP address or domain name 20
Recipe *20*
Activity *23*
Using "dig" to get information about an IP address or domain name 24
Recipe *25*
Activity *26*
Using "nslookup" to get information about an IP address or domain name 26
Recipe *26*
Activity *27*
Using the Google Hacking database to get vulnerabilities and exploit information about your target system and devices 27
Recipe *28*
Activity *33*
Using Google Search to get vulnerabilities and exploit information about your target system and devices 33
Recipe *33*
Activity *35*
Connecting with Shodan and getting detailed information about a target system using Shodan API 35
Recipe *36*
Activity *43*
Parsing information returned by Shodan 44
Recipe *44*
Activity *45*
Connecting with Censys and getting detailed information about a target system using Censys API 45
Recipe *46*
Activity *54*

Parsing information returned by Censys 54
Recipe *54*
Activity *55*
Connecting with IPinfo and getting detailed information about a target system using IPinfo API 55
Recipe *56*
Activity *58*
Parsing information returned by IPInfo 58
Recipe *58*
Activity *59*
Connecting with APIVoid and getting IP Reputation (is IP address blacklisted) details 59
Recipe *60*
Activity *64*
Checking the domain reputation using APIVoid 64
Recipe *65*
Activity *69*
Checking DNS records using APIVoid 70
Recipe *70*
Activity *72*
Checking SSL Information using APIVoid 72
Recipe *72*
Activity *76*
Using crt.sh to get certificate information about a domain 77
Recipe *77*
Activity *84*
Conclusion 84
Questions 85
Points to remember 85
Key terms 85
3. Active Reconnaissance 87
Introduction 87
Structure 87
Objectives 88

A note on using active reconnaissance to access target system information 88
Running the Python programs which need access to internal system features 88
Using ping to check connectivity to the target system 88
Recipe *89*
Activity *90*
Finding details about your network interfaces and ports using netstat 90
Recipe *90*
Activity *93*
Using traceroute to find out the hops to a target system 93
Recipe *93*
Activity *95*
A simple example of printing the content of a website using Web scraping 96
Recipe *97*
Activity *100*
Examples of what you can find out about a website using Web scraping 100
Recipe *100*
Crawling a website 107
Recipe *108*
Activity *111*
Scanning for open ports and services using nmap 111
Recipe *112*
Activity *120*
Discovering ciphers on a host using nmap 120
Recipe *121*
Activity *124*
Discovering hosts on a network using nmap 124
Recipe *125*
Activity *128*
Conclusion 128
Questions 128
Points to remember 129
Key terms 129

4. Development Environment for Advanced Techniques.....131
Introduction.....131
Structure.....132
Objectives.....132
Concepts related to creating your own cybersecurity lab.....132
Virtualization.....*132*
Hypervisor.....*132*
Virtual machine.....*133*
Target system.....*135*
Attack surface.....*135*
Vulnerable or exploitable VM.....*135*
Kali Linux.....*136*
Creating Python Virtual Environment.....136
Testing Python Virtual Environment.....139
Activity.....*140*
Development environment for advanced cybersecurity techniques.....141
Cybersecurity Lab on Hyper-V.....143
Cybersecurity lab on VirtualBox.....146
Using traceroute to find out the hops to the local VMs.....147
Recipe.....*147*
Conclusion.....149
Questions.....150
Points to remember.....150
Key terms.....150
5. Forensic Analysis.....151
Introduction.....151
Structure.....152
Objectives.....152
Understanding how to interface with "Wireshark" in Python.....152
Installing Wireshark.....*153*
Recipe.....*154*
Activity.....*159*
Creating a simple live network packet capturer using "Wireshark".....159
Recipe.....*160*

Activity *167*
Capturing network packets to a file using "Wireshark" 167
Recipe *167*
Activity *169*
Packet capture file analysis using "Wireshark" 169
Recipe *169*
Activity *173*
Analysing network packets using "tcpdump" 174
Installing tcpdump *174*
Recipe *175*
Activity *177*
Using Web scraping in forensic analysis 177
Recipe *178*
Activity *181*
Various logs, which can be used for forensic analysis, on Linux 181
Recipe *182*
Activity *183*
Various logs, which can be used for forensic analysis, on Windows 183
Recipe *184*
Activity *193*
Creating an Audit Trail of the system 193
Recipe *194*
Activity *195*
Using Exif data to analyze information about images, sound and other media format 195
Recipe *196*
Activity *200*
Identifying malicious actors, configuration, device type, and so on by using fingerprinting data 200
Recipe *201*
Activity *202*
Using process dumps in forensic analysis 202
Recipe *203*
Activity *207*
Creating a rudimentary Digital Forensics and Incident Response (DFIR) 208

Recipe *208*
Activity *213*
Conclusion 213
Questions 214
Points to remember 214
Key terms 215
6. Metadata Extraction and Parsing 217
Introduction 217
Structure 217
Objectives 217
Getting and parsing HTTP Response Headers for a target system or website 218
Recipe *219*
Activity *221*
Interpreting the vulnerabilities and weaknesses using HTTP Response Headers 221
Recipe *221*
Activity *224*
Parsing protocol headers for a few of the common protocols 224
Recipe *226*
Activity *232*
Interpreting other protocol header information 232
Recipe *233*
Activity *236*
Using simple techniques for file metadata extraction 236
Recipe *238*
Activity *242*
Using the metadata extracted from the files for reconnaissance and other insights 242
Recipe *243*
Activity *245*
Conclusion 245
Questions 245
Points to remember 246
Key terms 246

7. Malware and Phishing Analysis.....247
Introduction.....247
Structure.....247
Objectives.....248
Understanding phishing.....248
Simple examples of using spaCy.....250
Recipe.....251
Activity.....254
Malware analysis and threat detection using spaCy.....255
Recipe.....255
Activity.....258
Using fingerprinting to do malware analysis and detection.....258
Recipe.....259
Activity.....263
A simple way to simulate phishing.....263
Recipe.....265
Activity.....270
Using Kali Linux tools to simulate phishing for well-known sites.....270
Recipe.....271
Activity.....276
Identify phishing websites using HTTP header analysis.....276
Recipe.....276
Activity.....278
Conclusion.....278
Questions.....279
Points to remember.....279
Key terms.....280
8. Working with Wireless Devices.....281
Introduction.....281
Structure.....281
Objectives.....282
Using Wireshark to perform live packet capture of wireless interfaces.....282
Recipe.....282
Activity.....289

Packet capture file analysis using Wireshark....289
Recipe....289
Activity....291
Using spaCy to perform analysis of wireless interfaces and devices....292
Recipe....292
Activity....295
Using PyrCrack for simulating monitoring of the wireless interface....295
Recipe....296
Activity....300
Understanding how sniffing wireless traffic with pyshark works....300
Recipe....300
Activity....305
Conclusion....306
Questions....306
Points to remember....306
Key terms....307
9. Working with Network Utilities....309
Introduction....309
Structure....310
Objectives....310
Sniffing packets in promiscuous mode using Wireshark....310
Understanding promiscuous mode....310
Recipe....311
Activity....316
Performing network traffic analysis using Wireshark....316
Recipe....317
Activity....325
Using Scapy as a reconnaissance tool and network scanner....326
Recipe....326
Activity....330
Using Scapy to sniff network packets....330
Recipe....330
Activity....334
Simulating ARP spoofing (ARP cache poisoning)....335

Recipe *335*
Activity *341*
Using Fierce as a reconnaissance tool for domains 341
Recipe *342*
Activity *344*
Conclusion 344
Questions 345
Points to remember 345
Key terms 346
10. Source Code Review and Reverse Engineering 347
Introduction 347
Structure 348
Objectives 348
Using published source code to create new cybersecurity tools 348
Recipe *349*
Activity *356*
Understanding the functioning of tools using source code review 357
Recipe *357*
Activity *361*
Reading the header of binary files 361
Recipe 363
Activity 366
Reverse engineering using metadata analysis 366
Recipe *367*
Activity *369*
Searching for information in binary files 369
Recipe *369*
Activity *374*
Conclusion 374
Questions 375
Points to remember 375
Key terms 375
11. System Hardening, Discovery, and Implementation 377
Introduction 377

Structure 378
Objectives 378
Interfacing with Linux default firewall using Python 378
Recipe *379*
Activity *387*
Understanding Windows "netsh" utility 387
Interfacing with Windows default firewall using Python 391
Recipe *392*
Activity *395*
Working with other third-party firewalls *395*
Getting a list of software installed on a Windows system 396
Recipe *397*
Activity *400*
Getting insights into the accounts and privileges in Linux 400
Recipe *401*
Activity *404*
Getting insights into the accounts and privileges in Linux 404
Recipe *405*
Activity *406*
Conclusion 406
Questions 407
Points to remember 407
Key terms 408
12. Defensive Security Techniques 409
Introduction 409
Structure 410
Objectives 410
Creating a simple defensive security control 410
Recipe *411*
Activity *414*
Using Python to perform proactive security measures 414
Recipe *415*
Activity *418*
Monitoring if ports are open 418

Recipe *419*
Activity *420*
Monitoring logs 421
Recipe *422*
Activity *425*
Identifying attacks 425
Recipe *426*
Activity *429*
Identifying vulnerabilities and attack surface in a system 429
Recipe *430*
Activity *435*
Checking if any exploitable package is installed on the system using the CVSS database 435
Recipe *436*
Activity *438*
Using Kismet for intrusion detection 438
Recipe *439*
Activity *442*
Conclusion 443
Questions 443
Points to remember 444
Key terms 444
13. Offensive Security Techniques and Pen Testing 445
Introduction 445
Structure 445
Objectives 446
Understanding how to use Metasploit exploit payload 446
Recipe *447*
Activity *451*
Using Metasploit exploit code to exploit a vulnerability in a target system 451
Recipe *452*
Activity *461*
Using John the Ripper to crack passwords 462
Recipe *462*

Activity *465*
Using Nmap's vulners Nmap Scripting Engine script to discover vulnerabilities 465
Recipe *466*
Activity *468*
Using Nikto for penetration testing 469
Recipe *469*
Activity *472*
Using OWASP ZAP to perform continuous pen testing 473
Recipe *473*
Activity *477*
Conclusion 477
Questions 478
Points to remember 479
Key terms 479

Index 483-490

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.