1ST EDITION

ChatGPT for Cybersecurity Cookbook

Learn practical generative AI recipes to supercharge your cybersecurity skills

CLINT BODUNGEN

Foreword by Aaron Crow, OT Cybersecurity Professional & Thought Leader
Host of PrOTect IT All Podcast

ChatGPT for Cybersecurity Cookbook

Learn practical generative AI recipes to supercharge your cybersecurity skills

Clint Bodungen

packt

ChatGPT for Cybersecurity Cookbook

Group Product Manager: Niranjan Naikwadi
Publishing Product Manager: Nitin Nainani
Book Project Manager: Aishwarya Mohan
Senior Editors: Aamir Ahmed and Nathanya Dias
Technical Editor: Simran Haresh Udasi
Copy Editor: Safis Editing
Indexer: Manju Arasan
Production Designer: Shankar Kalbhor
DevRel Marketing Coordinator: Vinishka Kalra

First published: March 2024
Production reference: 1130324

Published by Packt Publishing Ltd.
Grosvenor House
11 St Paul's Square
Birmingham
B3 1RB, UK

ISBN 978-1-80512-404-7

www.packtpub.com

To my wife, Ashley, for her unwavering support throughout the many weekends and hours burning the midnight oil for this project. To my sons, Caleb and Connor, the future is what you make of it. You can accomplish anything if you just believe.

– Clint Bodungen

Foreword

In the relentless cyber battleground, where threats morph with each tick of the clock, generative **artificial intelligence** (**AI**) emerges as our digital sentinel. ChatGPT and its kin are not mere tools; they are force multipliers in our cyber arsenals. We're talking about a paradigm shift here – generative AI doesn't just uplift; it transforms the cybersecurity landscape. It lets us run rings around potential threats, streamline security measures, and forecast nefarious plots with an astuteness that's simply otherworldly.

This isn't just tech talk; it's about real muscle in the fight against digital adversaries. Imagine crafting a cyber training regimen so robust that it catapults neophytes into seasoned defenders within the data trenches. Generative AI is that game-changer, shattering the barriers to entry, democratizing the field, and nurturing a new generation of cyber mavens.

But there's more. With generative AI, we dive into data oceans and surface with those elusive security insights – the kind that traditional tools would miss. This is about harnessing AI to not just respond to threats but also to anticipate them, to be steps ahead of the adversary. We're entering an era where our collaboration with AI amplifies our strategic nous, sharpens our foresight, and fortifies our resilience.

As we join forces with AI, we're not just bolstering defenses; we're fostering a culture of cybersecurity innovation. We're empowering minds to push beyond the conventional, to envision a digital realm where safety is the norm, not the exception. This book is a testament to that vision, a guide on wielding AI's might to safeguard our cyber frontiers. Welcome to the future – a future where we stand united with AI in the vanguard of cybersecurity.

Aaron Crow

OT Cybersecurity Professional & Thought Leader

Host of PrOTect IT All Podcast

Contributors

About the author

Clint Bodungen is a globally recognized cybersecurity professional and thought leader with 25+ years of experience, and author of *Hacking Exposed: Industrial Control Systems*. He is a U.S. Air Force veteran, has worked for notable cybersecurity firms Symantec, Booz Allen Hamilton, and Kaspersky Lab, and is a co-founder of ThreatGEN, a cybersecurity gamification and training firm. Clint has been at the forefront of integrating gamification and AI into cybersecurity with his flagship product, *ThreatGEN® Red vs. Blue*, the world's first online multiplayer computer game designed to teach real-world cybersecurity. Clint continues his pursuit to help revolutionize the cybersecurity industry using gamification and generative AI.

I would first like to thank my amazing team at Packt Publishing for their patience and their trust in me to write this book. And special thanks to the cybersecurity community and the pioneers of the AI industry.

About the reviewers

Aaron Shbeeb is a lifelong programmer, cybersecurity enthusiast, and game developer. He has programmed in over a dozen programming languages both personally and professionally. He has also worked as a penetration tester and vulnerability researcher. Lately, his passion has been for developing *ThreatGEN® Red vs. Blue*, a cybersecurity training video game that he co-founded/co-developed with Clint Bodungen. Developing that game allows him to practice some of his favorite parts of software development such as system design, machine learning, and AI.

Pascal Ackerman, a principal security consultant, began his career in IT in 1999. He is a seasoned industrial security professional with a degree in electrical engineering and experience in industrial network design and support, information and network security, risk assessments, penetration testing, threat hunting, and forensics. His passion lies in analyzing new and existing threats to **Industrial Control System** (**ICS**) environments and he fights cyber adversaries both from his home base and while traveling the world with his family as a digital nomad.

Bradley Jackson navigates the intricate world of cybersecurity with a quiet dedication to Python and emerging technologies. His journey, though marked by meaningful professional accomplishments, finds its truest joy in life's simpler facets. At heart, Bradley is a family man, deeply devoted to his wife Kayla and their four children. This grounding influence of family life in Arkansas beautifully complements his thoughtful contributions to the *ChatGPT for Cybersecurity Cookbook*, reflecting a blend of practical wisdom with a down-to-earth approach to technology.

Table of Contents

7

Threat Monitoring and Detection 221

8

Incident Response 253

9

Using Local Models and Other Frameworks 277

10

The Latest OpenAI Features 305

Preface

In the ever-evolving domain of cybersecurity, the advent of generative AI and **large language models** (**LLMs**), epitomized by the introduction of ChatGPT by OpenAI, marks a significant leap forward. This book, dedicated to the exploration of ChatGPT's applications within cybersecurity, embarks on a journey from the tool's nascent stages as a basic chat interface to its current stature as an advanced platform reshaping cybersecurity methodologies.

Initially conceptualized to aid AI research through the analysis of user interactions, ChatGPT's journey from its initial release in late 2022 to its current form illustrates a remarkable evolution in a span of just over a year. The integration of sophisticated features such as web browsing, document analysis, and image creation through DALL-E, combined with advancements in speech recognition and text-to-image understanding, has transformed ChatGPT into a multi-faceted tool. This transformation is not merely technical but extends into functional realms, potentially significantly impacting cybersecurity practices.

A key facet in ChatGPT's evolution was the incorporation of code completion and debugging functionalities, which expanded its utility across technical domains, particularly in software development and secure coding. These advancements have significantly enhanced coding speed and efficiency and have effectively democratized programming skills and accessibility.

The Advanced Data Analysis feature (formerly known as Code Interpreter) has further opened new avenues in cybersecurity. It enables professionals to rapidly analyze and debug security-related code, automate the creation of secure coding guidelines, and develop custom security scripts. The capability to process and visualize data from diverse sources, including documents and images, and to generate detailed charts and graphs, transforms raw data into actionable cybersecurity insights.

ChatGPT's web-browsing capabilities have greatly enhanced its role in cybersecurity intelligence gathering. By enabling professionals to extract real-time threat information from a broad spectrum of online sources, ChatGPT facilitates a rapid response to emerging threats and supports informed strategic decision-making. This synthesis of data into concise, actionable intelligence underscores ChatGPT's value as a dynamic tool for cybersecurity experts navigating the rapidly evolving landscape of cyber threats.

Finally, this book extends beyond the confines of the ChatGPT web interface, venturing into the OpenAI API to unlock a world of possibilities, empowering you to not only utilize but also innovate with the OpenAI API. By delving into the creation of custom tools and expanding upon the inherent capabilities of the ChatGPT interface, you are equipped to tailor AI-powered solutions to their unique cybersecurity challenges.

This book serves as a quintessential guide for cybersecurity professionals looking to harness the power of ChatGPT in their projects and tasks by providing practical, step-by-step examples of how to employ ChatGPT in real-world scenarios.

Each chapter focuses on a unique facet of cybersecurity, from vulnerability assessment and code analysis to threat intelligence and incident response. Through these chapters, you are introduced to the innovative application of ChatGPT in creating vulnerability and threat assessment plans, analyzing and debugging security-related code, and even generating detailed threat reports. The book delves into using ChatGPT in conjunction with frameworks such as MITRE ATT&CK, automating the creation of secure coding guidelines, and crafting custom security scripts, thereby offering a comprehensive toolkit for enhancing cybersecurity infrastructure.

By integrating the advanced capabilities of ChatGPT, this book not only educates but also inspires professionals to explore new horizons in cybersecurity, making it an indispensable resource in the age of AI-driven security solutions.

Who this book is for

ChatGPT for Cybersecurity Cookbook is written for a diverse audience with a shared interest in the intersection of artificial intelligence and cybersecurity. Whether you are a seasoned cybersecurity professional aiming to incorporate the innovative capabilities of ChatGPT and the OpenAI API into your security practices, an IT professional eager to broaden your cybersecurity acumen with AI-powered tools, a student or emerging cybersecurity enthusiast keen on understanding and applying AI in security contexts, or a security researcher fascinated by the transformative potential of AI in cybersecurity, this book is tailored for you.

The content is structured to accommodate a spectrum of knowledge levels, initiating you with fundamental concepts before advancing to sophisticated applications. This inclusive approach ensures the book's relevance and accessibility to individuals across various stages of their cybersecurity journey.

What this book covers

Chapter 1, *Getting Started: ChatGPT, the OpenAI API, and Prompt Engineering*, introduces ChatGPT and the OpenAI API, laying the foundation for leveraging generative AI in cybersecurity. It covers the basics of setting up an account, mastering prompt engineering, and utilizing ChatGPT for tasks including code writing and role simulation, setting the stage for more advanced applications in subsequent chapters.

Chapter 2, *Vulnerability Assessment*, focuses on enhancing vulnerability assessment tasks, guiding you through using ChatGPT to create assessment plans, automate processes with the OpenAI API, and integrate with frameworks including MITRE ATT&CK for comprehensive threat reporting and analysis.

Chapter 3, *Code Analysis and Secure Development*, delves into the **secure software development lifecycle** (**SSDLC**), showing how ChatGPT can streamline the process from planning to maintenance. It highlights the use of AI in crafting security requirements, identifying vulnerabilities, and generating documentation to improve software security and maintainability.

Chapter 4, *Governance, Risk, and Compliance (GRC)*, offers insights into using ChatGPT for enhancing cybersecurity governance, risk management, and compliance efforts. It covers generating cybersecurity policies, deciphering complex standards, conducting cyber risk assessments, and creating risk reports to strengthen cybersecurity frameworks.

Chapter 5, *Security Awareness and Training*, focuses on leveraging ChatGPT in cybersecurity education and training. It explores creating engaging training materials, interactive assessments, phishing training tools, exam preparation aids, and employing gamification to enhance learning experiences in cybersecurity.

Chapter 6, *Red Teaming and Penetration Testing*, explores AI-enhanced techniques for red teaming and penetration testing. It includes generating realistic scenarios using the MITRE ATT&CK framework, conducting OSINT reconnaissance, automating asset discovery, and integrating AI with penetration testing tools for comprehensive security assessments.

Chapter 7, *Threat Monitoring and Detection*, addresses the use of ChatGPT in threat intelligence analysis, real-time log analysis, detecting **advanced persistent threats** (**APTs**), customizing threat detection rules, and using network traffic analysis to improve threat detection and response capabilities.

Chapter 8, *Incident Response*, focuses on utilizing ChatGPT to enhance incident response processes, including incident analysis, playbook generation, root cause analysis, and automating report creation to ensure efficient and effective responses to cybersecurity incidents.

Chapter 9, *Using Local Models and Other Frameworks*, investigates the use of local AI models and frameworks in cybersecurity, highlighting tools such as LMStudio and Hugging Face AutoTrain for privacy-enhanced threat hunting, penetration testing, and sensitive document review.

Chapter 10, *The Latest OpenAI Features*, provides an overview of the most recent OpenAI features and their applications in cybersecurity. It emphasizes leveraging ChatGPT's advanced capabilities for cyber threat intelligence, security data analysis, and employing visualization techniques for a deeper understanding of vulnerabilities.

To get the most out of this book

To maximize the benefits derived from this book, you are encouraged to possess the following:

- A foundational grasp of cybersecurity principles, including prevalent terminology and best practices, to contextualize the applications of ChatGPT within the security landscape. (*This book is not intended to be an introduction to cybersecurity.*)

- An understanding of programming fundamentals, particularly in Python, as the book employs Python scripts extensively to demonstrate interactions with the OpenAI API.
- Proficiency with command-line interfaces and a rudimentary knowledge of networking concepts, essential for executing the practical exercises and understanding the cybersecurity applications discussed.
- A basic familiarity with web technologies such as HTML and JavaScript, which underpin several web application security and penetration testing examples presented in the book.

Software/hardware covered in the book	**OS requirements**
Python 3.10 or higher	Windows, macOS, and Linux (any)
A code editor (such as VS Code)	Windows, macOS, and Linux (any)
A command-line/terminal application	Windows, macOS, and Linux (any)

If you are using the digital version of this book, we advise you to type the code yourself or access the code via the GitHub repository (link available in the next section). Doing so will help you avoid any potential errors related to the copying and pasting of code.

> **Important note**
> Generative AI and LLM technology is evolving extremely fast, so much so that in some cases you will discover that some examples in this book might already be outdated and not function as intended due to recent API and/or AI model updates, and even the ChatGPT web interface itself. As such, it is imperative to reference the most recent code and notes for this book from the official GitHub repository. Every effort will be made to keep the code up to date in order to reflect the latest changes and updates by OpenAI and other technology providers used throughout this book.

Download the example code files

You can download the example code files for this book from GitHub at `https://github.com/PacktPublishing/ChatGPT-for-Cybersecurity-Cookbook`. If there's an update to the code, it will be updated on the existing GitHub repository.

We also have other code bundles from our rich catalog of books and videos available at `https://github.com/PacktPublishing/`. Check them out!

Code in Action

Code in Action videos for this book can be viewed at (`https://bit.ly/3uNma17`).

Conventions used

There are a number of text conventions used throughout this book.

`Code in text`: Indicates code words in text, database table names, folder names, filenames, file extensions, pathnames, dummy URLs, user input, and Twitter handles. Here is an example: "If you are using a different shell configuration file, replace `~/.bashrc` with the appropriate file (for example, `., ~/.zshrc` or `~/.profile`)."

A block of code is set as follows:

```
import requests
url = "http://localhost:8001/v1/chat/completions"
headers = {"Content-Type": "application/json"}
data = { "messages": [{"content": "Analyze the Incident Response Plan
for key strategies"}], "use_context": True, "context_filter": None,
"include_sources": False, "stream": False }
response = requests.post(url, headers=headers, json=data)
result = response.json() print(result)
```

Bold: Indicates a new term, an important word, or words that you see onscreen. For example, words in menus or dialog boxes appear in the text like this. Here is an example: "In the **System Properties** window, click the **Environment Variables** button."

> **Tips or important notes**
>
> Appear like this.

Sections

In this book, you will find several headings that appear frequently (*Getting ready*, *How to do it...*, *How it works...*, *There's more...*, and *See also*).

To give clear instructions on how to complete a recipe, use these sections as follows:

Getting ready

This section tells you what to expect in the recipe and describes how to set up any software or any preliminary settings required for the recipe.

How to do it...

This section contains the steps required to follow the recipe.

How it works...

This section usually consists of a detailed explanation of what happened in the previous section.

There's more...

This section consists of additional information about the recipe in order to make you more knowledgeable about the recipe.

See also

This section provides helpful links to other useful information for the recipe.

Get in touch

Feedback from our readers is always welcome.

General feedback: If you have questions about any aspect of this book, mention the book title in the subject of your message and email us at `customercare@packtpub.com`.

Errata: Although we have taken every care to ensure the accuracy of our content, mistakes do happen. If you have found a mistake in this book, we would be grateful if you would report this to us. Please visit `www.packtpub.com/support/errata`, selecting your book, clicking on the Errata Submission Form link, and entering the details.

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 `copyright@packt.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 contributing to a book, please visit `authors.packtpub.com`.

Share Your Thoughts

Once you've read *ChatGPT for Cybersecurity Cookbook*, we'd love to hear your thoughts! Please click here to go straight to the Amazon review page for this book and share your feedback.

Your review is important to us and the tech community and will help us make sure we're delivering excellent quality content.

Download a free PDF copy of this book

Thanks for purchasing this book!

Do you like to read on the go but are unable to carry your print books everywhere?

Is your eBook purchase not compatible with the device of your choice?

Don't worry, now with every Packt book you get a DRM-free PDF version of that book at no cost.

Read anywhere, any place, on any device. Search, copy, and paste code from your favorite technical books directly into your application.

The perks don't stop there, you can get exclusive access to discounts, newsletters, and great free content in your inbox daily

Follow these simple steps to get the benefits:

1. Scan the QR code or visit the link below

`https://packt.link/free-ebook/9781805124047`

2. Submit your proof of purchase
3. That's it! We'll send your free PDF and other benefits to your email directly

1

Getting Started: ChatGPT, the OpenAI API, and Prompt Engineering

ChatGPT is a **large language model** (**LLM**) developed by **OpenAI**, which is specifically designed to generate context-aware responses and content based on the prompts provided by users. It leverages the power of **generative AI** to understand and respond intelligently to a wide range of queries, making it a valuable tool for numerous applications, including cybersecurity.

> **Important note**
>
> **Generative AI** is a branch of **artificial intelligence** (**AI**) that uses **machine learning** (**ML**) algorithms and **natural language processing** (**NLP**) to analyze patterns and structures within a dataset and generate new data that resembles the original dataset. You likely use this technology every day if you use autocorrect in word processing applications, mobile chat apps, and more. That said, the advent of LLMs goes far beyond simple autocomplete.
>
> LLMs are a type of generative AI that are trained on massive amounts of text data, enabling them to understand context, generate human-like responses, and create content based on user input. You may have already used LLMs if you have ever communicated with a helpdesk chatbot.
>
> **GPT** stands for **Generative Pre-Trained Transformer** and, as the name suggests, is an LLM that has been pre-trained to improve accuracy and/or provide specific knowledge-based data generation.

ChatGPT has raised concerns about plagiarism in some academic and content-creation communities. It has also been implicated in misinformation and social engineering campaigns due to its ability to generate realistic and human-like text. However, its potential to revolutionize various industries cannot be ignored. In particular, LLMs have shown great promise in more technical fields, such as programming and cybersecurity, due to their deep knowledge base and ability to perform complex tasks such as instantly analyzing data and even writing fully functional code.

In this chapter, we will guide you through the process of setting up an account with OpenAI, familiarizing yourself with ChatGPT, and mastering the art of prompt engineering (the key to leveraging the real power of this technology). We will also introduce you to the OpenAI API, equipping you with the necessary tools and techniques to harness ChatGPT's full potential.

You'll begin by learning how to create a ChatGPT account and generate an API key, which serves as your unique access point to the OpenAI platform. We'll then explore basic ChatGPT prompting techniques using various cybersecurity applications, such as instructing ChatGPT to write Python code that finds your IP address and simulating an AI CISO role by applying ChatGPT roles.

We'll dive deeper into enhancing your ChatGPT outputs with templates to generate comprehensive threat reports, as well as formatting output as tables for improved presentation, such as creating a security controls table. As you progress through this chapter, you'll learn how to set the OpenAI API key as an environment variable to streamline your development process, send requests and handle responses with Python, efficiently use files for prompts and API key access, and effectively employ prompt variables to create versatile applications, such as generating manual pages based on user inputs. By the end of this chapter, you'll have a solid understanding of the various aspects of ChatGPT and how to utilize its capabilities in the cybersecurity domain.

> **Tip**
>
> Even if you are already familiar with the basic ChatGPT and OpenAI API setup and mechanics, it will still be advantageous for you to review the recipes in *Chapter 1* as they are almost all set within the context of cybersecurity, which is reflected through some of the prompting examples.

In this chapter, we will cover the following recipes:

- Setting up a ChatGPT Account
- Creating an API Key and interacting with OpenAI
- Basic prompting (Application: Finding Your IP Address)
- Applying ChatGPT Roles (Application: AI CISO)
- Enhancing Output with Templates (Application: Threat Report)
- Formatting Output as a Table (Application: Security Controls Table)
- Setting the OpenAI API Key as an Environment Variable

- Sending API Requests and Handling Responses with Python
- Using Files for Prompts and API Key Access
- Using Prompt Variables (Application: Manual Page Generator)

Technical requirements

For this chapter, you will need a **web browser** and a stable **internet connection** to access the ChatGPT platform and set up your account. Basic familiarity with the Python programming language and working with the command line is necessary as you'll be using **Python 3.x**, which needs to be installed on your system so that you can work with the OpenAI GPT API and create Python scripts. A **code editor** will also be essential for writing and editing Python code and prompt files as you work through the recipes in this chapter.

The code files for this chapter can be found here: `https://github.com/PacktPublishing/ChatGPT-for-Cybersecurity-Cookbook`.

Setting up a ChatGPT Account

In this recipe, we will learn about generative AI, LLMs, and ChatGPT. Then, we will guide you through the process of setting up an account with OpenAI and exploring the features it offers.

Getting ready

To set up a ChatGPT account, you will need an active email address and a modern web browser.

> **Important note**
> Every effort has been made to ensure that every illustration and instruction is correct at the time of writing. However, this is such a fast-moving technology and many of the tools used in this book are currently being updated at a rapid pace. Therefore, you might find slight differences.

How to do it...

By setting up a ChatGPT account, you'll gain access to a powerful AI tool that can greatly enhance your cybersecurity workflow. In this section, we'll walk you through the steps of creating an account, allowing you to leverage ChatGPT's capabilities for a range of applications, from threat analysis to generating security reports:

1. Visit the OpenAI website at `https://platform.openai.com/` and click **Sign up**.
2. Enter your email address and click **Continue**. Alternatively, you can register with your existing Google or Microsoft account:

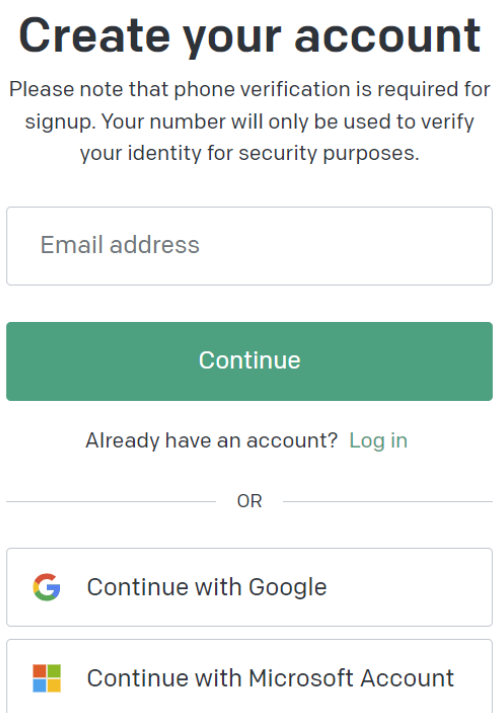

Figure 1.1 – OpenAI signup form

3. Enter a strong password and click **Continue**.
4. Check your email for a verification message from OpenAI. Click the link provided in the email to verify your account.
5. Once your account has been verified, enter the required information (first name, last name, optional organization name, and birthday) and click **Continue**.
6. Enter your phone number to verify by phone and click **Send code**.
7. When you receive the text message with the code, enter the code and click **Continue**.
8. Visit and bookmark `https://platform.openai.com/docs/` to start becoming familiar with OpenAI's documentation and features.

How it works...

By setting up an account with OpenAI, you gain access to the ChatGPT API and other features offered by the platform, such as **Playground** and all available models. This enables you to utilize ChatGPT's capabilities in your cybersecurity operations, enhancing your efficiency and decision-making process.

There's more...

When you sign up for a free OpenAI account, you get $18 in free credits. While you most likely won't use up all of your free credits throughout the recipes in this book, you will eventually with continued use. Consider upgrading to a paid OpenAI plan to access additional features, such as increased API usage limits and priority access to new features and improvements:

- **Upgrading to ChatGPT Plus**:

  ChatGPT Plus is a subscription plan that offers additional benefits beyond free access to ChatGPT. With a ChatGPT Plus subscription, you can expect faster response times, general access to ChatGPT even during peak times, and priority access to new features and improvements (this includes access to GPT-4 at the time of writing). This subscription is designed to provide an enhanced user experience and ensure that you can make the most out of ChatGPT for your cybersecurity needs.

- **Benefits of having an API key**:

  Having an API key is essential for utilizing ChatGPT's capabilities programmatically through the OpenAI API. With an API key, you can access ChatGPT directly from your applications, scripts, or tools, enabling more customized and automated interactions. This allows you to build a wide range of applications, integrating ChatGPT's intelligence to enhance your cybersecurity practices. By setting up an API key, you'll be able to harness the full power of ChatGPT and tailor its features to your specific requirements, making it an indispensable tool for your cybersecurity tasks.

> **Tip**
> I highly recommend upgrading to ChatGPT Plus so that you have access to GPT-4. While GPT-3.5 is still very powerful, GPT-4's coding efficiency and accuracy make it more suited to the types of use cases we will be covering in this book and with cybersecurity in general. At the time of writing, there are also other additional features in ChatGPT Plus, such as the availability of plugins and the code interpreter, which will be covered in later chapters.

Creating an API Key and interacting with OpenAI

In this recipe, we will guide you through the process of obtaining an OpenAI API key and introduce you to the OpenAI Playground, where you can experiment with different models and learn more about their capabilities.

Getting ready

To get an OpenAI API key, you will need to have an active OpenAI account. If you haven't already, complete the *Setting up a ChatGPT account* recipe to set up your ChatGPT account.

How to do it...

Creating an API key and interacting with OpenAI allows you to harness the power of ChatGPT and other OpenAI models for your applications. This means you'll be able to leverage these AI technologies to build powerful tools, automate tasks, and customize your interactions with the models. By the end of this recipe, you will have successfully created an API key for programmatic access to OpenAI models and learned how to experiment with them using the OpenAI Playground.

Now, let's proceed with the steps to create an API key and explore the OpenAI Playground:

1. Log in to your OpenAI account at `https://platform.openai.com`.
2. After logging in, click on your **profile picture/name** in the top-right corner of the screen and select **View API keys** from the drop-down menu:

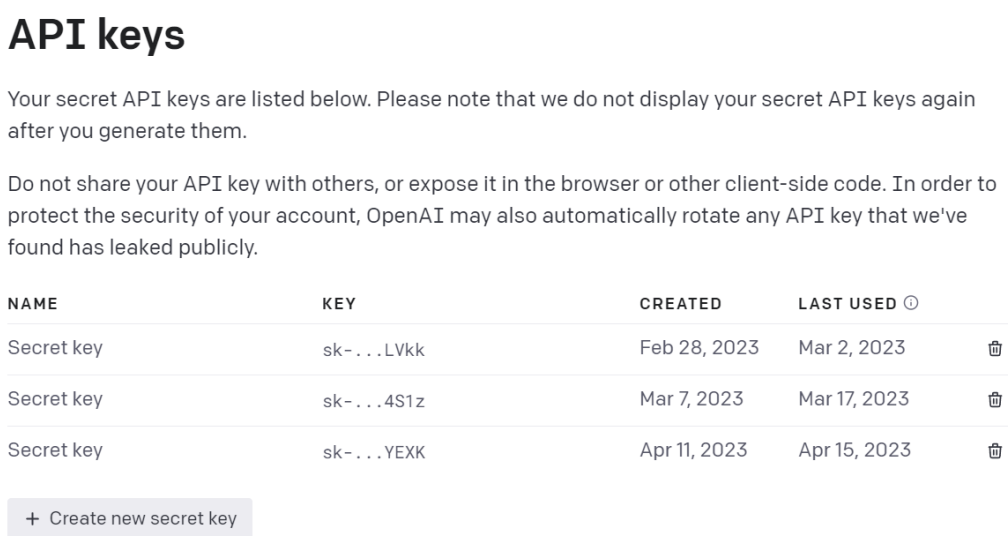

Figure 1.2 – The API keys screen

3. Click the **+ Create new secret key** button to generate a new API key.
4. Give your API key a name (optional) and click **Create secret key**:

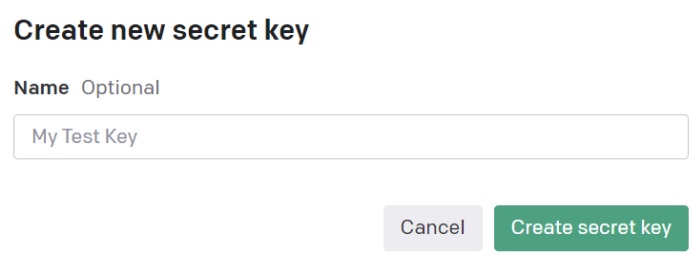

Figure 1.3 – Naming your API key

5. Your new API key will be displayed on the screen. Click the **copy icon**, , to copy the key to your clipboard:

> **Tip**
> Save your API key in a secure location immediately as you will need it later when working with the OpenAI API; you cannot view the key again in its entirety once it has been saved.

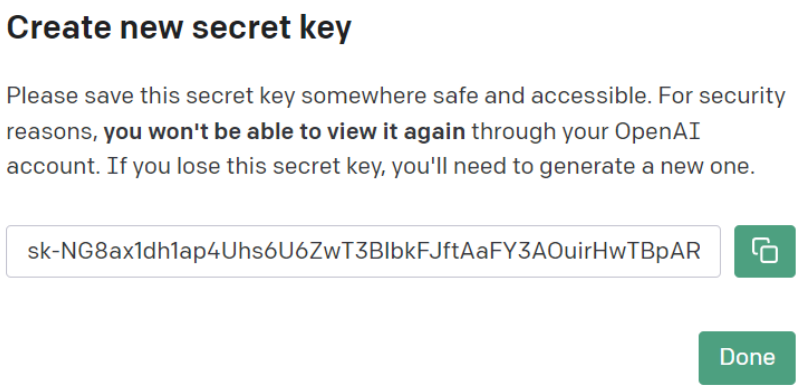

Figure 1.4 – Copying your API key

How it works...

By creating an API key, you enable programmatic access to ChatGPT and other OpenAI models through the OpenAI API. This allows you to integrate ChatGPT's capabilities into your applications, scripts, or tools, enabling more customized and automated interactions.

There's more...

The **OpenAI Playground** is an interactive tool that allows you to experiment with different OpenAI models, including ChatGPT, and their various parameters, but without requiring you to write any code. To access and use the Playground, follow these steps:

> **Important note**
> Using the Playground requires token credits; you are billed each month for the credits used. For the most part, this cost can be considered very affordable, depending on your perspective. However, excessive use can add up to significant costs if not monitored.

1. Log in to your OpenAI account.
2. Click **Playground** in the top navigation bar:

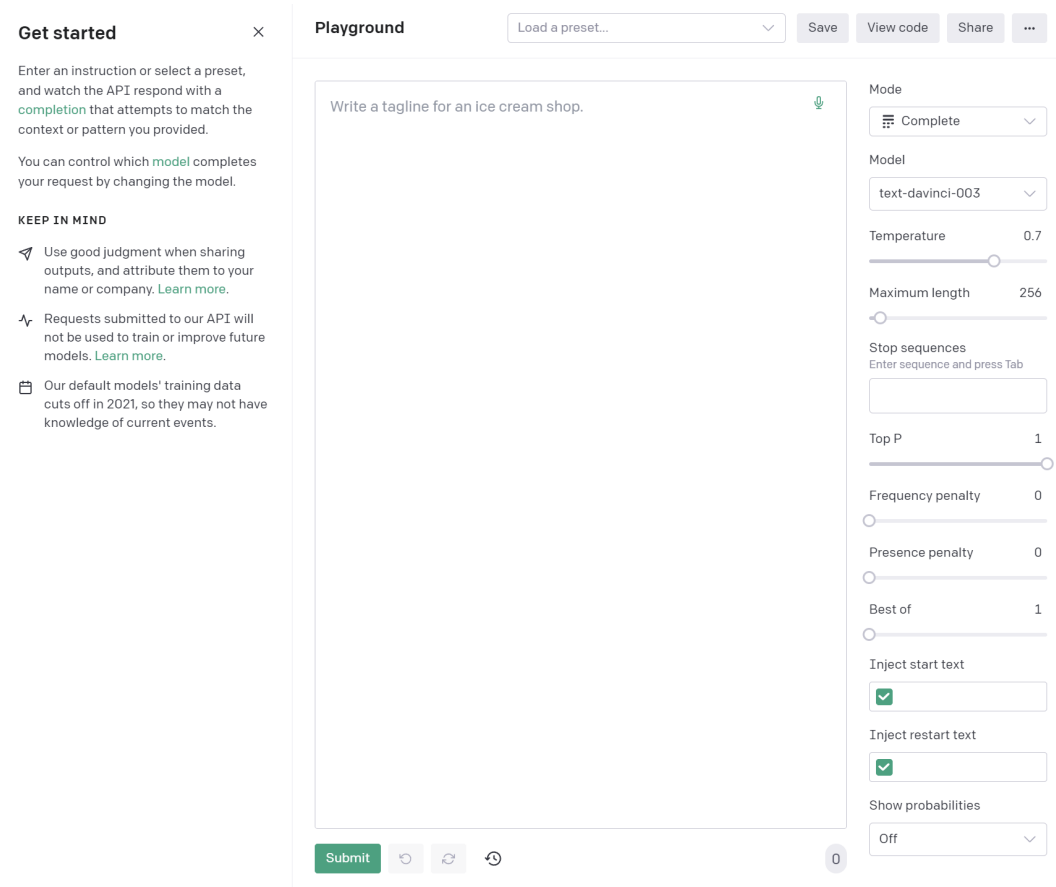

Figure 1.5 – The OpenAI Playground

3. In the Playground, you can choose from various models by selecting the model you want to use from the **Model** drop-down menu:

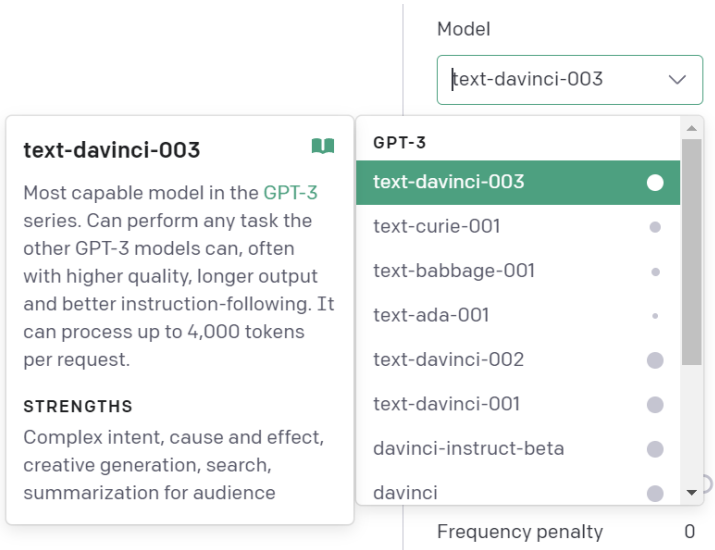

Figure 1.6 – Selecting a model

4. Enter your prompt in the textbox provided and click **Submit** to see the model's response:

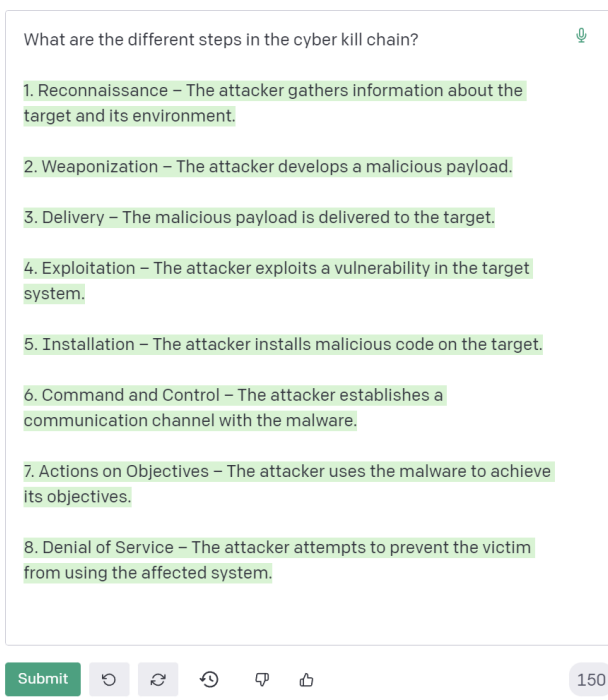

Figure 1.7 – Entering a prompt and generating a response

> **Tip**
> Even though you are not required to enter an API key to interact with the Playground, usage still counts toward your account's token/credit usage.

5. You can also adjust various settings, such as the maximum length, number of generated responses, and more, from the settings panel to the right of the message box:

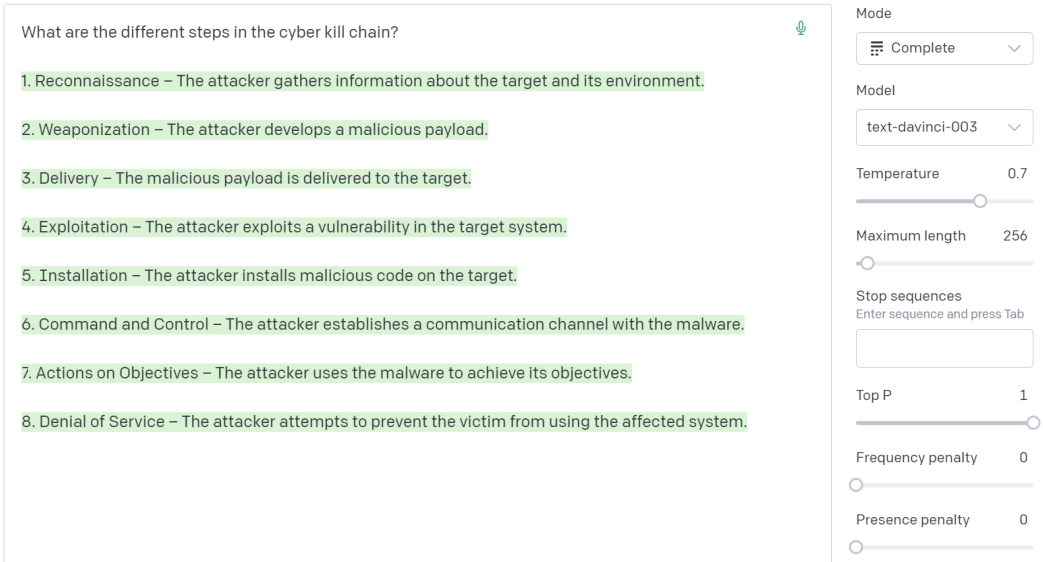

Figure 1.8 – Adjusting settings in the Playground

Two of the most important parameters are **Temperature** and **Maximum length**:

- The **Temperature** parameter affects the randomness and creativity of the model's responses. A higher temperature (for example, 0.8) will produce more diverse and creative outputs, while a lower temperature (for example, 0.2) will generate more focused and deterministic responses. By adjusting the temperature, you can control the balance between the model's creativity and adherence to the provided context or prompt.
- The **Maximum length** parameter controls the number of tokens (words or word pieces) the model will generate in its response. By setting a higher maximum length, you can obtain longer responses, while a lower maximum length will produce more concise outputs. Adjusting the maximum length can help you tailor the response length to your specific needs or requirements.

Feel free to experiment with these parameters in the OpenAI Playground or when using the API to find the optimal settings for your specific use case or desired output.

The Playground allows you to experiment with different prompt styles, presets, and model settings, helping you better understand how to tailor your prompts and API requests for optimal results:

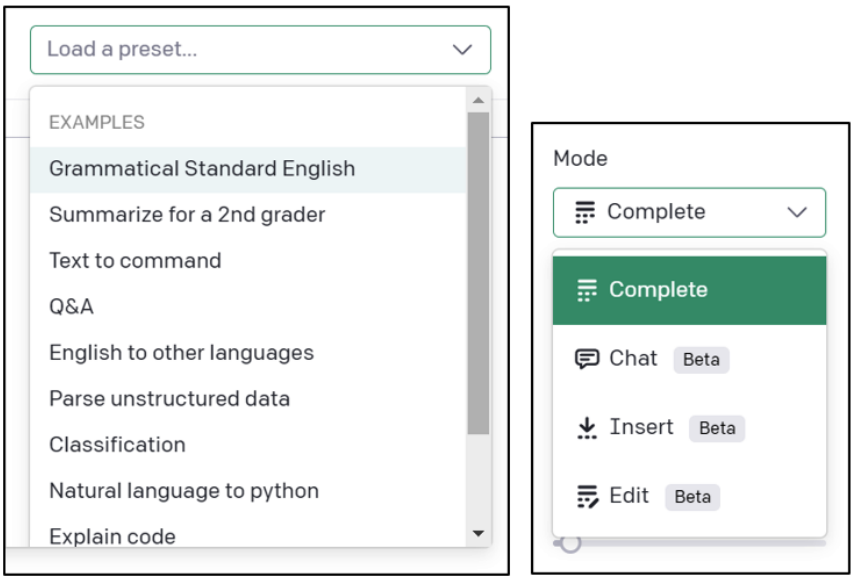

Figure 1.9 – Prompt presets and model modes

Tip

While we will be covering several of the different prompt settings using the API throughout this book, we won't cover them all. You are encouraged to review the *OpenAPI documentation* for more details.

Basic Prompting (Application: Finding Your IP Address)

In this recipe, we will explore the basics of ChatGPT prompting using the ChatGPT interface, which is different from the OpenAI Playground we used in the previous recipe. The advantage of using the ChatGPT interface is that it does not consume account credits and is better suited for generating formatted output, such as writing code or creating tables.

Getting ready

To use the ChatGPT interface, you will need to have an active OpenAI account. If you haven't already, complete the *Setting up a ChatGPT account* recipe to set up your ChatGPT account.

How to do it...

In this recipe, we'll guide you through using the ChatGPT interface to generate a Python script that retrieves a user's public IP address. By following these steps, you'll learn how to interact with ChatGPT in a conversation-like manner and receive context-aware responses, including code snippets.

Now, let's proceed with the steps in this recipe:

1. In your browser, go to `https://chat.openai.com` and click **Log in**.
2. Log in using your OpenAI credentials.
3. Once you are logged in, you will be taken to the ChatGPT interface. The interface is similar to a chat application, with a text box at the bottom where you can enter your prompts:

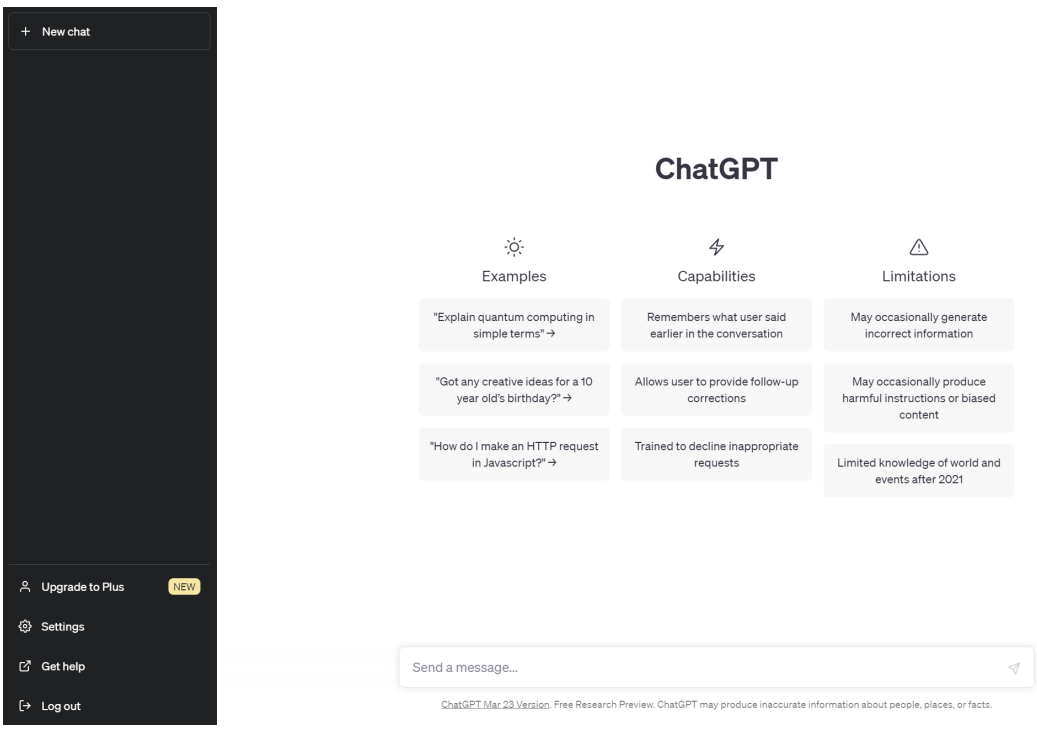

Figure 1.10 – The ChatGPT interface

4. ChatGPT uses a conversation-based approach, so you can simply type your prompt as a message and press *Enter* or click the ➤ button to receive a response from the model. For example, you can ask ChatGPT to generate a piece of Python code to find the public IP address of a user:

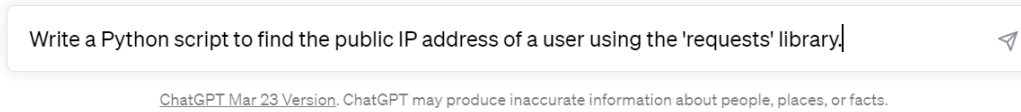

Figure 1.11 – Entering a prompt

ChatGPT will generate a response containing the requested Python code, along with a thorough explanation:

Figure 1.12 – ChatGPT response with code

5. Continue the conversation by asking follow-up questions or providing additional information, and ChatGPT will respond accordingly:

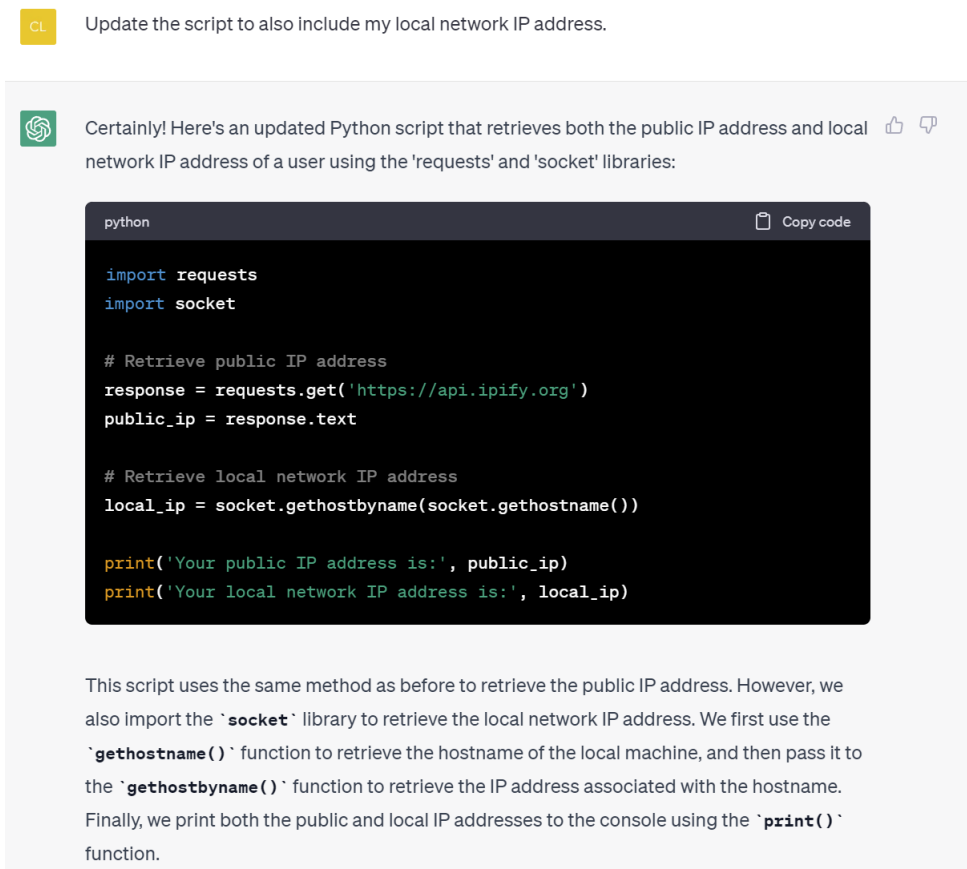

Figure 1.13 – ChatGPT contextual follow-up response

6. Run the ChatGPT-generated code by clicking on **Copy code**, paste it into your code editor of choice (I use *Visual Studio Code*), save it as a `.py` Python script, and run it from a terminal:

```
PS D:\GPT\ChatGPT for Cybersecurity Cookbook> python .\my_ip.py
Your public IP address is: [redacted]
Your local network IP address is: 192.168.1.105
```

Figure 1.14 – Running the ChatGPT-generated script