Cracking the Cybersecurity Interview

Essential strategies and learn concepts

Karl Gilbert

Sayanta Sen

www.bpbonline.com

First Edition 2024

ISBN: 978-93-55518-941

LIMITS OF LIABILITY AND DISCLAIMER OF WARRANTY

The information contained in this book is true to correct and the best of author's and publisher's knowledge. The author has made every effort to ensure the accuracy of these publications, but publisher cannot be held responsible for any loss or damage arising from any information in this book.

All trademarks referred to in the book are acknowledged as properties of their respective owners but BPB Publications cannot guarantee the accuracy of this information.

Dedicated to

My family
For their unending support, every day

- Karl Gilbert

My younger self

- Sayanta Sen

About the Authors

- **Karl Gilbert** is a seasoned cybersecurity professional with over a decade of experience in securing systems and applications from both offensive and defensive perspectives. Currently employed by a leading technology and hardware company, he plays a vital role in safeguarding their online and physical retail space against cyber attacks. With a keen interest in security research, he has uncovered multiple zero-day vulnerabilities in widely used libraries and software, earning him several Common Vulnerabilities and Exposures (CVEs). His prior roles have also seen him deeply involved in red teaming and hardware security. Beyond this, he is also extremely passionate about mentoring and sharing his knowledge with the next generation of cybersecurity professionals.

- Co-author **Sayanta Sen** has dedicated the past seven years to working with numerous corporations, helping them fortify their networks, systems, and cloud infrastructure against malicious actors and cyber-attacks. As an application and cloud security engineer, his unwavering commitment to protecting his clients' digital assets has earned him a reputation as a reliable and skilled professional. He has recently turned his focus towards security research and has already made his mark by obtaining a CVE for a widely used network library, with many more on the horizon.

About the Reviewers

- **Andre Froneman** is an accomplished Industrial Cyber Security specialist with a strong focus on digitizing and securing mining, automotive, and manufacturing environments. With a robust background in cybersecurity strategies, risk management, and industry-specific technologies, Andre brings a wealth of knowledge and hands-on experience to the table.

  Having worked extensively in the intersection of industrial operations and digital transformation, Andre has a deep understanding of the unique challenges and opportunities faced by companies in the mining, automotive, and manufacturing sectors. He is adept at developing and implementing tailored cybersecurity solutions that safeguard critical infrastructure, protect sensitive data, and ensure operational continuity in highly complex industrial environments.

  Andre works as an OT Cyber Security Specialist servicing the African market.

- **Shobhit** is the Security and compliance Director at Headspace, an on-demand mental health company in San Francisco, CA. Prior to Headspace, he worked for 12+ years in different facets of Security and information Assurance with HSBC, Deutsche Bank, Credit Suisse, PayPal, and Fidelity Investments to build and mature their security and compliance programs.

  He also works with ISACA to develop the exam questions for flagship certifications such as CISA, CISM, and CGEIT, serves as the technical reviewer for the CGEIT & CISA Review Manual, and is a published author for ISACA's COBIT 5 journal and an exam guide on CRISC. In his spare time, he likes to explore the inclined trails of the Bay Area, complete ultramarathons, blog on GRCMusings.com, and present at industry conferences.

  Shobhit completed his MS in Cybersecurity from Northeastern University, Boston, and holds CISSP, CCSP, CRISC, CISA, CISM, CGEIT, HITRUST CCSFP, ISO 27001 Lead Auditor, ISO 31000 Risk Management, and ITIL Foundation certifications.

Acknowledgements

First and foremost, I need to thank my co-author, Sayanta Sen. Your efforts and commitment to creating the best possible content have been truly remarkable. This book would not be what it is without your ideas and insightful input. Your visual representations of key concepts have made the content so much more engaging and accessible to our readers. This project is as much yours as it is mine.

To my amazing family, your unwavering support and encouragement have been the driving force behind everything I do. I am truly blessed to have you by my side, cheering me on every step of the way.

To my mentors, who have guided me throughout my journey in the industry, I cannot thank you enough. Your wisdom, expertise, and patience have shaped me into the professional I am today. I am forever indebted to you for the invaluable guidance and advice you have provided.

A special thank you to the incredible team at BPB. Your support throughout the process of writing this book has been nothing short of amazing. Your dedication and commitment to excellence have been truly inspiring, and I am grateful for the opportunity to collaborate with such a talented group of individuals.

Last but not least, I want to express my deepest gratitude to you, the readers of this book. Without your interest and passion for cybersecurity, this project would not have been possible. Your support means the world to me, and I am honored to have the opportunity to share my knowledge and experiences with you. Thank you for embarking on this journey with me, and I hope that this book serves as a valuable resource as you navigate the exciting world of cybersecurity.

- Karl Gilbert

I want to express my deepest gratitude to my friends and family for your unwavering support, love, and encouragement. To my parents, thank you for instilling in me the values of perseverance and hard work. Your love and wisdom have shaped me into who I am today. Special thanks to Kirit Sankar Gupta, whose mentorship has profoundly impacted my professional growth. Your support and insights have enriched this book in ways words cannot fully capture.

A heartfelt thank you to the incredible team at BPB. Your dedication and professionalism have not just been invaluable but have been crucial in bringing this project to completion.

I would also like to thank my mentors and colleagues for their guidance in the field of cybersecurity. This book, a testament to their influence, would not have been possible without the valuable experiences I have gained from my years in corporate. The lessons and experiences I've gained from working alongside you in the corporate world have been invaluable.

- Sayanta Sen

Preface

Welcome to the thrilling world of cybersecurity! If you are reading this book, chances are that you are either already passionate about this fascinating field or eager to explore its incredible opportunities.

As someone who has been involved in the cybersecurity industry for over a decade, we can confidently say that there has never been a better time to pursue a career in this dynamic and rapidly evolving field. With the number of unfilled cybersecurity jobs skyrocketing by 350% in just eight years and the industry set to cross the $400 billion mark by 2027, the demand for skilled professionals is at an all-time high.

But here is the thing: landing your dream job in cybersecurity is not just about having the right technical skills. It is also about being able to effectively communicate your knowledge and experience during the interview process. Throughout this book, we will take you on a comprehensive journey through the essential skills and knowledge you need to succeed in any cybersecurity interview. From the fundamentals of operating systems, networking, and coding to more specialized areas like threat modeling, application security, and incident response, we have got you covered.

To give you a taste of what is in store, here are some of the key chapters:

Chapter 1: UNIX, Linux, and Windows - In this chapter, we will explore the three most common operating systems that form the backbone of every digital ecosystem. You will gain a deep understanding of how these systems work, their various components, and how to secure them from a cybersecurity perspective.

Chapter 2: Networking, Routing, and Protocols - In this chapter, get ready to discuss the intricate world of computer networks and the protocols that keep them running. We will cover everything from the OSI model to IP addresses and network classes, empowering you with the knowledge to secure and defend these critical systems.

Chapter 3: Security of DBMS and SQL - In this chapter, we will learn how databases are the lifeblood of modern applications and explore the world of SQL and relational databases. You will learn about database security features, NoSQL databases, and how to protect against the dreaded SQL injection attack.

Chapter 4: Threat Modeling, Pentesting and Secure Coding - In this chapter, you will join us as we explore the art and science of threat modeling, penetration testing, and secure coding. You will learn how to identify potential risks, test your systems for vulnerabilities, and implement best practices to ensure your code is rock-solid.

Chapter 5: Application Security - In this chapter, we will learn that web applications are a prime target for cyber attackers, and we will arm you with the knowledge and skills to protect them. From the OWASP Top 10 to WAFs and application security layers, you will gain knowledge on how to build secure and resilient web apps.

Chapter 6: Network Security - In this chapter, we will explore network security in depth, exploring topics like network pentesting, scanning and enumeration, and post-exploitation techniques. You will also learn about firewalls, VLANs, and other defensive measures to keep your networks safe.

Chapter 7: Cloud Security - In this chapter, we will explain how the cloud has revolutionized the way we store and process data, but it also presents new security challenges. We will also explore the drivers behind cloud adoption, the various cloud services available, and how to conduct security assessments and implement defenses in the cloud.

Chapter 8: Red and Blue Teaming Activities - In this chapter, get ready to join the front lines of the cybersecurity battle as we explore the world of red and blue teaming. You will learn about adversarial simulations, the differences between red teaming and penetration testing, and how to prepare for a career in this exciting field.

Chapter 9: Security in SDLC - In this chapter, we will understand why integrating security into the software development lifecycle is crucial for building secure applications. We will also explore how to use Git to improve security, the benefits of shifting left, and how to implement secure SDLC techniques.

Chapter 10: Security in CI/CD - In this chapter, we will discuss how to secure your CI/CD pipelines, covering topics like security testing automation, supply chain attacks, and secrets management as Continuous Integration and Continuous Deployment (CI/CD) pipelines are essential for modern software development, but they also introduce new security risks.

Chapter 11: Firewalls, Endpoint Protections, Anti-Malware, and UTMs - In this chapter, we will take a comprehensive look at the various tools and technologies used to protect networks and endpoints. From firewalls and EDR to anti-malware and UTMs, you will learn how to use these tools effectively and bypass them when necessary.

Chapter 12: Security Information and Event Management - In this chapter, we will explore the purposes and utility of SIEMs, learn about the popular ELK Stack, and compare SIEMs with other enterprise security tools. SIEM systems are critical for monitoring and analyzing security events across an organization.

Chapter 13: Spreading Awareness - In this chapter, we will discuss how cybersecurity is not just the responsibility of the IT department; it is everyone's job. We will also get to learn strategies for spreading security awareness throughout your organization, including gamified learning, triage sessions, and more.

Chapter 14: Law and Compliance in Cyberspace - In this chapter, we will explore various legal frameworks and compliance standards, including HIPAA, PCI-DSS, and more. You will get to navigate the complex world of cybersecurity law, and compliance can be daunting, but it is essential for any aspiring infosec professional.

Chapter 15: Python, Bash, and PowerShell Proficiency - In this chapter, we will discover three of the most important languages for infosec: Python, Bash, and PowerShell. Scripting and automation are essential skills for any cybersecurity professional. You will learn how to use these tools for a variety of security tasks and see real-world examples of their power in action.

Coloured Images

Please follow the link to download the
Coloured Images of the book:

https://rebrand.ly/ikuz29h

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 contributing 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
UNIX, Linux, and Windows

Introduction

In this chapter, we will look at the three most common operating systems, the components that form the cornerstone of every cloud, network, system, and application—essentially everything in the digital world.

These operating systems have a number of moving parts. These primarily require a deep understanding of how the operating system works, so you have a better understanding of how to secure all of the components. As you progress through this chapter, you will gain an understanding of various operating system services, shells, and how commands get executed. In addition, you will also be able to look at all of the above from a security context.

Structure

The chapter discusses the following topics:

- Unix/Linux
- Windows

Objectives

The objective of this chapter is to help the reader gain a better understanding of how operating systems work, how the OS and its running services can be attacked, and how to better protect against such *attacks*.

Unix/Linux

Here, we will discuss concepts of UNIX-based or Linux operating systems in the following sections:

Terminal

A command line interface, the Linux terminal, is used to manage devices running Linux or UNIX operating systems. It is one of the many tools accessible to Linux/UNIX users for carrying out a given set of operations and is often regarded as the most effective approach.

The terminal has the following two major tasks:

- Take input from the user and send it to the system.
- Get output from the system and display it back to the user.

It has become so popular that Microsoft released their version of the terminal: **PowerShell**, MS's very own open-source command line. Apple switched its OS to Unix as its base and implemented the **Bash** and **Z shells** for Mac users. Here is what a shell looks like, as illustrated in *Figure 1.1*:

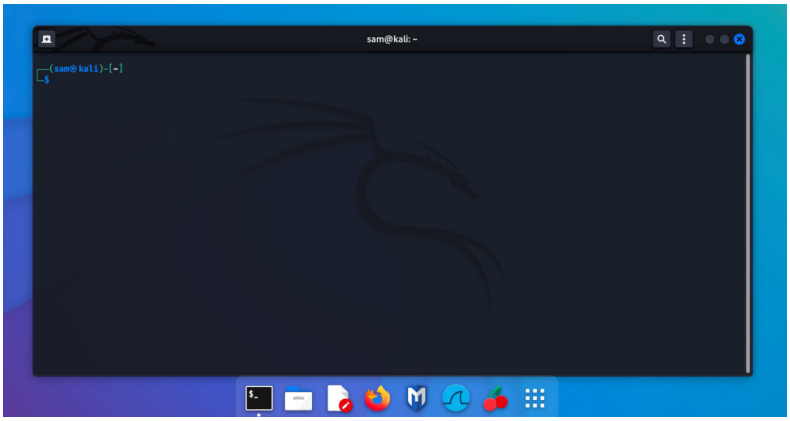

***Figure 1.1**: A shell running on Kali Linux*

Shell

A **shell** is an application that forms a bridge between the user and the system kernel. A user supplies commands to the kernel and gets the command's output in return. We can run applications and utilities on the kernel using a shell. So, a shell is a program that accepts a command from the user, checks whether the syntax is correct, and runs the program on the system. The ability to communicate with the kernel makes shells a crucial tool. Users would not be able to use the operating system's utilities without the ability to communicate with the kernel.

Types of shells

On a Linux system, there are several different shells to choose from. One or more of these shells, or a combination, are used.

Each of these shells has characteristics that set them apart from other shells for a particular application. Let us look at the various Linux shell types and their attributes and features.

The Bourne shell

The Bourne shell is recognized as the first UNIX shell created. The symbol for it is **`sh`**. It became popular mainly because of its small size and quick functioning. The Bourne shell's default path is **`/bin/sh`** and **`/sbin/sh`**. The root user is given the **`#`** prompt by default and **`$`** by default for non-root users.

The Bourne shell does have several significant flaws, however:

- Unlike most modern Linux shells, the Bourne shell cannot remember previously executed commands.
- It cannot perform logical and mathematical operations internally.
- Also, it lacks the functionality to provide a user-friendly interactive experience.

Figure 1.2 shows how **`/bin/sh`** looks like on Kali Linux:

```
┌──(sid3wind3r㉿kali)-[~]
└─$ /bin/sh
$
```

***Figure 1.2**: What /bin/sh looks like*

GNU Bourne-Again shell

The **GNU Bourne-Again shell** (**bash**), more often referred to as the **Bash shell**, was created to be interoperable with the Bourne shell. In contrast to the Bourne shell, it enables us to

view command history and alter it using arrow keys. It has helpful utilities from other Linux shells, including the **Korn** and **C shells**.

The GNU Bourne-Again shell's full path is at **/bin/bash**. The default prompts for the bash shell are **{bash-version_number}#** and **{bash-version_number}$** for root and non-root users, respectively. This is bash running on Kali Linux as shown in *Figure 1.3*:

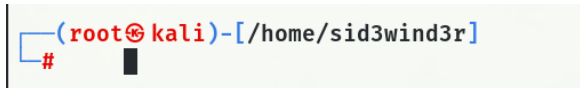

***Figure 1.3**: Bash shell running on Kali Linux*

The C shell

The **C shell**(**csh**) was created to include helpful programming capabilities, such as built-in math operations and syntax comparable to the C programming language.

In addition, it had command history, which was lacking in earlier Linux shells, like the Bourne shell. One of the key components of a C shell is **aliases**, where we can alias one command to a different keyword to make it easier to remember.

The C shell's full path is **/bin/csh**. The root user has **{hostname}#** prompt is used by default and **{hostname}%** for non-root users. Following is a screenshot of cshell:

***Figure 1.4**: Example of csh on Kali Linux*

The Korn shell

The Bourne shell happens to be a subset of an overarching utility called the **Korn shell** (**ksh**). It offers users extra functions in addition to supplying everything the Bourne shell would provide. It offers interactive capabilities comparable to the C shell while allowing built-in support for arithmetic operations.

The Korn shell has the following major features:

- It executes programs written for the Bourne shell and provides C-like text, array, and function manipulation.
- Compatible with scripts created for the C shell.
- It is quicker than most Linux shells, including the C shell.

The Korn shell's full path name is **/bin/ksh**. It uses the prompt **#** for the root user and **$** by default for non-root users.

The Z shell

The **Z shell**, sometimes known as **zsh**, is a bash shell extension with several customization-enhancing features. The **zsh** shell is a contemporary shell with all the capabilities we need and much more.

The z shell has several remarkable attributes, such as:

- Create filenames depending on specified criteria.
- Support for plugins and themes.
- A range of built-in features.

The Z shell's full path name is **`/bin/zsh`** and the standard prompt is **`%`** for non-root users and **`#`** for root users. However, Zsh allows users to customize their prompts extensively. The prompt in Zsh is controlled by the **`PS1`** (primary rompt) variable. Users can customize the appearance of the prompt by setting the **`PS1`** variable in their **`~/.zshrc`** configuration file.

Kernel

The kernel is the core of an OS and is responsible for managing the system's hardware and software. Its primary focus is on managing memory and processing time. It is a crucial component of any OS. The kernel is an intermediary between application-level processing and low-level hardware operations using inter-process communication and system calls.

If the device is already functioning, the kernel is the first piece of software to be put into memory during the boot process. Disc management, task management, and memory management are just a few things it is responsible for. It chooses which tasks should run in the CPU's dedicated execution space and which may stay in the main memory. It mediates communication between software and hardware.

The kernel's principal function is to manage data transfers between software (like user-level applications) and hardware (such as the CPU and disc memory).

Kernel modules

Modules that can be loaded and unloaded into the kernel are called **kernel modules**. They allow the kernel's capabilities to be expanded without requiring a system restart. It is possible to set a module to be either permanently installed or removable. A module must be marked as a loadable module in the kernel settings to be dynamically loaded or unloaded.