Preface

When breaking into the cybersecurity industry, specifically in the ethical hacking and penetration testing fields, you will often hear about the famous Linux distribution known as Kali Linux. Kali Linux is a penetration testing Linux distribution that is built to support the needs of cybersecurity professionals during each phase of a penetration test. As a cybersecurity author, lecturer, and industry professional, I've heard from many people within the cybersecurity and information technology industries, and even from students, about the importance of finding a book that guides the reader to thoroughly understand how to perform penetration testing from beginner to advanced level using a step-by-step approach with Kali Linux. This was the motivation and inspiration behind creating the ultimate book that will be easy to understand for everyone and help all readers to become proficient and develop new skills while using the latest tools and techniques.

Over the years, I've researched and created a lot of cybersecurity-related content, and one of the most important things about being both a red and blue teamer (offensive and defensive) is always staying up to date on how to discover the latest security vulnerabilities and understanding the **Tactics**, **Techniques, and Procedures** (**TTPs**) that are commonly used by cybercriminals. As a result, ethical hackers and penetration testers need to be equipped with the latest knowledge,

skills, and tools to efficiently discover and exploit hidden security vulnerabilities on their targets' systems and networks, with the intent of helping organizations reduce their attack surface and improve their cyber defenses. During the writing of this book, I've used a student-centric and learner-friendly approach, helping you to easily understand the most complex topics, terminologies, and why there is a need to test for security flaws on a system and network.

This book begins by introducing you to the mindset of a threat actor such as a hacker and comparing a hacker's mindset to that of penetration testers. It's important to understand how a threat actor thinks and what is most valuable to them. While penetration testers may have a similar mindset to a hacker, their objective is to discover and help resolve the security vulnerabilities before a real cyber attack occurs on an organization. Furthermore, you will learn how to create a lab environment using virtualization technologies to reduce the cost of buying equipment. The lab environment will emulate a network with vulnerable systems and web application servers. Additionally, a fully patched Windows Active Directory lab has been created to demonstrate the security vulnerabilities found within a Windows domain, where you will learn how to compromise Active Directory services.

You will soon learn how to perform real-world intelligence gathering on organizations using popular tools and strategies for reconnaissance and information gathering. Learning ethical hacking and penetration testing would not be complete without learning how to perform vulnerability assessments using industry-standard tools. Furthermore, you will spend some time learning how to perform exploitation on common security vulnerabilities. Following the exploitation phase,

you will be exposed to post-exploitation techniques and learn how to set up **Command and Control** (**C2**) operations to maintain access on a compromised network to expand your foothold as a penetration tester and exfiltrate data from a compromised host.

You will learn how to perform Active Directory enumeration and exploitation, as many organizations have a Windows environment running Active Directory.

You will learn how to abuse the trust of Active Directory and take over a Windows domain by creating a golden ticket, a silver ticket, and a skeleton key. Furthermore, wireless attacks are included to help aspiring penetration testers gain the skills needed to test for security vulnerabilities on wireless networks, such as exploiting the WPA3 wireless security standard. Finally, the last section includes techniques for discovering and exploiting web applications and performing social engineering techniques and procedures.

In this edition, the procedures for building virtual lab environments have been improved and made easier to understand and follow as a beginner. A new and dedicated chapter on **Open Source Intelligence** (**OSINT**) focuses on collecting and analyzing publicly available information on targeted systems, networks, and organizations to develop a profile of intelligence that can be exploited during penetration testing. The theory and practical labs were improved throughout the entire book, and new labs on web application and social engineering were included.

By completing this book, you will be taken through an amazing journey from beginner to expert in terms of learning, understanding, and developing your skills

in ethical hacking and penetration testing as an aspiring cybersecurity professional within the industry.

Who this book is for

This comprehensive book is meticulously designed for a diverse audience. It caters to the needs of students who are venturing into the field, trainers who are looking for reliable content to impart knowledge, lecturers who wish to supplement their curriculum with up-to-date information, and IT professionals who need to stay abreast of the latest in the industry. Furthermore, it is an excellent resource for anyone who harbors an interest in understanding the intricacies of ethical hacking, penetration testing, and cybersecurity.

The book has been crafted to serve dual purposes. It can be used as a self-study guide for those who prefer to learn at their own pace, and it can also be integrated into classroom-based training for a more structured learning experience. The topics covered are far-reaching and cover the essentials of the field, including discovering and exploiting security vulnerabilities, ethical hacking techniques, and learning penetration testing strategies and procedures.

The book is not limited to beginners who are new to the field of cybersecurity. It also provides sophisticated content that would intrigue and educate even a seasoned professional within the industry. The book offers a balance of theoretical knowledge and practical insights, making it a valuable resource for everyone. There’s a wealth of knowledge to be gained from this book, irrespective of your experience level in the field.

Moreover, the book also provides the hands-on experience needed to get started as an ethical hacker and a penetration tester. It aims to not only impart knowledge but also encourage the practical application of this knowledge in real-world scenarios. This practical approach enhances the learning experience and prepares the reader to face the real-world challenges of cybersecurity.

What this book covers

Chapter 1, *Introduction to Ethical Hacking*, introduces the reader to the concepts ethical hacking and penetration testing tactics and strategies while providing insights into a hacker's mindset.

Chapter 2, *Building a Penetration Testing Lab*, focuses on providing the practical skills for using virtualization technologies to efficiently build a personalized lab environment to safely practice ethical hacking and penetration testing while exploring new skills.

Chapter 3, *Setting up for Advanced Penetration Testing Techniques*, covers how to set up an enterprise Active Directory environment and wireless network for learning how to identify and exploit security vulnerabilities within organizations' infrastructure.

Chapter 4, *Passive Reconnaissance*, introduces the reader to passive reconnaissance and how to reduce their threat level when collecting information about a target during penetration testing.

Chapter 5, *Exploring Open Source Intelligence*, focuses on teaching the reader how to collect and analyze publicly available information to develop a profile about a target and weaponize the collected intelligence.

Chapter 6, *Active Reconnaissance*, teaches the reader how to perform active reconnaissance techniques to collect sensitive information from targeted systems and networks.

Chapter 7, *Performing Vulnerability Assessments*, focuses on performing vulnerability assessments on targeted systems and networks using free and open-source vulnerability management tools in the industry.

Chapter 8, *Understanding Network Penetration Testing*, introduces the reader to the fundamentals of network penetration testing, anti-malware evasion techniques, and working with wireless network adapters.

Chapter 9, *Performing Network Penetration Testing*, focuses on host discovery, identifying and exploiting vulnerabilities on Windows, and Linux-based systems, and performing online and offline password-cracking techniques.

Chapter 10, *Post-Exploitation Techniques*, introduces the reader to common post-exploitation techniques to expand their foothold on a compromised host, use lateral movement to identify additional targets on a different subnet, and perform data exfiltration from a compromised machine.

Chapter 11, *Delving into Command and Control Tactics*, introduces the reader to **Command and Control** (**C2**) operations and explores how C2 helps penetration

testers with remote manipulation from their compromised targets on a network.

Chapter 12, *Working with Active Directory Attacks*, focuses on discovering and exploiting the trust relationships in an Active Directory environment.

Chapter 13, *Advanced Active Directory Attacks*, explores advanced Active Directory penetration testing techniques and procedures, such as performing lateral and vertical movement and taking over the entire Windows domain environment.

Chapter 14, *Advanced Wireless Penetration Testing*, introduces the reader to wireless communication and how penetration testers can identify and exploit security vulnerabilities within enterprise wireless networks.

Chapter 15, *Social Engineering Attacks*, focuses on understanding the principles of social engineering and techniques used by penetration testers to identify human-based vulnerabilities that can be exploited by real threat actors.

Chapter 16, *Understanding Website Application Security*, focuses on discovering the web application security risks that are described in the OWASP Top 10: 2021 list of security vulnerabilities.

Chapter 17, *Advanced Website Application Penetration Testing*, focuses on performing advanced web application security testing to discover and exploit security flaws.

Chapter 18, Best Practices for the Real World, provides guidelines for aspiring ethical hackers and penetration testers to ensure that, after completing this book, you have a wealth of valuable knowledge and can adapt to good practices within the industry.

To get the most out of this book

- It's recommended that you have a solid foundation in networking concepts such as general knowledge of common network, and application-layer protocols from the **Transmission Control Protocol/Internet Protocol** (**TCP/IP**) network model.
- You should have a solid understanding of network infrastructure and devices, such as the role and function of routers, switches, firewalls, and other security solutions such as antimalware and threat detection systems.
- This book leverages virtualization technologies to ensure readers can construct a free lab environment on their personal computers, and so prior knowledge of virtualization concepts will be beneficial.

Download the example code files

The code bundle for the book is hosted on GitHub at **https://github.com/PacktPublishing/The-Ultimate-Kali-Linux-Book-3E**. We also have other code bundles from our rich catalog of books and videos available at **https://github.com/PacktPublishing/**. Check them out!

Download the color images

We also provide a PDF file that has color images of the screenshots/diagrams used in this book. You can download it here: **https://packt.link/gbp/9781835085806**.

Conventions used

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

`CodeInText`: Indicates code words in text, database table names, folder names, filenames, file extensions, pathnames, dummy URLs, user input, and Twitter handles. For example: “Mount the downloaded `WebStorm-10*.dmg` disk image file as another disk in your system.”

A block of code is set as follows:

```
[default]
exten => s,1,Dial(Zap/1|30)
exten => s,2,Voicemail(u100)
exten => s,102,Voicemail(b100)
exten => i,1,Voicemail(s0)
```

When we wish to draw your attention to a particular part of a code block, the relevant lines or items are set in bold:

```
[default]
exten => s,1,Dial(Zap/1|30)
exten => s,2,Voicemail(u100)
```

```
exten => s,102,Voicemail(b100)
exten => i,1,Voicemail(s0)
```

Any command-line input or output is written as follows:

```
# cp /usr/src/asterisk-addons/configs/cdr_mysql.conf.sample
     /etc/asterisk/cdr_mysql.conf
```

Bold: Indicates a new term, an important word, or words that you see on the screen. For instance, words in menus or dialog boxes appear in the text like this. For example: “Select **System info** from the **Administration** panel.”

Warnings or important notes appear like this.

Tips and tricks appear like this.

Disclaimer

The information within this book is intended to be used only in an ethical manner. Do not use any information from the book if you do not have written permission from the owner of the equipment. If you perform illegal actions, you are likely to be arrested and prosecuted to the full extent of the law. Neither Packt Publishing nor the author of this book takes any responsibility if you misuse any of the information contained within the book. The information herein must only

be used while testing environments with proper written authorization from the appropriate persons responsible.

Get in touch

Feedback from our readers is always welcome.

General feedback: Email `feedback@packtpub.com` and mention the book's title in the subject of your message. If you have questions about any aspect of this book, please email us at `questions@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 reported this to us. Please visit **http://www.packtpub.com/submit-errata**, click **Submit Errata**, and fill in the form.

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@packtpub.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 **http://authors.packtpub.com**.

Share your thoughts

Once you've read *The Ultimate Kali Linux Book*, 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/9781835085806

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