Kali Linux for Ethical Hacking

Penetration testing and vulnerability assessment for network security

Mohamed Atef

www.bpbonline.com

First Edition 2024

ISBN: 978-93-55517-043

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 beloved family

my wife ***Hanaa*** *and sons* ***Omar*** *and* ***Yousef***

About the Author

Mohamed Atef is a seasoned Cyber Security Specialist with over 20 years of extensive experience in security governance, compliance, and operations across diverse sectors including government, financial, healthcare, and private industries. His expertise encompasses the implementation of international standards such as ISO 27001, GDPR, PCI-DSS, and HIPAA, as well as regional standards including ISR and NESA in the UAE, and ECC and SAMA in KSA.

As a pivotal member of the award-winning security team at Dubai Municipality, Mohamed contributed to the team's recognition as the Best Security Team across the Dubai Government in 2017. He played a significant role in achieving 100% compliance with the 13 DESC KPIs in 2022, demonstrating his proficiency in implementing and maintaining robust security frameworks.

Throughout his career, Mohamed has successfully managed and executed comprehensive disaster recovery plans, ensuring business continuity under various scenarios and aligning with best practices and regulatory requirements. His technical background includes system administration for both Linux and Windows environments, along with hands-on experience in SIEM, vulnerability scanning, and penetration testing.

Mohamed has also designed and conducted role-based information security awareness campaigns, significantly enhancing organizational compliance and security posture. He has implemented enterprise-wide data protection strategies, including data classification frameworks and Data Loss Prevention (DLP) systems, effectively securing sensitive information.

In addition to his practical expertise, Mohamed is an accomplished author with five published books on cybersecurity and a frequent public speaker, dedicated to fostering a culture of security awareness and education. His certifications, including CISSP, CEH, and PMP, complement his extensive experience and commitment to the field of cybersecurity.

About the Reviewer

Darryn Brownfield started his career in the world of IT and security in 2010, working on a first line help desk for a leading IT reseller and MSP. During his time there he worked his way up to become a junior partner and a Security Solutions Architect. Driven with a passion for security, he then transitioned into the world of penetration testing by studying in his free time to become a pentest team leader.

Darryn is now the founder and CEO of the UK cyber security company Securebytes Solutions Ltd. With an extensive range of penetration testing and consultancy services, Darryn and his team at Securebytes provide actionable insights that empower clients to strengthen their security posture.

He holds various industry recognised and respected certifications such as the Offensive Security Certified Professional (OSCP), Practical Network Penetration Tester (PNPT), CREST Certified Registered Tester (CRT) and Certified Red Team Professional (CRTP).

Darryn is a bug bounty hunter and a member of the Synack Red Team (SRT), a private community of highly-curated and vetted security penetration testers.

Acknowledgement

I would like to extend my heartfelt gratitude to InfoSec4tc FZE for their invaluable support and encouragement throughout the writing of this book. Special thanks to my colleagues and mentors for their guidance and insights, which have been instrumental in shaping this work. Finally, I am deeply thankful to my family for their unwavering support and patience during this journey.

Preface

In the rapidly evolving world of cybersecurity, the role of ethical hackers has never been more crucial. This book, 'Kali Linux for Ethical Hacking,' aims to equip readers with the knowledge and skills necessary to navigate the complex landscape of cybersecurity threats. Kali Linux, a powerful platform for penetration testing and ethical hacking, serves as the cornerstone of this journey.

Throughout this book, readers will explore foundational concepts, advanced tools, and practical techniques to identify and mitigate vulnerabilities in various systems. Whether you are a beginner eager to enter the field or a seasoned professional seeking to enhance your expertise, this book provides comprehensive insights and hands-on exercises to strengthen your abilities as an ethical hacker.

The journey of creating this book has been both challenging and rewarding. It is my hope that the lessons and experiences shared here will inspire and empower you to contribute to the security and resilience of our digital world. As you delve into the pages ahead, remember that the pursuit of knowledge and the commitment to ethical practices are the keys to success in the field of ethical hacking.

Chapter 1: Foundations of Ethical Hacking and Kali Linux – Introduction to ethical hacking and Kali Linux, including setting up the environment and basic commands. Ethical hacking overview, average salary for ethical hackers, skills required for ethical hackers. Kali Linux as a penetration testing platform, setting up your environment, using a virtual environment. Navigating the Linux command line, file management and permissions, essential Linux commands. Customizing your Kali Linux environment, package management in Kali Linux, updating and upgrading Kali Linux.

Chapter 2: Information Gathering and Network Scanning – Techniques for gathering information and scanning networks to identify vulnerabilities. Passive and active information-gathering techniques, tools for OSINT gathering, WHOIS lookup, DNS information gathering. Network scanning and enumeration, working with Nmap and other scanning tools, DNS enumeration and zone transfers. Social engineering techniques, phishing, and tools for phishing.

Chapter 3: Executing Vulnerability Assessment – Conducting vulnerability assessments and analyzing results. Understanding software, hardware, network, and human vulnerabilities. Vulnerability scanning tools, reviewing results, taking action. Manual vulnerability assessment techniques, interpreting and prioritizing results, risk assessment and management.

Chapter 4: Exploitation Techniques – Various techniques to exploit vulnerabilities in systems and applications. Working with Metasploit, client-side and web application exploitation, password attacks and brute forcing. Exploiting common network services, exploiting service misconfigurations.

Chapter 5: Post-Exploitation Activities – Activities after exploiting a system, including maintaining access and covering tracks. Privilege escalation, maintaining persistence and lateral movement, data exfiltration and manipulation. Covering tracks and evading detection, understanding C2 channels.

Chapter 6: Wireless Network Security and Exploitation – Security of wireless networks and how to exploit common vulnerabilities. Wireless networking fundamentals, tools for wireless network exploitation, defending against wireless attacks. Bluetooth and IoT security, design best practices.

Chapter 7: Web Application Attacks – Common web application attacks and how to defend against them. Web application security fundamentals, common web application threats, understanding HTTP and HTTPS. Web application firewalls, scanning for vulnerabilities using Nikto, brute-forcing login forms with Hydra. Exploiting SQL injection with sqlmap, OWASP top ten, web application exploitation tools and techniques. Securing web applications, API security and testing, secure development best practices.

Chapter 8: Hands-on Shell Scripting with Error Debugging Automation – Shell scripting for automation in ethical hacking and error debugging. Shell scripting basics, crafting purpose-built scripts, exploring shell scripting utilities. Bash scripting basics, scripting operational harmony, parameters and argument passing. Automated scanning, payload delivery, data exfiltration, orchestrating automated reporting.

Chapter 9: Real-World Penetration Testing Scenarios – Real-world scenarios and practical applications of penetration testing techniques. Planning and scoping a penetration test, conducting the engagement, strategic probing. Reporting and remediation, lessons learned and ongoing improvement, continuous security monitoring and testing.

Code Bundle

Please follow the link to download the
Code Bundle of the book:

The code bundle for the book is also hosted on GitHub at
https://github.com/bpbpublications/Kali-Linux-for-Ethical-Hacking.
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 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

1. Foundations of Ethical Hacking and Kali Linux....1

Introduction....1
Structure....1
Objectives....2
Ethical hacking overview....2
Average salary for ethical hackers....3
Skills required for ethical hackers....4
Kali Linux: A powerful penetration testing platform....4
Setting up your Kali Linux environment....6
Using a virtual environment....7
The ethical hacker's mindset....8
Legal and ethical considerations....10
Navigating the Linux command line....12
File management and permissions....15
Essential Linux commands....18
Customizing your Kali Linux environment....20
Package management in Kali Linux....23
Updating and upgrading Kali Linux....25
Conclusion....27

2. Information Gathering and Network Scanning....29

Introduction....29
Structure....29
Objectives....30
Passive information-gathering techniques....30
Open-source intelligence (OSINT) gathering....30
Tools for OSINT gathering....31
WHOIS Lookup....32

Tools for WHOIS lookup 32
DNS information gathering 33
Tools for DNS information gathering: 33
Robtex 35
Email header analysis 36
Tools for email header analysis 36
Network metadata analysis 38
Tools for network metadata analysis 38
Active information gathering techniques 40
Port scanning with Nmap 41
Network scanning and enumeration 43
Use case: Network scanning and enumeration for a healthcare provider 45
Working with Nmap and other scanning tools 46
Use case: Network security audit for a Tech startup 47
DNS enumeration and zone transfers 48
Use case: DNS enumeration and zone transfer for a media company 49
Social engineering techniques 50
Phishing 50
Tools for Phishing 51
Conclusion 57

3. Executing Vulnerability Assessment 59

Introduction 59
Structure 60
Objectives 61
Understanding vulnerabilities 61
Software vulnerabilities 61
Types of software vulnerabilities 62
Buffer overflow as an example 62
Mitigation and best practices 63

Use case: Vulnerability assessment 63
Hardware vulnerabilities 64
Network vulnerabilities 64
Types of network vulnerabilities 65
Unprotected open port as an example 65
Using Nmap to identify network vulnerabilities 65
Mitigation and best practices 67
Use case: Vulnerability assessment 68
Human vulnerabilities 68
Types of human vulnerabilities 68
Using the Social-Engineer Toolkit (SET) to identify human vulnerabilities 69
Phishing as an example 71
Mitigation and best practices 71
Use case: Vulnerability assessment 72
Vulnerability scanning tools 73
Reviewing the results 74
Taking action 74
Installation 75
Manual vulnerability assessment techniques 76
Interpreting and prioritizing assessment results 78
Risk assessment and management 79
Vulnerability databases and resources 80
Use case: Acme Corp vulnerability assessment 82
Results 83
Conclusion 83

4. Exploitation Techniques 85

Introduction 85
Structure 86
Objectives 87

Exploitation frameworks in Kali Linux 87
Working with Metasploit 88
Introduction to Metasploit Framework 88
Getting started with msfconsole....89
Client-side and web application exploitation 91
First side: Client-side exploitation 91
Web application exploitation....92
Essential resources for web exploitation 92
Password attacks and brute forcing 93
Types of password attacks 93
Password cracking tools 94
Best practices and mitigations 94
Essential resources for understanding password attacks....95
Exploiting common network services....95
Popular network services and their vulnerabilities....95
Exploiting service misconfigurations....96
Mitigation strategies....97
Essential resources for service exploitation....97
Conclusion 97

5. Post-Exploitation Activities....99

Introduction 99
Structure 99
Objectives 100
Privilege escalation 100
Understanding privilege escalation 100
Common techniques and examples 101
Misconfigured permissions....101
Application vulnerabilities 101
Kernel exploits 102
Detection and prevention 102

Demonstrating privilege escalation with Kali Linux *103*
Exploiting Kernel vulnerabilities with Metasploit *104*
Leveraging LinEnum for a thorough scan *104*
Utilizing Windows-Exploit-suggester for Windows targets *105*
Escalating privileges using DirtyCow *105*
Maintaining persistence and lateral movement 106
Understanding persistence *106*
Common persistence techniques *106*
Understanding lateral movement *107*
Common techniques for lateral movement *107*
Demonstrating persistence and lateral movement with Kali Linux ... *107*
Data exfiltration and manipulation 109
Understanding data exfiltration *109*
Common exfiltration techniques *109*
Understanding data manipulation *110*
Examples of data manipulation *110*
Demonstrating data exfiltration and manipulation with Kali Linux *110*
Data exfiltration using netcat *111*
Covering your tracks and evading detection 112
Techniques to cover tracks *112*
Techniques for evading detection *112*
Demonstrating evasion and track covering with Kali Linux *113*
Understanding C2 channels 114
Techniques and protocols used in C2 ..... *115*
Demonstrating C2 communication with Kali Linux *115*
Conclusion 116

6. Wireless Network Security and Exploitation 117

Introduction 117
Structure 117
Wireless networking fundamentals 118

Types of wireless networks *118*
Wireless network components *118*
Basic Kali Linux commands for wireless networking *119*
Wireless network vulnerabilities and attacks 120
Tools for wireless network exploitation 122
Defending against wireless attacks 124
Bluetooth and IoT security 125
Design best practices 128
Conclusion 129

7. Web Application Attacks 131

Introduction 131
Structure 132
Objectives 132
Web application security fundamentals 133
Common web application components *133*
Common web application threats *134*
Understanding HTTP and HTTPS *135*
Cookies and sessions *135*
Web Application Firewalls *137*
Scanning for vulnerabilities using Nikto *138*
Brute forcing login forms with Hydra *138*
Exploiting SQL injection with sqlmap *139*
Web application attacks and vulnerabilities 141
OWASP top ten *141*
Man-in-the-Middle attacks *142*
Directory traversal *142*
Security misconfigurations *143*
Insecure deserialization *143*
Clickjacking *144*
Server-side request forgery *145*

Credential stuffing *145*
Unvalidated redirects and forwards *146*
Web application exploitation tools and techniques 146
Securing web applications 148
API security and testing 149
Secure development best practices 151
Conclusion 153

8. Hands-on Shell Scripting with Error Debugging Automation 155

Introduction 155
Structure 156
Objectives 156
Shell scripting with error debugging automation 156
Defining the shell script paradigm *157*
Shell Scripting within the ethical hacking ecosystem *157*
Transcending beyond basics *158*
Crafting purpose-built scripts *159*
Exploring shell scripting utilities *161*
Bash scripting basics 162
Unveiling the power of Bash *163*
Scripting operational harmony *164*
Parameters and argument passing *164*
Harnessing automation in ethical hacking *165*
Embarking on automated scanning *165*
Automated payload delivery and exploitation *166*
Automated data exfiltration *166*
Orchestrating automated reporting *167*
Preluding tool development: Identifying needs *167*
Crafting custom scanners *167*
Developing exploitation and payload tools *168*

Data processing and analytical tools *168*
Error handling and debugging 169
Navigating through the maze of error and debug *171*
Essence of error handling *171*
Journey into debugging *171*
Crafting robust scripts with error handling *172*
Interweaving tools into the Cybersecurity Tapestry *173*
Concerting Shell Scripts and security tools *173*
Facilitating data flow among tools *173*
Engendering scalability through modular scripting *174*
Conclusion 174

9. Real-World Penetration Testing Scenarios 177

Introduction 177
Structure 178
Objectives 178
Embarking on practical cybersecurity expeditions 179
Navigating through the nuances of practical engagements *179*
Engaging with the full spectrum of a penetration test *179*
Interweaving theory, practice, and ethical considerations *180*
Planning and scoping a penetration test 181
Crafting the blueprint of cybersecurity engagements *181*
Envisaging the objective: Defining clear goals *181*
Crafting boundaries: Scoping the engagement *182*
Navigating ethical and legal terrains *182*
Championing clear communication and collaboration *182*
Conducting the engagement 183
Conducting ethical hacking *184*
Strategic probing: Guided exploration and exploitation *184*
Adaptive maneuvering: Modulating strategies mid-engagement *184*

Precision in chaos: Managing unintended consequences *185*
Ephemeral victories: Managing and utilizing access *185*
Reporting and remediation 186
Harvesting insights: Translating cyber exploits into actionable Intelligence *187*
Crystalizing findings: The art of comprehensive reporting *188*
Client-centric communication: Bridging technical and non-technical realms *189*
Navigating through remediation: Guiding secure transformation *189*
Continuous collaborative enhancement: Fostering long-term security *190*
Ensuring the legacy of cybersecurity engagements *190*
Lessons learned and ongoing improvement 190
From cyber endeavors to cybersecurity evolution: Cultivating resilience through reflection *192*
Reflective mirror: Understanding and absorbing lessons learned *192*
Strategic evolution: Transforming lessons into cybersecurity maturity *192*
Inculcating a culture of continuous improvement *193*
Engagement legacy: Ensuring the sustained impact of penetration testing *193*
Red team vs. Blue team exercises 193
Dynamic duality: The symbiotic dance of offense and defense in cybersecurity *195*
Contrasting cohorts: Red teams and Blue teams defined *195*
Controlled conflagration: Orchestrating and managing cyber exercises *195*
Harvesting and applying insights: The real prize of simulated battles *196*
Continuous cybersecurity evolution: Maintaining momentum post-exercise *196*
Continuous security monitoring and testing 197

Vigilant watchfulness: Eternal guardianship in the cyber realm 198
Enduring oversight: The imperative of continuous security monitoring.....198
Evolving defenses: perpetual testing for adaptive cybersecurity.....199
Strategic synthesis: Melding monitoring and testing into a cohesive defense.....199
Safeguarding tomorrow: Futureproofing through continuous cybersecurity enhancement 199
Navigating the endless cyber frontier.....200
Reflected beginnings 200
Continuous voyage.....200
Towards infinite horizons.....201
Enduring gratitude and anticipation for future journeys 201
Conclusion 201
Index 203-210

Chapter 1
Foundations of Ethical Hacking and Kali Linux

Introduction

This chapter comprehensively introduces ethical hacking and Kali Linux. It provides readers with a foundational understanding of the tools, techniques, and concepts that will be covered throughout the rest of the book. This chapter establishes the importance of ethical hacking in today's digital landscape and introduces Kali Linux as a powerful platform for penetration testing and ethical hacking.

Structure

In this chapter, we will cover the following topics:

- Ethical hacking overview
- Kali Linux: A powerful penetration testing platform
- Setting up your Kali Linux environment
- The ethical hacker's mindset
- Legal and ethical considerations

- Navigating the Linux command line
- File management and permissions
- Essential Linux commands
- Customizing your Kali Linux environment
- Package management in Kali Linux
- Updating and upgrading Kali Linux

Objectives

The chapter begins by defining what ethical hacking is and the importance of conducting ethical hacking in today's digital landscape. It then introduces Kali Linux, an operating system designed for ethical hacking and penetration testing. The chapter explains the benefits of using Kali Linux, such as its extensive collection of tools and features, security and privacy enhancements, and user-friendly interface.

Next, the chapter explores the specifics of using Kali Linux for ethical hacking, including navigating the user interface, accessing various tools and features, and managing files and permissions. It covers some key tools and features of Kali Linux commonly used in ethical hacking, such as the Metasploit Framework, Nmap, Wireshark, and John the Ripper.

Throughout the chapter, hands-on exercises and examples demonstrate how to use the various tools and features of Kali Linux to conduct ethical hacking and penetration testing. This includes examples of conducting network scanning, vulnerability assessment, exploitation, and post-exploitation activities.

Overall, the chapter serves as a comprehensive introduction to the world of ethical hacking and Kali Linux, providing readers with a foundational understanding of the tools, techniques, and concepts covered throughout the rest of the book.

Ethical hacking overview

In this section, readers are introduced to the concept of ethical hacking. Ethical hacking, also referred to as penetration testing or white hat hacking. It intentionally and lawfully exploits computer systems, networks, and software applications to identify vulnerabilities and weaknesses. Ethical hackers use their expertise to discover and address security flaws before

malicious hackers can exploit them for malicious purposes. They work with organizations to assess the security posture of their digital infrastructure, identify potential vulnerabilities, and develop effective mitigation strategies.

Ethical hackers adopt the mindset of a malicious hacker, leveraging their knowledge of computer systems, networking protocols, and software vulnerabilities to simulate real-world cyber-attacks. By doing so, they identify and expose vulnerabilities that might go unnoticed. This proactive approach enables organizations to patch security weaknesses, strengthen defenses, and protect sensitive information.

Ethical hackers employ various techniques and methodologies to carry out their assessments. These include network scanning, vulnerability assessment, penetration testing, social engineering, and exploitation of security weaknesses. They utilize a wide range of tools and technologies to analyze and assess the security posture of systems, such as network scanners, vulnerability scanners, password crackers, and forensic tools. By combining technical expertise with critical thinking and problem-solving skills, ethical hackers uncover potential vulnerabilities and provide valuable insights to improve security measures.

In addition to technical proficiency, ethical hackers must understand legal and ethical considerations strongly. They operate within the boundaries of the law and obtain proper authorization before conducting any assessments. They adhere to strict ethical guidelines and respect the privacy of individuals and organizations they engage with. Confidentiality, integrity, and professionalism are essential traits that ethical hackers must uphold to maintain trust and credibility.

Average salary for ethical hackers

The field of ethical hacking offers lucrative career opportunities, given the increasing demand for cybersecurity professionals. The average salary for ethical hackers can vary depending on factors such as experience, certifications, geographical location, and the industry they work in.

According to industry reports and surveys, the average salary for ethical hackers' ranges from $80,000 to $120,000 per year, depending on the region and level of experience. However, experienced ethical hackers with advanced certifications and specialized skills can earn significantly higher salaries, often surpassing the six-figure mark. It is important to note that these figures are general estimates and can vary based on individual circumstances.