Penetration Testing with Kali NetHunter

Hands-on Android and iOS penetration testing

Gerald "Tripp" Roybal III

www.bpbonline.com

First Edition 2024

ISBN: 978-93-55516-510

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

Mom, ***Ashley****,* ***Nana****, Dad, Uncle* ***Kenny****,* ***Risa***

and

Everyone who believed in me from the beginning

About the Author

Gerald "Tripp" Roybal III is a seasoned professional red teamer with extensive experience in the field of cybersecurity. Tripp holds a bachelor's degree and has earned various certifications, including GPEN and CISSP. Based in Tokyo, Japan, Tripp founded the hacking educational collective TenguSec and has spoken at several conferences. When not competing in CTFs or earning bug bounties, Tripp enjoys music. Currently, he is the founder and CEO of Harmful Stimulus LLC.

Tripp's technical expertise spans various areas, including mobile, web, network, and infrastructure penetration testing, bug bounty programs, public speaking, and leadership.

About the Reviewers

- **Dr. James Horlock** is an experienced cyber security manager and ethical hacker with four years of penetration testing experience within the Big Four. Beyond corporate roles, he has shown a passion for teaching and learning education. With a PhD in Named Entity Extraction, he is pursuing advanced Cyber Security and Technology studies at Cardiff University. His constantly evolving skill set is enhanced by his experience in programming languages, operating systems, network protocols, and penetration testing tools. With a commitment to diversity and a sincere dedication to mentorship, he continues to shape the cybersecurity landscape through innovation and collaboration. He is married to his wife, Alexandra, and takes immense pride in both of his children.

- **Naresh Kumar Miryala** is a highly experienced engineering leader with nearly 20 years of industry experience and an assertive cloud, platform engineering, and artificial intelligence background. He has led high-performing cloud data platforms teams in his current role at Meta Platforms, Inc. He has a proven track record of cloud transformations, infrastructure implementation, database management, ERP solutions, and DevOps deployments. His expertise spans multiple domains such as database systems, large-scale backend infrastructure, security, multi-cloud deployments, cloud infrastructure, DevOps, and artificial intelligence.

  Naresh has contributed to esteemed organizations such as Oracle Corp and Computer Sciences Corporations, where he played a pivotal role in migrating and implementing enterprise technologies for Fortune 500 companies across the globe. His impact spans various industries worldwide, including pharmaceuticals, retail, banking, and gold mining companies.

  Naresh's experience in cloud migrations, particularly involving relational, open-source, and NoSQL databases, middleware, and applications, has granted him a comprehensive understanding of multi-faceted technical and business challenges in the modern world and developing innovative solutions across the industry to solve large-scale data transformation and security problems using artificial intelligence.

Acknowledgement

To my mother, who never stopped giving me ways to look at the world differently (intentionally and otherwise), I dedicate this book to your memory. I miss you.

To Nana, thank you for all you have given me over the years, including love and support. I could never repay you, but I will try to start by putting this book into your hands.

To my father, thank you for all the wisdom and lessons you have shared with me. Although we have had to make up for lost time, I think we have made remarkable progress. May the book in your hands stand as a part of your legacy.

To Risa, thank you for being everything I needed exactly when I needed it.

To Ashley, thank you for being a constant in my life that I would never be able to replace. Umbrella.

To the Sheehans, thank you for helping me bridge the most critical period of my journey to finding my footing in this world. Your kindness will never be forgotten and will be paid forward in any and every way.

I express my deepest gratitude to my family and friends in TenguSec, PupperSec, ChaHa, and SubProto for their unwavering support and encouragement over the years.

I am also grateful to BPB Publications for their guidance and expertise in bringing this book to fruition.

I would also like to acknowledge the valuable contributions of my colleagues, advisors, and mentors during my years growing as a hacker and a professional, who have taught me so much. There are too many of you, but I will scratch the surface by thanking James, Joe, Nick, Mike, Kyle, Carl, Dr. French, Cynthia, Mark, Shiraishi-san, Bryce, Ari, Jim, and Hanson-sensei.

Finally, I would like to thank all the readers who have taken an interest in my book and for their support in making it a reality.

Preface

Mobile devices have become an integral part of our lives, making it crucial to ensure the security of the applications and systems that run on them. As the demand for mobile security professionals grows, Penetration Testing with Kali NetHunter provides a comprehensive guide to the powerful Kali NetHunter platform, equipping readers with the essential tools and techniques for effective mobile penetration testing on Android and iOS devices.

This extensive resource will teach readers how to set up and configure Kali NetHunter on various devices, including rooted and unrooted Android devices. Additionally, details about jailbreaking iOS devices will be discussed. The book covers many critical topics, such as attacking smartphone applications, mobile application penetration testing, web app penetration testing for mobile devices, and assessing sensor and hardware security via mobile applications. Readers will explore advanced pentesting techniques, discover how to document findings, develop remediation plans, and explore the future of mobile penetration testing and security trends. Readers will gain hands-on skills to conduct mobile penetration tests through the guided exploitation of intentionally vulnerable applications.

Upon completing Penetration Testing with Kali NetHunter, readers will gain a deep understanding of mobile security testing methodologies and become proficient in using Kali NetHunter for mobile penetration testing. With the skills and knowledge acquired from this book, readers will be well-equipped to identify vulnerabilities, strengthen security measures, and protect their mobile applications and devices from potential threats.

With this book, you will gain the knowledge and skills to become a penetration tester focusing on mobile devices and technologies. I hope you will find this book informative and helpful.

Chapter 1: Introduction to Mobile Penetration Testing – The readers are introduced to the pivotal role of mobile security amidst the ever-evolving digital landscape, with a spotlight on the contrasting security paradigms of the Android and iOS platforms. The chapter presents Kali NetHunter, an Android-centric penetration testing suite from the creators of Kali Linux, showcasing essential tools like Metasploit, Nmap, Burp Suite, and Wireshark for identifying and exploiting vulnerabilities in mobile applications and networks. It elucidates common mobile application vulnerabilities—from insecure data storage to insufficient transport layer protection—and outlines the mobile penetration testing process from reconnaissance to remediation. This foundation equips readers with

a robust understanding of mobile security, the intricacies of Android and iOS, and the strategic application of Kali NetHunter in safeguarding mobile devices and applications against emerging threats.

Chapter 2: Setting Up Your Device – It takes readers through the meticulous process of installing and configuring Kali NetHunter across a spectrum of devices, from rooted to unrooted Android gadgets, paving the way for a solid start in mobile penetration testing. It outlines the crucial steps for unlocking bootloaders, flashing custom recoveries, and rooting with TWRP and Magisk while covering chroot deployments on unrooted devices. The narrative extends to jailbreaking iOS devices, shedding light on methods and tools like unc0ver, checkra1n, and Chimera, and installing Cydia to access a wider array of security resources. It sets up virtual landscapes for enthusiasts without physical devices using Android emulators and the iOS Simulator, creating a robust testing environment. Equipped with this chapter, readers will emerge skilled in preparing Android and iOS platforms for penetration testing, regardless of their hardware availability, marking a significant leap in their mobile security journey.

Chapter 3: Mobile Penetration Testing Methodology – It delves into the intricacies of Mobile Penetration Testing Methodology, a critical aspect of cybersecurity in the age of ubiquitous mobile devices. We will start by exploring standard penetration testing processes, including planning, reconnaissance, scanning, gaining and maintaining access, and analysis and reporting. Then, the focus shifts to the specialized domain of mobile penetration testing, dissecting its unique challenges and techniques. This involves a detailed look at both testing mobile devices and utilizing mobile devices as tools in penetration testing. From the static and dynamic analysis of mobile apps to the setup and exploitation techniques using mobile devices, this chapter is designed to offer a comprehensive understanding of the current landscape and methodologies in mobile penetration testing.

Chapter 4: Attacking Android Applications – It is a comprehensive exploration of Android's ecosystem, delving into its history, internal workings, and the unique aspects of Android applications. We will unravel the complexities of Android's architecture, examining its specific idiosyncrasies, the sandbox environment, and the permissions model that underpins its security. The discussion will extend to critical features like Secure Interprocess Communication, Paranoid Networking, and hardware-backed security. We will also shed light on the roles of Google Play Protect and the Android Keystore in safeguarding the platform. Much of the chapter is dedicated to the intricacies of Android security testing, covering everything from common vulnerabilities and malware to the specifics of Man-in-the-Middle attacks. This chapter is designed to provide a thorough

understanding of the multiple layers of security within the Android platform, equipping readers with the knowledge to navigate and secure this widely used operating system effectively.

Chapter 5: Attacking iOS Applications – It delves into the sophisticated methodologies for penetration testing on iOS applications, equipping readers with knowledge of client- and server-side vulnerabilities. Emphasizing a hands-on approach, the chapter explores key tools and technologies, such as Burp Suite for network traffic analysis, Frida for dynamic app analysis, Hopper for reverse engineering, MachOView for binary inspection, and Cydia Impactor for installing modified applications. These tools are crucial for identifying and exploiting vulnerabilities, ranging from flawed programming and insecure data storage on the device side to insecure server configurations and scripting issues. This comprehensive examination aims to empower readers with the skills to detect, exploit, and ultimately strengthen the security of iOS applications, contributing to a more secure digital ecosystem.

Chapter 6: Mobile Device Penetration Testing for Web Applications – It addresses the unique challenges of diverse operating systems, varied device configurations, and fluctuating network conditions. We discuss the nuances of operating systems like Android and iOS, each with distinct security features and vulnerabilities, from Android's open-source transparency to iOS's closed yet potentially exploitable ecosystem. The exploration extends to device configurations, where simple misconfigurations can lead to significant security risks and the impact of varying network conditions, such as the vulnerability shifts between secure and public networks. Addressing critical vulnerabilities like SQL injections, the chapter emphasizes rigorous testing methods, including input validation, to reinforce application security. This journey transcends mere vulnerability identification, aiming to fortify mobile applications, enhance overall ecosystem security, and adopt an attacking-to-protect approach, ensuring a comprehensive understanding of static and dynamic analysis and behavioral testing in mobile device penetration testing.

Chapter 7: Working with Kali NetHunter - It discusses the fascinating evolution of Kali NetHunter, tracing its development from the roots of Kali Linux, a Debian-based distribution, to its integration with NetHunter, an open-source Android penetration testing platform. This combination creates an unparalleled tool for exploiting various vulnerabilities via mobile devices. Central to NetHunter's prowess is its bespoke kernel, enabling 802.11 wireless injections, monitor mode, and the capability to launch Human Interface Device (HID) attacks. Furthermore, NetHunter brings the power of a complete Kali Linux desktop environment to Android devices, significantly enhancing mobile pen testing. We explore NetHunter's extensive toolset for wireless network analysis, including

Aircrack-ng and Kismet. The chapter also covers network scanning and exploitation tools such as Nmap, the renowned network mapper, and Metasploit, a comprehensive framework for crafting and executing exploit code. By the end of this chapter, readers will have a thorough understanding of the histories, functionalities, and applications of both Kali and NetHunter, solidifying their knowledge of advanced penetration testing techniques.

Chapter 8: Advanced Pentesting Techniques - It immerses readers in the specialized field of advanced penetration testing techniques tailored for mobile devices. Given the pervasive usage of smartphones, penetrating these devices forms a crucial part of red team operations. You will be diving into an array of intricate methodologies ranging from network-based attacks to binary exploitation and peripheral integrations, all in the context of mobile devices. Specifically, you will learn how Kali NetHunter enhances these operations.

Chapter 9: Developing a Vulnerability Remediation Plan - The readers will acquire the skills needed for detailed documentation, effective communication, and development of remediation plans following mobile penetration tests. It explores a range of technologies and methodologies essential for managing and reporting the results of these tests, with a particular focus on mobile security challenges. The chapter introduces tools like Dradis, Faraday, and KeepNote for creating structured reports that catalog vulnerabilities with supportive narratives and evidence, which are crucial in complex mobile environments. It emphasizes the need for clear communication with stakeholders, providing compelling strategies to present vulnerability data to different audiences, from technical teams to upper management. Best practices in both visual and written presentations are covered to ensure effective conveyance of remedial urgency. The latter part of the chapter guides readers through developing actionable remediation plans, utilizing frameworks like the OWASP Mobile Security Testing Guide and the OWASP Mobile Application Security Verification Standard. These resources offer structured remediation approaches, including best practices and checklists for mobile contexts. Readers will learn to create comprehensive action plans, prioritize remediation tasks using scoring systems like CVSS and DREAD, and gain insights into ongoing risk mitigation strategies.

Chapter 10: Detecting Vulnerabilities on Android Apps – It dives into the intricacies of Android application security with a hands-on approach, moving from abstract concepts to practical applications. You will learn through real scenarios, like exploiting insecure data storage with Android Debug Bridge (ADB) and examining SQLite databases for sensitive data. The chapter assumes a basic understanding of Android, exploring the anatomy of apps, including AndroidManifest.xml, APK structure, and coding in Java or Kotlin.

It emphasizes that mastering Android security is a continuous journey, adapting to new updates from Google and evolving threats, equipping you with skills and insights for proactive security management in the dynamic world of Android applications.

Chapter 11: Hands-on Practice: Vulnerable iOS Apps - It dives into iOS application security, debunking the myth of invincibility and providing a hands-on guide to uncovering and defending against potential threats. It emphasizes the importance of familiarizing oneself with iOS development tools like Objective-C or Swift, Xcode, and the iOS SDK for development and security analysis. Readers will explore static analysis using tools like Clang Static Analyzer and dynamic analysis through Frida and Cycript, which allow real-time examination and manipulation of running applications. This journey through iOS security is not just theoretical; it is a practical, hands-on approach to understanding and mitigating the vulnerabilities that can exist even within tightly controlled ecosystems, preparing readers to navigate and fortify the complex terrain of iOS application security.

Chapter 12: Mobile Security Career Roadmap - It delves into the wide arena of mobile security careers, exploring the journey from foundational knowledge to specialized expertise. We will dissect essential skill sets, from programming to reverse engineering, and navigate the spectrum of professional certifications like OSCP, CEH, and GIAC. Key job roles such as Penetration Testers, Mobile Application Security Analysts, and Researchers are highlighted, detailing the skills and mindset required for each.

Chapter 13: The Future of Pentesting and Security Trends- It discusses mobile penetration testing, which continually evolves with technological advancements. As new opportunities arise, so do novel threats, creating a dual-sided landscape of innovation and vulnerability. Mobile technology advancements offer immense benefits but introduce complex challenges, with threat actors exploiting new vulnerabilities. Mobile penetration testers must, therefore, anticipate future threats, staying ahead of technological developments to ensure robust security from the outset. This chapter explores the future of mobile security, examining current trends and their potential implications. It underscores the need for continuous adaptation, vigilance, and innovation in safeguarding the digital realm against emerging threats as technology advances into new frontiers.

Coloured Images

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

https://rebrand.ly/lli2lxm

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. Introduction to Mobile Penetration Testing 1

Introduction 1

Structure 1

Objectives 2

The growing need for mobile security 2

The rise of smartphones and tablets 2

The impact of mobile devices on daily life 4

Mobile security significance in the digital age 4

Mobile platforms: Android and iOS 5

A brief history of Android and iOS 5

Market share and usage statistics 6

Key differences between the platforms 7

Platform-specific security features and challenges 8

Overview of Kali NetHunter 9

The origins and development of Kali NetHunter 9

Key features and capabilities 10

Setting up Kali NetHunter on Android devices 11

Introduction to the Kali NetHunter user interface 11

Common mobile application vulnerabilities 11

Insecure data storage 11

Improper handling of user input 12

Weak or broken authentication mechanisms 13

Insufficient transport layer protection 14

Emerging trends in mobile app security 15

The mobile penetration testing process 15

Reconnaissance: Information gathering on target apps 16

Vulnerability assessment 16

Exploitation - Gaining access through vulnerabilities 17

Reporting and remediation: Documenting and countermeasures 18

Technologies, software, and tools used in mobile penetration testing 19
Network scanning tools *19*
Web app testing tools *20*
Mobile app reverse engineering *20*
Exploit frameworks *21*
Vulnerability management tools *22*
Mobile penetration testing methodologies 22
Following a structured methodology *23*
Prioritizing risk based on the threat model *23*
Combining automated and manual testing techniques *24*
Staying current with threats and vulnerabilities *25*
Collaborating with developers and stakeholders *25*
Conclusion 26
Points to remember 27
Questions 27

2. Setting Up Your Device 29
Introduction 29
Structure 29
Objectives 30
Determining which device you need 30
Importance of device selection *30*
Criteria for choosing the right device *31*
Specifics of device compatibility 32
Rooting android devices 36
Tools for rooting *39*
Bootloader unlocking and custom recovery installation *40*
Configuring Kali NetHunter for Android devices 42
The importance of Kali NetHunter in mobile penetration testing *42*
Installing and configuring Kali NetHunter *43*
Understanding the functionality of Kali NetHunter *44*
Kali NetHunter for unrooted Android devices 44

Challenges of unrooted Android devices *44*
Deploying Kali NetHunter in a Chroot environment *45*
Jailbreaking iOS devices 46
The process of jailbreaking iOS devices *46*
Types of jailbreaks *47*
Jailbreaking tools *48*
Gaining root access and installing alternative app stores *49*
Virtual and emulated devices 50
The significance of virtual and emulated devices *50*
Android emulators and the Android virtual device manager *50*
iOS tools *51*
Conclusion 52
Points to remember 53
Questions *53*

3. Mobile Penetration Testing Methodology 55
Introduction 55
Structure 55
Objectives 56
Standard penetration testing 56
Planning and reconnaissance *57*
Scanning and enumeration *58*
Gaining access *60*
Maintaining access *60*
Analysis and reporting *61*
Mobile penetration testing 64
Conducting penetration testing of mobile devices 65
Planning and reconnaissance *66*
Static and dynamic analysis *67*
Device and filesystem analysis *70*
Network communication analysis *71*
Reporting *73*

Conducting penetration testing with mobile devices 74
Setup *75*
Scanning and reconnaissance *75*
Exploitation *76*
Post-exploitation and analysis *77*
Reporting *77*
Conclusion 78
Points to remember 79
Questions 79

4. Attacking Android Applications 81
Introduction 81
Structure 81
Objectives 82
Android history 82
Android internals 85
Android applications 86
Entry points *86*
Activities *86*
URL schemes *87*
Content providers *88*
Services *88*
Broadcast receivers *89*
Intents *89*
Intent Filters *90*
Android-specific idiosyncrasies 91
Sandbox environment 93
Permissions model 93
Secure interprocess communications 94
Paranoid networking 95
Hardware-backed security 95
Google Play Protect 96

Keystore 97
Android security testing 97
Vulnerabilities 98
Android malware 99
Man-in-the-middle attacks 100
Static analysis 101
Dynamic analysis 102
Conclusion 103
Points to remember 103
Questions 104

5. Attacking iOS Applications 105
Introduction 105
Structure 105
Objectives 106
History of iOS 106
iOS security mechanisms 108
Sandboxing 108
Code signing 109
Hardware-based security 111
App transport security 112
iOS Vulnerabilities 113
Client-side vulnerabilities 114
Testing toolkit for iOS 116
Malicious iOS applications 118
Network interception 120
Conclusion 121
Points to remember 122
Questions 122

6. Mobile Device Penetration Testing for Web Applications 123
Introduction 123
Structure 123

Objectives 124
Mobile device considerations 124
Explanation of vulnerabilities 127
Vulnerability details 128
APIs 131
API testing 134
Insecure data handling 135
Verbose error messages 135
Tools 136
Conclusion 139
Points to remember 139
Questions 139

7. Working with Kali NetHunter 141
Introduction 141
Structure 141
Objectives 142
Kali NetHunter 142
History of NetHunter 143
NetHunter tools 144
Terminal 146
BadUSB attack 147
Bluetooth-Arsenal 148
Chroot Manager 149
Components 149
Custom commands 150
DuckHunter attacks 151
Exploit Database SearchSploit 151
Human interface device keyboard attacks 152
Home screen 153
Kali services 154
KeX Manager 155
MAC Changer 156

Man in the Middle Framework *156*
MANA Evil Access Point *157*
Metasploit Payload Generator *158*
Nmap Scan *158*
Social Engineer Toolkit *159*
USB-Arsenal *159*
Conclusion 160
Points to remember 160
Questions 161

8. Advanced Pentesting Techniques 163
Introduction 163
Structure 163
Objectives 164
Advanced mobile network attacks and defenses 164
ARP Spoofing with Kali NetHunter *164*
DNS hijacking: Dnsmasq and Kali NetHunter *165*
SSL/TLS stripping: SSLstrip and Kali NetHunter *166*
Defensive configurations for mobile devices *167*
Exploiting mobile operating system vulnerabilities 168
Kernel-level exploits on Android and iOS *169*
Privilege escalation techniques in Android and iOS *169*
Remote code execution: Strategies and tools *170*
Kali NetHunter's role in facilitating mobile OS exploits *171*
Advanced binary exploitation techniques 172
Return-oriented programming in mobile environments *172*
Leveraging Kali NetHunter for advanced binary exploitation *173*
Bypassing mobile security mechanisms 174
Application sandboxing: The walls that contain *174*
Code signing: Authenticity versus vulnerability *175*
Secure boot *176*
Kali NetHunter in mobile security bypass *177*

Post-exploitation techniques on mobile devices 177
Data exfiltration: Securing the payload *178*
Lateral movement and pivoting *179*
Maintaining persistence *180*
Leveraging Kali NetHunter for efficient post-exploitation *181*
Peripheral device integration via OTG cables 182
HackRF and YardStick One: RF tactics *182*
Ubertooth and nRF51: Bluetooth hacking *184*
IoT and Wi-Fi exploits with Flipper Zero and Wi-Fi Pineapple *185*
SharkJack: Ethernet-based attacks *186*
Enhancing mobile pentesting with peripheral devices *187*
Conclusion 187
Points to remember 188
Questions 189

9. Developing a Vulnerability Remediation Plan 191
Introduction 191
Structure 192
Objectives 192
Creating effective penetration testing reports 192
Introduction to documentation tools *193*
Report structure *194*
Use of templates *195*
Communicating vulnerabilities to stakeholders 196
Audience segmentation *196*
Visual Aids *197*
Effective communication *198*
Developing remediation plans 199
OWASP Guidelines *199*
Creating action plans *200*
Prioritizing vulnerabilities 200
Risk assessment *201*

Calculating risk *202*
Tracking progress and verifying remediation 204
Progress tracking tools *205*
Jira *207*
Trello *207*
Communication management *208*
Conclusion 209
Points to remember 209
Questions 210

10. Detecting Vulnerabilities on Android Apps 211
Introduction 211
Structure 211
Objectives 212
Setting up your testing environment 212
Step 1: Configuring the Burp Proxy Listener *213*
Step 2: Device proxy configuration *214*
Step 3: Installation of CA Certificate *215*
Step 4: Configuration verification *215*
Special note for Android emulators *216*
The penetration test 216
From analysis to identification 217
Understanding vulnerable Android apps 218
Damn Insecure and Vulnerable App *219*
Initial preparations *219*
Choice of installation methods *219*
Navigating to the APK file location using command prompt *219*
Verifying the status of connected Android devices *220*
Executing the installation of the DIVA application *220*
Post-installation steps *220*
Launching the installed application *220*
Insecure logging *220*

Initiating the challenge 220
Preparing the command-line interface 221
Interaction and data entry 221
Analyzing the logs for insecure practices 221
Hardcoding Issues – Part 1 222
Initiating the hardcoding challenge 222
Understanding the context 222
File conversion and extraction 222
Dex to Jar conversion 222
Decompiling the JAR file 223
Retrieving the hardcoded vendor key 223
Insecure Data Storage – Part 1 223
Accessing the Android shell 223
User credentials and Shared Preferences 224
Retrieving stored data 224
Insecure Data Storage – Part 2 224
Preliminary credential storage 224
Using SQLite3 for database access 224
Insecure Data Storage – Part 3 225
Initial data entry 225
Identifying the temporary storage method 226
Accessing the temporary file via shell 226
Insecure Data Storage – Part 4 227
Entering credentials into the application 227
Identifying the storage mechanism 227
Accessing the external storage via shell 227
Input Validation Issues – Part 1 228
Initial input tests 228
Understanding output variations 228
Exploiting input validation flaws 228
Input Validation Issues – Part 2 228
Initial URL manipulation tests 229

Local File Access 229
Targeting Shared Preferences 229
Access Control Issues – Part 1 229
Initial legitimate access 230
Identifying the Target Activity 230
Attempting unauthorized access 230
Evaluating the access control mechanism 230
Access Control Issues – Part 2 231
Decompiling the application 231
Analyzing the AndroidManifest.XML file 231
Examining the Java code files 231
Locating the chk_pin parameter 231
Inspecting the strings.XML File 232
Attempting unauthorized access 232
Verifying the security flaw 232
Access Control Issues – Part 3 232
Understanding the supposed security measure 232
Bypassing access control with Content Provider 232
Evaluating the security implications 233
Hardcoding Issues – Part 2 233
Extracting the native library 233
String extraction and analysis 233
Verifying the hardcoded vulnerability 234
Input Validation Issues – Part 3 234
Preparing for input testing 234
Executing the test 234
Observing the outcome 234
InsecureBankv2 235
GoatDroid 235
Securing the future 235
Conclusion 237
Points to remember 237

Questions 237

11. Hands-on Practice: Vulnerable iOS Apps 239

Introduction 239

Structure 239

Objectives 240

Crafting the testing ground 240

Xcode 240

iOS Simulator 241

Burp Suite 241

Jailbroken iOS device 241

Peeling back the layers: Analysis and identification 242

Fortifying the Bastions 243

Vulnerable iOS apps: Learning from built-in flaws 245

Setting up your iOS device 245

Installing essential development and reverse engineering tools on macOS 247

iGoat 250

iGoat exercise side channel data leaks: Backgrounding 251

Cut and paste functionality: A double-edged sword 252

iGoat exercise reverse engineering: String analysis in iOS applications 252

Damn Vulnerable iOS App 253

Inspecting insecure data storage with DVIAv2 256

Plist Storage 256

UserDefaults 256

Keychain access 256

Core data 256

Webkit Caching 257

Realm storage 257

Couchbase Lite 257

YapDatabase 257

Conclusion 258

Points to remember 258

Questions 259

12. Mobile Security Career Roadmap 261
Introduction 261
Structure 261
Objectives 262
Navigating the complexities of mobile security 262
The journey toward expertise 263
Specialization 263
Laying the groundwork: a strong foundational base 264
Key skillsets for a career in mobile security 265
Programming prowess 265
Diving into mobile operating systems 266
Reverse engineering: The investigative art 267
The web of network security 268
Professional certifications 268
The renowned OSCP distinction 268
Certified Ethical Hacker 269
GIAC Mobile Device Security Analyst 270
GIAC Penetration Tester 270
TryHackMe badges 271
The Cyber Mentor certifications 271
eLearnSecurity certifications 272
Certified Information Systems Security Professional 272
Beyond the big names: Diverse certification landscape 273
Job roles in mobile security: Navigating career pathways 274
Penetration Testers 274
Mobile application security analysts 274
Mobile security researchers 275
Networking and community involvement 276
Global confluence at conferences and gatherings 276
Black Hat 277
DEF CON 278
RSA 279

BSides *279*
Hackers On Planet Earth Conference *280*
Chaos Computing Congress *281*
ShmooCon *281*
NullCon *282*
Code Blue *283*
AV Tokyo *283*
Other events 284
Meetups *284*
Workshops *284*
Round tables and discussion panels *285*
Open Web Application Security Project chapter meetings *285*
2600 Meetings *286*
Hackerspaces *286*
Virtual Hubs: Online Forums and Platforms *287*
Staying current 287
Security blogs and podcasts 287
Social media and influential figures *288*
Continuous learning *289*
Crafting a successful career in mobile security 289
The tangible proof: Building a portfolio *289*
Communication skills 290
Building bridges: Cultivating a professional network 291
Conclusion 292
Points to remember 292
Questions 292

13. The Future of Pentesting and Security Trends 295
Introduction 295
Structure 295
Objectives 296
Emerging security threats 296

Mobile payment systems *296*
AR and VR threats *297*
Artificial intelligence-based mobile threats *298*
Edge computing threats *299*
Advances in mobile security technologies 300
Encryption evolution *301*
Enhanced biometrics *302*
Secure boot mechanisms *303*
AI in mobile security 304
5G, IoT, and mobile security 305
Internet of Things *306*
The double-edged sword of expanded connectivity *307*
Edge computing and its nuances *308*
The 5G infrastructure *309*
The road ahead for mobile penetration testers 310
Conclusion 311
Points to remember 311
Questions 312

Index 313-322

Chapter 1
Introduction to Mobile Penetration Testing

Introduction

The digital landscape is undergoing a profound transformation driven by the ubiquitous presence of mobile devices. Smartphones and tablets have transcended their roles as mere communication tools, becoming integral to all aspects of daily life. This chapter opens by highlighting the growing need for mobile security in an era where these devices store sensitive personal and business data. We will explore the rise of smartphones and tablets and their profound impact on our daily lives, setting the stage for a deep dive into the criticality of mobile security. The journey from the early days of Android and iOS to their current market dominance provides essential context to understand their role in the digital age. As we progress, the chapter will unfold the unique security features and challenges inherent to these platforms, underlining why a specialized focus on mobile security is not just important but essential in today's tech-centric world.

Structure

In this chapter, we will discuss the following topics:

- The growing need for mobile security
- Mobile platforms: Android and iOS
- Overview of Kali NetHunter

- Common mobile application vulnerabilities
- The mobile penetration testing process
- Technologies, software, and tools used in mobile penetration testing
- Mobile penetration testing methodologies

Objectives

The primary objective of this chapter is to provide a practical guide to securing mobile devices and platforms. We will delve into platform-specific security aspects of Android and iOS, examining their histories, market shares, and the key differences that influence their security postures. A special focus will be on Kali NetHunter, a tool that epitomizes the convergence of mobile flexibility with powerful penetration testing capabilities. The chapter aims to equip readers with the knowledge to set up and effectively use Kali NetHunter, understand common mobile application vulnerabilities, and engage in rigorous mobile penetration testing processes. By integrating technologies, software, and tools essential for mobile security, we aim to present a structured methodology for mobile penetration testing, emphasizing the importance of staying current with emerging threats and vulnerabilities. This comprehensive approach ensures that readers are not only aware of the risks but are also prepared with the tools and techniques to address them, fostering a collaborative environment with developers and stakeholders to bolster mobile security.

The growing need for mobile security

In a world where mobile devices are increasingly integral at the core of personal and professional lives, the need for robust mobile security has never been more critical. This section delves into the escalating threats in the mobile landscape, where the convenience of smartphones and tablets comes with the heightened risk of cyberattacks. From sophisticated malware targeting mobile banking apps to exploiting vulnerabilities in operating systems and apps, the spectrum of threats is vast and evolving. We will examine the current state of mobile security, highlighting the emerging trends in attacks and the corresponding necessity for stronger defense mechanisms. This overview underscores the risks and sets the stage for understanding the tools and strategies essential for protecting mobile devices in this ever-connected digital era.

The rise of smartphones and tablets

The rise of smartphones and tablets can be traced back to the early 2000s when devices like the Palm Pilot and the Nokia Communicator began to combine the functionalities of a phone and a computer. The smartphone market exploded with the introduction of Apple's iPhone in 2007, followed by the release of the first Android-powered device in 2008. Today, smartphones and tablets have become integral to people's lives, offering

various functionalities, including communication, productivity, entertainment, and much more.

In the early 2000s, the landscape of mobile technology began a significant transformation with the introduction of devices that combined the capabilities of a phone and a computer. Among these early pioneers were the Palm Pilot and the Nokia Communicator. As these continued to evolve, they began offering an increasingly wide range of functionalities. Communication capabilities expanded beyond voice calls and text messages to include emails, instant messaging, and video calls. Productivity tools like calendars, note-taking apps, and document editing software became commonplace, allowing users to work independently. At the same time, mobile devices started to serve as portable entertainment centers, providing access to music, movies, games, and social media platforms.

The convergence of these diverse features in a single, handheld device transformed how people interacted with technology and each other. Smartphones and tablets became more than just tools; they became extensions of ourselves, intimately connected to our daily routines and personal identities. This deep integration of mobile technology into our lives has also resulted in a greater sense of connection with others, as we can now instantly share our experiences, thoughts, and emotions through various digital platforms.

As we embrace the convenience and connectivity smartphones and tablets offer, we must acknowledge the potential security risks accompanying these powerful devices. The widespread adoption of mobile technology has made it an attractive target for cybercriminals and hackers, who seek to exploit vulnerabilities and gain unauthorized access to sensitive data. Consequently, understanding and addressing mobile security concerns has become critical for responsible device usage in the digital age. As we continue to rely on mobile technology for communication, productivity, and entertainment, it is crucial that we also prioritize mobile security to protect our devices and the valuable information they contain.

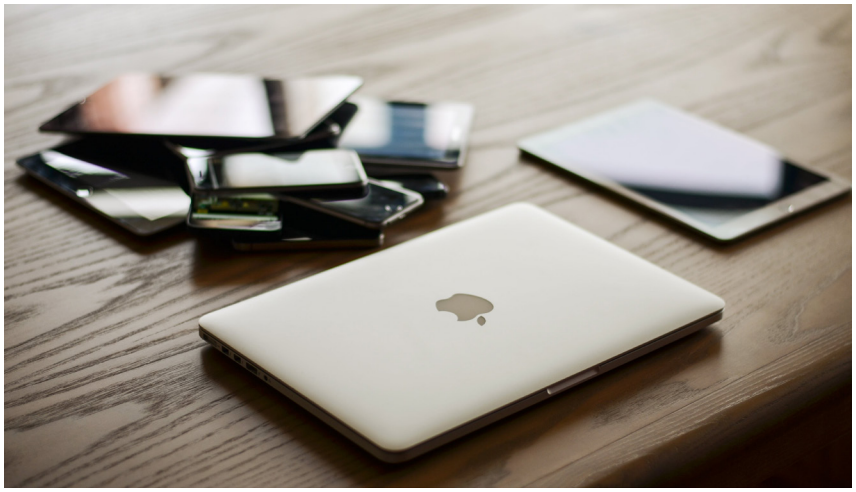

***Figure 1.1**: Examples of highly mobile technology*

The impact of mobile devices on daily life

One of the most significant changes mobile devices bring is the ease with which we can access information. With the world at our fingertips, we can instantly search for answers to questions, stay updated on current events, and learn about new topics at a moment's notice. This unprecedented access to information has not only empowered individuals but also fostered a more informed and engaged global community.

In addition to facilitating access to information, mobile devices have given rise to new forms of communication. Text messaging, social media, and video conferencing apps have expanded our ability to connect with others, transcending geographical boundaries and time constraints. These innovative communication channels have enabled us to share our thoughts, feelings, and experiences with friends, family, and strangers, fostering a sense of global connection and shared humanity.

Another remarkable aspect of mobile devices is their capacity to host an ever-growing range of applications designed to improve our daily lives. GPS navigation has revolutionized how we travel, making it easier than ever to explore unfamiliar places. Online banking and e-commerce apps have streamlined financial transactions, while social networking platforms and video streaming services provide endless entertainment and social interaction opportunities.

As we continue to rely on mobile devices for an increasing variety of tasks, the amount of personal and sensitive data being stored and transmitted through these devices has grown exponentially. From contact information and financial details to health records and private messages, our devices hold a treasure trove of data that is both valuable and vulnerable. This abundance of sensitive information has made mobile devices attractive targets for cybercriminals who seek to exploit security weaknesses and gain unauthorized access to our data.

Given these risks, we must prioritize mobile security and proactively protect our devices and their information. Staying informed about potential threats, following best practices for securing our devices, and remaining vigilant in the face of ever-evolving cyber risks, we can enjoy the many benefits of mobile technology while safeguarding our privacy and personal data.

Mobile security significance in the digital age

The pervasive use of mobile devices in our daily lives has led to an ever-growing need for robust security measures to safeguard the sensitive data these devices store and transmit. Cybercriminals have recognized the potential for exploiting vulnerabilities in both hardware and software as we rely more heavily on smartphones and tablets for various tasks. These bad actors aim to gain unauthorized access to personal information and infiltrate corporate networks, making mobile security a top priority in the digital age.

As cybercriminals increasingly target mobile platforms, individuals and businesses must proactively protect their devices and valuable information. This includes staying informed about potential threats, updating devices with the latest security patches, and following best practices for securing mobile devices. Taking these precautions, users can mitigate the risks associated with mobile technology and enjoy its many benefits with greater peace of mind.

In addition to the security challenges individual users face, the widespread adoption of mobile devices in the workplace has introduced new concerns for organizations. Often referred to as the **Bring Your Own Device** (**BYOD**) trend, this phenomenon involves employees using their devices for work-related tasks, blurring the lines between personal and professional data. While this approach can offer increased flexibility and productivity for employees, it also presents potential security risks that must be addressed by organizations.

To manage the security challenges associated with BYOD, organizations must develop comprehensive policies and guidelines that outline the proper use of personal devices in the workplace. This may include specifying which devices and applications are permitted, implementing secure methods for accessing corporate networks and data, and providing training and resources to help employees maintain the security of their devices. By establishing clear expectations and providing ongoing support, organizations can balance the benefits of BYOD and the need to protect sensitive data and resources.

Templates for this type of policy are widely available online, but the author recommends this one from PurpleSec:

https://purplesec.us/resources/cyber-security-policy-templates/bring-your-own-device/

Considering the many security challenges presented by the introduction of mobile devices into businesses and our daily lives, defenders need to understand what attackers already know. By gaining the ability to conduct penetration testing on and with mobile platforms, devices can be more robustly secured against attack. Through threat modeling and hands-on experience with attacking mobile devices, creating a more secure mobile device ecosystem will be possible.

Mobile platforms: Android and iOS

Although there have been other options along the way (Windows Phone OS was discontinued in 2015), the primary smartphone operating systems are Android and iOS. Although many options exist, such as Ubuntu Touch, PureOS, Blackberry OS, and Manjaro OS, the primary focus of this text will be Android and iOS. Let us take a look at each.

A brief history of Android and iOS

Android, the open-source mobile operating system developed by Google, debuted in 2008, revolutionizing the mobile technology landscape. The open-source nature of Android

offered a unique advantage, allowing manufacturers and developers to freely access and modify its code to suit their needs better. As a result, Android rapidly gained popularity and garnered support for a wide range of devices, from budget smartphones to high-end flagship models. This flexibility and versatility made Android an attractive choice for manufacturers and developers, who could tailor the platform to create unique user experiences.

Android's development was closely followed by the rise of its app ecosystem, which provided developers with the tools and resources to create an array of applications for Android devices. This vast and diverse app landscape has been instrumental in the widespread adoption of Android, giving users access to countless applications that cater to their specific needs and preferences. As the Android platform continues to evolve, its open-source roots remain a driving force behind its ongoing innovation and growth.

Meanwhile, iOS, the closed-source mobile operating system developed by Apple, was first introduced in 2007 with the launch of the groundbreaking iPhone. iOS quickly gained a reputation for its sleek design, intuitive user interface, and seamless user experience, setting a new standard for mobile technology. The success of the iPhone and the subsequent release of the iPad solidified iOS's position as a dominant force in the mobile device market, with Apple's products becoming synonymous with quality and innovation.

Apple's closed-source approach to iOS has allowed the company to maintain strict control over its hardware and software, ensuring a consistent and polished experience across its devices. This level of control has also enabled Apple to prioritize security and privacy features, providing users with a sense of trust and confidence in their devices. While the closed-source nature of iOS may limit customization options compared to Android, it has fostered a cohesive and user-friendly ecosystem that appeals to many consumers.

Android and iOS represent two distinct approaches to mobile operating systems, each with unique strengths and appeal. Android's open-source nature has allowed for a high degree of customization and flexibility, making it an attractive choice for various manufacturers and developers. On the other hand, iOS's closed-source model has enabled Apple to create a polished and cohesive ecosystem known for its sleek design and seamless user experience. Both platforms have played a pivotal role in shaping the mobile technology landscape, offering users various options to suit their preferences and needs.

Market share and usage statistics

Android and iOS are undoubtedly the two giants of the global smartphone market, with both platforms enjoying widespread popularity and success. Their combined dominance has shaped the mobile landscape, setting innovation and user experience standards. While Android and iOS share many similarities, their distinct differences have led to a significant disparity in market share, with Android taking the lead due to its widespread adoption by multiple manufacturers.

As of January 2024, according to StatCounter, Android held an impressive 69.94% of the global mobile operating system market share. This sizable lead can be attributed to several factors, including Android's open-source nature and support for various devices. With multiple manufacturers producing Android-powered smartphones and tablets, consumers can access various devices at various prices. This diversity and flexibility have contributed to Android's broad appeal and widespread adoption, allowing the platform to capture a substantial market share.

In contrast, iOS held around 29.32% of the global mobile operating system market share as of January 2024. While this figure may seem small compared to Android's dominance, it is essential to note that iOS is exclusively available on Apple's devices. Given Apple's focus on producing premium smartphones and tablets, its market share is considerable, reflecting the brand's strong appeal and loyal customer base. Apple's emphasis on design, user experience, and security has helped the company carve out a significant portion of the market despite the platform's exclusivity.

The dominance of Android and iOS in the global smartphone market is expected to continue, with both platforms constantly evolving and expanding their user base. Android's open-source approach and support for a diverse range of devices will likely continue to attract manufacturers and developers, further solidifying its market share. At the same time, Apple's commitment to design excellence, seamless user experience, and robust security features will ensure that iOS maintains its strong presence in the market.

Key differences between the platforms

Android and iOS, while both powerful and widely popular mobile operating systems, have several key differences that set them apart. One of the most significant differences between the two platforms is their approach to openness and customization. Android, being open-source, allows manufacturers and developers a high degree of flexibility in customizing the operating system to suit their specific needs. This openness has led to a diverse range of devices and user experiences within the Android ecosystem, catering to various preferences and budgets.

The open-source nature of Android also extends to its app distribution model, which permits the existence of third-party app stores alongside the official Google Play Store. This flexibility allows developers to distribute their apps through multiple channels while users can choose from a wider range of sources to find and install applications. However, it is essential to note that third-party app stores can sometimes pose security risks due to the potential presence of malicious apps. Users must exercise caution and ensure they download apps from trusted sources to maintain the security of their devices. We will be using a third-party app store for testing later, so the safe operation of third-party app stores is within the scope of this book.

Meanwhile, iOS adopts a closed-source approach, running exclusively on Apple devices such as the iPhone, iPad, and iPod Touch. This exclusivity ensures a consistent and polished