
Mobile Hacking Android Owasp

Bulletproof Android

Mobile Hacking

Mastering Android Security

Hacking Exposed Mobile

Hacking- The art Of Exploitation

AI Applications in Cyber Security and Communication Networks

Android Application Security Essentials

The Mobile Application Hacker's Handbook

Mobile Device Exploitation Cookbook

Learning Pentesting for Android Devices

Automated Security Analysis of Android and iOS Applications with Mobile Security Framework

iOS Hacker's Handbook

Wireless Penetration Testing: Up and Running

Practical IoT Hacking

Learn Ethical Hacking from Scratch

The Mobile Application Hacker's Handbook

Android Malware

Penetration Testing for Jobseekers

Hands-On Penetration Testing with Kali NetHunter

Hacking Wireless Access Points

Application Security for the Android Platform

Managed Code Rootkits

Penetration Testing

Mobile Application Security

Automated Security Analysis of Android and iOS Applications with Mobile Security Framework

Android Hacker's Handbook

Hacking Android
Ansible for DevOps
Hands-on Penetration Testing for Web Applications
CEH Certified Ethical Hacker Cert Guide
Bug Bounty Bootcamp
Cybersecurity – Attack and Defense Strategies
Android Best Practices
Hacking Web Apps
Practical Web Penetration Testing
Corporate Cybersecurity in the Aviation, Tourism, and Hospitality Sector
The Basics of Hacking and Penetration Testing
Mobile Application Penetration Testing
Ethical Hacker's Penetration Testing Guide
Certified Ethical Hacker Complete Training Guide with Practice Questions & Labs:

Mobile Hacking Android Owasp

Downloaded from ftp.wtvq.com by guest

FRANKLIN LIVIA

Bulletproof Android "O'Reilly Media, Inc."

HTML5 -- HTML injection & cross-site scripting (XSS) -- Cross-site request forgery (CSRF) -- SQL injection & data store manipulation
-- Breaking authentication schemes -- Abusing design deficiencies
-- Leveraging platform weaknesses -- Browser & privacy attacks.

Mobile Hacking No Starch Press

See your app through a hacker's eyes to find the real sources of vulnerability The Mobile Application Hacker's Handbook is a comprehensive guide to securing all mobile applications by approaching the issue from a hacker's point of view. Heavily practical, this book provides expert guidance toward discovering

and exploiting flaws in mobile applications on the iOS, Android, Blackberry, and Windows Phone platforms. You will learn a proven methodology for approaching mobile application assessments, and the techniques used to prevent, disrupt, and remediate the various types of attacks. Coverage includes data storage, cryptography, transport layers, data leakage, injection attacks, runtime manipulation, security controls, and cross-platform apps, with vulnerabilities highlighted and detailed information on the methods hackers use to get around standard security. Mobile applications are widely used in the consumer and enterprise markets to process and/or store sensitive data. There is currently little published on the topic of mobile security, but with over a million apps in the Apple App Store alone, the attack surface is significant. This book helps you secure mobile apps by

demonstrating the ways in which hackers exploit weak points and flaws to gain access to data. Understand the ways data can be stored, and how cryptography is defeated Set up an environment for identifying insecurities and the data leakages that arise Develop extensions to bypass security controls and perform injection attacks Learn the different attacks that apply specifically to cross-platform apps IT security breaches have made big headlines, with millions of consumers vulnerable as major corporations come under attack. Learning the tricks of the hacker's trade allows security professionals to lock the app up tight. For better mobile security and less vulnerable data, The Mobile Application Hacker's Handbook is a practical, comprehensive guide.

Mastering Android Security McGraw Hill Professional

Discover all the security risks and exploits that can threaten iOS-based mobile devices iOS is Apple's mobile operating system for the iPhone and iPad. With the introduction of iOS5, many security issues have come to light. This book explains and discusses them all. The award-winning author team, experts in Mac and iOS security, examines the vulnerabilities and the internals of iOS to show how attacks can be mitigated. The book explains how the operating system works, its overall security architecture, and the security risks associated with it, as well as exploits, rootkits, and other payloads developed for it. Covers iOS security architecture, vulnerability hunting, exploit writing, and how iOS jailbreaks work Explores iOS enterprise and encryption, code signing and memory protection, sandboxing, iPhone fuzzing, exploitation, ROP payloads, and baseband attacks Also examines kernel debugging and exploitation Companion website includes source

code and tools to facilitate your efforts iOS Hacker's Handbook arms you with the tools needed to identify, understand, and foil iOS attacks.

Hacking Exposed Mobile Syngress

Certified Ethical Hacker v10 Exam 312-50 Latest v10. This updated version includes three major enhancement, New modules added to cover complete CEHv10 blueprint. Book scrutinized to rectify grammar, punctuation, spelling and vocabulary errors. Added 150+ Exam Practice Questions to help you in the exam. CEHv10 Update CEH v10 covers new modules for the security of IoT devices, vulnerability analysis, focus on emerging attack vectors on the cloud, artificial intelligence, and machine learning including a complete malware analysis process. Our CEH workbook delivers a deep understanding of applications of the vulnerability analysis in a real-world environment. Information security is always a great challenge for networks and systems. Data breach statistics estimated millions of records stolen every day which evolved the need for Security. Almost each and every organization in the world demands security from identity theft, information leakage and the integrity of their data. The role and skills of Certified Ethical Hacker are becoming more significant and demanding than ever. EC-Council Certified Ethical Hacking (CEH) ensures the delivery of knowledge regarding fundamental and advanced security threats, evasion techniques from intrusion detection system and countermeasures of attacks as well as up-skill you to penetrate platforms to identify vulnerabilities in the architecture. CEH v10 update will cover the latest exam blueprint, comprised of 20 Modules which includes the practice of information security and hacking tools which are

popularly used by professionals to exploit any computer systems. CEHv10 course blueprint covers all five Phases of Ethical Hacking starting from Reconnaissance, Gaining Access, Enumeration, Maintaining Access till covering your tracks. While studying CEHv10, you will feel yourself into a Hacker's Mindset. Major additions in the CEHv10 course are Vulnerability Analysis, IoT Hacking, Focused on Emerging Attack Vectors, Hacking Challenges, and updates of latest threats & attacks including Ransomware, Android Malware, Banking & Financial malware, IoT botnets and much more. IPSpecialist CEH technology workbook will help you to learn Five Phases of Ethical Hacking with tools, techniques, and The methodology of Vulnerability Analysis to explore security loopholes, Vulnerability Management Life Cycle, and Tools used for Vulnerability analysis. DoS/DDoS, Session Hijacking, SQL Injection & much more. Threats to IoT platforms and defending techniques of IoT devices. Advance Vulnerability Analysis to identify security loopholes in a corporate network, infrastructure, and endpoints. Cryptography Concepts, Ciphers, Public Key Infrastructure (PKI), Cryptography attacks, Cryptanalysis tools and Methodology of Crypt Analysis. Penetration testing, security audit, vulnerability assessment, and penetration testing roadmap. Cloud computing concepts, threats, attacks, tools, and Wireless networks, Wireless network security, Threats, Attacks, and Countermeasures and much more.

Hacking- The art Of Exploitation Elsevier

Penetration testers simulate cyber attacks to find security weaknesses in networks, operating systems, and applications. Information security experts worldwide use penetration techniques to evaluate enterprise defenses. In Penetration

Testing, security expert, researcher, and trainer Georgia Weidman introduces you to the core skills and techniques that every pentester needs. Using a virtual machine-based lab that includes Kali Linux and vulnerable operating systems, you'll run through a series of practical lessons with tools like Wireshark, Nmap, and Burp Suite. As you follow along with the labs and launch attacks, you'll experience the key stages of an actual assessment—including information gathering, finding exploitable vulnerabilities, gaining access to systems, post exploitation, and more. Learn how to: -Crack passwords and wireless network keys with brute-forcing and wordlists -Test web applications for vulnerabilities -Use the Metasploit Framework to launch exploits and write your own Metasploit modules -Automate social-engineering attacks -Bypass antivirus software -Turn access to one machine into total control of the enterprise in the post exploitation phase You'll even explore writing your own exploits. Then it's on to mobile hacking—Weidman's particular area of research—with her tool, the Smartphone Pentest Framework. With its collection of hands-on lessons that cover key tools and strategies, Penetration Testing is the introduction that every aspiring hacker needs.

AI Applications in Cyber Security and Communication Networks
Packt Publishing Ltd

Bug Bounty Bootcamp teaches you how to hack web applications. You will learn how to perform reconnaissance on a target, how to identify vulnerabilities, and how to exploit them. You'll also learn how to navigate bug bounty programs set up by companies to reward security professionals for finding bugs in their web applications. Bug bounty programs are company-sponsored

programs that invite researchers to search for vulnerabilities on their applications and reward them for their findings. This book is designed to help beginners with little to no security experience learn web hacking, find bugs, and stay competitive in this booming and lucrative industry. You'll start by learning how to choose a program, write quality bug reports, and maintain professional relationships in the industry. Then you'll learn how to set up a web hacking lab and use a proxy to capture traffic. In Part 3 of the book, you'll explore the mechanisms of common web vulnerabilities, like XSS, SQL injection, and template injection, and receive detailed advice on how to find them and bypass common protections. You'll also learn how to chain multiple bugs to maximize the impact of your vulnerabilities. Finally, the book touches on advanced techniques rarely covered in introductory hacking books but that are crucial to understand to hack web applications. You'll learn how to hack mobile apps, review an application's source code for security issues, find vulnerabilities in APIs, and automate your hacking process. By the end of the book, you'll have learned the tools and techniques necessary to be a competent web hacker and find bugs on a bug bounty program.

Android Application Security Essentials Packt Publishing Ltd
Mobile Endgeräte, vor allem Smartphones und Tablets der Hersteller Apple und Google, sind inzwischen in fast jedem Haushalt vertreten. Auch in der Firmenwelt nehmen diese Geräte einen immer größeren Stellenwert ein und verarbeiten hochsensible Daten. Diese neuen Einsatzszenarien, gepaart mit Tausenden von Applikationen, schaffen neue Angriffsvektoren und Einfallstore in diese Geräte. Dieses Buch stellt die einzelnen

Angriffsszenarien und Schwachstellen in den verwendeten Applikationen detailliert vor und zeigt, wie Sie diese Schwachstellen aufspüren können. Am Beispiel der aktuellen Betriebssysteme (Android, iOS und Windows Mobile) erhalten Sie einen umfassenden Einblick ins Penetration Testing von mobilen Applikationen. Sie lernen typische Penetration-Testing-Tätigkeiten kennen und können nach der Lektüre Apps der großen Hersteller untersuchen und deren Sicherheit überprüfen. Behandelt werden u.a. folgende Themen: - Forensische Untersuchung des Betriebssystems, - Reversing von mobilen Applikationen, - SQL-Injection- und Path-Traversal-Angriffe, - Runtime-Manipulation von iOS-Apps mittels Cypcript, - Angriffe auf die HTTPS-Verbindung, - u.v.m. Vorausgesetzt werden fundierte Kenntnisse in Linux/Unix sowie erweiterte Kenntnisse in Java bzw. Objective-C.

The Mobile Application Hacker's Handbook John Wiley & Sons

The Basics of Hacking and Penetration Testing, Second Edition, serves as an introduction to the steps required to complete a penetration test or perform an ethical hack from beginning to end. The book teaches students how to properly utilize and interpret the results of the modern-day hacking tools required to complete a penetration test. It provides a simple and clean explanation of how to effectively utilize these tools, along with a four-step methodology for conducting a penetration test or hack, thus equipping students with the know-how required to jump start their careers and gain a better understanding of offensive security. Each chapter contains hands-on examples and exercises that are designed to teach learners how to interpret results and

utilize those results in later phases. Tool coverage includes: Backtrack Linux, Google reconnaissance, MetaGooFil, dig, Nmap, Nessus, Metasploit, Fast Track Autopwn, Netcat, and Hacker Defender rootkit. This is complemented by PowerPoint slides for use in class. This book is an ideal resource for security consultants, beginning InfoSec professionals, and students. - Each chapter contains hands-on examples and exercises that are designed to teach you how to interpret the results and utilize those results in later phases - Written by an author who works in the field as a Penetration Tester and who teaches Offensive Security, Penetration Testing, and Ethical Hacking, and Exploitation classes at Dakota State University - Utilizes the Kali Linux distribution and focuses on the seminal tools required to complete a penetration test

Mobile Device Exploitation Cookbook BPB Publications

This text introduces the spirit and theory of hacking as well as the science behind it all; it also provides some core techniques and tricks of hacking so you can think like a hacker, write your own hacks or thwart potential system attacks.

Learning Pentesting for Android Devices John Wiley & Sons

Web Applications are the core of any business today, and the need for specialized Application Security experts is increasing these days. Using this book, you will be able to learn Application Security testing and understand how to analyze a web application, conduct a web intrusion test, and a network infrastructure test.

Automated Security Analysis of Android and iOS Applications with Mobile Security Framework Cybellium Ltd

Examine, Attack, and Exploit Flaws and Vulnerabilities in

Advanced Wireless Networks KEY FEATURES ● Extensive hands-on lab instructions in using Kali Linux to crack wireless networks. ● Covers the misconceptions, failures, and best practices that can help any pen tester come up with their special cyber attacks. ● Extensive coverage of Android and iOS pentesting, as well as attacking techniques and simulated attack scenarios.

DESCRIPTION This book satisfies any IT professional's desire to become a successful ethical hacker who is willing to be employed in identifying and exploiting flaws in the organization's network environment. This book explains in detail how to conduct wireless penetration tests using a wide variety of tools to simulate cyber attacks on both Android and iOS mobile devices and wireless networks. This book walks you through the steps of wireless penetration testing from start to finish. Once Kali Linux has been installed on your laptop, as demonstrated, you will check the system requirements and install the wireless adapter. The book then explores the wireless LAN reconnaissance phase, which outlines the WEP and WPA/WPA2 security protocols and shows real-world attacks against them using Kali Linux tools like Aircrack-ng. Then, the book discusses the most recent and sophisticated cyberattacks that target access points and wireless devices and how to prepare a compelling and professionally presented report. As a bonus, it removes myths, addresses misconceptions, and corrects common misunderstandings that can be detrimental to one's professional credentials. Tips and advice that are easy to implement and can increase their marketability as a pentester are also provided, allowing them to quickly advance toward a satisfying career in the field. WHAT YOU WILL LEARN ● Learn all about breaking the WEP security

protocol and cracking authentication keys. ● Acquire the skills necessary to successfully attack the WPA/WPA2 protocol. ● Compromise the access points and take full control of the wireless network. ● Bring your laptop up to speed by setting up Kali Linux and a wifi adapter. ● Identify security flaws and scan for open wireless LANs. ● Investigate the process and steps involved in wireless penetration testing. WHO THIS BOOK IS FOR This book is primarily for pentesters, mobile penetration testing users, cybersecurity analysts, security engineers, and all IT professionals interested in pursuing a career in cybersecurity. Before diving into this book, familiarity with network security fundamentals is recommended. TABLE OF CONTENTS 1. Wireless Penetration Testing Lab Setup 2. Wireless Attacking Techniques and Methods 3. Wireless Information Gathering and Footprinting 4. Wireless Vulnerability Research 5. Gain Access to Wireless Network 6. Wireless Vulnerability Assessment 7. Client-side Attacks 8. Advanced Wireless Attacks 9. Wireless Post-Exploitation 10. Android Penetration Testing 11. iOS Penetration Testing 12. Reporting

iOS Hacker's Handbook Newnes

Hacking Wireless Access Points: Cracking, Tracking, and Signal Jacking provides readers with a deeper understanding of the hacking threats that exist with mobile phones, laptops, routers, and navigation systems. In addition, applications for Bluetooth and near field communication (NFC) technology continue to multiply, with athletic shoes, heart rate monitors, fitness sensors, cameras, printers, headsets, fitness trackers, household appliances, and the number and types of wireless devices all continuing to increase dramatically. The book demonstrates a

variety of ways that these vulnerabilities can be—and have been—exploited, and how the unfortunate consequences of such exploitations can be mitigated through the responsible use of technology. - Explains how the wireless access points in common, everyday devices can expose us to hacks and threats - Teaches how wireless access points can be hacked, also providing the techniques necessary to protect and defend data - Presents concrete examples and real-world guidance on how to protect against wireless access point attacks

Wireless Penetration Testing: Up and Running No Starch Press

The first comprehensive guide to discovering and preventing attacks on the Android OS As the Android operating system continues to increase its share of the smartphone market, smartphone hacking remains a growing threat. Written by experts who rank among the world's foremost Android security researchers, this book presents vulnerability discovery, analysis, and exploitation tools for the good guys. Following a detailed explanation of how the Android OS works and its overall security architecture, the authors examine how vulnerabilities can be discovered and exploits developed for various system components, preparing you to defend against them. If you are a mobile device administrator, security researcher, Android app developer, or consultant responsible for evaluating Android security, you will find this guide is essential to your toolbox. A crack team of leading Android security researchers explain Android security risks, security design and architecture, rooting, fuzz testing, and vulnerability analysis Covers Android application building blocks and security as well as debugging and auditing Android apps Prepares mobile device administrators, security

researchers, Android app developers, and security consultants to defend Android systems against attack Android Hacker's Handbook is the first comprehensive resource for IT professionals charged with smartphone security.

Practical IoT Hacking No Starch Press

This is an easy-to-follow guide, full of hands-on and real-world examples of applications. Each of the vulnerabilities discussed in the book is accompanied with the practical approach to the vulnerability, and the underlying security issue. This book is intended for all those who are looking to get started in Android security or Android application penetration testing. You don't need to be an Android developer to learn from this book, but it is highly recommended that developers have some experience in order to learn how to create secure applications for Android.

Learn Ethical Hacking from Scratch Packt Publishing Ltd
 Battle-Tested Best Practices for Securing Android Apps throughout the Development Lifecycle Android's immense popularity has made it today's #1 target for attack: high-profile victims include eHarmony, Facebook, and Delta Airlines, just to name a few. Today, every Android app needs to resist aggressive attacks and protect data, and in *Bulletproof Android™*, Godfrey Nolan shows you how. Unlike "black hat/gray hat" books, which focus on breaking code, this guide brings together complete best practices for hardening code throughout the entire development lifecycle. Using detailed examples from hundreds of apps he has personally audited, Nolan identifies common "anti-patterns" that expose apps to attack, and then demonstrates more secure solutions. Nolan covers authentication, networking, databases, server attacks, libraries, hardware, and more. He illuminates each

technique with code examples, offering expert advice on implementation and trade-offs. Each topic is supported with a complete sample app, which demonstrates real security problems and solutions. Learn how to Apply core practices for securing the platform Protect code, algorithms, and business rules from reverse engineering Eliminate hardcoding of keys, APIs, and other static data Eradicate extraneous data from production APKs Overcome the unique challenges of mobile authentication and login Transmit information securely using SSL Prevent man-in-the-middle attacks Safely store data in SQLite databases Prevent attacks against web servers and services Avoid side-channel data leakage through third-party libraries Secure APKs running on diverse devices and Android versions Achieve HIPAA or FIPS compliance Harden devices with encryption, SELinux, Knox, and MDM Preview emerging attacks and countermeasures This guide is a perfect complement to Nolan's *Android™ Security Essentials LiveLessons* (video training; ISBN-13: 978-0-13-382904-4) and reflects new risks that have been identified since the *LiveLessons* were released.

The Mobile Application Hacker's Handbook BPB Publications
 Convert Android to a powerful pentesting platform. Key Features Get up and running with Kali Linux NetHunter Connect your Android device and gain full control over Windows, OSX, or Linux devices Crack Wi-Fi passwords and gain access to devices connected over the same network collecting intellectual data Book Description Kali NetHunter is a version of the popular and powerful Kali Linux pentesting platform, designed to be installed on mobile devices. Hands-On Penetration Testing with Kali NetHunter will teach you the components of NetHunter and

how to install the software. You'll also learn about the different tools included and how to optimize and use a package, obtain desired results, perform tests, and make your environment more secure. Starting with an introduction to Kali NetHunter, you will delve into different phases of the pentesting process. This book will show you how to build your penetration testing environment and set up your lab. You will gain insight into gathering intellectual data, exploiting vulnerable areas, and gaining control over target systems. As you progress through the book, you will explore the NetHunter tools available for exploiting wired and wireless devices. You will work through new ways to deploy existing tools designed to reduce the chances of detection. In the concluding chapters, you will discover tips and best practices for integrating security hardening into your Android ecosystem. By the end of this book, you will have learned to successfully use a mobile penetration testing device based on Kali NetHunter and Android to accomplish the same tasks you would traditionally, but in a smaller and more mobile form factor. What you will learn

- Choose and configure a hardware device to use Kali NetHunter
- Use various tools during pentests
- Understand NetHunter suite components
- Discover tips to effectively use a compact mobile platform
- Create your own Kali NetHunter-enabled device and configure it for optimal results
- Learn to scan and gather information from a target
- Explore hardware adapters for testing and auditing wireless networks and Bluetooth devices

Who this book is for Hands-On Penetration Testing with Kali NetHunter is for pentesters, ethical hackers, and security professionals who want to learn to use Kali NetHunter for complete mobile penetration testing and are interested in

venturing into the mobile domain. Some prior understanding of networking assessment and Kali Linux will be helpful.

Android Malware Springer Science & Business Media

The definitive guide to hacking the world of the Internet of Things (IoT) -- Internet connected devices such as medical devices, home assistants, smart home appliances and more. Drawing from the real-life exploits of five highly regarded IoT security researchers, Practical IoT Hacking teaches you how to test IoT systems, devices, and protocols to mitigate risk. The book begins by walking you through common threats and a threat modeling framework. You'll develop a security testing methodology, discover the art of passive reconnaissance, and assess security on all layers of an IoT system. Next, you'll perform VLAN hopping, crack MQTT authentication, abuse UPnP, develop an mDNS poisoner, and craft WS-Discovery attacks. You'll tackle both hardware hacking and radio hacking, with in-depth coverage of attacks against embedded IoT devices and RFID systems. You'll also learn how to:

- Write a DICOM service scanner as an NSE module
- Hack a microcontroller through the UART and SWD interfaces
- Reverse engineer firmware and analyze mobile companion apps
- Develop an NFC fuzzer using Proxmark3
- Hack a smart home by jamming wireless alarms, playing back IP camera feeds, and controlling a smart treadmill

The tools and devices you'll use are affordable and readily available, so you can easily practice what you learn. Whether you're a security researcher, IT team member, or hacking hobbyist, you'll find Practical IoT Hacking indispensable in your efforts to hack all the things

REQUIREMENTS: Basic knowledge of Linux command line, TCP/IP, and programming

Penetration Testing for Jobseekers Packt Publishing Ltd
 Learn how to hack systems like black hat hackers and secure them like security experts
 Key Features Understand how computer systems work and their vulnerabilities Exploit weaknesses and hack into machines to test their security Learn how to secure systems from hackers
 Book Description This book starts with the basics of ethical hacking, how to practice hacking safely and legally, and how to install and interact with Kali Linux and the Linux terminal. You will explore network hacking, where you will see how to test the security of wired and wireless networks. You'll also learn how to crack the password for any Wi-Fi network (whether it uses WEP, WPA, or WPA2) and spy on the connected devices. Moving on, you will discover how to gain access to remote computer systems using client-side and server-side attacks. You will also get the hang of post-exploitation techniques, including remotely controlling and interacting with the systems that you compromised. Towards the end of the book, you will be able to pick up web application hacking techniques. You'll see how to discover, exploit, and prevent a number of website vulnerabilities, such as XSS and SQL injections. The attacks covered are practical techniques that work against real systems and are purely for educational purposes. At the end of each section, you will learn how to detect, prevent, and secure systems from these attacks. What you will learn Understand ethical hacking and the different fields and types of hackers Set up a penetration testing lab to practice safe and legal hacking Explore Linux basics, commands, and how to interact with the terminal Access password-protected networks and spy on connected clients Use server and client-side attacks to hack and

control remote computers Control a hacked system remotely and use it to hack other systems Discover, exploit, and prevent a number of web application vulnerabilities such as XSS and SQL injections Who this book is for Learning Ethical Hacking from Scratch is for anyone interested in learning how to hack and test the security of systems like professional hackers and security experts.

Hands-On Penetration Testing with Kali NetHunter Packt Publishing Ltd

With the Android platform fast becoming a target of malicious hackers, application security is crucial. This concise book provides the knowledge you need to design and implement robust, rugged, and secure apps for any Android device. You'll learn how to identify and manage the risks inherent in your design, and work to minimize a hacker's opportunity to compromise your app and steal user data. How is the Android platform structured to handle security? What services and tools are available to help you protect data? Up until now, no single resource has provided this vital information. With this guide, you'll learn how to address real threats to your app, whether or not you have previous experience with security issues. Examine Android's architecture and security model, and how it isolates the filesystem and database Learn how to use Android permissions and restricted system APIs Explore Android component types, and learn how to secure communications in a multi-tier app Use cryptographic tools to protect data stored on an Android device Secure the data transmitted from the device to other parties, including the servers that interact with your app
[Hacking Wireless Access Points](#) Syngress

Understand and Conduct Ethical Hacking and Security Assessments

KEY FEATURES

- Practical guidance on discovering, assessing, and mitigating web, network, mobile, and wireless vulnerabilities.
- Experimentation with Kali Linux, Burp Suite, MobSF, Metasploit and Aircrack-suite.
- In-depth explanation of topics focusing on how to crack ethical hacking interviews.

DESCRIPTION Penetration Testing for Job Seekers is an attempt to discover the way to a spectacular career in cyber security, specifically penetration testing. This book offers a practical approach by discussing several computer and network fundamentals before delving into various penetration testing approaches, tools, and techniques. Written by a veteran security professional, this book provides a detailed look at the dynamics that form a person's career as a penetration tester. This book is divided into ten chapters and covers numerous facets of penetration testing, including web application, network, Android application, wireless penetration testing, and creating excellent penetration test reports. This book also shows how to set up an in-house hacking lab from scratch to improve your skills. A penetration tester's professional path, possibilities, average day, and day-to-day obstacles are all outlined to help readers better grasp what they may anticipate from a cybersecurity career.

Using this book, readers will be able to boost their employability and job market relevance, allowing them to sprint towards a lucrative career as a penetration tester.

WHAT YOU WILL LEARN

- Perform penetration testing on web apps, networks, android apps, and wireless networks.
- Access to the most widely used penetration testing methodologies and standards in the industry.
- Use an artistic approach to find security holes in source code.
- Learn how to put together a high-quality penetration test report.
- Popular technical interview questions on ethical hacker and pen tester job roles.
- Exploration of different career options, paths, and possibilities in cyber security.

WHO THIS BOOK IS FOR This book is for aspiring security analysts, pen testers, ethical hackers, anyone who wants to learn how to become a successful pen tester. A fundamental understanding of network principles and workings is helpful but not required.

TABLE OF CONTENTS

1. Cybersecurity, Career Path, and Prospects
2. Introduction to Penetration Testing
3. Setting Up Your Lab for Penetration Testing
4. Web Application and API Penetration Testing
5. The Art of Secure Source Code Review
6. Penetration Testing Android Mobile Applications
7. Network Penetration Testing
8. Wireless Penetration Testing
9. Report Preparation and Documentation
10. A Day in the Life of a Pen Tester