Xda Developers Android Hackers Toolkit The Complete Guide To Rooting Roms And Theming By Tyler Jasonjune 5 2012 Paperback

Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications SecurityFlutter in ActionDecompiling AndroidMy Surface 2The Mobile Application Hacker's HandbookDigital Forensics and Cyber CrimeMastering Kali Linux for Advanced Penetration Testing50 Android HacksAdvanced Penetration TestingUnboxing Android USBXDA Developers' Android Hacker's ToolkitAndroid System ProgrammingCybersecurity ??? Attack and Defense StrategiesGoogle Apps HacksGray Hat Hacking, Second EditionAdvances in Digital Forensics XIIUbuntu 20.04 EssentialsHacking: the Unlocking of TransparencyAndroid ForensicsAndroid Hacker's HandbookFlutter ProjectsApp Inventor for AndroidMastering MetasploitInformation Security and Privacy ResearchThe Browser Hacker's HandbookSmashing Android UIAndroid MalwareSecurity Testing With Kali NethunterXDA Developers' Android Hacker's ToolkitHacking AndroidAndroid Security CookbookHacking Exposed MobileLearning Android ForensicsApplied Cryptography and Network SecurityMetasploit Penetration Testing CookbookThe Imaginary AppExam 98-349 MTA Windows Operating System FundamentalsEmbedded AndroidKali Linux - An Ethical Hacker's CookbookPython Hacking Essentials

Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security

Summary The best programming techniques are often the shortest and simplest—the hacks. In this compact and infinitely useful book, Android expert Carlos Sessa delivers 50 hacks that will save you time, stretch your skills, and maybe even make you smile. About this Book Hacks. Clever programming techniques to solve thorny little problems. Ten lines of code that save you two days of work. The little gems you learn from the old guy in the next cube or from the geniuses on Stack Overflow. That's just what you'll find in this compact and useful book. The name 50 Android Hacks says it all. Ranging from the mundane to the spectacular, each self-contained, fully illustrated hack is just a couple of pages long and includes annotated source code. These practical techniques are organized into twelve collections covering layout, animations, patterns, and more. What's Inside Hack 3 Creating a custom ViewGroup Hack 8 Slideshow using the Ken Burns effect Hack 20 The Model-View-Presenter pattern Hack 23 The SyncAdapter pattern Hack 31 Aspect-oriented programming in Android Hack 34 Using Scala inside Android Hack 43 Batching database operations Plus 43 more hacks! Most hacks work with Android 2.x and greater. Version-specific hacks are clearly marked. Purchase of the print book includes a free eBook in PDF, Kindle, and ePub formats from Manning Publications. About the Author Carlos Sessa is a passionate professional Android developer. He's active on Stack Overflow and is an avid hack collector. Table of Contents Working your way around layouts Creating cool animations View tips and tricks Tools Patterns Working with lists and adapters Useful libraries Interacting with other languages Ready-to-use snippets Beyond database basics Avoiding fragmentation Building tools

Flutter in Action

Make your Android device truly your own Are you eager to make your Android device your own but you're not sure where to start? Then this is the book for you. XDA is the world's most popular resource for Android hacking enthusiasts, and a huge community has grown around customizing Android devices with XDA. XDA's Android Hacker's Toolkit gives you the tools you need to customize your devices by hacking or rooting the android operating system. Providing a solid understanding of the internal workings of the Android operating system, this book walks you through the terminology and functions of the android operating system from the major nodes of the file system to basic OS operations. As you learn the fundamentals of Android hacking that can be used regardless of any new releases, you'll discover exciting ways to take complete control over your device. Teaches theory, preparation and practice, and understanding of the OS Explains the distinction between ROMing and theming Provides step-by-step instructions for Droid, Xoom, Galaxy Tab, LG Optimus, and more Identifies the right tools for various jobs Contains new models enabling you to root and customize your phone Offers incomparable information that has been tried and tested by the amazing XDA community of hackers, gadgeteers, and technicians XDA's Android Hacker's Toolkit is a simple, one-stop resource on hacking techniques for beginners.

Decompiling Android

This book constitutes the refereed proceedings of the 11th International Conference on Applied Cryptography and Network Security, ACNS 2013, held in Banff, Canada, in June 2013. The 33 revised full papers included in this volume were carefully reviewed and selected from 192 submissions. They are organized in topical sections on Cloud Cryptography; Secure Computation; Hash Function and Block Cipher; Signature; System Attack; Secure Implementation - Hardware; Secure Implementation - Software; Group-oriented Systems; Key Exchange and Leakage Resilience; Cryptographic Proof; Cryptosystems.

My Surface 2

Over 120 recipes to perform advanced penetration testing with Kali Linux About This Book Practical recipes to conduct effective penetration testing using the powerful Kali Linux Leverage tools like Metasploit, Wireshark, Nmap, and many more to detect vulnerabilities with ease Confidently perform networking and application attacks using task-oriented recipes Who This Book Is For This book is aimed at IT security professionals, pentesters, and security analysts who have basic knowledge of Kali Linux and want to conduct advanced penetration testing techniques. What You Will Learn Installing, setting up and customizing Kali for pentesting on multiple platforms Pentesting routers and embedded devices Bug hunting 2017 Pwning and escalating through corporate network Buffer overflows 101 Auditing wireless networks Fiddling around with software-defned radio Hacking on the run with NetHunter Writing good quality reports In Detail With the current rate of hacking, it is very important to pentest your environment in order to ensure advanced-level security. This book is packed with practical recipes that will quickly get you started with Kali Linux (version 2016.2) according to your needs, and move

on to core functionalities. This book will start with the installation and configuration of Kali Linux so that you can perform your tests. You will learn how to plan attack strategies and perform web application exploitation using tools such as Burp, and Jexboss. You will also learn how to perform network exploitation using Metasploit, Sparta, and Wireshark. Next, you will perform wireless and password attacks using tools such as Patator, John the Ripper, and airoscript-ng. Lastly, you will learn how to create an optimum quality pentest report! By the end of this book, you will know how to conduct advanced penetration testing thanks to the book's crisp and task-oriented recipes. Style and approach This is a recipe-based book that allows you to venture into some of the most cutting-edge practices and techniques to perform penetration testing with Kali Linux.

The Mobile Application Hacker's Handbook

Create Android mobile apps, no programming required! Even with limited programming experience, you can easily learn to create apps for the Android platform with this complete guide to App Inventor for Android. App Inventor for Android is a visual language that relies on simple programming blocks that users can drag and drop to create apps. This handy book gives you a series of fully worked-out apps, complete with their programming blocks, which you can customize for your own use or use as a starting point for creating the next killer app. And it's all without writing a single line of code. Don't miss the book's special section on Apps Inventor Design Patterns, which explains computer terms in simple terms and is an invaluable basic reference. Teaches programmers and non-programmers alike how to use App Inventor for Android to create Android apps Provides a series of fully worked-out apps that you can customize, download, and use on your Android phone or use as a starting point for building the next great app Includes a valuable reference section on App Inventor Design Patterns and general computer science concepts Shows you how to create apps that take advantage of the Android smartphone?s handy features, such as GPS, messaging, contacts, and more With App Inventor for Android and this complete guide, you'll soon be creating apps that incorporate all of the Android smartphone's fun features, such as the accelerometer, GPS, messaging, and more.

Digital Forensics and Cyber Crime

Target Audience This book is not for professional hackers. Instead, this book is made for beginners who have programming experience and are interested in hacking. Here, hacking techniques that can be easily understood have been described. If you only have a home PC, you can test all the examples provided here. I have included many figures that are intuitively understandable rather than a litany of explanations. Therefore, it is possible to gain some practical experience while hacking, since I have only used examples that can actually be implemented. This book is therefore necessary for ordinary people who have a curiosity of hackers and are interested in computers. Organization of the Book This book is made up of five major parts, from basic knowledge to actual hacking code. A beginner is naturally expected to become a hacker while reading this book. Hacking Preparation Briefly introduce the basic Python syntax that is necessary for hacking. Application Hacking Introduce the basic skills to hack an application, such as Keyboard hooking, API hooking and image file hacking. Web Hacking The Virtual

Box test environment configuration is used for a Web Shell attack to introduce web hacking, which is currently an important issue. The techniques include SQL Injection, Password Cracking, and a Web Shell Attack. Network Hacking A variety of tools and the Python language can be combined to support network hacking and to introduce the network hacking technique. Briefly, we introduce NMap with the Wireshark tool, and hacking techniques such as Port Scanning, Packet Sniffing, TCP SYN Flood, Slowris Attack are introduced. System Hacking System hacking is difficult to understand for beginners, and in this section, figures are used to introduce difficult concepts. The hacking techniques that are introduced include a Backdoor, Registry Handling, Stack Based Buffer Overflow, and SEH Based Buffer Overflow. While reading this book, it is possible to obtain answers for such problems one by one. After reading the last chapter, you will gain the confidence to be a hacker. Features of this book When you start to study hacking, the most difficult task is to configure the test environment. There are many problems that need to be addressed, such as choosing from the variety in operating systems, obtaining expensive equipment and using complex technology. Such problems are too difficult to take in at once, so this book overcomes this difficulty by implementing a simple idea. First, systems will be described as Windows-based. We are very familiar with Windows, so it is very easy to understand a description based on Windows. Since Windows, Linux, Unix, and Android are all operating systems, it is possible to expand the concepts that are discussed here. Second, we use a virtual machine called Virtual Box. For hacking, it is necessary to connect at least three or more computers on a network. Since it is a significant investment to buy a few computers only to study these techniques, a virtual machine can be used instead to easily implement a honeypot necessary to hack by creating multiple virtual machines on a single PC. Finally, abstract concepts are explained using figures. Rather than simply using words for descriptions, graphics are very effective in transferring information. An abstract concept can materialize through the use of graphics in order to improve the understanding on the part of the reader.

Mastering Kali Linux for Advanced Penetration Testing

Arguably one of the most highly regarded and widely used enterprise level operating systems available today is the Ubuntu 20.04 distribution. Not only is it considered to be among the most stable and reliable operating systems, it is also backed by the considerable resources and technical skills of Canonical, Ltd. Ubuntu 20.04 Essentials is designed to provide detailed information on the installation, use and administration of the Ubuntu 20.04 distribution. For beginners, the book covers topics such as operating system installation, the basics of the GNOME desktop environment, configuring email and web servers and installing packages and system updates. Additional installation topics such as dual booting with Microsoft Windows are also covered, together with all important security topics such as configuring a firewall and user and group administration. For the experienced user, topics such as remote desktop access, the Cockpit web interface, logical volume management (LVM), disk partitioning, swap management, KVM virtualization, Secure Shell (SSH), Linux Containers and file sharing using both Samba and NFS are covered in detail to provide a thorough overview of this enterprise class operating system.

50 Android Hacks

Unboxing Android USB focuses on apps that use USB. This book covers everything starting from simple tasks like managing media with USB to complex tasks like Android ADB and developing application which exploit the potential of USB framework. With use cases that help developers build real world apps in real-time utilizing the advanced features of USB framework Unboxing Android USB tries to cover every single aspect of the app development cycle in totality. Unboxing Android USB helps you learn newly introduced android open accessory protocol with unique examples such as using USB Keyboard with Android device without USB host mode enabled and switching from MTP to MSC. The book is organized based on the USB functions, with each chapter explaining different USB classes available in Android. The functionalities are explained by starting from the USB specification followed by block diagrams that explain different blocks available in that USB class, followed by sequence diagram that elucidates flow of control and data. Each chapter has a unique sample Android application that uses the particular USB function.

Advanced Penetration Testing

"A fantastic book for anyone looking to learn the tools and techniques needed to break in and stay in." --Bruce Potter, Founder, The Shmoo Group "Very highly recommended whether you are a seasoned professional or just starting out in the security business." --Simple Nomad, Hacker

Unboxing Android USB

Explore every nook and cranny of the Android OS to modify your device and guard it against security threats About This Book Understand and counteract against offensive security threats to your applications Maximize your device's power and potential to suit your needs and curiosity See exactly how your smartphone's OS is put together (and where the seams are) Who This Book Is For This book is for anyone who wants to learn about Android security. Software developers, QA professionals, and beginner- to intermediate-level security professionals will find this book helpful. Basic knowledge of Android programming would be a plus. What You Will Learn Acquaint yourself with the fundamental building blocks of Android Apps in the right way Pentest Android apps and perform various attacks in the real world using real case studies Take a look at how your personal data can be stolen by malicious attackers Understand the offensive maneuvers that hackers use Discover how to defend against threats Get to know the basic concepts of Android rooting See how developers make mistakes that allow attackers to steal data from phones Grasp ways to secure your Android apps and devices Find out how remote attacks are possible on Android devices In Detail With the mass explosion of Android mobile phones in the world, mobile devices have become an integral part of our everyday lives. Security of Android devices is a broad subject that should be part of our everyday lives to defend against ever-growing smartphone attacks. Everyone, starting with end users all the way up to developers and security professionals should care about android security. Hacking Android is a step-by-step guide that will get you started with Android security. You'll begin your journey at

the absolute basics, and then will slowly gear up to the concepts of Android rooting, application security assessments, malware, infecting APK files, and fuzzing. On this journey you'll get to grips with various tools and techniques that can be used in your everyday pentests. You'll gain the skills necessary to perform Android application vulnerability assessment and penetration testing and will create an Android pentesting lab. Style and approach This comprehensive guide takes a step-by-step approach and is explained in a conversational and easy-to-follow style. Each topic is explained sequentially in the process of performing a successful penetration test. We also include detailed explanations as well as screenshots of the basic and advanced concepts.

XDA Developers' Android Hacker's Toolkit

A comprehensive and detailed, step by step tutorial guide that takes you through important aspects of the Metasploit framework. If you are a penetration tester, security engineer, or someone who is looking to extend their penetration testing skills with Metasploit, then this book is ideal for you. The readers ofthis book must have a basic knowledge of using Metasploit. They are also expected to have knowledge of exploitation and an indepth understanding of object-oriented programming languages.

Android System Programming

Build a better defense against motivated, organized, professional attacks Advanced Penetration Testing: Hacking the World's Most Secure Networks takes hacking far beyond Kali linux and Metasploit to provide a more complex attack simulation. Featuring techniques not taught in any certification prep or covered by common defensive scanners, this book integrates social engineering, programming, and vulnerability exploits into a multidisciplinary approach for targeting and compromising high security environments. From discovering and creating attack vectors, and moving unseen through a target enterprise, to establishing command and exfiltrating data—even from organizations without a direct Internet connection—this guide contains the crucial techniques that provide a more accurate picture of your system's defense. Custom coding examples use VBA, Windows Scripting Host, C, Java, JavaScript, Flash, and more, with coverage of standard library applications and the use of scanning tools to bypass common defensive measures. Typical penetration testing consists of low-level hackers attacking a system with a list of known vulnerabilities, and defenders preventing those hacks using an equally well-known list of defensive scans. The professional hackers and nation states on the forefront of today's threats operate at a much more complex level—and this book shows you how to defend your high security network. Use targeted social engineering pretexts to create the initial compromise Leave a command and control structure in place for long-term access Escalate privilege and breach networks, operating systems, and trust structures Infiltrate further using harvested credentials while expanding control Today's threats are organized, professionally-run, and very much for-profit. Financial institutions, health care organizations, law enforcement, government agencies, and other high-value targets need to harden their IT infrastructure and human capital against targeted advanced attacks from motivated professionals. Advanced Penetration Testing goes beyond Kali linux and Metasploit and to provide you advanced pen

testing for high security networks.

Cybersecurity ??? Attack and Defense Strategies

Proven security tactics for today's mobile apps, devices, and networks "A great overview of the new threats created by mobile devices. The authors have heaps of experience in the topics and bring that to every chapter." -- Slashdot Hacking Exposed Mobile continues in the great tradition of the Hacking Exposed series, arming business leaders and technology practitioners with an in-depth understanding of the latest attacks and countermeasures--so they can leverage the power of mobile platforms while ensuring that security risks are contained." -- Jamil Farshchi, Senior Business Leader of Strategic Planning and Initiatives, VISA Identify and evade key threats across the expanding mobile risk landscape. Hacking Exposed Mobile: Security Secrets & Solutions covers the wide range of attacks to your mobile deployment alongside ready-to-use countermeasures. Find out how attackers compromise networks and devices, attack mobile services, and subvert mobile apps. Learn how to encrypt mobile data, fortify mobile platforms, and eradicate malware. This cutting-edge guide reveals secure mobile development guidelines, how to leverage mobile OS features and MDM to isolate apps and data, and the techniques the pros use to secure mobile payment systems. Tour the mobile risk ecosystem with expert guides to both attack and defense Learn how cellular network attacks compromise devices over-the-air See the latest Android and iOS attacks in action, and learn how to stop them Delve into mobile malware at the code level to understand how to write resilient apps Defend against server-side mobile attacks, including SQL and XML injection Discover mobile web attacks, including abuse of custom URI schemes and JavaScript bridges Develop stronger mobile authentication routines using OAuth and SAML Get comprehensive mobile app development security guidance covering everything from threat modeling to iOS- and Android-specific tips Get started quickly using our mobile pen testing and consumer security checklists

Google Apps Hacks

They consider the control and power exercised by software architecture; the app's prosthetic ability to enhance certain human capacities, in reality or in imagination; the app economy, and the divergent possibilities it offers of making a living or making a fortune; and the app as medium and remediator of reality. Also included (and documented in color) are selected projects by artists asked to design truly imaginary apps, "icons of the impossible." These include a female sexual arousal graph using Doppler images; "The Ultimate App," which accepts a payment and then closes, without providing information or functionality; and "iLuck," which uses GPS technology and four-leaf-clover icons to mark places where luck might be found. ContributorsChristian Ulrik Andersen, Thierry Bardini, Nandita Biswas Mellamphy, Benjamin H. Bratton, Drew S.

Gray Hat Hacking, Second Edition

A practical guide to testing your infrastructure security with Kali Linux, the preferred choice of pentesters and hackers Key Features Employ advanced

pentesting techniques with Kali Linux to build highly secured systems Discover various stealth techniques to remain undetected and defeat modern infrastructures Explore red teaming techniques to exploit secured environment Book Description This book takes you, as a tester or security practitioner, through the reconnaissance, vulnerability assessment, exploitation, privilege escalation, and post-exploitation activities used by pentesters. To start with, you'll use a laboratory environment to validate tools and techniques, along with an application that supports a collaborative approach for pentesting. You'll then progress to passive reconnaissance with open source intelligence and active reconnaissance of the external and internal infrastructure. You'll also focus on how to select, use, customize, and interpret the results from different vulnerability scanners, followed by examining specific routes to the target, which include bypassing physical security and the exfiltration of data using a variety of techniques. You'll discover concepts such as social engineering, attacking wireless networks, web services, and embedded devices. Once you are confident with these topics, you'll learn the practical aspects of attacking user client systems by backdooring with fileless techniques, followed by focusing on the most vulnerable part of the network – directly attacking the end user. By the end of this book, you'll have explored approaches for carrying out advanced pentesting in tightly secured environments, understood pentesting and hacking techniques employed on embedded peripheral devices. What you will learn Configure the most effective Kali Linux tools to test infrastructure security Employ stealth to avoid detection in the infrastructure being tested Recognize when stealth attacks are being used against your infrastructure Exploit networks and data systems using wired and wireless networks as well as web services Identify and download valuable data from target systems Maintain access to compromised systems Use social engineering to compromise the weakest part of the network - the end users Who this book is for This third edition of Mastering Kali Linux for Advanced Penetration Testing is for you if you are a security analyst, pentester, ethical hacker, IT professional, or security consultant wanting to maximize the success of your infrastructure testing using some of the advanced features of Kali Linux. Prior exposure of penetration testing and ethical hacking basics will be helpful in making the most out of this book.

Advances in Digital Forensics XII

Security Testing with Kali NetHunter Kali Linux NetHunter is an Ethical Hacking platform that allows you to run a mobile version of Kali Linux on a supported Android device. In Security Testing with Kali NetHunter, you will see the basic usage of NetHunter as we walk through the entire NetHunter tool menu, and learn by doing with hands on step-by-step tutorials. Topics Include: Kali NetHunter Introduction and Overview Shodan App (the "Hacker's Google") Using cSploit & DriveDroid Exploiting Windows and Linux Systems Human Interface Device Attacks Man-in-the-Middle Attacks Wi-Fi Attacks Metasploit Payload Generator Using NetHunter with a WiFi Pineapple Nano NetHunter not only brings the power of Kali Linux to a portable device, it also brings an inherent level of stealth to Ethical Hackers and Pentesters by the very fact that smartphones are in use everywhere.

Ubuntu 20.04 Essentials

Over 100 recipes for penetration testing using Metasploit and virtual machines Key

Features Special focus on the latest operating systems, exploits, and penetration testing techniques Learn new anti-virus evasion techniques and use Metasploit to evade countermeasures Automate post exploitation with AutoRunScript Exploit Android devices, record audio and video, send and read SMS, read call logs, and much more Build and analyze Metasploit modules in Ruby Integrate Metasploit with other penetration testing tools Book Description Metasploit is the world's leading penetration testing tool and helps security and IT professionals find, exploit, and validate vulnerabilities. Metasploit allows penetration testing automation, password auditing, web application scanning, social engineering, post exploitation, evidence collection, and reporting. Metasploit's integration with InsightVM (or Nexpose), Nessus, OpenVas, and other vulnerability scanners provides a validation solution that simplifies vulnerability prioritization and remediation reporting. Teams can collaborate in Metasploit and present their findings in consolidated reports. In this book, you will go through great recipes that will allow you to start using Metasploit effectively. With an ever increasing level of complexity, and covering everything from the fundamentals to more advanced features in Metasploit, this book is not just for beginners but also for professionals keen to master this awesome tool. You will begin by building your lab environment, setting up Metasploit, and learning how to perform intelligence gathering, threat modeling, vulnerability analysis, exploitation, and post exploitation—all inside Metasploit. You will learn how to create and customize payloads to evade anti-virus software and bypass an organization's defenses, exploit server vulnerabilities, attack client systems, compromise mobile phones, automate post exploitation, install backdoors, run keyloggers, highjack webcams, port public exploits to the framework, create your own modules, and much more. What you will learn Set up a complete penetration testing environment using Metasploit and virtual machines Master the world's leading penetration testing tool and use it in professional penetration testing Make the most of Metasploit with PostgreSQL, importing scan results, using workspaces, hosts, loot, notes, services, vulnerabilities, and exploit results Use Metasploit with the Penetration Testing Execution Standard methodology Use MSFvenom efficiently to generate payloads and backdoor files, and create shellcode Leverage Metasploit's advanced options, upgrade sessions, use proxies, use Meterpreter sleep control, and change timeouts to be stealthy Who this book is for If you are a Security professional or pentester and want to get into vulnerability exploitation and make the most of the Metasploit framework, then this book is for you. Some prior understanding of penetration testing and Metasploit is required.

Hacking: the Unlocking of Transparency

This book constitutes the thoroughly refereed post-conference proceedings of the 5th International ICST Conference on Digital Forensics and Cyber Crime, ICDF2C 2013, held in September 2013 in Moscow, Russia. The 16 revised full papers presented together with 2 extended abstracts and 1 poster paper were carefully reviewed and selected from 38 submissions. The papers cover diverse topics in the field of digital forensics and cybercrime, ranging from regulation of social networks to file carving, as well as technical issues, information warfare, cyber terrorism, critical infrastructure protection, standards, certification, accreditation, automation and digital forensics in the cloud.

Android Forensics

Hackers exploit browser vulnerabilities to attack deep withinnetworks The Browser Hacker's Handbook gives a practicalunderstanding of hacking the everyday web browser and using it as abeachhead to launch further attacks deep into corporate networks.Written by a team of highly experienced computer security experts,the handbook provides hands-on tutorials exploring a range ofcurrent attack methods. The web browser has become the most popular and widely usedcomputer "program" in the world. As the gateway to the Internet, itis part of the storefront to any business that operates online, butit is also one of the most vulnerable entry points of any system.With attacks on the rise, companies are increasingly employingbrowser-hardening techniques to protect the unique vulnerabilitiesinherent in all currently used browsers. The Browser Hacker'sHandbook thoroughly covers complex security issues and exploresrelevant topics such as: Bypassing the Same Origin Policy ARP spoofing, social engineering, and phishing to accessbrowsers DNS tunneling, attacking web applications, andproxying—all from the browser Exploiting the browser and its ecosystem (plugins andextensions) Cross-origin attacks, including Inter-protocol Communicationand Exploitation The Browser Hacker's Handbook is written with aprofessional security engagement in mind. Leveraging browsers aspivot points into a target's network should form an integralcomponent into any social engineering or red-team securityassessment. This handbook provides a complete methodology tounderstand and structure your next browser penetration test.

Android Hacker's Handbook

If you are a forensic analyst or an information security professional wanting to develop your knowledge of Android forensics, then this is the book for you. Some basic knowledge of the Android mobile platform is expected.

Flutter Projects

The open source nature of the platform has not only established a new direction for the industry, but enables a developer or forensic analyst to understand the device at the most fundamental level. Android Forensics covers an open source mobile device platform based on the Linux 2.6 kernel and managed by the Open Handset Alliance. The Android platform is a major source of digital forensic investigation and analysis. This book provides a thorough review of the Android platform including supported hardware devices, the structure of the Android development project and implementation of core services (wireless communication, data storage and other low-level functions). Finally, it will focus on teaching readers how to apply actual forensic techniques to recover data. Ability to forensically acquire Android devices using the techniques outlined in the book Detailed information about Android applications needed for forensics investigations Important information about SQLite, a file based structured data storage relevant for both Android and many other platforms.

App Inventor for Android

Decompiling Android looks at the the reason why Android apps can be decompiled to recover their source code, what it means to Android developers and how you can protect your code from prying eyes. This is also a good way to see how good and bad Android apps are constructed and how to learn from them in building your own apps. This is becoming an increasingly important topic as the Android marketplace grows and developers are unwittingly releasing the apps with lots of back doors allowing people to potentially obtain credit card information and database logins to back-end systems, as they don’t realize how easy it is to decompile their Android code. In depth examination of the Java and Android class file structures Tools and techniques for decompiling Android apps Tools and techniques for protecting your Android apps

Mastering Metasploit

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.

Information Security and Privacy Research

Make your Android device truly your own Are you eager to make your Android device your own but you're not sure where to start? Then this is the book for you. XDA is the world's most popular resource for Android hacking enthusiasts, and a huge community has grown around customizing Android devices with XDA. XDA's Android Hacker's Toolkit gives you the tools you need to customize your devices by hacking or rooting the android operating system. Providing a solid understanding of the internal workings of the Android operating system, this book walks you through the terminology and functions of the android operating system from the

major nodes of the file system to basic OS operations. As you learn the fundamentals of Android hacking that can be used regardless of any new releases, you'll discover exciting ways to take complete control over your device. Teaches theory, preparation and practice, and understanding of the OS Explains the distinction between ROMing and theming Provides step-by-step instructions for Droid, Xoom, Galaxy Tab, LG Optimus, and more Identifies the right tools for various jobs Contains new models enabling you to root and customize your phone Offers incomparable information that has been tried and tested by the amazing XDA community of hackers, gadgeteers, and technicians XDA's Android Hacker's Toolkit is a simple, one-stop resource on hacking techniques for beginners.

The Browser Hacker's Handbook

My Surface™ 2 Updated for Windows® RT 8.1 Step-by-step instructions with callouts to Surface 2 photos that show you exactly what to do Help when you run into Surface 2 problems or limitations Tips and Notes to help you get the most from your Surface 2 Full-color, step-by-step tasks walk you through getting and keeping your Surface 2 working just the way you want. Learn how to: • Get started quickly with Surface 2 and Windows RT 8.1 • Connect to Wi-Fi, share printers, and access files from your network or your SkyDrive cloud storage account • Get on the Web fast and enjoy it more with Internet Explorer 11 and the Bing search engine • Secure your Surface and control what your kids can do with it • Do all your Facebook and Twitter social networking through the People app • Find and play the music you love with Xbox Music, Radio, and Xbox Music Pass • Watch Netflix, YouTube, Hulu Plus, and other streaming video • Instantly retrieve up-to-the-minute news from top media and journalists • Create, edit, format, proof, and share documents with Word 2013 • Crunch numbers with Excel 2013 • Present on the go with PowerPoint 2013 • Use OneNote 2013 to organize notes, sync them across devices, and access them from anywhere • Manage email and track your calendar with Outlook 2013 • Go anywhere with Surface 2’s easy maps and directions • Capture, manage, touch up, and geotag your photos • Make sure your files are always safely backed up • Find the best new Windows Store Apps • Keep your Surface 2 working reliably, with maximum battery life • Personalize your Surface 2 using the newest customization settings • Get more help whenever you need it

Smashing Android UI

CCS'15: The 22nd ACM Conference on Computer and Communications Security Oct 12, 2015-Oct 16, 2015 Denver, USA. You can view more information about this proceeding and all of ACM’s other published conference proceedings from the ACM Digital Library: http://www.acm.org/dl.

Android Malware

Mobile devices, such as smart phones, have achieved computing and networking capabilities comparable to traditional personal computers. Their successful consumerization has also become a source of pain for adopting users and organizations. In particular, the widespread presence of information-stealing

applications and other types of mobile malware raises substantial security and privacy concerns. Android Malware presents a systematic view on state-of-the-art mobile malware that targets the popular Android mobile platform. Covering key topics like the Android malware history, malware behavior and classification, as well as, possible defense techniques.

Security Testing With Kali Nethunter

XDA Developers' Android Hacker's Toolkit

Summary In 2017, consumers downloaded 178 billion apps, and analysts predict growth to 258 billion by 2022. Mobile customers are demanding more—and better—apps, and it’s up to developers like you to write them! Flutter, a revolutionary new cross-platform software development kit created by Google, makes it easier than ever to write secure, high-performance native apps for iOS and Android. Flutter apps are blazingly fast because this open source solution compiles your Dart code to platform-specific programs with no JavaScript bridge! Flutter also supports hot reloading to update changes instantly. And thanks to its built-in widgets and rich motion APIs, Flutter’s apps are not just highly responsive, they’re stunning! Purchase of the print book includes a free eBook in PDF, Kindle, and ePub formats from Manning Publications. About the technology With Flutter, you can build mobile applications using a single, feature-rich SDK that includes everything from a rendering engine to a testing environment. Flutter compiles programs written in Google’s intuitive Dart language to platform-specific code so your iOS and Android games, utilities, and shopping platforms all run like native Java or Swift apps. About the book Flutter in Action teaches you to build professional-quality mobile applications using the Flutter SDK and the Dart programming language. You’ll begin with a quick tour of Dart essentials and then dive into engaging, well-described techniques for building beautiful user interfaces using Flutter’s huge collection of built-in widgets. The combination of diagrams, code examples, and annotations makes learning a snap. As you go, you’ll appreciate how the author makes easy reading of complex topics like routing, state management, and async programming. What's inside Understanding the Flutter approach to the UI All the Dart you need to get started Creating custom animations Testing and debugging About the reader You’ll need basic web or mobile app development skills. About the author Eric Windmill is a professional Dart developer and a contributor to open-source Flutter projects. His work is featured on the Flutter Showcase page. Table of Contents: PART 1 - MEET FLUTTER 1 ¦ Meet Flutter 2 ¦ A brief intro to Dart 3 ¦ Breaking into Flutter PART 2 - FLUTTER USER INTERACTION, STYLES, AND ANIMATIONS 4 ¦ Flutter UI: Important widgets, themes, and layout 5 ¦ User interaction: Forms and gestures 6 ¦ Pushing pixels: Flutter animations and using the canvas PART 3 - STATE MANAGEMENT AND ASYNCHRONOUS DART 7 ¦ Flutter routing in depth 8 ¦ Flutter state management 9 ¦ Async Dart and Flutter and infinite scrolling PART 4 - BEYOND FOUNDATIONS 10 ¦ Working with data: HTTP, Firestore, and JSON 11 ¦ Testing Flutter apps

Hacking Android

This book stems from a course about hacking that I usually taught on Telegram. Those who want to learn Ethical Hacking can become extremely skilled with an ease. The specialty of this book is that it includes the step by step instructions with screenshots of the process of hacking. You will start from just basics that is installing the environment to the advance level that is to make your own hacking attacks. "Hacking: The Unlocking of Transparency" will help you to understand terminologies, then concept and their working and finally the way to execute the attack. In hacking world, always remember, Security is a myth

Android Security Cookbook

This book constitutes the refereed proceedings of the 27th IFIP TC 11 International Information Security Conference, SEC 2012, held in Heraklion, Crete, Greece, in June 2012. The 42 revised full papers presented together with 11 short papers were carefully reviewed and selected from 167 submissions. The papers are organized in topical sections on attacks and malicious code, security architectures, system security, access control, database security, privacy attitudes and properties, social networks and social engineering, applied cryptography, anonymity and trust, usable security, security and trust models, security economics, and authentication and delegation.

Hacking Exposed Mobile

Embedded Android is for Developers wanting to create embedded systems based on Android and for those wanting to port Android to new hardware, or creating a custom development environment. Hackers and moders will also find this an indispensible guide to how Android works.

Learning Android Forensics

The Microsoft Technology Associate certification (MTA) curriculum helps instructors teach and validate fundamental technology concepts with a foundation for sudents' careers as well as the confidence they need to succeed in advanced studies. Through the use of MOAC MTA titles you can help ensure your students future success in and out of the classroom. This MTA text covers the following Windows Operating System vital fundamental skills: • Understanding Operating System Configurations • Installing and Upgrading Client Systems • Managing Applications, Managing Files and Folders • Managing Devices • Understanding Operating System Maintenance. Click here to learn more about Microsoft Technology Associate, (MTA) a new and innovative certification track designed to provide a pathway for future success in technology courses and careers.

Applied Cryptography and Network Security

Digital forensics deals with the acquisition, preservation, examination, analysis and presentation of electronic evidence. Networked computing, wireless communications and portable electronic devices have expanded the role of digital forensics beyond traditional computer crime investigations. Practically every crime now involves some aspect of digital evidence; digital forensics provides the

techniques and tools to articulate this evidence. Digital forensics also has myriad intelligence applications. Furthermore, it has a vital role in information assurance -- investigations of security breaches yield valuable information that can be used to design more secure systems. Advances in Digital Forensics XII describes original research results and innovative applications in the discipline of digital forensics. In addition, it highlights some of the major technical and legal issues related to digital evidence and electronic crime investigations. The areas of coverage include: Themes and Issues, Mobile Device Forensics, Network Forensics, Cloud Forensics, Social Media Forensics, Image Forensics, Forensic Techniques, and Forensic Tools. This book is the twelfth volume in the annual series produced by the International Federation for Information Processing (IFIP) Working Group 11.9 on Digital Forensics, an international community of scientists, engineers and practitioners dedicated to advancing the state of the art of research and practice in digital forensics. The book contains a selection of twenty edited papers from the Twelfth Annual IFIP WG 11.9 International Conference on Digital Forensics, held in New Delhi, India in the winter of 2016. Advances in Digital Forensics XII is an important resource for researchers, faculty members and graduate students, as well as for practitioners and individuals engaged in research and development efforts for the law enforcement and intelligence communities. Gilbert Peterson, Chair, IFIP WG 11.9 on Digital Forensics, is a Professor of Computer Engineering at the Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio, USA. Sujeet Shenoi is the F.P. Walter Professor of Computer Science and a Professor of Chemical Engineering at the University of Tulsa, Tulsa, Oklahoma, USA.

Metasploit Penetration Testing Cookbook

Android Security Cookbook' breaks down and enumerates the processes used to exploit and remediate Android app security vulnerabilities in the form of detailed recipes and walkthroughs. Android Security Cookbook is aimed at anyone who is curious about Android app security and wants to be able to take the necessary practical measures to protect themselves; this means that Android application developers, security researchers and analysts, penetration testers, and generally any CIO, CTO, or IT managers facing the impeding onslaught of mobile devices in the business environment will benefit from reading this book.

The Imaginary App

Can Google applications really become an alternative to the venerable Microsoft Office suite? Conventional wisdom may say no, but practical wisdom says otherwise. Right now, 100,000 small businesses are currently running trials of Google office applications. So are large corporations such as General Electric and Proctor & Gamble. Google Apps Hacks gets you in on the action with several ingenious ways to push Google's web, mobile, and desktop apps to the limit. The scores of clever hacks and workarounds in this book help you get more than the obvious out of a whole host of Google's web-based applications for word processing, spreadsheets, PowerPoint-style presentations, email, calendar, and more by giving you ways to exploit the suite's unique network functionality. You get plenty of ways to tinker with: Google Documents -- Share and edit documents with others in real time, view them on the run with Google Docs mobile service, and use Google Notebook for web research Google Spreadsheets -- Add real-time

data to spreadsheets, and generate charts and tables you can embed in web pages Google Presentations -- View them on a mobile phone and save them as video Gmail -- Send email to and from a mobile phone, adjust Gmail's layout with a style sheet, and a lot more iGoogle -- Create your own gadgets, program a screenscraper, add Flash games, and more Google Calendar -- Add web content events, public calendars, and your Outlook Calendar to this application Google Reader, Google Maps, Google Earth, and Google SketchUp: the new 3D modeling software tool Picasa, YouTube, and Google Video -- discover new ways to customize and use these media management apps In addition, Google Apps Hacks outlines ways you can create a simple web site with nothing but Google tools, including Page Creator, Blogger, Google Analytics, and content from other Google apps. This amazing collection just might convince you that Microsoft Office is not the last word in business applications. The price is certainly right.

Exam 98-349 MTA Windows Operating System Fundamentals

Build, customize, and debug your own Android system About This Book Master Android system-level programming by integrating, customizing, and extending popular open source projects Use Android emulators to explore the true potential of your hardware Master key debugging techniques to create a hassle-free development environment Who This Book Is For This book is for Android system programmers and developers who want to use Android and create indigenous projects with it. You should know the important points about the operating system and the C/C++ programming language. What You Will Learn Set up the Android development environment and organize source code repositories Get acquainted with the Android system architecture Build the Android emulator from the AOSP source tree Find out how to enable WiFi in the Android emulator Debug the boot up process using a customized Ramdisk Port your Android system to a new platform using VirtualBox Find out what recovery is and see how to enable it in the AOSP build Prepare and test OTA packages In Detail Android system programming involves both hardware and software knowledge to work on system level programming. The developers need to use various techniques to debug the different components in the target devices. With all the challenges, you usually have a deep learning curve to master relevant knowledge in this area. This book will not only give you the key knowledge you need to understand Android system programming, but will also prepare you as you get hands-on with projects and gain debugging skills that you can use in your future projects. You will start by exploring the basic setup of AOSP, and building and testing an emulator image. In the first project, you will learn how to customize and extend the Android emulator. Then you'll move on to the real challenge—building your own Android system on VirtualBox. You'll see how to debug the init process, resolve the bootloader issue, and enable various hardware interfaces. When you have a complete system, you will learn how to patch and upgrade it through recovery. Throughout the book, you will get to know useful tips on how to integrate and reuse existing open source projects such as LineageOS (CyanogenMod), Android-x86, Xposed, and GApps in your own system. Style and approach This is an easy-to-follow guide full of hands-on examples and system-level programming tips.

Embedded Android

Enhance your organization’s secure posture by improving your attack and defense strategies Key Features Gain a clear understanding of the attack methods, and patterns to recognize abnormal behavior within your organization with Blue Team tactics. Learn to unique techniques to gather exploitation intelligence, identify risk and demonstrate impact with Red Team and Blue Team strategies. A practical guide that will give you hands-on experience to mitigate risks and prevent attackers from infiltrating your system. Book Description The book will start talking about the security posture before moving to Red Team tactics, where you will learn the basic syntax for the Windows and Linux tools that are commonly used to perform the necessary operations. You will also gain hands-on experience of using new Red Team techniques with powerful tools such as python and PowerShell, which will enable you to discover vulnerabilities in your system and how to exploit them. Moving on, you will learn how a system is usually compromised by adversaries, and how they hack user's identity, and the various tools used by the Red Team to find vulnerabilities in a system. In the next section, you will learn about the defense strategies followed by the Blue Team to enhance the overall security of a system. You will also learn about an in-depth strategy to ensure that there are security controls in each network layer, and how you can carry out the recovery process of a compromised system. Finally, you will learn how to create a vulnerability management strategy and the different techniques for manual log analysis. By the end of this book, you will be well-versed with Red Team and Blue Team techniques and will have learned the techniques used nowadays to attack and defend systems. What you will learn Learn the importance of having a solid foundation for your security posture Understand the attack strategy using cyber security kill chain Learn how to enhance your defense strategy by improving your security policies, hardening your network, implementing active sensors, and leveraging threat intelligence Learn how to perform an incident investigation Get an in-depth understanding of the recovery process Understand continuous security monitoring and how to implement a vulnerability management strategy Learn how to perform log analysis to identify suspicious activities Who this book is for This book aims at IT professional who want to venture the IT security domain. IT pentester, Security consultants, and ethical hackers will also find this course useful. Prior knowledge of penetration testing would be beneficial.

Kali Linux - An Ethical Hacker's Cookbook

The first comprehensive guide to discovering and preventingattacks on the Android OS As the Android operating system continues to increase its shareof the smartphone market, smartphone hacking remains a growingthreat. Written by experts who rank among the world's foremostAndroid security researchers, this book presents vulnerabilitydiscovery, analysis, and exploitation tools for the good guys.Following a detailed explanation of how the Android OS works andits overall security architecture, the authors examine howvulnerabilities can be discovered and exploits developed forvarious system components, preparing you to defend againstthem. If you are a mobile device administrator, security researcher,Android app developer, or consultant responsible for evaluatingAndroid security, you will find this guide is essential to yourtoolbox. A crack team of leading Android security researchers explainAndroid security risks, security design and architecture, rooting,fuzz testing, and vulnerability analysis Covers Android application building blocks and security as wellas debugging and auditing Android apps Prepares

mobile device administrators, security researchers,Android app developers, and security consultants to defend Androidsystems against attack Android Hacker's Handbook is the first comprehensiveresource for IT professionals charged with smartphonesecurity.

Python Hacking Essentials

Learn Flutter and the Dart programming language by building impressive real-world mobile applications for Android and iOS Key Features Learn cross-platform mobile development with Flutter and Dart by building 11 real-world apps Create wide array of mobile projects such as 2D game, productivity timer, movie browsing app, and more Practical projects demonstrating Flutter development techniques with tips, tricks, and best practices Book Description Flutter is a modern reactive mobile framework that removes a lot of the complexity found in building native mobile apps for iOS and Android. With Flutter, developers can now build fast and native mobile apps from a single codebase. This book is packed with 11 projects that will help you build your own mobile applications using Flutter. It begins with an introduction to Dart programming and explains how it can be used with the Flutter SDK to customize mobile apps. Each chapter contains instructions on how to build an independent app from scratch, and each project focuses on important Flutter features.From building Flutter Widgets and applying animations to using databases (SQLite and sembast) and Firebase, you'll build on your knowledge through the chapters. As you progress, you'll learn how to connect to remote services, integrate maps, and even use Flare to create apps and games in Flutter. Gradually, you'll be able to create apps and games that are ready to be published on the Google Play Store and the App Store. In the concluding chapters, you'll learn how to use the BLoC pattern and various best practices related to creating enterprise apps with Flutter. By the end of this book, you will have the skills you need to write and deliver fully functional mobile apps using Flutter. What you will learn Design reusable mobile architectures that can be applied to apps at any scale Get up to speed with error handling and debugging for mobile application development Apply the principle of 'composition over inheritance' to break down complex problems into many simple problems Update your code and see the results immediately using Flutter's hot reload Identify and prevent bugs from reappearing with Flutter's developer tools Manage an app's state with Streams and the BLoC pattern Build a simple web application using Flutter Web Who this book is for This book is for mobile developers and software developers who want to learn Flutter to build state-of-the-art mobile apps. Although prior experience with Dart programming or Flutter is not required, knowledge of object-oriented programming (OOP), data structures and software design patterns will be beneficial.