File Type PDF Pwnage Guide

If you ally compulsion such a referred **Pwnage Guide** ebook that will have the funds for you worth, acquire the unconditionally best seller from us currently from several preferred authors. If you desire to entertaining books, lots of novels, tale, jokes, and more fictions collections are moreover launched, from best seller to one of the most current released.

You may not be perplexed to enjoy all book collections Pwnage Guide that we will definitely offer. It is not on the order of the costs. Its just about what you compulsion currently. This Pwnage Guide, as one of the most functioning sellers here will unconditionally be in the midst of the best options to review.

KEY=GUIDE - FREDDY NADIA

Penetration Testing: A Survival Guide

Packt Publishing Ltd *A complete pentesting guide facilitating smooth backtracking for working hackers About This Book Conduct network testing, surveillance, pen testing and forensics on MS Windows using Kali Linux Gain a deep understanding of the flaws in web applications and exploit them in a practical manner Pentest Android apps and perform various attacks in the real world using real case studies Who This Book Is For This course is for anyone who wants to learn about security. Basic knowledge of Android programming would be a plus. What You Will Learn Exploit several common Windows network vulnerabilities Recover lost files, investigate successful hacks, and discover hidden data in innocent-looking files Expose vulnerabilities present in web servers and their applications using server-side attacks Use SQL and cross-site scripting (XSS) attacks Check for XSS flaws using the burp suite proxy Acquaint yourself with the fundamental building blocks of Android Apps in the right way Take a look at how your personal data can be stolen by malicious attackers See how developers make mistakes that allow attackers to steal data from phones In Detail The need for penetration testers has grown well over what the IT industry ever anticipated. Running just a vulnerability scanner is no longer an effective method to determine whether a business is truly secure. This learning path will help you develop the most effective penetration testing skills to protect your Windows, web applications, and Android devices. The first module focuses on the Windows platform, which is one of the most common OSes, and managing its security spawned the discipline of IT security. Kali Linux is the premier platform for testing and maintaining Windows security. Employs the most advanced tools and techniques to reproduce the methods used by sophisticated hackers. In this module first,you'll be introduced to Kali's top ten tools and other useful reporting tools. Then, you will find your way around your target network and determine known vulnerabilities so you can exploit a system remotely. You'll not only learn to penetrate in the machine, but will also learn to work with Windows privilege escalations. The second module will help you get to grips with the tools used in Kali Linux 2.0 that relate to web application hacking. You will get to know about scripting and input validation flaws, AJAX, and security issues related to AJAX. You will also use an automated technique called fuzzing so you can identify flaws in a web application. Finally, you'll understand the web application vulnerabilities and the ways they can be exploited. In the last module, you'll get started with Android security. Android, being the platform with the largest consumer base, is the obvious primary target for attackers. You'll begin this journey with the absolute basics and will then slowly gear up to the concepts of Android rooting, application security assessments, malware, infecting APK files, and fuzzing. You'll gain the skills necessary to perform Android application vulnerability assessments and to create an Android pentesting lab. This Learning Path is a blend of content from the following Packt products: Kali Linux 2: Windows Penetration Testing by Wolf Halton and Bo Weaver Web Penetration Testing with Kali Linux, Second Edition by Juned Ahmed Ansari Hacking Android by Srinivasa Rao Kotipalli and Mohammed A. Imran Style and approach This course uses easy-to-understand yet professional language for explaining concepts to test your network's security.*

Computer Forensics Practical Guide

Investigating Computer Attacks

Booktango *This Computer Forensic Guide is meant for IT professional who wants to enter into Computer Forensic domain.*

Kali Linux Wireless Penetration Testing: Beginner's Guide

Packt Publishing Ltd *If you are a security professional, pentester, or anyone interested in getting to grips with wireless penetration testing, this is the book for you. Some familiarity with Kali Linux and wireless concepts is beneficial.*

Kali Linux Wireless Penetration Testing Beginner's Guide

Master wireless testing techniques to survey and attack wireless networks with Kali Linux, including the KRACK attack

Packt Publishing Ltd *Kali Linux Wireless Penetration Testing Beginner's Guide, Third Edition presents wireless pentesting from the ground up, and has been updated with the latest methodologies, including full coverage of the KRACK attack. About This Book Learn wireless penetration testing with Kali Linux Detect hidden wireless networks and discover their names Explore advanced Wi-Fi hacking techniques including rogue access point hosting and probe sniffing Develop your encryption cracking skills and gain an insight into the methods used by attackers and the underlying technologies that facilitate these attacks Who This Book Is For Kali Linux Wireless Penetration Testing Beginner's Guide, Third Edition is suitable for anyone who wants to learn more about pentesting and how to understand and defend against the latest wireless network attacks. What You Will Learn Understand the KRACK attack in full detail Create a wireless lab for your experiments Sniff out wireless packets, hidden networks, and SSIDs Capture and crack WPA-2 keys Sniff probe requests and track users through their SSID history Attack radius authentication systems Sniff wireless traffic and collect interesting data Decrypt encrypted traffic with stolen keys In Detail As wireless networks become ubiquitous in our lives, wireless penetration testing has become a key skill in the repertoire of the professional penetration tester. This has been highlighted again recently with the discovery of the KRACK attack which enables attackers to potentially break into Wi-Fi networks encrypted with WPA2. The Kali Linux security distribution comes with a myriad of tools used for networking attacks and detecting security loopholes. Kali Linux Wireless Penetration Testing Beginner's Guide, Third Edition has been updated to Kali Linux 2017.3 with the latest methodologies, including full coverage of the KRACK attack and how to defend against it. The book presents wireless pentesting from the ground up, introducing all elements of penetration testing with each new technology. You'll learn various wireless testing methodologies by example, from the basics of wireless routing and encryption through to detailed coverage of hacking methods and attacks such as the Hirte and Caffe Latte. Style and approach Kali Linux Wireless Penetration Testing Beginner's Guide, Third Edition is a practical, hands-on guide to modern wi-fi network hacking. It covers both the theory and practice of wireless pentesting, offering detailed, real-world coverage of the latest vulnerabilities and attacks.*

Pokémon: Black & White 2 - Strategy Guide

Gamer Guides *Inside this guide you will find: - Top tricks for beating all eight Gym Leader - Beat the Elite Four and the current Champion with style! - How and where to find the Pokemon you want to catch - Find and catch all Legendary Pokemon! - Post story-mode walkthrough with all hidden areas uncovered - Save time by finding the rarest of items for free! - Packed full with high-quality screenshots! - Tips and info on both Black and White versions - And LOADS more inside! Updates: - Added complete tables for every Wild Pokémon found in each area as well as encounter rates. - Fixed tables that weren't displaying correctly on the website. - Further editing improvements to text and formatting. - Completely reformatted for easier viewing on all devices! - All missing White 2 sections added, plus the mysterious Nature Preserve. - Expanded the Introduction and Gameplay section with loads of new information. - Videos for all the Gym Leader and Elite Four battles, plus legendary Pokemon. - Dozens of illustrative and pretty screenshots. - Missing areas amended - Expanded segment describing the intricacies of training a Pokémon - Concise and easy to understand explanations of advanced stat building systems - learn how to raise a prize Pokémon*

iPhone Hacks

Pushing the iPhone and iPod touch Beyond Their Limits

"O'Reilly Media, Inc." *With iPhone Hacks, you can make your iPhone do all you'd expect of a mobile smartphone -- and more. Learn tips and techniques to unleash little-known features, find and create innovative applications for both the iPhone and iPod touch, and unshackle these devices to run everything from network utilities to video game emulators. This book will teach you how to: Import your entire movie collection, sync with multiple computers, and save YouTube videos Remotely access your home network, audio, and video, and even control your desktop Develop native applications for the iPhone and iPod touch on Linux, Windows, or Mac Check email, receive MMS messages, use IRC, and record full-motion video Run any application in the iPhone's background, and mirror its display on a TV Make your iPhone emulate old-school video game platforms, and play classic console and arcade games Integrate your iPhone with your car stereo Build your own electronic bridges to connect keyboards, serial devices, and more to your iPhone without "jailbreaking" iPhone Hacks explains how to set up your iPhone the way you want it, and helps you give it capabilities that will rival your desktop computer. This cunning little handbook is exactly what you need to make the most of your iPhone.*

Kali Linux 2018: Windows Penetration Testing

Conduct network testing, surveillance, and pen testing on MS Windows using Kali Linux 2018, 2nd Edition

Packt Publishing Ltd *Become the ethical hacker you need to be to protect your network Key FeaturesSet up, configure, and run a newly installed Kali-Linux 2018.xFootprint, monitor, and audit your network and investigate any ongoing infestationsCustomize Kali Linux with this professional guide so it becomes your pen testing toolkitBook Description Microsoft Windows is one of the two most common OSes, and managing its security has spawned the discipline of IT security. Kali Linux is the premier platform for testing and maintaining Windows security. Kali is built on the Debian distribution of Linux and shares the legendary stability of that OS. This lets you focus on using the network penetration, password cracking, and forensics tools, and not the OS. This book has the most advanced tools and techniques to reproduce the methods used by sophisticated hackers to make you an expert in Kali Linux penetration testing. You will start by learning about the various desktop environments that now come with Kali. The book covers network sniffers and analysis tools to uncover the Windows protocols in use on the network. You will see several tools designed to improve your average in password acquisition, from hash cracking, online attacks, offline attacks, and rainbow tables to social engineering. It also demonstrates several use cases for Kali Linux tools like Social Engineering Toolkit, and Metasploit, to exploit Windows vulnerabilities. Finally, you will learn how to gain full system-level access to your compromised system and then maintain that access. By the end of this book, you will be able to quickly pen test your system and network using easy-to-follow instructions and support images. What you will learnLearn advanced set up techniques for Kali and the Linux operating systemUnderstand footprinting and reconnaissance of networksDiscover new advances and improvements to the Kali operating systemMap and enumerate your Windows networkExploit several common Windows network vulnerabilitiesAttack and defeat password schemes on WindowsDebug and reverse engineer Windows programsRecover lost files, investigate successful hacks, and discover hidden dataWho this book is for If you are a working ethical hacker who is looking to expand the offensive skillset with a thorough understanding of Kali Linux, then this is the book for you. Prior knowledge about Linux operating systems, BASH terminal, and Windows command line would be highly beneficial.*

UNBORED Games

Serious Fun for Everyone

Bloomsbury Publishing USA *From old-fashioned classics to new high-tech varieties, this comprehensive guide to playing games and creating fun includes intricate clapping games, bike rodeo and Google Earth challenges in this follow up to Unbored: The Essential Field Guide to Serious Fun.*

Web App Hacking

Carnage & Pwnage

From Wireless to Web Application to Container pownage, this issue covers attacks and exploitation and post exploitation. After you are on the system, what do you do? Do you want to exfil (take their data) or pivot and attack other systems first? we have you covered. This issue has a large focus on the OWASP top 10 web app vulnerabilities and even has a nice section for Docker container exploitation. Where there is a web, there is a way.

The Nix

A novel

Vintage *Winner of the Art Seidenbaum Award for First Fiction A New York Times 2016 Notable Book Entertainment Weekly's #1 Book of the Year A Washington Post 2016 Notable Book A Slate Top Ten Book NEW YORK TIMES BESTSELLER “The Nix is a mother-son psychodrama with ghosts and politics, but it’s also a tragicomedy about anger and sanctimony in America. . . . Nathan Hill is a maestro.” —John Irving From the suburban Midwest to New York City to the 1968 riots that rocked Chicago and beyond, The Nix explores—with sharp humor and a fierce tenderness—the resilience of love and home, even in times of radical change. It’s 2011, and Samuel Andresen-Anderson—college professor, stalled writer—has a Nix of his own: his mother, Faye. He hasn’t seen her in decades, not since she abandoned the family when he was a boy. Now she’s re-appeared, having committed an absurd crime that electrifies the nightly news, beguiles the internet, and inflames a politically divided country. The media paints Faye as a radical hippie with a sordid past, but as far as Samuel knows, his mother was an ordinary girl who married her high-school sweetheart. Which version of his mother is true? Two facts are certain: she’s facing some serious charges, and she needs Samuel’s help. To save her, Samuel will have to embark on his own journey, uncovering long-buried secrets about the woman he thought he knew, secrets that stretch across generations and have their origin all the way back in Norway, home of the mysterious Nix. As he does so, Samuel will confront not only Faye’s losses but also his own lost love, and will relearn everything he thought he knew about his mother, and himself.*

Unbored

The Essential Field Guide to Serious Fun

A&C Black *Unbored is the book every modern child needs. Brilliantly walking the line between cool and constructive, it's crammed with activities that are not only fun and doable but that also get kids standing on their own two feet. If you're a kid, you can: -- Build a tipi or an igloo -- Learn to knit -- Take stuff apart and fix it -- Find out how to be constructively critical -- Film a stop-action movie or edit your own music -- Do parkour like James Bond -- Make a little house for a mouse from lollipop sticks -- Be independent! Catch a bus solo or cook yourself lunch -- Make a fake exhaust for your bike so it sounds like you're revving up a motorcycle -- Design a board game -- Go camping (or glamping) -- Plan a road trip -- Get proactive and support the causes you care about -- Develop your taste and decorate your own room -- Make a rocket from a coke bottle -- Play farting games There are gross facts and fascinating stories, reports on what stuff is like (home schooling, working in an office...), Q&As with inspiring grown-ups, extracts from classic novels, lists of useful resources and best ever lists like the top clean rap songs, stop-motion movies or books about rebellion. Just as kids begin to disappear into their screens, here is a book that encourages them to use those tech skills to be creative, try new things and change the world. And it gets parents to join in. Unbored is fully illustrated, easy to use and appealing to young and old, girl and boy. Parents will be comforted by its anti-perfectionist spirit and humour. Kids will just think it's brilliant.*

Backtrack 5 Wireless Penetration Testing

Beginner's Guide

Packt Publishing Ltd *Wireless has become ubiquitous in today’s world. The mobility and flexibility provided by it makes our lives more comfortable and productive. But this comes at a cost – Wireless technologies are inherently insecure and can be easily broken. BackTrack is a penetration testing and security auditing distribution that comes with a myriad of wireless networking tools used to simulate network attacks and detect security loopholes. Backtrack 5 Wireless Penetration Testing Beginner’s Guide will take you through the journey of becoming a Wireless hacker. You will learn various wireless testing methodologies taught using live examples, which you will implement throughout this book. The engaging practical sessions very gradually grow in complexity giving you enough time to ramp up before you get to advanced wireless attacks. This book will take you through the basic concepts in Wireless and creating a lab environment for your experiments to the business of different lab sessions in wireless security basics, slowly turn on the heat and move to more complicated scenarios, and finally end your journey by conducting bleeding edge wireless attacks in your lab. There are many interesting and new things that you will learn in this book – War Driving, WLAN packet sniffing, Network Scanning, Circumventing hidden SSIDs and MAC filters, bypassing Shared Authentication, Cracking WEP and WPA/WPA2 encryption, Access Point MAC spoofing, Rogue Devices, Evil Twins, Denial of Service attacks, Viral SSIDs, Honeypot and Hotspot attacks, Caffe Latte WEP Attack, Man-in-the-Middle attacks, Evading Wireless Intrusion Prevention systems and a bunch of other cutting edge wireless attacks. If you were ever curious about what wireless security and hacking was all about, then this book will get you started by providing you with the knowledge and practical know-how to become a wireless hacker. Hands-on practical guide with a step-by-step approach to help you get started immediately with Wireless Penetration Testing*

The Nix

Vintage *"An epic novel about a son, the mother who left him as a child, and how his search to uncover the secrets of her life leads him to reclaim his own"--*

(Im)politeness and Moral Order in Online Interactions

John Benjamins Publishing Company *(Im)politeness and Moral Order in Online Interactions presents a timely response to the ‘moral turn’ in (im)politeness studies. This volume, presented by a roster of prominent figures in the field, documents and showcases the complexity of (im)politeness as social practice by focusing on the morality of (im)politeness in internet-mediated interactions. It includes, among others, studies on how the moral order is made explicit and salient in the production and perception of online impoliteness as social practice and how situated impoliteness can perform positive social and communicative functions. This volume confirms once again that (im)politeness can serve as a lens through which a variety of topics, genres, and contexts are intertwined together pointing to the very presence and existence of human beings, and is bound to be of interest to not only students and scholars engaged in the area of (im)politeness and internet pragmatics, but also to all those with a more general interest in the study of human (inter)actions in various situations and contexts. Originally published as special issue of Internet Pragmatics 1:2 (2018).*

Kali Linux 2: Windows Penetration Testing

Packt Publishing Ltd *Kali Linux: a complete pentesting toolkit facilitating smooth backtracking for working hackers About This Book Conduct network testing, surveillance, pen testing and forensics on MS Windows using Kali Linux Footprint, monitor, and audit your network and investigate any ongoing infestations Customize Kali Linux with this professional guide so it becomes your pen testing toolkit Who This Book Is For If you are a working ethical hacker who is looking to expand the offensive skillset with a thorough understanding of Kali Linux, then this is the book for you. Prior knowledge about Linux operating systems and the BASH terminal emulator along with Windows desktop and command line would be highly beneficial. What You Will Learn Set up Kali Linux for pen testing Map and enumerate your Windows network Exploit several common Windows network vulnerabilities Attack and defeat password schemes on Windows Debug and reverse-engineer Windows programs Recover lost files, investigate successful hacks and discover hidden data in innocent-looking files Catch and hold admin rights on the network, and maintain backdoors on the network after your initial testing is done In Detail Microsoft Windows is one of the two most common OS and managing its security has spawned the discipline of IT security. Kali Linux is the premier platform for testing and maintaining Windows security. Kali is built on the Debian distribution of Linux and shares the legendary stability of that OS. This lets you focus on using the network penetration, password cracking, forensics tools and not the OS. This book has the most advanced tools and techniques to reproduce the methods used by sophisticated hackers to make you an expert in Kali Linux penetration testing. First, you are introduced to Kali's top ten tools and other useful reporting tools. Then, you will find your way around your target network and determine known vulnerabilities to be able to exploit a system remotely. Next, you will prove that the vulnerabilities you have found are real and exploitable. You will learn to use tools in seven categories of exploitation tools. Further, you perform web access exploits using tools like websploit and more. Security is only as strong as the weakest link in the chain. Passwords are often that weak link. Thus, you learn about password attacks that can be used in concert with other approaches to break into and own a network. Moreover, you come to terms with network sniffing, which helps you understand which users are using services you can exploit, and IP spoofing, which can be used to poison a system's DNS cache. Once you gain access to a machine or network, maintaining access is important. Thus, you not only learn penetrating in the machine you also learn Windows privilege's escalations. With easy to follow step-by-step instructions and support images, you will be able to quickly pen test your system and network. Style and approach This book is a hands-on guide for Kali Linux pen testing. This book will provide all the practical knowledge needed to test your network's security using a proven hacker's methodology. The book uses easy-to-understand yet professional language for explaining concepts.*

Hanging Out, Messing Around, and Geeking Out, Tenth Anniversary Edition

Kids Living and Learning with New Media

MIT Press *The tenth-anniversary edition of a foundational text in digital media and learning, examining new media practices that range from podcasting to online romantic breakups. Hanging Out, Messing Around, and Geeking Out, first published in 2009, has become a foundational text in the field of digital media and learning. Reporting on an ambitious three-year ethnographic investigation into how young people live and learn with new media in varied settings—at home, in after-school programs, and in online spaces—it presents a flexible and useful framework for understanding the ways that young people engage with and through online platforms: hanging out, messing around, and geeking out, otherwise known as HOMAGO. Integrating twenty-three case studies—which include Harry Potter podcasting, video-game playing, music sharing, and online romantic breakups—in a unique collaborative authorship style, Hanging Out, Messing Around, and Geeking Out combines in-depth descriptions of specific group dynamics with conceptual analysis. Since its original publication, digital learning labs in libraries and museums around the country have been designed around the HOMAGO mode and educators have created HOMAGO guidebooks and toolkits. This tenth-anniversary edition features a new introduction by Mizuko Ito and Heather Horst that discusses how digital youth culture evolved in the intervening decade, and looks at how HOMAGO has been put into practice. This book was written as a collaborative effort by members of the Digital Youth Project, a three-year research effort funded by the John D. and Catherine T. MacArthur Foundation and conducted at the University of California, Berkeley, and the University of Southern California.*

Hacking and Penetration Testing with Low Power Devices

Syngress *Hacking and Penetration Testing with Low Power Devices shows you how to perform penetration tests using small, low-powered devices that are easily hidden and may be battery-powered. It shows how to use an army of devices, costing less than you might spend on a laptop, from distances of a mile or more. Hacking and Penetration Testing with Low Power Devices shows how to use devices running a version of The Deck, a full-featured penetration testing and forensics Linux distribution, and can run for days or weeks on batteries due to their low power consumption. Author Philip Polstra shows how to use various configurations, including a device the size of a deck of cards that can easily be attached to the back of a computer. While each device running The Deck is a full-featured pen-testing platform, connecting systems together via 802.15.3 networking gives you even more power and flexibility. This reference teaches you how to construct and power these devices, install operating systems, and fill out your toolbox of small low-power devices with hundreds of tools and scripts from the book's companion website. Hacking and Pen Testing with Low Power Devices puts all these tools into your hands and will help keep you at the top of your game performing cutting-edge pen tests from anywhere in the world! Understand how to plan and execute an effective penetration test using an army of low-power devices Learn how to configure and use open-source tools and easy-to-construct low-power devices Leverage IEEE 802.15.4 networking to perform penetration tests from up to a mile away, or use 802.15.4 gateways to perform pen tests from anywhere in the world Access penetration testing operating systems with hundreds of tools and scripts on the book's companion web site*

Geektionary

From Anime to Zettabyte, An A to Z Guide to All Things Geek

Simon and Schuster *"The last WoW module was clunky and a bit slow on my rig but it had a great toolset for building adventures for my avatar. Now I'm at sixtieth level! Awesome!" Whether it's about science fiction, Star Trek, sports, comics, or computers, geekspeak is full of mysterious words and phrases. But now there's an easy way to understand what it's all about. With this book you can dork out with the best of 'em. Here are more than 1,000 words and their definitions, including such gems as: LARP Red Shirt Wilhelm Scream Xenomorph Munchkin* So don't worry if you don't know what a midochlorian is or what to do with a proton pack. With this book, you'll never be confused again. Which doesn't mean what you think it means, unless you're a fan of roleplaying games.*

Word Up

A Lexicon and Guide to Communication in the 21st Century

The ABC of XYZ *Everyone says the English language is changing in this global digital age. Everyone says the generations don't understand each other. Word Up is the complete up-to-date Australian guide to where our language is headed. Fascinating, colourful, easy to use and full of surprises. Includes a youth lexicon.*

A Guide to Kernel Exploitation

Attacking the Core

Elsevier *A Guide to Kernel Exploitation: Attacking the Core discusses the theoretical techniques and approaches needed to develop reliable and effective kernel-level exploits, and applies them to different operating systems, namely, UNIX derivatives, Mac OS X, and Windows. Concepts and tactics are presented categorically so that even when a specifically detailed vulnerability has been patched, the foundational information provided will help hackers in writing a newer, better attack; or help pen testers, auditors, and the like develop a more concrete design and defensive structure. The book is organized into four parts. Part I introduces the kernel and sets out the theoretical basis on which to build the rest of the book. Part II focuses on different operating systems and describes exploits for them that target various bug classes. Part III on remote kernel exploitation analyzes the effects of the remote scenario and presents new techniques to target remote issues. It includes a step-by-step analysis of the development of a reliable, one-shot, remote exploit for a real vulnerabilitya bug affecting the SCTP subsystem found in the Linux kernel. Finally, Part IV wraps up the analysis on kernel exploitation and looks at what the future may hold. Covers a range of operating system families — UNIX derivatives, Mac OS X, Windows Details common scenarios such as generic memory corruption (stack overflow, heap overflow, etc.) issues, logical bugs and race conditions Delivers the reader from user-land exploitation to the world of kernel-land (OS) exploits/attacks, with a particular focus on the steps that lead to the creation of successful techniques, in order to give to the reader something more than just a set of tricks*

I Am Bride

How to Take the We Out of Wedding, and Other Useful Advice

Abrams Image *The first book from Upright Citizens Brigade comedian Laura Willcox, I AM BRIDE is a hysterical spoof of all the lavish, ridiculous, and stressful things a bride deals with when planning her BIG DAY. In this bridal gag gift, Laura Willcox writes in the voice of an overbearing, outrageous wedding planner, covering all aspects of a wedding--from the moment of engagement (hopefully with the ring you've been not so subtly emailing him about for months), all the way through the final minutes of the big day. Accompanied by Jason O'Malley's humorous illustrations, Willcox offers tongue-in-cheek advice for every wedding-planning moment, whether it's dreaming up the perfect wedding-weekend hashtag, planning a gift registry to make everyone jealous of your fabulous lifestyle, or figuring out how to distance yourself from the poor, unfortunate souls who didn't make the cut for your guest list. Laura Willcox's refreshing take on all things bride will turn tradition on its head, and have you rolling your eyes and reading passages out loud to your engaged (and married) friends. This funny book is a perfect gift for the friend who can't stop pinning to her dream wedding board, bridezilla-to-be, or any bride who would benefit from a much-needed break from the stress and madness of wedding planning.*

Gender, Age, and Digital Games in the Domestic Context

Routledge *Western digital game play has shifted in important ways over the last decade, with a plethora of personal devices affording a range of increasingly diverse play experiences. Despite the celebration of a more inclusive environment of digital game play, very little grounded research has been devoted to the examination of familial play and the domestication of digital games, as opposed to evolving public and educational contexts. This book is the first study to provide a situated investigation of the site of family play— the shared spaces and private places of gameplay within the domestic sphere. It carries out an empirically grounded and critical analysis of what marketing and sales discourses about shifts in the digital games audience actually look like in the space of the home, as well as the social and cultural role these ludic technologies take in the everyday practices of the family in the domestic context. It examines the material realities of video game technologies in the home; including time management and spatial organization, as well as the discursive role these devices play in discussions of technological competence and its complex relationship to age, generational differences, and gender performance. Harvey's interdisciplinary approach and innovative methodology will hold great critical appeal for those studying digital culture, children's media, and feminist studies of new media, as well as critical theories of technology and leisure and sport theory.*

IPhone Forensics

Recovering Evidence, Personal Data, and Corporate Assets

"O'Reilly Media, Inc." *"This book is a must for anyone attempting to examine the iPhone. The level of forensic detail is excellent. If only all guides to forensics were written with this clarity!"-Andrew Sheldon, Director of Evidence Talks, computer forensics experts With iPhone use increasing in business networks, IT and security professionals face a serious challenge: these devices store an enormous amount of information. If your staff conducts business with an iPhone, you need to know how to recover, analyze, and securely destroy sensitive data. iPhone Forensics supplies the knowledge necessary to conduct complete and highly specialized forensic analysis of the iPhone, iPhone 3G, and iPod Touch. This book helps you: Determine what type of data is stored on the device Break v1.x and v2.x passcode-protected iPhones to gain access to the device Build a custom recovery toolkit for the iPhone Interrupt iPhone 3G's "secure wipe" process Conduct data recovery of a v1.x and v2.x iPhone user disk partition, and preserve and recover the entire raw user disk partition Recover deleted voicemail, images, email, and other personal data, using data carving techniques Recover geotagged metadata from camera photos Discover Google map lookups, typing cache, and other data stored on the live file system Extract contact information from the iPhone's database Use different recovery strategies based on case needs And more. iPhone Forensics includes techniques used by more than 200 law enforcement agencies worldwide, and is a must-have for any corporate compliance and disaster recovery plan.*

Learning the iOS 4 SDK for JavaScript Programmers

Create Native Apps with Objective-C and Xcode

"O'Reilly Media, Inc." *Is it possible for JavaScript programmers to learn Apple's iOS 4 SDK and live to tell the tale? Technology guru Danny Goodman did, and with this book he leaves a well-marked trail for you to follow. An authority on JavaScript since its inception, Goodman understands the challenges you might face in creating native iOS apps with this SDK, and introduces Xcode, Objective-C, and Cocoa Touch in a context you'll readily understand. Why bother with the SDK when you can simply build web apps for Apple's iOS devices? Web apps can't access an iPhone's music library, camera, or iOS system software for maps, audio, and more. Nor can you sell web apps in the App Store. If you want to take full advantage of the iPhone and iPad, iOS 4 SDK is your tool -- and this is your book. Includes full coverage of iOS SDK 4.2. Learn the distinction between web app and iOS native app programming Create a workbench app to test code snippets throughout the learning process Get a structural view of an iOS app, and compare the process of building objects in Objective-C versus JavaScipt Discover how your code launches iOS apps and makes them user-ready Learn about iOS memory management details that are different from JavaScript, including pointers and data types Use Objective-C and Cocoa Touch to implement common JavaScript tasks*

OSINT Investigations

We Know What You Did That Summer

Do you want to learn more about OSINT or Open Source Intelligence or are interested in online investigations? If your answer is yes, this is the Cyber Secrets issue for you. Inside, you will learn how to manually get evidence from some online sources along with several tools that can help automate some of the processes. Most of the tools are prepackaged into CSI Linux, a forensic investigation platform, while not required for the vast majority of the OSINT material. HANDS-ON WALKTHROUGHS!!! Yes, we cover both theory and hands-on content from some great authors that have helped put this issue together.

The Hacker Playbook 2

Practical Guide to Penetration Testing

CreateSpace *Just as a professional athlete doesn't show up without a solid game plan, ethical hackers, IT professionals, and security researchers should not be unprepared, either. The Hacker Playbook provides them their own game plans. Written by a longtime security professional and CEO of Secure Planet, LLC, this step-by-step guide to the "game" of penetration hacking features hands-on examples and helpful advice from the top of the field. Through a series of football-style "plays," this straightforward guide gets to the root of many of the roadblocks people may face while penetration testing-including attacking different types of networks, pivoting through security controls, privilege escalation, and evading antivirus software. From "Pregame" research to "The Drive" and "The Lateral Pass," the practical plays listed can be read in order or referenced as needed. Either way, the valuable advice within will put you in the mindset of a penetration tester of a Fortune 500 company, regardless of your career or level of experience. This second version of The Hacker Playbook takes all the best "plays" from the original book and incorporates the latest attacks, tools, and lessons learned. Double the content compared to its predecessor, this guide further outlines building a lab, walks through test cases for attacks, and provides more customized code. Whether you're downing energy drinks while desperately looking for an exploit, or preparing for an exciting new job in IT security, this guide is an essential part of any ethical hacker's library-so there's no reason not to get in the game.*

Guide to Computer Forensics and Investigations

Cengage Learning *Updated with the latest advances from the field, GUIDE TO COMPUTER FORENSICS AND INVESTIGATIONS, Fifth Edition combines all-encompassing topic coverage and authoritative information from seasoned experts to deliver the most comprehensive forensics resource available. This proven author team's wide ranging areas of expertise mirror the breadth of coverage provided in the book, which focuses on techniques and practices for gathering and analyzing evidence used to solve crimes involving computers. Providing clear instruction on the tools and techniques of the trade, it introduces readers to every step of the computer forensics investigation-from lab set-up to testifying in court. It also details step-by-step guidance on how to use current forensics software. Appropriate for learners new to the field, it is also an excellent refresher and technology update for professionals in law enforcement, investigations, or computer security. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.*

PoC or GTFO

No Starch Press *This highly anticipated print collection gathers articles published in the much-loved International Journal of Proof-of-Concept or Get The Fuck Out. PoC||GTFO follows in the tradition of Phrack and Uninformed by publishing on the subjects of offensive security research, reverse engineering, and file format internals. Until now, the journal has only been available online or printed and distributed for free at hacker conferences worldwide. Consistent with the journal's quirky, biblical style, this book comes with all the trimmings: a leatherette cover, ribbon bookmark, bible paper, and gilt-edged pages. The book features more than 80 technical essays from numerous famous hackers, authors of classics like "Reliable Code Execution on a Tamagotchi," "ELFs are Dorky, Elves are Cool," "Burning a Phone," "Forget Not the Humble Timing Attack," and "A Sermon on Hacker Privilege." Twenty-four full-color pages by Ange Albertini illustrate many of the clever tricks described in the text.*

The Son Who Learned Obedience

A Theological Case Against the Eternal Submission of the Son

Wipf and Stock Publishers *This book offers a fresh perspective on the ongoing evangelical debate concerning whether the Son eternally submits to the Father. Beginning with the pro-Nicene account of will being a property of the single divine nature, Glenn Butner explores how language of eternal submission requires a modification of the classical theology of the divine will. This modification has problematic consequences for Christology, various atonement theories, and the doctrine of God, because as historically developed these doctrines shared the pro-Nicene assumption of a single divine will. This new angle on an old debate challenges the reader to move beyond the inaccurate characterization of views on eternal submission as "Arian" or "feminist" toward a more accurate understanding of the real theological issues at stake.*

Kali Linux 2: Windows Penetration Testing

Packt Publishing Ltd *Kali Linux: a complete pentesting toolkit facilitating smooth backtracking for working hackers About This Book Conduct network testing, surveillance, pen testing and forensics on MS Windows using Kali Linux Footprint, monitor, and audit your network and investigate any ongoing infestations Customize Kali Linux with this professional guide so it becomes your pen testing toolkit Who This Book Is For If you are a working ethical hacker who is looking to expand the offensive skillset with a thorough understanding of Kali Linux, then this is the book for you. Prior knowledge about Linux operating systems and the BASH terminal emulator along with Windows desktop and command line would be highly beneficial. What You Will Learn Set up Kali Linux for pen testing Map and enumerate your Windows network Exploit several common Windows network vulnerabilities Attack and defeat password schemes on Windows Debug and reverse-engineer Windows programs Recover lost files, investigate successful hacks and discover hidden data in innocent-looking files Catch and hold admin rights on the network, and maintain backdoors on the network after your initial testing is done In Detail Microsoft Windows is one of the two most common OS and managing its security has spawned the discipline of IT security. Kali Linux is the premier platform for testing and maintaining Windows security. Kali is built on the Debian distribution of Linux and shares the legendary stability of that OS. This lets you focus on using the network penetration, password cracking, forensics tools and not the OS. This book has the most advanced tools and techniques to reproduce the methods used by sophisticated hackers to make you an expert in Kali Linux penetration testing. First, you are introduced to Kali's top ten tools and other useful reporting tools. Then, you will find your way around your target network and determine known vulnerabilities to be able to exploit a system remotely. Next, you will prove that the vulnerabilities you have found are real and exploitable. You will learn to use tools in seven categories of exploitation tools. Further, you perform web access exploits using tools like websploit and more. Security is only as strong as the weakest link in the chain. Passwords are often that weak link. Thus, you learn about password attacks that can be used in concert with other approaches to break into and own a network. Moreover, you come to terms with network sniffing, which helps you understand which users are using services you can exploit, and IP spoofing, which can be used to poison a system's DNS cache. Once you gain access to a machine or network, maintaining access is important. Thus, you not only learn penetrating in the machine you also learn Windows privilege's escalations. With easy to follow step-by-step instructions and support images, you will be able to quickly pen test your system and network. Style and approach This book is a hands-on guide for Kali Linux pen testing. This book will provide all the practical knowledge needed to test your network's security using a proven hacker's methodology. The book uses easy-to-understand yet professional language for explaining concepts.*

The 8 Layers of the OSI Cake

A Forensic Taste of Each Layer

Do you do some form of Cyber Forensics or want to learn how or where to start? Whether you are specializing on dead box forensics, doing OSINT investigations, or working at a SOC, this publication has something for you.Inside, there are articles and hands on walkthroughs written by different authors covering the basics of the "8" layers of the OSI model("Cake") along with cyber forensics methods that fall into different areas of the stack. Included is information about the Dark Web, Forensic Imaging of drives, Data Recovery, Network Analysis (Ripping apart Trickbot traffic), Email Investigations, Visualizing threats and more...

Automating Open Source Intelligence

Algorithms for OSINT

Syngress *Algorithms for Automating Open Source Intelligence (OSINT) presents information on the gathering of information and extraction of actionable intelligence from openly available sources, including news broadcasts, public repositories, and more recently, social media. As OSINT has applications in crime fighting, state-based intelligence, and social research, this book provides recent advances in text mining, web crawling, and other algorithms that have led to advances in methods that can largely automate this process. The book is beneficial to both practitioners and academic researchers, with discussions of the latest advances in applications, a coherent set of methods and processes for automating OSINT, and interdisciplinary perspectives on the key problems identified within each discipline. Drawing upon years of practical experience and using numerous examples, editors Robert Layton, Paul Watters, and a distinguished list of contributors discuss Evidence Accumulation Strategies for OSINT, Named Entity Resolution in Social Media, Analyzing Social Media Campaigns for Group Size Estimation, Surveys and qualitative techniques in OSINT, and Geospatial reasoning of open data. Presents a coherent set of methods and processes for automating OSINT Focuses on algorithms and applications allowing the practitioner to get up and running quickly Includes fully developed case studies on the digital underground and predicting crime through OSINT Discusses the ethical considerations when using publicly available online data*

Reality Is Broken

Why Games Make Us Better and How They Can Change the World

Penguin *“McGonigal is a clear, methodical writer, and her ideas are well argued. Assertions are backed by countless psychological studies.” —The Boston Globe “Powerful and provocative . . . McGonigal makes a persuasive case that games have a lot to teach us about how to make our lives, and the world, better.” —San Jose Mercury News “Jane McGonigal's insights have the elegant, compact, deadly simplicity of plutonium, and the same explosive force.” —Cory Doctorow, author of Little Brother A visionary game designer reveals how we can harness the power of games to boost global happiness. With 174 million gamers in the United States alone, we now live in a world where every generation will be a gamer generation. But why, Jane McGonigal asks, should games be used for escapist entertainment alone? In this groundbreaking book, she shows how we can leverage the power of games to fix what is wrong with the real world-from social problems like depression and obesity to global issues like poverty and climate change-and introduces us to cutting-edge games that are already changing the business, education, and nonprofit worlds. Written for gamers and non-gamers alike, Reality Is Broken shows that the future will belong to those who can understand, design, and play games. Jane McGonigal is also the author of SuperBetter: A Revolutionary Approach to Getting Stronger, Happier, Braver and More Resilient.*

Zero Days, Thousands of Nights

The Life and Times of Zero-Day Vulnerabilities and Their Exploits

Rand Corporation *Zero-day vulnerabilities--software vulnerabilities for which no patch or fix has been publicly released-- and their exploits are useful in cyber operations--whether by criminals, militaries, or governments--as well as in defensive and academic settings. This report provides findings from real-world zero-day vulnerability and exploit data that could augment conventional proxy examples and expert opinion, complement current efforts to create a framework for deciding whether to disclose or retain a cache of zero-day vulnerabilities and exploits, inform ongoing policy debates regarding stockpiling and vulnerability disclosure, and add extra context for those examining the implications and resulting liability of attacks and data breaches for U.S. consumers, companies, insurers, and for the civil justice system broadly. The authors provide insights about the zero-day vulnerability research and exploit development industry; give information on what proportion of zero-day vulnerabilities are alive (undisclosed), dead (known), or somewhere in between; and establish some baseline metrics regarding the average lifespan of zero-day vulnerabilities, the likelihood of another party discovering a vulnerability within a given time period, and the time and costs involved in developing an exploit for a zero-day vulnerability"--Publisher's description.*

Think Like a Hacker

A Sysadmin's Guide to Cybersecurity

Targeted attack and determined human adversaries (DHA) have changed the information security game forever. Writing secure code is as important as ever; however, this satisfies only one piece of the puzzle. Effective defense against targeted attack requires IT professionals to understand how attackers use - and abuse - enterprise design to their advantage. Learn how advanced attackers break into networks. Understand how attackers use concepts of access and authorization to jump from one computer to the next. Dive into how and why attackers use custom implants and backdoors inside an enterprise. Be introduced to the concept of service-centric design - and how it can help improve both security and usability. To defend against hackers you must first learn to think like a hacker.

Android Software Internals Quick Reference

A Field Manual and Security Reference Guide to Java-based Android Components

Apress *Use this handy field guide as a quick reference book and cheat sheet for all of the techniques you use or reference day to day. Covering up to Android 11, this Android Java programming reference guide focuses on non-UI elements with a security focus. You won’t see Android UI development, nor will you see low-level C or kernel techniques. Instead, this book focuses on easily digestible, useful, and interesting techniques in Java and the Android system. This reference guide was created out of the need for myself to jot down all the useful techniques I commonly reached for, and so I’m now sharing these techniques with you, whether you are an Android internals software engineer or security researcher. What You Will Learn Discover the differences between and how to access application names, package names, IDs, and unique identifiers in Android Quickly reference common techniques such as storage, the activity lifecycle, and permissions Debug using the Android shell Work with Android's obfuscation and encryption capabilities Extract and decompile Android applications Carry out Android reflection and dex class loading Who This Book Is For Programmers, developers, and admins with at least prior Android and Java experience.*

Knife of Dreams

Book Eleven of 'The Wheel of Time'

Macmillan *The Wheel of Time is now an original series on Prime Video, starring Rosamund Pike as Moiraine! Since its debut in 1990, The Wheel of Time® by Robert Jordan has captivated millions of readers around the globe with its scope, originality, and compelling characters. The Wheel of Time turns and Ages come and go, leaving memories that become legend. Legend fades to myth, and even myth is long forgotten when the Age that gave it birth returns again. In the Third Age, an Age of Prophecy, the World and Time themselves hang in the balance. What was, what will be, and what is, may yet fall under the Shadow. The dead are walking, men die impossible deaths, and it seems as though reality itself has become unstable: All are signs of the imminence of Tarmon Gai'don, the Last Battle, when Rand al'Thor, the Dragon Reborn, must confront the Dark One as humanity's only hope. Unbeknownst to Rand, Perrin has made his own truce with the Seanchan. It is a deal made with the Dark One, in his eyes, but he will do whatever is needed to rescue his wife, Faile, and destroy the Shaido who captured her. Among the Shaido, Faile works to free herself while hiding a secret that might give her her freedom or cause her destruction. And at a town called Malden, the Two Rivers longbow will be matched against Shaido spears. Fleeing Ebou Dar through Seanchan-controlled Altara with the kidnapped Daughter of the Nine Moons, Mat attempts to court the woman to whom he is half-married, knowing that she will complete that ceremony eventually. But Tuon coolly leads him on a merry chase as he learns that even a gift can have deep significance among the Seanchan Blood and what he thinks he knows of women is not enough to save him. In Caemlyn, Elayne fights to gain the Lion Throne while trying to avert what seems a certain civil war should she win the crown... In the White Tower, Egwene struggles to undermine the sisters loyal to Elaida from within... The winds of time have become a storm, and things that everyone believes are fixed in place forever are changing before their eyes. Even the White Tower itself is no longer a place of safety. Now Rand, Perrin and Mat, Egwene and Elayne, Nynaeve and Lan, and even Loial, must ride those storm winds, or the Dark One will triumph. The Wheel of Time® New Spring: The Novel #1 The Eye of the World #2 The Great Hunt #3 The Dragon Reborn #4 The Shadow Rising #5 The Fires of Heaven #6 Lord of Chaos #7 A Crown of Swords #8 The Path of Daggers #9 Winter's Heart #10 Crossroads of Twilight #11 Knife of Dreams By Robert Jordan and Brandon Sanderson #12 The Gathering Storm #13 Towers of Midnight #14 A Memory of Light By Robert Jordan and Teresa Patterson The World of Robert Jordan's The Wheel of Time By Robert Jordan, Harriet McDougal, Alan Romanczuk, and Maria Simons The Wheel of Time Companion By Robert Jordan and Amy Romanczuk Patterns of the Wheel: Coloring Art Based on Robert Jordan's The Wheel of Time At the Publisher's request, this title is being sold without Digital Rights Management Software (DRM) applied.*

Hacking Exposed Wireless

McGraw Hill Professional *Secure Your Wireless Networks the Hacking Exposed Way Defend against the latest pervasive and devastating wireless attacks using the tactical security information contained in this comprehensive volume. Hacking Exposed Wireless reveals how hackers zero in on susceptible networks and peripherals, gain access, and execute debilitating attacks. Find out how to plug security holes in Wi-Fi/802.11 and Bluetooth systems and devices. You'll also learn how to launch wireless exploits from Metasploit, employ bulletproof authentication and encryption, and sidestep insecure wireless hotspots. The book includes vital details on new, previously unpublished attacks alongside real-world countermeasures. Understand the concepts behind RF electronics, Wi-Fi/802.11, and Bluetooth Find out how hackers use NetStumbler, WiSPY, Kismet, KisMAC, and AiroPeek to target vulnerable wireless networks Defend against WEP key brute-force, aircrack, and traffic injection hacks Crack WEP at new speeds using Field Programmable Gate Arrays or your spare PS3 CPU cycles Prevent rogue AP and certificate authentication attacks Perform packet injection from Linux Launch DoS attacks using device driver-independent tools Exploit wireless device drivers using the Metasploit 3.0 Framework Identify and avoid malicious hotspots Deploy WPA/802.11i authentication and encryption using PEAP, FreeRADIUS, and WPA pre-shared keys*

Hacking Exposed

Web Applications

McGraw-Hill Osborne Media *Get in-depth coverage of Web application platforms and their vulnerabilities, presented the same popular format as the international bestseller, Hacking Exposed. Covering hacking scenarios across different programming languages and depicting various types of attacks and countermeasures, this book offers you up-to-date and highly valuable insight into Web application security. "Required reading for Web architects and operators." -- Erik Olson, Microsoft Program Manager, Security, ASP.NET "Just as the original Hacking Exposed revealed the techniques the bad guys were hiding behind, Hacking Exposed Web Applications will do the same for this critical technology. Its methodical approach and appropriate detail will enlighten, educate, and go a long way toward making the Web a safer place in which to do business." -- from the Foreword by Mark Curphey, Chair of the Open Web Application Security Project "This is a serious technical guide that is also great reading -- scary enough to motivate folks to take Web security seriously but approachable enough to be an effective learning tool. Required reading for Web architects and operators." -- Erik Olson, Program Manager, Security, ASP.NET "What better way to defend against hackers than to understand the tools and techniques that are used to penetrate your site? Hacking Exposed Web Applications offers a detailed look at common vulnerabilities within your applications and explains how to protect yourself from them." -- Mike Mullins, Ecommerce Security Engineer for a leading specialty apparel retailer "At last, your personal guide to preventing the next generation of security threats. This book explains in intricate detail how you can do everything right when it comes to network security and still be owned at the Web application layer." -- Chip Andrews, www.sqlsecurity.com "If you're involved in writing Web-based applications using ASP/ASP.NET, Java, JSP, PHP, or other languages, the Hacking Exposed series is something you DEFINITELY need to read. Before writing one line of code, this book will spark ideas about how to design and secure your Web applications. There are techniques*