

## Mac Os X Hacking

Enterprise Mac Security is a definitive, expert-driven update of the popular, slash-dotted first edition which was written in part as a companion to the SANS Institute course for Mac OS X. It contains detailed Mac OS X security information, and walkthroughs on securing systems, including the new 10.11 operating system. A common misconception in the Mac community is that Mac's operating system is more secure than others. While this might be true in certain cases, security on the Mac has always still been a crucial issue. With the release of OS X 10.11, the operating system is taking large strides in getting even more secure. Even still, when sharing is enabled or remote control applications are installed, Mac OS X faces a variety of security threats, whether these have been exploited or not. This book caters to both the beginning home user and the seasoned security professional not accustomed to the Mac, establishing best practices for Mac OS X for a wide audience. The authors of this book are seasoned Mac and security professionals, having built many of the largest network infrastructures for Apple and spoken at both DEFCON and Black Hat on OS X security. What You Will Learn The newest security techniques on Mac OS X from the best and brightest Security details of Mac OS X for the desktop and server, and how to secure these systems The details of Mac forensics and Mac hacking How to tackle Apple wireless security Who This Book Is For This book is for new users, switchers, power users, and administrators that need to make sure their Mac systems are secure.

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

A common misconception in the Mac community is that the Mac is more secure than other operating systems. While this might be true in many cases, the fact that people actually use the computers is often not considered in this analysis. When sharing is enabled or remote control applications are installed, then a variety of security threats are established. This book enables users of the Mac to enable services while not sacrificing the security of their systems.

With El Capitan, Apple brings never-before-seen features to OS X—like a split-screen desktop, improved window controls, and amazing graphics. The new edition of David Pogue's #1 bestselling Mac book shows you how to use key new features such as swiping gestures, Notes, a new Spotlight search system, the Safari pinning feature, and Split View. Missing Manuals creator David Pogue is one of the most widely recognized technology authors in the world. A former New York Times technology columnist, he founded and now produces videos for Yahoo Tech.

Mac OS X Hacks

The Hacker's Guide to OS X

Defense against the Black Arts

Machine Learning for Hackers

Mac OS X: The Missing Manual, Tiger Edition

Beyond the Manual

**Discover the techniques behind beautiful design by deconstructing designs to understand them The term 'hacker' has been redefined to consist of anyone who has an insatiable curiosity as to how things work—and how they can try to make them better. This book is aimed at hackers of all skill levels and explains the classical principles and techniques behind beautiful designs by deconstructing those designs in order to understand what makes them so remarkable. Author and designer David Kadavy provides you with the framework for understanding good design and places a special emphasis on interactive mediums. You'll explore color theory, the role of proportion and geometry in design, and the relationship between medium and form. Packed with unique reverse engineering design examples, this book inspires and encourages you to discover and create new beauty in a variety of formats. Breaks down and studies the classical principles and techniques behind the creation of beautiful design Illustrates cultural and contextual considerations in communicating to a specific audience Discusses why design is important, the purpose of design, the various constraints of design, and how today's fonts are designed with the screen in mind Dissects the elements of color, size, scale, proportion, medium, and form Features a unique range of examples, including the graffiti in the ancient city of Pompeii, the lack of the color black in Monet's art, the style and sleekness of the iPhone, and more By the end of this book, you'll be able to apply the featured design principles to your own web designs, mobile apps, or other digital work.**

**Offers tips, techniques, and tools to help readers take advantage of Mac OS X, covering topics including user accounts, working with audio and video, running a mail server, and networking with Windows desktops.**

**With the advent of rich Internet applications, the explosion of social media, and the increased use of powerful cloud computing infrastructures, a new generation of attackers has added cunning new techniques to its arsenal. For anyone involved in defending an application or a network of systems, Hacking: The Next Generation is one of the few books to identify a variety of emerging attack vectors. You'll not only find valuable information on new hacks that attempt to exploit technical flaws, you'll also learn how attackers take advantage of individuals via social networking sites, and abuse vulnerabilities in wireless technologies and cloud infrastructures. Written by seasoned Internet security professionals, this book helps you understand the motives and psychology of**

hackers behind these attacks, enabling you to better prepare and defend against them. Learn how "inside out" techniques can poke holes into protected networks Understand the new wave of "blended threats" that take advantage of multiple application vulnerabilities to steal corporate data Recognize weaknesses in today's powerful cloud infrastructures and how they can be exploited Prevent attacks against the mobile workforce and their devices containing valuable data Be aware of attacks via social networking sites to obtain confidential information from executives and their assistants Get case studies that show how several layers of vulnerabilities can be used to compromise multinational corporations

With Leopard, Apple has unleashed the greatest version of Mac OS X yet, and David Pogue is back with another meticulous Missing Manual to cover the operating system with a wealth of detail. The new Mac OS X 10.5, better known as Leopard, is faster than its predecessors, but nothing's too fast for Pogue and this Missing Manual. It's just one of reasons this is the most popular computer book of all time. Mac OS X: The Missing Manual, Leopard Edition is the authoritative book for Mac users of all technical levels and experience. If you're new to the Mac, this book gives you a crystal-clear, jargon-free introduction to the Dock, the Mac OS X folder structure, and the Mail application. There are also mini-manuals on iLife applications such as iMovie, iDVD, and iPhoto, and a tutorial for Safari, Mac's web browser. This Missing Manual is amusing and fun to read, but Pogue doesn't take his subject lightly. Which new Leopard features work well and which do not? What should you look for? What should you avoid? Mac OS X: The Missing Manual, Leopard Edition offers an objective and straightforward instruction for using: Leopard's totally revamped Finder Spaces to group your windows and organize your Mac tasks Quick Look to view files before you open them The Time Machine, Leopard's new backup feature Spotlight to search for and find anything in your Mac Front Row, a new way to enjoy music, photos, and videos Enhanced Parental Controls that come with Leopard Quick tips for setting up and configuring your Mac to make it your own There's something new on practically every page of this new edition, and David Pogue brings his celebrated wit and expertise to every one of them. Mac's brought a new cat to town and Mac OS X: The Missing Manual, Leopard Edition is a great new way to tame it.

Your stepping stone to penetration testing

Ethical Hacking and Countermeasures: Linux, Macintosh and Mobile Systems

Creating and Automating Security Tools

iPhone Hacks

Mac Hacks

Mac OS X in a Nutshell

Introduces the UNIX environment in Mac OS X and explains concepts such as the Terminal application, compiling code, creating and installing packages, and building the Darwin kernel. Complete overview of Mac OS Jaguar (Mac OS X 10.2) including basic system and network administration features, hundreds of tips and tricks, with an overview of Mac OS X's Unix text editors and CVS.

Mac OS X was released in March 2001, but many components, such as Mach and BSD, are considerably older. Understanding the design, implementation, and workings of Mac OS X requires examination of several technologies that differ in their age, origins, philosophies, and roles. Mac OS X Internals: A Systems Approach is the first book that dissects the internals of the system, presenting a detailed picture that grows incrementally as you read. For example, you will learn the roles of the firmware, the bootloader, the Mach and BSD kernel components (including the process, virtual memory, IPC, and file system layers), the object-oriented I/O Kit driver framework, user libraries, and other core pieces of software. You will learn how these pieces connect and work internally, where they originated, and how they evolved. The book also covers several key areas of the Intel-based Macintosh computers. A solid understanding of system internals is immensely useful in design, development, and debugging for programmers of various skill levels. System programmers can use the book as a reference and to construct a better picture of how the core system works. Application programmers can gain a deeper understanding of how their applications interact with the system. System administrators and power users can use the book to harness the power of the rich environment offered by Mac OS X. Finally, members of the Windows, Linux, BSD, and other Unix communities will find the book valuable in comparing and contrasting Mac OS X with their respective systems. Mac OS X Internals focuses on the technical aspects of OS X and is so full of extremely useful information and programming examples that it will definitely become a mandatory tool for every Mac OS X programmer.

Mac OS X Leopard: Beyond the Manual is written for the sophisticated computer user who would find an introductory manual tedious. Features new to Leopard are emphasized, as are complex features that, though available in earlier versions of OS X, were not readily accessible. The narrative is fast-paced, concise, and respectful of the reader's familiarity with earlier versions of the program.

Mac OS X Hints

Serious Hacks, Mods and Customizations

Hacking- The art Of Exploitation

The Missing Manual

To the Apple's Core

Mac OS X Maximum Security

***As more and more vulnerabilities are found in the Mac OS X (Leopard) operating system, security researchers are realizing the importance of developing proof-of-concept exploits for those vulnerabilities. This unique tome is the first book to uncover the flaws in the Mac OS X operating system—and how to deal with them. Written by two white hat hackers, this book is aimed at making vital information known so that you can find ways to secure your Mac OS***

**X systems, and examines the sorts of attacks that are prevented by Leopard's security defenses, what attacks aren't, and how to best handle those weaknesses.**

**Presents fifty hacks to customize performance of a Mac, including automating tasks, increasing security, playing Wii games, and modifying wifi.**

**The EC-Council|Press Ethical Hacking and Countermeasures series is comprised of four books covering a broad base of topics in offensive network security, ethical hacking, and network defense and countermeasures. The content of this series is designed to immerse the reader into an interactive environment where they will be shown how to scan, test, hack, and secure information systems. A wide variety of tools, viruses, and malware is presented in these books, providing a complete understanding of the tactics and tools used by hackers. The full series of books helps prepare readers to take and succeed on the C|EH certification exam from EC-Council. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.**

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

**Mac OS X Internals**

**Mac OS X Leopard**

**Pushing the iPhone and iPod touch Beyond Their Limits**

**Mac OS X Panther Hacks**

**iOS Hacker's Handbook**

**Own it...Just Like Windows or Linux!**

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

The sexy, elegant design of the Apple PowerBook combined with the Unix-like OS X operating system based on FreeBSD, have once again made OS X the Apple of every hacker's eye. In this unique and engaging book covering the brand new OS X 10.4 Tiger, the world's foremost "true hackers unleash the power of OS X for everything from cutting edge research and development to just plain old fun. OS X 10.4 Tiger is a major upgrade for Mac OS X for running Apple's Macintosh computers and laptops. This book is not a reference to every feature and menu item for OS X. Rather, it teaches hackers of all types from software developers to security professionals to hobbyists, how to use the most powerful (and often obscure) features of OS X for wireless networking, WarDriving, software development, penetration testing, scripting administrative tasks, and much more. \* Analyst reports indicate that OS X sales will double in 2005. OS X Tiger is currently the #1 selling software product on Amazon and the 12-inch PowerBook is the #1 selling laptop \* Only book on the market directly appealing to groundswell of hackers migrating to OS X \* Each chapter written by hacker most commonly associated with that topic, such as Chris Hurley (Roamer) organizer of the World Wide War Drive

If you're an app developer with a solid foundation in Objective-C, this book is an absolute must—chances are very high that your company's iOS applications are vulnerable to attack. That's because malicious attackers now use an arsenal of tools to reverse-engineer, trace, and manipulate applications in ways that most programmers aren't aware of. This guide illustrates several types of iOS attacks, as well as the tools and techniques that hackers use. You'll learn best practices to help protect your applications, and discover how important it is to understand and strategize like your adversary. Examine subtle vulnerabilities in real-world applications—and avoid the same problems in your apps Learn how attackers infect apps with malware through code injection Discover how attackers defeat iOS keychain and data-protection encryption Use a debugger and custom code injection to manipulate the runtime Objective-C environment Prevent attackers from hijacking SSL sessions and stealing traffic Securely delete files and design your apps to prevent forensic data leakage Avoid debugging abuse, validate the integrity of run-time classes, and make your code harder to trace

## Get Free Mac Os X Hacking

This serious, but fun, down-and-dirty book will let you make Tiger purr, ensuring that your Mac's appearance, speed, usability, and security settings are what you want. Author Scott Knaster: Shows you how to speed it up, lock it down, or pull back the curtains. Dives into default system settings, unlocks hidden gems, and includes original Mac OS X programs with full source listings and explanations. Shows heavyweight hackers the tricks and modes of OS X booting, tweaks for login screens, and how to customize or even kill the Dock. Offers the inside scoop on Dashboard and Spotlight, including two sample widgets and one Spotlight importer, all with fully annotated source listings. Demonstrates how to install and use Unix and X11 applications, take advantage of command line tools, and create system services and active Dock badges. Order your copy today.

For OS X and iOS

Tips & Tools for unlocking the power of your Apple devices

Jaguar Edition

OS X Exploits and Defense

The Mac Hacker's Handbook

A Guide to Kernel Exploitation

Bigger in size, longer in length, broader in scope, and even more useful than our original Mac OS X Hacks, the new Big Book of Apple Hacks offers a grab bag of tips, tricks, and hacks to get the most out of Mac OS X Leopard, as well as the new line of iPods, iPhone, and Apple TV. With 125 entirely new hacks presented in step-by-step fashion, this practical book is for serious Apple computer and gadget users who really want to take control of these systems. Many of the hacks take you under the hood and show you how to tweak system preferences, alter or add keyboard shortcuts, mount drives and devices, and generally do things with your operating system and gadgets that Apple doesn't want you to do. The Big Book of Apple Hacks gives you: Hacks for both Mac OS X Leopard and Tiger, their related applications, and the hardware they run on or connect to. Includes tutorials and lots of background material, including informative sidebars "Quick Hacks" for tweaking system and gadget settings in minutes. Full-blown hacks for adjusting Mac OS X applications such as Mail, Safari, iCal, Front Row, or the iLife suite. Plenty of hacks and tips for the Mac mini, the MacBook laptops, and new Intel desktops. Tricks for running Windows on the Mac, under emulation in Parallels or as a standalone OS with Bootcamp. The Big Book of Apple Hacks is not only perfect for Mac fans and power users, but also for recent -- and aspiring -- "switchers" new to the Apple experience. Hacks are arranged by topic for quick and easy lookup, and each one stands on its own so you can pick and choose around and tweak whatever system or gadget strikes your fancy. Pick up this book and take control of Mac OS X and your favorite Apple gadget today!

Provides instructions on customizing the Macintosh operating system, covering such topics as changing the desktop themes, changing system sounds, altering an application's interface, and changing keyboard shortcuts.

The EC-Council | Press Ethical Hacking and Countermeasures Series is comprised of five books covering a broad base of topics in offensive network security, ethical hacking, and network defense and countermeasures. The content of this series is designed to immerse the reader into an interactive environment where they will be shown how to test, hack and secure information systems. With the full series of books, the reader will gain in-depth knowledge and practical experience with essential security systems and become prepared to succeed on the Certified Ethical Hacker, or C|EH, certification from EC-Council. This certification covers a plethora of offensive security topics ranging from how perimeter defenses work, to scanning and attacking simulated networks. A wide variety of tools, viruses, and malware is presented in this and the other four books to give you a complete understanding of the tactics and tools used by hackers. By gaining a thorough understanding of how hackers operate, an Ethical Hacker will be able to set up effective countermeasures and defensive systems to protect an organization's critical infrastructure and information. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

While Mac OS X is becoming more and more stable with each release, its UNIX/BSD underpinnings have security implications that ordinary Mac users have never before faced with. Mac OS X can be used as both a powerful Internet server, or, in the wrong hands, a very powerful attack launch point. Yet most Mac OS X books are generally simplistic -- with the exception of the author's Mac OS X Unleashed, the first book to address OS X's underlying BSD subsystem. Maximum Mac OS X Security takes a UNIX-oriented approach, going into significantly greater depth on OS X security topics: Setup basics, including Airport and network topology security. User administration and resource management with NetInfo. Types of attacks, how attacks work, and how to stop them. Network service security, such as e-mail, Web, and file sharing. Intrusion prevention and detection, and hands-on detection tools.

Exploiting OS X from the Root Up

Case Studies and Algorithms to Get You Started

Design for Hackers

Eh

Foundations of Mac OS X Leopard Security

Mac OS X and iOS Internals

**Offers tips, techniques, and tools to help readers take advantage of Mac OS X, covering topics including keyboard commands, iTunes, e-mail, remote connection, and Terminal.**

**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.**

**Written by two experienced penetration testers the material presented discusses the basics of the OS X environment and its vulnerabilities. Including but limited to; application porting, virtualization utilization and offensive tactics at the kernel, OS and wireless level. This book provides a comprehensive in-depth guide to exploiting and compromising the OS X platform while offering the necessary defense and countermeasure techniques that can be used to stop hackers As a resource to the reader, the companion website will provide links from the authors, commentary and updates. Provides relevant information including some of the latest OS X threats Easily accessible to those without any prior OS X experience Useful tips and strategies for exploiting and compromising OS X systems Includes discussion of defensive and countermeasure applications and how to use them Covers mobile IOS vulnerabilities**

**As technology has developed, computer hackers have become increasingly sophisticated, mastering the ability to hack into even the most impenetrable systems. The best way to secure a system is to understand the tools hackers use and know how to circumvent them. Defense against the Black Arts: How Hackers Do What They Do and How to Protect against It provides hands-on instruction to a host of techniques used to hack into a variety of systems. Exposing hacker methodology with concrete examples, this book shows you how to outwit computer predators at their own game. Among the many things you'll learn: How to get into a Windows operating system without having the username or password Vulnerabilities associated with passwords and how to keep them out of the hands of hackers How hackers use the techniques of computer forensic examiners to wreak havoc on individuals and companies Hiding one's IP address to avoid detection Manipulating data to and from a web page or application for nefarious reasons How to find virtually anything on the internet How hackers research the targets they plan to attack How network defenders collect traffic across the wire to indentify intrusions Using Metasploit to attack weaknesses in systems that are unpatched or have poorly implemented security measures The book profiles a variety of attack tools and examines how Facebook and other sites can be used to conduct social networking attacks. It also covers techniques utilized by hackers to attack modern operating systems, such as Windows 7, Windows Vista, and Mac OS X. The author explores a number of techniques that hackers can use to exploit physical access, network access, and wireless vectors. Using screenshots to clarify procedures, this practical manual uses step-by-step examples and relevant analogies to facilitate understanding, giving you an insider's view of the secrets of hackers.**

**Gray Hat C#**

**Attacking the Core**

**Hacking: The Next Generation**

**Modding Mac OS X**

**Mac OS X for Unix Geeks**

**A Systems Approach**

*Learn to write apps for some of today's hottest technologies, including the iPhone and iPad (using iOS), as well as the Mac (using OS X). It starts with Objective-C, the base language on which the native iOS software development kit (SDK) and the OS X are based. Learn Objective-C on the Mac: For OS X and iOS, Second Edition updates a best selling book and is an extensive, newly updated guide to Objective-C. Objective-C is a powerful, object-oriented extension of C, making this update the perfect follow-up to Dave Mark's bestselling Learn C on the Mac. Whether you're an experienced C programmer or you're coming from a different language such as C++ or Java, leading Mac experts Scott Knaster and Waqar Malik show how to harness the power of Objective-C in your apps! A complete course on the basics of Objective-C using Apple's newest Xcode tools An introduction to object-oriented programming Comprehensive coverage of new topics like blocks, GCD, ARC, class*

*extensions, as well as inheritance, composition, object initialization, categories, protocols, memory management, and organizing source files*  
*An introduction to building user interfaces using what is called the UIKit A primer for non-C programmers to get off the ground even faster*  
*If you're an experienced programmer interested in crunching data, this book will get you started with machine learning—a toolkit of algorithms that enables computers to train themselves to automate useful tasks. Authors Drew Conway and John Myles White help you understand machine learning and statistics tools through a series of hands-on case studies, instead of a traditional math-heavy presentation. Each chapter focuses on a specific problem in machine learning, such as classification, prediction, optimization, and recommendation. Using the R programming language, you'll learn how to analyze sample datasets and write simple machine learning algorithms. Machine Learning for Hackers is ideal for programmers from any background, including business, government, and academic research. Develop a naïve Bayesian classifier to determine if an email is spam, based only on its text Use linear regression to predict the number of page views for the top 1,000 websites Learn optimization techniques by attempting to break a simple letter cipher Compare and contrast U.S. Senators statistically, based on their voting records Build a "whom to follow" recommendation system from Twitter data*

*Demonstrates the operating system's basic features, including Internet access, file management, configuring the desktop, installing peripherals, and working with applications.*

*Learn to use C#'s powerful set of core libraries to automate tedious yet important tasks like performing vulnerability scans, malware analysis, and incident response. With some help from Mono, you can write your own practical security tools that will run on Mac, Linux, and even mobile devices. Following a crash course in C# and some of its advanced features, you'll learn how to: -Write fuzzers that use the HTTP and XML libraries to scan for SQL and XSS injection -Generate shellcode in Metasploit to create cross-platform and cross-architecture payloads -Automate Nessus, OpenVAS, and sqlmap to scan for vulnerabilities and exploit SQL injections -Write a .NET decompiler for Mac and Linux -Parse and read offline registry hives to dump system information -Automate the security tools Arachni and Metasploit using their MSGPACK RPCs Streamline and simplify your work day with Gray Hat C# and C#'s extensive repertoire of powerful tools and libraries.*

*Stealing Data, Hijacking Software, and How to Prevent It*

*Mac OS X Leopard: The Missing Manual*

*Hacking and Securing iOS Applications*

*OS X El Capitan: The Missing Manual*

*Extreme Makeovers for Your Mac*

*Enterprise Mac Security: Mac OS X*

**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 vulnerability—a 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

**An in-depth look into Mac OS X and iOS kernels** Powering Macs, iPhones, iPads and more, OS X and iOS are becoming ubiquitous. When it comes to documentation, however, much of them are shrouded in mystery. Cocoa and Carbon, the application frameworks, are neatly described, but system programmers find the rest lacking. This indispensable guide illuminates the darkest corners of those systems, starting with an architectural overview, then drilling all the way to the core. Provides you with a top down view of OS X and iOS Walks you through the phases of system startup—both Mac (EFi) and mobile (iBoot) Explains how processes, threads, virtual memory, and filesystems are maintained Covers the security architecture Reviews the internal APIs used by the system—BSD and Mach Dissects the kernel, XNU, into its sub components: Mach, the BSD Layer, and I/o kit, and explains each in detail Explains the inner workings of device drivers From architecture to implementation, this book is essential reading if you want to get serious about the internal workings of Mac OS X and iOS.

Contrary to popular belief, there has never been any shortage of Macintosh-related security issues. OS9 had issues that warranted attention. However, due to both



Like the animal it's named for, Mac OS X Panther is beautiful, sleek, superbly efficient, dangerously alluring, and all muscle under the surface. Beneath its appealing interface, it's a machine. Those coming to Mac OS X from previous incarnations of the operating system recognize much of the friendly face of the Macintosh they're used to, but they're also plunged into a new world. Unix converts to Mac OS X find a familiar FreeBSD-like operating system at the core and many of the command-line applications that they're familiar with: it's like an open invitation to tinker, experiment, and hack. Mac OS X Panther Hacks brings together the perfect combination of tips, tricks, and tools to help serious Mac users--regardless of their background--get the most out of their Mac. This revised collection reflects the real-world know-how of those well-steeped in Unix history and expertise, sharing their no-nonsense, sometimes quick-and-dirty solutions to administrative tasks and taking full advantage of everything a Unix desktop has to offer: Web, Mail, and FTP serving, security services, SSH, Perl and shell scripting, compiling, configuring, scheduling, networking, and more. Drawing on the experience of die-hard Macintosh users, customizing and modifying their hardware and software to meet their needs. The end result is cool stuff no power user should be without. The hacks range from the quick and easy to the more complex. Each can be read easily in a few minutes, saving countless hours of searching for the right answer. Mac OS X Panther Hacks provides practical solutions in topics such as: User Interface Accessories (iPod, USB devices, mobile phones, PDAs, etc.) Wired and wireless networking (Ethernet, WiFi, Bluetooth, etc.) Email (servers and clients) Messaging (iChat and associated apps) Printing and Faxing (sharing printers, fax server, etc.) Multimedia If you want more than your average Mac user--you want to experiment, unearth shortcuts, create useful tools, and come up with fun things to try on your own--this book will set you on the right track. Written for users who need to go beyond conventional manuals--Mac OS X Panther Hacks will bring your Mac to its full potential.

Learn Objective-C on the Mac

The Next Generation

Mac OS X Power Hound

Reverse Engineering Beauty

Exploiting Software: How To Break Code

Hacking Mac OS X Tiger