The Le Application Hackers Handbook

Learn how people break websites and how you can, too. Real-World Bug Hunting is the premier field guide to finding software bugs. Whether you're a cyber-security beginner who wants to make the internet safer or a seasoned developer who wants to write secure code, ethical hacker Peter Yaworski will show you how it's done. You'll learn about the most common types of bugs like cross-site scripting, insecure direct object references, and server-side request forgery. Using real-life case studies of rewarded vulnerabilities from applications like Twitter, Facebook, Google, and Uber, you'll see how hackers manage to invoke race conditions while transferring money, use URL parameter to cause users to like unintended tweets, and more. Each chapter introduces a vulnerability type accompanied by a series of actual reported bug bounties. The book's collection of tales from the field will teach you how attackers trick users into giving away their sensitive information and how sites may reveal their vulnerabilities to savvy users. You'll even learn how you could turn your challenging new hobby into a successful career. You'll learn: • How the internet works and basic web hacking concepts • How attackers compromise websites • How to identify functionality commonly associated with vulnerabilities • How to find bug bounty programs and submit effective vulnerability reports Real-World Bug Hunting is a fascinating soup-to-nuts primer on web security vulnerabilities, filled with stories from the trenches and practical wisdom. With your new understanding of site security and weaknesses, you can help make the web a safer place--and profit while you're at it.

Discover all the security risks and exploits that can threateniOS-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 tolight. This book explains and discusses them all. The award-winningauthor team, experts in Mac and iOS security, examines thevulnerabilities and the internals of iOS to show how attacks can bemitigated. The book explains how the operating system works, itsoverall security architecture, and the security risks associatedwith it, as well as exploits, rootkits, and other payloadsdeveloped for it. Covers iOS security architecture, vulnerability hunting,exploit writing, and how iOS jailbreaks work Explores iOS enterprise and encryption, code signing and memoryprotection, sandboxing, iPhone fuzzing, exploitation, ROP payloads,and baseband attacks Also examines kernel debugging and exploitation Companion website includes source code and tools to facilitateyour efforts iOS Hacker's Handbook arms you with the tools needed toidentify, understand, and foil iOS attacks.

Up-to-date strategies for thwarting the latest, most insidious network attacks This fully updated, industry-standard security resource shows, step by step, how to fortify computer networks by learning and applying effective ethical hacking techniques. Based on curricula developed by the authors at major security conferences and colleges, the book features actionable planning and analysis methods as well as practical steps for identifying and combating both targeted and opportunistic attacks. Gray Hat Hacking: The Ethical Hacker's Handbook, Sixth Edition clearly explains the enemy’s devious weapons, skills, and tactics and offers field-tested remedies, case studies, and testing labs. You will get complete coverage of Internet of Things, mobile, and Cloud security along with penetration testing, malware analysis, and reverse engineering techniques. State-of-the-art malware, ransomware, and system exploits are thoroughly explained. •Fully revised content includes 7 new chapters covering the latest threats •Includes proof-of-concept code stored on the GitHub repository •Authors train attendees at major security conferences, including RSA, Black Hat, Defcon, and Besides

This book combines detailed scientific historical research with characteristic philosophic breadth and verve.

The Hacker's Handbook

Hacking Exposed Web Applications, Second Edition

A Practical Guide to Hacking the Internet of Things

Discovering and Exploiting Security Flaws

Language Hacking French

The Taming of Chance

Before the Internet became widely known as a global tool for terrorists, one perceptive U.S. citizen recognized its ominous potential. Armed with clear evidence of computer espionage, he began a highly personal quest to expose a hidden network of spies that threatened national security. But would the authorities back him up? Cliff Stoll's dramatic firsthand account is "a computer-age detective story, instantly fascinating [and] astonishingly gripping" (Smithsonian). Cliff Stoll was an astronomer turned systems manager at Lawrence Berkeley Lab when a 75-cent accounting error alerted him to the presence of an unauthorized user on his system. The hacker's code name was "Hunter"—a mysterious invader who managed to break into U.S. computer systems and steal sensitive military and security information. Stoll began a one-man hunt of his own: spying on the spy. It was a dangerous game of deception, broken codes, satellites, and missile bases—a one-man sting operation that finally gained the attention of the CIA . . . and ultimately trapped an international spy ring fueled by cash, cocaine, and the KGB.

A fast, hands-on introduction to offensive hacking techniques Hands-On Hacking teaches readers to see through the eyes of their adversary and apply hacking techniques to better understand real-world risks to computer networks and data. Readers will benefit from the author's years of experience in the field hacking into computer networks and ultimately training others in the art of cyber-attacks. This book holds no punches and explains the tools, tactics and procedures used by ethical hackers and criminal crackers alike. We will take you on a journey through a hacker's perspective when focused on the computer infrastructure of a target company, exploring how to access the servers and data. Once the information gathering stage is complete, you'll look for flaws and their known exploits—including tools developed by real-world government financed state-actors. •An introduction to the same hacking techniques that malicious hackers will use against an organization •Written by infosec experts with proven history of publishing vulnerabilities and highlighting security flaws • Based on the tried and tested material used to train hackers all over the world in the art of breaching networks •Covers the fundamental basics of how computer networks are inherently vulnerable to attack, teaching the student how to apply hacking skills to uncover vulnerabilities We cover topics of breaching a company from the external network perimeter, hacking internal enterprise systems and web application vulnerabilities. Delving into the basics of exploitation with real-world practical examples, you won't find any hypothetical academic only attacks here. From start to finish this book will take the student through the steps necessary to breach an organization to improve its security. Written by world-renowned cybersecurity experts and educators, Hands-On Hacking teaches entry-level professionals seeking to learn ethical hacking techniques. If you are looking to understand penetration testing and ethical hacking, this book takes you from basic methods to advanced techniques in a structured learning format.

A guide to Web site security looks at the ways hackers target and attack vulnerable sites and provides information and case studies on countermeasures and security techniques.

Hacking Leadership is Mike Myatt's latest leadership book written for leaders at every level. Leadership isn't broken, but how it's currently being practiced certainly is. Everyone has blind spots. The purpose of Hacking Leadership is to equip leaders at every level with an actionable framework to identify blind spots and close leadership gaps. The bulk of the book is based on actionable, topical leadership and management hacks to bridge eleven gaps every business needs to cross in order to create a culture of leadership: leadership, purpose, future, mediocrity, culture, talent, knowledge, innovation, expectation, complexity, and failure. Each chapter: Gives readers specific techniques to identify, understand, and most importantly, implement individual, team and organizational leadership hacks. Addresses blind spots and leverage points most leaders and managers haven't thought about, which left unaddressed, will adversely impact growth, development, and performance. All leaders have blind-spots (gaps), which often go undetected for years or decades, and sadly, even when identified the methods for dealing with them are outdated and ineffective – they need to be hacked. Showcases case studies from the author's consulting practice, serving as a confidant with more than

150 public company CEOs. Some of those corporate clients include: AT&T, Bank of America, Deloitte, EMC, Humana, IBM, JP Morgan Chase, Merrill Lynch, PepsiCo, and other leading global brands. Hacking Leadership offers a fresh perspective that makes it easy for leaders to create a roadmap to identify, refine, develop, and achieve their leadership potential--and to create a more effective business that is financially solvent and professionally desirable.

Real-World Bug Hunting

A Hands-On Introduction to Hacking

Practical IoT Hacking

Hacking Connected Cars

The Hacking of the American Mind

Eh

While many resources for network and IT security are available, detailed knowledge regarding modern web application security has been lacking—until now. This practical guide provides both offensive and defensive security concepts that software engineers can easily learn and apply. Andrew Hoffman, a senior security engineer at Salesforce, introduces three pillars of web application security: recon, offense, and defense. You'll learn methods for effectively researching and analyzing modern web applications—including those you don't have direct access to. You'll also learn how to break into web applications using the latest hacking techniques. Finally, you'll learn how to develop mitigations for use in your own web applications to protect against hackers. Explore common vulnerabilities plaguing today's web applications Learn essential hacking techniques attackers use to exploit applications Map and document web applications for which you don't have direct access Develop and deploy customized exploits that can bypass common defenses Develop and deploy mitigations to protect your applications against hackers Integrate secure coding best practices into your development lifecycle Get practical tips to help you improve the overall security of your web applications

It's true that some people spend years studying French before they finally get around to speaking the language. But here's a better idea. Skip the years of study and jump right to the speaking part. Sound crazy? No, it's language hacking. Unlike most traditional language courses that try to teach you the rules of French, #LanguageHacking shows you how to learn and speak French through proven memory techniques, unconventional shortcuts and conversation strategies perfected by one of the world's greatest language learners, Benny Lewis, aka the Irish Polyglot. Using the language hacks -shortcuts that make learning simple - that Benny mastered while learning his 11 languages and his 'speak from the start' method, you will crack the language code and exponentially increase your language abilities so that you can get fluent faster. It's not magic. It's not a language gene. It's not something only "other people" can do. It's about being smart with how you learn, learning what's indispensable, skipping what's not, and using what you've learned to have real conversations in French from day one. The Method #LanguageHacking takes a modern approach to language learning, blending the power of online social collaboration with traditional methods. It focuses on the conversations that learners need to master right away, rather than presenting language in order of difficulty like most courses. This means that you can have conversations immediately, not after years of study. Each of the 10 units culminates with a speaking 'mission' that prepares you to use the language you've learned to talk about yourself. Through the language hacker online learner community, you can share your personalized speaking 'missions' with other learners - getting and giving feedback and extending your learning beyond the pages of the book . You don't need to go abroad to learn a language any more.

The first comprehensive guide to discovering and preventingattacks on the Android OS As the Android operating system continues to increase its shareof the smartphone market, smartphone hacking remains a growingthreat. Written by experts who rank among the world's

foremostAndroid security researchers, this book presents vulnerabilitydiscovery, analysis, and exploitation tools for the good guys.Following a detailed explanation of how the Android OS works andits overall security architecture, the authors examine howvulnerabilities can be discovered and exploits developed forvarious system components, preparing you to defend againstthem. If you are a mobile device administrator, security researcher,Android app developer, or consultant responsible for evaluatingAndroid security, you will find this guide is essential to yourtoolbox. A crack team of leading Android security researchers explainAndroid security risks, security design and architecture, rooting,fuzz testing, and vulnerability analysis Covers Android application building blocks and security as wellas debugging and auditing Android apps Prepares mobile device administrators, security researchers,Android app developers, and security consultants to defend Androidsystems against attack Android Hacker's Handbook is the first comprehensiveresource for IT professionals charged with smartphonesecurity.

Android Hacker's HandbookJohn Wiley & Sons

Penetration Testing

The Mac Hacker's Handbook

Hacker Linux Uncovered

Language Hacking Italian

Web Application Security Secrets and Solutions

Cert Ethi Hack (CEH Cert Guid

Tips for the practical use of debuggers, such as NuMega SoftIce, Microsoft Visual Studio Debugger, and Microsoft Kernel Debugger, with minimum binding to a specific environment are disclosed in this debugger guide. How debuggers operate and how to overcome obstacles and repair debuggers is demonstrated. Programmers will learn how to look at what is inside a computer system, how to reconstruct the operating algorithm of a program distributed without source code, how to modify the program, and how to debug drivers. The use of debugging applications and drivers in Windows and Unix operating systems on Intel Pentium/DEC Alpha-based processors is also detailed.

Stop hackers before they hack you! In order to outsmart a would-be hacker, you need to get into the hacker's mindset. And with this book, thinking like a bad guy has never been easier. In Hacking For Dummies, expert author Kevin Beaver shares his knowledge on penetration testing, vulnerability assessments, security best practices, and every aspect of ethical hacking that is essential in order to stop a hacker in their tracks. Whether you're worried about your laptop, smartphone, or desktop computer being compromised, this no-nonsense book helps you learn how to recognize the vulnerabilities in your systems so you can safeguard them more diligently—with confidence and ease. Get up to speed on Windows 10 hacks Learn about the latest mobile computing hacks Get free testing tools Find out about new system updates and improvements There's no such thing as being too safe—and this resourceful guide helps ensure you're protected.

Concentrating on Linux installation, tuning, and administration, this guide to protecting systems from security attacks demonstrates how

to install Linux so that it is tuned for the highest security and best performance, how to scan the network and encrypt the traffic for securing all private traffics in a public network, and how to monitor and log the system to detect potential security problems. Backup and recovery policies that provide a structure for secure operations are also considered, and information related to configuring an Apache server, e-mail service, and the Internet gateway using a proxy server, an FTP server, DSN server for mapping DNS names to IP addresses, and firewall for system protection is provided.

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

Gray Hat Hacking: The Ethical Hacker's Handbook, Sixth Edition

The Mobile Application Hacker's Handbook

Hands on Hacking

Concepts, Methodologies, Tools and Applications

IOS Application Security

Web App Hacking

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 scan, 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, providing 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 strong 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.

This book is a practical guide to discovering and exploiting security flaws in web applications. The authors explain each category of vulnerability using real-world examples, screen shots and code extracts. The book is extremely practical in focus, and describes in detail the steps involved in detecting and exploiting each kind of security weakness found within a variety of applications such as online banking, e-commerce and other web applications. The topics covered include bypassing login mechanisms, injecting code, exploiting logic flaws and compromising other users. Because every web application is different, attacking them entails bringing to bear various general principles, techniques and experience in an imaginative way. The most successful hackers go beyond this, and find ways to automate their bespoke attacks. This handbook describes a proven methodology that combines the virtues of human intelligence and computerized brute force, often with devastating results. The authors are professional penetration testers who have been involved in web application security for nearly a decade. They have presented training courses at the Black Hat security conferences throughout the world. Under the alias "PortSwigger", Dafydd developed the popular Burp Suite of web application hack tools.

Threatening the safety of individuals, computers, and entire networks, cyber crime attacks vary in severity and type. Studying this continually evolving discipline involves not only understanding different types of attacks, which range from identity theft to cyberwarfare, but also identifying methods for their prevention. Cyber Crime: Concepts, Methodologies, Tools and Applications is a three-volume reference that explores all aspects of computer-based crime and threats, offering solutions and best practices from experts in software development, information security, and law. As cyber crime continues to change and new types of threats emerge, research focuses on developing a critical understanding of different

types of attacks and how they can best be managed and eliminated. Here is the ultimate book on the worldwide movement of hackers, pranksters, and activists that operates under the non-name Anonymous, by the writer the Huffington Post says "knows all of Anonymous' deepest, darkest secrets." Half a dozen years ago, anthropologist Gabriella Coleman set out to study the rise of this global phenomenon just as some of its members were turning to political protest and dangerous disruption (before Anonymous shot to fame as a key player in the battles over WikiLeaks, the Arab Spring, and Occupy Wall Street). She ended up becoming so closely connected to Anonymous that the tricky story of her inside–outside status as Anon confidante, interpreter, and erstwhile mouthpiece forms one of the themes of this witty and entirely engrossing book. The narrative brims with details unearthed from within a notoriously mysterious subculture, whose semi-legendary tricksters—such as Topiary, tflow, Anachaos, and Sabu—emerge as complex, diverse, politically and culturally sophisticated people. Propelled by years of chats and encounters with a multitude of hackers, including imprisoned activist Jeremy Hammond and the double agent who helped put him away, Hector Monsegur, Hacker, Hoaxer, Whistleblower, Spy is filled with insights into the meaning of digital activism and little understood facets of culture in the Internet age, including the history of "trolling," the ethics and metaphysics of hacking, and the origins and manifold meanings of "the lulz."

iOS Hacker's Handbook

Hacking For Dummies

Hacker, Hoaxer, Whistleblower, Spy

Ethical Hacking and Countermeasures: Attack Phases

Profiling Hackers

The Definitive Guide to Attacking the Internet of Things

Avertissement : à ceux qui veulent apprendre l''art de l''attaque et qui veulent devenir les pionniers de ce nouveau monde, ce livre est écrit pour vous. Peu importe le dispositif que vous utilisez pour lire ces lignes, vous êtes déjà au milieu de l''arène du combat ! Et la question qui se pose maintenant : est-ce que savez-vous vous défendre ou pas ? Internet est un terrain de jeu très dangereux. Que vous soyez un hacker débutant qui veut apprendre le hacking Web ou un développeur en herbe qui met en ligne ses applications Web, une connaissance approfondie du fonctionnement de ces applications est requise pour savoir pénétrer/protéger ses applications avant que les pirates ne le fassent à votre place. À première vue, les applications Web semblent difficile à comprendre, on se perd rapidement dans l''océan d''informations, de failles, de patchs et de frameworks disponibles sur la toile, et cela décourage les gens qui débutent dans ce truc de Web App Hacking. Mais la vérité, c''est que vous ne pouvez pas abandonner si

facilement ; parce que sans ces connaissances, vous ne deviendrez jamais un vrai hacker/développeur. Peut-être que vous avez déjà tenté de suivre quelques tutoriels sur la sécurité des applications Web, que vous avez entendu parler de XSS, SQL, CSRF, mais que tous ces concepts ne sont pas très clairs dans votre tête, sans parler de l''aspect pratique de ces attaques. Mais ce que j''ai remarqué, c''est qu''il ne faut pas tomber dans le piège d''apprendre la façon d''attaquer une application sans comprendre comment l''application elle-même fonctionne. Comprendre la logique de votre application-cible est la clé pour la faire réagir comme vous voulez (aka : la hacké). Si vous voulez vraiment apprendre le hacking Web en partant de zéro, il faut que vous suiviez un plan d''apprentissage organisé en commençant par la compréhension de la technologie que vous voulez pénétrer/protéger, puis ensuite, exécuter des attaques en se basant sur la théorie que vous aurez acquise tout au long de votre formation. Prenez ce livre et fixez-vous une deadline de 20 jours pour le lire, le comprendre et appliquer toutes les attaques qui sont démontrées à l''intérieur, j''ai veillé à inclure uniquement ce dont vous avez besoin pour faire du pentesting Web efficace et rapide, donc pas de superflu dans ce livre. Si vous prenez au sérieux la lecture et l''application des concepts présentés dans ce livre, vous sortirez avec des compétences d''un vrai pentesteur. Vous découvrirez dans ce livre : Pourquoi les applications Web sont précieuses et les différents types utilisés de nos jours Comment créer un laboratoire de hacking sécurisé Pourquoi suivre une méthodologie de hacking est nécessaire pour tout hackeur Comment utiliser les outils de Kali Linux pour faire du pentesting de A à Z La fameuse SQLi est comment l''exploiter avec Kali Linux L''immortel XSS et comment l''utiliser pour voler des sessions actives Les meilleures habitudes de sécurité pour tout développeur Web Tout est organisé pour vous dans ce livre, tout ce que vous avez à faire maintenant, c''est de cliquer sur le bouton acheter et commencer votre parcours dans le Web App Hacking.

"Explores how industry has manipulated our most deep-seated survival instincts."—David Perlmutter, MD, Author, #1 New York Times bestseller, Grain Brain and Brain Maker The New York Times–bestselling author of Fat Chance reveals the corporate scheme to sell pleasure, driving the international epidemic of addiction, depression, and chronic disease. While researching the toxic and addictive properties of sugar for his New York Times bestseller Fat Chance, Robert Lustig made an alarming discovery—our pursuit of happiness is being subverted by a culture of addiction and depression from which we may never recover. Dopamine is the "reward" neurotransmitter that tells our brains we want more; yet every substance or behavior that releases dopamine in the

extreme leads to addiction. Serotonin is the "contentment" neurotransmitter that tells our brains we don't need any more; yet its deficiency leads to depression. Ideally, both are in optimal supply. Yet dopamine evolved to overwhelm serotonin—because our ancestors were more likely to survive if they were constantly motivated—with the result that constant desire can chemically destroy our ability to feel happiness, while sending us down the slippery slope to addiction. In the last forty years, government legislation and subsidies have promoted ever-available temptation (sugar, drugs, social media, porn) combined with constant stress (work, home, money, Internet), with the end result of an unprecedented epidemic of addiction, anxiety, depression, and chronic disease. And with the advent of neuromarketing, corporate America has successfully imprisoned us in an endless loop of desire and consumption from which there is no obvious escape. With his customary wit and incisiveness, Lustig not only reveals the science that drives these states of mind, he points his finger directly at the corporations that helped create this mess, and the government actors who facilitated it, and he offers solutions we can all use in the pursuit of happiness, even in the face of overwhelming opposition. Always fearless and provocative, Lustig marshals a call to action, with seminal implications for our health, our well-being, and our culture.

Beginning with a basic primer on reverse engineering-including computer internals, operating systems, and assembly language-and then discussing the various applications of reverse engineering, this book provides readers with practical, in-depth techniques for software reverse engineering. The book is broken into two parts, the first deals with security-related reverse engineering and the second explores the more practical aspects of reverse engineering. In addition, the author explains how to reverse engineer a third-party software library to improve interfacing and how to reverse engineer a competitor's software to build a better product. * The first popular book to show how software reverse engineering can help defend against security threats, speed up development, and unlock the secrets of competitive products * Helps developers plug security holes by demonstrating how hackers exploit reverse engineering techniques to crack copy-protection schemes and identify software targets for viruses and other malware * Offers a primer on advanced reverse-engineering, delving into "disassembly"-code-level reverse engineering-and explaining how to decipher assembly language

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

mobile applications on the iOS, Android, Blackberry, and Windows Phone platforms. You will learn a proven methodology for approaching mobile application assessments, and the techniques used to prevent, disrupt, and remediate the various types of attacks. Coverage includes data storage, cryptography, transport layers, data leakage, injection attacks, runtime manipulation, security controls, and cross-platform apps, with vulnerabilities highlighted and detailed information on the methods hackers use to get around standard security. Mobile applications are widely used in the consumer and enterprise markets to process and/or store sensitive data. There is currently little published on the topic of mobile security, but with over a million apps in the Apple App Store alone, the attack surface is significant. This book helps you secure mobile apps by demonstrating the ways in which hackers exploit weak points and flaws to gain access to data. Understand the ways data can be stored, and how cryptography is defeated Set up an environment for identifying insecurities and the data leakages that arise Develop extensions to bypass security controls and perform injection attacks Learn the different attacks that apply specifically to cross-platform apps IT security breaches have made big headlines, with millions of consumers vulnerable as major corporations come under attack. Learning the tricks of the hacker's trade allows security professionals to lock the app up tight. For better mobile security and less vulnerable data, The Mobile Application Hacker's Handbook is a practical, comprehensive guide.

Hacking Leadership

Tactics, Techniques, and Procedures

Exploitation and Countermeasures for Modern Web Applications

A Guide for the Penetration Tester

Reversing

There are some types of complex systems that are built like clockwork, with well-defined parts that interact in well-defined ways, so that the action of the whole can be precisely analyzed and anticipated with accuracy and precision. Some systems are not themselves so well-defined, but they can be modeled in ways that are like trained pilots in well-built planes, or electrolyte balance in healthy humans. But there are many systems for which that is not true; and among them are many whose understanding and control we would value. For example, the model for the trained pilot above fails exactly where the pilot is being most human; that is, where he is exercising the highest levels of judgment, or where he is learning and adapting to new conditions. Again, sometimes the kinds of complexity do not lead to easily analyzable models at all; here we might include most economic systems, in all forms of societies. There are several factors that seem to contribute to systems being hard to model, understand, or control. The human participants may act in ways that are so variable or so rich or so interactive that the only adequate

model of the system would be the entire system itself, so to speak. This is probably the case in true long term systems involving people learning and growing up in a changing society.

It's true that some people spend years studying Italian before they finally get around to speaking the language. But here's a better idea. Skip the years of study and jump right to the speaking part. Sound crazy? No, it's language hacking. Unlike most traditional language courses that try to teach you the rules of Italian, #LanguageHacking shows you how to learn and speak Italian through proven memory techniques, unconventional shortcuts and conversation strategies perfected by one of the world's greatest language learners, Benny Lewis, aka the Irish Polyglot. Using the language hacks -shortcuts that make learning simple - that Benny mastered while learning his 11 languages and his 'speak from the start' method, you will crack the language code and exponentially increase your language abilities so that you can get fluent faster. It's not magic. It's not a language gene. It's not something only "other people" can do. It's about being smart with how you learn, learning what's indispensable, skipping what's not, and using what you've learned to have real conversations in Italian from day one. The Method #LanguageHacking takes a modern approach to language learning, blending the power of online social collaboration with traditional methods. It focuses on the conversations that learners need to master right away, rather than presenting language in order of difficulty like most courses. This means that you can have conversations immediately, not after years of study. Each of the 10 units culminates with a speaking 'mission' that prepares you to use the language you've learned to talk about yourself. Through the language hacker online learner community, you can share your personalized speaking 'missions' with other learners - getting and giving feedback and extending your learning beyond the pages of the book . You don't need to go abroad to learn a language any more.

Written by all-star security experts, Practical IoT Hacking is a quick-start conceptual guide to testing and exploiting IoT systems and devices. Drawing from the real-life exploits of five highly regarded IoT security researchers, Practical IoT Hacking teaches you how to test IoT systems, devices, and protocols to mitigate risk. The book begins by walking you through common threats and a threat modeling framework. You'll develop a security testing methodology, discover the art of passive reconnaissance, and assess security on all layers of an IoT system. Next, you'll perform VLAN hopping, crack MQTT authentication, abuse UPnP, develop an mDNS poisoner, and craft WS-Discovery attacks. You'll tackle both hardware hacking and radio hacking, with in-depth coverage of attacks against embedded IoT devices and RFID systems. You'll also learn how to: • Write a DICOM service scanner as an NSE module • Hack a microcontroller through the UART and SWD interfaces • Reverse engineer firmware and analyze mobile companion apps • Develop an NFC fuzzer using Proxmark3 • Hack a smart home by jamming wireless alarms, playing back IP camera feeds, and controlling a smart treadmill The tools and devices you'll use are affordable and readily available, so you can easily practice what you learn. Whether you're a security researcher, IT team member, or hacking hobbyist, you'll find Practical IoT Hacking indispensable in your efforts to hack all the things REQUIREMENTS: Basic knowledge of Linux command line, TCP/IP, and

programming

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.

Hacking- The art Of Exploitation

The 11 Gaps Every Business Needs to Close and the Secrets to Closing Them Quickly

The Web Application Hacker's Handbook

Android Hacker's Handbook

Texture in the Work of Ian Hacking

Hacker Debugging Uncovered

Compiles programming hacks intended to help computer programmers build more efficient software, in an updated edition that covers cyclic redundancy checking and new algorithms and that includes exercises with answers.

This book offers a systematized overview of Ian Hacking's work. It presents Hacking's oeuvre as a network made up of four interconnected key nodes: styles of scientific thinking & doing, probability, making up people, and experimentation and scientific realism. Its central claim is that Michel Foucault's influence is the underlying thread that runs across the Canadian philosopher's oeuvre. Foucault's imprint on Hacking's work is usually mentioned in relation to styles of scientific reasoning and the human sciences. This research shows that Foucault's influence can in fact be extended beyond these fields, insofar the underlying interest to the whole corpus of Hacking's works, namely the analysis of conditions of possibility, is stimulated by the work of the French philosopher. Displacing scientific realism as the central focus of Ian Hacking's oeuvre opens up a very different landscape, showing, behind the apparent dispersion of his works, the far-reaching interest that amalgamates them: to reveal the historical and situated conditions of possibility for the emergence of scientific objects and concepts. This book shows how Hacking's deployment concepts such as looping effect, making up people, and interactive kinds, can complement Foucauldian analyses, offering an overarching perspective that can provide a better explanation of the objects of the human sciences and their behaviors.

Take a practioner's approach in analyzing the Internet of Things (IoT) devices and the security issues facing an IoT architecture. You'll review the architecture's central components, from hardware communication interfaces, such as UARTand SPI, to radio protocols, such as BLE or ZigBee. You'll also learn to assess a device physically by opening it, looking at the PCB, and identifying the chipsets and interfaces. You'll then use that information to gain entry to the device or to perform other actions, such as dumping encryption keys and firmware. As the IoT rises

to one of the most popular tech trends, manufactures need to take necessary steps to secure devices and protect them from attackers. The IoT Hacker's Handbook breaks down the Internet of Things, exploits it, and reveals how these devices can be built securely. What You'll LearnPerform a threat model of a real-world IoT device and locate all possible attacker entry points Use reverse engineering of firmware binaries to identify security issues Analyze,assess, and identify security issues in exploited ARM and MIPS based binariesSniff, capture, and exploit radio communication protocols, such as Bluetooth Low Energy (BLE), and ZigBee Who This Book is For Those interested in learning about IoT security, such as pentesters working in different domains, embedded device developers, or IT people wanting to move to an Internet of Things security role.

Hack your antivirus software to stamp out future vulnerabilities The Antivirus Hacker's Handbook guides you through the process of reverse engineering antivirus software. You explore how to detect and exploit vulnerabilities that can be leveraged to improve future software design, protect your network, and anticipate attacks that may sneak through your antivirus' line of defense. You'll begin building your knowledge by diving into the reverse engineering process, which details how to start from a finished antivirus software program and work your way back through its development using the functions and other key elements of the software. Next, you leverage your new knowledge about software development to evade, attack, and exploit antivirus software—all of which can help you strengthen your network and protect your data. While not all viruses are damaging, understanding how to better protect your computer against them can help you maintain the integrity of your network. Discover how to reverse engineer your antivirus software Explore methods of antivirus software evasion Consider different ways to attack and exploit antivirus software Understand the current state of the antivirus software market, and get recommendations for users and vendors who are leveraging this software The Antivirus Hacker's Handbook is the essential reference for software reverse engineers, penetration testers, security researchers, exploit writers, antivirus vendors, and software engineers who want to understand how to leverage current antivirus software to improve future applications.

Ethical Hacking and Countermeasures: Web Applications and Data Servers

Hacker's Delight

Le Guide Ultime du débutant Pour Apprendre les Bases du WEB Hacking Avec Kali Linux et Comment Protéger Ses Applications des Hackers

The Antivirus Hacker's Handbook

CUCKOO'S EGG

The Car Hacker's Handbook

Complex and controversial, hackers possess a wily, fascinating talent, the machinations of which are shrouded in secrecy. Providing in-depth exploration into this largely uncharted territory, Profiling Hackers: The Science of Criminal Profiling as Applied to the World of Hacking offers insight into the

hacking realm by telling attention-grabbing ta
A field manual on contextualizing cyber threats, vulnerabilities, and risks to connected cars through penetration testing and risk assessment Hacking Connected Cars deconstructs the tactics, techniques, and procedures (TTPs) used to hack into connected cars and autonomous vehicles to help you identify and mitigate vulnerabilities affecting cyber-physical vehicles. Written by a veteran of risk management and penetration testing of IoT devices and connected cars, this book provides a detailed account of how to perform penetration testing, threat modeling, and risk assessments of telematics control units and infotainment systems. This book demonstrates how vulnerabilities in wireless networking, Bluetooth, and GSM can be exploited to affect confidentiality, integrity, and availability of connected cars. Passenger vehicles have experienced a massive increase in connectivity over the past five years, and the trend will only continue to grow with the expansion of The Internet of Things and increasing consumer demand for always-on connectivity. Manufacturers and OEMs need the ability to push updates without requiring service visits, but this leaves the vehicle's systems open to attack. This book examines the issues in depth, providing cutting-edge preventative tactics that security practitioners, researchers, and vendors can use to keep connected cars safe without sacrificing connectivity. Perform penetration testing of infotainment systems and telematics control units through a step-by-step methodical guide Analyze risk levels surrounding vulnerabilities and threats that impact confidentiality, integrity, and availability Conduct penetration testing using the same tactics, techniques, and procedures used by hackers From relatively small features such as automatic parallel parking, to completely autonomous self-driving cars—all connected systems are vulnerable to attack. As connectivity becomes a way of life, the need for security expertise for in-vehicle systems is becoming increasingly urgent. Hacking Connected Cars provides practical, comprehensive guidance for keeping these vehicles secure.
Covers everything from illegal aspects to understandable explanations of telecomputing for every modem user. . . .a reference book on many communications subjects.--Computer Shopper. Sold over 40,000 copies in England. Revised U.S. version proven with direct mail success.
This is the eBook version of the print title. Note that the eBook does not provide access to the practice test software that accompanies the print book. Learn, prepare, and practice for CEH v8 exam success with this cert guide from Pearson IT Certification, a leader in IT certification learning. Master CEH

exam topics Assess your knowledge with chapter-ending quizzes Review key concepts with exam preparation tasks Certified Ethical Hacker (CEH) Cert Guide is a best-of-breed exam study guide. Leading security consultant and certification expert Michael Gregg shares preparation hints and test-taking tips, helping you identify areas of weakness and improve both your conceptual knowledge and hands-on skills. Material is presented in a concise manner, focusing on increasing your understanding and retention of exam topics. You'll get a complete test preparation routine organized around proven series elements and techniques. Exam topic lists make referencing easy. Chapter-ending Exam Preparation Tasks help you drill on key concepts you must know thoroughly. Review questions help you assess your knowledge, and a final preparation chapter guides you through tools and resources to help you craft your final study plan. This EC-Council authorized study guide helps you master all the topics on the CEH v8 (312-50) exam, including: Ethical hacking basics Technical foundations of hacking Footprinting and scanning Enumeration and system hacking Linux and automated assessment tools Trojans and backdoors Sniffers, session hijacking, and denial of service Web server hacking, web applications, and database attacks Wireless technologies, mobile security, and mobile attacks IDS, firewalls, and honeypots Buffer overflows, viruses, and worms Cryptographic attacks and defenses Physical security and social engineering

Alice and Bob Learn Application Security

A Field Guide to Web Hacking

Cyber Crime: Concepts, Methodologies, Tools and Applications

Michel Foucault as the Guiding Thread of Hacking's Thinking

The Science Behind the Corporate Takeover of Our Bodies and Brains

Adaptive Control of Ill-Defined Systems

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.

Learn application security from the very start, with this comprehensive and approachable guide! Alice and Bob Learn Application Security is an accessible and thorough resource for anyone seeking to incorporate, from the beginning of the System Development Life Cycle, best security practices in software development. This book covers all the basic subjects such as threat modeling and security testing, but also dives deep into more complex and advanced topics for securing modern software systems and architectures. Throughout, the book offers analogies, stories of the characters Alice and Bob, real-life examples, technical explanations and diagrams to ensure maximum clarity of the many abstract and complicated subjects. Topics include: Secure requirements, design, coding, and deployment Security Testing (all forms) Common Pitfalls Application Security Programs Securing Modern Applications

Software Developer Security Hygiene Alice and Bob Learn Application Security is perfect for aspiring application security engineers and practicing software developers, as well as software project managers, penetration testers, and chief information security officers who seek to build or improve their application security programs. Alice and Bob Learn Application Security illustrates all the included concepts with easy-to-understand examples and concrete practical applications, furthering the reader ' s ability to grasp and retain the foundational and advanced topics contained within.

Modern cars are more computerized than ever. Infotainment and navigation systems, Wi-Fi, automatic software updates, and other innovations aim to make driving more convenient. But vehicle technologies haven ' t kept pace with today ' s more hostile security environment, leaving millions vulnerable to attack. The Car Hacker ' s Handbook will give you a deeper understanding of the computer systems and embedded software in modern vehicles. It begins by examining vulnerabilities and providing detailed explanations of communications over the CAN bus and between devices and systems. Then, once you have an understanding of a vehicle ' s communication network, you ' ll learn how to intercept data and perform specific hacks to track vehicles, unlock doors, glitch engines, flood communication, and more. With a focus on low-cost, open source hacking tools such as Metasploit, Wireshark, Kayak, can-utils, and ChipWhisperer, The Car Hacker ' s Handbook will show you how to: –Build an accurate threat model for your vehicle –Reverse engineer the CAN bus to fake engine signals –Exploit vulnerabilities in diagnostic and data-logging systems –Hack the ECU and other firmware and embedded systems –Feed exploits through infotainment and vehicle-to-vehicle communication systems –Override factory settings with performance-tuning techniques –Build physical and virtual test benches to try out exploits safely If you ' re curious about automotive security and have the urge to hack a two-ton computer, make The Car Hacker ' s Handbook your first stop.

The Many Faces of Anonymous
Certified Ethical Hacker (CEH) Cert Guide
Web Application Security
Secrets of Reverse Engineering
The IoT Hacker's Handbook