The Le Application Hackers Handbook

The book introduces the principles of hardware design and describes the tools and techniques required to begin hacking. The DVD contains hack instructions for over 20 game consoles and hardware devices from Nintendo, Apple, Sony, Microsoft, Palm and more. The presentation of these 20 projects on DVD media provides users with benefits and options not available on the printed page. All images are hi-res color that can be enlarged or printed, the text is easily searched, and the user can copy the contents to their hard disk and add comments directly into the PDF files. The DVD media also lends itself well to group projects (it includes a 10 user license). The 160-page book includes chapters on hacking tools and electrical engineering basics, along with chapters on the background, design and functionality of each hardware device. * Packed full of high resolution colour images that reveal the smallest details of each step in a hack * Includes in depth coverage of the tools of the hacking trade and the basics of electrical engineering * DVD includes a "Using the Tools" video starring Joe "kingpin" Grand

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

Eliminating security holes in iOS apps is critical for any developer who wants to protect their users from the bad guys. In iOS Application Security, mobile security expert David Thiel reveals common iOS coding mistakes that create serious security problems and shows you how to find and fix them. After a crash course on iOS application structure and Objective-C design patterns, you'll move on to spotting bad code and plugging the holes. You'll learn about: –The iOS security model and the limits of its built-in protections –The myriad ways sensitive data can leak into places it shouldn't, such as through the pasteboard –How to implement encryption with the Keychain, the Data Protection API, and CommonCrypto –Legacy flaws from C that still cause problems in modern iOS applications –Privacy issues related to gathering user data and how to mitigate potential pitfalls Don't let your app's security leak become another headline. Whether you're looking to bolster your app's defenses or hunting bugs in other people's code, iOS Application Security will help you get the job done well.

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.

CEH can be said as a certified ethical hacker. This certification is a professional certificate and it is awarded by the EC council (international council of E-commerce consultant). An ethical hacker is a name that is given to penetration testing/ tester. An ethical hacker is employed by the organization with full trust with the employer (ethical hacker) for attempting the penetrating the computer system in order to find and fix all the computer security vulnerabilities. Computer security vulnerabilities also include illegal hacking (gaining authorization to some other computer systems). These activities are criminal activities in almost all countries. Doing a penetrating test in a particular system with the permission of the owner is done and also possible except in Germany. This certification validates the knowledge and skills that are required on how to look for the vulnerabilities as well as weaknesses in a particular computer.

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

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.

Sponsored by the Communication, Information Technologies, and Media Sociology section of the American Sociological Association (CITAMS), this volume celebrates the section's thirtieth anniversary. It looks at the history of the section, reviews some of its most important themes, and sets the agenda for future discussion.

Créez votre propre laboratoire de hacking ! Vous souhaitez, comme les hackers, apprendre à pénétrer les réseaux et les systèmes informatiques ? Les bases du hacking est une introduction aux techniques de hacking et aux tests d'intrusion. Grâce à des explications claires et à une approche originale, apprenez à utiliser tous les outils des professionnels de la sécurité et des hackers éthiques. Maîtrisez les quatre phases du test d'intrusion et du hacking : reconnaissance, scan, exploitation, post-exploitation. Informez-vous sur votre cible, trouvez ses vulnérabilités, exploitez-les pour attaquer, puis maintenez les accès ! Vous n'aurez besoin d'aucune expérience préalable pour comprendre et suivre les différentes étapes présentées dans cet ouvrage. En menant de véritables attaques et tests d'intrusion contre des machines virtuelles, vous saurez repérer les faiblesses des systèmes, et apprendrez toutes les techniques de la sécurité offensive. Pas-à-pas, grâce des exercices pratiques et simples, l'auteur vous enseignera les principes et les

techniques de hacking, depuis l’ingénierie sociale jusqu’aux rootkits, en passant par l’utilisation de tous les outils modernes (Kali, BackTrack Linux, MetaGooFil, Nmap, Nessus, Metasploit, w3af, Netcat et bien d’autres !).

WILEY-INTERSCIENCE PAPERBACK SERIES The Wiley-Interscience Paperback Series consists of selected books that have been made more accessible to consumers in an effort to increase global appeal and general circulation. With these new unabridged softcover volumes, Wiley hopes to extend the lives of these works by making them available to future generations of statisticians, mathematicians, and scientists. From the Reviews of History of Probability and Statistics and Their Applications before 1750 "This is a marvelous book . . . Anyone with the slightest interest in the history of statistics, or in understanding how modern ideas have developed, will find this an invaluable resource." –Short Book Reviews of ISI

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.

The book presents a remarkable collection of chapters covering a wide range of topics in the areas of intelligent systems and artificial intelligence, and their real-world applications. It gathers the proceedings of the Intelligent Systems Conference 2019, which attracted a total of 546 submissions from pioneering researchers, scientists, industrial engineers, and students from all around the world. These submissions underwent a double-blind peer-review process, after which 190 were selected for inclusion in these proceedings. As intelligent systems continue to replace and sometimes outperform human intelligence in decision-making processes, they have made it possible to tackle a host of problems more effectively. This branching out of computational intelligence in several directions and use of intelligent systems in everyday applications have created the need for an international conference as a venue for reporting on the latest innovations and trends. This book collects both theory and application based chapters on virtually all aspects of artificial intelligence; presenting state-of-the-art intelligent methods and techniques for solving real-world problems, along with a vision for future research, it represents a unique and valuable asset.

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.

As we enter the Industrial Revolution 4.0, demands for an increasing degree of trust and privacy protection continue to be voiced. The development of blockchain technology is very important because it can help frictionless and transparent financial transactions and improve the business experience, which in turn has far-reaching effects for economic, psychological, educational and organizational improvements in the way we work, teach, learn and care for ourselves and each other. Blockchain is an eccentric technology, but at the same time, the least understood and most disruptive technology of the day. This book covers the latest technologies of cryptocurrencies and blockchain technology and their applications. This book discusses the blockchain and cryptocurrencies related issues and also explains how to provide the security differently through an algorithm, framework, approaches, techniques and mechanisms. A comprehensive understanding of what blockchain is and how it works, as well as insights into how it will affect the future of your organization and industry as a whole and how to integrate blockchain technology into your business strategy. In addition, the book explores the blockchain and its with other technologies like Internet of Things, big data and artificial intelligence, etc.

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.

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.

Going beyond the issues of analyzing and optimizing programs as well as creating the means of protecting information, this guide takes on the programming problem of, once having found holes in a program, how to go about disassembling it without its source code. Covered are the hacking methods used to analyze programs using a debugger and disassembler. These methods include virtual functions, local and global variables, branching, loops, objects and their hierarchy, and mathematical operators. Also covered are methods of fighting disassemblers, self-modifying code in operating systems, and executing code in the stack. Advanced disassembler topics such as optimizing compilers and movable code are discussed as well.

Question : est-ce que ça vous intéresse d'apprendre le hacking des applications web, recevoir une formation vidéo gratuite et faire partie d'un groupe de hackers en investissant le minimum de temps et d'argent ? Alors lisez ce qui suit : Quand j'ai commencé avec tout ces trucs de hacking (il y a des années de cela.), entendre le mot «injection SQL» suffisait pour me dégoûter de tout ce qui en rapport avec le Web, ça me paraissait trop compliqué de comprendre ce type de vulnérabilité et leur exploitation, du coup, je ne faisais qu' éviter tout ce qui était en relation avec le pentesting Web. Peut-être, est ce votre cas aussi, vous n'êtes pas passionné par les failles qui touchent les applications web, ou peut-être que (comme moi) vous n'arrivez juste pas à bien comprendre comment ça fonctionne ! Mais laissez moi vous dire une chose : vous ne pouvez pas prétendre être hacker ou pentester en restant ignorant du Web app hacking, c'est juste impossible ! Ici, je vous propose de fixer le problème. L'erreur que j'ai faite et que font beaucoup de débutants, c'est qu'ils apprennent à utiliser des outils automatisés pour exploiter les failles les plus répandues sur la toile, peut-être que vous connaissez déjà sqlmap ou beef, mais en apprenant ces outils vous ne faites qu'à jouer le script kiddie ! Par contre, ce qu'il vous faut, c'est comprendre la logique des applications que vous êtes en train de tester, si vous voulez vraiment devenir hacker ... C'est votre seule voie. En comprenant le fonctionnement des applications Web, vous pourrez facilement comprendre la logique derrière la découverte et l'exploitation des failles qui les touchent. Quand j'ai suivi ce plan d'action, j'ai pu assimiler les différents concepts du hacking Web, participer à des programmes de chasse de faille et gagner des CTF (des compétitions de hacking). À la fin de la lecture de ce livre : Vous aurez appris à créer un environnement de hacking Web privé. Vous pourrez implémenter rapidement la meilleure méthodologie de pentesting Web. Vous pourrez prendre n'importe quelle application Web et la tester en quelques heures seulement. Vous aurez compris la logique du fonctionnement des applications Web et les failles qui les touches. Vous pourrez détecter les failles les plus dangereuses dans les applications Web. Vous saurez aussi utiliser des outils pour accélérer votre pentesting. Vous apprendrez comment contrôler des serveurs à distance et faire des exploitations avancées. Vous saurez manipuler les utilisateurs d'un réseau pour obtenir les informations que vous voulez. Ce qui fait que ce livre est différent des autres : Une formation vidéo gratuite qui accompagne le livre. Un accès à un groupe Facebook privé et faire partie d'une communauté de hackers engagés et motivés. ? 100% satisfait ou remboursé ! Si vous n'êtes pas satisfait du livre, vous pouvez le renvoyer dans les 7 jours et obtenir le remboursement intégral. Votre risque est nul. Vous pouvez conserver les

bonus ! Que vous soyez développeur, un administrateur système, ou un passionné de hacking, ce livre vous donnera les compétences nécessaires pour vous différencier de votre entourage et vous mettre au-dessus de la concurrence. À vous de reprendre le contrôle.

Are you worried about external hackers and rogue insiders breaking into your systems? Whether it’s social engineering, network infrastructure attacks, or application hacking, security breaches in your systems can devastate your business or personal life. In order to counter these cyber bad guys, you must become a hacker yourself—an ethical hacker. Hacking for Dummies shows you just how vulnerable your systems are to attackers. It shows you how to find your weak spots and perform penetration and other security tests. With the information found in this handy, straightforward book, you will be able to develop a plan to keep your information safe and sound. You’ll discover how to: Work ethically, respect privacy, and save your system from crashing Develop a hacking plan Treat social engineers and preserve their honesty Counter war dialing and scan infrastructures Understand the vulnerabilities of Windows, Linux, and Novell NetWare Prevent breaches in messaging systems, web applications, and databases Report your results and managing security changes Avoid deadly mistakes Get management involved with defending your systems As we enter into the digital era, protecting your systems and your company has never been more important. Don’t let skepticism delay your decisions and put your security at risk. With Hacking For Dummies, you can strengthen your defenses and prevent attacks from every angle!

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.

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.

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.

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.

Why study programming? Ethical gray hat hackers should study programming and learn as much about the subject as possible in order to find vulnerabilities in programs and get them fixed before unethical hackers take advantage of them. It is very much a foot race: if the vulnerability exists, who will find it first? The purpose of this chapter is to give you the survival skills necessary to understand upcoming chapters and later find the holes in software before the black hats do. In this chapter, we cover the following topics: • C programming language • Computer memory • Intel processors • Assembly language basics • Debugging with gdb • Python survival skills

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

The world as it exists today is barely recognizable as the same world that existed on hundred, or even fifty, years ago. The last century has seen innovation after innovation reshape and revolutionize almost every aspect of human existence. Far from bringing us to an end point - a settled state in which no further innovation is possible - the rate of change has increased exponentially in recent decades. It seems that we a set firmly on a path of endless enhancement. This leads us to ask: where does innovation come from, and how does it happen? The answer, quite simply, is people. People have ideas. People strive to make their ideas a reality. Through this, people create change. We call these people hackers. A hack is a small change to

the recognized way of doing things, which leads to a large-scale increase in efficiency, success, or achievement. Hackers break the rules and change the game. Hackers are the most important members of our society, of any society, as they hold the power to shape the future. This book celebrates the lives and achievements of some of history's greatest hackers: from Tim Berners-Lee to Jack Dorsey, from Leonardo da Vinci to Steve Jobs. Learn about who they were and how they functioned. Discover the characteristics that allow hackers to keep pushing forward, innovating, revolutionizing industries and changing the world.

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.

Asterisk Hacking provides detials of techniques people may not be aware of. It teaches the secrets the bad guys already know about stealing personal information through the most common, seemingly innocuous, highway into computer networks: the phone system. This book provides detials to readers what they can do to protect themselves, their families, their clients, and their network from this invisible threat. Power tips show how to make the most out of the phone system for defense or attack. Contains original code to perform previously unthought of tasks like changing caller id, narrowing a phone number down to a specific geographic location, and more! See through the eyes of the attacker and learn WHY they are motivated, something not touched upon in most other titles.

The Mobile Application Hacker's HandbookJohn Wiley & Sons

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.

Describes the security architecture of iOS and offers information on such topics as encryption, jailbreaks, code signing, sandboxing, iPhone fuzzing, and ROP payloads, along with ways to defend iOS devices.

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.

The stories about phishing attacks against banks are so true-to-life, it’s chilling.” --Joel Dubin, CISSP, Microsoft MVP in Security Every day, hackers are devising new ways to break into your network. Do you have what it takes to stop them? Find out in Hacker’s Challenge 3. Inside, top-tier security experts offer 20 brand-new, real-world network security incidents to test your computer forensics and response skills. All the latest hot-button topics are covered, including phishing and pharming scams, internal corporate hacking, Cisco IOS, wireless, iSCSI storage, VoIP, Windows, Mac OS X, and UNIX/Linux hacks, and much more. Each challenge includes a detailed explanation of the incident--how the break-in was detected, evidence and clues, technical background such as log files and network maps, and a series of questions for you to solve. In Part II, you’ll get a detailed analysis of how the experts solved each incident. Exerpt from “Big Bait, Big Phish”: The Challenge: “Could you find out what’s going on with the gobi web server? Customer order e-mails aren’t being sent out, and the thing’s chugging under a big load...” Rob e-mailed the development team reminding them not to send marketing e-mails from the gobi web server.... “Customer service is worried about some issue with tons of disputed false orders....” Rob noticed a suspicious pattern with the “false” orders: they were all being delivered to the same P.O.

box...He decided to investigate the access logs. An external JavaScript file being referenced seemed especially strange, so he tested to see if he could access it himself.... The attacker was manipulating the link parameter of the login.pl application. Rob needed to see the server side script that generated the login.pl page to determine the purpose.... The Solution: After reviewing the log files included in the challenge, propose your assessment: What is the significance of the attacker’s JavaScript file? What was an early clue that Rob missed that might have alerted him to something being amiss? What are some different ways the attacker could have delivered the payload? Who is this attack ultimately targeted against? Then, turn to the experts' answers to find out what really happened.

Ian Mann's Hacking the Human highlights the main sources of risk from social engineering and draws on psychological models to explain the basis for human vulnerabilities. Offering more than a simple checklist to follow, the book provides a rich mix of examples, applied research and practical solutions for security and IT professionals that enable you to create and develop a security solution that is most appropriate for your organization.

Copyright: 17e8a0762a2c9c3e243416fb19786bc0