practical toolkit that teams and companies in all industries can use to increase their customer base and market share, this book walks readers through the process of creating and executing their own custom-made growth hacking strategy. It is a must-read for any marketer, entrepreneur, innovator or manager looking to replace wasteful big bets and “spaghetti-on-the-wall” approaches with more consistent, replicable, cost-effective, and data-driven results.

Ethical Hacking

Ezrah Edwin 2020-04-14 This book is for those of you looking to add more skills to your arsenal. It teaches on all topics that an ethical hacker should know about and how to implement the skills of a professional hacker. The book will provide a brief history of ethical hacking. You will learn what ethical hacking means and how this term is different from general hacking. Hacking topics include physical threats as well as the non-physical threats in an organization that all skilled ethical hackers must understand. You’ll be provided with the rules of ethical hacking that you must memorize in order to properly implement. An ethical hacker is nothing without tools; therefore, there is a compiled list of some of the most prominent tools that will help you manage your hacking plans. Some of the tools include Wireshark, Burp Suite, and Metasploit. Also included are tricks on how to use Python to hack passwords. As an ethical hacker, you’ll learn how to beat the black hat hacker at his own game! Learn to recognize and counter social engineering attacks, trojan horses, malware, and more. In this book, you will discover many unexpected computer vulnerabilities as we categorize the systems in terms of vulnerability. You may be surprised to learn that simple apps under an office door can put your organization at risk for being hacked! In addition, you will learn in step-by-step detail how you can hack into a Windows operating system. Don’t worry— you don’t have to be an expert to be an ethical hacker. You just need an excellent guide, like this one. Click the Buy Now button to get started protecting yourself and your organization from unethical hackers.

The Art of Deception

Kevin D. Mitnick 2011-08-04 The world’s most infamous hacker offers an insider’s view of the low-tech threats to high-tech security. Kevin Mitnick’s exploits as a cyber-snooper and fugitive form one of the most exhaustive FBI manhunts in history and have spawned dozens of articles, books, films, and documentaries. Since his release from federal prison, in 1998, Mitnick has turned his life around and established himself as one of the most sought-after computer security experts worldwide. Now, in The Art of Deception, the world’s most notorious hacker gives new meaning to the old adage, “It takes a thief to catch a thief.” Focusing on the human factors involved with information security, Mitnick explains why all the firewalls and encryption protocols in the world will never be enough to stop a savvy grifter intent on rifling a corporate database or an irate employee determined to crash a system. With the help of many fascinating true stories of successful attacks on business and government, he illustrates just how susceptible even the most locked-down information systems are to a slick con artist impersonating an IRS agent. Narrating from the points of view of both the attacker and the victims, he explains why each attack was so successful and how it could have been prevented in an engaging and highly readable style reminiscent of a true-crime novel. And, perhaps most importantly, Mitnick offers advice for preventing these types of social engineering hacks through security protocols, training programs, and manuals that address the human element of security. Hacking for Penetration Testers

Johnny Long 2011-04-18 This book helps people find sensitive information on the Web. Google is one of the most popular sites on the internet with more than 380 million unique users per month (NielsenNetRatings 8/05). But, Google’s search capabilities are so powerful, they sometimes discover content that no one ever intended to be publicly available on the Web including: social security numbers, credit card numbers, trade secrets, and federally classified documents. Google Hacking for Penetration Testers Volume 2 shows the art of manipulating Google used by security professionals and system administrators to find this sensitive information and ‘self-police’ their own organizations. Readers will learn how to use Google Maps and Google Earth provide pinpoint military accuracy, see how bad guys can manipulate Google to create super worms, and see how they can ‘mash up’ Google with MySpace, LinkedIn, and more for passive reconnaissance. • Learn Google Searching Basics Explore Google’s Web-based interface, build Google queries, and work with Google URL’s. • Use Advanced Operators to Perform Advanced Queries Combine advanced operators and learn about colliding operators and bad searches. • Use the Ways of the Hacker Google See how to use caches for anonymity and review directory listings and traversal techniques. • Review Document Grading and Database Digging See the ways you can use Google to locate documents and then search within the documents to locate information. • Understand Google’s API in an Information Collection Framework Learns the principles of automating searches and the applications of data mining. • Locate Exploits and Finding Targets Locate exploit code and then vulnerable targets. • See Ten Simple Security Searches Learn a few searches that give good results just about every time and are good for a security assessment. • Track Down Web Servers Locate and profile web servers. login portals, network hardwar and utilities. • See How Bad Guys Troll for Data Find ways to search for usernames, passwords, credit card numbers, social security numbers, and other junk information. • Hack Google Services Learn more about the AJAX Search API, Calendar, Blogger, Blog Search, and more.

The Principles of Cybersecurity and Hacking

Zach Weibber 2012-12-09 Protecting yourself and your data from online attacks and hacking has never been more important than it is right now, especially in the digital age. And you know what they always say, knowledge is power. The Principles of Cybersecurity and Hacking series aims to provide you exactly with that knowledge, and with that power. This comprehensive, in-depth guide on the fundamentals, concepts and strategies of Cybersecurity and Hacking will take you to another level of protection in this digital world. It provides you with everything you need to know from starting from Beginner to Advanced through these 5 books: A Beginner’s Guide to Cybersecurity An Intermediate Guide to Cybersecurity An Advanced Guide to Cybersecurity A Beginner’s Guide to learn and Understand Hacking An Intermediate Guide to the Concepts of Hacking. In each book, you will learn and understand topics such as: Types of Cybersecurity Securing Mobile Devices Establishing a Risk Management Framework Social Engineering White Hat Hacking vs Black Hat Hacking And there’s so much more to learn, which you will all find in this book Hacking is real, and what better way to protect yourself than being pro-active and arming yourself with the knowledge on how it works and what you can do against it, so Get your copy now.

Effective Java

Joshua Bloch 2008-05-08 Are you looking for a deeper understanding of the Java 5 programming language so that you can write code that is clearer, more correct, more robust, and more reusable? Look no further! Effective Java™, Second Edition, brings together seventy-eight indispensable programmer’s rules of thumb: working, best-practices solutions for the programming challenges you encounter every day. This highly anticipated new edition of the classic, Java Award-winning work has been thoroughly updated to cover Java SE 5 and Java SE 6 features introduced since the first edition. Bloch explores new design patterns and language idioms, showing you how to make the most of features ranging from generics to enum annotations to autoboxing. Each chapter in the book consists of several “items” presented in the form of a short, standalone essay that provides specific advice, insight into Java platform subtleties, and outstanding code examples. The comprehensive descriptions and explanations for each item illuminate what to do, what not to do, and why. Highlights include: New coverage of generics, enums, annotations, and autoboxing for each Java release, enum value coercions and autoboxing utilities, and much more. Improved techniques for creating objects, including lazy initialization, factory classes, libraries, methods, and serialization. How to avoid the traps and pitfalls of commonly misunderstood subtleties of the language Focus on the language and its most fundamental libraries: java.lang, java.util, and, to a lesser extent, java.io and java.concurrent and java.util.concurrent. Simply put, Effective Java™, Second Edition, presents the most practical, authoritative guidelines available for writing efficient, well-designed programs.

Dark Territory


Hack Proofing Your Web Applications

Syngress 2001-06-18 From the authors of the bestselling Hack Proofing Your Network©: OPEC, Amazon, Yahoo! and Ebay! If these large, well-established and security-conscious web sites have problems, how can anyone be safe? How can any programmer expect to develop web applications that are secure? Hack Proofing Your Web Applications is the only book specifically written for application developers and webmasters who write programs that are used on web sites. It covers Java applications, XML, ColdFusion, and other database applications. Most hacking books focus on catching the hackers once they’re entered the site; this one shows programers how to design tight code that will deter hackers from the words go. Comes with up-to-the-minute web based support and a CD-ROM containing source codes and sample testing programs Unique approach: Unlike most hacking books this one is written for the application developer to help them build less vulnerable programs.

Hacking with Kali

James Mood 2011-12-05 Hacking with Kali introduces you the most current distribution of the de facto standard tool for Linux pen testing. Starting with use of the Kali live CD and progressing through installation on hard drives, thumb drives and SD cards, author James Mood walks you through creating a custom version of the Kali live distribution. You'll learn how to configure networking components, storage devices and system services such as Samba and web services. Once you're familiar with the basic components of the software, you'll learn how to use Kali through the phases of the penetration testing lifecycle: one major tool from each phase is explained. The book culminates with a chapter on reporting that will provide examples of documents used prior to, during and after the pen test. This guide will benefit information security professionals at all levels, hackers, systems administrators, network administrators, and beginning and intermediate professional pen testers, as well as students majoring in information security. Provides detailed explanations of the complete penetration testing lifecycle Complete links of the Kali information, resources and distribution downloads Hands-on exercises reinforce topics.