

Business Analyst Resume Hacking Shortcuts To Outshining Your Peers And Getting Interviews Business Administration Book 1

Hacker extraordinaire Kevin Mitnick delivers the explosive encore to his bestselling *The Art of Deception*. Kevin Mitnick, the world's most celebrated hacker, now devotes his life to helping businesses and governments combat data thieves, cybervandals, and other malicious computer intruders. In his bestselling *The Art of Deception*, Mitnick presented fictionalized case studies that illustrated how savvy computer crackers use "social engineering" to compromise even the most technically secure computer systems. Now, in his new book, Mitnick goes one step further, offering hair-raising stories of real-life computer break-ins and showing how the victims could have prevented them. Mitnick's reputation within the hacker community gave him unique credibility with the perpetrators of these crimes, who freely shared their stories with him—and whose exploits Mitnick now reveals in detail for the first time, including: A group of friends who won nearly a million dollars in Las Vegas by reverse-engineering slot machines Two teenagers who were persuaded by terrorists to hack into the Lockheed Martin computer systems Two convicts who joined forces to become hackers inside a Texas prison A "Robin Hood" hacker who penetrated the computer systems of many prominent companies—and then told them how he gained access With riveting "you are there" descriptions of real computer break-ins, indispensable tips on countermeasures security professionals need to implement now, and Mitnick's own aerobic commentary on the crimes he describes, this book is sure to reach a wide audience—and attract the attention of both law enforcement agencies and the media.

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

Get complete instructions for manipulating, processing, cleaning, and crunching datasets in Python. Updated for Python 3.6, the second edition of this hands-on guide is packed with practical case studies that show you how to solve a broad set of data analysis problems effectively. You'll learn the latest versions of pandas, NumPy, IPython, and Jupyter in the process. Written by Wes McKinney, the creator of the Python pandas project, this book is a practical, modern introduction to data science tools in Python. It's ideal for analysts new to Python and for Python programmers new to data science and scientific computing. Data files and related material are available on GitHub. Use the IPython shell and Jupyter notebook for exploratory computing. Learn basic and advanced features in NumPy (Numerical Python). Get started with data analysis tools in the pandas library. Use flexible tools to load, clean, transform, merge, and reshape data. Create informative visualizations with matplotlib. Apply the pandas groupby facility to slice, dice, and summarize datasets. Analyze and manipulate regular and irregular time series data. Learn how to solve real-world data analysis problems with thorough, detailed examples.

The contents in this book will provide practical hands on implementation and demonstration guide on how you can use Kali Linux to deploy various attacks on both wired and wireless networks. If you are truly interested in becoming an Ethical Hacker or Penetration Tester, this book is for you. NOTE: If you attempt to use any of this tools on a wired or wireless network without being authorized and you disturb or damage any systems, that would be considered illegal hack and working. Therefore, I would like to encourage all readers to implement any tool described in this book for WHITE HAT USE ONLY!BUY THIS BOOK NOW AND GET STARTED TODAY!This book will cover:-How to Install Virtual Box & Kali Linux-Pen Testing @ Stage 1, Stage 2 and Stage 3-What Penetration Testing Standards exist-How to scan for open ports, host and network devices-Burp Suite Proxy setup and Spidering hosts-How to deploy SQL Injection with SQLmap-How to implement Dictionary Attack with Aircump-ng-How to deploy ARP Poisoning with EtterCAP-How to capture Traffic with Port Mirroring & with Xplico-How to deploy Passive Reconnaissance-How to implement MITM Attack with Ettercap & SSLstrip-How to Manipulate Packets with Scapy-How to deploy Deauthentication Attack-How to capture IPv6 Packets with Parasite6-How to deploy Evil Twin Deauthentication Attack with mdk3-How to deploy DoS Attack with MK03-How to implement Brute Force Attack with TCP Hydra-How to deploy Armitage-Hail Mary-The Metasploit Framework-How to use SET aka Social-Engineering Toolkit and more.BUY THIS BOOK NOW AND GET STARTED TODAY!

The Guardian Index

Embrace the Case Interview

Cracking Case Interviews

Android Hacker's Handbook

Growth Hacking

Cool Hacks, Mods, and Customizations for the Sony?PlayStation?Portable

You don't need to be a wizard to transform a game you like into a game you love. Imagine if you could give your favorite PC game a more informative heads-up display or instantly collect all that loot from your latest epic battle. Bring your knowledge of Windows-based development and memory management, and Game Hacking will teach you what you need to become a true game hacker. Learn the basics, like reverse engineering, assembly code analysis, programmatic memory manipulation, and code injection, and hone your new skills with hands-on example code and practice binaries. Level up as you learn how to:-Scan and modify memory with Cheat Engine -Explore program structure and execution flow with OllyDbg -Log processes and pinpoint useful data files with Process Monitor -Manipulate control flow through NOPing, hooking, and more -Locate and dissect common game memory structures You'll even discover the secrets behind common game bots, including:-Extrasensory perception hacks, such as wall-hacks and heads-up displays -Responsive hacks, such as autohealers and combo bots -Bots with artificial intelligence, such as cave walkers and automatic looters Game hacking might seem like black magic, but it doesn't have to be. Once you understand how bots are made, you'll be better positioned to defend against them in your own games. Journey through the inner workings of PC games with Game Hacking, and leave with a deeper understanding of both game design and computer security.

The first comprehensive guide to discovering and preventing attacks on the Android OS As the Android operating system continues to increase its share of the smartphone market, smartphone hacking remains a growing threat. Written by experts who rank among the world's foremost Android security researchers, this book presents vulnerability discovery, analysis, and exploitation tools for the good guys. Following a detailed explanation of how the Android OS works and its overall security architecture, the authors examine how vulnerabilities can be discovered and exploits developed for various system components, preparing you to defend against them. If you are a mobile device administrator, security researcher, Android app developer, or consultant responsible for evaluating Android security, you will find this guide is essential to your toolbox. A crack team of leading Android security researchers explain Android security risks, security design and architecture, rooting, fuzz testing, and vulnerability analysis. Covers Android application building blocks and security as well as debugging and auditing Android apps Prepares mobile device administrators, security researchers, Android app developers, and security consultants to defend Android systems against attack Android Hacker's Handbook is the first comprehensive resource for IT professionals charged with smartphone security.

Explains how and why hackers break into computers, steal information, and deny services to machines' legitimate users, and discusses strategies and tools used by hackers and how to defend against them.

Finally, a resume book created for IT professionals. Whether you're just getting out of school and looking for your first job, or you're an IT veteran with years of experience, this book has everything you need. In How to Write an Amazing IT Resume, you'll learn how to write a resume that makes an impact. You'll discover how to:-Clear the automated screener-Sail past the IT recruiter-Hook the hiring manager...and get that interview! Perfect for:-IT business analysts-Technical analysts-Developers-Web designers-Helpdesk technicians-Administrators-Network architects-Software engineers-IT managers and directors>Your resume is the most important thing you'll ever write.

You only get one shot for that IT dream job, so make it count!

Certified Ethical Hacker Study Guide

A Complete Reference with Custom Security Hacking Toolkit

Strategies and Tips for Going IT Alone

Controlling the Human Element of Security

The Hands-On Guide to Dissecting Malicious Software

Black Hat Go

The Seven Habits of Highly Effective People

"The security of information systems has not improved at a rate consistent with the growth and sophistication of the attacks being made against them. To address this problem, we must improve the underlying strategies and techniques used to create our systems. Specifically, we must build security in from the start, rather than append it as an afterthought. That's the point of Secure Coding in C and C++. In careful detail, this book shows software developers how to build high-quality systems that are less vulnerable to costly and even catastrophic attack. It's a book that every developer should read before the start of any serious project." --Frank Abagnale, author, lecturer, and leading consultant on fraud prevention and secure documents Learn the Root Causes of Software Vulnerabilities and How to Avoid Them Commonly exploited software vulnerabilities are usually caused by avoidable software defects. Having analyzed nearly 18,000 vulnerability reports over the past ten years, the CERT/Coordination Center (CERT/CC) has determined that a relatively small number of root causes account for most of them. This book identifies and explains these causes and shows the steps that can be taken to prevent exploitation. Moreover, this book encourages programmers to adopt security best practices and develop a security mindset that can help protect software from tomorrow's attacks, not just today's. Drawing on the CERT/CC's reports and conclusions, Robert Secord systematically identifies the program errors most likely to lead to security breaches, shows how they can be exploited, reviews the potential consequences, and presents secure alternatives. Coverage includes technical detail on how to improve the overall security of any C/C++ application Thwart buffer overflows and stack-smashing attacks that exploit insecure string manipulation logic Avoid vulnerabilities and security flaws resulting from the incorrect use of dynamic memory management functions Eliminate integer-related problems: integer overflows, sign errors, and truncation errors Correctly use formatted output functions without introducing format-string vulnerabilities Avoid I/O vulnerabilities, including race conditions

Secure Coding in C and C++ presents hundreds of examples of secure code, insecure code, and exploits, implemented for Windows and Linux. If you're responsible for creating secure C or C++ software--or for keeping it safe--no other book offers you this much detailed, expert assistance. Full Coverage of All Exam Objectives for the CEH Exams 312-50 and EC0-350 Thoroughly prepare for the challenging CEH Certified Ethical Hackers exam with this comprehensive study guide. The book provides full coverage of exam topics, real-world examples, and includes a CD with chapter review questions, two full-length practice exams, electronic flashcards, a glossary of key terms, and the entire book in a searchable pdf e-book. What's Inside: Covers ethics and legal issues, footprinting, scanning, enumeration, system hacking, trojans and backdoors, sniffers, denial of service, social engineering, session hijacking, hacking Web servers, Web application vulnerabilities, and more Walks you through exam topics and includes plenty of real-world scenarios to help reinforce concepts Includes a CD with an assessment test, review questions, practice exams, electronic flashcards, and the entire book in a searchable pdf

Embrace the Case Interview walks you through each step on the path to your dream consulting job as described by a former management consultant who conducted over 100 interviews for a top-tier firm. First, we cover how to get the interview including how to be memorable when speaking with firms prior to the interview and how to write a killer resume and cover letter. Second, we cover the behavioral part of the interview. Often overlooked, the behavioral part of the interview covers your personal experiences and is often just as valuable as the case interview. We discuss the traits interviewers are looking for and how to answer their questions in a structured way. Third, we take an in-depth look at the case interview itself. Unlike books that focus on segmenting cases and applying frameworks, you will learn a single, flexible structure that you will apply to any case with deadly effectiveness. In addition to structuring the case, you will learn approaches for the cases' other parts including qualitative questions, quantitative problems, exhibit analysis, and synthesis. Embrace the Case Interview places a strong emphasis on the quality of your learning rather than just doing hundreds of cases. As such, each example case contains an in-depth discussion of the text book answer to help you improve. For more information, please visit [embracethecaseinterview.com](#). Enjoy the book and best of luck in your upcoming interviews!

"A fantastic book for anyone looking to learn the tools and techniques needed to break in and stay in." --Bruce Potter, Founder, The Shmoo Group "Very highly recommended whether you are a seasoned professional or just starting out in the security business." --Simple Nomad, Hacker

Python for Data Analysis

The Real Stories Behind the Exploits of Hackers, Intruders and Deceivers

Successful Business Analysis Consulting

Developing Autonomous Bots for Online Games

Excel 2013: The Missing Manual

How to Write an Amazing IT Resume

Hacking Windows XP

Who are computer hackers? What is free software? And what does the emergence of a community dedicated to the production of free and open source software--and to hacking as a technical, aesthetic, and moral project--reveal about the values of contemporary liberalism? Exploring the rise and political significance of the free and open source software (FOSS) movement in the United States and Europe, *Influence People* details the ethics behind hackers' devotion to FOSS, the social codes that guide its production, and the political struggles through which hackers question the scope and direction of copyright and patent law. In telling the story of the FOSS movement, the book unfolds a broader narrative involving computing, the politics of access, and intellectual property. E. Gabriel Coleman tracks the ways in which hackers collaborate and examines passionate manifestos, hacker humor, free software project governance, and festive hacker conferences. Looking at the ways that hackers sustain their productive freedom, Coleman shows that these activists, driven by a commitment to their work, reformulate key ideals including free speech, transparency, and meritocracy, and refuse restrictive intellectual protections. Coleman demonstrates how hacking, so often marginalized or misunderstood, sheds light on the continuing relevance of liberalism in online collaboration.

Cutting-edge techniques for finding and fixing critical security flaws Fortify your network and avert digital catastrophe with proven strategies from a team of security experts. Completely updated and featuring 13 new chapters, *Gray Hat Hacking, The Ethical Hacker's Handbook, Fifth Edition* explains the enemy's current weapons, skills, and tactics and offers field-tested remedies, case studies, and ready-to-try testing labs. Find out how hackers gain access, overtake network devices, script and inject malicious code, and plunder Web applications and browsers. Android-based exploits, reverse engineering techniques, and cyber law are thoroughly covered in this state-of-the-art resource. And the new topic of exploiting the Internet of things is introduced in this edition. •Build and launch spoofing exploits with Ettercap •Induce error conditions and crash software using fuzzers •Use advanced reverse engineering to exploit Windows and Linux software •Bypass Windows Access Control and memory protection schemes •Exploit web applications with Padding Oracle Attacks •Learn the use-after-free technique used in recent zero days •Hijack web browsers with advanced XSS attacks •Understand ransomware and how it takes control of your desktop •Dissect Android malware with JEB and DAD decompilers •Find one-day vulnerabilities with binary diffing •Exploit wireless systems with Software Defined Radios (SDR) •Exploit Internet of things devices •Dissect and exploit embedded devices •Understand bug bounty programs •Deploy next-generation honeypots

•Dissect ATM malware and analyze common ATM attacks •Learn the business side of ethical hacking

Malware analysis is big business, and attacks can cost a company dearly. When malware breaches your defenses, you need to act quickly to cure current infections and prevent future ones from occurring. For those who want to stay ahead of the latest malware, *Practical Malware Analysis* will teach you the tools and techniques used by professional analysts. With this book as your guide, you'll be able to safely analyze, debug, and disable nearly any malicious software that comes your way. You'll learn how to:-Set up a safe virtual environment to analyze malware -Quickly extract network signatures and host-based indicators -Use key analysis tools like IDA Pro, OllyDbg, and WinDbg -Overcome malware tricks like obfuscation, anti-disassembly, anti-debugging, and anti-virtual machine techniques -Use your debugger to analyze malware -Develop a methodology for tracking malware and get practical experience with five of the most popular packers -Analyze special cases of malware with shellcode, C++, and 64-bit code Hands-on labs throughout the book challenge you to practice and synthesize your skills as you dissect real malware samples, and pages of detailed dissections offer an over-the-shoulder look at how the pros do it. You'll learn how to crack open malware, see how it really works, determine what damage it has done, thoroughly clean your network, and ensure that the malware never comes back. Malware analysis is a cat-and-mouse game with rules that are constantly changing, so make sure you have the fundamentals. Whether you're tasked with securing one network or a thousand networks, or you're making a living as a malware analyst, you'll find what you need to succeed in *Practical Malware Analysis*.

The #1 menace for computer systems worldwide, network hacking can result in mysterious server crashes, data loss, and other problems that are not only costly to fix but difficult to recognize. Author John Chirillo knows how these can be prevented, and in this book he brings to the table the perspective of someone who has been invited to break into the networks of many Fortune 1000 companies in order to evaluate their security policies and conduct security audits. He gets inside every detail of the hacker's world, including how hackers exploit security holes in private and public networks and how network hacking tools work. As a huge value-add, the author is including the first release of a powerful software hack attack tool that can be configured to meet individual customer needs.

Practical Malware Analysis

Silicon Valley's Best Kept Secret

Tribe of Hackers

Excel Hacks

Hack Attacks Revealed

Go Programming For Hackers and Pentesters

Hackers Beware

Like the best-selling *Black Hat Python*, *Black Hat Go* explores the darker side of the popular Go programming language. This collection of short scripts will help you test your systems, build and automate tools to fit your needs, and improve your offensive security skillset. *Black Hat Go* explores the darker side of Go, the popular programming language revered by hackers for its simplicity, efficiency, and reliability. It provides an arsenal of practical tactics from the perspective of security practitioners and hackers to help you test your systems, build and automate tools to fit your needs, and improve your offensive security skillset. all using the power of Go. You'll begin your journey with a basic overview of Go's syntax and philosophy and then start to explore examples that you can leverage for tool development, including common network protocols like HTTP, DNS, and SMB. You'll then dig into various tactics and problems that penetration testers encounter, addressing things like data piling, packet sniffing, and exploit development. You'll create dynamic, pluggable tools before diving into cryptography, attacking Microsoft Windows, and implementing steganography. You'll learn how to:-Make performance tools that can be used for your own security projects •Create usable tools that interact with remote APIs •Scope arbitrary HTML data •Use Go's standard package, net/http, for building HTTP servers •Write your own DNS server and proxy •Use DNS tunneling to establish a C2 channel out of a restrictive network •Create a vulnerability fuzzer to discover an application's security weaknesses •Use plug-ins and extensions to future-proof productsBuild an RC2 symmetric-key brute-force • Implant data within a Portable Network Graphics (PNG)

With more than 600 security tools in its arsenal, the Kali Linux distribution can be overwhelming. Experienced and aspiring security professionals alike may find it challenging to select the most appropriate tool for conducting a given test. This practical book covers Kali's expansive security capabilities and helps you identify the tools you need to conduct a wide range of security tests and penetration tests. You'll also explore the vulnerabilities that make those tests necessary. Author Ric Messier takes you through the foundations of Kali Linux and explains methods for conducting tests on networks, web applications, wireless security, password vulnerability, and more. You'll discover different techniques for extending Kali tools and creating your own toolset. Learn tools for stress testing network stacks and applications Perform network reconnaissance to determine what's available to attackers Execute penetration tests using automated exploit tools such as Metasploit Use cracking tools to see if passwords meet complexity requirements Test wireless capabilities by injecting frames and cracking passwords Assess web application vulnerabilities with automated or proxy-based tools Create advanced attack techniques by extending Kali tools or developing your own Use Kali Linux to generate reports once testing is complete

To land a management consulting job at any of the top firms, including McKinsey, Bain, BCG, Deloitte, Oliver Wyman, and Accenture, you must get through several rounds of case interviews. Whether your interview is in a few weeks or even tomorrow, this book is written to get you the maximum amount of knowledge in the least amount of time. Think of this book as taking the express lane towards preparing to master consulting case studies and get out of the interview process as quickly as possible. This volume is the most useful and most comprehensive book you need to know in a clear and direct way. With this book you will: Understand the nine different parts of a case interview, and know exactly what to say and do in each step Learn the only framework strategy that you need to memorize to craft unique and tailored frameworks for every possible case scenario Gain knowledge of basic business terms and principles so that you can develop an astute business intuition Acquire the skills to solve any market sizing or other quantitative problem Uncover how to differentiate yourself from the thousands of other candidates who are fighting to get the same job you are Practice your case interview skills with included practice cases and sample answers. Curious about how to perform penetration testing? Have you always wanted to become an ethical hacker but haven't got the time or the money to take expensive workshops? Then this book is for you! With just 2 hours of daily dedication you could be able to start your practice as an ethical hacker, of course as long as you not only read the chapters but perform all the labs included with this book. Table of contents:- Chapter 1 - Introduction to Ethical Hacking - Chapter 2 - Reconnaissance or footprinting - Chapter 3 - Scanning - Chapter 4 - Enumeration - Chapter 5 - Exploitation or hacking - Chapter 6 - Writing the audit report without suffering a major breakdown - Chapter 7 - Relevant international certificates - Final Recommendations - Please leave us a review - About the author - Glossary of technical terms - Appendix A: Tips for successful labs - Notes and references Note: The labs are updated for Kali Linux 2!

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

Case Interview Secrets

Restoring the Character Ethic

Hacking the PSP

The Complete Guide from Getting the Interview to Landing the Job

Get the Interview Every Time

Best Practices for Success

Tap into the wisdom of experts to learn what every programmer should know, no matter what language you use. With the 97 short and extremely useful tips for programmers in this book, you'll expand your skills by adopting new approaches to old problems, learning appropriate best practices, and honing your craft through sound advice. With contributions from some of the most experienced and respected practitioners in the industry—including Michael Feather, Peter Goodfellow, Diomidis Spinellis, Cay Horstmann, Venity Stoh, and many more--this book contains practical knowledge and principles that you can apply to all kinds of projects. A few of the 97 things you should know: "Code in the Language of the Domain" by Dan North "Write Tests for People" by Gerard Meszaros "Convenience Is Not an -ility" by Gregor Hohpe "Know Your IDE" by Heinz Kabutz "A Message to the Future" by Linda Rising "The Boy Scout Rule" by Robert C. Martin (Uncle Bob) "Beware the Share" by Udi Dahan

Offers step-by-step instructions on getting the most out of Windows XP, covering such topics as customizing the login screen, desktop, and Windows interface; increasing the performance of system; and computer security.

The definitive guide on the roles and responsibilities of the business analyst Business Analyst offers a complete description of the process of business analysis in solving business problems. Filled with tips, tricks, techniques, and guerilla tactics to help execute the process in the face of sometimes overwhelming political or social obstacles, this guide is also filled with real world stories from the author's more than thirty years of experience working as a business analyst. Provides techniques and tips to execute the at-times tricky job of business analyst Written by an industry expert with over thirty years of experience Straightforward and insightful, Business Analysis is a valuable contribution to your ability to be successful in this role in today's business environment. Discover all the security risks and exploits that can threaten iOS-based mobile devices iOS is Apple's mobile operating system for the iPhone and iPad. With the introduction of iOS5, many security issues have come to light. This book explains and discusses them all. The award-winning author team, experts in Mac and iOS security, examines the vulnerabilities and the internals of iOS to show how attacks can be mitigated. The book explains how the operating system works, its overall security architecture, and the security risks associated with it, as well as exploits, rootkits, and other payloads developed for it. Covers iOS security architecture, vulnerability hunting, exploit writing, and how iOS jailbreaks work Explores iOS enterprise and encryption, code signing and memory protection, sandboxing, iPhone fuzzing, exploitation, ROP payloads, and baseband attacks Also examines kernel debugging and exploitation Companion website includes source code and tools to facilitate your efforts iOS Hacker's Handbook arms you with the tools needed to identify, understand, and foil iOS attacks.

Your Shortcut Guide to Mastering Consulting Interviews

The Mac Hacker's Handbook

A Former McKinsey Interviewer Reveals how to Get Multiple Job Offers in Consulting

Ethical Hacking With Kali Linux

Data Wrangling with Pandas, NumPy, and IPython

Business Analysis

The Ethics and Aesthetics of Hacking

CEH Certified Ethical Hacker Study GuideJohn Wiley & Sons

Cheng, a former McKinsey management consultant, reveals his proven, insider's method for acing the case interview.

Provides information on getting the most out of a PSP, covering such topics as playing multiplayer games wirelessly, reading the comics, changing game backgrounds, and finding free downloads.

This volume in the *Business Analyst Interview Preparation Series* by renowned expert and best-selling author, Karl Wiegers, and a group of noteworthy contributors, provides experienced, advanced-level business analysis and project management practitioners with proven strategies and tips for making the successful transition from highly respected internal expert to a fulfilling and financially rewarding career in consulting. Key Features: Addresses how to effectively lay the foundation and structure of your consulting business; how to lead or avoid the many pitfalls of working outside the corporate world and working remotely from home; and how to balance life, family, and work Presents a list of next steps at the end of each chapter with actions you can take immediately to begin applying the guidance and tips provided Furnishes valuable strategies and tips for such essentials as setting rates for your services, invoicing, purchasing appropriate insurance, establishing important business rules or policies, managing your finances and taxes, and other administrative aspects of your consultancy Articulates how to market your services, land both new and repeat business, negotiate deals, and craft written agreements with clients Describes how to establish multiple revenue streams, ways to leverage your work to develop sources of passive income, and some important issues of copyright, fair use, and managing and protecting your valuable intellectual property Provides sample checklists to help you keep all the activities you will be juggling as a consultant under control Identifies effective techniques for engaging clients in various situations, as well as warning signs about clients who can cause you headaches and how to deal with them Supplies solutions to a wide variety of problems and challenges of the consulting world, contributed by a group of noteworthy independent consultants with diverse experiences Discusses other common consultant activities that can generate a steady flow of revenue such as training, presenting at conferences, and other public speaking, and provides guidance and tips for delivering effective presentations with confidence Offers strategies and tips pertaining to partnering with other consultants on larger projects and how to make such arrangements work Examines the value of participating in professional associations and pursuing relevant professional certifications as a way to market your services and attract new clients and opportunities Explores the benefits of writing white papers and articles for magazines, journals, websites, and blogs as a means to simultaneously share your knowledge with the world and market your expertise to prospective clients Elaborates on the process and value of writing a book in the area in which you consult, how to get it published and distributed by a reputable publishing company that can reach your market, how to write the book

• Author and best-selling author, Karl Wiegers, and how a good selling book can be a powerful tool for getting clients and building your business WAV offers downloadable templates for consulting, writing, speaking, and licensing agreements, and checklists and forms to help you plan and manage your consulting business--available from the Web Added Value(tm) Download Resource Center at [www.jcrosspub.com](#)

Learning Kali Linux

Become a Consultant at McKinsey, BCG, Bain, Etc.

The Hacker Crackdown, Law and Disorder on the Electronic Frontier

Reversing

Democratizing Innovation

Pushing the iPhone and iPod touch Beyond Their Limits

Gray Hat Hacking, Second Edition

Top consulting firms like McKinsey, BCG, and Bain only hire about 1% of their job applicants. Becoming a management consultant is difficult, but it is possible if you use a proven approach at each stage of the process.Cracking Case Interviews is a comprehensive "one-stop shop" for landing a job in consulting. This book will help you: Write the perfect consulting resume and cover letter that gets multiple interview invitations from top consultants Learn the 7 different parts of a case interview and exactly what you need to do in each step Master maps tips and tricks to solve market sizing and other case interview questions quickly and accurately Discover the most commonly used frameworks in consulting and how you can use them for inspiration, and without relying on them Practice with 5 full-length sample cases that are based on McKinsey, BCG, and Bain case interviews Prepare answers to behavioural interview questions, like "Why consulting?", "Why McKinsey?", or "Tell me about a time you led a team." Max Serrano and Jonathan Yarde are former consultants and instructors at IGotAnOffer, the #1 website for case interview preparation, which has helped place over 2,000 applicants in consulting careers since 2015. This book translates the countless hours the authors have spent coaching undergraduates, MBAs, PhDs, MDs, JDs, and experienced hires on their consulting applications. With iPhone Hacks, you can make your iPhone do all you'd expect of a mobile smartphone -- and more. Learn tips and techniques to unleash little-known features, find and create innovative applications for both the iPhone and iPod touch, and unshackle these devices to run everything from network utilities to video game emulators. This book will teach you how to: Import your entire movie collection, sync with multiple computers, and save YouTube videos Remotely access your home network, audio, and video, and even control your desktop Develop native applications for the iPhone and iPod touch on Linux, Windows, or Mac Check email, receive MMS messages, use IRC, and record full-motion video Run any application in the iPhone's background, and mirror its display on a TV Make your iPhone emulate old-school video game platforms, and play classic console and arcade games Integrate your iPhone with your car stereo Build your own electronic bridges to connect keyboards, serial devices, and more to your iPhone without "jailbreaking" iPhone Hacks explains how to set up your iPhone the way you want it, and helps you give it capabilities that will rival your desktop computer. This cunning little handbook is exactly what you need to make the most of your iPhone.

The world's most popular spreadsheet program is now more powerful than ever, but it's also more complex. That's where this Missing Manual comes in. With crystal-clear explanations and hands-on examples, *Excel 2013: The Missing Manual* shows you how to master Excel so you can easily track, analyze, and chart your data. You'll be using new features like PowerPivot and Flash Fill in no time. The important stuff you need to know: Go from novice to ace. Learn how to ace. Learn how to ace. Learn how to ace. Learn how to ace. Learn how to ace. Illustrate trends. Discover the clearest way to present your data using Excel's new Quick Analysis feature. Broaden your analysis. Use pivot tables, slicers, and timelines to examine your data from different perspectives. Import data. Pull data from a variety of sources, including website data feeds and corporate databases. Work from the Web. Launch and manage your workbooks on the road, using the new Excel Web App. Share your worksheets. Store Excel files on SkyDrive and collaborate with colleagues on Facebook, Twitter, and LinkedIn. Master the new data model. Use PowerPivot to work with millions of rows of data. Make calculations. Review financial data, use math and scientific formulas, and perform statistical analyses.

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-desperado and fugitive form one of the most exhaustive FBI manhunt 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 fireworks 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 point 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.

Cybersecurity Advice from the Best Hackers in the World

How to Conduct Professional Pestings in 21 Days Or Less!

The Art of Deception

Tips & Tools for Streamlining Your Spreadsheets

Security Testing, Penetration Testing, and Ethical Hacking

How To Win Friends And Influence People

Hacking the Case Interview

This book is part of the *TREDDITION CLASSICS*. It contains classical literature works from over two thousand years. Most of these titles have been out of print and off the bookstore shelves for decades. The book series is intended to preserve the cultural legacy and to promote the timeless works of classical literature. Readers of a *TREDDITION CLASSICS* book support the mission to save many of the amazing works of literature from oblivion. This series is available in paperback and Kindle. You can read any of the books in this series, or you can read them all. The process of user-centered innovation: how it can benefit both users and manufacturers and how its emergence will bring changes in business models and in public policy. Innovation is rapidly becoming democratized. Users, aided by improvements in computer and communications technology, increasingly can develop their own new products and services. These innovating users--both individuals and firms--often freely share their innovations with others, creating user-innovation communities and a rich intellectual commons. In *Democratizing Innovation*, Eric von Hippel looks closely at this emerging system of user-centered innovation. He explains why and when users find it profitable to develop new products and services for themselves, and why it often pays users to reveal their innovations freely for the use of all. The trend toward democratized innovation can be seen in software and information products--most notably in the free and open-source software movement--but also in physical products. Von Hippel's many examples of user innovation in action range from surgical equipment to surfboards to software security features. He shows that product and service development is concentrated among "lead users," who are ahead on marketplace trends and whose innovations are often commercially attractive. Von Hippel argues that manufacturers should redesign their innovation processes and that they should systematically seek out innovations developed by users. He points to businesses--the custom semiconductor industry is one example--that have learned to assist user-innovators by providing them with toolkits for developing new products. User innovation has a positive impact on social welfare, and von Hippel proposes that government policies, including R&D subsidies and tax credits, should be realigned to eliminate biases against it. The goal of a democratized user-centered innovation system, says von Hippel, is well worth striving for: "An electronic version of this book is available under a Creative Commons license.

Use interview preparation, which has helped place over 2,000 applicants in consulting careers since 2015. This book translates the countless hours the authors have spent coaching undergraduates, MBAs, PhDs, MDs, JDs, and experienced hires on their consulting applications. With iPhone Hacks, you can make your iPhone do all you'd expect of a mobile smartphone -- and more. Learn tips and techniques to unleash little-known features, find and create innovative applications for both the iPhone and iPod touch, and unshackle these devices to run everything from network utilities to video game emulators. This book will teach you how to: Import your entire movie collection, sync with multiple computers, and save YouTube videos Remotely access your home network, audio, and video, and even control your desktop Develop native applications for the iPhone and iPod touch on Linux, Windows, or Mac Check email, receive MMS messages, use IRC, and record full-motion video Run any application in the iPhone's background, and mirror its display on a TV Make your iPhone emulate old-school video game platforms, and play classic console and arcade games Integrate your iPhone with your car stereo Build your own electronic bridges to connect keyboards, serial devices, and more to your iPhone without "jailbreaking" iPhone Hacks explains how to set up your iPhone the way you want it, and helps you give it capabilities that will rival your desktop computer. This cunning little handbook is exactly what you need to make the most of your iPhone.

The world's most popular spreadsheet program is now more powerful than ever, but it's also more complex. That's where this Missing Manual comes in. With crystal-clear explanations and hands-on examples, *Excel 2013: The Missing Manual* shows you how to master Excel so you can easily track, analyze, and chart your data. You'll be using new features like PowerPivot and Flash Fill in no time. The important stuff you need to know: Go from novice to ace. Learn how to ace. Learn how to ace. Learn how to ace. Learn how to ace. Illustrate trends. Discover the clearest way to present your data using Excel's new Quick Analysis feature. Broaden your analysis. Use pivot tables, slicers, and timelines to examine your data from different perspectives. Import data. Pull data from a variety of sources, including website data feeds and corporate databases. Work from the Web. Launch and manage your workbooks on the road, using the new Excel Web App. Share your worksheets. Store Excel files on SkyDrive and collaborate with colleagues on Facebook, Twitter, and LinkedIn. Master the new data model. Use PowerPivot to work with millions of rows of data. Make calculations. Review financial data, use math and scientific formulas, and perform statistical analyses.

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-desperado and fugitive form one of the most exhaustive FBI manhunt 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 fireworks 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 point 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.

Cybersecurity Advice from the Best Hackers in the World

How to Conduct Professional Pestings in 21 Days Or Less!

The Art of Deception

Tips & Tools for Streamlining Your Spreadsheets

Security Testing, Penetration Testing, and Ethical Hacking

How To Win Friends And Influence People

Hacking the Case Interview

This book is part of the *TREDDITION CLASSICS*. It contains classical literature works from over two thousand years. Most of these titles have been out of print and off the bookstore shelves for decades. The book series is intended to preserve the cultural legacy and to promote the timeless works of classical literature. Readers of a *TREDDITION CLASSICS* book support the mission to save many of the amazing works of literature from oblivion. This series is available in paperback and Kindle. You can read any of the books in this series, or you can read them all. The process of user-centered innovation: how it can benefit both users and manufacturers and how its emergence will bring changes in business models and in public policy. Innovation is rapidly becoming democratized. Users, aided by improvements in computer and communications technology, increasingly can develop their

This unique guide includes inspiring interviews from 70 security experts, including Lesley Carhart, Ming Chow, Bruce Potter, Robert M. Lee, and Jayson E. Street. Get the scoop on the biggest cybersecurity myths and misconceptions about security Learn what qualities and credentials you need to advance in the cybersecurity field Uncover which life hacks are worth your while Understand how social media and the Internet of Things has changed cybersecurity Discover what it takes to make the move from the corporate world to your own cybersecurity venture Find your favorite hackers online and continue the conversation Tribe of Hackers is a must-have resource for security professionals who are looking to advance their careers, gain a fresh perspective, and get serious about cybersecurity with thought-provoking insights from the world's most noteworthy hackers and influential security specialists.

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.

Millions of users create and share Excel spreadsheets every day, but few go deeply enough to learn the techniques that will make their work much easier. There are many ways to take advantage of Excel's advanced capabilities without spending hours on advanced study. Excel Hacks provides more than 130 hacks -- clever tools, tips and techniques -- that will leapfrog your work beyond the ordinary. Now expanded to include Excel 2007, this resourceful, roll-up-your-sleeves guide gives you little known "backdoor" tricks for several Excel versions using different platforms and external applications. Think of this book as a toolbox. When a need arises or a problem occurs, you can simply use the right tool for the job. Hacks are grouped into chapters so you can find what you need quickly, including ways to: Reduce workbook and worksheet frustration -- manage how users interact with worksheets, find and highlight information, and deal with debris and corruption. Analyze and manage data -- extend and automate these features, moving beyond the limited tasks they were designed to perform. Hack names -- learn not only how to name cells and ranges, but also how to create names that adapt to the data in your spreadsheet. Get the most out of PivotTables -- avoid the problems that make them frustrating and learn how to extend them. Create customized charts -- tweak and combine Excel's built-in charting capabilities. Hack formulas and functions -- subjects range from moving formulas around to dealing with datatype issues to improving recalculation time. Make the most of macros -- including ways to manage them and use them to extend other features. Use the enhanced capabilities of Microsoft Office 2007 to combine Excel with Word, Access, and Outlook. You can either browse through the book or read it from cover to cover, studying the procedures and scripts to learn more about Excel. However you use it, Excel Hacks will help you increase productivity and give you hours of "hacking" enjoyment along the way.

In Growth Hacking: Silicon Valley's Best Kept Secret, growth consultants Raymond Fong and Chad Ridderssen deconstruct the phenomenon used by Silicon Valley's fast growing tech elite, growth hacking. Raymond and Chad's framework, the ASP(TM), is an easy to understand blueprint that empowers any business to apply growth hacking. The ASP(TM) was developed through their work in the tech community and used to produce high-leverage, scalable growth for companies in a variety of industries including several companies featured on ABC's TV show Shark Tank. If you're looking for creative, cost-effective ways to grow your business, then ASP(TM) is the answer.

iOS Hacker's Handbook

Learn Fast How To Hack Like A Pro

iPhone Hacks

The Art of Intrusion