

Counter Hack Reloaded

Enterprise Cybersecurity empowers organizations of all sizes to defend themselves with next-generation cybersecurity programs against the escalating threat of modern targeted cyberattacks. This book presents a comprehensive framework for managing all aspects of an enterprise cybersecurity program. It enables an enterprise to architect, design, implement, and operate a coherent cybersecurity program that is seamlessly coordinated with policy, programmatics, IT life cycle, and assessment. Fail-safe cyberdefense is a pipe dream. Given sufficient time, an intelligent attacker can eventually defeat defensive measures protecting an enterprise's computer systems and IT networks. To prevail, an enterprise cybersecurity program must manage risk by detecting attacks early enough and delaying them long enough that the defenders have time to respond effectively. Enterprise Cybersecurity shows players at all levels of responsibility how to unify their organization's people, budgets, technologies, and processes into a cost-efficient cybersecurity program capable of countering advanced cyberattacks and containing damage in the event of a breach. The authors of Enterprise Cybersecurity explain at both strategic and tactical levels how to accomplish the mission of leading, designing, deploying, operating, managing, and supporting cybersecurity capabilities in an enterprise environment. The authors are recognized experts and thought leaders in this rapidly evolving field, drawing on decades of collective experience in cybersecurity and IT. In capacities ranging from executive strategist to systems architect to cybercombatant, Scott E. Donaldson, Stanley G. Siegel, Chris K. Williams, and Abdul Aslam have fought on the front lines of cybersecurity against advanced persistent threats to government, military, and business entities.

This book captures the state of the art research in the area of malicious code detection, prevention and mitigation. It contains cutting-edge behavior-based techniques to analyze and detect obfuscated malware. The book analyzes current trends in malware activity online, including botnets and malicious code for profit, and it proposes effective models for detection and prevention of attacks using. Furthermore, the book introduces novel techniques for creating services that protect their own integrity and safety, plus the data they manage.

Part of the Jones & Bartlett Learning Information Systems Security and Assurance Series <http://www.issaseries.com> Revised and updated to address the many changes in this evolving field, the Second Edition of Legal Issues in Information Security (Textbook with Lab Manual) addresses the area where law and information security concerns intersect. Information systems security and legal compliance are now required to protect critical governmental and corporate infrastructure, intellectual property created by individuals and organizations alike, and information that individuals believe should be protected from unreasonable intrusion. Organizations must build numerous information security and privacy responses into their daily operations to protect the business itself, fully meet legal requirements, and to meet the expectations of employees and customers. Instructor Materials for Legal Issues in Information Security include: PowerPoint Lecture Slides Instructor's Guide Sample Course Syllabus Quiz & Exam Questions Case Scenarios/Handouts New to the Second Edition: • Includes discussions of amendments in several relevant federal and state laws and regulations since 2011 • Reviews relevant court decisions that have come to light since the publication of the first edition • Includes numerous information security data breaches highlighting new vulnerabilities

Building a Practical Information Security Program provides users with a strategic view on how to build an information security program that aligns with business objectives. The information provided enables both executive management and IT managers not only to validate existing security programs, but also to build new business-driven security programs. In addition, the subject matter supports aspiring security engineers to forge a career path to successfully manage a security program, thereby adding value and reducing risk to the business. Readers learn how to translate technical challenges into business requirements, understand when to "go big or go home," explore in-depth defense strategies, and review tactics on when to absorb risks. This book explains how to properly plan and implement an infosec program based on business strategy and results. Provides a roadmap on how to build a security program that will protect companies from intrusion Shows how to focus the security program on its essential mission and move past FUD (fear, uncertainty, and doubt) to provide business value Teaches how to build consensus with an effective business-focused program

This text emphasizes the three major driving forces behind e-commerce: technological change, business development, and social issues, to provide a coherent conceptual framework for understanding the field.

#1 NEW YORK TIMES BESTSELLER • NOW A MAJOR MOTION PICTURE • Look for special features inside. Join the Random House Reader's Circle for author chats and more. In boyhood, Louis Zamperini was an incorrigible delinquent. As a teenager, he channeled his defiance into running, discovering a prodigious talent that had carried him to the Berlin Olympics. But when World War II began, the athlete became an airman, embarking on a journey that led to a doomed flight on a May afternoon in 1943. When his Army Air Forces bomber crashed into the Pacific Ocean, against all odds, Zamperini survived, adrift on a foundering life raft. Ahead of Zamperini lay thousands of miles of open ocean, leaping sharks, thirst and starvation, enemy aircraft, and, beyond, a trial even greater. Driven to the limits of endurance, Zamperini would answer desperation with ingenuity; suffering with hope, resolve, and humor; brutality with rebellion. His fate, whether triumph or tragedy, would be suspended on the fraying wire of his will. Appearing in paperback for the first time—with twenty arresting new photos and an extensive Q&A with the author—Unbroken is an unforgettable testament to the resilience of the human mind, body, and spirit, brought vividly to life by Seabiscuit author Laura Hillenbrand. Hailed as the top nonfiction book of the year by Time magazine • Winner of the Los Angeles Times Book Prize for biography and the Indies Choice Adult Nonfiction Book of the Year award "Extraordinarily moving . . . a powerfully drawn survival epic."—The Wall Street Journal "[A] one-in-a-billion story . . . designed to wrench from self-respecting critics all the blurby adjectives we normally try to avoid: It is amazing, unforgettable, gripping, harrowing, chilling, and inspiring."—New York "Staggering . . . mesmerizing . . . Hillenbrand's writing is so ferociously cinematic, the events she describes so incredible, you don't dare take your eyes off the page."—People "A meticulous, soaring and beautifully written account of an extraordinary life."—The Washington Post "Ambitious and powerful . . . a startling narrative and an inspirational book."—The New York Times Book Review "Magnificent . . . incredible . . . [Hillenbrand] has crafted another masterful blend of sports, history and overcoming terrific odds; this is biography taken to the nth degree, a chronicle of a remarkable life lived through extraordinary times."—The Dallas Morning News "An astonishing testament to the superhuman power of tenacity."—Entertainment Weekly "A tale of triumph and redemption . . . astonishingly detailed."—O: The Oprah Magazine "[A] masterfully told true story . . . nothing less than a marvel."—Washingtonian "[Hillenbrand tells this] story with cool elegance but at a thrilling sprinter's pace."—Time "Hillenbrand [is] one of our best writers of narrative history. You don't have to be a sports fan or a war-history buff to devour this book—you just have to love great storytelling."—Rebecca Skloot, author of The Immortal Life of Henrietta Lacks

The classic guide to network security—now fully updated!"Bob and Alice are back!" Widely regarded as the most comprehensive yet comprehensible guide to network security, the first edition of Network Security received critical acclaim for its lucid and witty explanations of the inner workings of network security protocols. In the second edition, this most distinguished of author teams draws on hard-won experience to explain the latest developments in this field that has become so critical to our global network-dependent society. Network Security, Second Edition brings together clear, insightful, and clever explanations of every key facet of information security, from the basics to advanced cryptography and authentication, secure Web and email services, and emerging security standards. Coverage includes: All-new discussions of the Advanced Encryption Standard (AES), IPsec, SSL, and Web security Cryptography: In-depth, exceptionally clear introductions to secret and public keys, hashes, message digests, and other crucial concepts Authentication: Proving identity across networks, common attacks against authentication systems, authenticating people, and avoiding the pitfalls of authentication handshakes Core Internet security standards: Kerberos 4/5, IPsec, SSL, PKIX, and X.509 Email security: Key elements of a secure email system-plus detailed

coverage of PEM, S/MIME, and PGP Web security: Security issues associated with URLs, HTTP, HTML, and cookies Security implementations in diverse platforms, including Windows, NetWare, and Lotus Notes The authors go far beyond documenting standards and technology: They contrast competing schemes, explain strengths and weaknesses, and identify the crucial errors most likely to compromise secure systems. Network Security will appeal to a wide range of professionals, from those who design or evaluate security systems to system administrators and programmers who want a better understanding of this important field. It can also be used as a textbook at the graduate or advanced undergraduate level.

The wonders and advantages of modern age electronics and the World Wide Web have also, unfortunately, ushered in a new age of terrorism. The growing connectivity among secure and insecure networks has created new opportunities for unauthorized intrusions into sensitive or proprietary computer systems. Some of these vulnerabilities are waiting to be exploited, while numerous others already have. Everyday that a vulnerability or threat goes unchecked greatly increases an attack and the damage it can cause. Who knows what the prospects for a cascade of failures across US infrastructures could lead to. What type of group or individual would exploit this vulnerability, and why would they do it? "Inside the Mind of a Criminal Hacker" sets the stage and cast of characters for examples and scenarios such as this, providing the security specialist a window into the enemy's mind - necessary in order to develop a well configured defense. Written by leading security and counter-terrorism experts, whose experience include first-hand exposure in working with government branches & agencies (such as the FBI, US Army, Department of Homeland Security), this book sets a standard for the fight against the cyber-terrorist. Proving, that at the heart of the very best defense is knowing and understanding your enemy. * This book will demonstrate the motives and motivations of criminal hackers through profiling attackers at post attack and forensic levels. * This book is essential to those who need to truly "know thy enemy" in order to prepare the best defense. * . The breadth of material in "Inside the Criminal Mind" will surprise every security specialist and cyber-terrorist buff of how much they do and (more importantly) don't know about the types of adversaries they stand to face.

"I finally get it! I used to hear words like rootkit, buffer overflow, and idle scanning, and they just didn't make any sense. I asked other people and they didn't seem to know how these things work, or at least they couldn't explain them in a way that I could understand. Counter Hack Reloaded is the clearest explanation of these tools I have ever seen. Thank you!"--Stephen Northcutt, CEO, SANS Institute "Ed Skoudis does it again! With this new edition, Ed takes a phenomenal work to the next level! This book is a 'must-have' and a 'must-read' for anyone remotely associated with computers and computer security." -Harlan Carvey, CISSP, author of Windows Forensics and Incident Recovery "Ed Skoudis is a rare individual. He knows the innards of all the various systems, knows all the latest exploits and defenses, and yet is able to explain everything at just the right level. The first edition of Counter Hack was a fascinating read. It's technically intriguing and very clear. ... A book on vulnerabilities, though, will get out of date, and so we definitely needed this updated and significantly rewritten second edition. This book is a wonderful overview of the field." -From the Foreword by Radia Perlman, series editor, The Radia Perlman Series in Computer Networking and Security; author of Interconnections ; and coauthor of Network Security: Private Communications in a Public World "What a great partnership! Ed Skoudis and Tom Liston share an uncanny talent for explaining even the most challenging security concepts in a clear and enjoyable manner. Counter Hack Reloaded is an indispensable resource for those who want to improve their defenses and understand the mechanics of computer attacks." -Lenny Zeltser, coauthor of Malware: Fighting Malicious Code "Ed Skoudis does it again! With this new edition, Ed takes a phenomenal work to the next level! This book is a 'must-have' and a 'must-read' for anyone remotely associated with computers and computer security." -Harlan Carvey, CISSP, author of Windows Forensics and Incident Recovery "In addition to having breadth of knowledge about and probing insights into network security, Ed Skoudis's real strength is in his ability to show complex topics in an understandable form. By the time he's done, what started off as a hopeless conglomeration of acronyms starts to sound comfortable and familiar. This book is your best source for understanding attack strategies, attack tools, and the defenses against bot ...

Network Security Essentials, Third Edition is a thorough, up-to-date introduction to the deterrence, prevention, detection, and correction of security violations involving information delivery across networks and the Internet.

While you're reading this, a hacker could be prying and spying his way into your company's IT systems, sabotaging your operations, stealing confidential information, shutting down your Web site, or wreaking havoc in other diabolical ways. Hackers For Dummies helps you hack into a hacker's mindset and take security precautions to help you avoid a hack attack. It outlines computer hacker tricks and techniques you can use to assess the security of your own information systems, find security vulnerabilities, and fix them before malicious and criminal hackers can exploit them. It covers: Hacking methodology and researching public information to see what a hacker can quickly learn about your operations Social engineering (how hackers manipulate employees to gain information and access), physical security, and password vulnerabilities Network infrastructure, including port scanners, SNMP scanning, banner grabbing, scanning, and wireless LAN vulnerabilities Operating systems, including Windows, Linux, and Novell NetWare Application hacking, including malware (Trojan horses, viruses, worms, rootkits, logic bombs, and more), e-mail and instant messaging, and Web applications Tests, tools (commercial, shareware, and freeware), and techniques that offer the most bang for your ethical hacking buck With this guide you can develop and implement a comprehensive security assessment plan, get essential support from management, test your system for vulnerabilities, take countermeasures, and protect your network infrastructure. You discover how to beat hackers at their own game, with: A hacking toolkit, including War dialing software, password cracking software, network scanning software, network vulnerability assessment software, a network analyzer, a Web application assessment tool, and more All kinds of countermeasures and ways to plug security holes A list of more than 100 security sites, tools, and resources Ethical hacking helps you fight hacking with hacking, pinpoint security flaws within your systems, and implement countermeasures. Complete with tons of screen shots, step-by-step instructions for some countermeasures, and actual case studies from IT security professionals, this is an invaluable guide, whether you're an Internet security professional, part of a penetration-testing team, or in charge of IT security for a large or small business. This guide empowers network and system administrators to defend their information and computing assets--whether or not they have security experience. Skoudis presents comprehensive, insider's explanations of today's most destructive hacker tools and tactics, and specific, proven countermeasures for both UNIX and Windows environments.

Never HIGHLIGHT a Book Again! Virtually all of the testable terms, concepts, persons, places, and events from the textbook are included. Cram101 Just the FACTS101 studyguides give all of the outlines, highlights, notes, and quizzes for your textbook with optional online comprehensive practice tests. Only Cram101 is Textbook Specific. Accompanys: 9780131481046 .

This 25th anniversary edition of Steven Levy's classic book traces the exploits of the computer revolution's original hackers -- those brilliant and eccentric nerds from the late 1950s through the early '80s who took risks, bent the rules, and pushed the world

in a radical new direction. With updated material from noteworthy hackers such as Bill Gates, Mark Zuckerberg, Richard Stallman, and Steve Wozniak, Hackers is a fascinating story that begins in early computer research labs and leads to the first home computers. Levy profiles the imaginative brainiacs who found clever and unorthodox solutions to computer engineering problems. They had a shared sense of values, known as "the hacker ethic," that still thrives today. Hackers captures a seminal period in recent history when underground activities blazed a trail for today's digital world, from MIT students finagling access to clunky computer-card machines to the DIY culture that spawned the Altair and the Apple II.

Written by a former NYPD cyber cop, this is the only book available that discusses the hard questions cyber crime investigators are asking. The book begins with the chapter "What is Cyber Crime?" This introductory chapter describes the most common challenges faced by cyber investigators today. The following chapters discuss the methodologies behind cyber investigations; and frequently encountered pitfalls. Issues relating to cyber crime definitions, the electronic crime scene, computer forensics, and preparing and presenting a cyber crime investigation in court will be examined. Not only will these topics be generally be discussed and explained for the novice, but the hard questions —the questions that have the power to divide this community— will also be examined in a comprehensive and thoughtful manner. This book will serve as a foundational text for the cyber crime community to begin to move past current difficulties into its next evolution. This book has been written by a retired NYPD cyber cop, who has worked many high-profile computer crime cases Discusses the complex relationship between the public and private sector with regards to cyber crime Provides essential information for IT security professionals and first responders on maintaining chain of evidence

Intended for a first course in performance evaluation, this is a self-contained treatment covering all aspects of queuing theory. It starts by introducing readers to the terminology and usefulness of queueing theory and continues by considering Markovian queues in equilibrium, Little's law, reversibility, transient analysis, and computation, plus the M/G/1 queueing system. It then moves on to cover networks of queues, and concludes with techniques for numerical solutions, a discussion of the PANACEA technique, discrete time queueing systems and simulation, and stochastic Petri networks. The whole is backed by case studies of distributed queueing networks arising in industrial applications. This third edition includes a new chapter on self-similar traffic, many new problems, and solutions for many exercises.

This practical, tutorial-style book uses the Kali Linux distribution to teach Linux basics with a focus on how hackers would use them. Topics include Linux command line basics, filesystems, networking, BASH basics, package management, logging, and the Linux kernel and drivers. If you're getting started along the exciting path of hacking, cybersecurity, and pentesting, Linux Basics for Hackers is an excellent first step. Using Kali Linux, an advanced penetration testing distribution of Linux, you'll learn the basics of using the Linux operating system and acquire the tools and techniques you'll need to take control of a Linux environment. First, you'll learn how to install Kali on a virtual machine and get an introduction to basic Linux concepts. Next, you'll tackle broader Linux topics like manipulating text, controlling file and directory permissions, and managing user environment variables. You'll then focus in on foundational hacking concepts like security and anonymity and learn scripting skills with bash and Python. Practical tutorials and exercises throughout will reinforce and test your skills as you learn how to: - Cover your tracks by changing your network information and manipulating the rsyslog logging utility - Write a tool to scan for network connections, and connect and listen to wireless networks - Keep your internet activity stealthy using Tor, proxy servers, VPNs, and encrypted email - Write a bash script to scan open ports for potential targets - Use and abuse services like MySQL, Apache web server, and OpenSSH - Build your own hacking tools, such as a remote video spy camera and a password cracker Hacking is complex, and there is no single way in. Why not start at the beginning with Linux Basics for Hackers?

The first book completely devoted to this important part of security in a Windows environment.

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 Broad 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 DHCP 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 of 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 linkage of the Kali information, resources and distribution downloads Hands-on exercises reinforce topics

Computer Security, Second Edition offers security newcomers a grounding in the basic principles involved in preventing security breaches and protecting electronic data. It outlines security strategies to counter problems that will be faced in UNIX and Windows NT operating systems, distributed systems, the Web, and object-oriented systems.

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.

For years, Counter Hack has been the primary resource for every network/system administrator and security professional who needs a deep, hands-on understanding of hacker attacks and countermeasures. Now, leading network security expert Ed Skoudis, with Tom Liston, has thoroughly updated this best-selling guide, showing how to defeat today's newest, most sophisticated, and most destructive attacks. For this second edition, more than half the content is new and updated, including coverage of the latest hacker techniques for scanning networks, gaining and maintaining access, and preventing detection. The authors walk you through each attack and demystify every tool and tactic. You'll learn exactly how to establish effective defenses, recognize attacks in progress, and respond quickly and effectively in both UNIX/Linux and Windows environments. Important features of this new edition include All-new "anatomy-of-an-attack" scenarios and tools An all-new section on wireless hacking: war driving, wireless sniffing attacks, and more Fully updated coverage of reconnaissance tools, including Nmap port scanning and "Google hacking" New coverage of tools for gaining access, including uncovering Windows and Linux vulnerabilities with Metasploit New information on dangerous, hard-to-detect, kernel-mode rootkits

This book helps people find sensitive information on the Web. Google is one of the 5 most popular sites on the internet with more than 380 million unique users per month (Nielsen/NetRatings 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 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 URLs. • Use Advanced Operators to Perform Advanced Queries Combine advanced operators and learn about colliding operators and bad search-fu. • Learn the Ways of the Google Hacker See how to use caches for anonymity and review directory listings and traversal techniques. • Review Document Grinding and Database Digging See the ways to use Google to locate documents and then search within the documents to locate information. • Understand Google's Part in an Information Collection Framework Learn 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 hardware and utilities. • See How Bad Guys Troll for Data Find ways to search for usernames, passwords, credit card numbers, social security numbers, and other juicy information. • Hack Google Services Learn more about the AJAX Search API, Calendar, Blogger, Blog Search, and more.

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 wallhacks 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. IRC (Internet Relay Chat) may very well turn out to be the world's most successful hack. In 1988, Jarkko Oikarinen wrote the original IRC program at the University of Oulu, Finland. As he says in his foreword, "IRC started as one summer trainee's programming exercise. A hack grew into a software development project that hundreds of people participated in, and then became a worldwide environment where tens of thousands of people now spend time with each other. I have found many of my friends through IRC and learnt a significant part of my present software engineering knowledge while using and working with IRC. That would not have been possible without learning from code examples and hacks from others". IRC has continued to grow in popularity since its inception. Millions of people from all over the world now use IRC to chat with friends, discuss projects and collaborate on research. With a simple, clearly defined protocol, IRC has become one of the most accessible chat environments, with clients written for a multitude of operating systems. And IRC is more than just a simple chat system it is a network of intercommunicating servers, allowing thousands of clients to connect from anywhere in the world using the IRC protocol. While IRC is easy to get into and many people are happy to use it without being aware of what's happening under the hood, there are those who hunger for more knowledge, and this book is for them. IRC Hacks is a collection of tips and tools that cover just about everything needed to become a true IRC master, featuring contributions from some of the most renowned IRC hackers, many of whom collaborated on IRC, grouping together to form the channel #irchacks on the freenode IRC network (irc.freenode.net). Like all of our Hacks books, there are many different ways to use IRC Hacks. You can read the book from cover to cover, but you might be

better served by picking an interesting item from the table of contents and just diving in. If you're relatively new to IRC, you should consider starting with a few hacks from each progressive chapter. Chapter 1 starts you off by showing you how to connect to IRC, while Chapter 2 acquaints you with the everyday concepts you'll need to use IRC effectively. Chapter 3 is all about users and channels, and introduces the first pieces of code. Chapter 4 shows you how to make useful enhancements to IRC clients. Chapter 5 is where you will learn the basics about creating IRC bots, with Chapters 6-12 introducing more complex bots that can be used for logging, servicing communities, searching, announcing, networking, managing channels or simply for having fun. Chapter 13 delves into the IRC protocol in more detail, and Chapter 14 demonstrates some interesting alternative methods for connecting to IRC. Finally, Chapter 15 will move you on to new pastures by showing you how to set up your own IRC server. This book presents an opportunity to learn how IRC works and how to make best use of some of the features that have made it the most successful, most scalable, and most mature chat system on this planet. IRC Hacks delves deep into the possibilities.

Penetration Tester's Open Source Toolkit, Third Edition, discusses the open source tools available to penetration testers, the ways to use them, and the situations in which they apply. Great commercial penetration testing tools can be very expensive and sometimes hard to use or of questionable accuracy. This book helps solve both of these problems. The open source, no-cost penetration testing tools presented do a great job and can be modified by the student for each situation. This edition offers instruction on how and in which situations the penetration tester can best use them. Real-life scenarios support and expand upon explanations throughout. It also presents core technologies for each type of testing and the best tools for the job. The book consists of 10 chapters that covers a wide range of topics such as reconnaissance; scanning and enumeration; client-side attacks and human weaknesses; hacking database services; Web server and Web application testing; enterprise application testing; wireless penetrating testing; and building penetration test labs. The chapters also include case studies where the tools that are discussed are applied. New to this edition: enterprise application testing, client-side attacks and updates on Metasploit and Backtrack. This book is for people who are interested in penetration testing or professionals engaged in penetration testing. Those working in the areas of database, network, system, or application administration, as well as architects, can gain insights into how penetration testers perform testing in their specific areas of expertise and learn what to expect from a penetration test. This book can also serve as a reference for security or audit professionals. Details current open source penetration testing tools Presents core technologies for each type of testing and the best tools for the job New to this edition: Enterprise application testing, client-side attacks and updates on Metasploit and Backtrack Describes various types of malware, including viruses, worms, user-level RootKits, and kernel-level manipulation, their characteristics and attack method, and how to defend against an attack.

A handbook of survival and warfare for the citizens of Woodstock Nation A classic of counterculture literature and one of the most influential--and controversial--documents of the twentieth century, Steal This Book is as valuable today as the day it was published. It has been in print continuously for more than four decades, and it has educated and inspired countless thousands of young activists. Conceived as an instruction manual for radical social change, Steal This Book is divided into three sections--Survive! Fight! and Liberate! Ever wonder how to start a guerilla radio station? Or maybe you want to brush up on your shoplifting techniques. Perhaps you're just looking for the best free entertainment in New York City. (The Frick Collection--"Great when you're stoned.") Packed with information, advice, and Abbie's unique outlaw wisdom ("Avoid all needle drugs--the only dope worth shooting is Richard Nixon."), Steal This Book is a timeless reminder that, no matter what the struggle, freedom is always worth fighting for. "All Power to the Imagination was his credo. Abbie was the best."--Studs Terkel

Dissecting the Hack: The V3rb0t3n Network ventures further into cutting-edge techniques and methods than its predecessor, Dissecting the Hack: The F0rb1dd3n Network. It forgoes the basics and delves straight into the action, as our heroes are chased around the world in a global race against the clock. The danger they face will forever reshape their lives and the price they pay for their actions will not only affect themselves, but could possibly shake the foundations of an entire nation. The book is divided into two parts. The first part, entitled "The V3rb0t3n Network," continues the fictional story of Bob and Leon, two hackers caught up in an adventure in which they learn the deadly consequence of digital actions. The second part, "Security Threats Are Real" (STAR), focuses on these real-world lessons and advanced techniques, as used by characters in the story. This gives the reader not only textbook knowledge, but real-world context around how cyber-attacks may manifest. "The V3rb0t3n Network" can be read as a stand-alone story or as an illustration of the issues described in STAR. Scattered throughout "The V3rb0t3n Network" are "Easter eggs"—references, hints, phrases, and more that will lead readers to insights into hacker culture. Drawing on "The V3rb0t3n Network," STAR explains the various aspects of reconnaissance; the scanning phase of an attack; the attacker's search for network weaknesses and vulnerabilities to exploit; the various angles of attack used by the characters in the story; basic methods of erasing information and obscuring an attacker's presence on a computer system; and the underlying hacking culture. All new volume of Dissecting the Hack by Jayson Street, with technical edit by Brian Martin Uses actual hacking and security tools in its story – helps to familiarize readers with the many devices and their code Features cool new hacks and social engineering techniques, in real life context for ease of learning

As global society becomes more and more dependent, politically and economically, on the flow of information, the power of those who can disrupt and manipulate that flow also increases. In Hacktivism and Cyberwars Tim Jordan and Paul Taylor provide a detailed history of hacktivism's evolution from early hacking culture to its present day status as the radical face of online politics. They describe the ways in which hacktivism has re-appropriated hacking techniques to create an innovative new form of political protest. A full explanation is given of the different strands of hacktivism and the 'cyberwars' it has created, ranging from such avant garde groups as the Electronic Disturbance Theatre to more virtually

focused groups labelled 'The Digitally Correct'. The full social and historical context of hacktivism is portrayed to take into account its position in terms of new social movements, direct action and its contribution to the globalization debate. This book provides an important corrective flip-side to mainstream accounts of E-commerce and broadens the conceptualization of the internet to take into full account the other side of the digital divide.

This book gives detailed instructions on how to use, optimize, and troubleshoot mod_perl. It shows how to get this Apache module running quickly and easily.

Computer Security: Principles and Practice, 2e, is ideal for courses in Computer/Network Security. In recent years, the need for education in computer security and related topics has grown dramatically – and is essential for anyone studying Computer Science or Computer Engineering. This is the only text available to provide integrated, comprehensive, up-to-date coverage of the broad range of topics in this subject. In addition to an extensive pedagogical program, the book provides unparalleled support for both research and modeling projects, giving students a broader perspective. The Text and Academic Authors Association named Computer Security: Principles and Practice, 1e, the winner of the Textbook Excellence Award for the best Computer Science textbook of 2008.

Metasploit Toolkit for Penetration Testing, Exploit Development, and Vulnerability Research is the first book available for the Metasploit Framework (MSF), which is the attack platform of choice for one of the fastest growing careers in IT security: Penetration Testing. The book will provide professional penetration testers and security researchers with a fully integrated suite of tools for discovering, running, and testing exploit code. This book discusses how to use the Metasploit Framework (MSF) as an exploitation platform. The book begins with a detailed discussion of the three MSF interfaces: msfweb, msfconsole, and msfcli. This chapter demonstrates all of the features offered by the MSF as an exploitation platform. With a solid understanding of MSF's capabilities, the book then details techniques for dramatically reducing the amount of time required for developing functional exploits. By working through a real-world vulnerabilities against popular closed source applications, the reader will learn how to use the tools and MSF to quickly build reliable attacks as standalone exploits. The section will also explain how to integrate an exploit directly into the Metasploit Framework by providing a line-by-line analysis of an integrated exploit module. Details as to how the Metasploit engine drives the behind-the-scenes exploitation process will be covered, and along the way the reader will come to understand the advantages of exploitation frameworks. The final section of the book examines the Meterpreter payload system and teaches readers to develop completely new extensions that will integrate fluidly with the Metasploit Framework. A November 2004 survey conducted by "CSO Magazine" stated that 42% of chief security officers considered penetration testing to be a security priority for their organizations. The Metasploit Framework is the most popular open source exploit platform, and there are no competing books.

Hands-On Ethical Hacking and Network Defense, Second Edition provides an in-depth understanding of how to effectively protect computer networks. This book describes the tools and penetration testing methodologies used by ethical hackers and provides a thorough discussion of what and who an ethical hacker is and how important they are in protecting corporate and government data from cyber attacks. Readers are provided with updated computer security resources that describe new vulnerabilities and innovative methods to protect networks. Also included is a thorough update of federal and state computer crime laws, as well as changes in penalties for illegal computer hacking. With cyber-terrorism and corporate espionage threatening the fiber of our world, the need for trained network security professionals continues to grow. Hands-On Ethical Hacking and Network Defense, Second Edition provides a structured knowledge base to prepare readers to be security professionals who understand how to protect a network by using the skills and tools of an ethical hacker. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

Empowers network and system administrators to defend their information and computing assets. This guide presents explanations of destructive hacker tools and tactics - and specific counter measures for both UNIX and Windows environments. It provides information about how hackers build elegant attacks from simple building blocks, and more.

This text covers all the basic concepts and tools Unix/Linux users need to master: Unix vs Linux, GUIs, the command line interface, the online manual, syntax, the shell, standard I/O and redirection, pipes and filters, vi and Emacs, the Unix file system, and job control. Hahn offers a thoroughly readable approach to teaching Unix & Linux by emphasizing core ideas and carefully explaining unfamiliar terminology. The book walks readers through Unix & Linux systems from the very beginning, assuming no prior knowledge, and laying out material in a logical, straightforward manner.

Suddenly your Web server becomes unavailable. When you investigate, you realize that a flood of packets is surging into your network. You have just become one of the hundreds of thousands of victims of a denial-of-service attack, a pervasive and growing threat to the Internet. What do you do? Internet Denial of Service sheds light on a complex and fascinating form of computer attack that impacts the confidentiality, integrity, and availability of millions of computers worldwide. It tells the network administrator, corporate CTO, incident responder, and student how DDoS attacks are prepared and executed, how to think about DDoS, and how to arrange computer and network defenses. It also provides a suite of actions that can be taken before, during, and after an attack. Inside, you'll find comprehensive information on the following topics: How denial-of-service attacks are waged How to improve your network's resilience to denial-of-service attacks What to do when you are involved in a denial-of-service attack The laws that apply to these attacks and their implications How often denial-of-service attacks occur, how strong they are, and the kinds of damage they can cause Real examples of denial-of-service attacks as experienced by the attacker, victim, and unwitting accomplices The authors' extensive experience in handling denial-of-service attacks and researching defense approaches is laid out clearly in practical, detailed terms.

A handy reference guide for data analysts and data scientists to help to obtain value from big data analytics using Spark on Hadoop clusters. About This Book This book is based on the latest 2.0 version of Apache Spark and 2.7 version of Hadoop integrated with most commonly used tools. Learn all Spark stack components including latest topics such as DataFrames, DataSets, GraphFrames, Structured Streaming, DataFrame based ML Pipelines and SparkR. Integrations with frameworks such as HDFS, YARN and tools such as Jupyter, Zeppelin, NiFi, Mahout, HBase Spark Connector, GraphFrames, H2O and Hivemall. Who This Book Is For Though this book is primarily aimed at data analysts and data scientists, it will also help architects, programmers, and practitioners. Knowledge of either Spark or Hadoop would be beneficial. It is assumed that you have basic programming background in Scala, Python, SQL, or R programming with basic Linux experience. Working experience within big data environments is not mandatory. What You Will Learn Find out and implement the tools and techniques of big data analytics using Spark on Hadoop clusters with wide variety of tools used with Spark and Hadoop Understand all the Hadoop and Spark ecosystem components Get to know all the Spark components: Spark Core, Spark SQL, DataFrames, DataSets, Conventional and Structured Streaming, MLLib, ML Pipelines and Graphx See batch and real-time data analytics using Spark Core, Spark SQL, and Conventional and Structured Streaming Get to grips with data science and machine learning using MLLib, ML Pipelines, H2O, Hivemall, Graphx, SparkR and Hivemall. In Detail Big Data Analytics book aims at providing the fundamentals of Apache Spark and Hadoop. All Spark components – Spark Core, Spark SQL, DataFrames, Data sets, Conventional Streaming, Structured Streaming, MLLib, Graphx and Hadoop core components – HDFS, MapReduce and Yarn are explored in greater depth with implementation examples on Spark + Hadoop clusters. It is moving away from MapReduce to Spark. So, advantages of Spark over MapReduce are explained at great depth to reap

benefits of in-memory speeds. DataFrames API, Data Sources API and new Data set API are explained for building Big Data analytical applications. Real-time data analytics using Spark Streaming with Apache Kafka and HBase is covered to help building streaming applications. New Structured streaming concept is explained with an IOT (Internet of Things) use case. Machine learning techniques are covered using MLLib, ML Pipelines and SparkR and Graph Analytics are covered with GraphX and GraphFrames components of Spark. Readers will also get an opportunity to get started with web based notebooks such as Jupyter, Apache Zeppelin and data flow tool Apache NiFi to analyze and visualize data. Style and approach This step-by-step pragmatic guide will make life easy no matter what your level of experience. You will deep dive into Apache Spark on Hadoop clusters through ample exciting real-life examples. Practical tutorial explains data science in simple terms to help programmers and data analysts get started with Data Science

[Copyright: 2421b445775efc58130b24e1a7d5ba8b](#)