Guida Al Pentesting Con Parrot Security Os

A practical guide to testing your infrastructure security with Kali Linux, the preferred choice of pentesters and hackers Key FeaturesEmploy advanced pentesting techniques with Kali Linux to build highly secured systemsDiscover various stealth techniques to remain undetected and defeat modern infrastructuresExplore red teaming techniques to exploit secured environmentBook Description This book takes you, as a tester or security practitioner, through the reconnaissance, vulnerability assessment, exploitation, privilege escalation, and post-exploitation activities used by pentesters. To start with, you'll use a laboratory environment to validate tools and techniques, along with an application that supports a collaborative approach for pentesting. You'll then progress to passive reconnaissance with open source intelligence and active reconnaissance of the external and internal infrastructure. You'll also focus on how to select, use, customize, and interpret the results from different vulnerability scanners, followed by examining specific routes to the target, which include bypassing physical security and the exfiltration of data using a variety of techniques. You'll discover concepts such as social engineering, attacking wireless networks, web services, and embedded devices. Once you are confident with these topics, you'll learn the practical aspects of attacking user client systems by backdooring with fileless techniques, followed by focusing on the most vulnerable part of the network – directly attacking the end user. By the end of this book, you'll have explored approaches for carrying out advanced pentesting in tightly secured environments, understood pentesting and hacking techniques employed on embedded peripheral devices. What you will learnConfigure the most effective Kali Linux tools to test infrastructure securityEmploy stealth to avoid detection in the infrastructure being testedRecognize when stealth attacks are being used against your infrastructureExploit networks and data systems using wired and wireless networks as well as web servicesIdentify and download valuable data from target systemsMaintain access to compromised systemsUse social engineering to compromise the weakest part of the network - the end usersWho this book is for This third edition of Mastering Kali Linux for Advanced Penetration Testing is for you if you are a security analyst, pentester, ethical hacker, IT professional, or security consultant wanting to maximize the success of your infrastructure testing using some of the advanced features of Kali Linux. Prior exposure of penetration testing and ethical hacking basics will be helpful in making the most out of this book.

Penetration testers simulate cyber attacks to find security weaknesses in networks, operating systems, and applications. Information security experts worldwide use penetration techniques to evaluate enterprise defenses. In Penetration Testing, security expert, researcher, and trainer Georgia Weidman introduces you to the core skills and techniques that every pentester needs. Using a virtual machine–based lab that includes Kali Linux and vulnerable operating systems, you'll run through a series of practical lessons with tools like Wireshark, Nmap, and Burp Suite. As you follow along with the labs and launch attacks, you'll experience the key stages of an actual assessment—including information gathering, finding exploitable vulnerabilities, gaining access to systems, post exploitation, and more. Learn how to: –Crack passwords and wireless network keys with brute-forcing and wordlists –Test web applications for vulnerabilities –Use the Metasploit Framework to launch exploits and write your own

Metasploit modules –Automate social-engineering attacks –Bypass antivirus software –Turn access to one machine into total control of the enterprise in the post exploitation phase You'll even explore writing your own exploits. Then it's on to mobile hacking—Weidman's particular area of research—with her tool, the Smartphone Pentest Framework. With its collection of hands-on lessons that cover key tools and strategies, Penetration Testing is the introduction that every aspiring hacker needs.
More than 160 tales from eighty tribal groups gives us a rich and lively panorama of the Native American mythic heritage. From across the continent comes tales of creation and love; heroes and war; animals, tricksters, and the end of the world. In addition to mining the best folkloric sources of the nineteenth century, the editors have also included a broad selection of contemporary Native American voices. With black-and-white illustrations throughout Selected and edited by Richard Erdoes and Alfonso Ortiz Part of the Pantheon Fairy Tale and Folklore Library
Outlining the main methods and techniques available to ornithologists, this book brings together in one authoritative source contributions containing information on avian ecology and conservation.
Invent Your Own Computer Games with Python, 4E
American Indian Myths and Legends
A Cookbook for Hackers, Forensic Analysts, Penetration Testers and Security Engineers
Android Security Cookbook

Hacklog, Volume 2: Web Hacking
With a New Chapter and Updated Epilogue on Coronavirus A Financial Times Best Health Book of 2019 and a New York Times Book Review Editors ' Choice "Honigsbaum does a superb job covering a century ' s worth of pandemics and the fears they invariably unleash." —Howard Markel, MD, PhD, director of the Center for the History of Medicine, University of Michigan How can we understand the COVID-19 pandemic? Ever since the 1918 Spanish influenza pandemic, scientists have dreamed of preventing such catastrophic outbreaks of infectious disease. Yet despite a century of medical progress, viral and bacterial disasters continue to take us by surprise, inciting panic and dominating news cycles. In The Pandemic Century, a lively account of scares both infamous and less known, medical historian Mark Honigsbaum combines reportage with the history of science and medical sociology to artfully reconstruct epidemiological mysteries and the ecology of infectious diseases. We meet dedicated disease detectives, obstructive or incompetent public health officials, and brilliant scientists often blinded by their own knowledge of bacteria and viruses—and see how fear of disease often exacerbates racial, religious, and ethnic tensions. Now updated with a new chapter and epilogue.
Guida Al Pentesting Con Parrot Security OSCreatespace Independent Publishing Platform
This is an easy-to-follow guide, full of hands-on and real-world examples of applications. Each of the vulnerabilities discussed in the book is accompanied with the practical approach to the vulnerability, and the underlying security issue. This book is intended for all those who are looking to get started in Android security or Android application penetration testing. You don ' t need to be an Android developer to learn from this book, but it is highly recommended that developers have some experience in order to learn how to create secure applications for Android.

This revised edition includes a New Intergalactic Introduction by the Author. Mary Daly's New Intergalactic Introduction explores her process as a Crafty Pirate on the Journey of Writing Gyn/Ecology and reveals the autobiographical context of this "Thunderbolt of Rage" that she first hurled against the patriarchs in 1979 and no hurls again in the Re-Surging Movement of Radical Feminism in the Be-Dazzling Nineties.

Hacking Is the Most Important Skill Set of the 21st Century!

The Car Hacker's Handbook

Manuale sulla Sicurezza Informatica e Hacking Etico

A Handbook of Techniques

Gyn/Ecology

A Short and Cheerful Guide

A practical guide to testing your network's security with Kali Linux, the preferred choice of penetration testers and hackers. About This Book Employ advanced pentesting techniques with Kali Linux to build highly-secured systems Get to grips with various stealth techniques to remain undetected and defeat the latest defenses and follow proven approaches Select and configure the most effective tools from Kali Linux to test network security and prepare your business against malicious threats and save costs Who This Book Is For Penetration Testers, IT professional or a security consultant who wants to maximize the success of your network testing using some of the advanced features of Kali Linux, then this book is for you.Some prior exposure to basics of penetration testing/ethical hacking would be helpful in making the most out of this title. What You Will Learn Select and configure the most effective tools from Kali Linux to test network security Employ stealth to avoid detection in the network being tested Recognize when stealth attacks are being used against your network Exploit networks and data systems using wired and wireless networks as well as web services Identify and download valuable data from target systems Maintain access to compromised systems Use social engineering to compromise the weakest part of the network—the end users In Detail This book will take you, as a tester or security practitioner through the journey of reconnaissance, vulnerability assessment, exploitation, and post-exploitation activities used by penetration testers and hackers. We will start off by using a laboratory environment to validate tools and techniques, and using an application that supports a collaborative approach to penetration testing. Further we will get acquainted with passive reconnaissance with open source intelligence and active reconnaissance of the external and internal networks. We will also focus on how to select, use, customize, and interpret the results from a variety of different vulnerability scanners. Specific routes to the target will also be examined, including bypassing physical security and exfiltration of data using different techniques. You will also get to grips with concepts such as social engineering, attacking wireless networks, exploitation of web applications and remote access connections. Later you will learn the practical aspects of attacking user client systems by backdooring executable files. You will focus on the most vulnerable part of the network—directly and bypassing the controls, attacking the end user and maintaining persistence access through social media. You will also explore approaches to carrying out advanced penetration testing in tightly secured environments, and the book's hands-on approach will help you understand everything you need to know during a Red teaming exercise or penetration testing Style and approach An advanced level tutorial that follows a practical approach and proven methods to maintain top notch security of your networks.

Here is the ultimate book on the worldwide movement of hackers, pranksters, and activists that operates under the non-name Anonymous, by the writer the Huffington Post says "knows all of Anonymous' deepest, darkest secrets." Half a dozen years ago, anthropologist Gabriella Coleman set out to study the rise of this global phenomenon just as some of its members were

turning to political protest and dangerous disruption (before Anonymous shot to fame as a key player in the battles over WikiLeaks, the Arab Spring, and Occupy Wall Street). She ended up becoming so closely connected to Anonymous that the tricky story of her inside–outside status as Anon confidante, interpreter, and erstwhile mouthpiece forms one of the themes of this witty and entirely engrossing book. The narrative brims with details unearthed from within a notoriously mysterious subculture, whose semi-legendary tricksters—such as Topiary, tflow, Anachaos, and Sabu—emerge as complex, diverse, politically and culturally sophisticated people. Propelled by years of chats and encounters with a multitude of hackers, including imprisoned activist Jeremy Hammond and the double agent who helped put him away, Hector Monsegur, Hacker, Hoaxer, Whistleblower, Spy is filled with insights into the meaning of digital activism and little understood facets of culture in the Internet age, including the history of "trolling," the ethics and metaphysics of hacking, and the origins and manifold meanings of "the lulz."

M.J. Holliday and her crew interrupt the frantic schedule of their reality TV show, Ghoul Getters, and hotfoot it to New Mexico, where a dreadful demon is waging tribal warfare. Same Whitefeather- M.J.'s spirit guide-urgently needs her help to stop this evil spirit from wiping out the descendants of his tribe. It doesn't take a psychic to predict that M.J.'s going to have a devil of a time making New Mexico a demon-free zone.

Invent Your Own Computer Games with Python will teach you how to make computer games using the popular Python programming language—even if you've never programmed before! Begin by building classic games like Hangman, Guess the Number, and Tic-Tac-Toe, and then work your way up to more advanced games, like a text-based treasure hunting game and an animated collision-dodging game with sound effects. Along the way, you'll learn key programming and math concepts that will help you take your game programming to the next level. Learn how to: –Combine loops, variables, and flow control statements into real working programs –Choose the right data structures for the job, such as lists, dictionaries, and tuples –Add graphics and animation to your games with the pygame module –Handle keyboard and mouse input –Program simple artificial intelligence so you can play against the computer –Use cryptography to convert text messages into secret code –Debug your programs and find common errors As you work through each game, you'll build a solid foundation in Python and an understanding of computer science fundamentals. What new game will you create with the power of Python? The projects in this book are compatible with Python 3.

Pocket Style Manual

Penetration Testing

Google Hacking for Penetration Testers

Collecting Data from the Modern Web

Where the Red Fern Grows

Bird Ecology and Conservation

The legendary comedian, actor, and writer of Monty Python, Fawlty Towers, and A Fish Called Wanda fame shares his key ideas about creativity: that it's a learnable, improvable skill. "Many people have written about creativity, but although they were very, very clever, they weren't actually creative. I like to think I'm writing about it from the inside."—John Cleese You might think that creativity is some mysterious, rare gift—one that only a few possess. But you'd be wrong. As John Cleese shows in this short, practical, and often amusing guide, creativity is a skill that anyone can acquire. Drawing on his lifelong experience as a writer, Cleese shares his insights into the nature of creativity and offers advice on how to get your own inventive juices flowing. What do you need to do to get yourself in the right frame of mind?

When do you know that you've come up with an idea that might be worth pursuing? What should you do if you think you've hit a brick wall? We can all be more creative. John Cleese shows us how.

Android Security Cookbook' breaks down and enumerates the processes used to exploit and remediate Android app security vulnerabilities in the form of detailed recipes and walkthroughs. Android Security Cookbook is aimed at anyone who is curious about Android app security and wants to be able to take the necessary practical measures to protect themselves; this means that Android application developers, security researchers and analysts, penetration testers, and generally any CIO, CTO, or IT managers facing the impeding onslaught of mobile devices in the business environment will benefit from reading this book.

From the acclaimed New York Times bestselling author: An essential volume for generations of writers young and old. The twenty-fifth anniversary edition of this modern classic will continue to spark creative minds for years to come. For a quarter century, more than a million readers—scribes and scribblers of all ages and abilities—have been inspired by Anne Lamott's hilarious, big-hearted, homespun advice. Advice that begins with the simple words of wisdom passed down from Anne's father—also a writer—in the iconic passage that gives the book its title: "Thirty years ago my older brother, who was ten years old at the time, was trying to get a report on birds written that he'd had three months to write. It was due the next day. We were out at our family cabin in Bolinas, and he was at the kitchen table close to tears, surrounded by binder paper and pencils and unopened books on birds, immobilized by the hugeness of the task ahead. Then my father sat down beside him, put his arm around my brother's shoulder, and said, 'Bird by bird, buddy. Just take it bird by bird.'"

2018 version of the OSINT Tools and Resources Handbook. This version is almost three times the size of the last public release in 2016. It reflects the changing intelligence needs of our clients in both the public and private sector, as well as the many areas we have been active in over the past two years.

Manual of Parrot Behavior

The Linux Kernel Module Programming Guide

A Guide for the Penetration Tester

The Many Faces of Anonymous

A Hands-On Introduction to Hacking

An Introduction to Creative Problem Solving

From the author of the New York Times bestseller The Inevitable— a sweeping vision of technology as a living force that can expand our individual potential In this provocative book, one of today's most respected thinkers turns the conversation about technology on its head by viewing technology as a natural system, an extension of biological evolution. By mapping the behavior of life, we paradoxically get a glimpse at where technology is headed-or "what it wants." Kevin Kelly offers a dozen trajectories in the coming decades for this near-living system. And as we align ourselves with technology's agenda, we can

capture its colossal potential. This visionary and optimistic book explores how technology gives our lives greater meaning and is a must-read for anyone curious about the future.

Learn web scraping and crawling techniques to access unlimited data from any web source in any format. With this practical guide, you'll learn how to use Python scripts and web APIs to gather and process data from thousands—or even millions—of web pages at once. Ideal for programmers, security professionals, and web administrators familiar with Python, this book not only teaches basic web scraping mechanics, but also delves into more advanced topics, such as analyzing raw data or using scrapers for frontend website testing. Code samples are available to help you understand the concepts in practice. Learn how to parse complicated HTML pages Traverse multiple pages and sites Get a general overview of APIs and how they work Learn several methods for storing the data you scrape Download, read, and extract data from documents Use tools and techniques to clean badly formatted data Read and write natural languages Crawl through forms and logins Understand how to scrape JavaScript Learn image processing and text recognition

The real challenge of programming isn't learning a language's syntax—it's learning to creatively solve problems so you can build something great. In this one-of-a-kind text, author V. Anton Spraul breaks down the ways that programmers solve problems and teaches you what other introductory books often ignore: how to Think Like a Programmer. Each chapter tackles a single programming concept, like classes, pointers, and recursion, and open-ended exercises throughout challenge you to apply your knowledge. You'll also learn how to: -Split problems into discrete components to make them easier to solve -Make the most of code reuse with functions, classes, and libraries -Pick the perfect data structure for a particular job -Master more advanced programming tools like recursion and dynamic memory -Organize your thoughts and develop strategies to tackle particular types of problems Although the book's examples are written in C++, the creative problem-solving concepts they illustrate go beyond any particular language; in fact, they often reach outside the realm of computer science. As the most skillful programmers know, writing great code is a creative art—and the first step in creating your masterpiece is learning to Think Like a Programmer.

Life of Pi is a masterful and utterly original novel that is at once the story of a young castaway who faces immeasurable hardships on the high seas, and a meditation on religion, faith, art and life that is as witty as it is profound. Using the threads of all of our best stories, Yann Martel has woven a glorious spiritual adventure that makes us question what it means to be alive, and to believe.

Mastering Kali Linux for Advanced Penetration Testing

China's Secret Strategy to Replace America as the Global Superpower

The Last Lecture

The House of the Spirits

Pathology of Pet and Aviary Birds

Fierce Invalids Home From Hot Climates

A free, world-class education for anyone, anywhere. This is the goal of the Khan

Academy, a passion project that grew from an ex-engineer and hedge funder's online tutoring sessions with his niece, who was struggling with algebra, into a worldwide phenomenon. Today millions of students, parents, and teachers use the Khan Academy's free videos and software, which have expanded to encompass nearly every conceivable subject; and Academy techniques are being employed with exciting results in a growing number of classrooms around the globe. Like many innovators, Khan rethinks existing assumptions and imagines what education could be if freed from them. And his core idea-liberating teachers from lecturing and state-mandated calendars and opening up class time for truly human interaction-has become his life's passion. Schools seek his advice about connecting to students in a digital age, and people of all ages and backgrounds flock to the site to utilize this fresh approach to learning. In THE ONE WORLD SCHOOLHOUSE, Khan presents his radical vision for the future of education, as well as his own remarkable story, for the first time. In these pages, you will discover, among other things: How both students and teachers are being bound by a broken top-down model invented in Prussia two centuries ago Why technology will make classrooms more human and teachers more important How and why we can afford to pay educators the same as other professionals How we can bring creativity and true human interactivity back to learning Why we should be very optimistic about the future of learning. Parents and politicians routinely bemoan the state of our education system. Statistics suggest we've fallen behind the rest of the world in literacy, math, and sciences. With a shrewd reading of history, Khan explains how this crisis presented itself, and why a return to "mastery learning," abandoned in the twentieth century and ingeniously revived by tools like the Khan Academy, could offer the best opportunity to level the playing field, and to give all of our children a world-class education now. More than just a solution, THE ONE WORLD SCHOOLHOUSE serves as a call for free, universal, global education, and an explanation of how Khan's simple yet revolutionary thinking can help achieve this inspiring goal. Violent Python shows you how to move from a theoretical understanding of offensive computing concepts to a practical implementation. Instead of relying on another attacker's tools, this book will teach you to forge your own weapons using the Python programming language. This book demonstrates how to write Python scripts to automate large-scale network attacks, extract metadata, and investigate forensic artifacts. It also shows how to write code to intercept and analyze network traffic using Python, craft and spoof wireless frames to attack wireless and Bluetooth devices, and how to data-mine popular social media websites and evade modern anti-virus. Demonstrates how to write Python scripts to automate large-scale network attacks, extract metadata, and investigate forensic artifacts Write code to intercept and analyze network traffic using Python. Craft and spoof wireless frames to attack wireless and Bluetooth devices Data-mine popular social media websites and evade modern anti-virus One of the U.S. government's leading China experts reveals the hidden strategy fueling that country's rise – and how Americans have been seduced into helping China overtake us as the world's leading superpower. For more than forty years, the United States has played an indispensable role helping the Chinese

government build a booming economy, develop its scientific and military capabilities, and take its place on the world stage, in the belief that China's rise will bring us cooperation, diplomacy, and free trade. But what if the "China Dream" is to replace us, just as America replaced the British Empire, without firing a shot? Based on interviews with Chinese defectors and newly declassified, previously undisclosed national security documents, The Hundred-Year Marathon reveals China's secret strategy to supplant the United States as the world's dominant power, and to do so by 2049, the one-hundredth anniversary of the founding of the People's Republic. Michael Pillsbury, a fluent Mandarin speaker who has served in senior national security positions in the U.S. government since the days of Richard Nixon and Henry Kissinger, draws on his decades of contact with the "hawks" in China's military and intelligence agencies and translates their documents, speeches, and books to show how the teachings of traditional Chinese statecraft underpin their actions. He offers an inside look at how the Chinese really view America and its leaders – as barbarians who will be the architects of their own demise. Pillsbury also explains how the U.S. government has helped – sometimes unwittingly and sometimes deliberately – to make this "China Dream" come true, and he calls for the United States to implement a new, more competitive strategy toward China as it really is, and not as we might wish it to be. The Hundred-Year Marathon is a wake-up call as we face the greatest national security challenge of the twenty-first century.

Descrizione In questo manuale viene spiegato come effettuare un test di intrusione nei confronti di un sistema, una rete o una applicazione Web. Dopo aver presentato qualche indispensabile nozione teorica, ogni attacco viene descritto 'lato hacker', partendo da un approccio pi semplice possibile per poi arrivare ad un livello avanzato della procedura; il tutto spiegato in maniera esaustiva e analizzando ogni passaggio. A chi rivolto il libro Destinatari di questo testo sono tutti coloro che vogliono saperne di pi in fatto di Cyber Security applicata, abbiano un minimo di cultura informatica e siano incuriositi dalle potenzialit del mondo Unix-like; il testo, tuttavia, pu risultare utile anche al Pentester o al responsabile IT professionista, che avr a disposizione un repertorio di scenari e attacchi tipici da poter consultare rapidamente. Argomenti trattati Introduzione al Pentesting Information gathering Vulnerability assessment Exploitation Privilege escalation Post exploitation Reporting Comandi principali terminale Linux e Unix-like

Bird by Bird

Hacker, Hoaxer, Whistleblower, Spy

Blackwood's Edinburgh magazine

IoT Penetration Testing Cookbook

A Ghost Hunter Mystery

Actionable Gamification

Hacklog, Volume 2: Web Hacking è il secondo volume pensato per l'apprendimento della Sicurezza Informatica ed Ethical Hacking. È stato ideato per far in modo che tutti, sia i professionisti che i principianti, riescano ad apprendere i meccanismi e i metodi che

stanno alla base degli attacchi ad Infrastrutture e Applicazioni nel World Wide Web. Hacklog, Volume 2: Web Hacking è un volume stand-alone: non è necessario aver letto il Volume 1, sebbene possa essere molto d'aiuto nelle fasi ritenute ormai consolidate (come l'uso di strumenti di anonimizzazione che precedono un attacco informatico). Non richiede particolari abilità o conoscenze e può essere letto da tutti, sia dall'appassionato che dall'esperto. In questo corso imparerai ad analizzare un'infrastruttura Web, a conoscerne le debolezze che si celano dietro errate configurazioni e a trovare e sfruttare vulnerabilità presenti nelle Web App di ogni giorno, esponendosi giornalmente al cyber-crimine della rete. Sarai in grado di creare un ambiente di test personalizzato in cui effettuare attacchi in tutta sicurezza e studiarne le caratteristiche, scrivere brevi exploit e infettare macchine; quindi, ti verrà insegnato come difenderti da questi attacchi, mitigando le vulnerabilità più comuni, e sanificare l'ambiente infetto. Hacklog, Volume 2: Web Hacking è un progetto rilasciato in Creative Commons 4.0 Italia, volto all'apprendimento e alla comunicazione libera per tutti. La versione cartacea è disponibile con fini promozionali e non ha nulla di diverso da quella presente in formato digitale, distribuita gratuitamente in rete. -- IMPORTANTE -- Leggi prima di acquistare: questo libro è disponibile gratuitamente in rete. La versione qui presente fa riferimento solo alla versione Kindle (obbligatoriamente imposto da Amazon a pagamento) e alla versione cartacea. Se vuoi puoi scaricare gratuitamente questo ebook direttamente sul nostro sito ufficiale. Acquistandolo, finanzierai il progetto e con esso i prossimi volumi. Attenzione: il corso Hacklog, Volume 2: Web Hacking prevede l'uso del Sistema Operativo Debian GNU/Linux. Se non hai mai utilizzato questo Sistema Operativo, ti consigliamo caldamente di seguire il breve corso introduttivo che lo riguarda scaricabile sul sito ufficiale www.hacklog.net. Gratuito, ovviamente.

Learn all about implementing a good gamification design into your products, workplace, and lifestyle Key Features Explore what makes a game fun and engaging Gain insight into the Octalysis Framework and its applications Discover the potential of the Core Drives of gamification through real-world scenarios Book Description Effective gamification is a combination of game design, game dynamics, user experience, and ROI-driving business implementations. This book explores the interplay between these disciplines and captures the core principles that contribute to a good gamification design. The book starts with an overview of the Octalysis Framework and the 8 Core Drives that can be used to build strategies around the various systems that make games engaging. As the book progresses, each chapter delves deep into a Core Drive, explaining its design and how it should be used. Finally, to apply all the concepts and techniques that you learn throughout, the book contains a brief showcase of using the Octalysis Framework to design a project experience from scratch. After reading this book, you'll have the knowledge and skills to enable the widespread adoption of good gamification and human-focused design in all types of industries. What you will learn

Discover ways to use gamification techniques in real-world situations Design fun, engaging, and rewarding experiences with Octalysis Understand what gamification means and how to categorize it Leverage the power of different Core Drives in your applications Explore how Left Brain and Right Brain Core Drives differ in motivation and design methodologies Examine the fascinating intricacies of White Hat and Black Hat Core Drives Who this book is for Anyone who wants to implement gamification principles and techniques into their products, workplace, and lifestyle will find this book useful.

“As clever and witty a novel as anyone has written in a long time . . . Robbins takes readers on a wild, delightful ride. . . . A delight from beginning to end.”—Buffalo News Switters is a contradiction for all seasons: an anarchist who works for the government; a pacifist who carries a gun; a vegetarian who sops up ham gravy; a cyberwhiz who hates computers; a man who, though obsessed with the preservation of innocence, is aching to deflower his high-school-age stepsister (only to become equally enamored of a nun ten years his senior). Yet there is nothing remotely wishy-washy about Switters. He doesn’t merely pack a pistol. He is a pistol. And as we dog Switters’s strangely elevated heels across four continents, in and out of love and danger, discovering in the process the “true” Third Secret of Fatima, we experience Tom Robbins—that fearless storyteller, spiritual renegade, and verbal break dancer—at the top of his game. On one level this is a fast-paced CIA adventure story with comic overtones; on another it’s a serious novel of ideas that brings the Big Picture into unexpected focus; but perhaps more than anything else, Fierce Invalids is a sexy celebration of language and life. Praise for Fierce Invalids Home From Hot Climates “Superb.”—New York Post “Dangerous? Wicked? Forbidden? You bet. . . . Pour yourself a bowl of chips and dig in.”—Daily News, New York “Robbins is a great writer . . . and definitely a provocative rascal.”—The Tennessean “Whoever said truth is stranger than fiction never read a Tom Robbins novel. . . Clever, creative, and witty, Robbins tosses off impassioned observations like handfuls of flower petals.”—San Diego Union-Tribune

"We cannot change the cards we are dealt, just how we play the hand."---Randy Pausch A lot of professors give talks titled "The Last Lecture." Professors are asked to consider their demise and to ruminate on what matters most to them. And while they speak, audiences can't help but mull the same question: What wisdom would we impart to the world if we knew it was our last chance? If we had to vanish tomorrow, what would we want as our legacy? When Randy Pausch, a computer science professor at Carnegie Mellon, was asked to give such a lecture, he didn't have to imagine it as his last, since he had recently been diagnosed with terminal cancer. But the lecture he gave--"Really Achieving Your Childhood Dreams"--wasn't about dying. It was about the importance of overcoming obstacles, of enabling the dreams of others, of seizing every moment (because "time is all you have...and you may find one day that you have less than you think"). It was a summation of everything Randy had come to believe. It was

about living. In this book, Randy Pausch has combined the humor, inspiration and intelligence that made his lecture such a phenomenon and given it an indelible form. It is a book that will be shared for generations to come.

Getting Started Becoming a Master Hacker

Some Instructions on Writing and Life

Education Reimagined

The One World Schoolhouse

Learn Kali Linux 2019

The Metaethics of Radical Feminism

This authoritative reference, the first of its kind, is a necessary addition to the library of any practitioner or behaviorist who sees avain companion animals. Because of their beauty, intelligence, playfulness and ability in mimicry, parrots are the most widely kept companion birds. It is estimated that more than half of the psittacine cases presented to clinicians are the result of behavioral problems-problems inherent to captivity. Bringing together a host of international experts on avian behavior, Manual of Parrot Behavior explores the many facets of psittacine behavior, both normal and abnormal. The book not only provides readers with a solid understanding of the basic principles of psittacine behavior but also offers useful techniques of diagnosis and treatment for specific problems. Covers both normal and abnormal parrot behavior Offers practical techniques on diagnosis and treatment of behavior problems Written by a team of international experts on avian behavior A necessary addition to the library of any practitioner of behaviorist who sees avian companion animals

The Trueba family embodies strong feelings. This family saga starts at the beginning of the 20th century and continues through the assassination of Allende in 1973.

A beloved classic that captures the powerful bond between man and man’s best friend. Billy has long dreamt of owning not one, but two, dogs. So when he’s finally able to save up enough money for two pups to call his own—Old Dan and Little Ann—he’s ecstatic. It doesn’t matter that times are tough; together they’ll roam the hills of the Ozarks. Soon Billy and his hounds become the finest hunting team in the valley. Stories of their great achievements spread throughout the region, and the combination of Old Dan’s brawn, Little Ann’s brains, and Billy’s sheer will seems unbeatable. But tragedy awaits these determined hunters—now friends—and Billy learns that hope can grow out of despair, and that the seeds of the future can come from the scars of the past. Praise for Where the Red Fern Grows A Top 100 Children’s Novel, School Library Journal's A Fuse #8 Production A Must-Read for Kids 9 to 14, NPR Winner of Multiple State Awards Over 7 million copies in print! “Very touching.” —The New York Times Book Review “One of the great classics of children’s literature . . . Any child who doesn’t get to read this beloved and powerfully emotional book has

missed out on an important piece of childhood for the last 40-plus years." —Common Sense Media "An exciting tale of love and adventure you'll never forget." —School Library Journal "A book of unadorned naturalness." —Kirkus Reviews "Written with so much feeling and sentiment that adults as well as children are drawn [in] with a passion." —Arizona Daily Star "It's a story about a young boy and his two hunting dogs and . . . I can't even go on without getting a little misty." —The Huffington Post "We tear up just thinking about it." —Time on the film adaptation

Linux Kernel Module Programming Guide is for people who want to write kernel modules. It takes a hands-on approach starting with writing a small "hello, world" program, and quickly moves from there. Far from a boring text on programming, Linux Kernel Module Programming Guide has a lively style that entertains while it educates. An excellent guide for anyone wishing to get started on kernel module programming. *** Money raised from the sale of this book supports the development of free software and documentation.

Think Like a Programmer

Perform powerful penetration testing using Kali Linux, Metasploit, Nessus, Nmap, and Wireshark

Learning Pentesting for Android Devices

The Hundred-Year Marathon

Creativity

The Pandemic Century: One Hundred Years of Panic, Hysteria, and Hubris

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

The Car Hacker's Handbook your first stop.

Explore the latest ethical hacking tools and techniques in Kali Linux 2019 to perform penetration testing from scratch Key FeaturesGet up and running with Kali Linux 2019.2Gain comprehensive insights into security concepts such as social engineering, wireless network exploitation, and web application attacksLearn to use Linux commands in the way ethical hackers do to gain control of your environmentBook Description The current rise in hacking and security breaches makes it more important than ever to effectively pentest your environment, ensuring endpoint protection. This book will take you through the latest version of Kali Linux and help you use various tools and techniques to efficiently deal with crucial security aspects. Through real-world examples, you'll understand how to set up a lab and later explore core penetration testing concepts. Throughout the course of this book, you'll get up to speed with gathering sensitive information and even discover different vulnerability assessment tools bundled in Kali Linux 2019. In later chapters, you'll gain insights into concepts such as social engineering, attacking wireless networks, exploitation of web applications and remote access connections to further build on your pentesting skills. You'll also focus on techniques such as bypassing controls, attacking the end user and maintaining persistence access through social media. Finally, this pentesting book covers best practices for performing complex penetration testing techniques in a highly secured environment. By the end of this book, you'll be able to use Kali Linux to detect vulnerabilities and secure your system by applying penetration testing techniques of varying complexity. What you will learnExplore the fundamentals of ethical hackingLearn how to install and configure Kali LinuxGet up to speed with performing wireless network pentestingGain insights into passive and active information gatheringUnderstand web application pentesting Decode WEP, WPA, and WPA2 encryptions using a variety of methods, such as the fake authentication attack, the ARP request replay attack, and the dictionary attackWho this book is for If you are an IT security professional or a security consultant who wants to get started with penetration testing using Kali Linux 2019.2, then this book is for you. The book will also help if you're simply looking to learn more about ethical hacking and various security breaches. Although prior knowledge of Kali Linux is not necessary, some understanding of cybersecurity will be useful.

Pathology of Pet and Aviary Birds, Second Edition provides a comprehensive reference to the gross and histologic features of diseases seen in pet and aviary birds, with more than 850 images depicting disease lesions. • Provides a complete resource for identifying both common and not-so-common diseases in a wide range of avian species • Includes more than 850 full-color images to show disease lesions • Offers context for the interpretation of pathologic findings, promoting an understanding of the pathogenesis and epizootiology of disease • Adds information on pigeons and chickens, pathophysiology, prognosis and trends, and globally relevant

diseases • Aids pathologists, diagnosticians, and avian veterinarians in identifying lesions in pet birds

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 reconaissance. • 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.

Web Scraping with Python

Identify vulnerabilities and secure your smart devices

American Psycho

Violent Python

Guida Al Pentesting Con Parrot Security OS

A Novel

A cult classic, adapted into a film starring Christian Bale. Is evil something you are? Or is it something you do? Patrick Bateman has it all: good looks, youth, charm, a job on Wall Street, reservations at every new restaurant in town and a line of girls around the block. He is also a psychopath. A man addicted to his superficial, perfect life, he pulls us into a dark underworld where the American Dream becomes a nightmare . .

. With an introduction by Irvine Welsh, Bret Easton Ellis's American Psycho is one of the most controversial and talked-about novels of all time. A multi-million-copy bestseller hailed as a modern classic, it is a violent black comedy about the darkest side of human nature.

Over 80 recipes to master IoT security techniques. About This Book Identify vulnerabilities in IoT device architectures and firmware using software and hardware pentesting techniques Understand radio communication analysis with concepts such as sniffing the air and capturing radio signals A recipe based guide that will teach you to pentest new and unique set of IoT devices. Who This Book Is For This book targets IoT developers, IoT enthusiasts, pentesters, and security professionals who are interested in learning about IoT security. Prior knowledge of basic pentesting would be beneficial. What You Will Learn Set up an IoT pentesting lab Explore various threat modeling concepts Exhibit the ability to analyze and exploit firmware vulnerabilities Demonstrate the automation of application binary analysis for iOS and Android using MobSF Set up a Burp Suite and use it for web app testing Identify UART and JTAG pinouts, solder headers, and hardware debugging Get solutions to common wireless protocols Explore the mobile security and firmware best practices Master various advanced IoT exploitation techniques and security automation In Detail IoT is an upcoming trend in the IT industry today; there are a lot of IoT devices on the market, but there is a minimal understanding of how to safeguard them. If you are a security enthusiast or pentester, this book will help you understand how to exploit and secure IoT devices. This book follows a recipe-based approach, giving you practical experience in securing upcoming smart devices. It starts with practical recipes on how to analyze IoT device architectures and identify vulnerabilities. Then, it focuses on enhancing your pentesting skill set, teaching you how to exploit a vulnerable IoT device, along with identifying vulnerabilities in IoT device firmware. Next, this book teaches you how to secure embedded devices and exploit smart devices with hardware techniques. Moving forward, this book reveals advanced hardware pentesting techniques, along with software-defined, radio-based IoT pentesting with Zigbee and Z-Wave. Finally, this book also covers how to use new and unique pentesting techniques for different IoT devices, along with smart devices connected to the cloud. By the end of this book, you will have a fair understanding of how to use different pentesting techniques to exploit and secure various IoT devices. Style and approach This recipe-based book will teach you how to use advanced IoT exploitation and security automation.

This tutorial-style book follows upon Occupytheweb's Best Selling "Linux Basics for Hackers" and takes the reader along the next step to becoming a Master Hacker. Occupytheweb offers his unique style to guide the reader through the various professions where hackers are in high demand (cyber intelligence, pentesting, bug bounty, cyber warfare, and many others) and offers the perspective of the history of hacking and the legal framework. This book then guides the reader through the essential skills and tools before offering step-by-step tutorials of the essential tools and techniques of the hacker including reconnaissance, password cracking, vulnerability scanning, Metasploit 5, antivirus evasion, covering your tracks, Python, and social engineering. Where the reader may want a deeper understanding of a particular subject, there are links to more complete articles on a particular subject.Master OTW provides a fresh and unique approach of using the NSA's EternalBlue malware as a case study. The reader is given a glimpse into one of history's most devasting pieces of malware from the vulnerability, exploitation, packet-level analysis and reverse-engineering Python. This section of the book should be enlightening for both the novice and the advanced practioner.Master OTW doesn't just provide tools and techniques, but rather he provides the unique insights into the mindset and strategic thinking of the hacker.This is a must read for anyone considering a career into cyber security!

Life of Pi

Secure your network with Kali Linux 2019.1 – the ultimate white hat hackers' toolkit

What Technology Wants

Beyond Points, Badges, and Leaderboards

Ghoul Interrupted

Open Source Intelligence Tools and Resources Handbook