How To Hack Like A Legend A Hacker S Tale Breaking Into A Secretive Offshore Company Hacking The Planet

Thank you definitely much for downloading **how to hack like a legend a hacker s tale breaking into a secretive offshore company hacking the planet**.Most likely you have knowledge that, people have see numerous time for their favorite books taking into consideration this how to hack like a legend a hacker s tale breaking into a secretive offshore company hacking the planet, but stop stirring in harmful downloads.

Rather than enjoying a good book in imitation of a cup of coffee in the afternoon, instead they juggled considering some harmful virus inside their computer. **how to hack like a legend a hacker s tale breaking into a secretive offshore company hacking the planet** is easy to use in our digital library an online entry to it is set as public consequently you can download it instantly. Our digital library saves in combination countries, allowing you to get the most less latency times to download any of our books next this one. Merely said, the how to hack like a legend a hacker s tale breaking into a secretive offshore company hacking the planet is universally compatible as soon as any devices to read.

Hack//legend of the Twilight 2 - Tatsuya (CRT) Hamazaki 2008-01-03
Shugo and Reina get more than they expected when they begin playing the online game, The World, the most advanced computer game ever created.
Kingpin - Kevin Poulsen 2012-02-07
Former hacker Kevin Poulsen has, over the past decade, built a reputation as one of the top investigative reporters on the cybercrime beat. In Kingpin, he pours his unmatched access and expertise into book form for the first time, delivering a gripping cat-and-mouse narrative—and an unprecedented view into the twenty-first century's signature form of organized crime. The word spread through the hacking underground like some unstoppable new virus: Someone—some brilliant, audacious crook—had just staged a hostile takeover of an online criminal network that siphoned billions of dollars from the US economy. The FBI rushed to launch an ambitious undercover operation aimed at tracking down this new kingpin; other agencies around the world deployed dozens of moles and double agents. Together, the cybercops lured numerous unsuspecting hackers into their clutches. . . . Yet at every turn, their main quarry displayed an uncanny ability to sniff out their snitches and see through their plots. The culprit they sought was the most unlikely of criminals: a brilliant programmer with a hippie ethic and a supervillain's double identity. As prominent "white-hat" hacker Max "Vision" Butler, he was a celebrity throughout the programming world, even serving as a consultant to the FBI. But as the black-hat "Iceman," he found in the world of data theft an irresistible opportunity to test his outsized abilities. He infiltrated thousands of computers around the country, sucking down millions of credit card numbers at will. He effortlessly hacked his fellow hackers, stealing their ill-gotten gains from under their noses. Together with a smooth-talking con artist, he ran a massive real-world crime ring. And for years, he did it all with seeming impunity, even as countless rivals ran afoul of police. Yet as he watched the fraudsters around him squabble, their ranks riddled with infiltrators, their methods inefficient, he began to see in their dysfunction the ultimate challenge: He would stage his coup and fix what was broken, run things as they should be run—even if it meant painting a bull's-eye on his forehead. Through the story of this criminal's remarkable rise, and of law enforcement's quest to track him down, Kingpin lays bare the workings of a silent crime wave still affecting millions of Americans. In these pages, we are ushered into vast online-fraud supermarkets stocked with credit card numbers, counterfeit checks, hacked bank accounts, dead drops, and fake passports. We learn the workings of the numerous hacks—browser exploits, phishing attacks, Trojan horses, and much more—these fraudsters use to ply their trade, and trace the complex routes by which they turn stolen data into millions of dollars. And thanks to Poulsen's remarkable access to both cops and criminals, we step inside the quiet, desperate arms race that law enforcement continues to fight with these scammers today. Ultimately, Kingpin is a journey into an underworld of startling scope and power, one in which ordinary American teenagers work hand in hand with murderous Russian mobsters and where a simple Wi-Fi connection can unleash a torrent of gold worth millions.
Malware, Rootkits & Botnets A Beginner's Guide - Christopher C. Elisan 2012-09-05
Security Smarts for the Self-Guided IT Professional Learn how to improve the security posture of your organization and defend against some of the most pervasive network attacks. Malware, Rootkits & Botnets: A Beginner's Guide explains the nature, sophistication, and danger of these risks and offers best practices for thwarting them. After reviewing the current threat landscape, the book describes the entire threat lifecycle, explaining how cybercriminals create, deploy, and manage the malware, rootkits, and botnets under their control. You'll learn proven techniques for identifying and mitigating these malicious attacks. Templates, checklists, and examples give you the hands-on help you need to get started protecting your network right away. Malware, Rootkits & Botnets: A Beginner's Guide features: Lingo--Common security terms defined so that you're in the know on the job IMHO--Frank and relevant opinions based on the author's years of industry experience Budget Note--Tips for getting security technologies and processes into your organization's budget In Actual Practice--Exceptions to the rules of security explained in real-world contexts Your Plan--Customizable checklists you can use on the job now Into Action--Tips on how, why, and when to apply new skills and techniques at work
Exploding the Phone - Phil Lapsley 2013-02-05
"A rollicking history of the telephone system and the hackers who exploited its flaws." —Kirkus Reviews, starred review Before smartphones, back even before the Internet and personal computers, a misfit group of technophiles, blind teenagers, hippies, and outlaws figured out how to hack the world's largest machine: the telephone system. Starting with Alexander Graham Bell's revolutionary "harmonic telegraph," by the middle of the twentieth century the phone system had grown into something extraordinary, a web of cutting-edge switching machines and human operators that linked together millions of people like never before. But the network had a billion-dollar flaw, and once people discovered it, things would never be the same. Exploding the Phone tells this story in full for the first time. It traces the birth of long-distance communication and the telephone, the rise of AT&T's monopoly, the creation of the sophisticated machines that made it all work, and the discovery of Ma Bell's Achilles' heel. Phil Lapsley expertly weaves together the clandestine underground of "phone phreaks" who turned the network into their electronic playground, the mobsters who exploited its flaws to avoid the feds, the explosion of telephone hacking in the counterculture, and the war between the phreaks, the phone company, and the FBI. The product of extensive original research, Exploding the Phone is a groundbreaking, captivating book that "does for the phone phreaks what Steven Levy's Hackers did for computer pioneers" (Boing Boing). "An authoritative, jaunty and enjoyable account of their sometimes comical, sometimes impressive and sometimes disquieting misdeeds." —The Wall Street Journal "Brilliantly researched." —The Atlantic "A fantastically fun romp through the world of early phone hackers, who sought free long distance, and in the end helped launch the computer era." —The Seattle Times
How to Investigate Like a Rockstar - Sparc Flow 2017-08-17
"There are two kinds of companies: those that have been breached and those that do not know it yet." The company calling us just discovered an anomaly on their most critical systems. Our job is to conduct a deep

forensic analysis, perform threat assessment, and uncover all malware programs left by hackers. Digital Forensics We follow the attacker's footprint across a variety of systems and create an infection timeline to help us understand their motives. We go as deep as memory analysis, perfect disk copy, threat hunting and malware analysis while sharing insights into real crisis management. Rebuilding systems Finally, we tackle the most important issues of any security incident response: how to kick the attackers out of the systems and regain trust in machines that have been breached. For those that read hacking books like the "Art of Exploitation" or "How to Hack Like a Pornstar," you finally get to experience what it feels like to be on the other side of the Firewall!

How to Hack Like a Ghost - Sparc Flow 2021-05-11

How to Hack Like a Ghost takes you deep inside the mind of a hacker as you carry out a fictionalized attack against a tech company, teaching cutting-edge hacking techniques along the way. Go deep into the mind of a master hacker as he breaks into a hostile, cloud-based security environment. Sparc Flow invites you to shadow him every step of the way, from recon to infiltration, as you hack a shady, data-driven political consulting firm. While the target is fictional, the corporation’s vulnerabilities are based on real-life weaknesses in today’s advanced cybersecurity defense systems. You’ll experience all the thrills, frustrations, dead-ends, and eureka moments of his mission first-hand, while picking up practical, cutting-edge techniques for penetrating cloud technologies. There are no do-overs for hackers, so your training starts with basic OpSec procedures, using an ephemeral OS, Tor, bouncing servers, and detailed code to build an anonymous, replaceable hacking infrastructure guaranteed to avoid detection. From there, you’ll examine some effective recon techniques, develop tools from scratch, and deconstruct low-level features in common systems to gain access to the target. Spark Flow’s clever insights, witty reasoning, and stealth maneuvers teach you how to think on your toes and adapt his skills to your own hacking tasks. You'll learn: • How to set up and use an array of disposable machines that can renew in a matter of seconds to change your internet footprint • How to do effective recon, like harvesting hidden domains and taking advantage of DevOps automation systems to trawl for credentials • How to look inside and gain access to AWS’s storage systems • How cloud security systems like Kubernetes work, and how to hack them • Dynamic techniques for escalating privileges Packed with interesting tricks, ingenious tips, and links to external resources, this fast-paced, hands-on guide to penetrating modern cloud systems will help hackers of all stripes succeed on their next adventure.

How to Hack Like a Legend - Sparc Flow 2022-10-25

Tag along with a master hacker on a truly memorable attack. From reconnaissance to infiltration, you’ll experience their every thought, frustration, and strategic decision-making first-hand in this exhilarating narrative journey into a highly defended Windows environment driven by AI. Step into the shoes of a master hacker and break into an intelligent, highly defensive Windows environment. You’ll be infiltrating the suspicious (fictional) offshoring company G & S Trust and their hostile Microsoft stronghold. While the target is fictional, the corporation’s vulnerabilities are based on real-life weaknesses in today’s advanced Windows defense systems. You’ll experience all the thrills, frustrations, dead-ends, and eureka moments of the mission first-hand, while picking up practical, cutting-edge techniques for evading Microsoft’s best security systems. The adventure starts with setting up your elite hacking infrastructure complete with virtual Windows system. After some thorough passive recon, you’ll craft a sophisticated phishing campaign to steal credentials and gain initial access. Once inside you’ll identify the security systems, scrape passwords, plant persistent backdoors, and delve deep into areas you don’t belong. Throughout your task you’ll get caught, change tack on a tee, dance around defensive monitoring systems, anddisable tools from the inside. Spark Flow’s clever insights, witty reasoning, andstealth maneuvers teach you to be patient, persevere, and adapt your skills at the drop of a hat. You’ll learn how to: Identify and evade Microsoft security systems like Advanced Threat Analysis,QRadar, MDE, and AMSI Seek out subdomains and open ports with Censys, Python scripts, and other OSINT tools Scrape password hashes using Kerberoasting Plant camouflaged C# backdoors and payloads Grab victims’ credentials with more advanced techniques like reflection anddomain replication Like other titles in the How to Hack series, this book is packed with interesting tricks, ingenious tips, and links to useful resources to give you a fast-paced, hands-on guide to penetrating and bypassing Microsoft security systems.

Silence on the Wire - Michal Zalewski 2005

"This book will be riveting reading for security professionals and students, as well as technophiles interested in learning about how computer security fits into the big picture and high-level hackers seeking to broaden their understanding of their craft."--BOOK JACKET.

How to Hack Like a God: Master the Secrets of Hacking Through Real Life Scenarios - Sparc Flow 2017-04-17

Follow me on a step-by-step hacking journey where we pwn a high-profile fashion company. From zero initial access to remotely recording board meetings, we will detail every custom script and technique used in this attack, drawn from real-life findings, to paint the most realistic picture possible. Whether you are a wannabe pentester dreaming about real-life hacking experiences or an experienced ethical hacker tired of countless Metasploit tutorials, you will find unique gems in this book for you to try: -Playing with Kerberos -Bypassing Citrix & Applocker -Mainframe hacking -Fileless WMI persistence -NoSQL injections -Wiegand protocol -Exfiltration techniques -Antivirus evasion tricks -And much more advanced hacking techniques I have documented almost every tool and custom script used in this book. I strongly encourage you to test them out yourself and master their capabilities (and limitations) in an environment you own and control. Hack (safely) the Planet! (Previously published as How to Hack a Fashion Brand)

The Dharma Bums - Jack Kerouac 1971-05-27

Jack Kerouac’s classic novel about friendship, the search for meaning, and the allure of nature First published in 1958, a year after On the Road put the Beat Generation on the map, The Dharma Bums stands as one of Jack Kerouac's most powerful and influential novels. The story focuses on two ebullient young Americans--mountaineer, poet, and Zen Buddhist Japhy Ryder, and Ray Smith, a zestful, innocent writer--whose quest for Truth leads them on a heroic odyssey, from marathon parties and poetry jam sessions in San Francisco's Bohemia to solitude and mountain climbing in the High Sierras.

How to Hack Like a Legend - Sparc Flow 2022-10-25

Tag along with a master hacker on a truly memorable attack. From reconnaissance to infiltration, you’ll experience their every thought, frustration, and strategic decision-making first-hand in this exhilarating narrative journey into a highly defended Windows environment driven by AI. Step into the shoes of a master hacker and break into an intelligent, highly defensive Windows environment. You’ll be infiltrating the suspicious (fictional) offshoring company G & S Trust and their hostile Microsoft stronghold. While the target is fictional, the corporation’s vulnerabilities are based on real-life weaknesses in today’s advanced Windows defense systems. You’ll experience all the thrills, frustrations, dead-ends, and eureka moments of the mission first-hand, while picking up practical, cutting-edge techniques for evading Microsoft’s best security systems. The adventure starts with setting up your elite hacking infrastructure complete with virtual Windows system. After some thorough passive recon, you’ll craft a sophisticated phishing campaign to steal credentials and gain initial access. Once inside you’ll identify the security systems, scrape passwords, plant persistent backdoors, and delve deep into areas you don’t belong. Throughout your task you’ll get caught, change tack on a tee, dance around defensive monitoring systems, anddisable tools from the inside. Spark Flow’s clever insights, witty reasoning, andstealth maneuvers teach you to be patient, persevere, and adapt your skills at the drop of a hat. You’ll learn how to: Identify and evade Microsoft security systems like Advanced Threat Analysis,QRadar, MDE, and AMSI Seek out subdomains and open ports with Censys, Python scripts, and other OSINT tools Scrape password hashes using Kerberoasting Plant camouflaged C# backdoors and payloads Grab victims’ credentials with more advanced techniques like reflection anddomain replication Like other titles in the How to Hack series, this book is packed with interesting tricks, ingenious tips, and links to useful resources to give you a fast-paced, hands-on guide to penetrating and bypassing Microsoft security systems.

Linux Basics for Hackers - OccupyTheWeb 2018-12-04

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?

Game Hacking - Nick Cano 2016-07-01

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.

Go H*ck Yourself - Bryson Payne 2022-01-18

Learn firsthand just how easy a cyberattack can be. Go H*ck Yourself is an eye-opening, hands-on introduction to the world of hacking, from an award-winning cybersecurity coach. As you perform common attacks against yourself, you’ll be shocked by how easy they are to carry out—and realize just how vulnerable most people really are. You’ll be guided through setting up a virtual hacking lab so you can safely try out attacks without putting yourself or others at risk. Then step-by-step instructions will walk you through executing every major type of attack, including physical access hacks, Google hacking and reconnaissance, social engineering and phishing, malware, password cracking, web hacking, and phone hacking. You’ll even hack a virtual car! You’ll experience each hack from the point of view of both the attacker and the target. Most importantly, every hack is grounded in real-life examples and paired with practical cyber defense tips, so you’ll understand how to guard against the hacks you perform. You’ll learn: • How to practice hacking within a safe, virtual environment • How to use popular hacking tools the way real hackers do, like Kali Linux, Metasploit, and John the Ripper • How to infect devices with malware, steal and crack passwords, phish for sensitive information, and more • How to use hacking skills for good, such as to access files on an old laptop when you can’t remember the password • Valuable strategies for protecting yourself from cyber attacks You can’t truly understand cyber threats or defend against them until you’ve experienced them firsthand. By hacking yourself before the bad guys do, you’ll gain the knowledge you need to keep you and your loved ones safe.

Penetration Testing Azure for Ethical Hackers - David Okeyode 2021-11-25

Simulate real-world attacks using tactics, techniques, and procedures that adversaries use during cloud breaches Key FeaturesUnderstand the different Azure attack techniques and methodologies used by hackersFind out how you can ensure end-to-end cybersecurity in the Azure ecosystemDiscover various tools and techniques to perform successful penetration tests on your Azure infrastructureBook Description “If you're looking for this book, you need it.” — 5* Amazon Review Curious about how safe Azure really is? Put your knowledge to work with this practical guide to penetration testing. This book offers a no-faff, hands-on approach to exploring Azure penetration testing methodologies, which will get up and running in no time with the help of real-world examples, scripts, and ready-to-use source code. As you learn about the Microsoft Azure platform and understand how hackers can attack resources hosted in the Azure cloud, you'll find out how to protect your environment by identifying vulnerabilities, along with extending your pentesting tools and capabilities. First, you'll be taken through the prerequisites for pentesting Azure and shown how to set up a pentesting lab. You'll then simulate attacks on Azure assets such as web applications and virtual machines from anonymous and authenticated perspectives. In the later chapters, you'll learn about the opportunities for privilege escalation in Azure tenants and ways in which an attacker can create persistent access to an environment. By the end of this book, you'll be able to leverage your ethical hacking skills to identify and implement different tools and techniques to perform successful penetration tests on your own Azure infrastructure. What you will learnIdentify how administrators misconfigure Azure services, leaving them open to exploitationUnderstand how to detect cloud infrastructure, service, and application misconfigurationsExplore processes and techniques for exploiting common Azure security issuesUse on-premises networks to pivot and escalate access within AzureDiagnose gaps and weaknesses in Azure security implementationsUnderstand how attackers can escalate privileges in Azure ADWho this book is for This book is for new and experienced infosec enthusiasts who want to learn how to simulate real-world Azure attacks using tactics, techniques, and procedures (TTPs) that adversaries use in cloud breaches. Any technology professional working with the Azure platform (including Azure administrators, developers, and DevOps engineers) interested in learning how attackers exploit vulnerabilities in Azure hosted infrastructure, applications, and services will find this book useful.

A Hacker Manifesto - McKenzie Wark 2009-06-30

A double is haunting the world--the double of abstraction, the virtual reality of information, programming or poetry, math or music, curves or colorings upon which the fortunes of states and armies, companies and communities now depend. The bold aim of this book is to make manifest the origins, purpose, and interests of the emerging class responsible for making this new world--for producing the new concepts, new perceptions, and new sensations out of the stuff of raw data. "A Hacker Manifesto" deftly defines the fraught territory between the ever more strident demands by drug and media companies for protection of their patents and copyrights and the pervasive popular culture of file sharing and pirating. This vexed ground, the realm of so-called "intellectual property," gives rise to a whole new kind of class conflict, one that pits the creators of information--the hacker class of researchers and authors, artists and biologists, chemists and musicians, philosophers and programmers--against a possessing class who would monopolize what the hacker produces. Drawing in equal measure on Guy Debord and Gilles Deleuze, "A Hacker Manifesto" offers a systematic restatement of Marxist thought for the age of cyberspace and globalization. In the widespread revolt against commodified information, McKenzie Wark sees a utopian promise, beyond the property form, and a new progressive class, the hacker class, who voice a shared interest in a new information commons.

The Ballad of the White Horse - Gilbert Keith Chesterton 1911

How to Hack Like a GHOST - Sparc Flow 2020-02-29

There are a thousand and one ways to hack an Active Directory environment. But, what happens when end up in a full Cloud environment with thousands of servers, containers and not a single Windows machine to get you going?When we land in an environment designed in the Cloud and engineered using the latest DevOps practices, our hacker intuition needs a little nudge to follow along. How did the company build their systems and what erroneous assumptions can we take advantage of?This book covers the basics of hacking in this new era of Cloud and DevOps: Break container isolation, achieve persistence on Kubernetes cluster and navigate the treacherous sea of AWS detection features to make way with the company's most precious data.Whether you are a fresh infosec student or a Windows veteran, you will certainly find a couple of interesting tricks to help you in your next adventure.

The Basics of Hacking and Penetration Testing - Patrick Engebretson 2013-06-24

The Basics of Hacking and Penetration Testing, Second Edition, serves as an introduction to the steps required to complete a penetration test or perform an ethical hack from beginning to end. The book teaches students how to properly utilize and interpret the results of the modern-day hacking tools required to complete a penetration test. It provides a simple and clean explanation of how to effectively utilize these tools, along with a four-step methodology for conducting a penetration test or hack, thus equipping students with the know-how required to jump start their careers and gain a better understanding of offensive security. Each chapter contains hands-on examples and exercises that are designed to teach learners how to interpret results and utilize those results in later phases. Tool coverage includes: Backtrack Linux, Google reconnaissance, MetaGooFil, dig, Nmap, Nessus, Metasploit, Fast Track Autopwn, Netcat, and Hacker Defender rootkit. This is complemented by PowerPoint slides for use in class. This book is an ideal resource for security consultants, beginning InfoSec professionals, and students. Each chapter contains hands-on examples and exercises that are designed to teach you how to interpret the results and utilize those results in later phases. Written by an author who works in the field as a Penetration Tester and who teaches Offensive Security, Penetration Testing, and Ethical Hacking, and Exploitation classes at Dakota State University. Utilizes the Kali Linux distribution and focuses on the seminal tools required to complete a penetration test.

Someday Is Not a Day in the Week - Sam Horn 2019-03-12

"Inspired me to ask myself why and to stop postponing the forgotten dreams." —Geneen Roth, #1 New York Times bestselling author of Women Food and God and This Messy Magnificent Life Full of inspirational insights and advice, lifehacks, and real-world examples, Someday is Not a Day in the Week is CEO Sam Horn’s motivational guide to help readers get what they want in life today rather than "someday." Are you: • Working, working, working? • Busy taking care of everyone but yourself? • Wondering what to do with the rest of your life? • Planning to do what makes you happy someday when you have more time, money, or freedom? What if someday never happens? As the Buddha said, “The thing is, we think we have time.” Sam Horn is a woman on a mission about not waiting for SOMEDAY ... and this is her manifesto. Her dad’s dream was to visit all the National Parks when he retired. He worked six to seven days a week for decades. A week into his long-delayed dream, he had a stroke. Sam doesn’t want that to happen to you. She took her business on the road for a Year by the Water. During her travels, she asked people, “Do you like your life? Your job? If so, why? If not, why not?” The surprising insights about what makes people happy or unhappy, what they’re doing about it (or not), and why...will inspire you to carve out time for what truly matters now, not later. Life is much too precious to postpone. It’s time to put yourself in your own story. The good news is, there are “hacks” you can do right now to make your life more of what you want it to be. And you don’t have to be selfish, quit your job, or win the lottery to do them. Sam Horn offers actionable, practical advice in short, snappy chapters to show you how to get started on your best life — now.

Cyberjutsu - Ben McCarty 2021-04-26

Like Sun Tzu's Art of War for Modern Business, this book uses ancient ninja scrolls as the foundation for teaching readers about cyber-warfare, espionage and security. Cyberjutsu is a practical cybersecurity field guide based on the techniques, tactics, and procedures of the ancient ninja. Cyber warfare specialist Ben McCarty’s analysis of declassified Japanese scrolls will show how you can apply ninja methods to combat today’s security challenges like information warfare, deceptive infiltration, espionage, and zero-day attacks. Learn how to use key ninja techniques to find gaps in a target’s defense, strike where the enemy is negligent, master the art of invisibility, and more. McCarty outlines specific, in-depth security mitigations such as fending off social engineering attacks by being present with “the correct mind,” mapping your network like an adversary to prevent breaches, and leveraging ninja-like traps to protect your systems. You’ll also learn how to: Use threat modeling to reveal network vulnerabilities Identify insider threats in your organization Deploy countermeasures like network sensors, time-based controls, air gaps, and authentication protocols Guard against malware command and-control servers Detect attackers, prevent supply-chain attacks, and counter zero-day exploits Cyberjutsu is the playbook that every modern cybersecurity professional needs to channel their inner ninja. Turn to the old ways to combat the latest cyber threats and stay one step ahead of your adversaries.

The Car Hacker's Handbook - Craig Smith 2016-03-01

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.

Hack - LitRPG Reads 2018-04-30

ONE MORE LEVEL Ever dream of being trapped in a virtual reality RPG? Craving one more quest? Read on, adventurer! Sarah, Eric and Josh secretly log onto the new Tower of Gates VRMMORPG and stumble on a world unlike any they have seen before. Swords, sorcery, and intrigue abound. While not planning on staying in the unreleased game long, life happens. They soon learn the stakes are even higher than they imagined. To survive, they will need all their strength, courage, and wisdom, not to mention help from friendly NPCs, magic items, and everything else as they delve deeper into the game. Hack is the first book of the Tower of Gates LitRPG Saga. Previously published as the first half of Goblin. Extensive rewritten and professionally edited. Enjoy...

How to Hack Like a Legend - Sparc Flow 2018-04-11

This is the story of a hacker who met his match while breaking into a company: machine learning, behavioral analysis, artificial intelligence... Most hacking tools simply crash and burn in such a hostile environment. What is a hacker to do when facing such a fully equipped opponent? Note: the source code of all custom attack payloads are provided and explained thoroughly in the book. Cybersecurity at its best We start by building a resilient C2 infrastructure using cloud providers, HTTP redirectors and SSH tunnels. The idea is to hide behind an array of disposable machines that we can renew in a matter of seconds to completely change our internet footprint. We then set up step-by-step a phishing platform: fake website, postfix server, DKIM signing, SPF and DMARC. The Art of intrusion Instead of hacking directly our mark(an offshore company), we target one of their suppliers that we identified using OSINT techniques. We collect a couple of passwords thanks to our phishing platform and leverage the remote Citrix access to put our first foot inside. We bypass Applocker and Constrained Language on PowerShell to achieve code execution, then start our Active Directory reconnaissance. Minutes later, we are kicked out of the network due to suspicious activity. The art of exploitation We exploit a flaw in password patterns to get back on the Citrix server. We are facing MS ATA and the QRADAR SIEM. We learn to evade them using various hacking tricks and manage to disable all new Windows Server 2016 security features (AMSI, ScriptBlock Logging, etc.). We also face Windows next-gen antivirus (ATP) while trying to get credentials belonging to developers we suspect are working on the product used by the offshore company. We end up backdooring the accounting software in a way to evade most security and functional tests. Forget penetration testing, time for some red team Our backdoor triggers a fileless malware that give us access to our final target's internal network. After that it's just a cakewalk to achieve domain admin privileges and access personal data of thousands of shell companies and their end beneficiaries. This book's edition assumes prior knowledge of basic computer security principles such as NTLM, pass-the-hash, Windows Active Directory, group policy objects and so forth. If you are scantly comfortable with these concepts, I strongly encourage you to first read How to Hack Like a Pornstar (http: //amzn.to/2iwprf6) or How to Hack Like a God (http: //amzn.to/2iwA3KX) before taking on this book.

Practical Reverse Engineering - Bruce Dang 2014-02-03
Analyzing how hacks are done, so as to stop them in thefuture Reverse engineering is the process of analyzing hardware orsoftware and understanding it, without having access to the sourcecode or design documents. Hackers are able to reverse engineersystems and exploit what they find with scary results. Now the goodguys can use the same tools to thwart these threats. PracticalReverse Engineering goes under the hood of reverse engineeringfor security analysts, security engineers, and system programmers,so they can learn how to use these same processes to stop hackersin their tracks. The book covers x86, x64, and ARM (the first book to cover allthree); Windows kernel-mode code rootkits and drivers; virtualmachine protection techniques; and much more. Best of all, itoffers a systematic approach to the material, with plenty ofhands-on exercises and real-world examples. Offers a systematic approach to understanding reverseengineering, with hands-on exercises and real-world examples Covers x86, x64, and advanced RISC machine (ARM) architecturesas well as deobfuscation and virtual machine protectiontechniques Provides special coverage of Windows kernel-mode code(rootkits/drivers), a topic not often covered elsewhere, andexplains how to analyze drivers step by step Demystifies topics that have a steep learning curve Includes a bonus chapter on reverse engineering tools Practical Reverse Engineering: Using x86, x64, ARM, WindowsKernel, and Reversing Tools provides crucial, up-to-dateguidance for a broad range of IT professionals.
The Legend of Sleepy Hollow Book & CD - Disney Book Group 2019-07-02
If you were asked to choose the most fabulous character in English literature, who would it be? Perhaps the one and only Ichabod Crane. Just in time for the 70th anniversary of the release of The Adventures of Ichabod and Mr. Toad, relive the action of The Legend of Sleepy Hollow with this storybook and CD set, featuring word-for-word narration and sound effects!
Hacking University - Isaac Cody 2016-07-22
Have you ever wanted to be a hacker? Does cracking passwords and the exfiltration of data intrigue you? Hacking University: Freshman Edition is a beginner's guide to the complex security concepts involved with hacking. Whether you are an aspiring "hacktivist" or a security-minded individual, this book can start you on your career of exploration. This book contains demonstrations of hacking techniques and actual code. Aspiring hackers can follow along to get a feel for how professions operate, and persons wishing to hide themselves from hackers can view the same methods for information on how to protect themselves. What makes this hacking book different from other hacking books you might asked? Well it is essentially brings the most up to date information that will allow you to start hacking today. Every skill has to start from somewhere and I firmly believe this book is the perfect platform to get you on your way to start a specialized skill-set in Hacking. By reading this book you will learn the following: The rich history behind hacking Modern security and its place in the business world Common terminology and technical jargon in security How to program a fork bomb How to crack a Wi-Fi password Methods for protecting and concealing yourself as a hacker How to prevent counter-hacks and deter government surveillance The different types of malware and what they do Various types of hacking attacks and how perform or protect yourself from them And much more! Hacking University: Freshman Edition is a wonderful overview of the types of topics that hackers like to learn about. By purchasing this book, you too can learn the well-kept secrets of hackers. Get your copy today! Scroll up and hit the buy button to download now!
Warcross - Marie Lu 2019-08-13
From #1 New York Times bestselling author Marie Lu—when a game called Warcross takes the world by storm, one girl hacks her way into its dangerous depths. For the millions who log in every day, Warcross isn’t just a game—it’s a way of life. The obsession started ten years ago and its fan base now spans the globe, some eager to escape from reality and others hoping to make a profit. Struggling to make ends meet, teenage hacker Emika Chen works as a bounty hunter, tracking down Warcross players who bet on the game illegally. But the bounty-hunting world is a competitive one, and survival has not been easy. To make some quick cash, Emika takes a risk and hacks into the opening game of the international Warcross Championships—only to accidentally glitch herself into the action and become an overnight sensation. Convinced she’s going to be arrested, Emika is shocked when instead she gets a call from the game’s creator, the elusive young billionaire Hideo Tanaka, with an irresistible offer. He needs a spy on the inside of this year’s tournament in order to uncover a security problem . . . and he wants Emika for the job. With no time to lose, Emika’s whisked off to Tokyo and thrust into a world of fame and fortune that she’s only dreamed of. But soon her investigation uncovers a sinister plot, with major consequences for the entire Warcross empire. In this sci-fi thriller, #1 New York Times bestselling author Marie Lu conjures an immersive, exhilarating world where choosing who to trust may be the biggest gamble of all.
Prodigy - Marie Lu 2014-04-08
The second book in Marie Lu’s New York Times bestselling LEGEND trilogy—perfect for fans of THE HUNGER GAMES and DIVERGENT! June and Day arrive in Vegas just as the unthinkable happens: the Elector Primo dies, and his son Anden takes his place. With the Republic edging closer to chaos, the two join a group of Patriot rebels eager to help Day rescue his brother and offer passage to the Colonies. They have only one request—June and Day must assassinate the new Elector. It’s their chance to change the nation, to give voice to a people silenced for too long. But as June realizes this Elector is nothing like his father, she’s haunted by the choice ahead. What if Anden is a new beginning? What if revolution must be more than loss and vengeance, anger and blood—what if the Patriots are wrong? In this highly-anticipated sequel to the New York Times bestseller Legend, Lu delivers a breathtaking thriller with high stakes and cinematic action. "Masterful." —The Los Angeles Times "Lu's action-packed series is the real deal." —Entertainment Weekly
Ethical Hacking - Daniel Graham 2021-09-21
A hands-on guide to hacking computer systems from the ground up, from capturing traffic to crafting sneaky, successful trojans. A crash course in modern hacking techniques, Ethical Hacking is already being used to prepare the next generation of offensive security experts. In its many hands-on labs, you’ll explore crucial skills for any aspiring penetration tester, security researcher, or malware analyst. You’ll begin with the basics: capturing a victim’s network traffic with an ARP spoofing attack and then viewing it in Wireshark. From there, you’ll deploy reverse shells that let you remotely run commands on a victim’s computer, encrypt files by writing your own ransomware in Python, and fake emails like the ones used in phishing attacks. In advanced chapters, you’ll learn how to fuzz for new vulnerabilities, craft trojans and rootkits, exploit websites with SQL injection, and escalate your privileges to extract credentials, which you’ll use to traverse a private network. You’ll work with a wide range of professional penetration testing tools—and learn to write your own tools in Python—as you practice tasks like: • Deploying the Metasploit framework’s reverse shells and embedding them in innocent-seeming files • Capturing passwords in a corporate Windows network using Mimikatz • Scanning (almost) every device on the internet to find potential victims • Installing Linux rootkits that modify a victim’s operating system • Performing advanced Cross-Site Scripting (XSS) attacks that execute sophisticated JavaScript payloads Along the way, you’ll gain a foundation in the relevant computing technologies. Discover how advanced fuzzers work behind the scenes, learn how internet traffic gets encrypted, explore the inner mechanisms of nation-state malware like Drovorub, and much more. Developed with feedback from cybersecurity students, Ethical Hacking addresses contemporary issues in the field not often covered in other books and will prepare you for a career in penetration testing. Most importantly, you’ll be able to think like an ethical hacker: someone who can carefully analyze systems and creatively gain access to them.
Black Hat Go - Tom Steele 2020-02-04
Like the best-selling Black Hat Python, Black Hat Go explores the darker side of the popular Go programming language. This collection of short scripts will help you test your systems, build and automate tools to fit your needs, and improve your offensive security skillset. Black Hat Go explores the darker side of Go, the popular programming language revered by hackers for its simplicity, efficiency, and reliability. It provides an arsenal of practical tactics from the perspective of security practitioners and hackers to help you test your systems, build and automate tools to fit your needs, and improve your offensive security skillset, all using the power of Go. You'll begin your journey with a basic overview of Go's syntax and philosophy and then start to explore examples that you can leverage for tool development, including common network protocols like HTTP, DNS, and SMB. You'll then dig into various tactics and problems that penetration testers encounter, addressing things like data pilfering, packet sniffing, and exploit development. You'll create dynamic, pluggable tools before diving into cryptography, attacking Microsoft Windows, and implementing steganography. You'll learn how to: • Make performant tools that can be used

for your own security projects • Create usable tools that interact with remote APIs • Scrape arbitrary HTML data • Use Go's standard package, net/http, for building HTTP servers • Write your own DNS server and proxy • Use DNS tunneling to establish a C2 channel out of a restrictive network • Create a vulnerability fuzzer to discover an application's security weaknesses • Use plug-ins and extensions to future-proof productsBuild an RC2 symmetric-key brute-forcer • Implant data within a Portable Network Graphics (PNG) image. Are you ready to add to your arsenal of security tools? Then let's Go!

Erak's Ransom (Ranger's Apprentice Book 7) - John Flanagan 2011-10-06

Erak's Ransom is the seventh thrilling book in John Flanagan’s Ranger’s Apprentice series – over eight million sold worldwide. In the wake of Araluen's uneasy truce with the raiding Skandians comes word that the Skandian leader has been captured by a dangerous desert tribe. The Rangers – and Will – are sent to free him. But the desert is like nothing these warriors have seen before. Strangers in a strange land, they are brutalized by sandstorms, beaten by the unrelenting heat, tricked by one tribe that plays by its own rules, and surprisingly befriended by another. Like a desert mirage, nothing is as it seems. Yet one thing is constant: the bravery of the Rangers. Perfect for fans of J.R.R. Tolkien’s Lord of the Rings, T.H. White’s The Sword in the Stone, Christopher Paolini’s Eragon series and Rick Riordan’s Percy Jackson series.

We Are Anonymous - Parmy Olson 2012-06-05

A thrilling, exclusive expose of the hacker collectives Anonymous and LulzSec. WE ARE ANONYMOUS is the first full account of how a loosely assembled group of hackers scattered across the globe formed a new kind of insurgency, seized headlines, and tortured the feds-and the ultimate betrayal that would eventually bring them down. Parmy Olson goes behind the headlines and into the world of Anonymous and LulzSec with unprecedented access, drawing upon hundreds of conversations with the hackers themselves, including exclusive interviews with all six core members of LulzSec. In late 2010, thousands of hacktivists joined a mass digital assault on the websites of VISA, MasterCard, and PayPal to protest their treatment of WikiLeaks. Other targets were wide ranging-the websites of corporations from Sony Entertainment and Fox to the Vatican and the Church of Scientology were hacked, defaced, and embarrassed-and the message was that no one was safe. Thousands of user accounts from pornography websites were released, exposing government employees and military personnel. Although some attacks were perpetrated by masses of users who were rallied on the message boards of 4Chan, many others were masterminded by a small, tight-knit group of hackers who formed a splinter group of Anonymous called LulzSec. The legend of Anonymous and LulzSec grew in the wake of each ambitious hack. But how were they penetrating intricate corporate security systems? Were they anarchists or activists? Teams or lone wolves? A cabal of skilled hackers or a disorganized bunch of kids? WE ARE ANONYMOUS delves deep into the internet's underbelly to tell the incredible full story of the global cyber insurgency movement, and its implications for the future of computer security.

The Legend of Greg - Chris Rylander 2019-05-21

A boy discovers his destiny could totally stink in the first book in this riotously funny middle-grade fantasy-adventure trilogy. Risk-averse Greg Belmont is content with being ordinary. He's got a friend--that's right, just one--at his fancy prep school, and a pretty cool dad. The problem is, Greg isn't ordinary . . . he's actually an honest-to-goodness, fantastical Dwarf! He discovers the truth the day his dad brings home a gross new tea--one that awakens bizarre abilities in Greg. Then a murderous Bro-Troll kidnaps his dad and Greg is whisked away to the Underground, where Dwarves have lived for centuries right beneath the streets of Chicago. With the help of some awesome new friends and a talking ax, Greg learns all about the history of the Dwarves, which has been marked with tales of epic failure since the dawn of time. However, the return of the magic they once wielded means big changes are afoot, escalating tensions with the Dwarves' sworn enemy: the Elves. Brimming with humor and action, Chris Rylander's The Legend of Greg turns dwarf lore on its head, delivering an adventure readers won't be able to resist.

IOS Application Security - David Thiel 2016

Legends - Terry Goodkind 1999-10-21

The second of three volumes, which were originally published in one volume as: Legends.

Ultimate Hacking Challenge - Sparc Flow 2017-06-03

This is not your regular hacking book. Hell, some might say it is not even a book. This is a training program that gives you a free coupon to access dedicated and real machines with real flaws for 24 hours straight. Reading about hacking is fun, hacking real systems is a whole other level of awesomeness! This program is an opportunity to hone your skills on the training platform at www.hacklikeapornstar.com/training: no simulation, no regex based wargames, no far-fetched hacking-like tricks that only work in CTF games... You get a free coupon to access real machines with real and common flaws. The kind of vulnerabilities you find in every corporate environment around the world: - Bypassing application whitelisting - Privilege escalation - Pivoting on other machines It's up to you to exploit them in a meaningful way without screwing up the system. I strongly encourage you to take on the training, struggle with the challenge on your own for a few minutes before reading the chapter describing the solution. Try your usual techniques, read about new ones, and have fun. If you are looking for a passive read about hacking, there are other interesting (and more comprehensive) books to try (preferably mine). This piece of work is about concrete action! This is, in my opinion, the best way to fully internalize the concepts and reflexes that make a great hacker. In case you are discovering the world of hacking/pentesting, I planted several links to resources explaining the different concepts we are dealing with.

True Believer: The Rise and Fall of Stan Lee - Abraham Riesman 2021-02-16

The definitive, revelatory biography of Marvel Comics icon Stan Lee, a writer and entrepreneur who reshaped global pop culture—at a steep personal cost HUGO AWARD FINALIST • “A biography that reads like a thriller or a whodunit . . . scrupulously honest, deeply damning, and sometimes even heartbreaking.”—Neil Gaiman Stan Lee was one of the most famous and beloved entertainers to emerge from the twentieth century. He served as head editor of Marvel Comics for three decades and, in that time, became known as the creator of more pieces of internationally recognizable intellectual property than nearly anyone: Spider-Man, the Avengers, the X-Men, Black Panther, the Incredible Hulk . . . the list goes on. His carnival-barker marketing prowess helped save the comic-book industry and superhero fiction. His cameos in Marvel movies have charmed billions. When he died in 2018, grief poured in from around the world, further cementing his legacy. But what if Stan Lee wasn’t who he said he was? To craft the definitive biography of Lee, Abraham Riesman conducted more than 150 interviews and investigated thousands of pages of private documents, turning up never-before-published revelations about Lee’s life and work. True Believer tackles tough questions: Did Lee actually create the characters he gained fame for creating? Was he complicit in millions of dollars’ worth of fraud in his post-Marvel life? Which members of the cavalcade of grifters who surrounded him were most responsible for the misery of his final days? And, above all, what drove this man to achieve so much yet always boast of more?

Legend - Marie Lu 2013-04-16

"Legend doesn't merely survive the hype, it deserves it." From the New York Times bestselling author of The Young Elites What was once the western United States is now home to the Republic, a nation perpetually at war with its neighbors. Born into an elite family in one of the Republic's wealthiest districts, fifteen-year-old June is a prodigy being groomed for success in the Republic's highest military circles. Born into the slums, fifteen-year-old Day is the country's most wanted criminal. But his motives may not be as malicious as they seem. From very different worlds, June and Day have no reason to cross paths - until the day June's brother, Metias, is murdered and Day becomes the prime suspect. Caught in the ultimate game of cat and mouse, Day is in a race for his family's survival, while June seeks to avenge Metias's death. But in a shocking turn of events, the two uncover the truth of what has really brought them together, and the sinister lengths their country will go to keep its secrets. Full of nonstop action, suspense, and romance, this novel is sure to move readers as much as it thrills.

CUCKOO'S EGG - Clifford Stoll 2012-05-23

Before the Internet became widely known as a global tool for terrorists, one perceptive U.S. citizen recognized its ominous potential. Armed with clear evidence of computer espionage, he began a highly personal quest to expose a hidden network of spies that threatened national security. But would the authorities back him up? Cliff Stoll's dramatic firsthand account is "a computer-age detective story, instantly fascinating [and] astonishingly gripping" (Smithsonian). Cliff Stoll was an astronomer turned systems manager at Lawrence Berkeley Lab when a 75-cent accounting error alerted him to the presence of

an unauthorized user on his system. The hacker's code name was "Hunter"—a mysterious invader who managed to break into U.S. computer systems and steal sensitive military and security information. Stoll began a one-man hunt of his own: spying on the spy. It was a dangerous game of deception, broken codes, satellites, and missile bases—a one-man sting operation that finally gained the attention of the CIA . . . and ultimately trapped an international spy ring fueled by cash, cocaine, and the KGB.