

Ghost In The Shell Readme 1995 2017

Essay Collection covering the point where software, law and social justice meet.

The young witch Wadanohara has just returned from a journey across the oceans, searching for a clue to her lost memories. Now that she has come home, along with her familiars Memoca, Dolphi and Fukami, Wadanohara must continue her quest while ensuring the safety of the ocean kingdom she hails from. But a mysterious figure from her past has appeared and demands that she leave her ocean home forever. What dark event transpired in Wadanohara's past and what does it portend for her future?

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

Web penetration testing by becoming an ethical hacker. Protect the web by learning the tools, and the tricks of the web application attacker. Key Features Builds on books and courses on penetration testing for beginners Covers both attack and defense perspectives Examines which tool to deploy to suit different applications and situations Book Description Becoming the Hacker will teach you how to approach web penetration testing with an attacker's mindset. While testing web applications for performance is common, the ever-changing threat landscape makes security testing much more difficult for the defender. There are many web application tools that claim to provide a complete survey and defense against potential threats, but they must be analyzed in line with the security needs of each web application or service. We must understand how an attacker approaches a web application and the implications of breaching its defenses. Through the first part of the book, Adrian Pruteanu walks you through commonly encountered vulnerabilities and how to take advantage of them to achieve your goal. The latter part of the book shifts gears and puts the newly learned techniques into practice, going over scenarios where the target may be a popular content management system or a containerized application and its network. Becoming the Hacker is a clear guide to web application security from an attacker's point of view, from which both sides can benefit. What you will learn Study the mindset of an attacker Adopt defensive strategies Classify and plan for standard web application security threats Prepare to combat standard system security problems Defend WordPress and mobile applications Use security tools and plan for defense against remote execution Who this book is for The reader should have basic security experience, for example, through running a network or encountering security issues during application development. Formal education in security is useful, but not required. This title is suitable for people with at least two years of experience in development, network management, or DevOps, or with an established interest in security.

(Or, What Became of 21st Century Cinema?)

Becoming the Hacker

R Markdown

□□□□

The Effective Engineer

The Ghost in the Shell

Get started in white-hat ethical hacking using Kali Linux. This book starts off by giving you an overview of security trends, where you will learn the OSI security architecture. This will form the foundation for the rest of Beginning Ethical Hacking with Kali Linux. With the theory out of the way, you'll move on to an introduction to VirtualBox, networking, and common Linux commands, followed by the step-by-step procedure to build your own web server and acquire the skill to be anonymous. When you have finished the examples in the first part of your book, you will have all you need to carry out safe and ethical hacking experiments. After an introduction to Kali Linux, you will carry out your first penetration tests with Python and code raw binary packets for use in those tests. You will learn how to find secret directories on a target system, use a TCP client in Python, and scan ports using NMAP. Along the way you will

discover effective ways to collect important information, track email, and use important tools such as DMITRY and Maltego, as well as take a look at the five phases of penetration testing. The coverage of vulnerability analysis includes sniffing and spoofing, why ARP poisoning is a threat, how Sniffjoke prevents poisoning, how to analyze protocols with Wireshark, and using sniffing packets with Scapy. The next part of the book shows you detecting SQL injection vulnerabilities, using sqlmap, and applying brute force or password attacks. Besides learning these tools, you will see how to use OpenVas, Nikto, Vega, and Burp Suite. The book will explain the information assurance model and the hacking framework Metasploit, taking you through important commands, exploit and payload basics. Moving on to hashes and passwords you will learn password testing and hacking techniques with John the Ripper and Rainbow. You will then dive into classic and modern encryption techniques where you will learn the conventional cryptosystem. In the final chapter you will acquire the skill of exploiting remote Windows and Linux systems and you will learn how to own a target completely. What You Will Learn Master common Linux commands and networking techniques Build your own Kali web server and learn to be anonymous Carry out penetration testing using Python Detect sniffing attacks and SQL injection vulnerabilities Learn tools such as Sniffjoke, Wireshark, Scapy, sqlmap, OpenVas, Nikto, and Burp Suite Use Metasploit with Kali Linux Exploit remote Windows and Linux systems Who This Book Is For Developers new to ethical hacking with a basic understanding of Linux programming.

A complete pentesting guide facilitating smooth backtracking for working hackers About This Book Conduct network testing, surveillance, pen testing and forensics on MS Windows using Kali Linux Gain a deep understanding of the flaws in web applications and exploit them in a practical manner Pentest Android apps and perform various attacks in the real world using real case studies Who This Book Is For This course is for anyone who wants to learn about security. Basic knowledge of Android programming would be a plus. What You Will Learn Exploit several common Windows network vulnerabilities Recover lost files, investigate successful hacks, and discover hidden data in innocent-looking files Expose vulnerabilities present in web servers and their applications using server-side attacks Use SQL and cross-site scripting (XSS) attacks Check for XSS flaws using the burp suite proxy Acquaint yourself with the fundamental building blocks of Android Apps in the right way Take a look at how your personal data can be stolen by malicious attackers See how developers make mistakes that allow attackers to steal data from phones In Detail The need for penetration testers has grown well over what the IT industry ever anticipated. Running just a vulnerability scanner is no longer an effective method to determine whether a business is truly secure. This learning path will help you develop the most effective penetration testing skills to protect your Windows, web applications, and Android devices. The first module focuses on the Windows platform, which is one of the most common OSes, and managing its security spawned the discipline of IT security. Kali Linux is the premier platform for testing and maintaining Windows security. Employs the most advanced tools and techniques to reproduce the methods used by sophisticated hackers. In this module first, you'll be introduced to Kali's top ten tools and other useful reporting tools. Then, you will find your way around your target network and determine known vulnerabilities so you can exploit a system remotely. You'll not only learn to penetrate in the machine, but will also learn to work with Windows privilege escalations. The second module will help you get to grips with the tools used in Kali Linux 2.0 that relate to web application hacking. You will get to know about scripting and input validation flaws, AJAX, and security issues related to AJAX. You will also use an automated technique called fuzzing so you can identify flaws in a web application. Finally, you'll understand the web application vulnerabilities and the ways they can be exploited. In the last module, you'll get started with Android security. Android, being the platform with the largest consumer base, is the obvious primary target for attackers. You'll begin this journey with the absolute basics and will then slowly gear up to the concepts of Android rooting, application security assessments, malware, infecting APK files, and fuzzing. You'll gain the skills necessary to perform Android application vulnerability assessments and to create an Android pentesting lab. This Learning Path is a blend of content from the following Packt products: Kali Linux 2: Windows Penetration Testing by Wolf Halton and Bo Weaver Web Penetration Testing with Kali Linux, Second Edition by Juned Ahmed Ansari Hacking Android by Srinivasa Rao Kotipalli and Mohammed A. Imran Style and approach This course uses easy-to-understand yet professional language for explaining concepts to test your network's security.

The definitive history of the most influential cyberpunk anime of all time! This beautiful, color hardcover guide begins with the seminal feature that inspired The Matrix and many other films, comics, and novels, and ends with the live-action Hollywood adaptation starring Scarlett Johansson. Follow the franchise that made manga master Shirow Masamune, legendary director Mamoru Oshii, and the studio Production I.G the legends they are today. In-depth interviews, stunning concept art, and tales of behind-the-scenes triumphs and near-tragedies from the 22-year history of The Ghost in the Shell. Begin with the original anime, which was released in Japan in 1995 and subsequently took the West by storm, through the award-winning sequel Innocence and the global smash hit TV adaptation Stand Alone Complex, all the way up to 2017, with the release of the new live-action film from Paramount Pictures. There are hundreds--if not thousands--of techniques used to compromise both Windows and Unix-based systems. Malicious code and new exploit scripts are released on a daily basis, and each evolution becomes more and more sophisticated. Keeping up with the myriad of systems used by hackers in the wild is a formidable task, and scrambling to patch each potential vulnerability or address each new attack one-by-one is a bit like emptying the Atlantic with paper cup. If you're a network administrator, the pressure is on you to defend your systems from attack. But short of devoting your life to becoming a security expert, what can you do to ensure the safety of your mission critical systems? Where do you start? Using the steps laid out by professional security analysts and consultants to identify and assess risks, Network Security Assessment offers an efficient testing model that an administrator can adopt, refine, and reuse to create proactive defensive strategies to protect their systems from the threats that are out there, as well as those still being developed. This thorough and insightful guide covers offensive technologies by grouping and analyzing them at a higher level--from both an offensive and defensive standpoint--helping administrators design and deploy networks that are immune to offensive exploits, tools, and scripts. Network administrators who need to develop and implement a security assessment program will find everything they're looking for--a proven, expert-tested methodology on which to base their own comprehensive program--in this time-saving new book.

Beginning Ethical Hacking with Kali Linux
Reamde

Investigating Cryptocurrencies

A Novel

From Bash to Z Shell

The Swamp

"Stephenson has a once-in-a-generation gift: he makes complex ideas clear, and he makes them funny, heartbreaking, and thrilling." —Time The #1 New York Times bestselling author of *Anathem*, Neal Stephenson is continually rocking the literary world with his brazen and brilliant fictional creations—whether he's reimagining the past (*The Baroque Cycle*), inventing the future (*Snow Crash*), or both (*Cryptonomicon*). With *Reamde*, this visionary author whose mind-stretching fiction has been enthusiastically compared to the work of Thomas Pynchon, Don DeLillo, Kurt Vonnegut, and David Foster Wallace—not to mention William Gibson and Michael Crichton—once again blazes new ground with a high-stakes thriller that will enthrall his loyal audience, science and science fiction, and espionage fiction fans equally. The breathtaking tale of a wealthy tech entrepreneur caught in the very real crossfire of his own online fantasy war game, *Reamde* is a new high—and a new world—for the remarkable Neal Stephenson.

The Singularity. It is the era of the posthuman. Artificial intelligences have surpassed the limits of human intellect. Biotechnological beings have rendered people all but extinct. Molecular nanotechnology runs rampant, replicating and reprogramming at will. Contact with extraterrestrial life grows more imminent with each new day. Struggling to survive and thrive in this accelerated world are three generations of the Macx clan: Manfred, an entrepreneur dealing in intelligence amplification technology whose mind is divided between his physical environment and the Internet; his daughter, Amber, on the run from her domineering mother, seeking her fortune in the outer system as an indentured astronaut; and Sirhan, Amber's son, who finds his destiny linked to the fate of all of humanity. For something is systematically dismantling the nine planets of the solar system. Something beyond human comprehension. Something that has no use for biological life in any form...

One of the world's most erudite and entertaining film critics on the state of cinema in the post-digital—and post-9/11—age. This witty and allusive book, in the style of classic film theorists/critics like André Bazin and Siegfried Kracauer, includes considerations of global cinema's most important figures and films, from Lars von Trier and Zia Jiangke to *WALL-E*, *Avatar* and *Inception*.

NEW HARDCOVER DELUXE EDITION! * Definitive new edition supervised by creator Shirow Masamune * In the original, right-to-left format with Japanese sound effects for the first time! * Brand new bonus content * Released simultaneously with deluxe editions of *The Ghost in the Shell 1* and *2* The "lost" *Ghost in the Shell* stories, created by Shirow Masamune after completing work on the original *Ghost in the Shell* manga and prior to his tour-de-force, *Ghost in the Shell 2: Man-Machine Interface*. Focusing on Section 9 agents in their daily battle against technocrime, *Human-Error Processor*. Features the stories "Fat Cat," "Drive Slave," "Mines of Mind," and "Lost Past."

PoC or GTFO

Ghost in the Shell: Global Neural Network

Free Software, Free Society

Penetration Testing: A Survival Guide

Understanding, Extracting, and Analyzing Blockchain Evidence

Selected Essays of Richard M. Stallman

Section 9, a cybernetically enhanced squad that is the Prime Minister's top crime fighting force, investigate a variety of cases, including the kidnapping of a high-ranking government official.

The bestselling series from author Tappei Nagatsuki continues in this spin-off where some of your favorite characters capture the spotlight!

Embargoed to 30th March 2017 Witness the incredible artwork behind the creation of Ghost in the Shell, the live-action feature film based on the Japanese manga classic and starring Scarlett Johansson. As well as featuring beautiful concept art, stunning on-set photography and exclusive interviews with major cast and crew members, delve into the advanced special effects that bring Japan and the cyborg elements of the story to life. A compelling chronicle of an epic creative journey.

This collection of short expository, critical and speculative texts offers a field guide to the cultural, political, social and aesthetic impact of software. Experts from a range of disciplines each take a key topic in software and the understanding of software, such as algorithms and logical structures.

Wadanohara and the Great Blue Sea

The Playbook for Getting Inside the Mind of the Attacker

End-to-end penetration testing solutions

The Ghost in the Shell 1 Deluxe Edition

The Linux Cookbook, 2nd Edition

Accelerando

Introducing *The Effective Engineer*--the only book designed specifically for today's software engineers, based on extensive interviews with engineering leaders at top tech companies, and packed with hundreds of techniques to accelerate your career.

NEW HARDCOVER DELUXE EDITION! Now a major motion picture! * Definitive new edition supervised by creator Shirow Masamune * In the original, right-to-left format with Japanese sound effects for the first time! * Brand new bonus content * Released simultaneously with deluxe editions of The Ghost in the Shell 1.5 and 2 Deep into the twenty-first century, the line between man and machine has been blurred as humans rely on the enhancement of mechanical implants and robots are upgraded with human tissue. In this rapidly converging landscape, cyborg superagent Major Motoko Kusanagi is charged to track down the craftiest and most dangerous terrorists and cybercriminals, including "ghost hackers" who are capable of exploiting the human/machine interface and reprogramming humans to become puppets to carry out the hackers' criminal ends.

This highly anticipated print collection gathers articles published in the much-loved International Journal of Proof-of-Concept or Get The Fuck Out. PoC||GTFO follows in the tradition of Phrack and Uninformed by publishing on the subjects of offensive security research, reverse engineering, and file format internals. Until now, the journal has only been available online or printed and distributed for free at hacker conferences worldwide. Consistent with the journal's quirky, biblical style, this book comes with all the trimmings: a leatherette cover, ribbon bookmark, bible paper, and gilt-edged pages. The book features more than 80 technical essays from numerous famous hackers, authors of classics like "Reliable Code Execution on a Tamagotchi," "ELFs are Dorky, Elves are Cool," "Burning a Phone," "Forget Not the Humble Timing Attack," and "A Sermon on Hacker Privilege." Twenty-four full-color pages by Ange Albertini illustrate many of the clever tricks described in the text.

Understand malware analysis and its practical implementation Key Features Explore the key concepts of malware analysis and memory forensics using real-world examples Learn the art of detecting, analyzing, and investigating malware threats Understand adversary tactics and techniques Book Description Malware analysis and memory forensics are powerful analysis and investigation techniques used in reverse engineering, digital forensics, and incident response. With adversaries becoming sophisticated and carrying out advanced malware attacks on critical infrastructures, data centers, and private and public organizations, detecting, responding to, and investigating such intrusions is critical to information security professionals. Malware analysis and memory forensics have become must-have skills to fight advanced malware, targeted attacks, and security breaches. This book teaches you the concepts, techniques, and tools to understand the behavior and characteristics of malware through malware analysis. It also teaches you techniques to investigate and hunt malware using memory forensics. This book introduces you to the basics of malware analysis, and then gradually progresses into the more advanced concepts of code analysis and memory forensics. It uses real-world malware samples, infected memory images, and visual diagrams to help you gain a better understanding of the subject and to equip you with the skills required to analyze, investigate, and respond to malware-related incidents. What you will learn Create a safe and isolated lab environment for malware analysis Extract the metadata associated with malware Determine malware's interaction with the system Perform code analysis using IDA Pro and x64dbg Reverse-engineer various malware functionalities Reverse engineer and decode common encoding/encryption algorithms Reverse-engineer malware code injection and hooking techniques Investigate and hunt malware using memory forensics Who this book is for This book is for incident responders, cyber-security investigators, system administrators, malware analyst, forensic practitioners, student, or curious security professionals interested in learning malware analysis and memory forensics. Knowledge of programming languages such as C and Python is helpful but is not mandatory. If you have written few lines of code and have a basic understanding of programming concepts, you ' ll be able to get most out of this book.

Wonderland

PDF Hacks

The Art of Nanaco Yashiro

The Dream of the Lion King

How to Leverage Your Efforts in Software Engineering to Make a Disproportionate and Meaningful Impact

Learning Malware Analysis

The essential early work by the modern master of Japanese literary comics Yoshiharu Tsuge is one of the most influential and acclaimed practitioners of literary comics in Japan. The Swamp collects work from his early years, showing a major talent coming into his own. Bucking the tradition of mystery and adventure stories, Tsuge's fiction focused on the lives of the citizens of Japan. These mesmerizing comics, like those of his contemporary Yoshihiro Tatsumi, reveal a gritty, at times desperate postwar Japan, while displaying Tsuge's unique sense of humor and point of view. "Chirpy" is a simple domestic drama about expectations, fidelity, and escape. A couple purchase a beautiful white bird with a red beak. It is said that the bird will grow attached to its owners and never fly away. While the girlfriend is working as a hostess, flirting with men for money, the boyfriend decides to draw a portrait of the new family member, and disaster strikes. In "The Swamp," a simple rural encounter is charged with sexual tension that is alluring but also fraught with danger. When a young woman happens upon a wing-shot goose, she tries to calm it then suddenly snaps its neck. Later, she befriends a young hunter and offers him shelter, but her motivations remain unclear, especially when the hunter notices a snake in the room where they'll both be sleeping. The Swamp is a landmark in English manga-publishing history and the first in a series of Tsuge books Drawn & Quarterly will be publishing.

Presents information on getting the most out of a PC's hardware and software, covering such topics as upgrading the BIOS, configuring the hard drive, installing more RAM, improving CPU performance, and adding COM ports.

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.

A practical and concise guide to finite difference and finite element methods. Well-tested MATLAB® codes are available online.

Network Security Assessment

The Definitive Guide

JavaScript Cookbook

Stand Alone Complex. Episode 1, Section 9

Kali Linux - An Ethical Hacker's Cookbook

Numerical Solution of Differential Equations

R Markdown: The Definitive Guide is the first official book authored by the core R Markdown developers that provides a comprehensive and accurate reference to the R Markdown ecosystem. With R Markdown, you can easily create reproducible data analysis reports, presentations, dashboards, interactive applications, books, dissertations, websites, and journal articles, while enjoying the simplicity of Markdown and the great power of R and other languages. In this book, you will learn

Basics: Syntax of Markdown and R code chunks, how to generate figures and tables, and how to use other computing languages

Built-in output formats of R Markdown: PDF/HTML/Word/RTF/Markdown documents and ioslides/Slidy/Beamer/PowerPoint presentations

Extensions and applications: Dashboards, Tufte handouts, xaringan/reveal.js presentations, websites, books, journal articles, and interactive tutorials

Advanced topics: Parameterized reports, HTML widgets, document templates, custom output formats, and Shiny documents.

Yihui Xie is a software engineer at RStudio. He has authored and co-authored several R packages, including knitr, rmarkdown, bookdown, blogdown, shiny, xaringan, and animation. He has published three other books, *Dynamic Documents with R and knitr*, *bookdown: Authoring Books and Technical Documents with R Markdown*, and *blogdown: Creating Websites with R Markdown*. J.J. Allaire is the founder of RStudio and the creator of the RStudio IDE. He is an author of several packages in the R Markdown ecosystem including rmarkdown, flexdashboard, learnr, and radix. Garrett Golemund is the co-author of *R for Data Science* and author of *Hands-On Programming with R*. He wrote the lubridate R package and works for RStudio as an advocate who trains engineers to do data science with R and the Tidyverse.

Investigate crimes involving cryptocurrencies and other blockchain technologies Bitcoin has traditionally been the payment system of choice for a criminal trading on the Dark Web, and now many other blockchain cryptocurrencies are entering the mainstream as traders are accepting them from low-end investors putting their money into the market. Worse still, the blockchain can even be used to hide information and covert messaging, unknown to most investigators. *Investigating Cryptocurrencies* is the first book to help corporate, law enforcement, and other investigators understand the technical concepts and the techniques for investigating crimes utilizing the blockchain and related digital currencies such as Bitcoin and Ethereum. **Understand blockchain and transaction technologies** Set up and run cryptocurrency accounts Build information about specific addresses Access raw data on blockchain ledgers Identify users of cryptocurrencies Extracting cryptocurrency data from live and imaged computers Following the money With nearly

\$150 billion in cryptocurrency circulating and \$3 billion changing hands daily, crimes committed with or paid for with digital cash are a serious business. Luckily, Investigating Cryptocurrencies Forensics shows you how to detect it and, more importantly, stop it in its tracks.

More physicists today are taking on the role of software developer as part of their research, but software development isn't always easy or obvious, even for physicists. This practical book teaches essential software development skills to help you automate and accomplish nearly any aspect of research in a physics-based field. Written by two PhDs in nuclear engineering, this book includes practical examples drawn from a working knowledge of physics concepts. You'll learn how to use the Python programming language to perform everything from collecting and analyzing data to building software and publishing your results. In four parts, this book includes: Getting Started: Jump into Python, the command line, data containers, functions, flow control and logic, and classes and objects Getting It Done: Learn about regular expressions, analysis and visualization, NumPy, storing data in files and HDF5, important data structures in physics, computing in parallel, and deploying software Getting It Right: Build pipelines and software, learn to use local and remote version control, and debug and test your code Getting It Out There: Document your code, process and publish your findings, and collaborate efficiently; dive into software licenses, ownership, and copyright procedures

A covert mission in Shanghai reunites Kusanagi with a wartime rival amid shifting loyalties. The infiltration of an anti-cyberization cult calls for Section 9's most "human" members to do things the old-fashioned way. A deep dive into the mind of a criminal forces Kusanagi to question the nature of imagination - and her own identity. The stories in Global Neural Network bring a 21st-century perspective to its questions of human identity and the border between mind and machine that made The Ghost in the Shell one of the most revered manga of all time, and unleash top Western comics artists on eye-popping action scenes starring Kusanagi, Batou, Togusa, Aramaki, and all the members of Section 9! Original stories by: * Alex de Campi (Twisted Romance) & Giannis Milonogiannis (Prophet) * Brenden Fletcher (Gotham Academy, Motor Crush) & LRNZ (Golem) * Genevieve Valentine (Mechanique, Icon), & Brent Schoonover (The Astonishing Ant-Man) * Max Gladstone (the Craft Sequence) & David López (All-New Wolverine)

Field Guide to Research with Python

Beowulf Cluster Computing with Linux

How to Hack Like a Ghost

The Icon Programming Language

PC Hacks

The Ghost in the Shell 1. 5 Deluxe Edition

In this mind-altering romp—where the term “Metaverse” was first coined—you’ll experience a future America so bizarre, so outrageous, you’ll recognize it immediately • One of Time’s 100 best English-language novels Only once in a great while does a writer come along who defies comparison—a writer so original he redefines the way we look at the world. Neal Stephenson is such a writer and Snow Crash is such a novel, weaving virtual reality, Sumerian myth, and just about everything in between with a cool, hip cybersensibility to bring us the gigathriller of the information age. In reality, Hiro Protagonist delivers pizza for Uncle Enzo’s CosoNostra Pizza Inc., but in the Metaverse he’s a warrior prince. Plunging headlong into the enigma of a new computer virus that’s striking down hackers everywhere, he races along the neon-lit streets on a search-and-destroy mission for the shadowy virtual villain threatening to bring about infocalypse. Praise for Snow Crash “[Snow Crash is] a cross between Neuromancer and Thomas Pynchon’s Vineland. This is no mere hyperbole.”—The San Francisco Bay Guardian “Fast-forward free-style mall mythology for the twenty-first century.”—William Gibson “Brilliantly realized . . . Stephenson turns out to be an engaging guide to an onrushing tomorrow.”—The New York Times Book Review

Why reinvent the wheel every time you run into a problem with JavaScript? This cookbook is chock-full of code recipes that address common programming tasks, as well as techniques for building web apps that work in any browser. Just copy and paste the code samples into your project—you’ll get the job done faster and learn more about JavaScript in the process. You'll also learn how to take advantage of the latest features in ECMAScript 5 and HTML5, including the new cross-domain widget communication technique, HTML5's video and audio elements, and the drawing canvas. You'll find recipes for using these features with JavaScript to build high-quality application interfaces. Create interactive web and desktop applications Work with JavaScript objects, such as String, Array, Number, and Math Use JavaScript with Scalable Vector Graphics (SVG) and the canvas element Store data in various ways, from the simple to the complex Program the new HTML5 audio and video elements Implement concurrent programming with Web Workers Use and create jQuery plug-ins Use ARIA and JavaScript to create fully accessible rich internet applications

Over 120 recipes to perform advanced penetration testing with Kali Linux About This Book Practical recipes to conduct effective penetration testing using the powerful Kali Linux Leverage tools like Metasploit, Wireshark, Nmap, and many more to detect vulnerabilities with ease Confidently perform networking and application attacks using task-oriented recipes Who This Book Is For This book is aimed at IT security professionals, pentesters, and security analysts who have basic knowledge of Kali Linux and want to conduct advanced penetration testing techniques. What You Will Learn Installing, setting up and customizing Kali for pentesting on multiple platforms Pentesting routers and embedded devices Bug

hunting 2017 Pwning and escalating through corporate network Buffer overflows 101 Auditing wireless networks Fiddling around with software-defined radio Hacking on the run with NetHunter Writing good quality reports In Detail With the current rate of hacking, it is very important to pentest your environment in order to ensure advanced-level security. This book is packed with practical recipes that will quickly get you started with Kali Linux (version 2016.2) according to your needs, and move on to core functionalities. This book will start with the installation and configuration of Kali Linux so that you can perform your tests. You will learn how to plan attack strategies and perform web application exploitation using tools such as Burp, and Jexboss. You will also learn how to perform network exploitation using Metasploit, Sparta, and Wireshark. Next, you will perform wireless and password attacks using tools such as Patator, John the Ripper, and airoscript-ng. Lastly, you will learn how to create an optimum quality pentest report! By the end of this book, you will know how to conduct advanced penetration testing thanks to the book's crisp and task-oriented recipes. Style and approach This is a recipe-based book that allows you to venture into some of the most cutting-edge practices and techniques to perform penetration testing with Kali Linux.

The first commercial collection of work by Nanaco Yashiro, an illustrator who has attracted international attention for her fluid lines, vivid colors, and vintage style. Nanaco Yashiro's illustrations feature various motifs such as a woman in a feathered robe from Japanese mythology, a large tiger reminiscent of Arabia, a man in a spacesuit, and concept art for an imaginary movie about heaven and hell that the illustrator created herself and are each drawn sometimes in delicately refined watercolor brushwork and at other times in bold strokes with acrylic gouache. While the themes and motifs may vary, all of them depict Nanaco Yashiro's signature style which is sure to continue fascinating her audience forever. This book contains nearly 120 carefully selected illustrations, including many that have been newly drawn for this book, which are grouped in different themes, such as plants, animals, beautiful women, and fairytales, allowing readers to enjoy the lovely and mysterious world of Yashiro's works. This book will not only appeal to Nanaco Yashiro's current fans but will also captivate those who are new to her beautiful, delicate, and colorful illustrations.

The Art of Ghost in the Shell

Tips and Techniques for Everyday Use

Explore the concepts, tools, and techniques to analyze and investigate Windows malware

Film After Film

100 Industrial-Strength Tips & Tools

Why's (Poignant) Guide to Ruby

* In-depth, unique coverage of ZSH, one of most modern and powerful of all shells. Also covers Bash, the preferred shell for most serious Linux and Unix users. * Very strong author and tech review team: Co-author Peter Stephenson has been involved in the development of Zsh since the 1990s when he started to write the FAQ. For the last few years, he has served as coordinator of the shell's development. Tech Reviewers: Ed Schaefer is the "Shell Corner" columnist for SysAdmin Magazine and Bart Schaefer is one of the lead developers of Zsh development. * Book is immediately useful, packed with short example and suggestions that the reader can put to use in their shell environment. * Extensive coverage of interactive and advanced shell features, including shell extensions, completion functions, and shortcuts. * Great book for users of all expertise; perennial seller.

Provides step-by-step instructions on how to use the computer operating system Linux.

Shows readers how to create PDF documents that are far more powerful than simple representations of paper pages, helps them get around common PDF issues, and introduces them to tools that will allow them to manage content in PDF, navigating it and reusing it as necessary. Original. (Intermediate).

March 6, 2035. Motoko Aramaki is a hyper-advanced cyborg, a counter-terrorist Net security expert, heading the investigative department of the giant multi-national Poseidon Industrial. Partly transcending the physical world and existing in a virtual world of networks, Motoko is a fusion of multiple entities and identities, deploying remotely controlled prosthetic humanoid surrogates around the globe to investigate a series of bizarre incidents.

Know Your Network

Effective Computation in Physics

The Ghost in the Shell Readme, 1995-2017

Snow Crash

Android Hacker's Handbook

Re:ZERO -Starting Life in Another World- Ex, Vol. 1 (light novel)

Enabling technologies - An overview of cluster computing / Thomas Sterling / - Node Hardware / Thomas Sterling / - Linux / Peter H. Beckman / - Network Hardware / Thomas Sterling /

Sterling / - Setting Up clusters : installation and configuration - How fast is my beowulf? / David Bailey / - Parallel programming / - Parallel programming with MPI / William Gropp / - Adv

programming / William Gropp / - Parallel programming with PVM / Al Geist / - Fault-tolerant and adaptive programs with PVM / Al Geist / - Managing clusters / - Cluster workload manag

Condor : a distributed job scheduler / - Maui scheduler : A multifunction cluster scheduler / David B. Jackson / - PBS : portable batch system / James Patton Jones / - PVFS : parallel virtu

Chiba city : the Argonne scalable cluster.

Conquering the Command Line

The Ghost in the Shell Volume 2

A Lexicon

Computational Techniques for Resolving Security Issues
Software Studies
Breaching the Cloud