Php Socket Programming Tutorial Binarytides

Hardening a Linux system can make it much more difficult for an attacker to exploit it. This book will enable system administrators and network engineers to protect their Linux systems, and the sensitive data on those systems.
Hack your antivirus software to stamp out future vulnerabilities The Antivirus Hacker's Handbook guides you through the process of reverse engineering antivirus software. You explore how to detect and exploit vulnerabilities that can be leveraged to improve future software design, protect your network, and anticipate attacks that may sneak through your antivirus' line of defense. You'll begin building your knowledge by diving into the reverse engineering process, which details how to start from a finished antivirus software program and work your way back through its development using the functions and other key elements of the software. Next, you leverage your new knowledge about software development to evade, attack, and exploit antivirus software—all of which can help you strengthen your network and protect your data. While not all viruses are damaging, understanding how to better protect your computer against them can help you maintain the integrity of your network. Discover how to reverse engineer your antivirus software Explore methods of antivirus software evasion Consider different ways to attack and exploit antivirus software Understand the current state of the antivirus software market, and get recommendations for users and vendors who are leveraging this software The Antivirus Hacker's Handbook is the essential reference for software reverse engineers, penetration testers, security researchers, exploit writers, antivirus vendors, and software engineers who want to understand how to leverage current antivirus software to improve future applications.
An illustrated collection of scary stories with humorous endings features such elements as a boy being followed home by a coffin, a rapping noise in a haunted house, and strange intruders at the front door. Reprint.
Updated with improvements, updates, and new features included in Ubuntu MATE's 20.04 LTS (Long Term Support) release, I have written the third edition of this book for computer users who just want the information they need to learn how to use Ubuntu MATE and its applications. Reading this book can help you build your confidence and competence in using Ubuntu MATE. It is written from the perspective that Ubuntu MATE is a typical modern Linux for the average computer user who needs to do things like browsing the Internet, checking email, using a word processor, reading and storing document files, viewing and editing photos, watching videos, listening to music, and subscribing to podcasts. Many of the applications available in Ubuntu MATE are also available in other flavors of Ubuntu and in other distributions (versions) of Linux. The applications I mention in this book work in the same way regardless of the operating system.While it's is great for users who have migrated from Windows or macOS, Ubuntu MATE is also an excellent choice for any kind of computer user, from the casual home user to the professional software developer. That's because of its modern, functionally thought-out design. Ubuntu MATE is capable enough for even the most experienced computer user because, well, it's Linux! It has the power of every other Linux built-in. Simply put, it provides a practical alternative to other software that can run on your computer. Whether you are new to Linux, upgrading from Windows or macOS to Linux, or just thinking about moving to Linux, this book will provide you with practical, day-to-day advice on how you can use Ubuntu MATE and its applications. This book is a guide for new users and a reference for all users of Linux.
Linux Kernel Module Programming Guide is for people who want to write kernel modules. It takes a hands-on approach starting with writing a small "hello, world" program, and quickly moves from there. Far from a boring text on programming, Linux Kernel Module Programming Guide has a lively style that entertains while it educates. An excellent guide for anyone wishing to get started on kernel module programming. *** Money raised from the sale of this book supports the development of free software and documentation.
Michael Lewis' Flash Boys revealed how high-frequency trading has created a ruthless breed of traders capable of winning whichever way the market turns. In Rogue Code, Mark Russinovich takes it one step further to show how their grip on high finance makes the stock market vulnerable to hackers who could bring about worldwide financial collapse. Cyber security expert Jeff Aiken knows that no computer system is completely secure. When he's called to investigate a possible breach at the New York Stock Exchange, he discovers not only that their system has been infiltrated but that someone on the inside knows. Yet for some reason, they have allowed the hackers to steal millions of dollars from accounts without trying to stop the theft. When Jeff uncovers the crime, the NYSE suddenly turns on him. Accused of grand larceny, he must find and expose the criminals behind the theft, not just to prove his innocence but to stop a multibillion-dollar heist that could upend the U.S. economy. Unwilling to heed Jeff's warnings, the NYSE plans to continue with a major IPO using a new, untested system, one that might be susceptible both to hackers and to ruthless high-frequency traders willing to take any risk to turn a profit. Now Jeff Aiken must unearth the truth on his own, following the thread to the back alleys of Rio de Janeiro to take on one of the world's most ruthless cartels. Praised for his combination of real-world technology and quick-paced action, with Rogue Code Mark Russinovich delivers an intense thriller about a cyber threat that seems all too possible---and the Wall Street traders who might allow it to happen. Includes a foreword by Haim Bodek, author of The Problem of HFT: Collected Writings on High Frequency Trading & Stock Market Structure Reform.
Don't let the idea of exercise daunt you. A fit, trim-and less-stressed-body is just around the corner. And a gym membership and large bulky home equipment aren't even part of the equation. Simply follow the informative, yet fun, tips and techniques in Your Personal Coach by celebrity fitness guru Valerie Orsoni and you'll be looking and feeling good in no time. Each quick exercise or idea is something that can be easily incorporated into your existing lifestyle and will become lifelong healthy habits. Orsoni's proven nutritional and fitness advice includes: How to fit in exercise while you're on a plane, at the playground, in the kitchen, on line, at work, on a cell phone, or shopping Exercises to increase bone density Professional dancers' secrets to a natural breast lift How to increase self-confidence and decrease back pain by

improving your posture Strategies to avoid feeling overwhelmed so you can target your trouble zones Easy ways to instantly de-stress

A comprehensive guide to mastering the art of preventing your Linux system from getting compromised. Key Features Leverage this guide to confidently deliver a system that reduces the risk of being hacked Perform a number of advanced Linux security techniques such as network service detection, user authentication, controlling special permissions, encrypting file systems, and much more Master the art of securing a Linux environment with this end-to-end practical guide Book Description This book has extensive coverage of techniques that will help prevent attackers from breaching your system, by building a much more secure Linux environment. You will learn various security techniques such as SSH hardening, network service detection, setting up firewalls, encrypting file systems, protecting user accounts, authentication processes, and so on. Moving forward, you will also develop hands-on skills with advanced Linux permissions, access control, special modes, and more. Lastly, this book will also cover best practices and troubleshooting techniques to get your work done efficiently. By the end of this book, you will be confident in delivering a system that will be much harder to compromise. What you will learn Use various techniques to prevent intruders from accessing sensitive data Prevent intruders from planting malware, and detect whether malware has been planted Prevent insiders from accessing data that they aren’t authorized to access Do quick checks to see whether a computer is running network services that it doesn’t need to run Learn security techniques that are common to all Linux distros, and some that are distro-specific Who this book is for If you are a systems administrator or a network engineer interested in making your Linux environment more secure, then this book is for you. Security consultants wanting to enhance their Linux security skills will also benefit from this book. Prior knowledge of Linux is mandatory.

The book you have been waiting for to make you a Master of TShark Network Forensics, is finally here!!! Be it you are a Network Engineer, a Network Forensics Analyst, someone new to packet analysis or someone who occasionally looks at packet, this book is guaranteed to improve your TShark skills, while moving you from Zero to Hero. Mastering TShark Network Forensics, can be considered the definitive repository of practical TShark knowledge. It is your one-stop shop for all you need to master TShark, with adequate references to allow you to go deeper on peripheral topics if you so choose. Book Objectives: Introduce packet capturing architecture Teach the basics of TShark Teach some not so basic TShark tricks Solve real world challenges with TShark Identify services hiding behind other protocols Perform "hands-free" packet capture with TShark Analyze and decrypt TLS encrypted traffic Analyze and decrypt WPA2 Personal Traffic Going way beyond - Leveraging TShark and Python for IP threat intelligence Introduce Lua scripts Introduce packet editing Introduce packet merging Introduce packet rewriting Introduce remote packet capturing Who is this book for?While this book is written specifically for Network Forensics Analysts, it is equally beneficial to anyone who supports the network infrastructure. This means, Network Administrators, Security Specialists, Network Engineers, etc., will all benefit from this book. Considering the preceding, I believe the following represents the right audience for this book: Individuals starting off their Cybersecurity careers Individuals working in a Cyber/Security Operations Center (C/SOC) General practitioners of Cybersecurity Experienced Cybersecurity Ninjas who may be looking for a trick or two Anyone who just wishes to learn more about TShark and its uses in network forensics Anyone involved in network forensics More importantly, anyhow who is looking for a good read Not sure if this book is for you? Take a glimpse at the sample chapter before committing to it. Mastering TShark sample chapters can be found at: https: //bit.ly/TShark All PCAPS used within this book can be found at: https: //github.com/SecurityNik/SUWtHEh- As an addition to this book, the tool, pktIntel: Tool used to perform threat intelligence against packet data can be found at: https: //github.com/SecurityNik/pktIntel

Most web applications are changed and adapted quite frequently and quickly. Their environment, for example the size and the behavior of the user base, are constantly changing. What was sufficient yesterday can be insufficient today. Especially in a web environment it is important to monitor and continuously improve the internal quality not only when developing, but also when maintaining the software. Jenkins is the leading open-source continuous integration server. Thanks to its thriving plugin ecosystem, it supports building and testing virtually any project. This book explains how you can leverage Jenkins to monitor the various aspects of software quality in a PHP software project.

TCP/IP Illustrated, Volume 1, Second Edition, is a detailed and visual guide to today's TCP/IP protocol suite. Fully updated for the newest innovations, it demonstrates each protocol in action through realistic examples from modern Linux, Windows, and Mac OS environments. There's no better way to discover why TCP/IP works as it does, how it reacts to common conditions, and how to apply it in your own applications and networks. Building on the late W. Richard Stevens' classic first edition, author Kevin R. Fall adds his cutting-edge experience as a leader in TCP/IP protocol research, updating the book to fully reflect the latest protocols and best practices.

PHP Beyond the WebApress

A tutorial and reference to Java-based APIs for application software development covers such topics as XDoclet, JavaServer Faces, Hibernate API, Enterprise JavaBeans, and J2EE security.

Target Audience This book is not for professional hackers. Instead, this book is made for beginners who have programming experience and are interested in hacking. Here, hacking techniques that can be easily understood have been described. If you only have a home PC, you can test all the examples provided here. I have included many figures that are intuitively understandable rather than a litany of explanations. Therefore, it is possible to gain some practical experience while hacking, since I have only used examples that can actually be implemented. This book is therefore necessary for ordinary people who have a curiosity of hackers and are interested in computers. Organization of the Book This book is made up of five major parts, from basic knowledge to actual hacking code. A beginner is naturally expected to become a hacker while reading this book. Hacking Preparation Briefly introduce the basic Python syntax that is necessary for hacking. Application Hacking Introduce the basic skills to hack an application, such as Keyboard hooking, API hooking and image file hacking. Web Hacking The Virtual Box test environment configuration is used for a Web Shell attack to introduce web hacking, which is currently an important issue. The techniques include SQL Injection, Password Cracking, and a Web Shell Attack. Network Hacking A variety of tools and the Python language can be combined to support network hacking and to introduce the network hacking technique. Briefly, we introduce NMap with the Wireshark tool, and hacking techniques such as Port Scanning, Packet Sniffing, TCP SYN Flood, Slowris Attack are introduced. System Hacking System hacking is difficult to understand for beginners, and in this section, figures are used to introduce difficult concepts. The hacking techniques that are introduced include a Backdoor, Registry Handling, Stack Based Buffer Overflow, and SEH Based Buffer Overflow. While reading this book, it is possible to obtain answers for such problems one by one. After reading the last chapter, you will gain the confidence to be a hacker. Features of this book When you start to study hacking, the most difficult task is to configure the test environment. There are many problems that need to be addressed, such as choosing from the variety in operating systems, obtaining expensive equipment and using complex technology. Such problems are too difficult to take in at once, so this book overcomes this difficulty by implementing a simple idea. First, systems will be described as Windows-based. We are very familiar with Windows, so it is very easy to understand a description based on Windows. Since Windows, Linux, Unix, and Android are all operating systems, it is possible to expand the concepts that are discussed here. Second, we use a virtual machine called Virtual Box. For hacking, it is necessary to connect at least three or more computers on a

network. Since it is a significant investment to buy a few computers only to study these techniques, a virtual machine can be used instead to easily implement a honeypot necessary to hack by creating multiple virtual machines on a single PC. Finally, abstract concepts are explained using figures. Rather than simply using words for descriptions, graphics are very effective in transferring information. An abstract concept can materialize through the use of graphics in order to improve the understanding on the part of the reader.

Start building amazing projects with the Raspberry Pi right out of the box About This Book Explore the vast range of opportunities provided by Raspberry Pi and other hardware components such as a webcam, the Pi camera, and sensors Get hands-on experience with coding, networking, and hardware with the Raspberry Pi platform Learn through ample screenshots that offer a play-by-play account of how to implement Raspberry-Pi-based real-life projects Who This Book Is For What's the best way to learn how to use your Raspberry Pi? By example! If you want something exciting to do whilst getting to grips with what your Pi can offer, this is the book for you. With both simple and complex projects, you'll create a wide variety of cool toys and functions with your Raspberry Pi - all with minimal coding experience necessary. What You Will Learn Set up your Raspberry Pi and get it ready for some interesting real-life projects Work with images, videos, webcams, and the Pi camera and create amazing time-lapse videos Explore the amazing world of Minecraft Pi Get to know how to use PiGlow for GPIO programming Interface your Pi with Grove Sensors and implement IoT applications Build your own cluster with Raspberry Pi Understand the networking and network programming fundamentals In Detail Want to put your Raspberry Pi through its paces right out of the box? This tutorial guide is designed to get you learning all the tricks of the Raspberry Pi through building complete, hands-on hardware projects. Speed through the basics and then dive right in to development! Discover that you can do almost anything with your Raspberry Pi with a taste of almost everything. Get started with Pi Gaming as you learn how to set up Minecraft, and then program your own game with the help of Pygame. Turn the Pi into your own home security system with complete guidance on setting up a webcam spy camera and OpenCV computer vision for image recognition capabilities. Get to grips with GPIO programming to make a Pi-based glowing LED system, build a complete functioning motion tracker, and more. Finally, get ready to tackle projects that push your Pi to its limits. Construct a complete Internet of Things home automation system with the Raspberry Pi to control your house via Twitter; turn your Pi into a super-computer through linking multiple boards into a cluster and then add in advanced network capabilities for super speedy processing! Style and approach This step-by-step guide to building Raspberry-Pi-based projects is explained in a conversational and easy-to-follow style. Each topic is explained sequentially in the process of creating real-life projects, and detailed explanations of the basic and advanced features of various Python libraries are also included.

In the right setting, a single scathing word can prove deadlier than a poisoned dagger. Behind the scenes of heroic battles and magical realms lies a seething underbelly of danger and deception. This world of intrigue holds endless possibilities for adventure, as heroes duel with words instead of steel, plot daring heists, and engage in battles of wills against relentless nemeses. A high-stakes game of shadows and secrets is yours to master--if you have the wits! Whether the heroes are taming the blood-soaked back alleys of their favorite metropolis or jockeying for the queen's favor alongside highborn nobles, Pathfinder RPG Ultimate Intrigue is an invaluable companion to the Pathfinder RPG Core Rulebook. This imaginative tabletop game builds upon more than 10 years of system development and an Open Playtest featuring more than 50,000 gamers to create a cutting-edge RPG experience that brings the all-time best-selling set of fantasy rules into a new era. Pathfinder RPG Ultimate Intrigue includes: * The vigilante, a new character class that lives two lives--that of an unassuming member of the community, and a cloaked crusader with his own agenda! * New archetypes for alchemists, bards, druids, hunters, inquisitors, investigators, mesmerists, rangers, rogues, slayers, spiritualists, and more! * New feats and magic items for characters of all sorts, granting mastery of street-smart combat, impenetrable disguises, and misdirection. * Dozens of spells to manipulate tense social settings, whether to reveal adversaries' secrets or hide the truth. * A complete system of influence, providing new goals and rewards to challenge players and link their fortunes to nonplayer characters and organizations. * Systems and advice to help Game Masters introduce a variety of new encounters into their games¬--daring heists, extended pursuits, and tense searches for buried secrets. * Rules for social combat and verbal duels, allowing characters to use words as weapons to sway hearts and humiliate foes. * ... and much, much more!

An in-depth guide of the FreeBSD Operating System Architecture. This manual is available online for free at freebsd.org. This manual is printed in grayscale.

Taking a highly practical approach and a playful tone, Kali Linux CTF Blueprints provides step-by-step guides to setting up vulnerabilities, in-depth guidance to exploiting them, and a variety of advice and ideas to build and customising your own challenges. If you are a penetration testing team leader or individual who wishes to challenge yourself or your friends in the creation of penetration testing assault courses, this is the book for you. The book assumes a basic level of penetration skills and familiarity with the Kali Linux operating system.

Memory forensics provides cutting edge technology to help investigate digital attacks Memory forensics is the art of analyzing computer memory (RAM) to solve digital crimes. As a follow-up to the best seller Malware Analyst's Cookbook, experts in the fields of malware, security, and digital forensics bring you a step-by-step guide to memory forensics—now the most sought after skill in the digital forensics and incident response fields. Beginning with introductory concepts and moving toward the advanced, The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory is based on a five day training course that the authors have presented to hundreds of students. It is the only book on the market that focuses exclusively on memory forensics and how to deploy such techniques properly. Discover memory forensics techniques: How volatile memory analysis improves digital investigations Proper investigative steps for detecting stealth malware and advanced threats How to use free, open source tools for conducting thorough memory forensics Ways to acquire memory from suspect systems in a forensically sound manner The next era of malware and security breaches are more sophisticated and targeted, and the volatile memory of a computer is often overlooked or destroyed as part of the incident response process. The Art of Memory Forensics explains the latest technological innovations in digital forensics to help bridge this gap. It covers the most popular and recently released versions of Windows, Linux, and Mac, including both the 32 and 64-bit editions.

Turn Vim into a full-blown development environment using Vim 8's new features and this sequel to the beloved bestseller Practical Vim. Integrate your editor with tools for building, testing, linting, indexing, and searching your codebase. Discover the future of Vim with Neovim: a fork of Vim that includes a built-in terminal emulator that will transform your workflow. Whether you choose to switch to Neovim or stick with Vim 8, you'll be a better developer. A serious tool for programmers and web developers, no other text editor comes close to Vim for speed and efficiency. Make Vim the centerpiece of a Unix-based IDE as you discover new ways to work with Vim 8 and Neovim in more than 20 hands-on tips. Execute tasks asynchronously, allowing you to continue in Vim while linting, grepping, building a project, or running a test suite. Install plugins to be loaded on startup - or on-demand when you need them - with Vim 8's new package support. Save and restore sessions, enabling you to quit Vim and restart again while preserving your window layout and undo history. Use Neovim as a drop-in replacement for Vim - it supports all of the features Vim 8 offers and more, including an integrated terminal that lets you quickly perform interactive commands. And if you enjoy using tmux and Vim together, you'll love Neovim's terminal emulator, which lets you run an interactive shell in a buffer. The terminal

buffers fit naturally with Vim's split windows, and you can use Normal mode commands to scroll, search, copy, and paste. On top of all that: Neovim's terminal buffers are scriptable. With Vim at the core of your development environment, you'll become a faster and more efficient developer. What You Need: You'll need a Unix-based environment and an up-to-date release of Vim (8.0 or newer). For the tips about running a terminal emulator, you'll need to install Neovim.

Introduction to the Command Line is a visual guide that teaches the most important Unix and Linux shell commands in a simple and straight forward manner. Command line programs covered in this book are demonstrated with typical usage to aid in the learning process and help you master the command line quickly and easily.Covers popular Unix, Linux, and BSD systems.

Enhance your organization’s secure posture by improving your attack and defense strategies Key Features Gain a clear understanding of the attack methods, and patterns to recognize abnormal behavior within your organization with Blue Team tactics. Learn to unique techniques to gather exploitation intelligence, identify risk and demonstrate impact with Red Team and Blue Team strategies. A practical guide that will give you hands-on experience to mitigate risks and prevent attackers from infiltrating your system. Book Description The book will start talking about the security posture before moving to Red Team tactics, where you will learn the basic syntax for the Windows and Linux tools that are commonly used to perform the necessary operations. You will also gain hands-on experience of using new Red Team techniques with powerful tools such as python and PowerShell, which will enable you to discover vulnerabilities in your system and how to exploit them. Moving on, you will learn how a system is usually compromised by adversaries, and how they hack user's identity, and the various tools used by the Red Team to find vulnerabilities in a system. In the next section, you will learn about the defense strategies followed by the Blue Team to enhance the overall security of a system. You will also learn about an in-depth strategy to ensure that there are security controls in each network layer, and how you can carry out the recovery process of a compromised system. Finally, you will learn how to create a vulnerability management strategy and the different techniques for manual log analysis. By the end of this book, you will be well-versed with Red Team and Blue Team techniques and will have learned the techniques used nowadays to attack and defend systems. What you will learn Learn the importance of having a solid foundation for your security posture Understand the attack strategy using cyber security kill chain Learn how to enhance your defense strategy by improving your security policies, hardening your network, implementing active sensors, and leveraging threat intelligence Learn how to perform an incident investigation Get an in-depth understanding of the recovery process Understand continuous security monitoring and how to implement a vulnerability management strategy Learn how to perform log analysis to identify suspicious activities Who this book is for This book aims at IT professional who want to venture the IT security domain. IT pentester, Security consultants, and ethical hackers will also find this course useful. Prior knowledge of penetration testing would be beneficial.

What is SQL injection? -- Testing for SQL injection -- Reviewing code for SQL injection -- Exploiting SQL injection -- Blind SQL injection exploitation -- Exploiting the operating system -- Advanced topics -- Code-level defenses -- Platform level defenses -- Confirming and recovering from SQL injection attacks -- References.

For system administrators, programmers, and end users, shell command or carefully crafted shell script can save you time and effort, or facilitate consistency and repeatability for a variety of common tasks. This cookbook provides more than 300 practical recipes for using bash, the popular Unix shell that enables you to harness and customize the power of any Unix or Linux system. Ideal for new and experienced users alike—including proficient Windows users and sysadmins—this updated second edition helps you solve a wide range of problems. You’ll learn ways to handle input/output, file manipulation, program execution, administrative tasks, and many other challenges. Each recipe includes one or more scripting examples and a discussion of why the solution works. You’ll find recipes for problems including: Standard output and input, and executing commands Shell variables, shell logic, and arithmetic Intermediate shell tools and advanced scripting Searching for files with find, locate, and slocate Working with dates and times Creating shell scripts for various end-user tasks Working with tasks that require parsing Writing secure shell scripts Configuring and customizing bash

Provides information on competency-based interviews, offers sample questions and answers, and includes fill-in-the-blank exercises.

Demonstrates socket programming fundamentals, including writing servers, creating secure applications, address conversion functions, socket types, and TCP/IP protocols and options

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.

This concise book shows you how to create PHP command line interface (CLI) scripts, including user interaction and scripts to automate and assist your workflow. Learn to quickly create useful and effective command line software and scripts using the world's most popular web scripting language, PHP. Enjoy the benefits of writing CLI scripts in PHP: save money by redeploying existing skills, not learning new ones. Save time and increase productivity by using a high-level language. Make money by providing your clients with a full-stack service. What You'll Learn Learn about the PHP CLI SAPI Find out how to use it to run PHP scripts off-line Easily deal with user input and console output Work with helper libraries and software Find out the differences between programming for the web and for the CLI Who This Book Is For Experienced PHP programmers and web developers.

The programming language Python was conceived in the late 1980s, [1] and its implementation was started in December 1989[2] by Guido van Rossum at CWI in the Netherlands as a successor to the ABC (programming language) capable of exception handling and interfacing with the Amoeba operating system.[3] Van Rossum is Python's principal author, and his continuing central

role in deciding the direction of Python is reflected in the title given to him by the Python community, Benevolent Dictator for Life (BDFL).[4][5] Python was named for the BBC TV show Monty Python's Flying Circus.[6] Python 2.0 was released on October 16, 2000, with many major new features, including a cycle-detecting garbage collector (in addition to reference counting) for memory management and support for Unicode. However, the most important change was to the development process itself, with a shift to a more transparent and community-backed process.[7] Python 3.0, a major, backwards-incompatible release, was released on December 3, 2008[8] after a long period of testing. Many of its major features have also been backported to the backwards-compatible Python 2.6 and 2.7.[9] In February 1991, van Rossum published the code (labeled version 0.9.0) to alt.sources.[10] Already present at this stage in development were classes with inheritance, exception handling, functions, and the core datatypes of list, dict, str and so on. Also in this initial release was a module system borrowed from Modula-3; Van Rossum describes the module as "one of Python's major programming units."[1] Python's exception model also resembles Modula-3's, with the addition of an else clause.[3] In 1994 comp.lang.python, the primary discussion forum for Python, was formed, marking a milestone in the growth of Python's userbase.[1] Python reached version 1.0 in January 1994. The major new features included in this release were the functional programming tools lambda, map, filter and reduce. Van Rossum stated that "Python acquired lambda, reduce(), filter() and map(), courtesy of a Lisp hacker who missed them and submitted working patches."[11] The last version released while Van Rossum was at CWI was Python 1.2. In 1995, Van Rossum continued his work on Python at the Corporation for National Research Initiatives (CNRI) in Reston, Virginia whence he released several versions. By version 1.4, Python had acquired several new features. Notable among these are the Modula-3 inspired keyword arguments (which are also similar to Common Lisp's keyword arguments) and built-in support for complex numbers. Also included is a basic form of data hiding by name mangling, though this is easily bypassed.[12] During Van Rossum's stay at CNRI, he launched the Computer Programming for Everybody (CP4E) initiative, intending to make programming more accessible to more people, with a basic "literacy" in programming languages, similar to the basic English literacy and mathematics skills required by most employers. Python served a central role in this: because of its focus on clean syntax, it was already suitable, and CP4E's goals bore similarities to its predecessor, ABC. The project was funded by DARPA.[13] As of 2007, the CP4E project is inactive, and while Python attempts to be easily learnable and not too arcane in its syntax and semantics, reaching out to non-programmers is not an active concern.[14] Here are what people are saying about the book: This is the best beginner's tutorial I've ever seen! Thank you for your effort. -- Walt Michalik The best thing i found was "A Byte of Python," which is simply a brilliant book for a beginner. It's well written, the concepts are well explained with self evident examples. -- Joshua Robin Excellent gentle introduction to programming #Python for beginners -- Shan Rajasekaran Best newbie guide to python -- Nickson Kaigi start to love python with every single page read -- Herbert Feutl perfect beginners guide for python, will give u key to unlock magical world of python

Use your existing web-based PHP skills to write all types of software: CLI scripts, desktop software, network servers, and more. This book gives you the tools, techniques, and background necessary to write just about any type of software you can think of, using the PHP you know. PHP Beyond the Web shows you how to take your knowledge of PHP development for the web and utilise it with a much wider range of software systems. Enjoy the benefits of PHP after reading this book: save money by redeploying existing skills, not learning new ones; save time and increase productivity by using a high-level language; and make money by providing your clients a full-stack service (not just websites). PHP is no longer just a great scripting language for websites, it's now a powerful general-purpose programming language. Expand your use of PHP into your back-end systems, server software, data processing services, desktop interfaces, and more. What You'll Learn Write interactive shell scripts Work with system daemons Write desktop software Build network servers Interface with electronics using PHP and the Raspberry Pi Manage performance, deployment, licensing, and system interaction Discover the software tools for development and get other great sources of technical information and help Who This Book Is For Experienced PHP programmers or experienced programmers interested in leveraging PHP outside the web development context. /div

Build your own sophisticated modular home security system using the popular Raspberry Pi board About This Book This book guides you through building a complete home security system with Raspberry Pi and helps you remotely access it from a mobile device over the Internet It covers the fundamentals of interfacing sensors and cameras with the Raspberry Pi so that you can connect it to the outside world It follows a modular approach so that you can choose the modules and features you want for your customized home security system Who This Book Is For This book is for anyone who is interested in building a modular home security system from scratch using a Raspberry Pi board, basic electronics, sensors, and simple scripts. This book is ideal for enthusiastic novice programmers, electronics hobbyists, and engineering professionals. It would be great if you have some basic soldering skills in order to build some of the interface modules. What You Will Learn Understand the concepts behind alarm systems and intrusion detection devices Connect sensors and devices to the on-board digital GPIO ports safely Monitor and control connected devices easily using Bash shell scripting Build an I/O port expander using the I2C bus and connect sensors and anti-tamper circuits Capture and store images using motion detectors and cameras Access and manage your system remotely from your mobile phone Receive intrusion alerts and images through your e-mail Build a sophisticated multi-zone alarm system In Detail The Raspberry Pi is a powerful low-cost credit-card-sized computer, which lends itself perfectly as the controller for a sophisticated home security system. Using the on-board interfaces available, the Raspberry Pi can be expanded to allow the connection of a virtually infinite number of security sensors and devices. The Raspberry Pi has the processing power and interfaces available to build a sophisticated home security system but at a fraction of the cost of commercially available systems. Building a Home Security System with Raspberry Pi starts off by showing you the Raspberry Pi and how to set up the Linux-based operating system. It then guides you through connecting switch sensors and LEDs to the native GPIO connector safely, and how to access them using simple Bash scripts. As you dive further in, you'll learn how to build an input/output expansion board using the I2C interface and power supply, allowing the connection of the large number of sensors needed for a typical home security setup. In the later chapters of the book, we'll look at more sophisticated topics such as adding cameras, remotely accessing the system using your mobile phone, receiving intrusion alerts and images by e-mail, and more. By the end of the book, you will be well-versed with the use of Raspberry Pi to power a home-based security system that sends message alerts whenever it is triggered and will be able to build a truly sophisticated and modular home security system. You will also gain a good understanding of Raspberry Pi's ecosystem and be able to write the functions required for a security system. Style and approach This easy-to-follow guide comprises a series of projects, where every chapter introduces a new concept and at the end of the book, all these concepts are brought together to create an entire home security system. This book features clear diagrams and code every step of

the way.
This book is an anthology of effective database management techniques representing the collective wisdom of the OakTable Network. With an emphasis upon performance—but also branching into security, national language, and other issues—the book helps you deliver the most value for your company’s investment in Oracle Database technologies. You’ll learn to effectively plan for and monitor performance, to troubleshoot systematically when things go wrong, and to manage your database rather than letting it manage you.
Just as a professional athlete doesn't show up without a solid game plan, ethical hackers, IT professionals, and security researchers should not be unprepared, either. The Hacker Playbook provides them their own game plans. Written by a longtime security professional and CEO of Secure Planet, LLC, this step-by-step guide to the "game" of penetration hacking features hands-on examples and helpful advice from the top of the field. Through a series of football-style "plays," this straightforward guide gets to the root of many of the roadblocks people may face while penetration testing-including attacking different types of networks, pivoting through security controls, privilege escalation, and evading antivirus software. From "Pregame" research to "The Drive" and "The Lateral Pass," the practical plays listed can be read in order or referenced as needed. Either way, the valuable advice within will put you in the mindset of a penetration tester of a Fortune 500 company, regardless of your career or level of experience. This second version of The Hacker Playbook takes all the best "plays" from the original book and incorporates the latest attacks, tools, and lessons learned. Double the content compared to its predecessor, this guide further outlines building a lab, walks through test cases for attacks, and provides more customized code. Whether you're downing energy drinks while desperately looking for an exploit, or preparing for an exciting new job in IT security, this guide is an essential part of any ethical hacker's library-so there's no reason not to get in the game.
With better ways to get your photos online and new options for creating printed projects, iPhoto '11 makes it easier than ever to transfer photos from a digital camera, organize them, and publish, print, or share them in maps—but there's still no printed manual for the program. Fortunately, David Pogue and Lesa Snider team up in this witty, authoritative book that should have been in the box. Organize your collection. Discover all of the options for grouping your pictures—by events, in albums, or based on who’s in the photo or where it was taken. Sharpen your editing skills. Learn how to use iPhoto’s beefed-up editing options, including its Photoshop-like adjustments panel. Share images online. Get your photos to everyone on your list by publishing them to Flickr, Facebook, and MobileMe. Dive into creative projects. Have fun building slideshows (with music), gift books, calendars, and cards.
An inspirational story of a man who overcame obstacles and challenges to achieve his dreams. In an accident in 1980, Limbie, a healthy young man, was reduced to a quadriplegic. Read through his fears, sorrow, hope and courage in this heart-open honest book.
This book leverages the Cyber Kill Chain to teach you how to hack and detect, from a network forensics perspective. Thus lots of packet and log analysis! There are lots of books that teach you how to hack. So the main purpose of this book is not really about hacking. However, the problem with many of those books, is they don''t teach you how to detect your activities. This means, you the reader have to go read another book, in order to understand the traces of network evidence, indicators of compromise (IoC), events of interests (EoI) and the breadcrumbs which are left behind, as part of your activities related to system compromise. Therefore, this book is truly meant to help you the reader detect sooner, whenever someone compromises your network. Remember, it is not if you will be compromised but when. This statement is assuming you have not already been compromised. To ensure you enjoy this book, it is written from the perspective of storytelling. While most technology related books are done from a how-to guide style, this one is not. However, the objectives remain the same. I believe tying the technical material in with a story, will add more context, make the message clearer and the learning process easier. An important note, as Neysa (Threat Actor) hacks, she plans to use the Lockheed Martin Cyber Kill Chain model as her framework. By leveraging the Cyber Kill Chain, she anticipates she can operate similar to an advanced persistent threat (APT). Where possible, she will follow the model exactly as it is. However, where needed, she may deviate while still being focused on achieving the actions and objectives as identified by the Cyber Kill Chain. For each of the attacks Neysa (Threat Actor) performs, where possible, Nakia (newly hired Cybersecurity Ninja) will leverage her Cybersecurity Ninja awesomeness, to detect Neysa''s actions. More importantly, for each of the attacks that Nakia detects, she must provide answers to the who, what, when, where, why and how to Saadia, the owner of SecurityNik Inc. These are critical questions every incident handler must answer. Now, the reality is, in many cases you may not be able to tell "why" it happened, as you don''t typically know your adversaries motive. However, Nakia will do her best to provide the necessary guidance, thus ensuring she gives Saadia actionable intelligence to decide on the way forward. Here is why you should get this book. Nik''s approach to viewing both the attacker and defender''s side of the compromise is an amazing way to correlate the causes and consequences of every action in an attack. This not only helps the reader learn, but is entertaining and will cause readers to flip all around the book to make sure they catch every detail. Tyler Hudak, Information Security By showing both the offensive and defensive sides of an attack, Nik helps each side better understand how the other operates. Joe Schottman, SANS Advisory Board Member Hack and Detect provides a window into a modern day attack from an advanced persistent threat in an easy to follow story format. Nik walks through the Cyber Kill Chain from both an offensive perspective, showing tools and tricks an attacker would leverage, and a defensive perspective, highlighting the breadcrumbs which are left behind. By following along step by step with virtual machines the reader is able to obtain a greater understanding of how the attacks work in the real world and gain valuable insight into defending against them. Daniel McAuley, Manager Infrastructure and Technology Group Looking to follow along without building a lab? I got you! Grab the full set of pcaps, logs, etc from my GitHub page at https://github.com/SecurityNik/SUWtHEh- Looking for sample chapters? You''re covered here too!!:http://bit.ly/NikAlleyne-Hack-and-Detect-Book www.securitynik.com