

Ultravnc Installation Guide

IBM® is a Platinum level Partner in the Oracle Partner Network, which delivers the proven combination of industry insight, extensive real-world Oracle applications experience, deep technical skills, and high-performance servers and storage to create a complete business solution with a defined return on investment. From application selection, purchase, and implementation to upgrade and maintenance, we help organizations reduce the total cost of ownership and the complexity of managing their current and future applications environment while building a solid base for business growth. Oracle Database running on Linux is available for deployment on IBM LinuxONE by using Redhat Enterprise Linux (RHEL) or SUSE Linux Enterprise Server (SLES). This enterprise-grade solution is designed to add value to Oracle Database solutions. This IBM Redpaper® publication focuses on accepted good practices for installing and getting started by using Oracle Database, which provides you with an environment that is optimized for performance, scalability, flexibility, and ease-of-management.

The popularity of wireless networking has grown exponentially over the past few years, despite a general downward trend in the telecommunications industry. More and more computers and users worldwide communicate via radio waves every day, cutting the tethers of the cabled network both at home and at work. Wireless technology changes not only the way we talk to our devices, but also what we ask them to do. With greater flexibility, broader range, and increased mobility, wireless networks let us live, work, and think differently. Wireless networks also open up a vast range of tasty new hack possibilities, from fine-tuning network frequencies to hot-rodding handhelds. The second edition of *Wireless Hacks*, co-authored by Rob Flickenger and Roger Weeks, brings readers more of the practical tips and tricks that made the first edition a runaway hit, selling nearly 30,000 copies.

Completely revised and updated, this version includes over 30 brand new hacks, major overhauls of over 30 more, and timely adjustments and touchups to dozens of other hacks introduced in the first edition. From passive network scanning to aligning long-distance antennas, beefing up wireless network security, and beyond, *Wireless Hacks* answers real-life networking needs with direct solutions. Flickenger and Weeks both have extensive experience in systems and network administration, and share a passion for making wireless more broadly available. The authors include detailed coverage for important new changes in specifications and in hardware and software, and they delve deep into cellular and Bluetooth technologies. Whether you need your wireless network to extend to the edge of your desk, fit into your backpack, or cross county lines, the proven techniques in *Wireless Hacks* will show you how to get the coverage and functionality you're looking for.

Red teams can show flaws that exist in your network before they are compromised by malicious actors and blue teams traditionally assess current security measures and identify security flaws. The teams can provide valuable feedback to each other, but this is often overlooked, enter the purple team. The purple team allows for the integration of red team tactics and blue team security measures. The purple team field manual is a manual for all security professionals and integrates red and blue team methodologies.

This book addresses automated software fingerprinting in binary code, especially for cybersecurity applications. The reader will gain a thorough understanding of binary code analysis and several software fingerprinting techniques for cybersecurity applications, such as malware detection, vulnerability analysis, and digital forensics. More specifically, it starts with an overview of binary code analysis and its challenges, and then discusses the existing state-of-the-art approaches and their cybersecurity applications. Furthermore, it discusses and details a set of practical techniques for compiler provenance extraction, library function identification, function fingerprinting, code reuse detection, free open-source software identification, vulnerability search, and authorship attribution. It also illustrates several case studies to demonstrate the efficiency, scalability and accuracy of the above-mentioned proposed techniques and tools. This book also introduces several innovative quantitative and qualitative techniques that synergistically leverage machine learning, program analysis, and software engineering methods to solve binary code fingerprinting problems, which are highly relevant to cybersecurity and digital forensics applications. The above-mentioned techniques are cautiously designed to gain satisfactory levels of efficiency and accuracy. Researchers working in academia, industry and governmental agencies focusing on Cybersecurity will want to purchase this book. Software engineers and advanced-level students studying computer science, computer engineering and software engineering will also want to purchase this book.

Binary Code Fingerprinting for Cybersecurity

Defeating the Hacker

PC Magazine

The No-nonsense Guide to Training in Libraries

Microsoft Windows 7

Linux Networking Cookbook

Featuring crucial information on how to secure a network, this text covers IT security, hackers, crackers, phishers, spammers, scammers, virus-writers, Trojan horses, malware, spyware - and how to keep these technical afflictions out of computer systems.

A guide to the failings of Windows 98 explains how to customize the system so as to avoid the inconvenience of software applications that overwrite file associations, repetitive warning screens, and unused icons crowding the desktop

Prepare for success on the new PenTest+ certification exam and an exciting career in penetration testing In the revamped Second Edition of CompTIA PenTest+ Study Guide: Exam PT0-002, veteran information security experts Dr. Mike Chapple and David Seidl deliver a comprehensive roadmap to the foundational and advanced skills every pentester (penetration tester) needs to secure their CompTIA PenTest+ certification, ace their next interview, and succeed in an exciting new career in a growing field. You'll learn to perform security assessments of traditional servers, desktop and mobile operating systems, cloud installations, Internet-of-Things devices, and industrial or embedded systems. You'll plan and scope a penetration testing engagement including vulnerability scanning, understand legal and regulatory compliance requirements, analyze test results, and produce a written report with remediation techniques. This book will: Prepare you for success on the newly introduced CompTIA PenTest+ PT0-002 Exam Multiply your career opportunities with a certification that complies with ISO 17024 standards and meets Department of Defense Directive

8140/8570.01-M requirements Allow access to the Sybex online learning center, with chapter review questions, full-length practice exams, hundreds of electronic flashcards, and a glossary of key terms Perfect for anyone preparing for the updated CompTIA PenTest+ certification exam, CompTIA PenTest+ Study Guide: Exam PT0-002 is also a must-read resource for aspiring penetration testers and IT security professionals seeking to expand and improve their skillset.

Web Survey Creator Reference GuideLulu.comCompTIA PenTest+ Study GuideExamJohn Wiley & Sons

The Definitive Guide of the PfSense Open Source Firewall and Router Distribution

A High Speed Guide to Starting a Business

Internet Accessible Remote Laboratories: Scalable E-Learning Tools for Engineering and Science Disciplines

3 Weeks to Startup

E-Learning: Strategies for Delivering Knowledge in the Digital Age

An Essential Guide for the Accidental Admin

Singapore's leading tech magazine gives its readers the power to decide with its informative articles and in-depth reviews.

Companion CD includes a 30-day trial version of Camtasia Studio 5! Camtasia Studio 5: The Definitive Guide introduces readers to the latest features of Camtasia Studio, including the revamped Recorder application, automated zooming and panning with SmartFocus, and upload via FTP. Readers learn the entire process of creating top-notch software tutorials, marketing spots, and demonstrations, beginning with developing goals and determining the audience to scripting, recording, editing, producing, and sharing the video. Appropriate for users at all levels, this book provides a practical guide to getting the most out of Camtasia Studio. Learn how to record audio and video streams and add special effects with Camtasia Recorder; extend and split media clips, add callouts and Flash hotspots, and create quizzes and surveys; enhance your videos with a picture-in-picture track; convert your PowerPoint presentations to Camtasia Studio recordings; produce your videos for distribution via CD, DVD, the web, and portable media players

This concise guide covers every edition of Windows 7 in Visual QuickStart style, with plenty of screenshots, numbered steps, tips, and sidebars. You'll learn how to use new and updated features, including the redesigned taskbar; jump lists; libraries; federated search; desktop gadgets; window-management shortcuts; and the improved versions of Internet Explorer, Mail, Messenger, Photo Gallery, Movie Maker, and Media Player. You'll also find information on setup; installation; upgrading from other Windows versions; troubleshooting; hardware; and organizing your documents, music, photos, and videos. Laptop and mobile users will learn how to connect from the road, jump onto a public wireless network, and conserve battery power. Author Chris Fehily also walks you through setting up a network or homegroup, connecting to the internet, configuring routers and firewalls, and hooking up printers and other devices. You'll learn how to use security features to protect your PC and network and share files while keeping personal stuff private.

"This book presents current developments in the multidisciplinary creation of Internet accessible remote laboratories, offering perspectives on teaching with online laboratories, pedagogical design, system architectures for remote laboratories, future trends, and policy issues in the use of remote laboratories"--Provided by publisher.

Application to Malicious Code Fingerprinting

PfSense.org

The Independent Guide to IBM-standard Personal Computing

Network Security Assessment

Master Your Raspberry Pi in 30 Days

Securing Cisco IP Telephony Networks

Internet and intranet technologies offer tremendous opportunities to bring learning into the mainstream of business. E-Learning outlines how to develop an organization-wide learning strategy based on cutting-edge technologies and explains the dramatic strategic, organizational, and technology issues involved. Written for professionals responsible for leading the revolution in workplace learning, E-Learning takes a broad, strategic perspective on corporate learning. This wake-up call for executives everywhere discusses: • Requirements for building a viable e-learning strategy • How online learning will change the nature of training organizations • Knowledge management and other new forms of e-learning Marc J. Rosenberg, Ph.D. (Hillsborough, NJ) is an independent consultant specializing in knowledge management, e-learning strategy and the reinvention of training. Prior to this, he was a senior direction and knowledge management field leader for consulting firm DiamondCluster International.

Companion CD includes a trial version of Camtasia Studio 4! With the latest release of Camtasia Studio, TechSmith continues to enhance its industry-leading screen video recording and editing tool. Camtasia Studio 4: The Definitive Guide describes the newest features and takes the user through the entire process of creating top-notch software tutorials, marketing spots, and demonstrations. This book provides a practical guide to getting the most out of Camtasia Studio, with topics ranging from developing goals, determining the audience, and storyboarding to recording, editing, and producing. Learn how to; record content and create special effects with the Camtasia Recorder; select, rearrange, trim, and extend video clips; enhance your audio using new sound manipulation techniques; collect data from viewers with the survey feature; produce your video for distribution via CD, DVD, the web, and portable media players; add closed captioning to make your videos more accessible. With this text, learn how to record content and creat special effects with the Camtasia Recorder Select, rearrange, trim, and extend video clips; enhance your audio using new sound manipulation techniques; collect data from viewers with the survey feature; produce your video for distribution via CD, DVD, the web, and portable media players; add closed captioning to make your videos more accessible.

Maximum PC is the magazine that every computer fanatic, PC gamer or content creator must read. Each and every issue is packed with punishing product reviews, insightful and innovative how-to stories and the illuminating technical articles that enthusiasts crave.

Dive deeper into Windows 7—with new content and new resources on CD! The Deluxe Edition of the ultimate, in-depth reference to Windows 7 has been fully updated for SP1 and Internet Explorer 9, and features 300+ pages of additional coverage and advanced topics. It ' s now packed with even more timesaving solutions, troubleshooting tips, and workarounds from the experts—and includes a fully searchable eBook and other online resources. Topics include installation, configuration, and setup; network connections and troubleshooting; remote access; managing programs; controlling user access and accounts; advanced file management; working with Internet Explorer 9; managing security features and issues; using Windows Live Essentials 2011; performance monitoring and tuning; backups and maintenance; sharing networked resources; hardware and device drivers. For customers who purchase an ebook version of this title, instructions for downloading the CD files can be found in the ebook.

SSL Remote Access VPNs (Network Security)

Maximum PC

Network Know-How

Camtasia Studio 4

Kali Linux Cookbook - Second Edition

CASP+ CompTIA Advanced Security Practitioner Certification All-in-One Exam Guide, Second Edition (Exam CAS-003)

Are the machines in your office living isolated lives? Do you have a few computers at home that you want to connect to each other and the Internet? The best way to share files on a group of computers is to create a network. But how do you do that? Network Know-How is your guide to connecting your machines, filled with practical advice that will show you how to get things done. You'll learn the nitty-gritty of network setup, design, and maintenance, from running cables and placing wireless access points to configuring file sharing and printing. This practical and comprehensive guide will teach you how to implement security, create intranets, and more. You'll learn how to: –Connect Windows, Macintosh, and Linux computers –Implement network addressing –Configure your network adapters, hubs, switches, and router –Share music, photos, and documents –Automate household appliances and stream digital audio and video to your home entertainment center –Troubleshoot network slowdowns and failures No matter which operating system you use, and even if you've never installed or run a network before, you'll get what you need to know in Network Know-How.

Written by pfSense co-founder Chris Buechler and pfSense consultant Jim Pingle, this Definitive Guide to pfSense covers installation and basic configuration through advanced networking and firewalling with the popular open source firewall and router distribution. This book is designed to be a friendly step-by-step guide to common networking and security tasks, plus a thorough reference of pfSense's capabilities. The book covers hardware and system planning, installation and upgrades, backups, firewalling fundamentals, port forwarding and Network Address Translation, bridging, Virtual LANs (VLAN), Multi-WAN, Virtual Private Networks (VPN) using IPsec, PPTP, and OpenVPN, traffic shaping, load balancing, wireless networking and captive portal setups, redundant firewalls and High Availability, system monitoring, logging, traffic analysis, sniffing, packet capturing, troubleshooting, and software package and third-party software installations and upgrades.

Every computer crime leaves tracks—you just have to know where to find them. This book shows you how to collect and analyze the digital evidence left behind in a digital crime scene. Computers have always been susceptible to unwanted intrusions, but as the sophistication of computer technology increases so does the need to anticipate, and safeguard against, a corresponding rise in computer-related criminal activity. Computer forensics, the newest branch of computer security, focuses on the aftermath of a computer security incident. The goal of computer forensics is to conduct a structured investigation to determine exactly what happened, who was responsible, and to perform the investigation in such a way that the results are useful in a criminal proceeding. Written by two experts in digital investigation, Computer Forensics provides extensive information on how to handle the computer as evidence. Kruse and Heiser walk the reader through the complete forensics process—from the initial collection of evidence through the final report. Topics include an overview of the forensic relevance of encryption, the examination of digital evidence for clues, and the most effective way to present your evidence and conclusions in court. Unique forensic issues associated with both the Unix and the Windows NT/2000 operating systems are thoroughly covered. This book provides a detailed methodology for collecting, preserving, and effectively using evidence by addressing the three A's of computer forensics: Acquire the evidence without altering or damaging the original data. Authenticate that your recorded evidence is the same as the original seized data. Analyze the data without modifying the recovered data. Computer Forensics is written for everyone who is responsible for investigating digital criminal incidents or who may be interested in the techniques that such investigators use. It is equally helpful to those investigating hacked web servers, and those who are investigating the source of illegal pornography.

Three weeks? Can you really start a business in three weeks? Yes, you can. Tim Berry, business planning expert and principal author of Business Plan Pro, the country's bestselling business plan software, and Sabrina Parsons, co-founder of Palo Alto Software UK, unveil a new, more innovative business landscape and show you how to streamline your startup using the fastest resource in the world—the internet. Eliminate the exhausting, time-consuming legwork involved in traditional startup plans, and instead fast track your business using a wealth of online tools and services. Berry and Parsons help you build your business step by step, including establishing your business plan, making your business legal, financing your venture, hiring your staff and more—using online tools and resources at every stage. Discover how easy it is to reach your dream of opening your own business faster than you ever thought possible. Let the countdown begin—you're just 3 weeks away from opening the doors to your new business!

HWM

The Complete Guide to Network Access Control

Exam

Lifehacker

From Asterisk to Zebra with Easy-to-Use Recipes

Tips & Tools for Building, Extending, and Securing Your Network

A new edition, packed with even more clever tricks and methods that make everyday life easier Lifehackers redefine personal productivity with creative and clever methods for making life easier and more enjoyable. This new edition of a perennial bestseller boasts new and exciting tips, tricks, and methods that strike a perfect balance between current technology and common sense solutions for getting things done. Exploring the many ways technology has changed since the previous edition, this new edition has been updated to reflect the latest and greatest in technological and personal productivity. The new "hacks" run the gamut of working with the latest Windows and Mac operating systems for both Windows and Apple, getting more done with smartphones and their operating systems, and dealing with the evolution of the web. Even the most tried-and-true hacks have been updated to reflect the contemporary tech world and the tools it provides us. Technology is supposed to make our lives easier by helping us work more efficiently. Lifehacker: The Guide to Working Smarter, Faster, and Better, Third Edition is your guide to making that happen!

The completely updated NETWORK+ GUIDE TO NETWORKS, 6th Edition gives students the technical skills and industry know-how required to begin an exciting career installing, configuring, and troubleshooting computer networks. The text also prepares students for CompTIA's Network+ N10-005 certification exam with fundamentals in protocols, topologies, hardware, and network design. After exploring TCP/IP, Ethernet, wireless transmission, and security concepts, as well as an all-new chapter on virtual networks, students can increase their knowledge with the practical On-the-Job stories, Review Questions, Hands-On Projects, and Case Projects. NETWORK+ GUIDE TO NETWORKS, 6th Edition also includes reference appendices, a glossary, and full-color illustrations. The features of the text combined with its emphasis on real-world problem solving, provides students with the tools they need to succeed in any computing environment. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

Kali Linux is an open source Linux distribution for security, digital forensics, and penetration testing tools, and is now an operating system for Linux users. It is the successor to BackTrack, the world's most popular penetration testing distribution tool. In this age, where online information is at its most vulnerable, knowing how to execute penetration testing techniques such as wireless and password attacks, which hackers use to break into your system or network, help you plug loopholes before it's too late and can save you countless hours and money. Kali Linux Cookbook, Second Edition is an invaluable guide, teaching you how to install Kali Linux and set up a virtual environment to perform your tests. You will learn how to eavesdrop and intercept traffic on wireless networks, bypass intrusion detection systems, attack web applications, check for open ports, and perform data forensics. This book follows the logical approach of a penetration test from start to finish with many screenshots and illustrations that help to explain each tool in detail. This book serves as an excellent source of information for security professionals and novices alike.

Explaining how to use the new features of Windows 7, a comprehensive manual details hundreds of timesaving solutions, troubleshooting tips, and workarounds, along with information on such topics as Internet Explorer 8, Windows Media Center, networking, and security.

Windows 98 Annoyances

Upgrade Your Life

Wireless Hacks

Best practices and Getting Started Guide for Oracle on IBM LinuxONE

A Step-by-step Guide for Beginners on Raspberry Pi

*Members of AVIEN (the Anti-Virus Information Exchange Network) have been setting agendas in malware management for several years: they led the way on generic filtering at the gateway, and in the sharing of information about new threats at a speed that even anti-virus companies were hard-pressed to match. AVIEN members represent the best-protected large organizations in the world, and millions of users. When they talk, security vendors listen: so should you. AVIEN's sister organization AVIEWS is an invaluable meeting ground between the security vendors and researchers who know most about malicious code and anti-malware technology, and the top security administrators of AVIEN who use those technologies in real life. This new book uniquely combines the knowledge of these two groups of experts. Anyone who is responsible for the security of business information systems should be aware of this major addition to security literature. * "Customer Power" takes up the theme of the sometimes stormy relationship between the antivirus industry and its customers, and tries to dispel some common myths. It then considers the roles of the independent researcher, the vendor-employed specialist, and the corporate security specialist. * "Stalkers on Your Desktop" considers the thorny issue of malware nomenclature and then takes a brief historical look at how we got here, before expanding on some of the malware-related problems we face today. * "A Tangled Web" discusses threats and countermeasures in the context of the World Wide Web. * "Big Bad Bots" tackles bots and botnets, arguably Public Cyber-Enemy Number One. * "Crème de la CyberCrime" takes readers into the underworld of old-school virus writing, criminal business models, and predicting future malware hotspots. * "Defense in Depth" takes a broad look at DiD in the enterprise, and looks at some specific tools and technologies. * "Perilous Outsourcing" offers sound advice on how to avoid the perils and pitfalls of outsourcing, incorporating a few horrible examples of how not to do it. * "Education in Education" offers some insights into user education from an educationalist's perspective, and looks at various aspects of security in schools and other educational establishments. * "DIY Malware Analysis" is a hands-on, hands-dirty approach to security management, considering malware analysis and forensics techniques and tools. * "Antivirus Evaluation & Testing" continues the D-I-Y theme, discussing at length some of the thorny issues around the evaluation and testing of antimlware software. * "AVIEN & AVIEWS: the Future" looks at future developments in AVIEN and AVIEWS. * Unique, knowledgeable, unbiased and hype-free commentary. * Written by members of the anti-malware community; most malware books are written by outsiders. * Combines the expertise of truly knowledgeable systems administrators and managers, with that of the researchers who are most experienced in the analysis of malicious code, and the development and maintenance of defensive programs.*

World-class preparation for the new PenTest+ exam The CompTIA PenTest+ Study Guide: Exam PT0-001 offers comprehensive preparation for the newest intermediate cybersecurity certification exam. With expert coverage of Exam PT0-001 objectives, this book is your ideal companion throughout all stages of study; whether you're just embarking on your certification journey or finalizing preparations for the big day, this invaluable resource helps you solidify your understanding of essential skills and concepts. Access to the Sybex online learning environment allows you to study anytime, anywhere with electronic flashcards, a searchable glossary, and more, while hundreds of practice exam questions help you step up your preparations and avoid surprises on exam day. The CompTIA PenTest+ certification validates your skills and knowledge surrounding second-generation penetration testing, vulnerability assessment, and vulnerability management on a variety of systems and devices, making it the latest go-to qualification in an increasingly mobile world. This book contains everything you need to prepare; identify what you already know, learn what you don't know, and face the exam with full confidence! Perform security assessments on desktops and mobile devices, as well as cloud, IoT, industrial and embedded systems Identify security weaknesses and

manage system vulnerabilities Ensure that existing cybersecurity practices, configurations, and policies conform with current best practices Simulate cyberattacks to pinpoint security weaknesses in operating systems, networks, and applications As our information technology advances, so do the threats against it. It's an arms race for complexity and sophistication, and the expansion of networked devices and the Internet of Things has integrated cybersecurity into nearly every aspect of our lives. The PenTest+ certification equips you with the skills you need to identify potential problems—and fix them—and the CompTIA PenTest+ Study Guide: Exam PT0-001 is the central component of a complete preparation plan.

This book contains the refereed proceedings of the 11th International Conference on Agile Software Development, XP 2010, held in Trondheim, Norway, in June 2010. In order to better evaluate the submitted papers and to highlight the applicational aspects of agile software practices, there were two different program committees, one for research papers and one for experience reports. Regarding the research papers, 11 out of 39 submissions were accepted as full papers; and as far as the experience reports were concerned, the respective number was 15 out of 50 submissions. In addition to these papers, this volume also includes the short research papers, the abstracts of the posters, the position papers of the PhD symposium, and the abstracts of the panel on “Collaboration in an Agile World”.

This book is aimed at helping experienced trainers, as well as those who are still developing their skills, and provides guidance on the design and delivery of effective training courses with topics including: the people side of training; use of technologies to support training practices; different approaches to learning and teaching; planning and designing training; delivering training: face-to-face and blended learning; evaluation of training events and continuous improvement; and learning and development in the workplace. This guide uses case studies and examples of best practice from public, school, academic, special, and government libraries.

Windows 7 Inside Out, Deluxe Edition

The Definitive Guide

Computer Forensics

Windows 7 Inside Out

11th International Conference, XP 2010, Trondheim, Norway, June 1-4, 2010, Proceedings

CompTIA PenTest+ Study Guide

The book teaches the reader about all aspects of NAC/NAP technology. It begins with an introduction on the evolution of NAC/NAP, followed by a detailed explanation into the various technologies and terms associated with NAC/NAP. Next, detailed examples of why the various types of NAC/NAP are necessary are provided. These examples include specific real-world hacking scenarios that the NAC/NAP solutions would prevent. The next portion of the book covers the three leading NAC/NAP offerings, which include Cisco NAC, Microsoft NAP and Mobile NAC. Additional NAC/NAP solutions are also covered, and the book concludes with case studies on companies that have implemented the solutions.

Interest in agile development continues to grow: the number of practitioners adopting such methodologies is increasing as well as the number of researchers investigating the effectiveness of the different practices and proposing improvements. The XP conference series has actively participated in these processes and supported the evolution of Agile, promoting the conference as a place where practitioners and researchers meet to exchange ideas, experiences, and build connections. XP 2010 continued in the tradition of this conference series and provided an interesting and varied program. As usual, we had a number of different kinds of activities in the conference program including: research papers, experience reports, tutorials, workshops, panels, lightning talks, and posters. These proceedings contain full - search papers, short research papers, and experience reports. Moreover, we have also included in these proceedings the abstracts of the posters, the position papers of the PhD symposium, and the abstract of the panel. This year we had two different program committees for evaluating research papers and experience reports. Each committee included experts in the specific area. This approach allowed us to better evaluate the quality of the papers and provide better suggestions to the authors to improve the quality of their contributions.

Publisher's Note: Products purchased from Third Party sellers are not guaranteed by the publisher for quality, authenticity, or access to any online entitlements included with the product. Complete coverage of every topic on the CompTIA Advanced Security Practitioner certification exam Get complete coverage of all objectives included on the CompTIA CASP+ exam CAS-003 from this comprehensive resource. Written by a team of leading information security experts, this authoritative guide fully addresses the skills required for securing a network and managing risk. You ' ll find learning objectives at the beginning of each chapter, exam tips, practice exam questions, and in-depth explanations. Designed to help you pass the exam with ease, this definitive volume also serves as an essential on-the-job reference. Covers all exam domains, including:•Threats, attacks, and vulnerabilities•Technologies and tools •Architecture and design•Identity and access management •Risk management•Cryptography and PKIElectronic content includes:•200 practice exam questions

SSL Remote Access VPNs An introduction to designing and configuring SSL virtual private networks Jazib Frahim, CCIE® No. 5459 Qiang Huang, CCIE No. 4937 Cisco® SSL VPN solutions (formerly known as Cisco WebVPN solutions) give you a flexible and secure way to extend networking resources to virtually any remote user with access to the Internet and a web browser. Remote access based on SSL VPN delivers secure access to network resources by establishing an encrypted tunnel across the Internet using a broadband (cable or DSL) or ISP dialup connection. SSL Remote Access VPNs provides you with a basic working knowledge of SSL virtual private networks on Cisco SSL VPN-capable devices. Design guidance is provided to assist you in implementing SSL VPN in existing network infrastructures. This includes examining existing hardware and software to determine whether they are SSL VPN capable, providing design recommendations, and guiding you on setting up the Cisco SSL VPN devices. Common deployment scenarios are covered to assist you in deploying an SSL VPN in your network. SSL Remote Access VPNs gives you everything you need to know to understand, design, install, configure, and troubleshoot all the components that make up an effective, secure SSL VPN solution. Jazib Frahim, CCIE® No. 5459, is currently working as a technical leader in the Worldwide Security Services Practice of the Cisco Advanced Services for Network Security. He is responsible for guiding customers in the design and implementation of their networks, with a focus on network security. He holds two CCIEs, one in routing and switching and the other in security. Qiang Huang, CCIE No. 4937, is a product manager in the Cisco Campus Switch System Technology Group, focusing on driving the security and intelligent services roadmap for market-leading modular Ethernet switching platforms. During his time at Cisco, Qiang has played an important role in a number of technology groups, including the Cisco TAC security and VPN team, where he was responsible for trouble-shooting complicated customer deployments in security and VPN solutions. Qiang has extensive knowledge of security and VPN technologies and experience in real-life customer deployments. Qiang holds CCIE certifications in routing and switching, security, and ISP Dial. Understand remote access VPN technologies, such as Point-to-Point Tunneling Protocol (PPTP), Internet Protocol Security (IPsec), Layer 2 Forwarding (L2F), Layer 2 Tunneling (L2TP) over IPsec, and SSL VPN Learn about the building blocks of SSL VPN, including

cryptographic algorithms and SSL and Transport Layer Security (TLS) Evaluate common design best practices for planning and designing an SSL VPN solution Gain insight into SSL VPN functionality on Cisco Adaptive Security Appliance (ASA) and Cisco IOS® routers Install and configure SSL VPNs on Cisco ASA and Cisco IOS routers Manage your SSL VPN deployment using Cisco Security Manager This security book is part of the Cisco Press® Networking Technology Series. Security titles from Cisco Press help networking professionals secure critical data and resources, prevent and mitigate network attacks, and build end-to-end self-defending networks. Category: Networking: Security Covers: SSL VPNs

Implementing NAP and NAC Security Technologies

Know Your Network

A Non-technical Guide to Computer Security

Scalable E-Learning Tools for Engineering and Science Disciplines

Purple Team Field Manual

Web Survey Creator Reference Guide

This soup-to-nuts collection of recipes covers everything you need to know to perform your job as a Linux network administrator, whether new to the job or have years of experience. With Linux Networking Cookbook, you'll dive straight into the gnarly hands-on work of building and maintaining a computer network. Running a network doesn't mean you have all the answers. Networking is a complex subject with reams of reference material that's difficult to keep straight, much less remember. If you want a book that lays out the steps for specific tasks, explains the commands and configurations, and does not tax your patience with endless ramblings and meanderings into theory and obscure RFCs, this is the book for you. You will find recipes for: Building a gateway, firewall, and wireless access point on a Linux network Build a VoIP server with Asterisk Secure remote administration with SSH Building secure VPNs with OpenVPN, and a Linux PPTP VPN server Simple sign-on with Samba for mixed Linux/Windows LANs Centralized network directory with OpenLDAP Network monitoring with Nagios or Munin Getting acquainted with IPv6 Setting up hands-free networks installations of new systems Linux system administration via serial console and more. Each recipe includes a clear, hands-on solution with tested code, plus a discussion on why it works. When you need to solve a network problem without delay, and don't have the time or patience to comb through reference books or the Web for answers, Linux Networking Cookbook gives you exactly what you need.

The real-world guide to securing Cisco-based IP telephony applications, devices, and networks Cisco IP telephony leverages converged networks to dramatically reduce TCO and improve ROI. However, its critical importance to business communications and deep integration with enterprise IP networks make it susceptible to attacks that legacy telecom systems did not face. Now, there's a comprehensive guide to securing IP telephony components that ride atop data network infrastructures—and thereby providing IP telephony services that are safer, more reliable, more stable, and more scalable. Securing Cisco IP Telephony Networks provides comprehensive, up-to-date details for securing Cisco IP telephony equipment, underlying infrastructure, and telephony applications. Drawing on ten years of experience, senior network consultant Akhil Bhatia offers a complete security framework for use in any Cisco IP telephony environment. You'll find best practices and detailed configuration examples for securing Cisco Unified Communications Manager (CUCM), Cisco Unity/Unity Connection, Cisco Unified Presence, Cisco Voice Gateways, Cisco IP Telephony Endpoints, and many other Cisco IP Telephony applications. The book showcases easy-to-follow Cisco IP Telephony applications and network security-centric examples in every chapter. This guide is invaluable to every technical professional and decision-maker concerned with securing Cisco IP telephony networks, including network engineers, administrators, architects, managers, analysts, IT directors, and consultants. Recognize vulnerabilities caused by IP network integration, as well as VoIP's unique security requirements Discover how hackers target IP telephony networks and proactively protect against each facet of their attacks Implement a proven methodology for end-to-end Cisco IP Telephony security Use a layered (defense-in-depth) approach that builds on underlying network security design Secure CUCM, Cisco Unity/Unity Connection, CUPS, CUCM Express, and Cisco Unity Express platforms against internal and external threats Establish physical security, Layer 2 and Layer 3 security, and Cisco ASA-based perimeter security Complete coverage of IP Telephony encryption and authentication fundamentals Configure Cisco IOS Voice Gateways to help prevent toll fraud and deter attacks Secure Cisco Voice Gatekeepers and Cisco Unified Border Element (CUBE) against rogue endpoints and other attack vectors Secure Cisco IP telephony endpoints—Cisco Unified IP Phones (wired, wireless, and soft phone) from malicious insiders and external threats This IP communication book is part of the Cisco Press® Networking Technology Series. IP communications titles from Cisco Press help networking professionals understand voice and IP telephony technologies, plan and design converged networks, and implement network solutions for increased productivity.

A practical handbook for network administrators who need to develop and implement security assessment programs, exploring a variety of offensive technologies, explaining how to design and deploy networks that are immune to offensive tools and scripts, and detailing an effective testing model. Original. (Intermediate)

From beginner to expert in Raspberry Pi. Learn useful Linux skills and practice multiples project with step-by-step guides How To Become a Raspberry Pi Expert Even If You Are Not Already A Linux Guru? The Raspberry Pi is a device that can scare many people when they are first introduced to this. How can a cheap electronic circuit with a mysterious operating system be a good idea for me? Yes, the Raspberry Pi is a small computer (close to a credit card size) that runs mostly on Linux and that can be plugged to a standard screen, mouse and keyboard. So, this is pretty little different from what you're used to. That's why it may be difficult or at least not motivating to get started on Raspberry Pi. But don't worry with this book you will get everything you need for a good start, whatever your current level is. About the author Patrick Fromaget graduated from higher school in computer science. He started as a web developer, before specializing in system administration. He has always been passionate about IT and has managed Linux servers for over 15 years. In 2018, he launched the RaspberryTips.com website to share his knowledge for the Raspberry Pi and help other people to progress. More than 100 tutorials have been written on the site, on various subjects. From the site has enjoyed growing success and a YouTube channel was also launched on the subject in 2020, to help the most visual. What is this book? This book is a challenge you take, to lead you from the beginning towards mastering the Raspberry Pi device. The course is divided into 30 steps. The idea is to make one little step a day to be an expert in 30 days. In each step you discover a new concept, go through the details and go to practice. Each day is a new, progressive step towards your goal. In the beginning you learn more about the hardware, then you will learn how to use the operating system (Raspbian). The second part of the book is more about step-by-step projects, programming, and other topics on systems and software. So, it's really a book for all audiences: - If you don't know anything yet, you can read the book in order - If you already have a base on Raspberry Pi or Linux, some chapters can be browsed quickly - And even if you already have a correct level, you will inevitably find information there to go even further Ready to take off? Linux is a skill in great demand in business, and learning it on a different computer is the best way to learn it. The Raspberry Pi was created to teach IT and programming in schools, and it's never too late to learn. To go through the learning process, you need a companion, and you have found it here. This book is a must-have for anyone who wants to improve its skills on Raspberry Pi and Linux in general. Buy it today to become a Raspberry Pi expert in 30 days!

PTFM

Visual QuickStart Guide

The Guide to Working Smarter, Faster, and Better

The Lifehacker Guide to Working Smarter, Faster, Better

PC World

AVIEN Malware Defense Guide for the Enterprise