

Steganos Online Shield Vpn Serial Key Free

A thorough guide to Linux TCP/IP network administration examines the major flavors of Linux; covers routing, file management, directory services, e-mail, security, and internetworking with Samba; and provides implementation examples, troubleshooting tips, and much more. Original. (Advanced).

TOEFL 1200 Words in 30 Days is for students in narrow time frame to prepare tests. Its proper vocabulary and organization bring great efficiency and convenience to tens of thousands and help them up scores. In fact, it isn't simply an ebook. Based on its proven contents, Pacific Lava School offers online options to let students build vocabulary quicker and easier from www.pacificlava.com and www.ienglishtest.com. Various online courses and resources are contributed by the author, Pacific Lava School. It means what you get isn't only an ebook of word list, you also have lots of fantastic accompanied tools in word building journey. Some of them are deserved to let you know here. 1. TOEFL 1200 Words in 30 Days, free online course shared the same title and word list exactly as this ebook. It provides online practice. If you are ESL student, you can get explanation of each word in 20 languages. 2. DIY Vocabulary Test, free online resource. It makes dynamical test sheet to help you evaluate your level and progress anytime and anyplace. To match with this ebook's contents, please ensure to select TOEFL and Basic level. 3. DIY Vocabulary EBook, online resource. It is a great tool to make your own PDF word list. In DIY ebook, you can skip known word, include local explanation, and/or expand your list from basic level (1200 of this ebook) to all levels' 4800 words. In summary, Pacific Lava School appreciates every second and every coin that students invest on vocabulary building and does its best to assist them to be successful. Choose this ebook equals to start from a right point for your vocabulary building. Come on, the bright future is shining ahead!

Eleventh Hour CISSP provides you with a study guide keyed directly to the most current version of the CISSP exam. This book is streamlined to include only core certification information and is presented for ease of last minute studying. Main objectives of the exam are covered concisely with key concepts highlighted. The CISSP certification is the most prestigious, globally recognized, vendor neutral exam for information security professionals. Over 67,000 professionals are certified worldwide with many more joining their ranks. This new Second Edition is aligned to cover all of the material in the most current version of the exam's Common Body of Knowledge. All 10 domains are covered as completely and as concisely as possible, giving you the best possible chance of acing the exam. All-new Second Edition updated for the most current version of the exam's Common Body of Knowledge The only guide you need for last minute studying Answers the toughest questions and highlights core topics No fluff - streamlined for maximum efficiency of study – perfect

for professionals who are updating their certification or taking the test for the first time

Ideal for any business traveler, this glossary covers topics relating to banking and finance - from office practice to stock market and accounting terminology. The Glossary of International Banking

Annotation A comprehensive and broad introduction to computer and intrusion forensics, covering the areas of law enforcement, national security and corporate fraud, this practical book helps professionals understand case studies from around the world, and treats key emerging areas such as stegoforensics, image identification, authorship categorization, and machine learning.

Explains how to use the music editing, mixing, and composing program, covering topics including using the edit view, working with loops and waves, editing voices, using real-time effects, and batch processing.

This textbook provides a comprehensive overview of different methods and sources of information-gathering for peace and conflict students and researchers, as well as the challenges presented by such work. Research on conflict-ridden societies carries special challenges for the collection and evaluation of information about the conflict and its actors. First, due to the nature of information emerging, incentives to misrepresent and propaganda is common. News coverage is sometimes poor and reporting is often incomplete, selective and biased. Second, the sensitivity of the topic and the questions posed in peace and conflict research means that access to and the security of informants can be a problem. Peace and conflict research as a discipline encompasses a number of different approaches for obtaining empirical information which serve as a basis for analyzing various research topics. This book provides a comprehensive overview of different methods and sources of information-gathering for students and researchers, as well as the challenges presented by such work. It offers: tools for evaluating sources and information suggestions on where different types of information can be found advice on using different types of sources, including news reports and written narratives practical guidelines for constructing large-scale datasets insights and guidelines for comparative fieldwork, in-depth interviews, focus groups, and surveys reflection and discussion on important ethical concerns in peace research This book will be of much interest for students and researchers of peace and conflict studies, conflict resolution, war and conflict studies, development studies, security studies and IR, as well as for NGO workers/researchers. Kristine Höglund is Associate Professor at the Department of Peace and Conflict Research, Uppsala University. She has a PhD in Peace and Conflict Research from Uppsala University Sweden (2004). She is author of Peacemaking in the Shadow of Violence. Magnus Öberg is Associate Professor at the Department of Peace and Conflict Research, Uppsala University, and Associate Editor of the Journal of Peace Research (since 2006). He has a PhD in Peace and Conflict Research from Uppsala University (2003) and is co-editor of Resources, Governance, and Civil Conflict (Routledge, 2008).

A hands-on introduction to programming with Visual Basic for DOS, including a disk containing all the program code covered. This book takes a painless approach that first-time users will find reassuring--a quick-start, step-by-step tutorial on object-oriented programming; dozens of easy-to-follow sample programs; helpful icons highlighting special tips and warnings; and a rich supply of screen images.

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

The EC-Council|Press Ethical Hacking and Countermeasures series is comprised of four books covering a broad base of topics in offensive network security, ethical hacking, and network defense and countermeasures. The content of this series is designed to immerse the reader into an interactive environment where they will be shown how to scan, test, hack, and secure information systems. A wide variety of tools, viruses, and malware is presented in these books, providing a complete understanding of the tactics and tools used by hackers. The full series of books helps prepare readers to take and succeed on the C|EH certification exam from EC-Council. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

This book is the first of a series of How To Pass OSCP books and focus on techniques used in Windows Privilege Escalation. This is a step-by-step guide that walks you through the whole process of how to escalate privilege in Windows environment using many common techniques. We start by gathering as much information about the target as possible either manually or using automated scripts. Next, we search for misconfigured services or scheduled tasks, insufficient file permission on binaries or services, vulnerable kernel, vulnerable software running with high privileges, sensitive information stored on local files, credential saved in the memory, registry settings that always elevate privileges before executing a binary, hard-coded credential contained in the application configuration files, and many more. Table of Contents Introduction Section One: Windows Configuration Chapter 1: AlwaysInstallElevated Section Two: Domain Controller Chapter 2: Zerologon Section Three: Windows Service Chapter 3: Service - Insecure File Permission Chapter 4: Service - Unquoted Path Chapter 5: Service - Bin Path Chapter 6: Service - Registry Chapter 7: Service - DLL Hijacking Section Four: Scheduled Tasks Chapter 8: Scheduled Tasks Section Five: Windows Registry Chapter 9: Autorun Chapter 10: Startup Applications Section Six: Windows Kernel Chapter 11: Kernel - EternalBlue Chapter 12: Kernel - MS15-051 Chapter 13: Kernel - MS14-058 Section Seven: Potato Exploits Chapter 14: Juicy Potato Chapter 15: Rogue Potato Section Eight: Password Mining Chapter 16: Password Mining - Memory Chapter 17: Password Mining - Registry Chapter 18: Password Mining - SiteList Chapter 19: Password Mining - Unattended Chapter 20: Password Mining - Web.config Section Nine: UAC Bypass Chapter 21: User Account Control Bypass For more information, please visit <http://www.howtopassoscp.com/>.

One-volume coverage of all the core concepts, terminology, issues, and practical skills modern computer security professionals need to know * *The most up-to-date computer security concepts text on the market. *Strong coverage and comprehensive analysis of key attacks, including denial of service, malware, and viruses. *Covers oft-neglected subject areas such as cyberterrorism, computer fraud, and industrial espionage. *Contains end-of-chapter exercises, projects, review questions, and plenty of realworld tips. Computer Security Fundamentals, Second Edition is designed to be the ideal one volume gateway into the entire field of computer security. It brings together thoroughly updated coverage of all basic concepts, terminology, and issues, along with the practical skills essential to security. Drawing on his extensive experience as both an IT professional and instructor, Chuck Easttom thoroughly covers core topics such as vulnerability assessment, virus attacks, buffer overflow, hacking, spyware, network defense, firewalls, VPNs, Intrusion Detection Systems, and passwords. Unlike many

other authors, however, he also fully addresses more specialized issues, including cyber terrorism, industrial espionage and encryption - including public/private key systems, digital signatures, and certificates. This edition has been extensively updated to address the latest issues and technologies, including cyberbullying/cyberstalking, session hijacking, steganography, and more. Its examples have been updated to reflect the current state-of-the-art in both attacks and defense. End-of-chapter exercises, projects, and review questions guide readers in applying the knowledge they've gained, and Easttom offers many tips that readers would otherwise have to discover through hard experience.

Provides information on how to use the components provided in the Delphi visual programming system to create Windows applications
Discover the properties and real-world applications of the Fibonacci and the Catalan numbers With clear explanations and easy-to-follow examples, Fibonacci and Catalan Numbers: An Introduction offers a fascinating overview of these topics that is accessible to a broad range of readers. Beginning with a historical development of each topic, the book guides readers through the essential properties of the Fibonacci numbers, offering many introductory-level examples. The author explains the relationship of the Fibonacci numbers to compositions and palindromes, tilings, graph theory, and the Lucas numbers. The book proceeds to explore the Catalan numbers, with the author drawing from their history to provide a solid foundation of the underlying properties. The relationship of the Catalan numbers to various concepts is then presented in examples dealing with partial orders, total orders, topological sorting, graph theory, rooted-ordered binary trees, pattern avoidance, and the Narayana numbers. The book features various aids and insights that allow readers to develop a complete understanding of the presented topics, including: Real-world examples that demonstrate the application of the Fibonacci and the Catalan numbers to such fields as sports, botany, chemistry, physics, and computer science More than 300 exercises that enable readers to explore many of the presented examples in greater depth Illustrations that clarify and simplify the concepts Fibonacci and Catalan Numbers is an excellent book for courses on discrete mathematics, combinatorics, and number theory, especially at the undergraduate level. Undergraduates will find the book to be an excellent source for independent study, as well as a source of topics for research. Further, a great deal of the material can also be used for enrichment in high school courses.

Annotation This cutting-edge new book delivers a comprehensive treatment of the emerging field of computer forensics, making it a valuable resource for IT professionals in private businesses and government organizations, as well as lawyers and law enforcement professionals. Regina Scheyvens and Donovan Storey draw upon a rich and diverse set of fieldwork experiences across the developing world, in both rural and urban settings, and utilize case studies to illustrate the many common issues and challenges that both new and experienced fieldwork researchers will face.

All in on Swift! iOS 10 and Xcode 8 make it clearer than ever that Swift is Apple's language of the future. Core frameworks have been redesigned to work better with Swift, and the language itself continues to evolve quickly. iOS 10 SDK Development is the pure-Swift approach to developing for the iOS platform. This completely revised and updated edition of the bestselling iOS guide shows you how to pull in the SDK's enormous feature set and deliver powerful, real-world apps for iPhone and iPad using modern Swift programming techniques. Swift is the language of the future for iOS development, and this completely revised and updated book is your guide. From the community-driven changes in Swift 3 to the overhaul of iOS' Foundation framework to make it more "Swiftly," iOS 10 and Xcode 8 mark an "all in" commitment to Swift, and this new edition matches that commitment. Learn not just the syntax of the Swift language but also stylish Swift, the idiomatic uses of the language, and best practices you'll find in the wild. From there, move into developing a complete, real-world podcast client sample

application-completely new for this edition-featuring Internet access, tables, navigation, and media playback, all with the most modern approaches provided by Apple's iOS 10 frameworks and tools. Go beyond code to master the practices that professional developers rely on: testing, debugging, publishing on the App Store, and managing your app over the long haul. As a bonus, you'll get a taste of cutting-edge iOS 10 features, such as the new Siri voice-command API. Swift's time is here. Whether you're new to Swift or just catching up on iOS' latest features, iOS 10 SDK Development will help you master the language and the platform.

The ultimate hands-on guide to IT security and proactivedefense The Network Security Test Lab is a hands-on, step-by-stepguide to ultimate IT security implementation. Covering the fullcomplement of malware, viruses, and other attack technologies, thisessential guide walks you through the security assessment andpenetration testing process, and provides the set-up guidance youneed to build your own security-testing lab. You'll look inside theactual attacks to decode their methods, and learn how to runattacks in an isolated sandbox to better understand how attackerstarget systems, and how to build the defenses that stop them.You'll be introduced to tools like Wireshark, Networkminer, Nmap,Metasploit, and more as you discover techniques for defendingagainst network attacks, social networking bugs, malware, and themost prevalent malicious traffic. You also get access to opensource tools, demo software, and a bootable version of Linux tofacilitate hands-on learning and help you implement your newskills. Security technology continues to evolve, and yet not a week goesby without news of a new security breach or a new exploit beingreleased. The Network Security Test Lab is the ultimateguide when you are on the front lines of defense, providing themost up-to-date methods of thwarting would-be attackers. Get acquainted with your hardware, gear, and test platform Learn how attackers penetrate existing security systems Detect malicious activity and build effective defenses Investigate and analyze attacks to inform defense strategy The Network Security Test Lab is your complete, essentialguide.

From the Rosetta Stone to public-key cryptography, the art and science of cryptology has been used to unlock the vivid history of ancient cultures, to turn the tide of warfare, and to thwart potential hackers from attacking computer systems. Codes: The Guide to Secrecy from Ancient to Modern Times explores the depth and breadth of the field, remain

If your job is to design or implement IT security solutions or if you're studying for any security certification, this is the how-to guide you've been looking for. Here's how to assess your needs, gather the tools, and create a controlled environment in which you can experiment, test, and develop the solutions that work. With liberal examples from real-world scenarios, it tells you exactly how to implement a strategy to secure your systems now and in the future. Note: CD-ROM/DVD and other supplementary materials are not included as part of eBook file. Implementing Cisco IOS Network Security (IINS) is a Cisco-authorized, self-paced learning tool for CCNA® Security foundation learning. This book provides you with the knowledge needed to secure Cisco® routers and switches and their associated networks. By reading this book, you will gain a thorough understanding of how to troubleshoot and monitor network devices to maintain integrity, confidentiality, and availability of data and devices, as well as the technologies that Cisco uses in its security infrastructure. This book focuses on the necessity of a comprehensive security policy and how it affects the posture of the network. You will learn how to perform basic tasks to secure a small branch type office network using Cisco IOS® security features available through the Cisco Router and Security Device Manager (SDM) web-based graphical user interface (GUI) and through the command-line interface (CLI) on Cisco routers and switches. The author also provides, when appropriate, parallels with Cisco ASA appliances. Whether you are preparing for CCNA Security certification or simply want to gain a better understanding of Cisco IOS security fundamentals, you will benefit from the information provided in this book. Implementing Cisco IOS Network Security (IINS) is part of a recommended learning path from Cisco that includes simulation and hands-on training from authorized

Cisco Learning Partners and self-study products from Cisco Press. To find out more about instructor-led training, e-learning, and hands-on instruction offered by authorized Cisco Learning Partners worldwide, please visit www.cisco.com/go/authorizedtraining. Develop a comprehensive network security policy to counter threats against information security Configure routers on the network perimeter with Cisco IOS Software security features Configure firewall features including ACLs and Cisco IOS zone-based policy firewalls to perform basic security operations on a network Configure site-to-site VPNs using Cisco IOS features Configure IPS on Cisco network routers Configure LAN devices to control access, resist attacks, shield other network devices and systems, and protect the integrity and confidentiality of network traffic This volume is in the Certification Self-Study Series offered by Cisco Press®. Books in this series provide officially developed self-study solutions to help networking professionals understand technology implementations and prepare for the Cisco Career Certifications examinations.

CISSP Study Guide, Third Edition provides readers with information on the CISSP certification, the most prestigious, globally-recognized, vendor-neutral exam for information security professionals. With over 100,000 professionals certified worldwide, and many more joining their ranks, this new third edition presents everything a reader needs to know on the newest version of the exam's Common Body of Knowledge. The eight domains are covered completely and as concisely as possible, allowing users to ace the exam. Each domain has its own chapter that includes a specially-designed pedagogy to help users pass the exam, including clearly-stated exam objectives, unique terms and definitions, exam warnings, "learning by example" modules, hands-on exercises, and chapter ending questions. Provides the most complete and effective study guide to prepare users for passing the CISSP exam, giving them exactly what they need to pass the test Authored by Eric Conrad who has prepared hundreds of professionals for passing the CISSP exam through SANS, a popular and well-known organization for information security professionals Covers all of the new information in the Common Body of Knowledge updated in January 2015, and also provides two exams, tiered end-of-chapter questions for a gradual learning curve, and a complete self-test appendix

Typical missions projects involve dozens of people in identical T-shirts getting on an airplane to go somewhere and help a needy community. But do those projects actually help people in the long run? Does this work create long-term systemic change in individuals and the community? And does the work lead to intentionally sharing Christ? In other words, is our mission work based on good missions strategy that brings about sustainable change and kingdom impact for communities, or is our approach focused only on creating a positive experience for everyone involved? So You Want to Dig a Well in Africa? highlights ten common myths people and organizations believe about missions. Exploring the ways in which American churches take on missions, author Jeff Palmer * highlights pitfalls of equating mission trips with ministry projects; * offers valuable techniques to avoid unintentional but harmful practices that stem from a poor community development model; * presents tools for designing, implementing, and evaluating strong, mercy-oriented

mission strategies; and * discusses key elements for evaluating mission programs: participation, sustainability, and transformation. Offering a resource for those seeking to work for the good of people but also for the glory of God, this guide highlights faulty models used for mercy-oriented missions and give a framework for creating sustainable change in people and communities.

Explains how to use fundamental DOS knowledge to develop batch files, manage files and directories, and use batch techniques to work productively

The Definitive, Up-to-Date Guide to Digital Forensics The rapid proliferation of cyber crime is increasing the demand for digital forensics experts in both law enforcement and in the private sector. In Digital Archaeology, expert practitioner Michael Graves has written the most thorough, realistic, and up-to-date guide to the principles and techniques of modern digital forensics. Graves begins by providing a solid understanding of the legal underpinnings of and critical laws affecting computer forensics, including key principles of evidence and case law. Next, he explains how to systematically and thoroughly investigate computer systems to unearth crimes or other misbehavior, and back it up with evidence that will stand up in court. Drawing on the analogy of archaeological research, Graves explains each key tool and method investigators use to reliably uncover hidden information in digital systems. His detailed demonstrations often include the actual syntax of command-line utilities. Along the way, he presents exclusive coverage of facilities management, a full chapter on the crucial topic of first response to a digital crime scene, and up-to-the-minute coverage of investigating evidence in the cloud. Graves concludes by presenting coverage of important professional and business issues associated with building a career in digital forensics, including current licensing and certification requirements. Topics Covered Include Acquiring and analyzing data in ways consistent with forensic procedure Recovering and examining e-mail, Web, and networking activity Investigating users' behavior on mobile devices Overcoming anti-forensics measures that seek to prevent data capture and analysis Performing comprehensive electronic discovery in connection with lawsuits Effectively managing cases and documenting the evidence you find Planning and building your career in digital forensics Digital Archaeology is a key resource for anyone preparing for a career as a professional investigator; for IT professionals who are sometimes called upon to assist in investigations; and for those seeking an explanation of the processes involved in preparing an effective defense, including how to avoid the legally indefensible destruction of digital evidence.

Tulloch provides A-Z detail about Microsoft networking technologies with the accuracy and expertise of those who know these products best-Microsoft itself. Along with critical coverage of Microsoft Windows NT(r) and BackOffice(r) resources, this reference also enumerates third-party products and general networking terminology-providing comprehensive

network-related information for all IT professionals.

Interviewing is an invaluable tool for the qualitative researcher. Steinar Kvale provides coverage of both the theoretical background and the practical aspects of the interview process, incorporating discussion of the wide variety of methods in interview based research and the different approaches to reading the data. Consideration is also given to the crucial issue of how to ensure scientific rigour.

The thesis of this book is that people and religions that have one religious book as guidance cannot be true (in the larger sense of shared truth) and that government that are faith-based cannot represent all the people. Free and open discussions and serious debate are essential for arriving at truth and democratic government. And religion is detrimental to world eace. The discussions presented assert that: there are many religions and that ALL their gods are “pretend” (given arbitrary characteristics), and new gods/religions have been easily made by many persons who visit the desert, wilderness, mountain-top, or any place of solitude where they were able to receive god’s calling without witnesses, and then they decree that god wants to speak through them (and only to them) and echoed by their appointed priests. If they can get gullible people to follow them and their god’s rules, they can establish their own religion (and warriors). The primary focus of the book’s discussions will be to establish “ground rules” for establishing “truth.” Then as examples, discussions are presented with other explanations of “miracles” in order to reconsider some of the Bible dogma specifically attributed to Jehovah, Moses, Passover, and the roles of all the gods involved in the story of the Exodus. The Bible (or Torah) may tell a different story when we discount miracles and explain them with other real possibilities. The conclusions may be different when we explore the plausibility that 1) Moses was the son of Pharaoh Amenhotep IV (later called Akhenaten who converted Egypt to a monotheistic religion) and Jochebed (a lesser wife—if married at all) and that 2) Moses was an Aten Priest who killed King Tut. The Exodus (and Adam and Eve) would have different explanations if Jehovah were not invented until on Mount Sinai in 1311 BCE (Before the Common Era) . . . not “In the Beginning” of the existence of the world. Also, the Passover, “the Jews” took in leaving Egypt would be logical if one sees Moses’ attempt to assert his claim to the pharaoh throne. And the Jews wandering in the desert would be reasonable if one considers that they were advised and supported by Moses’ father-in-law, Jethro, who was the nomadic high priest of the Druze religion (also a monotheistic type). These possibilities are herein explored in some detail, and the events are presented with a “psychological history” that includes the back stories, motivation, and relationships behind the characters and events. These discussions encourage rational thought and open-mindedness.

Candidates for the CISSP exam can now go directly to the source for study materials that are indispensable in achieving certification. The Official (ISC)2 Guide to the CISSP Exam is derived from the actual CBK review course created and administered by the non-profit security

consortium (ISC)2. In addition to being an invaluable study guide, this book is detailed enough to serve as an authoritative information security resource. Both of the guide's co-authors are CISSPs, and the entire text has been reviewed and approved by Hal Tipton, Co-Founder and Past President of ISSA and Co-Founder of (ISC)2. The ten subject areas included, each a section from the Common Body of Knowledge (CBK), have been reviewed by multiple CISSPs, all of whom are recognized leaders in their fields. A CISSP certification garners significant respect, signifying that the recipient has demonstrated a higher standard of knowledge, proficiency, and ethics. This book ensures that a student is fully prepared to face the exam's rigorous criteria. It is crafted to match the overall theme of the exam, which emphasizes a general, solutions-oriented knowledge of security that organizations want.

Implementing Cisco IOS Network Security (IINS) Foundation Learning Guide Second Edition Foundation learning for the CCNA Security IINS 640-554 exam Implementing Cisco IOS Network Security (IINS) Foundation Learning Guide, Second Edition, is a Cisco-authorized, self-paced learning tool for CCNA® Security 640-554 foundation learning. This book provides you with the knowledge needed to secure Cisco® networks. By reading this book, you will gain a thorough understanding of how to develop a security infrastructure, recognize threats and vulnerabilities to networks, and mitigate security threats. This book focuses on using Cisco IOS routers to protect the network by capitalizing on their advanced features as a perimeter router, firewall, intrusion prevention system, and site-to-site VPN device. The book also covers the use of Cisco Catalyst switches for basic network security, the Cisco Secure Access Control System (ACS), and the Cisco Adaptive Security Appliance (ASA). You learn how to perform basic tasks to secure a small branch office network using Cisco IOS security features available through web-based GUIs (Cisco Configuration Professional) and the CLI on Cisco routers, switches, and ASAs. Whether you are preparing for CCNA Security certification or simply want to gain a better understanding of Cisco IOS security fundamentals, you will benefit from the information provided in this book. Implementing Cisco IOS Network Security (IINS) Foundation Learning Guide, Second Edition, is part of a recommended learning path from Cisco that includes simulation and hands-on training from authorized Cisco Learning Partners and self-study products from Cisco Press. To find out more about instructor-led training, e-learning, and hands-on instruction offered by authorized Cisco Learning Partners worldwide, please visit www.cisco.com/go/authorizedtraining. -- Develop a comprehensive network security policy to counter threats against information security -- Secure borderless networks -- Learn how to use Cisco IOS Network Foundation Protection (NFP) and Cisco Configuration Professional (CCP) -- Securely implement the management and reporting features of Cisco IOS devices -- Deploy Cisco Catalyst Switch security features -- Understand IPv6 security features -- Plan threat control strategies -- Filter traffic with access control lists -- Configure ASA and Cisco IOS zone-based firewalls -- Implement intrusion prevention systems (IPS) and network address translation (NAT) -- Secure connectivity with site-to-site IPsec VPNs and remote access VPNs This volume is in the Foundation Learning Guide Series offered by Cisco Press®. These guides are developed together with Cisco as the only authorized, self-paced learning tools that help networking professionals build their understanding of networking concepts and prepare for Cisco certification exams. Category: Cisco Certification Covers: CCNA Security IINS exam 640-554

Twelve Years a Slave (1853) is a memoir and slave narrative by Solomon Northup, as told to and edited by David Wilson. Northup, a black man who was born free in New York, details his kidnapping in Washington, D.C. and subsequent sale into slavery. After having been kept in bondage for 12 years in Louisiana by various masters, Northup was able to write to friends and family in New York, who were in turn able to secure his release. Northup's account provides extensive details on the slave markets in Washington, D.C. and New Orleans and describes at length cotton and sugar cultivation on major plantations in Louisiana.

It is a time of breathtaking Singularity technology. A time when most human beings spend the majority of their lives in the alternate worlds of the cyberspace, the global mesh of full-immersion virtual realities. Traditional social and political structures are breaking down under the enormous weight of absolute creative freedom and terrestrial immortality. The invention of a device for resurrecting the dead is the catalyst which catapults the world into a struggle that will determine the shape of the future, the fate of government and religion, and even the nature of life itself. Virtual adventure and meatspace drama. Intrigue and suspense. Romance and bullet ballet. High ideals and low cunning. War of weapons, war of values. A brilliantly imagined technological backdrop. Vivid, vibrant characters. And something to make you think on almost every page.

In recent decades there has been increasing attention to mass atrocities such as genocide, war crimes, crimes against humanity, and other gross human rights violations. At the same time, there has been a vast increase in the number of academics and researchers seeking to analyze the causes of, and offer practical responses to, these atrocities. Yet there remains insufficient discussion of the practical and ethical challenges surrounding research into serious abuses and dealing with vulnerable populations. The aim of this edited volume is to guide researchers in identifying and addressing challenges in conducting qualitative research in difficult circumstances, such as conducting research in autocratic or uncooperative regimes, with governmental or non-governmental officials, and perhaps most importantly, with reluctant respondents such as victims of genocide or (on the other side of the coin) war criminals. The volume proceeds in five substantive sections, each addressing a different challenge of conducting field research in conflict-affected or repressive situations: Ethics Access Veracity Security Identity, objectivity, behaviour. This important text will be vital reading for students, scholars and researchers in the areas of research methods, international relations, anthropology and human rights. It will also be of keen interest to policy practitioners and NGOs, and especially relevant for those working in the regions of Africa, Latin America, and Asia.

[Copyright: 37be7766d759bca4e412399afb68170b](#)