Next Generation Firewall Forcepoint

Secure Cloud TransformationImplementing DirectAccess with Windows Server 2016Data Management, Analytics and InnovationFail Fast Or Win BigThe Best Damn Firewall Book PeriodConfiguring NetScreen FirewallsDetection of Intrusions and Malware, and Vulnerability AssessmentQGIS By ExampleHackers BewareHandbook of e-Business SecurityThe Perfect WeaponCisco Next-Generation Security SolutionsModern Development Paths of Agricultural ProductionCompTIA Security+ SY0-501 Cert GuideSecurity Yearbook 2020Configuring Juniper Networks NetScreen and SSG FirewallsSoftware-Defined Networking and SecurityProceedings of the International Conference on Soft Computing SystemsCybersecurity for Hospitals and Healthcare FacilitiesManaged Code RootkitsCybersecurity ??? Attack and Defense StrategiesCisco ASAUnclassified and SecureICGSCE 2014Advances in E-business Engineering for Ubiquitous ComputingCult of the Dead CowCisco ASANavigating the Digital AgeMore Awesome Than MoneyThe Best Damn Firewall Book PeriodRansomwareNetwork Security BibleBasics of Computer ApplicationJUNOS CookbookInformation Security HandbookAdvanced Persistent ThreatThe Responsibilities of Online Service ProvidersAccess DeniedZero Trust NetworksBonds Of Freedom

Secure Cloud Transformation

This book presents the latest findings in the areas of data management and smart computing, big data management, artificial intelligence and data analytics, along with advances in network technologies. It addresses state-of-the-art topics and discusses challenges and solutions for future development. Gathering original, unpublished contributions by scientists from around the globe, the book is mainly intended for a professional audience of researchers and practitioners in academia and industry.

Implementing DirectAccess with Windows Server 2016

The newest threat to security has been categorized as the Advanced Persistent Threat or APT. The APT bypasses most of an organization's current security devices, and is typically carried out by an organized group, such as a foreign nation state or rogue group with both the capability and the intent to persistently and effectively target a specific entity and wreak havoc. Most organizations do not understand how to deal with it and what is needed to protect their network from compromise. In Advanced Persistent Threat: Understanding the Danger and How to Protect your Organization Eric Cole discusses the critical information that readers need to know about APT and how to avoid being a victim. Advanced Persistent Threat is the first comprehensive manual that discusses how attackers are breaking into systems and what to do to protect and defend against these intrusions. How and why organizations are being attacked How to develop a "Risk based Approach to

Security" Tools for protecting data and preventing attacks Critical information on how to respond and recover from an intrusion The emerging threat to Cloud based networks

Data Management, Analytics and Innovation

The biggest online threat to businesses and consumers today is ransomware, a category of malware that can encrypt your computer files until you pay a ransom to unlock them. With this practical book, you'll learn how easily ransomware infects your system and what steps you can take to stop the attack before it sets foot in the network. Security experts Allan Liska and Timothy Gallo explain how the success of these attacks has spawned not only several variants of ransomware, but also a litany of ever-changing ways they're delivered to targets. You'll learn pragmatic methods for responding quickly to a ransomware attack, as well as how to protect yourself from becoming infected in the first place. Learn how ransomware enters your system and encrypts your files Understand why ransomware use has grown, especially in recent years Examine the organizations behind ransomware and the victims they target Learn how wannabe hackers use Ransomware as a Service (RaaS) to launch campaigns Understand how ransom is paid—and the pros and cons of paying Use methods to protect your organization's workstations and servers

Fail Fast Or Win Big

Implement information security effectively as per your organization's needs. About This Book Learn to build your own information security framework, the best fit for your organization Build on the concepts of threat modeling, incidence response, and security analysis Practical use cases and best practices for information security Who This Book Is For This book is for security analysts and professionals who deal with security mechanisms in an organization. If you are looking for an end to end guide on information security and risk analysis with no prior knowledge of this domain, then this book is for you. What You Will Learn Develop your own information security framework Build your incident response mechanism Discover cloud security considerations Get to know the system development life cycle Get your security operation center up and running Know the various security testing types Balance security as per your business needs Implement information security best practices In Detail Having an information security mechanism is one of the most crucial factors for any organization. Important assets of organization demand a proper risk management and threat model for security, and so information security concepts are gaining a lot of traction. This book starts with the concept of information security and shows you why it's important. It then moves on to modules such as threat modeling, risk management, and mitigation. It also covers the concepts of incident response systems, information rights management, and more. Moving on, it guides you to build your own information security framework as the best fit for your organization. Toward the end, you'll discover some best practices that can be implemented to make your security framework strong. By the end of this book, you will be well-

versed with all the factors involved in information security, which will help you build a security framework that is a perfect fit your organization's requirements. Style and approach This book takes a practical approach, walking you through information security fundamentals, along with information security best practices.

The Best Damn Firewall Book Period

This is a compact notes for XII Computer Application Students of WBCHSE Board.

Configuring NetScreen Firewalls

This book provides readers insights into cyber maneuvering or adaptive and intelligent cyber defense. It describes the required models and security supporting functions that enable the analysis of potential threats, detection of attacks, and implementation of countermeasures while expending attacker resources and preserving user experience. This book not only presents significant education-oriented content, but uses advanced content to reveal a blueprint for helping network security professionals design and implement a secure Software-Defined Infrastructure (SDI) for cloud networking environments. These solutions are a less intrusive alternative to security countermeasures taken at the host level and offer centralized control of the distributed network. The concepts, techniques, and strategies discussed in this book are ideal for students, educators, and security practitioners looking for a clear and concise text to avant-garde cyber security installations or simply to use as a reference. Hand-on labs and lecture slides are located at http://virtualnetworksecurity.thothlab.com/. Features Discusses virtual network security concepts Considers proactive security using moving target defense Reviews attack representation models based on attack graphs and attack trees Examines service function chaining in virtual networks with security considerations Recognizes machine learning and AI in network security

Detection of Intrusions and Malware, and Vulnerability Assessment

The Juniper Networks routing platforms are becoming the go-to solution for core, edge, metro and remote office networks, and JUNOS software is behind it all. The operating system is so full of industrial-strength routing protocols and IP innovations that those treading into the world of JUNOS will need clarification, explanation, and a showcase example or two. Look no further. This JUNOS Cookbook provides it all and more. Yes, you can mine through the 5,000 pages of documentation or take a two-thousand-dollar training course, but JUNOS's interprocess sophistication can be baffling unless you know the shortcuts and tricks, as well as those rays of illuminating comprehension that can come only from those who live with it. JUNOS Cookbook is the first comprehensive book about JUNOS software and it provides over 200 time-saving

step-by-step techniques including discussions about the processes and alternative ways to perform the same task. It's been tested and tech-reviewed by field engineers who know how to take JUNOS out for a spin and it's applicable to the entire line of M-, T-, and J-series routers. JUNOS Cookbook will not only pay for itself the first few times you use it, it will make your network easier to manage and update. "Aviva Garrett has done a tremendous job of distilling the features of JUNOS software in a form that will be useful for a wide audience-students, field engineers, network architects, and other networking professionals alike will benefit from this book. For many people, this is the only book on JUNOS they will need."Pradeep Sindhu, CTO and Founder, Juniper Networks "This cookbook is superb. Aviva Garrett has masterfully assembled a complete set of practical real-world examples with step-by-step instructions. Security, management, routing: it's all here!"Stephen Gill, Research Fellow, Team Cymru "A technical time-saver for any NOC or SOC working with JUNOS. It's clear, concise, and informative recipes are are an invaluable resource. "Scott A. McIntyre, Security Officer, XS4ALL Internet B.V

QGIS By Example

This is the eBook version of the printed book. If the print book includes a CD-ROM, this content is not included within the eBook version. For organizations of all sizes, the Cisco ASA product family offers powerful new tools for maximizing network security. Cisco ASA: All-in-One Firewall, IPS, Anti-X and VPN Adaptive Security Appliance, Second Edition, is Cisco's authoritative practitioner's guide to planning, deploying, managing, and troubleshooting security with Cisco ASA. Written by two leading Cisco security experts, this book presents each Cisco ASA solution in depth, offering comprehensive sample configurations, proven troubleshooting methodologies, and debugging examples. Readers will learn about the Cisco ASA Firewall solution and capabilities; secure configuration and troubleshooting of site-to-site and remote access VPNs; Intrusion Prevention System features built into Cisco ASA's Advanced Inspection and Prevention Security Services Module (AIP-SSM); and Anti-X features in the ASA Content Security and Control Security Services Module (CSC-SSM). This new edition has been updated with detailed information on the latest ASA models and features. Everything network professionals need to know to identify, mitigate, and respond to network attacks with Cisco ASA Includes detailed configuration examples, with screenshots and command line references Covers the ASA 8.2 release Presents complete troubleshooting methodologies and architectural references

Hackers Beware

A study of Internet blocking and filtering around the world: analyses by leading researchers and survey results that document filtering practices in dozens of countries. Many countries around the world block or filter Internet content, denying access to information that they deem too sensitive for ordinary citizens—most often about politics, but sometimes

relating to sexuality, culture, or religion. Access Denied documents and analyzes Internet filtering practices in more than three dozen countries, offering the first rigorously conducted study of an accelerating trend. Internet filtering takes place in more than three dozen states worldwide, including many countries in Asia, the Middle East, and North Africa. Related Internet content-control mechanisms are also in place in Canada, the United States and a cluster of countries in Europe. Drawing on a just-completed survey of global Internet filtering undertaken by the OpenNet Initiative (a collaboration of the Berkman Center for Internet and Society at Harvard Law School, the Citizen Lab at the University of Toronto, the Oxford Internet Institute at Oxford University, and the University of Cambridge) and relying on work by regional experts and an extensive network of researchers, Access Denied examines the political, legal, social, and cultural contexts of Internet filtering in these states from a variety of perspectives. Chapters discuss the mechanisms and politics of Internet filtering, the strengths and limitations of the technology that powers it, the relevance of international law, ethical considerations for corporations that supply states with the tools for blocking and filtering, and the implications of Internet filtering for activist communities that increasingly rely on Internet technologies for communicating their missions. Reports on Internet content regulation in forty different countries follow, with each two-page country profile outlining the types of content blocked by category and documenting key findings. Contributors Ross Anderson, Malcolm Birdling, Ronald Deibert, Robert Faris, Vesselina Haralampieva [as per Rob Faris], Steven Murdoch, Helmi Noman, John Palfrey, Rafal Rohozinski, Mary Rundle, Nart Villeneuve, Stephanie Wang, Jonathan Zittrain

Handbook of e-Business Security

The Second Edition of the Best Damn Firewall Book Period is completely revised and updated to include all of the most recent releases from Microsoft, Cisco, Juniper Network, and Check Point. Compiled from the best of the Syngress firewall library and authored by product experts such as Dr. Tom Shinder on ISA Server, this volume is an indispensable addition to a serious networking professionals toolkit. Coverage includes migrating to ISA Server 2006, integrating Windows Firewall and Vista security into your enterprise, successfully integrating Voice over IP applications around firewalls, and analyzing security log files. Sections are organized by major vendor, and include hardware, software and VPN configurations for each product line. New to this Edition: Microsoft firewall protection, from Windows Firewall to ISA Server 2006 Cisco PIX Version 7, including VPN configuration and IDS Analyzing Firewall Logs and Reports VoIP and Firewall Bypassing

The Perfect Weapon

Learn how to detect and prevent the hacking of medical equipment at hospitals and healthcare facilities. A cyber-physical attack on building equipment pales in comparison to the damage a determined hacker can do if he/she gains access to a medical-grade network as a medical-grade network controls the diagnostic, treatment, and life support equipment on which

lives depend. News reports inform us how hackers strike hospitals with ransomware that prevents staff from accessing patient records or scheduling appointments. Unfortunately, medical equipment also can be hacked and shut down remotely as a form of extortion. Criminal hackers will not ask for a $500 payment to unlock an MRI, PET or CT scan, or X-ray machine—they will ask for much more. Litigation is bound to follow and the resulting punitive awards will drive up hospital insurance costs and healthcare costs in general. This will undoubtedly result in increased regulations for hospitals and higher costs for compliance. Unless hospitals and other healthcare facilities take the steps necessary to secure their medical-grade networks, they will be targeted for cyber-physical attack, possibly with life-threatening consequences. Cybersecurity for Hospitals and Healthcare Facilities is a wake-up call explaining what hackers can do, why hackers would target a hospital, the way hackers research a target, ways hackers can gain access to a medical-grade network (cyber-attack vectors), and ways hackers hope to monetize their cyber-attack. By understanding and detecting the threats, you can take action now—before your hospital becomes the next victim. What You Will Learn: Determine how vulnerable hospital and healthcare building equipment is to cyber-physical attack Identify possible ways hackers can hack hospital and healthcare facility equipment Recognize the cyber-attack vectors—or paths by which a hacker or cracker can gain access to a computer, a medical-grade network server, or expensive medical equipment in order to deliver a payload or malicious outcome Detect and prevent man-in-the-middle or denial-of-service cyber-attacks Find and prevent hacking of the hospital database and hospital web application Who This Book Is For: Hospital administrators, healthcare professionals, hospital & healthcare facility engineers and building managers, hospital & healthcare facility IT professionals, and HIPAA professionals

Cisco Next-Generation Security Solutions

QGIS is a leading user-friendly, cross-platform, open source, desktop geographic information system (GIS). It provides many useful capabilities and features and their number is continuously growing. More and more private users and companies choose QGIS as their primary GIS software because it is very easy to use, feature-rich, extensible, and has a big and constantly growing community. This book guides you from QGIS installation through data loading, and preparation to performing most common GIS analyses. You will perform different types of GIS analyses including density, visibility, and suitability analysis on practical, real-world data. Finally, you will learn how to become more productive and automate your everyday work with the help of the QGIS Processing framework and by developing your own Python plugins. By the end of this book, you will have all the necessary knowledge about handling and analyzing spatial data.

Modern Development Paths of Agricultural Production

Welcome to the all-new second edition of Navigating the Digital Age. This edition brings together more than 50 leaders and visionaries from business, science, technology, government, aca¬demia, cybersecurity, and law enforce¬ment. Each has

contributed an exclusive chapter designed to make us think in depth about the ramifications of this digi-tal world we are creating. Our purpose is to shed light on the vast possibilities that digital technologies present for us, with an emphasis on solving the existential challenge of cybersecurity. An important focus of the book is centered on doing business in the Digital Age-par¬ticularly around the need to foster a mu¬tual understanding between technical and non-technical executives when it comes to the existential issues surrounding cybersecurity. This book has come together in three parts. In Part 1, we focus on the future of threat and risks. Part 2 emphasizes lessons from today's world, and Part 3 is designed to help you ensure you are covered today. Each part has its own flavor and personal¬ity, reflective of its goals and purpose. Part 1 is a bit more futuristic, Part 2 a bit more experiential, and Part 3 a bit more practical. How we work together, learn from our mistakes, deliver a secure and safe digital future-those are the elements that make up the core thinking behind this book. We cannot afford to be complacent. Whether you are a leader in business, government, or education, you should be knowledgeable, diligent, and action-oriented. It is our sincerest hope that this book provides answers, ideas, and inspiration.If we fail on the cybersecurity front, we put all of our hopes and aspirations at risk. So we start this book with a simple proposition: When it comes to cybersecurity, we must succeed.

CompTIA Security+ SY0-501 Cert Guide

There are a lot of e-business security concerns. Knowing about e-business security issues will likely help overcome them. Keep in mind, companies that have control over their e-business are likely to prosper most. In other words, setting up and maintaining a secure e-business is essential and important to business growth. This book covers state-of-the art practices in e-business security, including privacy, trust, security of transactions, big data, cloud computing, social network, and distributed systems.

Security Yearbook 2020

Cisco® ASA All-in-One Next-Generation Firewall, IPS, and VPN Services, Third Edition Identify, mitigate, and respond to today's highly-sophisticated network attacks. Today, network attackers are far more sophisticated, relentless, and dangerous. In response, Cisco ASA: All-in-One Next-Generation Firewall, IPS, and VPN Services has been fully updated to cover the newest techniques and Cisco technologies for maximizing end-to-end security in your environment. Three leading Cisco security experts guide you through every step of creating a complete security plan with Cisco ASA, and then deploying, configuring, operating, and troubleshooting your solution. Fully updated for today's newest ASA releases, this edition adds new coverage of ASA 5500-X, ASA 5585-X, ASA Services Module, ASA next-generation firewall services, EtherChannel, Global ACLs, clustering, IPv6 improvements, IKEv2, AnyConnect Secure Mobility VPN clients, and more. The authors explain significant recent licensing changes; introduce enhancements to ASA IPS; and walk you through configuring

IPsec, SSL VPN, and NAT/PAT. You'll learn how to apply Cisco ASA adaptive identification and mitigation services to systematically strengthen security in network environments of all sizes and types. The authors present up-to-date sample configurations, proven design scenarios, and actual debugs– all designed to help you make the most of Cisco ASA in your rapidly evolving network. Jazib Frahim, CCIE® No. 5459 (Routing and Switching; Security), Principal Engineer in the Global Security Solutions team, guides top-tier Cisco customers in security-focused network design and implementation. He architects, develops, and launches new security services concepts. His books include Cisco SSL VPN Solutions and Cisco Network Admission Control, Volume II: NAC Deployment and Troubleshooting. Omar Santos, CISSP No. 463598, Cisco Product Security Incident Response Team (PSIRT) technical leader, leads and mentors engineers and incident managers in investigating and resolving vulnerabilities in Cisco products and protecting Cisco customers. Through 18 years in IT and cybersecurity, he has designed, implemented, and supported numerous secure networks for Fortune® 500 companies and the U.S. government. He is also the author of several other books and numerous whitepapers and articles. Andrew Ossipov, CCIE® No. 18483 and CISSP No. 344324, is a Cisco Technical Marketing Engineer focused on firewalls, intrusion prevention, and data center security. Drawing on more than 16 years in networking, he works to solve complex customer technical problems, architect new features and products, and define future directions for Cisco's product portfolio. He holds several pending patents. Understand, install, configure, license, maintain, and troubleshoot the newest ASA devices Efficiently implement Authentication, Authorization, and Accounting (AAA) services Control and provision network access with packet filtering, context-aware Cisco ASA next-generation firewall services, and new NAT/PAT concepts Configure IP routing, application inspection, and QoS Create firewall contexts with unique configurations, interfaces, policies, routing tables, and administration Enable integrated protection against many types of malware and advanced persistent threats (APTs) via Cisco Cloud Web Security and Cisco Security Intelligence Operations (SIO) Implement high availability with failover and elastic scalability with clustering Deploy, troubleshoot, monitor, tune, and manage Intrusion Prevention System (IPS) features Implement site-to-site IPsec VPNs and all forms of remote-access VPNs (IPsec, clientless SSL, and client-based SSL) Configure and troubleshoot Public Key Infrastructure (PKI) Use IKEv2 to more effectively resist attacks against VPNs Leverage IPv6 support for IPS, packet inspection, transparent firewalls, and site-to-site IPsec VPNs

Configuring Juniper Networks NetScreen and SSG Firewalls

The first book on the market covering the #2 best-selling firewall appliances in the world from NetScreen. This book continues Syngress' history from ISA Server to Check Point to Cisco Pix of being first to market with best-selling firewall books for security professionals. Configuring NetScreen Firewalls is the first book to deliver an in-depth look at the NetScreen firewall product line. It covers all of the aspects of the NetScreen product line from the SOHO devices to the Enterprise NetScreen firewalls. Also covered are advanced troubleshooting techniques and the NetScreen Security Manager. This book offers novice users a complete opportunity to learn the NetScreen firewall appliance. Advanced users will find it a

rich technical resource. * NetScreen is the #2 best-selling firewall appliance in the world (behind only Cisco PIX) and there are no competing books. * Covers the materials found on the NetScreen NCSA 5.0 exam. * Syngress firewall books are consistent best-sellers with market-leading books on ISA Server, Cisco PIX, and Check Point Next Generation.

Software-Defined Networking and Security

Learn how to design, plan, implement, and support a secure remote access solution using DirectAccess in Windows Server 2016. Remote Access has been included in the Windows operating system for many years. With each new operating system release, new features and capabilities have been included to allow network engineers and security administrators to provide remote access in a secure and cost-effective manner. DirectAccess in Windows Server 2016 provides seamless and transparent, always on remote network connectivity for managed Windows devices. DirectAccess is built on commonly deployed Windows platform technologies and is designed to streamline and simplify the remote access experience for end users. In addition, DirectAccess connectivity is bidirectional, allowing administrators to more effectively manage and secure their field-based assets. Implementing DirectAccess with Windows Server 2016 provides a high-level overview of how DirectAccess works. The vision and evolution of DirectAccess are outlined and business cases and market drivers are explained. DirectAccess is evaluated against traditional VPN and this book describes the Windows platform technologies that underpin this solution. In addition, this book: Explains how the technology works and the specific IT pain points that it addresses Includes detailed, prescriptive guidance for those tasked with implementing DirectAccess using Windows Server 2016 Addresses real-world deployment scenarios for small and large organizations Contains valuable tips, tricks, and implementation best practices for security and performance"/li> What you'll learn A high-level understanding of the various remote access technologies included in Windows Server 2016. Common uses cases for remote access, and how best to deploy them in a secure, stable, reliable, and highly available manner. Valuable insight in to design best practices and learn how to implement DirectAccess and VPN with Windows Server 2016 according to deployment best practices. Who This Book Is For IT administrators, network, and security administrators and engineers, systems management professionals, compliance auditors, and IT executive management (CIO, CISO) are the target audience for this title.

Proceedings of the International Conference on Soft Computing Systems

The perimeter defenses guarding your network perhaps are not as secure as you think. Hosts behind the firewall have no defenses of their own, so when a host in the "trusted" zone is breached, access to your data center is not far behind. That's an all-too-familiar scenario today. With this practical book, you'll learn the principles behind zero trust architecture, along with details necessary to implement it. The Zero Trust Model treats all hosts as if they're internet-facing, and considers the entire network to be compromised and hostile. By taking this approach, you'll focus on building strong authentication,

authorization, and encryption throughout, while providing compartmentalized access and better operational agility. Understand how perimeter-based defenses have evolved to become the broken model we use today Explore two case studies of zero trust in production networks on the client side (Google) and on the server side (PagerDuty) Get example configuration for open source tools that you can use to build a zero trust network Learn how to migrate from a perimeter-based network to a zero trust network in production

Cybersecurity for Hospitals and Healthcare Facilities

This is the eBook version of the print title. Note that the eBook may not provide access to the practice test software that accompanies the print book. Access to the companion files are available through product registration at Pearson IT Certification, or see the instructions in the back pages of your eBook. Learn, prepare, and practice for CompTIA Security+ SY0-501 exam success with this CompTIA approved Cert Guide from Pearson IT Certification, a leader in IT certification learning and a CompTIA Authorized Platinum Partner. · Master CompTIA Security+ SY0-501 exam topics · Assess your knowledge with chapter-ending quizzes · Review key concepts with exam preparation tasks · Practice with realistic exam questions CompTIA Security+ SY0-501 Cert Guide is a best-of-breed exam study guide. Best-selling author and expert instructor David L. Prowse shares preparation hints and test-taking tips, helping you identify areas of weakness and improve both your conceptual knowledge and hands-on skills. Material is presented in a concise manner, focusing on increasing your understanding and retention of exam topics. The book presents you with an organized test-preparation routine through the use of proven series elements and techniques. Exam topic lists make referencing easy. Chapter-ending chapter review activities help you drill on key concepts you must know thoroughly. Review questions help you assess your knowledge, and a final preparation chapter guides you through tools and resources to help you craft your final study plan. Well regarded for its level of detail, assessment features, and challenging review questions and exercises, this CompTIA approved study guide helps you master the concepts and techniques that will enable you to succeed on the exam the first time. The CompTIA approved study guide helps you master all the topics on the Security+ exam, including · Core computer system security · OS hardening and virtualization · Application security · Network design elements · Networking ports, protocols, and threats · Network perimeter security · Physical security and authentication models · Access control · Vulnerability and risk assessment · Monitoring and auditing · Cryptography, including PKI · Redundancy and disaster recovery · Social Engineering · Policies and procedures

Managed Code Rootkits

Juniper Networks Secure Access SSL VPN appliances provide a complete range of remote access appliances for the smallest companies up to the largest service providers. This comprehensive configuration guide will allow system administrators and

security professionals to configure these appliances to allow remote and mobile access for employees. If you manage and secure a larger enterprise, this book will help you to provide remote and/or extranet access for employees, partners, and customers from a single platform. Configure Juniper's Instant Virtual Extranet (IVE) Install and set up IVE through either the command line interface (CLI) or Web-based console Master the "3 Rs": Realms, Roles, and Resources Realize the potential of the "3Rs" for endpoint security, sign-in policies, and authorization of servers Get Inside both the Windows and Java Versions of Secure Application Manager (SAM) Learn to implement SAM, manage the end-user experience, and troubleshoot SAM in the field Integrate IVE with Terminal Services and Citrix Enable terminal services proxy and configure role options, configure Citrix using a custom ICA, configure terminal services resource policies and profiles, and configure terminal services and Citrix using a hosted Java applet Ensure Endpoint Security Use Host Checker, Cache Cleaner, Secure Virtual Workspace, and IVE/IDP integration to secure your network Manage the Remote Access Needs of Your Organization Configure Web access, file access and telnet/SSH access for remote users and offices Configure Core Networking Components through the System Menu Create clusters, manage virtual systems, and monitor logs, reports, and alerts Create Bullet-Proof Sign-in Policies Create standard and custom sign-in pages for both user and administrator access and Secure Meeting pages Use the IVE for Log-Related Tasks Perform log filtering, log management, syslog exporting, SNMP management, and system resource monitoring and reporting.

Cybersecurity ??? Attack and Defense Strategies

This book presents the latest trends in scientific methods and enabling technologies to advance e-business. It consists of selected high-quality papers from the 16th International Conference on E-Business Engineering (ICEBE 2019), held in Shanghai, China, on 11-13 October 2019. ICEBE is a leading international forum for researchers, engineers, and business specialists to exchange cutting-edge ideas, findings, and experiences in the field of e-business. The book covers a range of topics, including agents for e-business, big data for e-business, Internet of Things, mobile and autonomous computing, security/privacy/trust, service-oriented and cloud computing, software engineering, blockchain, and industry applications.

Cisco ASA

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.

Unclassified and Secure

This report describes a way for the U.S. Department of Defense to better secure unclassified networks holding defense information--through the establishment of a cybersecurity program designed to strengthen the protections of these networks.

ICGSCE 2014

This book presents the latest trends and challenges in the development of general engineering and mechanical engineering in the agriculture and horticulture sectors.

Advances in E-business Engineering for Ubiquitous Computing

Security Yearbook 2020 is the story of the people, companies, and events that comprise the history of of the IT security industry. In this inaugural edition you will discover the early history of Symantec, Network Associates, BorderWare, Check Point Software, and dozens of other companies that contributed to the growth of an industry that now is comprised of 2,336

vendors of security products. In addition to the history there are stories from industry pioneers such as Gil Shwed CEO and founder, Check Point Software Chris Blask Co-inventor of Borderware Firewall and NAT (network address translation) Ron Moritz Executive at Finjan, Symantec, CA, Microsoft, Our Crowd Barry Schrager Progenitor of RACF and creator of ACF2 David Cowan Partner at Bessemer and founder of Verisign The directory lists all the vendors alphabetically, by country, and by category, making an invaluable desk reference for students, practioners, researchers, and investors.

Cult of the Dead Cow

A Story of love and ambition set around the creation of a dream school in the Little Red Dot of Asia,Singapore Shekharan is consumed by the fire of ambition – so much so that he ends up scorching his lady-love Angela's beloved dream. She is faced with heart-wrenching choices. What does she sacrifice? Is she able to pull back her pet project from the edge of disaster? 'Bonds of Freedom' unravels the dramatic answers to these and other riveting questions.

Cisco ASA

The shocking untold story of the elite secret society of hackers fighting to protect our privacy, our freedom -- even democracy itself Cult of the Dead Cow is the tale of the oldest, most respected, and most famous American hacking group of all time. Though until now it has remained mostly anonymous, its members invented the concept of hacktivism, released the top tool for testing password security, and created what was for years the best technique for controlling computers from afar, forcing giant companies to work harder to protect customers. They contributed to the development of Tor, the most important privacy tool on the net, and helped build cyberweapons that advanced US security without injuring anyone. With its origins in the earliest days of the Internet, the cDc is full of oddball characters -- activists, artists, even future politicians. Many of these hackers have become top executives and advisors walking the corridors of power in Washington and Silicon Valley. The most famous is former Texas Congressman and current presidential candidate Beto O'Rourke, whose time in the cDc set him up to found a tech business, launch an alternative publication in El Paso, and make long-shot bets on unconventional campaigns. Today, the group and its followers are battling electoral misinformation, making personal data safer, and battling to keep technology a force for good instead of for surveillance and oppression. Cult of the Dead Cow shows how governments, corporations, and criminals came to hold immense power over individuals and how we can fight back against them.

Navigating the Digital Age

Explains how and why hackers break into computers, steal information, and deny services to machines' legitimate users,

and discusses strategies and tools used by hackers and how to defend against them.

More Awesome Than Money

Managed Code Rootkits is the first book to cover application-level rootkits and other types of malware inside the application VM, which runs a platform-independent programming environment for processes. The book, divided into four parts, points out high-level attacks, which are developed in intermediate language. The initial part of the book offers an overview of managed code rootkits. It explores environment models of managed code and the relationship of managed code to rootkits by studying how they use application VMs. It also discusses attackers of managed code rootkits and various attack scenarios. The second part of the book covers the development of managed code rootkits, starting with the tools used in producing managed code rootkits through their deployment. The next part focuses on countermeasures that can possibly be used against managed code rootkits, including technical solutions, prevention, detection, and response tactics. The book concludes by presenting techniques that are somehow similar to managed code rootkits, which can be used in solving problems. Named a 2011 Best Hacking and Pen Testing Book by InfoSec Reviews Introduces the reader briefly to managed code environments and rootkits in general Completely details a new type of rootkit hiding in the application level and demonstrates how a hacker can change language runtime implementation Focuses on managed code including Java, .NET, Android Dalvik and reviews malware development scanarios

The Best Damn Firewall Book Period

This book includes selected papers from the ICGSCE 2014 with focus on the current trends of global resources used to meet the growing demands to improve life style coupled with environmental and social problems related to the resource consumption with emphasize to move towards sustainable development. It provides a platform for scientists and academicians from local and international universities and industries to promote, share and discuss various new issues and developments in different areas of Chemical Engineering with respect to global sustainability. Under the sustainability umbrella the topics covered are; alternative energy sources, alternative feedstock for energy and chemicals, alternative raw materials for household commodity, green process with minimal environmental impact, process intensification, waste minimization, recycling of wastes and providing quality water, food and medicines. Other topics covered include: 1. Oil and gas, Biofuel, Fuel cell, Renewable energy 2. Green technology, Sustainability, Environmental, Carbon sequestration, Carbon footprint, Natural resources 3. Chemical processes, Separation technology, Biotechnology, Nanotechnology, Food technology, Particle technology, Corrosion, Pharmaceutical, Phytochemical, Oleochemical 4. Process modeling, Process Simulation, Process control 5. Advanced material, Polymer, Catalyst, Enzyme 6. Policy, Regulations, Strategy and implementation, Safety, Management of science, Engineering education 7. Process Safety and Loss Prevention,

Environmental and chemical risk assessment, Transportation risk analysis, Inherent safety.

Ransomware

SOON TO BE AN HBO® DOCUMENTARY FROM AWARD-WINNING DIRECTOR JOHN MAGGIO * "An important--and deeply sobering--new book about cyberwarfare" (Nicholas Kristof, New York Times), now updated with a new chapter. The Perfect Weapon is the startling inside story of how the rise of cyberweapons transformed geopolitics like nothing since the invention of the atomic bomb. Cheap to acquire, easy to deny, and usable for a variety of malicious purposes, cyber is now the weapon of choice for democracies, dictators, and terrorists. Two presidents--Bush and Obama--drew first blood with Operation Olympic Games, which used malicious code to blow up Iran's nuclear centrifuges, and yet America proved remarkably unprepared when its own weapons were stolen from its arsenal and, during President Trump's first year, turned back on the United States and its allies. And if Obama would begin his presidency by helping to launch the new era of cyberwar, he would end it struggling unsuccessfully to defend against Russia's broad attack on the 2016 US election. Moving from the White House Situation Room to the dens of Chinese government hackers to the boardrooms of Silicon Valley, New York Times national security correspondent David Sanger reveals a world coming face-to-face with the perils of technological revolution, where everyone is a target. "Timely and bracing . . . With the deep knowledge and bright clarity that have long characterized his work, Sanger recounts the cunning and dangerous development of cyberspace into the global battlefield of the 21st century." --Washington Post

Network Security Bible

A must for working network and security professionals as well as anyone in IS seeking to build competence in the increasingly important field of security Written by three high-profile experts, including Eric Cole, an ex-CIA security guru who appears regularly on CNN and elsewhere in the media, and Ronald Krutz, a security pioneer who cowrote The CISSP Prep Guide and other security bestsellers Covers everything from basic security principles and practices to the latest security threats and responses, including proven methods for diagnosing network vulnerabilities and insider secrets for boosting security effectiveness

Basics of Computer Application

This book constitutes the proceedings of the 16th International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, DIMVA 2019, held in Gothenburg, Sweden, in June 2019. The 23 full papers presented in this volume were carefully reviewed and selected from 80 submissions. The contributions were organized in topical sections

named: wild wild web; cyber-physical systems; malware; software security and binary analysis; network security; and attack mitigation.

JUNOS Cookbook

Network threats are emerging and changing faster than ever before. Cisco Next-Generation Network Security technologies give you all the visibility and control you need to anticipate and meet tomorrow's threats, wherever they appear. Now, three Cisco network security experts introduce these products and solutions, and offer expert guidance for planning, deploying, and operating them. The authors present authoritative coverage of Cisco ASA with FirePOWER Services; Cisco Firepower Threat Defense (FTD); Cisco Next-Generation IPS appliances; the Cisco Web Security Appliance (WSA) with integrated Advanced Malware Protection (AMP); Cisco Email Security Appliance (ESA) with integrated Advanced Malware Protection (AMP); Cisco AMP ThreatGrid Malware Analysis and Threat Intelligence, and the Cisco Firepower Management Center (FMC). You'll find everything you need to succeed: easy-to-follow configurations, application case studies, practical triage and troubleshooting methodologies, and much more. Effectively respond to changing threat landscapes and attack continuums Design Cisco ASA with FirePOWER Services and Cisco Firepower Threat Defense (FTD) solutions Set up, configure, and troubleshoot the Cisco ASA FirePOWER Services module and Cisco Firepower Threat Defense Walk through installing AMP Private Clouds Deploy Cisco AMP for Networks, and configure malware and file policies Implement AMP for Content Security, and configure File Reputation and File Analysis Services Master Cisco AMP for Endpoints, including custom detection, application control, and policy management Make the most of the AMP ThreatGrid dynamic malware analysis engine Manage Next-Generation Security Devices with the Firepower Management Center (FMC) Plan, implement, and configure Cisco Next-Generation IPS—including performance and redundancy Create Cisco Next-Generation IPS custom reports and analyses Quickly identify the root causes of security problems

Information Security Handbook

This volume focuses on the responsibilities of online service providers (OSPs) in contemporary societies. It examines the complexity and global dimensions of the rapidly evolving and serious challenges posed by the exponential development of Internet services and resources. It looks at the major actors – such as Facebook, Google, Twitter, and Yahoo! – and their significant influence on the informational environment and users' interactions within it, as well as the responsibilities and liabilities such influence entails. It discusses the position of OSPs as information gatekeepers and how they have gone from offering connecting and information-sharing services to paying members to providing open, free infrastructure and applications that facilitate digital expression and the communication of information. The book seeks consensus on the principles that should shape OSPs' responsibilities and practices, taking into account business ethics and policies. Finally, it

discusses the rights of users and international regulations that are in place or currently lacking.

Advanced Persistent Threat

All organizations are embarking on a journey to the cloud. Their users are online and taking advantage of productivity tools like SalesForce. Enterprises are in the midst of transitioning to Office 365. This book maps the journey of 16 leading enterprises around the world including Fannie Mae, Siemens, Google, Microsoft, and Amazon itself.

The Responsibilities of Online Service Providers

This book is essential reading for anyone wanting to protect Internet-connected computers from unauthorized access. Coverage includes TCP/IP, setting up firewalls, testing and maintaining firewalls, and much more. All of the major important firewall products are covered including Microsoft Internet Security and Acceleration Server (ISA), ISS BlackICE, Symantec Firewall, Check Point NG, and PIX Firewall. Firewall configuration strategies and techniques are covered in depth. The book answers questions about firewalls, from How do I make Web/HTTP work through my firewall? To What is a DMZ, and why do I want one? And What are some common attacks, and how can I protect my system against them? The Internet's explosive growth over the last decade has forced IT professionals to work even harder to secure the private networks connected to it—from erecting firewalls that keep out malicious intruders to building virtual private networks (VPNs) that permit protected, fully encrypted communications over the Internet's vulnerable public infrastructure. The Best Damn Firewalls Book Period covers the most popular Firewall products, from Cisco's PIX Firewall to Microsoft's ISA Server to CheckPoint NG, and all the components of an effective firewall set up. Anything needed to protect the perimeter of a network can be found in this book. - This book is all encompassing, covering general Firewall issues and protocols, as well as specific products. - Anyone studying for a security specific certification, such as SANS' GIAC Certified Firewall Analyst (GCFW) will find this book an invaluable resource. - The only book to cover all major firewall products from A to Z: CheckPoint, ISA Server, Symatec, BlackICE, PIX Firewall and Nokia.

Access Denied

Their proposition sounded so simple that it took a few minutes to grasp its audacity. The four NYU undergrads-classic computer nerds-wanted to build a social network that would allow users to control the information they shared about themselves, instead of surrendering their privacy (and personal data) to big businesses like Facebook. They were hoping to raise $10,000 in 30 days, enough to keep them in ramen and pizza for the summer in a basement in San Francisco while they coded. Their project was called "Diaspora." Apparently, the world had been waiting. Their 2010 Kickstarter campaign

ended the first day with three backers. Before long they had raised $200,000. In a matter of days, the Diaspora Four had received a global commission to re-bottle the genie of personal privacy. The ambitions of the Diaspora Four were underwritten by that heroic mix of optimism and naivete you only seem to have when you're twenty, egged on by the elite of the digital community. But as the months wore on and the money wore out, they couldn't get there-coding failures, bad business decisions, over-reach and under-organization, and the inevitable conflicts of personality and goals. When Ilya committed suicide in the fall of 2011, they found out how much they had all been on their own all along.

Zero Trust Networks

Entrepreneurs have long been taught that to be successful, they need to spend months perfecting a business plan and finding investors before they can finally launch their business. But with the marketplace changing at lightning speed, this notion is not only outdated-it's costly. There's no point to building a business in a bubble. Today's entrepreneurs must embrace the idea of "failing fast." They need to connect with real customers and determine quickly whether their idea is worth pursuing, needs new direction, or should be abandoned altogether. Fail Fast or Win Big shows entrepreneurs how to: Create a rapid prototype of their product or service * Develop a business model instead of a business plan * Test it repeatedly with customers so they can spot failure early * Continue to refine the model based on customer interactions * Leverage their network and resources in order to run lean The longer it takes to launch a company, the more changes there will have been in the market place. Featuring real-life examples of entrepreneurs who set out to fail fast and ended up winning big, this ground breaking guide reveals how the right kind of risk can really pay off.

Bonds Of Freedom

The book is a collection of high-quality peer-reviewed research papers presented in International Conference on Soft Computing Systems (ICSCS 2015) held at Noorul Islam Centre for Higher Education, Chennai, India. These research papers provide the latest developments in the emerging areas of Soft Computing in Engineering and Technology. The book is organized in two volumes and discusses a wide variety of industrial, engineering and scientific applications of the emerging techniques. It presents invited papers from the inventors/originators of new applications and advanced technologies.

ROMANCE ACTION & ADVENTURE MYSTERY & THRILLER BIOGRAPHIES & HISTORY CHILDREN'S YOUNG ADULT FANTASY HISTORICAL FICTION HORROR LITERARY FICTION NON-FICTION SCIENCE FICTION