

Read Online Network Security Essentials Pdf For Free

Security+ Essentials Nov 12 2020 Few Information Technology skills are in more demand these days than those related to security and few qualifications in this field are more respected than CompTIA's Security+ certification. Security+ Essentials is an eBook designed to provide the knowledge necessary to pass the CompTIA Security+ exam. Topics covered include I.T. infrastructure security, access control, cryptography, intrusion detection, firewall configuration, threat types, public key infrastructure and more. If you are planning to study for the Security+ exam, or simply want to learn more about I.T. Security in general, Security+ Essentials is an ideal source of information.

Microsoft Windows Security Essentials Mar 17 2021 Windows security concepts and technologies for IT beginners IT security can be a complex topic, especially for those new to the field of IT. This full-color book, with a focus on the Microsoft Technology Associate (MTA) program, offers a clear and easy-to-understand approach to Windows security risks and attacks for newcomers to the world of IT. By paring down to just the essentials, beginners gain a solid foundation of security concepts upon which more advanced topics and technologies can be built. This straightforward guide begins each chapter by laying out a list of topics to be discussed, followed by a concise discussion of the core networking skills you need to have to gain a strong handle on the subject matter. Chapters conclude with review questions and suggested labs so you can measure your level of understanding of the chapter's content. Serves as an ideal resource for gaining a solid understanding of fundamental security concepts and skills Offers a straightforward and direct approach to security basics and covers anti-malware software products, firewalls, network topologies and devices, network ports, and more Reviews all the topics you need to know for taking the MTA 98-367 exam Provides an overview of security components, looks at securing access with permissions, addresses audit policies and network auditing, and examines protecting clients and servers If you're new to IT and interested in entering the IT workforce, then Microsoft Windows Security Essentials is essential reading.

CompTIA Security+ Certification Guide Jun 19 2021 CompTIA Security+ Certification Guide makes the most complex Security+ concepts easy to understand despite having no prior knowledge. It offers exam tips in every chapter along with access to practical exercises and exam checklist that map to the exam objectives and it is the perfect study guide to help you pass CompTIA Security+ SY0-501 exam.

Workplace Security Essentials Sep 03 2022 Summary: A practical how-to guide for improving workplace safety and security without spending significant resources.

Security+ Guide to Network Security Fundamentals Dec 14 2020 Reflecting the latest trends and developments from the information security field, best-selling Security+ Guide to Network Security Fundamentals, Fourth Edition, provides a complete introduction to practical network and computer security and maps to the CompTIA Security+ SY0-301 Certification Exam. The text covers the fundamentals of network security, including compliance and operational security; threats and vulnerabilities; application, data, and host security; access control and identity management; and cryptography. The updated edition includes new topics, such as psychological approaches to social engineering attacks, Web application attacks, penetration testing, data loss prevention, cloud computing security, and application programming development security. The new edition features activities that link to the Information Security Community Site, which offers video lectures, podcats, discussion boards,

additional hands-on activities and more to provide a wealth of resources and up-to-the minute information. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

Information Security Essentials Nov 05 2022 As technological and legal changes have hollowed out the protections that reporters and news organizations have depended upon for decades, information security concerns facing journalists as they report, produce, and disseminate the news have only intensified. From source prosecutions to physical attacks and online harassment, the last two decades have seen a dramatic increase in the risks faced by journalists at all levels even as the media industry confronts drastic cutbacks in budgets and staff. As a result, few professional or aspiring journalists have a comprehensive understanding of what is required to keep their sources, stories, colleagues, and reputations safe. This book is an essential guide to protecting news writers, sources, and organizations in the digital era. Susan E. McGregor provides a systematic understanding of the key technical, legal, and conceptual issues that anyone teaching, studying, or practicing journalism should know. Bringing together expert insights from both leading academics and security professionals who work at and with news organizations from BuzzFeed to the Associated Press, she lays out key principles and approaches for building information security into journalistic practice. McGregor draws on firsthand experience as a Wall Street Journal staffer, followed by a decade of researching, testing, and developing information security tools and practices. Filled with practical but evergreen advice that can enhance the security and efficacy of everything from daily beat reporting to long-term investigative projects, Information Security Essentials is a vital tool for journalists at all levels.

GSEC GIAC Security Essentials Certification All-in-One Exam Guide Jan 15 2021 "All-in-One Is All You Need." Get complete coverage of all the objectives on Global Information Assurance Certification's Security Essentials (GSEC) exam inside this comprehensive resource. GSEC GIAC Security Essentials Certification All-in-One Exam Guide provides 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 authoritative resource also serves as an essential on-the-job reference. COVERS ALL EXAM TOPICS, INCLUDING: Networking fundamentals Network design Authentication and access control Network security Linux and Windows Encryption Risk management Virtual machines Vulnerability control Malware Physical security Wireless technologies VoIP ELECTRONIC CONTENT FEATURES: TWO PRACTICE EXAMS AUTHOR VIDEOS PDF eBook

Cyber Security Essentials Dec 06 2022 The sophisticated methods used in recent high-profile cyber incidents have driven many to need to understand how such security issues work. Demystifying the complexity often associated with information assurance, Cyber Security Essentials provides a clear understanding of the concepts behind prevalent threats, tactics, and procedures. To accomplish this, the team of security professionals from VeriSign's iDefense Security Intelligence Services supply an extensive review of the computer security landscape. Although the text is accessible to those new to cyber security, its comprehensive nature makes it ideal for experts who need to explain how computer security works to non-technical staff. Providing a fundamental understanding of the theory behind the key issues impacting cyber security, the book: Covers attacker methods and motivations, exploitation trends, malicious code techniques, and the latest threat vectors Addresses more than 75 key security concepts in a series of concise, well-illustrated summaries designed for most levels of technical understanding Supplies actionable advice for the mitigation of threats Breaks down the code used to write exploits into understandable diagrams This book is not about the latest attack trends or botnets. It's about the reasons why these problems continue to plague us. By better

understanding the logic presented in these pages, readers will be prepared to transition to a career in the growing field of cyber security and enable proactive responses to the threats and attacks on the horizon.

Security Automation Essentials: Streamlined Enterprise Security Management & Monitoring with SCAP Sep 10 2020 Master the latest digital security automation technologies Achieve a unified view of security across your IT infrastructure using the cutting-edge techniques contained in this authoritative volume. Security Automation Essentials: Streamlined Enterprise Security Management & Monitoring with SCAP lays out comprehensive technical, administrative, and operational strategies for security management. Discover how to define baseline requirements, automatically confirm patches and updates, identify vulnerabilities, write customized auditing content, and evaluate compliance across your enterprise. Throughout, the authors provide detailed case studies and tips on selecting appropriate security components. Understand SCAP (Security Content Automation Protocol) technologies and standards Track compliance using benchmarks and scoring systems Build machine-readable configuration checks using XCCDF, OVAL, and OCIL Perform vulnerability assessments and find misconfiguration Maximize product interoperability through the use of standard enumeration Assess and monitor residual risk using CVSS values Use SCAP editors and XML to create and debug automated checks Accurately assess threats using software assurance automation

Network Security Essentials Oct 24 2021 " For courses in Corporate, Computer and Network Security . " Network Security: Innovations and Improvements Network Security Essentials: Applications and Standards introduces readers to the critical importance of internet security in our age of universal electronic connectivity. Amidst viruses, hackers, and electronic fraud, organizations and individuals are constantly at risk of having their private information compromised. This creates a heightened need to protect data and resources from disclosure, guarantee their authenticity, and safeguard systems from network-based attacks. The Sixth Edition covers the expanding developments in the cryptography and network security disciplines, giving readers a practical survey of applications and standards. The text places emphasis on applications widely used for Internet and corporate networks, as well as extensively deployed internet standards.

Security-Essentials : In a World Gone Mad Dec 26 2021 One of the core responsibilities of any emergency preparedness situation is to just simply survive, to put the pieces of your life back together and move on, Unfortunately, many of us today are not prepared for the dangers that could occur at a moment's notice. Today we are living in a world where families are no longer safe in their neighborhoods, children are no longer safe at schools, churches, airports, grocery stores and other public places are now prime targets for gun violence and mass shootings. Our city infrastructures and water sources are compromised, the growing food shortage around the world will no doubt cause the average man to do the unthinkable just to provide for his family. With the threat of a nuclear war, and rising gas prices, would make anyone believe that we are truly living in a world gone mad, Security Essentials not only address some of these issues, but let you know how to survive, put your life back together, and move on.

Network Security Essentials: Applications and Standards, 4/e Apr 17 2021

Cybersecurity Essentials Feb 25 2022 An accessible introduction to cybersecurity concepts and practices Cybersecurity Essentials provides a comprehensive introduction to the field, with expert coverage of essential topics required for entry-level cybersecurity certifications. An effective defense consists of four distinct challenges: securing the infrastructure, securing devices, securing local networks, and securing the perimeter. Overcoming these challenges requires a detailed understanding of the

concepts and practices within each realm. This book covers each challenge individually for greater depth of information, with real-world scenarios that show what vulnerabilities look like in everyday computing scenarios. Each part concludes with a summary of key concepts, review questions, and hands-on exercises, allowing you to test your understanding while exercising your new critical skills. Cybersecurity jobs range from basic configuration to advanced systems analysis and defense assessment. This book provides the foundational information you need to understand the basics of the field, identify your place within it, and start down the security certification path. Learn security and surveillance fundamentals Secure and protect remote access and devices Understand network topologies, protocols, and strategies Identify threats and mount an effective defense Cybersecurity Essentials gives you the building blocks for an entry level security certification and provides a foundation of cybersecurity knowledge

Wireless Security Essentials May 31 2022 As wireless device usage increases worldwide, so does the potential for malicious code attacks. In this timely book, a leading national authority on wireless security describes security risks inherent in current wireless technologies and standards, and schools readers in proven security measures they can take to minimize the chance of attacks to their systems. * Russell Dean Vines is the coauthor of the bestselling security certification title, The CISSP Prep Guide (0-471-41356-9) * Book focuses on identifying and minimizing vulnerabilities by implementing proven security methodologies, and provides readers with a solid working knowledge of wireless technology and Internet-connected mobile devices

Identifying and Exploring Security Essentials Apr 05 2020 This new book gives readers a unique approach to the study of security issues, useful for either those already in the field or before they actually find themselves employed in a specific security-related job. Written in a clear, easy-to-understand style, this book gives readers the opportunity to look at security from various perspectives; it grounds them firmly in the history and fundamentals of the field, as well as prepares them for today's most difficult security challenges. Topics comprehensively covered in this book include: the use of technology in physical security; understanding security in the context of setting; security scenarios; public and private police relations; legal liability; internal resource identification; external community connections; and more. Homeland security means security issues are not just for security practitioners anymore. Everyone should be actively educating themselves about security-related subjects, and become familiar with security needs in various target environments. As such, this book is not only for those in the security field, but for others such as school principals, hospital workers, office managers and business executives, and owners and managers of all types of businesses.

Solaris 10 Security Essentials Feb 13 2021 Solaris™ 10 Security Essentials describes the various security technologies contained in the Solaris operating system. The book describes how to make installations secure and how to configure the OS to the particular needs of your environment, whether your systems are on the edge of the Internet or running a data center. The authors present the material in a straightforward way that makes a seemingly arcane subject accessible to system administrators at all levels. The strengths of the Solaris operating system's security model are its scalability and its adaptability. It can protect a single user with login authentication or multiple users with Internet and intranet configurations requiring user-rights management, authentication, encryption, IP security, key management, and more. This book is written for users who need to secure their laptops, network administrators who must secure an entire company, and everyone in between. The book's topics include Zones virtualization security System hardening Trusted Extensions (Multi-layered Security) Privileges and role-based access control (RBAC) Cryptographic services and key management Auditing

Network security Pluggable Authentication Modules (PAM) Solaris™ 10 Security Essentials is the first in a new series on Solaris system administration. It is a superb guide to deploying and managing secure computer environments.

Network Security Essentials Sep 22 2021 Network Security Essentials, Third Edition is a thorough, up-to-date introduction to the deterrence, prevention, detection, and correction of security violations involving information delivery across networks and the Internet.

CISSP Guide to Security Essentials Oct 04 2022 CISSP GUIDE TO SECURITY ESSENTIALS, Second Edition, provides complete, focused coverage to prepare students and professionals alike for success on the Certified Information Systems Security Professional (CISSP) certification exam. The text opens with an overview of the current state of information security, including relevant legislation and standards, before proceeding to explore all ten CISSP domains in great detail, from security architecture and design to access control and cryptography. Each chapter opens with a brief review of relevant theory and concepts, followed by a strong focus on real-world applications and learning tools designed for effective exam preparation, including key terms, chapter summaries, study questions, hands-on exercises, and case projects. Developed by the author of more than 30 books on information security the Second Edition of this trusted text has been updated to reflect important new developments in technology and industry practices, providing an accurate guide to the entire CISSP common body of knowledge. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

UNIX System Security Essentials Feb 02 2020 How can a broad variety of UNIX operating system users keep the system secure? This book provides answers for users, system administrators and programmers. The author pinpoints the critical threats to data security the UNIX system users should recognize, avoid and overcome. Includes a summary of the key UNIX system security commands and system calls.

Microsoft Security Essentials User Manual (Digital Short Cut), e-Pub May 19 2021 Microsoft Security Essentials User Manual is the unofficial user's manual for Microsoft's new free anti-malware program. It shows users how to use MSE to safeguard your computer from viruses and spyware, how to download and configure MSE, how to manually scan for malware, how to keep the program updated, and how to schedule regular maintenance. Understand the malware threat Download and install MSE Configure MSE for your system Set up automatic scanning Use real-time protection Configure advanced options Update your copy of MSE Scan your system Learn how automatic scans differ from custom scans View your scanning history and eliminate threat

Workplace Security Essentials Aug 02 2022 Whether you are a business owner, department manager, or even a concerned employee, Workplace Security Essentials will show you how to improve workplace safety and security using real-life examples and step-by-step instructions. Every organization, be it large or small, needs to be prepared to protect its facilities, inventory, and, most importantly, its staff. Workplace Security Essentials is the perfect training resource to help businesses implement successful security measures, boost employee morale and reduce turnover, protect the company's reputation and public profile, and develop the ability to process and analyze risks of all kinds. Workplace Security Essentials helps the reader understand how different business units can work together and make security a business function—not a burden or extra cost. Shows how to identify threats using tried-and-true methods for assessing risk in any size organization Uses real-world examples and scenarios to illustrate what can go wrong-and what can go right when you are prepared Prepares the reader for worst-case

scenarios and domestic violence that may spill over into the workplace Provides a clear understanding of various electronic systems, video surveillance, and burglar alarms, and how to manage a security guard force

GSEC GIAC Security Essentials Certification All-in-One Exam Guide, Second Edition Jan 03 2020 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. Fully updated coverage of every topic on the current version of the GSEC exam Get complete coverage of all the objectives on Global Information Assurance Certification's Security Essentials (GSEC) exam inside this comprehensive resource. GSEC GIAC Security Essentials Certification All-in-One Exam Guide, Second Edition provides 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 authoritative resource also serves as an essential on-the-job reference. Covers all exam topics, including: •Networking fundamentals •Network design •Cloud computing •Authentication and access control •Unix/Linux •Windows •Encryption •Risk management •Virtual machines •Vulnerability control •Malware •Incident response •Wireless technologies •Log Management •IoT and embedded devices Online content features: •Two practice exams •Test engine that provides full-length practice exams and customizable quizzes •Author videos

Optimizing IEEE 802.11i Resource and Security Essentials Oct 31 2019 In the past decade, the number of wireless devices has grown exponentially. Decades ago, all systems were wired computer systems. Wireless technology was not accessible in mobile and portable devices until in recent years, and has followed a variety of methods for encryption and resource management. The purpose of the research in Optimizing IEEE 802.11i Resources and Security Essentials is to determine the issues of the performance in current encryption methods in AES-CCMP in different types of devices and handle it so that an optimized resource usage would be achieved with the required security. Two modes for 802.11i for two different groups of devices is suggested and evaluated with the current encryption method for AES-CCMP to compare the performance. Almost every organization in today's world relies on wireless networks to transmit information, and much of that information should be kept secure. Banking, healthcare, and the military are all vital industries that rely on wireless security for a huge section of their operations. Security experts of today and tomorrow will learn a lot from Optimizing IEEE 802.11i Resources and Security Essentials, and it can be used for master level in computer science, information security, wireless network security and cryptography. The research in this book covers how to best balance security concerns with limited resources available on wireless devices as well as how to optimize security resources on higher-end non-mobile devices

Internet Security Fundamentals Oct 12 2020 An easy to understand guide of the most commonly faced security threats any computer user is likely to come across via email, social media and online shopping. This is not aimed at people studying Internet Security or CISSP, but general users, though still helpful to both. Antivirus software is now incredibly advanced, but the problem of viruses is worse than ever! This is because many viruses trick the user into installing them. The same way that the most sophisticated alarm system and door security is not much use if you open the door from the inside to let someone in. This book explains in easy to understand terms, why you cannot just rely on antivirus, but also need to be aware of the various scams and tricks used by criminals.

Security Essentials Jul 09 2020 The Security Essentials Study Guide provides users with a valuable means of review and practice essential for important knowledge and skills. The first half of the study guide provides practice exercises that reinforce concepts and skills

learned in the corresponding textbook chapters. The completion of these activities greatly enhances the comprehension of the topics covered in the corresponding textbook chapter. The second half of the study guide includes a CompTIA Security+ Reference Guide to help learners study and prepare for the CompTIA Security+ Exam. The reference guide includes a detailed review of each CompTIA objective, including examples and related concepts.

Computer and Network Security Essentials Jan 27 2022 This book introduces readers to the tools needed to protect IT resources and communicate with security specialists when there is a security problem. The book covers a wide range of security topics including Cryptographic Technologies, Network Security, Security Management, Information Assurance, Security Applications, Computer Security, Hardware Security, and Biometrics and Forensics. It introduces the concepts, techniques, methods, approaches, and trends needed by security specialists to improve their security skills and capabilities. Further, it provides a glimpse into future directions where security techniques, policies, applications, and theories are headed. The book represents a collection of carefully selected and reviewed chapters written by diverse security experts in the listed fields and edited by prominent security researchers. Complementary slides are available for download on the book's website at Springer.com.

Practical Paranoia Aug 10 2020 Version 1.2, updated October 4, 2015. The best-selling, easiest, step-by-step, comprehensive guide to securing your home or business Windows 10 computers. GUARANTEED Official workbook for the Practical Paranoia: Security Essentials Workshop. Designed for both workshop use and self-study. The entire workshop is contained within the book. Includes all instructor presentations, hands-on assignments, links to all software, and security checklist. You don't need to be paranoid to know they are out there to get your computer, data, and identity. * 2,000,000 laptops were stolen or lost in the US last year. * Malware attacks on Windows computers are commonplace. * Dozens of eyes may be able to see your name and password, along with the contents of every email you send. * Once the bad guy has his hands on your PC, it takes under one minute to bypass your password to gain access to all your data. * With a slight bit of social engineering your Google and Microsoft accounts, along with all their data, is freely accessible. * Through PRISM and other avenues, our government has access to your online browsing and email history. You don't need to be an Windows Engineer to protect your system! In this easy, step-by-step guide, CIO, Security Specialist, and Certified IT Consultant Marc L. Mintz takes any Windows user-from the novice with no technical skills, to experienced IT professional-through the process of fully encrypting and hardening the security of their computer, data, email, documents, network, Instant Messaging, storage devices, computer, browsing, and entire Internet experience. Guaranteed to be the easiest to follow and most comprehensive Windows 10 book available.

Cyber Security Essentials Apr 29 2022 The sophisticated methods used in recent high-profile cyber incidents have driven many to need to understand how such security issues work. Demystifying the complexity often associated with information assurance, Cyber Security Essentials provides a clear understanding of the concepts behind prevalent threats, tactics, and procedures. To accomplish

Security Essentials Sep 30 2019 Security Essentials provides foundational skills and knowledge needed to work as a security professional. In this text, you will explore not only various threats and vulnerabilities that affect computer systems but also how to secure an organization against them. Topics covered include enabling user security and authentication, implementing physical security controls, hardening and securing networked devices, and designing and administering secure networks, among other

important data security concepts. This text is aligned to the CompTIA Security+ SY0-601 Certification Exam Objectives. Each chapter opens with a list of exam objectives covered within the chapter. In addition, CompTIA objectives are noted with a Security+ icon in the margin at the point of coverage in the content. Chapters conclude with a set of sample Security+ Exam questions to help study and prepare for certification. The CompTIA Security+ Exam is one of CompTIA's four Core Skills Certifications, which provide a pathway to careers in either cybersecurity or IT infrastructure. Additionally, the text includes content that goes beyond the scope of the CompTIA Security+ Certification Exam. Information about soft skills and employment is included, as well as appendices detailing commonly encountered ASCII characters; important acronyms and abbreviations; and decimal, binary, octal, and hexadecimal number conversions. Security Essentials introduces information on data security and presents these topics in a way that helps the reader earn CompTIA Security+ Certification and stand out in an increasingly competitive job market.

CISSP Guide to Security Essentials Mar 29 2022 CISSP GUIDE TO SECURITY ESSENTIALS, Second Edition, provides complete, focused coverage to prepare students and professionals alike for success on the Certified Information Systems Security Professional (CISSP) certification exam. The text opens with an overview of the current state of information security, including relevant legislation and standards, before proceeding to explore all ten CISSP domains in great detail, from security architecture and design to access control and cryptography. Each chapter opens with a brief review of relevant theory and concepts, followed by a strong focus on real-world applications and learning tools designed for effective exam preparation, including key terms, chapter summaries, study questions, hands-on exercises, and case projects. Developed by the author of more than 30 books on information security, the Second Edition of this trusted text has been updated to reflect important new developments in technology and industry practices, providing an accurate guide to the entire CISSP common body of knowledge. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

GSEC GIAC Security Essentials Certification All-in-One Exam Guide Aug 22 2021 Providing learning objectives at the beginning of each chapter; exam tips; practice exam questions; and in-depth explanations; this comprehensive resource will help you prepare for - and pass - the Global Information Assurance Certification's Security Essentials (GSEC) exam.

--

Lees' Process Safety Essentials Jun 07 2020 Lees' Process Safety Essentials is a single-volume digest presenting the critical, practical content from Lees' Loss Prevention for day-to-day use and reference. It is portable, authoritative, affordable, and accessible — ideal for those on the move, students, and individuals without access to the full three volumes of Lees'. This book provides a convenient summary of the main content of Lees', primarily drawn from the hazard identification, assessment, and control content of volumes one and two. Users can access Essentials for day-to-day reference on topics including plant location and layout; human factors and human error; fire, explosion and toxic release; engineering for sustainable development; and much more. This handy volume is a valuable reference, both for students or early-career professionals who may not need the full scope of Lees', and for more experienced professionals needing quick, convenient access to information. Boils down the essence of Lees'—the process safety encyclopedia trusted worldwide for over 30 years Provides safety professionals with the core information they need to understand the most common safety and loss prevention challenges Covers the latest standards and presents information, including recent incidents such as Texas City and Buncefield

Microsoft Windows Security Essentials Jan 07 2023 Windows security concepts and technologies for IT beginners IT security can be a complex topic, especially for those new to the field of IT. This full-color book, with a focus on the Microsoft Technology Associate (MTA) program, offers a clear and easy-to-understand approach to Windows security risks and attacks for newcomers to the world of IT. By paring down to just the essentials, beginners gain a solid foundation of security concepts upon which more advanced topics and technologies can be built. This straightforward guide begins each chapter by laying out a list of topics to be discussed, followed by a concise discussion of the core networking skills you need to have to gain a strong handle on the subject matter. Chapters conclude with review questions and suggested labs so you can measure your level of understanding of the chapter's content. Serves as an ideal resource for gaining a solid understanding of fundamental security concepts and skills Offers a straightforward and direct approach to security basics and covers anti-malware software products, firewalls, network topologies and devices, network ports, and more Reviews all the topics you need to know for taking the MTA98-367 exam Provides an overview of security components, looks at securing access with permissions, addresses audit policies and network auditing, and examines protecting clients and servers If you're new to IT and interested in entering the IT workforce, then Microsoft Windows Security Essentials is essential reading.

Windows PowerShell 2.0 Bible Aug 29 2019 Here's the complete guide to Windows PowerShell 2.0 for administrators and developers Windows PowerShell is Microsoft's next-generation scripting and automation language. This comprehensive volume provides the background that IT administrators and developers need in order to start using PowerShell automation in exciting new ways. It explains what PowerShell is, how to use the language, and specific ways to apply PowerShell in various technologies. Windows PowerShell is Microsoft's standard automation tool and something that every Windows administrator will eventually have to understand; this book provides the background necessary to apply PowerShell automation. Covers how to use the language and specific ways to apply PowerShell in a variety of scenarios Addresses new features in the latest version of PowerShell and the additional functionality delivered by new products that provided direct or indirect ways to use PowerShell for scripting and automation purposes Explores the language fundamentals and how to use PowerShell for desktop, server, server application, and virtualization/cloud situations This thorough guide goes well beyond theory to offer real-world information and new scripting techniques, enabling administrators and developers to make the most of PowerShell 2.0.

Homeland Security Jul 21 2021 Homeland Security: The Essentials, Second Edition concisely outlines the risks facing the US today and the structures we have put in place to deal with them. The authors expertly delineate the bedrock principles of preparing for, mitigating, managing, and recovering from emergencies and disasters. From cyberwarfare, to devastating tornadoes, to car bombs, all hazards currently fall within the purview of the Department of Homeland Security, yet the federal role must be closely aligned with the work of partners in the private sector. The book lays a solid foundation for the study of present and future threats to our communities and to national security, also challenging readers to imagine more effective ways to manage these risks. Highlights and expands on key content from the bestselling book Introduction to Homeland Security Concisely delineates the bedrock principles of preparing for, mitigating, managing, and recovering from emergencies and disasters Provides coverage of the Boston Marathon bombing Explains the border security, immigration, and intelligence functions in detail Analyzes the NIST Cybersecurity Framework for critical infrastructure protection Explores the emergence of social media as a tool for reporting

on homeland security issues

ASP.NET Web API Security Essentials May 07 2020 Take the security of your ASP.NET Web API to the next level using some of the most amazing security techniques around

About This Book This book has been completely updated for ASP.NET Web API 2.0 including the new features of ASP.NET Web API such as Cross-Origin Resource Sharing (CORS) and OWIN self-hosting Learn various techniques to secure ASP.NET Web API, including basic authentication using authentication filters, forms, Windows Authentication, external authentication services, and integrating ASP.NET's Identity system

An easy-to-follow guide to enable SSL, prevent Cross-Site Request Forgery (CSRF) attacks, and enable CORS in ASP.NET Web API

Who This Book Is For This book is intended for anyone who has previous knowledge of developing ASP.NET Web API applications. Good working knowledge and experience with C# and .NET Framework are prerequisites for this book.

What You Will Learn Secure your web API by enabling Secured Socket Layer (SSL) Manage your application's user accounts by integrating ASP.NET's Identity system Ensure the security of your web API by implementing basic authentication Implement forms and Windows authentication to secure your web API Use external authentication such as Facebook and Twitter to authenticate a request to a web API Protect your web API from CSRF attacks Enable CORS in your web API to explicitly allow some cross-origin requests while rejecting others Fortify your web API using OAuth2 In Detail This book incorporates the new features of ASP.NET Web API 2 that will help you to secure an ASP.NET Web API and make a well-informed decision when choosing the right security mechanism for your security requirements. We start by showing you how to set up a browser client to utilize ASP.NET Web API services. We then cover ASP.NET Web API's security architecture, authentication, and authorization to help you secure a web API from unauthorized users. Next, you will learn how to use SSL with ASP.NET Web API, including using SSL client certificates, and integrate the ASP.NET Identity system with ASP.NET Web API. We'll show you how to secure a web API using OAuth2 to authenticate against a membership database using OWIN middleware. You will be able to use local logins to send authenticated requests using OAuth2. We also explain how to secure a web API using forms authentication and how users can log in with their Windows credentials using integrated Windows authentication. You will come to understand the need for external authentication services to enable OAuth/OpenID and social media authentication. We'll then help you implement anti-Cross-Site Request Forgery (CSRF) measures in ASP.NET Web API. Finally, you will discover how to enable Cross-Origin Resource Sharing (CORS) in your web API application.

Style and approach Each chapter is dedicated to a specific security technique, in a task-based and easy-to-follow way. Most of the chapters are accompanied with source code that demonstrates the step-by-step guidelines of implementing the technique, and includes an explanation of how each technique works.

Android Application Security Essentials Jul 01 2022 Android Application Security Essentials is packed with examples, screenshots, illustrations, and real world use cases to secure your apps the right way. If you are looking for guidance and detailed instructions on how to secure app data, then this book is for you. Developers, architects, managers, and technologists who wish to enhance their knowledge of Android security will find this book interesting. Some prior knowledge of development on the Android stack is desirable but not required.

VMware View Security Essentials Dec 02 2019 A practical and fast-paced guide that gives you all the information you need to secure your virtual environment. This book is a "how-to" for the novice, a "reference guide" for the advanced user, and a "go to" for the experienced user in all the aspects of VMware View desktop virtualization security.

Zscaler Cloud Security Essentials Nov 24 2021 Harness the capabilities of Zscaler to deliver a secure, cloud-based, scalable web proxy and provide a zero-trust network access solution for private enterprise application access to end users Key Features Get up to speed with Zscaler without the need for expensive training Implement Zscaler Internet Access (ZIA) and Zscaler Private Access (ZPA) security solutions with real-world deployments Find out how to choose the right options and features to architect a customized solution with Zscaler Book Description Many organizations are moving away from on-premises solutions to simplify administration and reduce expensive hardware upgrades. This book uses real-world examples of deployments to help you explore Zscaler, an information security platform that offers cloud-based security for both web traffic and private enterprise applications. You'll start by understanding how Zscaler was born in the cloud, how it evolved into a mature product, and how it continues to do so with the addition of sophisticated features that are necessary to stay ahead in today's corporate environment. The book then covers Zscaler Internet Access and Zscaler Private Access architectures in detail, before moving on to show you how to map future security requirements to ZIA features and transition your business applications to ZPA. As you make progress, you'll get to grips with all the essential features needed to architect a customized security solution and support it. Finally, you'll find out how to troubleshoot the newly implemented ZIA and ZPA solutions and make them work efficiently for your enterprise. By the end of this Zscaler book, you'll have developed the skills to design, deploy, implement, and support a customized Zscaler security solution. What you will learn Understand the need for Zscaler in the modern enterprise Study the fundamental architecture of the Zscaler cloud Get to grips with the essential features of ZIA and ZPA Find out how to architect a Zscaler solution Discover best practices for deploying and implementing Zscaler solutions Familiarize yourself with the tasks involved in the operational maintenance of the Zscaler solution Who this book is for This book is for security engineers, security architects, security managers, and security operations specialists who may be involved in transitioning to or from Zscaler or want to learn about deployment, implementation, and support of a Zscaler solution. Anyone looking to step into the ever-expanding world of zero-trust network access using the Zscaler solution will also find this book useful.

Network Security Essentials Mar 05 2020 This book provides a practical, up-to-date, and comprehensive survey of network-based and Internet-based security applications and standards. This books covers e-mail security, IP security, Web security, and network management security. It also includes a concise section on the discipline of cryptography—covering algorithms and protocols underlying network security applications, encryption, hash functions, digital signatures, and key exchange. For system engineers, engineers, programmers, system managers, network managers, product marketing personnel, and system support specialists.