

Network Security With Openssl

Yeah, reviewing a book **Network Security With Openssl** could build up your close connections listings. This is just one of the solutions for you to be successful. As understood, success does not suggest that you have extraordinary points.

Comprehending as well as concord even more than further will manage to pay for each success. neighboring to, the notice as competently as insight of this Network Security With Openssl can be taken as without difficulty as picked to act.

Mastering Python for Networking and Security - José Manuel Ortega 2018-09-28

Nowadays, configuring a network and automating security protocols are quite difficult to implement. However, using Python makes it easy to automate this whole process. This book explains the process of using Python for building networks, detecting network errors, and performing different security protocols using Python Scripting.

[Linux Security Cookbook](#) - Daniel J. Barrett 2003-06-02

Computer security is an ongoing process, a relentless contest between system administrators and intruders. A good administrator needs to stay one step ahead of any adversaries, which often involves a continuing process of education. If you're grounded in the basics of security, however, you won't necessarily want a complete treatise on the subject each time you pick up a book. Sometimes you want to get straight to the point. That's exactly what the new Linux Security Cookbook does. Rather than provide a total security solution for Linux computers, the authors present a series of easy-to-follow recipes--short, focused pieces of code that administrators can use to improve security and perform common tasks securely. The Linux Security Cookbook includes real solutions to a wide range of targeted problems, such as sending encrypted email within Emacs, restricting access to network services at particular times of day, firewalling a webserver, preventing IP spoofing, setting up key-based SSH authentication, and much more. With over 150 ready-to-use scripts and configuration files, this unique book helps administrators secure their systems without having to look up specific syntax. The book begins with recipes devised to establish a secure system, then moves on to secure day-to-day practices, and concludes with techniques to help your system stay secure. Some of the "recipes" you'll find in this book are: Controlling access to your system from firewalls down to individual services, using iptables, ipchains, xinetd, inetd, and more Monitoring your network with tcpdump, dsniiff, netstat, and other tools Protecting network connections with Secure Shell (SSH) and stunnel Safeguarding email sessions with Secure Sockets Layer (SSL) Encrypting files and email messages with GnuPG Probing your own security with password crackers, nmap, and handy scripts This cookbook's proven techniques are derived from hard-won experience. Whether you're responsible for security on a home Linux system or for a large corporation, or somewhere in between, you'll find valuable, to-the-point, practical recipes for dealing with everyday security issues. This book is a system saver.

Practical UNIX and Internet Security - Simson Garfinkel 2003-02-21

When Practical Unix Security was first published more than a decade ago, it became an instant classic. Crammed with information about host security, it saved many a Unix system administrator from disaster. The second edition added much-needed Internet security coverage and doubled the size of the original volume. The third edition is a comprehensive update of this very popular book - a companion for the Unix/Linux system administrator who needs to secure his or her organization's system, networks, and web presence in an increasingly hostile world. Focusing on the four most popular Unix variants today--Solaris, Mac OS X, Linux, and FreeBSD--this book contains new information on PAM (Pluggable Authentication Modules), LDAP, SMB/Samba, anti-theft technologies, embedded systems, wireless and laptop issues, forensics, intrusion detection, chroot jails, telephone scanners and firewalls, virtual and cryptographic filesystems, WebNFS, kernel security levels, outsourcing, legal issues, new Internet protocols and cryptographic algorithms, and much more. Practical Unix & Internet Security consists of six parts: Computer security basics: introduction to security problems and solutions, Unix history and lineage, and the importance of security policies as a basic element of system security. Security building blocks: fundamentals of Unix passwords, users, groups, the Unix filesystem, cryptography, physical security, and personnel security. Network security: a detailed look at modem and dialup security, TCP/IP, securing individual network services, Sun's RPC, various host

and network authentication systems (e.g., NIS, NIS+, and Kerberos), NFS and other filesystems, and the importance of secure programming. Secure operations: keeping up to date in today's changing security world, backups, defending against attacks, performing integrity management, and auditing. Handling security incidents: discovering a break-in, dealing with programmed threats and denial of service attacks, and legal aspects of computer security. Appendixes: a comprehensive security checklist and a detailed bibliography of paper and electronic references for further reading and research. Packed with 1000 pages of helpful text, scripts, checklists, tips, and warnings, this third edition remains the definitive reference for Unix administrators and anyone who cares about protecting their systems and data from today's threats.

SSL and TLS - Eric Rescorla 2001

"This is the best book on SSL/TLS. Rescorla knows SSL/TLS as well as anyone and presents it both clearly and completely.... At times, I felt like he's been looking over my shoulder when I designed SSL v3. If network security matters to you, buy this book." Paul Kocher, Cryptography Research, Inc. Co-Designer of SSL v3 "Having the right crypto is necessary but not sufficient to having secure communications. If you're using SSL/TLS, you should have "SSL and TLS" sitting on your shelf right next to "Applied Cryptography." Bruce Schneier, Counterpane Internet Security, Inc. Author of "Applied Cryptography" "Everything you wanted to know about SSL/TLS in one place. It covers the protocols down to the level of packet traces. It covers how to write software that uses SSL/TLS. And it contrasts SSL with other approaches. All this while being technically sound and readable!" Radia Perlman, Sun Microsystems, Inc. Author of "Interconnections" Secure Sockets Layer (SSL) and its IETF successor, Transport Layer Security (TLS), are the leading Internet security protocols, providing security for e-commerce, web services, and many other network functions. Using SSL/TLS effectively requires a firm grasp of its role in network communications, its security properties, and its performance characteristics. "SSL and TLS" provides total coverage of the protocols from the bits on the wire up to application programming. This comprehensive book not only describes how SSL/TLS is supposed to behave but also uses the author's free ssldump diagnostic tool to show the protocols in action. The author covers each protocol feature, first explaining how it works and then illustrating it in a live implementation. This unique presentation bridges the difficult gap between specification and implementation that is a common source of confusion and incompatibility. In addition to describing the protocols, "SSL and TLS" delivers the essential details required by security architects, application designers, and software engineers. Use the practical design rules in this book to quickly design fast and secure systems using SSL/TLS. These design rules are illustrated with chapters covering the new IETF standards for HTTP and SMTP over TLS. Written by an experienced SSL implementor, "SSL and TLS" contains detailed information on programming SSL applications. The author discusses the common problems faced by implementors and provides complete sample programs illustrating the solutions in both C and Java. The sample programs use the free OpenSSL and PureTLS toolkits so the reader can immediately run the examples. 0201615983B04062001

[Cyber Security and Digital Forensics](#) - Kavita Khanna 2021-10-01

This book features high-quality research papers presented at the International Conference on Applications and Techniques in Cyber Security and Digital Forensics (ICCSDF 2021), held at The NorthCap University, Gurugram, Haryana, India, during April 3-4, 2021. This book discusses the topics ranging from information security to cryptography, mobile application attacks to digital forensics, and from cyber security to blockchain. The goal of the book is to provide 360-degree view of cybersecurity to the readers which include cyber security issues, threats, vulnerabilities, novel idea, latest technique and technology, and mitigation of threats and attacks along with demonstration of practical applications. This book also highlights the latest development, challenges, methodologies as well as other emerging areas in this field. It

brings current understanding of common Web vulnerabilities while maintaining awareness and knowledge of contemporary standards, practices, procedures, and methods of Open Web Application Security Project. It also expounds how to recover information after a cybercrime.

Hands-On Network Programming with C - Lewis Van Winkle
2019-05-13

A comprehensive guide to programming with network sockets, implementing Internet protocols, designing IoT devices, and much more with C. Key Features Leverage your C or C++ programming skills to build powerful network applications. Get to grips with a variety of network protocols that allow you to load web pages, send emails, and do much more. Write portable network code for operating systems such as Windows, Linux, and macOS. Book Description Network programming, a challenging topic in C, is made easy to understand with a careful exposition of socket programming APIs. This book gets you started with modern network programming in C and the right use of relevant operating system APIs. This book covers core concepts, such as hostname resolution with DNS, that are crucial to the functioning of the modern web. You'll delve into the fundamental network protocols, TCP and UDP. Essential techniques for networking paradigms such as client-server and peer-to-peer models are explained with the help of practical examples. You'll also study HTTP and HTTPS (the protocols responsible for web pages) from both the client and server perspective. To keep up with current trends, you'll apply the concepts covered in this book to gain insights into web programming for IoT. You'll even get to grips with network monitoring and implementing security best practices. By the end of this book, you'll have experience of working with client-server applications, and be able to implement new network programs in C. The code in this book is compatible with the older C99 version as well as the latest C18 and C++17 standards. Special consideration is given to writing robust, reliable, and secure code that is portable across operating systems, including Winsock sockets for Windows and POSIX sockets for Linux and macOS. What you will learn Uncover cross-platform socket programming APIs. Implement techniques for supporting IPv4 and IPv6. Understand how TCP and UDP connections work over IP. Discover how hostname resolution and DNS work. Interface with web APIs using HTTP and HTTPS. Acquire hands-on experience with Simple Mail Transfer Protocol (SMTP). Apply network programming to the Internet of Things (IoT). Who this book is for If you're a developer or a system administrator who wants to enter the world of network programming, this book is for you. Basic knowledge of C programming is assumed.

Linux Server Security - Michael D. Bauer 2005

Provides advice on ways to ensure network security, covering such topics as DNS, Apache web server, OpenLDAP, email encryption, Cyrus IMAP service, and FTP server.

Cryptographic Hardware and Embedded Systems - CHES 2016 - Benedikt Gierlichs 2016-08-03

This book constitutes the proceedings of the 18th International Conference on Cryptographic Hardware and Embedded Systems, CHES 2016, held in Santa Barbara, CA, USA, in August 2016. The 30 full papers presented in this volume were carefully reviewed and selected from 148 submissions. They were organized in topical sections named: side channel analysis; automotive security; invasive attacks; side channel countermeasures; new directions; software implementations; cache attacks; physical unclonable functions; hardware implementations; and fault attacks.

OpenSSL Cookbook - Ivan Ristic 2013-10-03

A guide to the most frequently used OpenSSL features and commands, written by Ivan Ristic. Comprehensive coverage of OpenSSL installation, configuration, and key and certificate management. Includes SSL/TLS Deployment Best Practices, a design and deployment guide. Written by a well-known practitioner in the field and the author of SSL Labs and the SSL/TLS configuration assessment tool. Available in a variety of digital formats (PDF, EPUB, Mobi/Kindle); no DRM. Continuously updated. OpenSSL Cookbook is built around one chapter from Bulletproof SSL/TLS and PKI, a larger work that provides complete coverage of SSL/TLS and PKI topics. To download your free copy in various formats, visit feistyduck.com/books/openssl-cookbook/

Schneier on Security - Bruce Schneier 2009-03-16

Presenting invaluable advice from the world's most famous computer security expert, this intensely readable collection features some of the most insightful and informative coverage of the strengths and weaknesses of computer security and the price people pay -- figuratively and literally -- when security fails. Discussing the issues surrounding things such as airplanes, passports, voting machines, ID cards, cameras,

passwords, Internet banking, sporting events, computers, and castles, this book is a must-read for anyone who values security at any level -- business, technical, or personal.

The Networking CD Bookshelf - Craig Hunt 2002

More and more, technology professionals are relying on the Web, online help, and other online information sources to solve their tough problems. Now, with O'Reilly's "Networking CD Bookshelf, Version 2.0, you can have the same convenient online access to your favorite O'Reilly books--all from your CD-ROM drive. We've packed seven of our best-selling guides onto this CD-ROM, giving you 4,016 pages of O'Reilly references and tutorials --fully searchable and cross-referenced, so you can search either the individual index for each book or the master index for the entire collection. Included are the complete, unabridged versions of these popular titles: "TCP/IP Network Administration, 3rd Edition DNS & Bind, 4th Edition Building Internet Firewalls, 2nd Edition SSH, The Secure Shell: The Definitive Guide Network Troubleshooting Tools Managing NFS & NIS, 2nd Edition Essential SNMP. As a bonus, you also get the new paperback version of "TCP/IP Network Administration, 3rd Edition. Now it's easier than ever to find what you need to know about managing, administering, and protecting networks. This unique CD-ROM is a dream come true for network and system administrators--potent combination of books that offers unprecedented power and flexibility in this ever-expanding field. Formatted in HTML, "The Networking CD Bookshelf, Version 2.0, can be accessed with any web browser, so you have a complete library of technical books that you can carry with you anywhere you need it. No other resource makes so much valuable information so easy to find and so convenient to use.

Network Security Tools - Nitesh Dhanjani 2005-04-04

If you're an advanced security professional, then you know that the battle to protect online privacy continues to rage on. Security chat rooms, especially, are resounding with calls for vendors to take more responsibility to release products that are more secure. In fact, with all the information and code that is passed on a daily basis, it's a fight that may never end. Fortunately, there are a number of open source security tools that give you a leg up in the battle. Often a security tool does exactly what you want, right out of the box. More frequently, you need to customize the tool to fit the needs of your network structure. Network Security Tools shows experienced administrators how to modify, customize, and extend popular open source security tools such as Nikto, Ettercap, and Nessus. This concise, high-end guide discusses the common customizations and extensions for these tools, then shows you how to write even more specialized attack and penetration reviews that are suited to your unique network environment. It also explains how tools like port scanners, packet injectors, network sniffers, and web assessment tools function. Some of the topics covered include: Writing your own network sniffers and packet injection tools. Writing plugins for Nessus, Ettercap, and Nikto. Developing exploits for Metasploit. Code analysis for web applications. Writing kernel modules for security applications, and understanding rootkits. While many books on security are either tediously academic or overly sensational, Network Security Tools takes an even-handed and accessible approach that will let you quickly review the problem and implement new, practical solutions--without reinventing the wheel. In an age when security is critical, Network Security Tools is the resource you want at your side when locking down your network.

SSL & TLS Essentials - Stephen A. Thomas 2000-02-25

CD-ROM includes: Full-text, electronic edition of text.

Planning for PKI - Russ Housley 2001-03-27

An in-depth technical guide on the security technology driving Internet e-commerce expansion. "Planning for PKI" examines the number-one Internet security technology that will be widely adopted in the next two years. Written by two of the architects of the Internet PKI standards, this book provides authoritative technical guidance for network engineers, architects, and managers who need to implement the right PKI architecture for their organization. The authors discuss results and lessons learned from early PKI pilots, helping readers evaluate PKI deployment impact on current network architecture while avoiding the pitfalls of early technical mistakes. Four technical case studies detail the do's and don'ts of PKI implementation, illustrating both successes and failures of different deployments. Readers will also learn how to leverage future PKI-related technologies for additional benefits.

Practical Cryptography in Python - Seth James Nielson 2019-09-27

Develop a greater intuition for the proper use of cryptography. This book teaches the basics of writing cryptographic algorithms in Python, demystifies cryptographic internals, and demonstrates common ways

cryptography is used incorrectly. Cryptography is the lifeblood of the digital world's security infrastructure. From governments around the world to the average consumer, most communications are protected in some form or another by cryptography. These days, even Google searches are encrypted. Despite its ubiquity, cryptography is easy to misconfigure, misuse, and misunderstand. Developers building cryptographic operations into their applications are not typically experts in the subject, and may not fully grasp the implication of different algorithms, modes, and other parameters. The concepts in this book are largely taught by example, including incorrect uses of cryptography and how "bad" cryptography can be broken. By digging into the guts of cryptography, you can experience what works, what doesn't, and why. What You'll Learn Understand where cryptography is used, why, and how it gets misused Know what secure hashing is used for and its basic properties Get up to speed on algorithms and modes for block ciphers such as AES, and see how bad configurations break Use message integrity and/or digital signatures to protect messages Utilize modern symmetric ciphers such as AES-GCM and CHACHA Practice the basics of public key cryptography, including ECDSA signatures Discover how RSA encryption can be broken if insecure padding is used Employ TLS connections for secure communications Find out how certificates work and modern improvements such as certificate pinning and certificate transparency (CT) logs Who This Book Is For IT administrators and software developers familiar with Python. Although readers may have some knowledge of cryptography, the book assumes that the reader is starting from scratch.

Secure Programming Cookbook for C and C++ - John Viega
2003-07-14

Password sniffing, spoofing, buffer overflows, and denial of service: these are only a few of the attacks on today's computer systems and networks. At the root of this epidemic is poorly written, poorly tested, and insecure code that puts everyone at risk. Clearly, today's developers need help figuring out how to write code that attackers won't be able to exploit. But writing such code is surprisingly difficult. *Secure Programming Cookbook for C and C++* is an important new resource for developers serious about writing secure code. It contains a wealth of solutions to problems faced by those who care about the security of their applications. It covers a wide range of topics, including safe initialization, access control, input validation, symmetric and public key cryptography, cryptographic hashes and MACs, authentication and key exchange, PKI, random numbers, and anti-tampering. The rich set of code samples provided in the book's more than 200 recipes will help programmers secure the C and C++ programs they write for both Unix® (including Linux®) and Windows® environments. Readers will learn: How to avoid common programming errors, such as buffer overflows, race conditions, and format string problems How to properly SSL-enable applications How to create secure channels for client-server communication without SSL How to integrate Public Key Infrastructure (PKI) into applications Best practices for using cryptography properly Techniques and strategies for properly validating input to programs How to launch programs securely How to use file access mechanisms properly Techniques for protecting applications from reverse engineering The book's web site supplements the book by providing a place to post new recipes, including those written in additional languages like Perl, Java, and Python. Monthly prizes will reward the best recipes submitted by readers. *Secure Programming Cookbook for C and C++* is destined to become an essential part of any developer's library, a code companion developers will turn to again and again as they seek to protect their systems from attackers and reduce the risks they face in today's dangerous world.

Hacking Exposed Wireless - Johnny Cache 2007-04-10

Secure Your Wireless Networks the Hacking Exposed Way Defend against the latest pervasive and devastating wireless attacks using the tactical security information contained in this comprehensive volume. *Hacking Exposed Wireless* reveals how hackers zero in on susceptible networks and peripherals, gain access, and execute debilitating attacks. Find out how to plug security holes in Wi-Fi/802.11 and Bluetooth systems and devices. You'll also learn how to launch wireless exploits from Metasploit, employ bulletproof authentication and encryption, and sidestep insecure wireless hotspots. The book includes vital details on new, previously unpublished attacks alongside real-world countermeasures. Understand the concepts behind RF electronics, Wi-Fi/802.11, and Bluetooth Find out how hackers use NetStumbler, WiSPY, Kismet, KisMAC, and AiroPeek to target vulnerable wireless networks Defend against WEP key brute-force, aircrack, and traffic injection hacks Crack WEP at new speeds using Field Programmable Gate Arrays or your

spare PS3 CPU cycles Prevent rogue AP and certificate authentication attacks Perform packet injection from Linux Launch DoS attacks using device driver-independent tools Exploit wireless device drivers using the Metasploit 3.0 Framework Identify and avoid malicious hotspots Deploy WPA/802.11i authentication and encryption using PEAP, FreeRADIUS, and WPA pre-shared keys

SSL and TLS: Theory and Practice, Second Edition - Rolf Oppliger
2016-03-31

This completely revised and expanded second edition of *SSL and TLS: Theory and Practice* provides an overview and a comprehensive discussion of the Secure Sockets Layer (SSL), Transport Layer Security (TLS), and Datagram TLS (DTLS) protocols that are omnipresent in today's e-commerce and e-business applications and respective security solutions. It provides complete details on the theory and practice of the protocols, offering readers a solid understanding of their design principles and modes of operation. Updates to this edition include coverage of the recent attacks against the protocols, newly specified extensions and firewall traversal, as well as recent developments related to public key certificates and respective infrastructures. This book targets software developers, security professionals, consultants, protocol designers, and chief security officers who will gain insight and perspective on the many details of the SSL, TLS, and DTLS protocols, such as cipher suites, certificate management, and alert messages. The book also comprehensively discusses the advantages and disadvantages of the protocols compared to other Internet security protocols and provides the details necessary to correctly implement the protocols while saving time on the security practitioner's side.

High Performance Browser Networking - Ilya Grigorik 2013-09-11

How prepared are you to build fast and efficient web applications? This eloquent book provides what every web developer should know about the network, from fundamental limitations that affect performance to major innovations for building even more powerful browser applications—including HTTP 2.0 and XHR improvements, Server-Sent Events (SSE), WebSocket, and WebRTC. Author Ilya Grigorik, a web performance engineer at Google, demonstrates performance optimization best practices for TCP, UDP, and TLS protocols, and explains unique wireless and mobile network optimization requirements. You'll then dive into performance characteristics of technologies such as HTTP 2.0, client-side network scripting with XHR, real-time streaming with SSE and WebSocket, and P2P communication with WebRTC. Deliver superlative TCP, UDP, and TLS performance Speed up network performance over 3G/4G mobile networks Develop fast and energy-efficient mobile applications Address bottlenecks in HTTP 1.x and other browser protocols Plan for and deliver the best HTTP 2.0 performance Enable efficient real-time streaming in the browser Create efficient peer-to-peer videoconferencing and low-latency applications with real-time WebRTC transports

Web Security, Privacy & Commerce - Simson Garfinkel 2002

"*Web Security, Privacy & Commerce*" cuts through the hype and the front page stories. It tells readers what the real risks are and explains how to minimize them. Whether a casual (but concerned) Web surfer or a system administrator responsible for the security of a critical Web server, this book will tell users what they need to know.

Load Balancing Servers, Firewalls, and Caches - Chandra Kopparapu
2002-02-05

From an industry insider—a close look at high-performance, end-to-end switching solutions Load balancers are fast becoming an indispensable solution for handling the huge traffic demands of the Web. Their ability to solve a multitude of network and server bottlenecks in the Internet age ranges from dramatic improvements in server farm scalability to removing the firewall as a network bottleneck. This book provides a detailed, up-to-date, technical discussion of this fast-growing, multibillion dollar market, covering the full spectrum of topics—from server and firewall load balancing to transparent cache switching to global server load balancing. In the process, the author delivers insight into the way new technologies are deployed in network infrastructure and how they work. Written by an industry expert who hails from a leading Web switch vendor, this book will help network and server administrators improve the scalability, availability, manageability, and security of their servers, firewalls, caches, and Web sites.

Bulletproof SSL and TLS - Ivan Ristic 2013-10

Bulletproof SSL and TLS is a complete guide to using SSL and TLS encryption to deploy secure servers and web applications. Written by Ivan Ristic, the author of the popular SSL Labs web site, this book will teach you everything you need to know to protect your systems from

eavesdropping and impersonation attacks. In this book, you'll find just the right mix of theory, protocol detail, vulnerability and weakness information, and deployment advice to get your job done: - Comprehensive coverage of the ever-changing field of SSL/TLS and Internet PKI, with updates to the digital version - For IT security professionals, help to understand the risks - For system administrators, help to deploy systems securely - For developers, help to design and implement secure web applications - Practical and concise, with added depth when details are relevant - Introduction to cryptography and the latest TLS protocol version - Discussion of weaknesses at every level, covering implementation issues, HTTP and browser problems, and protocol vulnerabilities - Coverage of the latest attacks, such as BEAST, CRIME, BREACH, Lucky 13, RC4 biases, Triple Handshake Attack, and Heartbleed - Thorough deployment advice, including advanced technologies, such as Strict Transport Security, Content Security Policy, and pinning - Guide to using OpenSSL to generate keys and certificates and to create and run a private certification authority - Guide to using OpenSSL to test servers for vulnerabilities - Practical advice for secure server configuration using Apache httpd, IIS, Java, Nginx, Microsoft Windows, and Tomcat This book is available in paperback and a variety of digital formats without DRM.

Network Security Hacks - Andrew Lockhart 2004

Introduces more than one hundred effective ways to ensure security in a Linux, UNIX, or Windows network, covering both TCP/IP-based services and host-based security techniques, with examples of applied encryption, intrusion detections, and logging.

Cryptography for Developers - Tom St Denis 2006-12-01

The only guide for software developers who must learn and implement cryptography safely and cost effectively. *Cryptography for Developers* begins with a chapter that introduces the subject of cryptography to the reader. The second chapter discusses how to implement large integer arithmetic as required by RSA and ECC public key algorithms The subsequent chapters discuss the implementation of symmetric ciphers, one-way hashes, message authentication codes, combined authentication and encryption modes, public key cryptography and finally portable coding practices. Each chapter includes in-depth discussion on memory/size/speed performance trade-offs as well as what cryptographic problems are solved with the specific topics at hand. The author is the developer of the industry standard cryptographic suite of tools called LibTom A regular expert speaker at industry conferences and events on this development

Demystifying Cryptography with OpenSSL 3.0 - Alexei Khlebnikov 2022-10-26

Use OpenSSL to add security features to your application, including cryptographically strong symmetric and asymmetric encryption, digital signatures, SSL/TLS connectivity, and PKI handling Key Features Secure your applications against common network security threats using OpenSSL Get to grips with the latest version of OpenSSL, its new features, and advantages Learn about PKI, cryptography, certificate authorities, and more using real-world examples Book Description Security and networking are essential features of software today. The modern internet is full of worms, Trojan horses, men-in-the-middle, and other threats. This is why maintaining security is more important than ever. OpenSSL is one of the most widely used and essential open source projects on the internet for this purpose. If you are a software developer, system administrator, network security engineer, or DevOps specialist, you've probably stumbled upon this toolset in the past - but how do you make the most out of it? With the help of this book, you will learn the most important features of OpenSSL, and gain insight into its full potential. This book contains step-by-step explanations of essential cryptography and network security concepts, as well as practical examples illustrating the usage of those concepts. You'll start by learning the basics, such as how to perform symmetric encryption and calculate message digests. Next, you will discover more about cryptography: MAC and HMAC, public and private keys, and digital signatures. As you progress, you will explore best practices for using X.509 certificates, public key infrastructure, and TLS connections. By the end of this book, you'll be able to use the most popular features of OpenSSL, allowing you to implement cryptography and TLS in your applications and network infrastructure. What you will learn Understand how to use symmetric cryptography Get to grips with message digests, MAC, and HMAC Discover asymmetric cryptography and digital signatures Focus on how to apply and use X.509 certificates Dive into TLS and its proper usage Manage advanced and special usages of TLS Find out how to run a mini certificate authority for your organization Who this book is for This book

is for software developers, system administrators, DevOps specialists, network security engineers, and analysts, or anyone who wants to keep their applications and infrastructure secure. Software developers will learn how to use the OpenSSL library to empower their software with cryptography and TLS. DevOps professionals and sysadmins will learn how to work with cryptographic keys and certificates on the command line, and how to set up a mini-CA for their organization. A basic understanding of security and networking is required.

ASN.1 Complete - John Larmouth 2000

ASN.1 Complete teaches you everything you need to know about ASN.1- whether you're specifying a new protocol or implementing an existing one in a software or hardware development project. Inside, the author begins with an overview of ASN.1's most commonly encountered features, detailing and illustrating standard techniques for using them. He then goes on to apply the same practice-oriented approach to all of the notation's other features, providing you with an easy-to-navigate, truly comprehensive tutorial. The book also includes thorough documentation of both the Basic and the Packed Encoding Rules- indispensable coverage for anyone doing hand-encoding, and a valuable resource for anyone wanting a deeper understanding of how ASN.1 and ASN.1 tools work. The concluding section takes up the history of ASN.1, in terms of both the evolution of the notation itself and the role it has played in hundreds of protocols and thousands of applications developed since its inception. Features Covers all the features-common and not so common-available to you when writing a protocol specification using ASN.1. Teaches you to read, understand, and implement a specification written using ASN.1. Explains how ASN.1 tools work and how to use them. Contains hundreds of detailed examples, all verified using OSS's ASN.1 Tools package. Considers ASN.1 in relation to other protocol specification standards.

Embedded Systems Security - David Kleidermacher 2012-03-16

Front Cover; Dedication; Embedded Systems Security: Practical Methods for Safe and Secure Software and Systems Development; Copyright; Contents; Foreword; Preface; About this Book; Audience; Organization; Approach; Acknowledgements; Chapter 1 -- Introduction to Embedded Systems Security; 1.1What is Security?; 1.2What is an Embedded System?; 1.3Embedded Security Trends; 1.4Security Policies; 1.5Security Threats; 1.6Wrap-up; 1.7Key Points; 1.8 Bibliography and Notes; Chapter 2 -- Systems Software Considerations; 2.1The Role of the Operating System; 2.2Multiple Independent Levels of Security.

SSH, The Secure Shell - Daniel J. Barrett 2005-05-10

Are you serious about network security? Then check out SSH, the Secure Shell, which provides key-based authentication and transparent encryption for your network connections. It's reliable, robust, and reasonably easy to use, and both free and commercial implementations are widely available for most operating systems. While it doesn't solve every privacy and security problem, SSH eliminates several of them very effectively. Everything you want to know about SSH is in our second edition of SSH, *The Secure Shell: The Definitive Guide*. This updated book thoroughly covers the latest SSH-2 protocol for system administrators and end users interested in using this increasingly popular TCP/IP-based solution. How does it work? Whenever data is sent to the network, SSH automatically encrypts it. When data reaches its intended recipient, SSH decrypts it. The result is "transparent" encryption-users can work normally, unaware that their communications are already encrypted. SSH supports secure file transfer between computers, secure remote logins, and a unique "tunneling" capability that adds encryption to otherwise insecure network applications. With SSH, users can freely navigate the Internet, and system administrators can secure their networks or perform remote administration. Written for a wide, technical audience, *SSH, The Secure Shell: The Definitive Guide* covers several implementations of SSH for different operating systems and computing environments. Whether you're an individual running Linux machines at home, a corporate network administrator with thousands of users, or a PC/Mac owner who just wants a secure way to telnet or transfer files between machines, our indispensable guide has you covered. It starts with simple installation and use of SSH, and works its way to in-depth case studies on large, sensitive computer networks. No matter where or how you're shipping information, *SSH, The Secure Shell: The Definitive Guide* will show you how to do it securely.

Network Security Essentials: Applications and Standards, 4/e - William Stallings 2003

Building Open Source Network Security Tools - Mike Schiffman 2002-12-03

Learn how to protect your network with this guide to building complete and fully functional network security tools. Although open source network security tools come in all shapes and sizes, a company will eventually discover that these tools are lacking in some area—whether it's additional functionality, a specific feature, or a narrower scope. Written by security expert Mike Schiffman, this comprehensive book will show you how to build your own network security tools that meet the needs of your company. To accomplish this, you'll first learn about the Network Security Tool Paradigm in addition to currently available components including libpcap, libnet, libnids, libsf, libdnet, and OpenSSL. Schiffman offers a detailed discussion of these components, helping you gain a better understanding of the native datatypes and exported functions. Next, you'll find several key techniques that are built from the components as well as easy-to-parse programming examples. The book then ties the model, code, and concepts together, explaining how you can use this information to craft intricate and robust security programs. Schiffman provides you with cost-effective, time-saving guidance on how to build customized network security tools using existing components. He explores: A multilayered model for describing network security tools The ins and outs of several specific security-related components How to combine these components into several useful network security techniques Four different classifications for network security tools: passive reconnaissance, active reconnaissance, attack and penetration, and defensive How to combine techniques to build customized network security tools The companion Web site contains all of the code from the book.

Network Security with OpenSSL - John Viega 2002-06-17

Most applications these days are at least somewhat network aware, but how do you protect those applications against common network security threats? Many developers are turning to OpenSSL, an open source version of SSL/TLS, which is the most widely used protocol for secure network communications. The OpenSSL library is seeing widespread adoption for web sites that require cryptographic functions to protect a broad range of sensitive information, such as credit card numbers and other financial transactions. The library is the only free, full-featured SSL implementation for C and C++, and it can be used programmatically or from the command line to secure most TCP-based network protocols. Network Security with OpenSSL enables developers to use this protocol much more effectively. Traditionally, getting something simple done in OpenSSL could easily take weeks. This concise book gives you the guidance you need to avoid pitfalls, while allowing you to take advantage of the library's advanced features. And, instead of bogging you down in the technical details of how SSL works under the hood, this book provides only the information that is necessary to use OpenSSL safely and effectively. In step-by-step fashion, the book details the challenges in securing network communications, and shows you how to use OpenSSL tools to best meet those challenges. As a system or network administrator, you will benefit from the thorough treatment of the OpenSSL command-line interface, as well as from step-by-step directions for obtaining certificates and setting up your own certification authority. As a developer, you will further benefit from the in-depth discussions and examples of how to use OpenSSL in your own programs. Although OpenSSL is written in C, information on how to use OpenSSL with Perl, Python and PHP is also included. OpenSSL may well answer your need to protect sensitive data. If that's the case, Network Security with OpenSSL is the only guide available on the subject.

Financial Cryptography and Data Security - George Danezis 2012-01-16

This book constitutes the thoroughly refereed post-conference proceedings of the 15th International Conference on Financial Cryptography and Data Security, FC 2011, held in Gros Islet, St. Lucia, in February/March 2011. The 16 revised full papers and 10 revised short papers presented were carefully reviewed and selected from 65 initial submissions. The papers cover all aspects of securing transactions and systems and feature current research focusing on fundamental and applied real-world deployments on all aspects surrounding commerce security; as well as on systems security and inter-disciplinary efforts.

Network Security Assessment - Chris McNab 2007-11

How secure is your network? The best way to find out is to attack it. Network Security Assessment provides you with the tricks and tools professional security consultants use to identify and assess risks in Internet-based networks—the same penetration testing model they use to secure government, military, and commercial networks. With this book, you can adopt, refine, and reuse this testing model to design and deploy networks that are hardened and immune from attack. Network Security

Assessment demonstrates how a determined attacker scours Internet-based networks in search of vulnerable components, from the network to the application level. This new edition is up-to-date on the latest hacking techniques, but rather than focus on individual issues, it looks at the bigger picture by grouping and analyzing threats at a high-level. By grouping threats in this way, you learn to create defensive strategies against entire attack categories, providing protection now and into the future. Network Security Assessment helps you assess: Web services, including Microsoft IIS, Apache, Tomcat, and subsystems such as OpenSSL, Microsoft FrontPage, and Outlook Web Access (OWA) Web application technologies, including ASP, JSP, PHP, middleware, and backend databases such as MySQL, Oracle, and Microsoft SQL Server Microsoft Windows networking components, including RPC, NetBIOS, and CIFS services SMTP, POP3, and IMAP email services IP services that provide secure inbound network access, including IPsec, Microsoft PPTP, and SSL VPNs Unix RPC services on Linux, Solaris, IRIX, and other platforms Various types of application-level vulnerabilities that hacker tools and scripts exploit Assessment is the first step any organization should take to start managing information risks correctly. With techniques to identify and assess risks in line with CESG CHECK and NSA IAM government standards, Network Security Assessment gives you a precise method to do just that.

Network Security Assessment - Chris McNab 2004

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

Linux Unwired - Roger Weeks 2004

Provides information on the basics of wireless computing and the technologies that are supported by Linux.

Web Penetration Testing with Kali Linux - Gilberto Najera-Gutierrez 2018-02-28

Build your defense against web attacks with Kali Linux, including command injection flaws, crypto implementation layers, and web application security holes. Key Features Know how to set up your lab with Kali Linux Discover the core concepts of web penetration testing Get the tools and techniques you need with Kali Linux Book Description Web Penetration Testing with Kali Linux - Third Edition shows you how to set up a lab, helps you understand the nature and mechanics of attacking websites, and explains classical attacks in great depth. This edition is heavily updated for the latest Kali Linux changes and the most recent attacks. Kali Linux shines when it comes to client-side attacks and fuzzing in particular. From the start of the book, you'll be given a thorough grounding in the concepts of hacking and penetration testing, and you'll see the tools used in Kali Linux that relate to web application hacking. You'll gain a deep understanding of classical SQL, command-injection flaws, and the many ways to exploit these flaws. Web penetration testing also needs a general overview of client-side attacks, which is rounded out by a long discussion of scripting and input validation flaws. There is also an important chapter on cryptographic implementation flaws, where we discuss the most recent problems with cryptographic layers in the networking stack. The importance of these attacks cannot be overstated, and defending against them is relevant to most internet users and, of course, penetration testers. At the end of the book, you'll use an automated technique called fuzzing to identify flaws in a web application. Finally, you'll gain an understanding of web application vulnerabilities and the ways they can be exploited using the tools in Kali Linux. What you will learn Learn how to set up your lab with Kali Linux Understand the core concepts of web penetration testing Get to know the tools and techniques you need to use with Kali Linux Identify the difference between hacking a web application and network hacking Expose vulnerabilities present in web servers and their applications using server-side attacks Understand the different techniques used to identify the flavor of web applications See standard attacks such as exploiting cross-site request forgery and cross-site scripting flaws Get an overview of the art of client-side attacks Explore automated attacks such as fuzzing web applications Who this book is for Since this book sets out to cover a large number of tools and security fields, it can work as an introduction to practical security skills for beginners in security. In addition, web programmers and also system administrators would benefit from this rigorous introduction to web penetration testing. Basic system administration skills are necessary, and the ability to read code is a must.

Android Security Internals - Nikolay Elenkov 2014-10-14

There are more than one billion Android devices in use today, each one a potential target. Unfortunately, many fundamental Android security features have been little more than a black box to all but the most elite security professionals—until now. In *Android Security Internals*, top Android security expert Nikolay Elenkov takes us under the hood of the Android security system. Elenkov describes Android security architecture from the bottom up, delving into the implementation of major security-related components and subsystems, like Binder IPC, permissions, cryptographic providers, and device administration. You'll learn: -How Android permissions are declared, used, and enforced -How Android manages application packages and employs code signing to verify their authenticity -How Android implements the Java Cryptography Architecture (JCA) and Java Secure Socket Extension (JSSE) frameworks -About Android's credential storage system and APIs, which let applications store cryptographic keys securely -About the online account management framework and how Google accounts integrate with Android -About the implementation of verified boot, disk encryption, lockscreen, and other device security features -How Android's bootloader and recovery OS are used to perform full system updates, and how to obtain root access With its unprecedented level of depth and detail, *Android Security Internals* is a must-have for any security-minded Android developer.

Linux for Networking Professionals - Rob VandenBrink 2021-11-11

Get to grips with the most common as well as complex Linux networking configurations, tools, and services to enhance your professional skills
Key Features Learn how to solve critical networking problems using real-world examples Configure common networking services step by step in an enterprise environment Discover how to build infrastructure with an eye toward defense against common attacks
Book Description As Linux continues to gain prominence, there has been a rise in network services being deployed on Linux for cost and flexibility reasons. If you are a networking professional or an infrastructure engineer involved with networks, extensive knowledge of Linux networking is a must. This book will guide you in building a strong foundation of Linux networking concepts. The book begins by covering various major distributions, how to pick the right distro, and basic Linux network configurations. You'll then move on to Linux network diagnostics, setting up a Linux firewall, and using Linux as a host for network services. You'll discover a wide range of network services, why they're important, and how to configure them in an enterprise environment. Finally, as you work with the example builds in this Linux book, you'll learn to configure various services to defend against common attacks. As you advance to the final chapters, you'll be well on your way towards building the underpinnings for an all-Linux datacenter. By the end of this book, you'll be able to not only configure common Linux network services confidently, but also use tried-and-tested methodologies for future Linux installations. What you will learn
Use Linux as a troubleshooting and diagnostics platform
Explore Linux-based network services
Configure a Linux firewall and set it up for network services
Deploy and configure Domain Name System (DNS) and Dynamic Host Configuration Protocol (DHCP) services securely
Configure Linux for load balancing, authentication, and authorization services
Use Linux as a logging platform for network monitoring
Deploy and configure Intrusion Prevention Services (IPS)
Set up Honeypot solutions to detect and foil attacks
Who this book is for This book is for IT and Windows professionals and admins looking for guidance in managing Linux-based networks. Basic knowledge of networking is necessary to get started with this book.

Secure Coding in C and C++ - Robert C. Seacord 2005-09-09

"The security of information systems has not improved at a rate consistent with the growth and sophistication of the attacks being made against them. To address this problem, we must improve the underlying strategies and techniques used to create our systems. Specifically, we must build security in from the start, rather than append it as an afterthought. That's the point of *Secure Coding in C and C++*. In careful detail, this book shows software developers how to build high-quality systems that are less vulnerable to costly and even catastrophic attack. It's a book that every developer should read before the start of any serious project." --Frank Abagnale, author, lecturer, and leading consultant on fraud prevention and secure documents
Learn the Root Causes of Software Vulnerabilities and How to Avoid Them Commonly exploited software vulnerabilities are usually caused by avoidable software defects. Having analyzed nearly 18,000 vulnerability reports over the past ten years, the CERT/Coordination Center (CERT/CC) has determined that a relatively small number of root causes account for most of them. This book identifies and explains these causes and shows the steps that can be taken to prevent exploitation. Moreover, this book encourages programmers to adopt security best practices and develop a security mindset that can help protect software from tomorrow's attacks, not just today's. Drawing on the CERT/CC's reports and conclusions, Robert Seacord systematically identifies the program errors most likely to lead to security breaches, shows how they can be exploited, reviews the potential consequences, and presents secure alternatives. Coverage includes technical detail on how to Improve the overall security of any C/C++ application Thwart buffer overflows and stack-smashing attacks that exploit insecure string manipulation logic Avoid vulnerabilities and security flaws resulting from the incorrect use of dynamic memory management functions Eliminate integer-related problems: integer overflows, sign errors, and truncation errors Correctly use formatted output functions without introducing format-string vulnerabilities Avoid I/O vulnerabilities, including race conditions
Secure Coding in C and C++ presents hundreds of examples of secure code, insecure code, and exploits, implemented for Windows and Linux. If you're responsible for creating secure C or C++ software--or for keeping it safe--no other book offers you this much detailed, expert assistance.

Implementing SSL / TLS Using Cryptography and PKI - Joshua Davies 2011-01-07

Hands-on, practical guide to implementing SSL and TLS protocols for Internet security If you are a network professional who knows C programming, this practical book is for you. Focused on how to implement Secure Socket Layer (SSL) and Transport Layer Security (TLS), this book guides you through all necessary steps, whether or not you have a working knowledge of cryptography. The book covers SSLv2, TLS 1.0, and TLS 1.2, including implementations of the relevant cryptographic protocols, secure hashing, certificate parsing, certificate generation, and more. Coverage includes: Understanding Internet Security Protecting against Eavesdroppers with Symmetric Cryptography Secure Key Exchange over an Insecure Medium with Public Key Cryptography Authenticating Communications Using Digital Signatures Creating a Network of Trust Using X.509 Certificates A Usable, Secure Communications Protocol: Client-Side TLS Adding Server-Side TLS 1.0 Support Advanced SSL Topics Adding TLS 1.2 Support to Your TLS Library Other Applications of SSL A Binary Representation of Integers: A Primer Installing TCPDump and OpenSSL Understanding the Pitfalls of SSLv2 Set up and launch a working implementation of SSL with this practical guide.