Sec506 Securing Linux Unix Sans

Geekonomics
Hackers Beware
A Hands-on Introduction
Ethical Hacking
Red Hat RHCE 8 (EX294) Cert Guide
Understanding Cybercrime
Cybersecurity: The Hacker Proof Guide To Cybersecurity, Internet Safety, Cybercrime, & Preventing Attacks
Offensive Countermeasures
Counter Hack Reloaded
Malware
Cybercrime, Organized Crime, and Societal Responses
Network Intrusion Detection
Right and Wrong for IT Professionals
Hacker Techniques, Tools, and Incident Handling
Moving From Zero to Hero
Securing HP NonStop Servers in an Open Systems World
Deep Learning with Python
Criminal Justice Resource Manual
Cyber crime strategy
Digital Crime and Forensic Science in Cyberspace
Law in Cyber Space
Protecting Mobile Devices and their Applications
The Real Cost of Insecure Software
Hands on Hacking
TCP/IP, OSS and SQL
Foundations, Technologies and Applications
Techniques of Crime Scene Investigation
A Beginners Guide to Learning the World of Ethical Hacking
Crime in the Digital Sublime
Fifth Edition
Learning by Practicing - Mastering TShark Network Forensics
Defending Free speech in the Digital Age
Virtualization Security
Cybersecurity Operations Handbook
International Approaches
Incident Response & Computer Forensics, Third Edition
The No-nonsense Guide
Phenomena, Challenges and Legal Response
Fighting Malicious Code

HALLIE SAVAGE

Geekonomics West Academic
Securing virtual environments for VMware, Citrix, and Microsoft hypervisors Virtualization changes the playing field when it comes to security. There are new attack vectors, new operational patterns and complexity, and changes in IT architecture and deployment life cycles. What's more, the technologies, best practices, and strategies used for securing physical environments do not provide sufficient protection for virtual environments. This book includes step-by-step configurations for the security controls that come with the three leading hypervisor--VMware vSphere and ESXi, Microsoft Hyper-V on Windows Server 2008, and Citrix XenServer. Includes strategy for securely implementing network policies and integrating virtual networks into the existing physical infrastructure Discusses vSphere and Hyper-V native virtual switches as well as the Cisco Nexus 1000v and Open vSwitch switches Offers effective practices for securing virtual machines without creating additional operational overhead for administrators Contains methods for integrating virtualization into existing workflows and creating new policies and processes for change and configuration management so that virtualization can help make these critical operations processes more effective This must-have resource offers tips and tricks for improving disaster recovery and business continuity, security-specific scripts, and examples of how Virtual Desktop Infrastructure benefits security.
Hackers Beware Trust Genics
The Government published the UK Cyber Security Strategy in June 2009 (Cm. 7642, ISBN 97801017674223), and established the Office of Cyber Security to provide strategic leadership across Government. This document sets out the Home Office's approach to tackling cyber crime, showing how to tackle such crimes directly through the provision of a law enforcement response, and indirectly through cross-Government working and through the development of relationships with industry, charities and other groups, as well as internationally. The publication is divided into five chapters and looks at the following areas, including: the broader cyber security context; cyber crime: the current position; the Government response and how the Home Office will tackle cyber crime.
A Hands-on Introduction Createspace Independent Publishing Platform
The definitive guide to incident response--updated for the first time in a decade! Thoroughly revised to cover the latest and most effective tools and techniques, Incident Response & Computer Forensics, Third Edition arms you with the information you need to get your organization out of trouble when data breaches occur. This practical resource covers the entire lifecycle of incident response, including preparation, data collection, data analysis, and remediation. Real-world case studies reveal the methods behind--and remediation strategies for--today's most insidious attacks. Architect an infrastructure that allows for methodical investigation and remediation Develop leads, identify indicators of compromise, and determine incident scope Collect and preserve live data Perform forensic duplication Analyze data from networks, enterprise services, and applications Investigate Windows and Mac OS X systems Perform malware triage Write detailed incident response reports Create and implement comprehensive remediation plans

Ethical Hacking IGI Global
A fast, hands-on introduction to offensive hacking techniques Hands-On Hacking teaches readers to see through the eyes of their adversary and apply hacking techniques to better understand real-world risks to computer networks and data. Readers will benefit from the author's years of experience in the field hacking into computer networks and ultimately training others in the art of cyber-attacks. This book holds no punches and explains the tools, tactics and procedures used by ethical hackers and criminal crackers alike. We will take you on a journey through a hacker's perspective when focused on the computer infrastructure of a target company, exploring how to access the servers and data. Once the information gathering stage is complete, you'll look for flaws and their known exploits—including tools developed by real-world government financed state-actors. • An introduction to the same hacking techniques that malicious hackers will use against an organization • Written by infosec experts with proven history of publishing vulnerabilities and highlighting security flaws • Based on the tried and tested material used to train hackers all over the world in the art of breaching networks • Covers the fundamental basics of how computer networks are inherently vulnerable to attack, teaching the student how to apply hacking skills to uncover vulnerabilities We cover topics of breaching a company from the external network perimeter, hacking internal enterprise systems and web application vulnerabilities. Delving into the basics of exploitation with real-world practical examples, you won't find any hypothetical academic only attacks here. From start to finish this book will take the student through the steps necessary to breach an organization to improve its security. Written by world-renowned cybersecurity experts and educators, Hands-On Hacking teaches entry-level professionals seeking to learn ethical hacking techniques. If you are looking to understand penetration testing and ethical hacking, this book takes you from basic methods to advanced techniques in a structured learning format.
Red Hat RHCE 8 (EX294) Cert Guide Commonwealth Secretariat
Humanists are sometimes accused of being so focused on the human race that they ignore the environment and other species. This book is designed to address these criticisms. The contributors, all humanists in the naturalistic tradition, show that in fact humanism as a worldview has much to offer environmentalism. Since humanists are committed to working for a global community in which all humans can flourish, they are as concerned about ecological degradation as environmentalists. But in regard to what should be done about environmental problems, humanists do not hesitate to use the best scientific information and technology to reclaim the natural world while ensuring the welfare of all human beings. Humanists stress that science and technology must be used responsibly and that human beings must learn to give up destructive ideological fantasies, whether political or religious. The contributors are Vern L. Bullough, Gwen Whitehead Brewer, Richard Gilbert, Michael J. Kami, Gerald Larue, Timothy J. Madigan, Sarah Oelberg, Don Page, Howard B. Radest, Philip J. Regal, Andreas Rosenberg, Harvey Sarles, David Schafer, John M. Swomley, Robert B. Tapp, Michael Werner, and Carol Wintermute.
Digital Crime and Forensic Science in Cyberspace
The book you have been waiting for to make you a Master of TShark Network Forensics, is finally here!!! Be it you are a Network Engineer, a Network Forensics Analyst, someone new to packet analysis or someone who occasionally looks at packet, this book is guaranteed to improve your TShark knowledge. It is your one-stop shop for all you need to master TShark, with adequate references to allow you to go deeper on peripheral topics if you so choose. Book Objectives: Introduce packet capturing architecture Teach the basics of TShark Teach some not so basic TShark tricks Solve real world challenges with TShark Identify services hiding behind other protocols Perform "hands-free" packet capture with TShark Analyze and decrypt TLS encrypted traffic Analyze and decrypt WPA2 Personal Traffic Going way beyond - Leveraging TShark and Python for IP threat intelligence Introduce Lua scripts Introduce packet editing Introduce packet merging Introduce packet rewriting Introduce remote packet capturing Who is this book for?While this book is written specifically for Network Forensics Analysts, it is equally beneficial to anyone who supports the network infrastructure. This means, Network Administrators, Security Specialists, Network Engineers, etc., will all benefit from this book. Considering the preceding, I believe the following represents the right audience for this book: Individuals starting off their Cybersecurity careers Individuals working in a Cyber/Security Operations Center (C/SOC) General practitioners of Cybersecurity Experienced Cybersecurity Ninjas who may be looking for a trick or two Anyone who just wishes to learn more about TShark and its uses in network forensics Anyone involved in network forensics More importantly, anyhow who is looking for a good read Not sure if this book is for you? Take a glimpse at the sample chapter before committing to it. Mastering TShark sample chapters can be found at: https: //bit.ly/TShark All PCAPS used within this book can be found at: https: //github.com/SecurityNik/SUWtHEh- As an addition to this book, the tool, pktIntel: Tool used to perform threat intelligence against packet data can be found at: https: //github.com/SecurityNik/pktIntel
Understanding Cybercrime MIT Press
This timely book provides contributions on international, comparative crime phenomena: gangs, trafficking, fear of crime, and crime prevention. It highlights contributions originally prepared for the XVII World Congress of Criminology and for the 2015 Cybercrime Conference in Oñati, Spain which have been selected, reviewed, and adapted for inclusion in this volume. The work features international contributors sharing the latest research and approaches from a variety of global regions. The first part examines the impact of gangs on criminal activities and violence. The second part explores illegal trafficking of people, drugs, and other illicit goods as a global phenomenon, aided by the ease of international travel, funds transfer, and communication. Finally, international approaches to crime detection prevention are presented. The work provides case studies and fieldwork that will be relevant across a variety of disciplines and a rich resource for future research. This work is relevant for researchers in criminology and criminal justice, as well as related fields such as international and comparative law, public policy, and public health.
Cybersecurity: The Hacker Proof Guide To Cybersecurity, Internet Safety, Cybercrime, & Preventing Attacks Jones & Bartlett Learning
The DISASTER RECOVERY/VIRTUALIZATION SECURITY SERIES is comprised of two books that are designed to fortify disaster recovery preparation and virtualization technology knowledge of information security students, system administrators, systems engineers, enterprise system architects, and any IT professional who is concerned about the integrity of their network infrastructure. Topics include disaster recovery planning, risk control policies and countermeasures, disaster recovery tools and services, and virtualization principles. The series when used in its entirety helps prepare readers to take and succeed on the E|CDR and E|CVT, Disaster Recovery and Virtualization Technology certification exam from EC-Council. The EC-Council Certified Disaster Recovery and Virtualization Technology professional will have a better understanding of how to set up disaster recovery plans using traditional and virtual technologies to ensure business continuity in the event of a disaster. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.
Offensive Countermeasures McGraw Hill Professional
A first-person account of the fight to preserve First Amendment rights in the digital age. Lawyer and writer Mike Godwin has been at the forefront of the struggle to preserve freedom of speech on the Internet. In Cyber Rights he recounts the major cases and issues in which he was involved and offers his views on free speech and other constitutional rights in the digital age. Godwin shows how the law and the Constitution apply, or should apply, in cyberspace and defends the Net against those who would damage it for their own purposes. Godwin details events and phenomena that have shaped our understanding of rights in cyberspace—including early antihacker fears that colored law enforcement activities in the early 1990s, the struggle between the Church of Scientology and its critics on the Net, disputes about protecting copyrighted works on the Net, and what he calls "the great cyberporn panic." That panic, he shows, laid bare the plans of those hoping to use our children in an effort to impose a new censorship regime on what otherwise could be the most liberating communications medium the world has seen. Most important, Godwin shows how anyone—not just lawyers, journalists, policy makers, and the rich and well connected—can use the Net to hold media and political institutions accountable and to ensure that the truth is known.
Counter Hack Reloaded Apress
Red Hat RHCE(TM) 8 Cert Guide is designed to help you pass the newest version of the Hat Certified Engineer exam for Red Hat Enterprise Linux 8, and master the skills you need to automate Linux and execute common system administration tasks with Red Hat(R) Ansible(R) Engine. The most comprehensive and time-efficient RHCE 8 prep guide available, it's also an extraordinarily cost-effective complement to other training, including the author's own RHCE Complete Video Course. Authored by a leading Red Hat trainer, consultant, and speaker, it presents focused, straight-to-the-point coverage of every exam topic, including: Performing Core Red Hat system administration tasks Understanding Ansible core components Installing and configuring Ansible control nodes Configuring Ansible managed nodes Administering scripts Performing system administration tasks with Ansible modules Working with roles Using advanced Ansible features such as templates and Ansible Vault From start to finish, this guide is organized to help you focus your study time where you need the most help, so you can retain more, and earn higher scores. It offers: Step-by-step chapter labs to help you practice what you've just learned Pre-exam theoretical exam to help you decide if you're ready for the real exam Two realistic RHCE sample exams delivered through Pearson's state-of-the-art test engine Pre-chapter "Do I Know This Already" (DIKTA) quizzes to assess your knowledge of each chapter's content, so you can decide how much time to spend on each section Foundation Topics sections thoroughly explaining concepts and theory, and linking them to real-world configurations and commands Key Topics icons flagging every figure, table, or list you absolutely must understand and remember End of chapter Glossary terms Chapter-ending Exam Preparation sections delivering even more exercises and troubleshooting scenarios
Malware McGraw Hill Professional
LIMITED TIME OFFER: Hacking eBook: $4.99 NOW $2.99! Hacking Paperback: $23.23 NOW $13.23! Learn How To Become An Ethical Hacker In Only 12 Hours... What if you could learn how to stop attackers from hacking into your website or personal accounts. Imagine finding leaks inside large corporate companies and you can help them protecting their data [and make money]. What if you had access to everything on the internet by leveraging your superior hacking skills? Sounds good? This is just a fraction of what you could do with Ethical Hacking in Kali Linux and we would love to show you how in just 12 Hours! Bullsh*t you say? Here at Cyberpunk University, we believe that we have the ability to learn Ethical Hacking to anybody within 12 hours. We know how quite tricky it is to learn and be a master of any programming language or skill. Our team is comprised of professionals who have been in the industry of information technology for decades and our experience made us able to create information products such as this step-by-step guide. We took out all the NONSENSE and tell you what to do, and more important, HOW TO DO IT! What will you find in this book: -How to setup your new hacking environment -How to use the Linux Terminal and master it's functions -How to be completely Anonymous online like the Pro's -How to setup NMAP -Which tools the REAL hackers use to crack passwords -How you can use multiple tools to gather information with Wireless Hacking -BONUS: The FREE Hacking: The No-Nonsense Pro Tips Infographic containing "The Newbie Hacking Index" & "Security Tools The Pro's Use In Kali Linux." Buy This Book NOW To Learn How To Be An Ethical Hacker in Only 12 Hours! Pick up your copy today by clicking the BUY NOW button at the top of this page!
Cybercrime, Organized Crime, and Societal Responses CRC Press
Secure today's mobile devices and applications Implement a systematic approach to security in your mobile application development with help from this practical guide. Featuring case studies, code examples, and best practices, Mobile Application Security details how to protect against vulnerabilities in the latest smartphone and PDA platforms. Maximize isolation, lockdown internal and removable storage, work with sandboxing and signing, and encrypt sensitive user information. Safeguards against viruses, worms, malware, and buffer overflow exploits are also covered in this comprehensive resource. Design highly isolated, secure, and authenticated mobile applications Use the Google Android emulator, debugger, and third-party security tools Configure Apple iPhone APIs to prevent overflow and SQL injection attacks Employ private and public key cryptography on Windows Mobile devices Enforce fine-grained security policies using the BlackBerry Enterprise Server Plug holes in Java Mobile Edition, SymbianOS, and WebOS applications Test for XSS, CSRF, HTTP redirects, and phishing attacks on WAP/Mobile HTML applications Identify and eliminate threats from Bluetooth, SMS, and GPS services Himanshu Dwivedi is a co-founder of iSEC Partners (www.isecpartners.com), an information security firm specializing in application security. Chris Clark is a principal security consultant with iSEC Partners. David Thiel is a principal security consultant with iSEC Partners.
Network Intrusion Detection John Wiley & Sons
Discover the practical aspects of implementing deep-learning solutions using the rich Python ecosystem. This book bridges the gap between the

academic state-of-the-art and the industry state-of-the-practice by introducing you to deep learning frameworks such as Keras, Theano, and Caffe. The practicalities of these frameworks is often acquired by practitioners by reading source code, manuals, and posting questions on community forums, which tends to be a slow and a painful process. Deep Learning with Python allows you to ramp up to such practical know-how in a short period of time and focus more on the domain, models, and algorithms. This book briefly covers the mathematical prerequisites and fundamentals of deep learning, making this book a good starting point for software developers who want to get started in deep learning. A brief survey of deep learning architectures is also included. Deep Learning with Python also introduces you to key concepts of automatic differentiation and GPU computation which, while not central to deep learning, are critical when it comes to conducting large scale experiments. What You Will Learn Leverage deep learning frameworks in Python namely, Keras, Theano, and Caffe Gain the fundamentals of deep learning with mathematical prerequisites Discover the practical considerations of large scale experiments Take deep learning models to production Who This Book Is For Software developers who want to try out deep learning as a practical solution to a particular problem. Software developers in a data science team who want to take deep learning models developed by data scientists to production.

Right and Wrong for IT Professionals Sams Publishing

Cyber attacks are on the rise. The media constantly report about data breaches and increasingly sophisticated cybercrime. Even governments are affected. At the same time, it is obvious that technology alone cannot solve the problem. What can countries do? Which issues can be addressed by policies and legislation? How to draft a good law? The report assists countries in understanding what cybercrime is about, what the challenges are in fighting such crime and supports them in drafting policies and laws.

Hacker Techniques, Tools, and Incident Handling John Wiley & Sons

The second edition of Kerrs popular computer crimes text reflects the many new caselaw and statutory developments since the publication of the first edition in 2006. It also adds a new section on encryption that covers both Fourth Amendment and Fifth Amendment issues raised by its use to conceal criminal activity. Computer crime law will be an essential area for tomorrow's criminal law practitioners, and this book offers an engaging and user-friendly introduction to the field. It is part traditional casebook, part treatise: It both straightforwardly explains the law and presents many exciting and new questions of law that courts are only now beginning to consider. The book reflects the author's practice experience, as well: Orin Kerr was a computer crime prosecutor at the Justice Department for three years, and the book combines theoretical insights with practical tips for working with actual cases. No advanced knowledge of computers and the Internet is required or assumed This book covers every aspect of crime in the digital age. Topics range from Internet surveillance law and the Fourth Amendment to computer hacking laws and international computer crimes. More and more crimes involve digital evidence, and computer crime law will be an essential area for tomorrow's criminal law practitioners. Many U.S. Attorney's Offices have started computer crime units, as have many state Attorney General offices, and any student with a background in this emerging area of law will have a leg up on the competition. This is the first law school book dedicated entirely to computer crime law. The materials are authored entirely by Orin Kerr, a new star in the area of criminal law and Internet law who has recently published articles in the Harvard Law Review, Columbia Law Review, NYU Law Review, and Michigan Law Review. The book is filled with ideas for future scholarship, including hundreds of important questions that have never been addressed in the scholarly literature. The book reflects the author's practice experience, as well: Kerr was a computer crime prosecutor at the Justice Department for three years, and the book combines theoretical insights with practical tips for working with actual cases. Students will find it easy and fun to read, and professors will find it an angaging introduction to a new world of scholarly ideas. The book is ideally suited either for a 2-credit seminar or a 3-credit course, and should appeal both to criminal law professors and those interested in cyberlaw or law and technology. No advanced knowledge of computers and the Internet is required or assumed.

Moving From Zero to Hero The Stationery Office

Recent corporate events have exposed the frequency and consequences of poor system security implementations and inadequate protection of private information. In a world of increasingly complex computing environments, myriad compliance regulations and the soaring costs of security breaches, it is economically essential for companies to become proactive in implementing effective system and data security measures. This volume is a comprehensive reference for understanding security risks, mitigations and best practices as they apply to the various components of these business-critical computing environments. HP NonStop Servers are used by Financial, Medical, Manufacturing enterprises where there can be no down time. Securing HP NonStop Servers in an Open Systems World: OSS, TCP/IP, and SQL takes a wide angle view of NonStop Server use. This book addresses protection of the Open Systems Services environment, network interfaces including TCP/IP and standard SQL databases. It lays out a roadmap of changes since our first book HP has made to Safeguard, elaborating on the advantages and disadvantages of implementing each new version. Even the security aspects of managing Operating System upgrades are given attention. Auditors, security policy makers, information security administrators and system managers will find the practical information they need for putting security principles into practice to meet industry standards as well as compliance regulations. * Addresses security issues in Open Systems Services * Critical security topics for network interfaces TCP/IP, SQL, etc. * Updates to safeguard thru since publication of XYPRO's last book

Securing HP NonStop Servers in an Open Systems World Prentice Hall Professional

The reason as to why I decided to write this book is the fact that many of us lives with a belief that we have only four common domains in this world, which are land, sea, air and outer space. But currently due to the development of science and technology a fifth common domain has been created, and that is cyberspace. This new common domain creates a new environment for the commission of crimes known as cyber crimes. And because of its nature, it became difficult to deal with these natures of crimes. The widespread digital accessibility creates new opportunities for the unprincipled because the manners in which offenders commit crimes changed from traditional to digital means. A lot of currencies are lost by both businesses and consumers to computer-criminals. Fair enough, computers and networks can be used to harass victims or set them up for violent attacks such as to coordinate and carry out terrorist activities that threaten us all. Coming back to our country Tanzania, regrettably in many cases law enforcement institutions have insulated behind these criminals, deficient in the technology and the trained recruits to address this fresh and rising risk. To make things worse, old laws did not fairly prevent the crimes from being committed. Furthermore, new laws had not quite caught up to the reality of what was happening, and there were few court precedents to look to for guidance. It is from this book whereby the position of cyber security, prevention and detection in Tanzania against cyber crimes, is determined. Actually, by looking at the Cyber Crime Act No.14 of 2015 on how the concepts above have been provided and implemented. Magalla Jr.Note de l'éditeur (FRENCH):Cet essai juridique en anglais traite du droit des nouvelles technologies de l'information et de la communication (NTIC) en Tanzanie, en particulier de la cybercriminalité, de sa définition, de sa prévention et de sa répression en fonction des formes multiples qu'elle prend dans le cyber espace. Après avoir dépeint le cadre général et international du droit des NTIC, l'auteur va décrire la situation tanzanienne. L'approche se veut à la fois doctrinale et pratique. Les principales sources du droit des NTIC sont décrites et l'ouvrage se termine sur des cas pratiques rencontrés dans des tribunaux tanzaniens.

Deep Learning with Python Elsevier

Explains how and why hackers break into computers, steal information, and deny services to machines' legitimate users, and discusses strategies and tools used by hackers and how to defend against them.

Criminal Justice Resource Manual Psychology Press

This book is a training aid and reference for intrusion detection analysts. While the authors refer to research and theory, they focus their attention on providing practical information. New to this edition is coverage of packet dissection, IP datagram fields, forensics, and snort filters.

Cyber crime strategy CreateSpace

The comprehensive A-to-Z guide on network security, fully revised and updated Network security is constantly evolving, and this comprehensive guide has been thoroughly updated to cover the newest developments. If you are responsible for network security, this is the reference you need at your side. Covering new techniques, technology, and methods for approaching security, it also examines new trends and best practices being used by many organizations. The revised Network Security Bible complements the Cisco Academy course instruction in networking security. Covers all core areas of network security and how they interrelate Fully revised to address new techniques, technology, and methods for securing an enterprise worldwide Examines new trends and best practices in use by organizations to secure their enterprises Features additional chapters on areas related to data protection/correlation and forensics Includes cutting-edge topics such as integrated cybersecurity and sections on Security Landscape, with chapters on validating security, data protection, forensics, and attacks and threats If you need to get up to date or stay current on network security, Network Security Bible, 2nd Edition covers everything you need to know.

Related with Sec506 Securing Linux Unix Sans:
• Commercial Pesticide Applicator License Practice Test : click here