

## Aircap Wireless User Guide

*The Latest Linux Security Solutions This authoritative guide will help you secure your Linux network--whether you use Linux as a desktop OS, for Internet services, for telecommunications, or for wireless services. Completely rewritten the ISECOM way, Hacking Exposed Linux, Third Edition provides the most up-to-date coverage available from a large team of topic-focused experts. The book is based on the latest ISECOM security research and shows you, in full detail, how to lock out intruders and defend your Linux systems against catastrophic attacks. Secure Linux by using attacks and countermeasures from the latest OSSTMM research Follow attack techniques of PSTN, ISDN, and PSDN over Linux Harden VoIP, Bluetooth, RF, RFID, and IR devices on Linux Block Linux signal jamming, cloning, and eavesdropping attacks Apply Trusted Computing and cryptography tools for your best defense Fix vulnerabilities in DNS, SMTP, and Web 2.0 services Prevent SPAM, Trojan, phishing, DoS, and DDoS exploits Find and repair errors in C code with static analysis and Hoare Logic*

*This significantly revised and expanded edition discusses how to use Wireshark to capture raw network traffic, filter and analyze packets, and diagnose common network problems.*

*Provides information on ways to use Wireshark to capture and analyze packets, covering such topics as building customized capture and display filters, graphing traffic patterns, and building statistics and reports.*

*Leverage the power of Wireshark to troubleshoot your networking issues by using effective packet analysis techniques and performing improved protocol analysis About This Book Gain hands-on experience of troubleshooting errors in TCP/IP and SSL protocols through practical use cases Identify and overcome security flaws in your network to get a deeper insight into security analysis This is a fast-paced book that focuses on quick and effective packet captures through practical examples and exercises Who This Book Is For If you are a network or system administrator who wants to effectively capture packets, a security consultant who wants to audit packet flows, or a white hat hacker who wants to view sensitive information and remediate it, this book is for you. This book requires decoding skills and a basic understanding of networking. What You Will Learn Utilize Wireshark's advanced features to analyze packet captures Locate the vulnerabilities in an application server Get to know more about protocols such as DHCPv6, DHCP, DNS, SNMP, and HTTP with Wireshark Capture network packets with tcpdump and snoop with examples Find out about security aspects such as OS-level ARP scanning Set up 802.11 WLAN captures and discover more about the WAN protocol Enhance your troubleshooting skills by understanding practical TCP/IP handshake and state diagrams In Detail Wireshark provides a very useful way to decode an RFC and examine it. The packet*

*captures displayed in Wireshark give you an insight into the security and flaws of different protocols, which will help you perform the security research and protocol debugging. The book starts by introducing you to various packet analyzers and helping you find out which one best suits your needs. You will learn how to use the command line and the Wireshark GUI to capture packets by employing filters. Moving on, you will acquire knowledge about TCP/IP communication and its use cases. You will then get an understanding of the SSL/TLS flow with Wireshark and tackle the associated problems with it. Next, you will perform analysis on application-related protocols. We follow this with some best practices to analyze wireless traffic. By the end of the book, you will have developed the skills needed for you to identify packets for malicious attacks, intrusions, and other malware attacks. Style and approach This is an easy-to-follow guide packed with illustrations and equipped with lab exercises to help you reproduce scenarios using a sample program and command lines.*

*CEH Certified Ethical Hacker Bundle, Second Edition*

*CEH v9*

*Exam CWSP-205*

*Network+ Guide to Networks*

*A Hands-On Guide to Reliable Security Audits*

*CWDP Certified Wireless Design Professional Official Study Guide*

***Prepare with the only official study guide for the CWNA-106 The CWNA: Certified Wireless Network Administrator Official Study Guide: Exam CWNA-106 is the officially endorsed CWNA testprep for the leading wireless certification. Expert authors and CWNEs David D. Coleman and David A. Westcott guide readers through the skills and concepts candidates need to know for the exam, using hands-on methods to convey an in-depth understanding of wireless network administration. Readers should have a basic knowledge of Radio Frequency behavior, experience with WLAN hardware peripherals and protocols, and an interest in designing, installing, and managing wireless networks. Wireless technology is taking over the tech industry, and the demand for competent, certified professionals is far outpacing the supply. A CWNA certification denotes advanced-level proficiency in the field, with a complete understanding of wireless LAN components, features, and function—but the only way to pass the exam is to truly understand the material, not just the talking points. The CWNA: Certified Wireless Network Administrator Official Study Guide thoroughly covers each exam objective, and includes review questions, assessment tests, and exercises to test your skills. Topics include: Radio Frequency technologies, regulations, and standards 802.11 protocols Network implementation and security 802.11 RF site surveying Readers also get access to a suite of study tools including an electronic test engine with hundreds or practice test questions, electronic flashcards, exercise peripherals, and industry White Papers, which serve as valuable backup references. In preparing for the CWNA-106 exam, the ideal study guide should cover all of the exam topics in depth—CWNA: Certified Wireless Network Administrator Official Study Guide does just that, making it an excellent, comprehensive study guide.***

***How safe is your network? Intrusion Alert: an Ethical Hacking Guide to Intrusion Detection provides an in-depth look at the intrusion detection systems that are currently available to help protect your networks from cyber criminals. The book begins by explaining various security concepts and the basics of security attacks, and then goes on to provide an introduction intrusion detection systems (IDS), how these systems work, and principles of IDS and the IDS architecture. The second section of the book deals with the installation and configuration of various IDS tools including tcpdump, ISA Server 2004 and Snort. Readers learn to implement these products, understand essential administration and maintenance tasks, and fine tune and use the data they provide appropriately.***

***Thoroughly revised to cover all CEH v10 exam objectives, this bundle includes two books, online resources, and a bonus quick review guide This fully updated, money-saving self-study set prepares you for the CEH v10 exam. You can start by reading CEH Certified Ethical Hacker All-in-One Exam Guide, Fourth Edition to learn about every topic included in the v10 exam objectives. Next, you can reinforce what you've learned with the 650+ practice questions featured in CEH Certified Ethical Hacker Practice Exams, Fourth Edition. The CEH Certified Ethical Hacker Bundle, Fourth Edition also includes a bonus a quick review guide that can be used as the final piece for exam preparation. A bonus voucher code for four hours of lab time from Practice Labs, a virtual machine platform providing access to real hardware and software, can be combined with the two hours of lab time included with the All-in-One Exam Guide and provides the hands-on experience that's tested in the optional new CEH Practical exam. This edition features up-to-date coverage of all five phases of ethical hacking: reconnaissance, gaining access, enumeration, maintaining access, and covering tracks. •In all, the bundle includes more than 1,000 accurate questions with detailed answer explanations•Online content includes customizable practice exam software containing 600 practice questions in total and voucher codes for six free hours of lab time from Practice Labs•Bonus Quick Review Guide only available with this bundle•This bundle is 22% cheaper than buying the two books separately and includes exclusive online content***

***Hands-On Ethical Hacking and Network Defense, Second Edition provides an in-depth understanding of how to effectively protect computer networks. This book describes the tools and penetration testing methodologies used by ethical hackers and provides a thorough discussion of what and who an ethical hacker is and how important they are in protecting corporate and government data from cyber attacks. Readers are provided with updated computer security resources that describe new vulnerabilities and innovative methods to protect networks. Also included is a thorough update of federal and state computer crime laws, as well as changes in penalties for illegal computer hacking. With cyber-terrorism and corporate espionage threatening the fiber of our world, the need for trained network security professionals continues to grow. Hands-On Ethical Hacking and Network Defense, Second Edition provides a structured knowledge base to prepare readers to be security professionals who understand how to protect a network by using the skills and tools of an ethical hacker. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.***

***Kismet Hacking***

***A Practical Guide to Implementing 802. 11n and 802. 11ac Wireless Networks for Enterprise-Based Applications***

***An Ethical Hacking Guide to Intrusion Detection***

***CEH Certified Ethical Hacker All-in-One Exam Guide, Fourth Edition***

***Kali Linux Wireless Penetration Testing Cookbook***

***Certified Ethical Hacker Complete Training Guide with Practice Questions & Labs:***

**Complete CWNA–106 prep, with full coverage and hands–on practice CWNA Certified Wireless Network Administrator Deluxe Study Guide is your official study guide for the leading wireless certification program. Updated for the new CWNA–106 exam, this book provides coverage of all exam objectives, plus review questions and hands–on exercises that help you build your skills and your confidence before exam day. Start with a pre–assessment test to find out how much you already know, then fill in the gaps with detailed coverage of radio frequency technology, regulations and standards, protocols and devices, network implementation and security, RF site surveying, and much more. Sybex’s interactive online learning environment and test bank gives you access to hundreds of questions and robust study tools, including chapter tests, practice exams, flashcards, a glossary of key terms, and bonus chapter material all to help you prepare for and increase your chances of passing the exam the first time around. Find your starting point with a pre–assessment test Get up to speed on all CWNA–106 exam objectives Sharpen your practical skills with hands–on exercises Test your knowledge with practice exam questions Savvy candidates know that strategic prep is essential to first–time success, and CWNA Certified Wireless Network Administrator Deluxe Study Guide is your toolbox for building the next step in your wireless career.**

**Kismet is the industry standard for examining wireless network traffic, and is used by over 250,000 security professionals, wireless networking enthusiasts, and WarDriving hobbyists. Unlike other wireless networking books that have been published in recent years that geared towards Windows users, Kismet Hacking is geared to those individuals that use the Linux operating system. People who use Linux and want to use wireless tools need to use Kismet. Now with the introduction of Kismet NewCore, they have a book that will answer all their questions about using this great tool. This book continues in the successful vein of books for wireless users such as WarDriving: Drive, Detect Defend. \*Wardrive Running Kismet from the BackTrack Live CD \*Build and Integrate Drones with your Kismet Server \*Map Your Data with GPSMap, KisMap, WiGLE and GpsDrive**

**Master Wireshark to solve real-world security problems If you don’t already use Wireshark for a wide range of information security tasks, you will after this book. Mature and powerful, Wireshark is commonly used to find root cause of challenging network issues. This book extends that power to information security professionals, complete with a downloadable, virtual lab environment. Wireshark for Security Professionals covers both offensive and defensive concepts that can be applied to essentially any InfoSec role. Whether into network security, malware analysis, intrusion detection, or penetration testing, this book demonstrates Wireshark through relevant and useful examples. Master Wireshark through both lab scenarios and exercises. Early in the book, a virtual lab environment is provided for the purpose of getting hands-on experience with**

**Wireshark.** Wireshark is combined with two popular platforms: Kali, the security-focused Linux distribution, and the Metasploit Framework, the open-source framework for security testing. Lab-based virtual systems generate network traffic for analysis, investigation and demonstration. In addition to following along with the labs you will be challenged with end-of-chapter exercises to expand on covered material. Lastly, this book explores Wireshark with Lua, the light-weight programming language. Lua allows you to extend and customize Wireshark's features for your needs as a security professional. Lua source code is available both in the book and online. Lua code and lab source code are available online through GitHub, which the book also introduces. The book's final two chapters greatly draw on Lua and TShark, the command-line interface of Wireshark. By the end of the book you will gain the following: Master the basics of Wireshark Explore the virtual w4sp-lab environment that mimics a real-world network Gain experience using the Debian-based Kali OS among other systems Understand the technical details behind network attacks Execute exploitation and grasp offensive and defensive activities, exploring them through Wireshark Employ Lua to extend Wireshark features and create useful scripts To sum up, the book content, labs and online material, coupled with many referenced sources of PCAP traces, together present a dynamic and robust manual for information security professionals seeking to leverage Wireshark.

This is Cisco's comprehensive practical guide to planning, designing, installing, testing, and supporting both 802.11ac and 802.11n wireless networks for enterprise-based applications. Fully updated for the new 802.11ac standard, this Second Edition delivers expert hands-on guidance for mastering 802.11ac's fundamentally different design, site survey, implementation, and network configuration techniques. *Designing and Deploying 802.11 Wireless Networks, Second Edition* presents multiple examples using Cisco wireless products, while offering methodologies and tips that are applicable with any vendor's equipment. The authors offer in-depth coverage of building new wireless networks and migrating existing wireless networks (802.11a,b,g,n) to 802.11ac. After introducing fundamental wireless and 802.11 concepts, the authors present fully-updated coverage of all aspects of network design: requirements, architecture, performance, roaming, RF considerations, security, and much more. Drawing on extensive field experience, they walk through installation and testing, and share comprehensive operational guidance for managing security, troubleshooting roaming and connections, and training support staff. This edition's revamped coverage ranges from new site survey methods to best practices for WPA authentication configuration; advanced design guidelines for city-wide deployments to the latest Cisco equipment. Simply put, you'll find all you need to succeed with your next wireless project -- in any environment, no matter how challenging.

**CWNA Certified Wireless Network Administrator Official Deluxe Study Guide**

**A Step-by-Step Guide**

**The Network Security Test Lab**

## Packet Analysis with Wireshark

### The Definitive Guide

CWNA

**Fully revised for the CEH v8 exam objectives, this money-saving self-study bundle includes two eBooks, electronic content, and a bonus quick review guide. CEH Certified Ethical Hacker All-in-One Exam Guide, Second Edition Complete coverage of all CEH exam objectives Ideal as both a study tool and an on-the-job resource Electronic content includes hundreds of practice exam questions CEH Certified Ethical Hacker Practice Exams, Second Edition 650+ practice exam questions covering all CEH exam objectives Realistic questions with detailed answer explanations NEW pre-assessment test CEH Quick Review Guide Final overview of key exam topics CEH Certified Ethical Hacker Bundle, Second Edition covers all exam topics, including: Introduction to ethical hacking Reconnaissance and footprinting Scanning and enumeration Sniffing and evasion Attacking a system Hacking web servers and applications Wireless network hacking Trojans and other attacks Cryptography Social engineering and physical security Penetration testing**

**An all-new exam guide for version 8 of the Computer Hacking Forensic Investigator (CHFI) exam from EC-Council Get complete coverage of all the material included on version 8 of the EC-Council's Computer Hacking Forensic Investigator exam from this comprehensive resource. Written by an expert information security professional and educator, this authoritative guide addresses the tools and techniques required to successfully conduct a computer forensic investigation. You'll find learning objectives at the beginning of each chapter, exam tips, practice exam questions, and in-depth explanations. Designed to help you pass this challenging exam, this definitive volume also serves as an essential on-the-job reference. CHFI Computer Hacking Forensic Investigator Certification All-in-One Exam Guide covers all exam topics, including: Computer forensics investigation process Setting up a computer forensics lab First responder procedures Search and seizure laws Collecting and transporting digital evidence Understanding hard disks and file systems Recovering deleted files and partitions Windows forensics Forensics investigations using the AccessData Forensic Toolkit (FTK) and Guidance Software's EnCase Forensic Network, wireless, and mobile forensics Investigating web attacks Preparing investigative reports Becoming an expert witness Electronic content includes: 300 practice exam questions Test engine that provides full-length practice exams and customized quizzes by chapter or by exam domain**

**Over 60 powerful recipes to scan, exploit, and crack wireless networks for ethical purposes About This Book Expose wireless security threats through the eyes of an attacker, Recipes to help you proactively identify vulnerabilities and apply intelligent remediation, Acquire and apply key wireless pentesting skills used by industry experts Who This Book Is For If you are a security professional, administrator, and a network professional who wants to enhance their wireless penetration testing skills and knowledge then this book is**

**for you. Some prior experience with networking security and concepts is expected. What You Will Learn**  
**Deploy and configure a wireless cyber lab that resembles an enterprise production environment**  
**Install Kali Linux 2017.3 on your laptop and configure the wireless adapter**  
**Learn the fundamentals of commonly used wireless penetration testing techniques**  
**Scan and enumerate Wireless LANs and access points**  
**Use vulnerability scanning techniques to reveal flaws and weaknesses**  
**Attack Access Points to gain access to critical networks**  
**In Detail More and more organizations are moving towards wireless networks, and Wi-Fi is a popular choice. The security of wireless networks is more important than ever before due to the widespread usage of Wi-Fi networks. This book contains recipes that will enable you to maximize the success of your wireless network testing using the advanced ethical hacking features of Kali Linux. This book will go through techniques associated with a wide range of wireless penetration tasks, including WLAN discovery scanning, WEP cracking, WPA/WPA2 cracking, attacking access point systems, operating system identification, vulnerability mapping, and validation of results. You will learn how to utilize the arsenal of tools available in Kali Linux to penetrate any wireless networking environment. You will also be shown how to identify remote services, how to assess security risks, and how various attacks are performed. By finishing the recipes, you will feel confident conducting wireless penetration tests and will be able to protect yourself or your organization from wireless security threats. Style and approach The book will provide the foundation principles, techniques, and in-depth analysis to effectively master wireless penetration testing. It will aid you in understanding and mastering many of the most powerful and useful wireless testing techniques in the industry.**

**Sybex is now the official publisher for CWNP, the certifying vendor for the CWNA program. This valuable guide covers all objectives for the newest version of the PW0-104 exam, including radio technologies; antenna concepts; wireless LAN hardware and software; network design, installation and management; wireless standards and organizations; 802.11 network architecture; wireless LAN security; performing site surveys; and troubleshooting. Also included are hands-on exercises, chapter review questions, a detailed glossary, and a pre-assessment test. The CD-ROM features two bonus exams, over 150 flashcards, and numerous White Papers and demo software. Note: CD-ROM materials for eBook purchases can be downloaded from CWNP's website at [www.cwnp.com/sybex](http://www.cwnp.com/sybex).**

**CEH Certified Ethical Hacker All-in-One Exam Guide, Fifth Edition**

**Certified Ethical Hacker (CEH) Version 9 Cert Guide**

**Certified Wireless Network Administrator Official Study Guide: Exam CWNA-106**

**CWSP Certified Wireless Security Professional Official Study Guide**

**CEH Certified Ethical Hacker Bundle, Fourth Edition**

**This is the eBook edition of the Certified Ethical Hacker (CEH) Version 9 Cert Guide. This**

eBook does not include the practice exam that comes with the print edition. In this best-of-breed study guide, Certified Ethical Hacker (CEH) Version 9 Cert Guide, leading expert Michael Gregg helps you master all the topics you need to know to succeed on your Certified Ethical Hacker Version 9 exam and advance your career in IT security. Michael's concise, focused approach explains every exam objective from a real-world perspective, helping you quickly identify weaknesses and retain everything you need to know. Every feature of this book is designed to support both efficient exam preparation and long-term mastery:

- Opening Topics Lists identify the topics you need to learn in each chapter and list EC-Council's official exam objectives
- Key Topics figures, tables, and lists call attention to the information that's most crucial for exam success
- Exam Preparation Tasks enable you to review key topics, complete memory tables, define key terms, work through scenarios, and answer review questions...going beyond mere facts to master the concepts that are crucial to passing the exam and enhancing your career
- Key Terms are listed in each chapter and defined in a complete glossary, explaining all the field's essential terminology

This study guide helps you master all the topics on the latest CEH exam, including

- Ethical hacking basics
- Technical foundations of hacking
- Footprinting and scanning
- Enumeration and system hacking
- Linux distro's, such as Kali and automated assessment tools
- Trojans and backdoors
- Sniffers, session hijacking, and denial of service
- Web server hacking, web applications, and database attacks
- Wireless technologies, mobile security, and mobile attacks
- IDS, firewalls, and honeypots
- Buffer overflows, viruses, and worms
- Cryptographic attacks and defenses
- Cloud security and social engineering

**Certified Ethical Hacker Complete Training Guide with Practice Questions & Labs:Exam: 312-50IPSpecialist**

**Certified Ethical Hacker v10 Exam 312-50 Latest v10.** This updated version includes three major enhancement, New modules added to cover complete CEHv10 blueprint. Book scrutinized to rectify grammar, punctuation, spelling and vocabulary errors. Added 150+ Exam Practice Questions to help you in the exam. CEHv10 Update CEH v10 covers new modules for the security of IoT devices, vulnerability analysis, focus on emerging attack vectors on the cloud, artificial intelligence, and machine learning including a complete malware analysis process. Our CEH workbook delivers a deep understanding of applications of the vulnerability analysis in a real-world environment. Information security is always a great challenge for networks and systems. Data breach



statistics estimated millions of records stolen every day which evolved the need for Security. Almost each and every organization in the world demands security from identity theft, information leakage and the integrity of their data. The role and skills of Certified Ethical Hacker are becoming more significant and demanding than ever. EC-Council Certified Ethical Hacking (CEH) ensures the delivery of knowledge regarding fundamental and advanced security threats, evasion techniques from intrusion detection system and countermeasures of attacks as well as up-skill you to penetrate platforms to identify vulnerabilities in the architecture. CEH v10 update will cover the latest exam blueprint, comprised of 20 Modules which includes the practice of information security and hacking tools which are popularly used by professionals to exploit any computer systems. CEHv10 course blueprint covers all five Phases of Ethical Hacking starting from Reconnaissance, Gaining Access, Enumeration, Maintaining Access till covering your tracks. While studying CEHv10, you will feel yourself into a Hacker's Mindset. Major additions in the CEHv10 course are Vulnerability Analysis, IoT Hacking, Focused on Emerging Attack Vectors, Hacking Challenges, and updates of latest threats & attacks including Ransomware, Android Malware, Banking & Financial malware, IoT botnets and much more. IPSpecialist CEH technology workbook will help you to learn Five Phases of Ethical Hacking with tools, techniques, and The methodology of Vulnerability Analysis to explore security loopholes, Vulnerability Management Life Cycle, and Tools used for Vulnerability analysis. DoS/DDoS, Session Hijacking, SQL Injection & much more. Threats to IoT platforms and defending techniques of IoT devices. Advance Vulnerability Analysis to identify security loopholes in a corporate network, infrastructure, and endpoints. Cryptography Concepts, Ciphers, Public Key Infrastructure (PKI), Cryptography attacks, Cryptanalysis tools and Methodology of Crypt Analysis. Penetration testing, security audit, vulnerability assessment, and penetration testing roadmap. Cloud computing concepts, threats, attacks, tools, and Wireless networks, Wireless network security, Threats, Attacks, and Countermeasures and much more. The most detailed, comprehensive coverage of CWSP-205 exam objectives CWSP: Certified Wireless Security Professional Study Guide offers comprehensive preparation for the CWSP-205 exam. Fully updated to align with the new 2015 exam, this guide covers all exam objectives and gives you access to the Sybex interactive online learning system so you can go into the test fully confident in your skills. Coverage includes WLAN discovery, intrusion and attack, 802.11 protocol analysis, wireless intrusion prevention system implementation, Layer 2 and 3 VPN over

802.11 networks, managed endpoint security systems, and more. Content new to this edition features discussions about BYOD and guest access, as well as detailed and insightful guidance on troubleshooting. With more than double the coverage of the “official” exam guide, plus access to interactive learning tools, this book is your ultimate solution for CWSP-205 exam prep. The CWSP is the leading vendor-neutral security certification administered for IT professionals, developed for those working with and securing wireless networks. As an advanced certification, the CWSP requires rigorous preparation – and this book provides more coverage and expert insight than any other source. Learn the ins and outs of advanced network security

**Study 100 percent of CWSP-205 objectives**  
**Test your understanding with two complete practice exams**  
**Gauge your level of preparedness with a pre-test assessment**  
**The CWSP is a springboard for more advanced certifications, and the premier qualification employers look for in the field. If you’ve already earned the CWTS and the CWNA, it’s time to take your career to the next level.**

**CWSP: Certified Wireless Security Professional Study Guide is your ideal companion for effective, efficient CWSP-205 preparation.**

**SSCP Systems Security Certified Practitioner All-in-One Exam Guide, Second Edition**

**CWNA Certified Wireless Network Administrator Official Study Guide**

**CWSP Certified Wireless Security Professional Study Guide**

**Practical Packet Analysis, 2nd Edition**

**Cert Eth Hck (CEH Cert Guid**

**Linux Security Secrets and Solutions**

Fully up-to-date coverage of every topic on the CEH v9 certification exam Thoroughly revised for current exam objectives, this integrated self-study system offers complete coverage of the EC Council's Certified Ethical Hacker v9 exam. Inside, IT security expert Matt Walker discusses all of the tools, techniques, and exploits relevant to the CEH exam. Readers will find learning objectives at the beginning of each chapter, exam tips, end-of-chapter reviews, and practice exam questions with in-depth answer explanations. An integrated study system based on proven pedagogy, **CEH Certified Ethical Hacker All-in-One Exam Guide, Third Edition**, features brand-new explanations of cloud computing and mobile platforms and addresses vulnerabilities to the latest technologies and operating systems. Readers will learn about footprinting and reconnaissance, malware, hacking Web applications and mobile platforms, cloud computing vulnerabilities, and much more. Designed to help you pass the exam with ease, this authoritative resource will also serve as an essential on-the-job reference. Features more than 400 accurate practice questions, including new performance-based questions Electronic content includes 2 complete practice exams and a PDF copy of the book Written by an experienced educator with more than 30 years of experience in the field

This fully updated study guide offers complete coverage of every topic on the latest version of the SSCP exam. Take the 2018 edition of the challenging Systems Security Certified Practitioner (SSCP) exam with confidence using the detailed information contained in this highly effective self-study guide. The book provides 100% coverage of the revised SSCP Common Body of Knowledge (CBK) as developed by the International Information Systems Security Certification Consortium (ISC)². Written by bestselling IT security certification author and trainer Darril Gibson, *SSCP Systems Security Certified Practitioner All-in-One Exam Guide, Third Edition* clearly explains all exam domains. You will get lists of topics covered at the beginning of each chapter, exam tips, practice exam questions, and in-depth answer explanations. Designed to help you pass the exam with ease, *SSCP Systems Security Certified Practitioner All-in-One Exam Guide, Third Edition* also serves as an essential on-the-job reference. •Features 100% coverage of every objective on the SSCP exam•Electronic content includes 250+ practice questions and a secured book PDF•Written by an industry-recognized expert and experienced trainer

**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. Up-to-date coverage of every topic on the CEH v10 exam. Thoroughly updated for CEH v10 exam objectives, this integrated self-study system offers complete coverage of the EC-Council's Certified Ethical Hacker exam. In this new edition, IT security expert Matt Walker discusses the latest tools, techniques, and exploits relevant to the exam. You'll find 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 comprehensive resource also serves as an essential on-the-job reference. Covers all exam topics, including: •Ethical hacking fundamentals•Reconnaissance and footprinting•Scanning and enumeration•Sniffing and evasion•Attacking a system•Hacking web servers and applications•Wireless network hacking•Security in cloud computing•Trojans and other attacks•Cryptography•Social engineering and physical security•Penetration testing Digital content includes: •300 practice exam questions•Test engine that provides full-length practice exams and customized quizzes by chapter

**Designing and Deploying 802.11 Wireless Networks Second Edition** A Practical Guide to Implementing 802.11n and 802.11ac  
Wireless Networks For Enterprise-Based Applications Plan, deploy, and operate high-performance 802.11ac and 802.11n wireless networks. The new 802.11ac standard enables WLANs to deliver significantly higher performance. Network equipment manufacturers have refocused on 802.11ac- and 802.11n-compliant solutions, rapidly moving older versions of 802.11 toward "legacy" status. Now, there's a complete guide to planning, designing, installing, testing, and supporting 802.11ac and 802.11n wireless networks in any environment, for virtually any application. Jim Geier offers practical methods, tips, and recommendations that draw on his decades of experience deploying wireless solutions and shaping wireless standards. He carefully introduces 802.11ac's fundamentally different design, site survey, implementation, and network configuration techniques, helping you maximize performance and avoid pitfalls. Geier organizes each phase of WLAN deployment into clearly defined steps, making the entire planning and deployment process easy to understand and execute. He illuminates key concepts and methods through realistic case studies based on current Cisco products, while offering tips and techniques you can use with any vendor's equipment. To build your skills with key tasks, you'll find several

hands-on exercises relying on free or inexpensive tools. Whether you're deploying an entirely new wireless network or migrating from older equipment, this guide contains all the expert knowledge you'll need to succeed. Jim Geier has 30 years of experience planning, designing, analyzing and implementing communications, wireless, and mobile systems. Geier is founder and Principal Consultant of Wireless-Nets, Ltd., providing wireless analysis and design services to product manufacturers. He is also president, CEO, and co-founder of Health Grade Networks, providing wireless network solutions to hospitals, airports, and manufacturing facilities. His books include the first edition of *Designing and Deploying 802.11n Wireless Networks* (Cisco Press); as well as *Implementing 802.1X Security Solutions* and *Wireless Networking Handbook*. Geier has been active in the IEEE 802.11 Working Group and Wi-Fi Alliance; has chaired the IEEE Computer Society (Dayton Section) and various conferences; and served as expert witness in patent litigation related to wireless and cellular technologies. Review key 802.11 concepts, applications, markets, and technologies Compare ad hoc, mesh, and infrastructure WLANs and their components Consider the impact of radio signal interference, security vulnerabilities, multipath propagation, roaming, and battery limitations Thoroughly understand today's 802.11 standards in the context of actual network deployment and support Plan your deployment: scoping, staffing, schedules, budgets, risks, feasibility analysis, and requirements Architect access networks and distribution system for maximum reliability, manageability, and performance Make the right tradeoffs and decisions to optimize range, performance, and roaming Secure WLANs via encryption, authentication, rogue AP detection, RF shielding, and policies Master design and site survey tools and methods for planning 802.11ac networks and migrations Efficiently install and test any 802.11ac or 802.11n wireless network Establish specialized support for wireless networks, including help desk operations Systematically troubleshoot connectivity, performance, and roaming issues Design efficient mesh networks and city-wide deployments

Certified Ethical Hacker (CEH) Cert Guide

Using Wireshark and the Metasploit Framework

Network Intrusion Alert

Exam: 312-50

Hacking Exposed Linux

CHFI Computer Hacking Forensic Investigator Certification All-in-One Exam Guide

The official study guide for the Certified Wireless Analysis Professional certification from CWNP Four leading wireless experts thoroughly prepare you for the vendor-neutral CWAP exam administered by CWNP, the industry leader for enterprise Wi-Fi training and certification. This official study guide not only covers all exam objectives for the CWAP exam, it also prepares you to administer and troubleshoot complex enterprise WLAN environments. Covers all exam objectives for the Certified Wireless Analysis Professional (CWAP) exam Covers 802.11 physical (PHY) and 802.11 MAC layer frame formats and technologies Also covers 802.11 operation and frame exchanges, spectrum analysis and troubleshooting, and protocol analysis and troubleshooting Includes hands-on exercises using the Wireshark protocol analyzer and Fluke Network's Spectrum analyzer software Companion

CD includes two practice exams and over 150 electronic flashcards Advancing your skills as a wireless administrator professional? Start by passing the CWAP exam with the complete test prep you ' ll find in this practical study guide and CD. Note: CD-ROM materials for eBook purchases can be downloaded from <http://booksupport.wiley.com> .

Sybex is now the official publisher for Certified Wireless Network Professional, the certifying vendor for the CWSP program. This guide covers all exam objectives, including WLAN discovery techniques, intrusion and attack techniques, 802.11 protocol analysis. Wireless intrusion-prevention systems implementation, layer 2 and 3 VPNs used over 802.11 networks, and managed endpoint security systems. It also covers enterprise/SMB/SOHO/Public-Network Security design models and security solution implementation, building robust security networks, wireless LAN management systems, and much more.

Ethereal is the #2 most popular open source security tool used by system administrators and security professionals. This all new book builds on the success of Syngress ' best-selling book Ethereal Packet Sniffing. Wireshark & Ethereal Network Protocol Analyzer Toolkit provides complete information and step-by-step Instructions for analyzing protocols and network traffic on Windows, Unix or Mac OS X networks. First, readers will learn about the types of sniffers available today and see the benefits of using Ethereal. Readers will then learn to install Ethereal in multiple environments including Windows, Unix and Mac OS X as well as building Ethereal from source and will also be guided through Ethereal ' s graphical user interface. The following sections will teach readers to use command-line options of Ethereal as well as using Tethereal to capture live packets from the wire or to read saved capture files. This section also details how to import and export files between Ethereal and WinDump, Snort, Snoop, Microsoft Network Monitor, and EtherPeek. The book then teaches the reader to master advanced tasks such as creating sub-trees, displaying bitfields in a graphical view, tracking requests and reply packet pairs as well as exclusive coverage of MATE, Ethereal ' s brand new configurable upper level analysis engine. The final section to the book teaches readers to enable Ethereal to read new Data sources, program their own protocol dissectors, and to create and customize Ethereal reports. Ethereal is the #2 most popular open source security tool, according to a recent study conducted by insecure.org Syngress' first Ethereal book has consistently been one of the best selling security books for the past 2 years

As we all know by now, wireless networks offer many advantages over fixed (or wired) networks. Foremost on that list is mobility, since going wireless frees you from the tether of an Ethernet cable at a desk. But that's just the tip of the cable-free iceberg. Wireless networks are also more flexible, faster and easier for you to use, and more affordable to deploy and maintain. The de facto standard for wireless networking is the 802.11 protocol, which includes Wi-Fi (the wireless standard known as 802.11b) and its faster cousin, 802.11g. With easy-to-install 802.11 network hardware available everywhere you turn, the choice seems simple, and many people dive into wireless computing with less thought and planning than they'd give to a wired network. But it's wise to be familiar with both the capabilities and risks associated with the 802.11 protocols. And 802.11 Wireless Networks: The Definitive Guide, 2nd Edition is the perfect place to start. This updated edition covers everything you'll ever need to know about wireless technology. Designed with the system administrator or serious home user in mind, it's a no-nonsense guide for setting up 802.11

on Windows and Linux. Among the wide range of topics covered are discussions on: deployment considerations network monitoring and performance tuning wireless security issues how to use and select access points network monitoring essentials wireless card configuration security issues unique to wireless networks With wireless technology, the advantages to its users are indeed plentiful. Companies no longer have to deal with the hassle and expense of wiring buildings, and households with several computers can avoid fights over who's online. And now, with 802.11 Wireless Networks: The Definitive Guide, 2nd Edition, you can integrate wireless technology into your current infrastructure with the utmost confidence.

Exam PW0-270

Penetration Testing Fundamentals

CEH: Certified Ethical Hacker Version 8 Study Guide

Hands-On Ethical Hacking and Network Defense

Designing and Deploying 802.11 Wireless Networks

Wireshark & Ethereal Network Protocol Analyzer Toolkit

*This fully-updated, integrated self-study system offers complete coverage of the revised 2015 Systems Security Certified Practitioner (SSCP) exam domains Thoroughly revised for the April 2015 exam update, SSCP Systems Security Certified Practitioner All-in-One Exam Guide, Second Edition enables you to take the exam with complete confidence. To aid in self-study, each chapter includes Exam Tips that highlight key exam information, chapter summaries that reinforce salient points, and end-of-chapter questions that are an accurate reflection of the content and question format of the real exam. Beyond exam prep, the practical examples and real-world insights offered in this guide make it an ideal on-the-job reference for IT security professionals. You will learn the security concepts, tools, and procedures needed to employ and enforce solid security policies and effectively react to security incidents. Features 100% coverage of the revised SSCP Common Body of Knowledge (CBK), effective April 2015 Electronic content contains two full-length, customizable practice exams in the Total Tester exam engine Written by a bestselling IT security certification and training expert*

*Readers master the technical skills and industry know-how required to begin an exciting career installing, configuring, and troubleshooting computer networks with the completely updated NETWORK+ GUIDE TO NETWORKS, 7E. Readers prepare for success on CompTIA's Network+ N10-006 certification exam with fully mapped coverage of all objectives, including protocols, topologies, hardware, network design, and troubleshooting. New interactive features cater to the grazing reader, making essential information easily accessible and helping learners visualize high-level concepts. This edition introduces the latest developing technology with a fresh, logical organization. New OSI layer icons visually link concepts and the OSI model. New and updated On the Job stories, Applying Concepts activities, Hands-On and Case Projects encourage further exploration of chapter concepts. This edition's emphasis on real-world problem solving provides the tools to succeed in any computing environment. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.*

*Up-to-date coverage of every topic on the CEH v11 exam Thoroughly updated for CEH v11 exam objectives, this integrated self-study system offers complete coverage of the EC-Council's Certified Ethical Hacker exam. In this new edition, IT security expert Matt Walker discusses the latest tools, techniques, and exploits relevant to the exam. You'll find 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 comprehensive resource also serves as an essential on-the-job reference. Covers all exam topics, including: Ethical hacking fundamentals Reconnaissance and footprinting Scanning and enumeration Sniffing and evasion Attacking a system Hacking web servers and applications Wireless network hacking Mobile, IoT, and OT Security in cloud computing Trojans and other attacks, including malware analysis Cryptography Social engineering and physical security Penetration testing Online content includes: 300 practice exam questions Test engine that provides full-length practice exams and customized quizzes by chapter or exam domain The ultimate hands-on guide to IT security and proactivedefense The Network Security Test Lab is a hands-on, step-by-stepguide to ultimate IT security implementation. Covering the fullcomplement of malware, viruses, and other attack technologies, thisessential guide walks you through the security assessment andpenetration testing process, and provides the set-up guidance youneed to build your own security-testing lab. You'll look inside theactual attacks to decode their methods, and learn how to runattacks in an isolated sandbox to better understand how attackerstarget systems, and how to build the defenses that stop them. You'll be introduced to tools like Wireshark, Networkminer, Nmap, Metasploit, and more as you discover techniques for defendingagainst network attacks, social networking bugs, malware, and themost prevalent malicious traffic. You also get access to opensource tools, demo software, and a bootable version of Linux tofacilitate hands-on learning and help you implement your newskills. Security technology continues to evolve, and yet not a week goesby without news of a new security breach or a new exploit beingreleased. The Network Security Test Lab is the ultimateguide when you are on the front lines of defense, providing themost up-to-date methods of thwarting would-be attackers. Get acquainted with your hardware, gear, and test platform Learn how attackers penetrate existing security systems Detect malicious activity and build effective defenses Investigate and analyze attacks to inform defense strategy The Network Security Test Lab is your complete, essentialguide.*

*CWAP Certified Wireless Analysis Professional Official Study Guide*

*Exam PW0-104*

*Exam PW0-204*

*Practical Packet Analysis*

*Exam PW0-250*

*CEH Certified Ethical Hacker All-in-One Exam Guide, Third Edition*

*The official study guide for the Certified Wireless Design Professional (CWDP) exam from CWNP! This official guide is what you need to prepare for the vendor-neutral CWDP exam (PW0-250), which tests an IT professional's ability to design, plan, and troubleshoot a wireless network. Administered by CWNP, the industry leader for enterprise Wi-Fi training and certification, the CWDP exam is for those*

*operating in large WLAN deployments. This practical guide not only covers all exam objectives, it also gives you practical information on designing for complex environments such as businesses, hospitals, educational facilities, and in outdoor spaces. Covers all exam objectives for the Certified Wireless Design Professional (CWDP) exam, exam PW0-250 Covers planning, developing a WLAN design strategy and RF, conducting advanced site surveying, developing 802.11 security, and troubleshooting Companion CD includes two practice exams and over 100 electronic flashcards Sybex is the official publisher for Certified Wireless Network Professional, Inc., the certifying vendor for the CWAP program If you want to prepare for CWNP certification, a Sybex Study Guide is what you need! Note: CD-ROM materials for eBook purchases can be downloaded from <http://booksupport.wiley.com>.*

*With a mixture of theory, examples, and well-integrated figures, Embedded Software for the IoT helps the reader understand the details in the technologies behind the devices used in the Internet of Things. It provides an overview of IoT, parameters of designing an embedded system, and good practice concerning code, version control and defect-tracking needed to build and maintain a connected embedded system. After presenting a discussion on the history of the internet and the word wide web the book introduces modern CPUs and operating systems. The author then delves into an in-depth view of core IoT domains including: Wired and wireless networking Digital filters Security in embedded and networked systems Statistical Process Control for Industry 4.0 This book will benefit software developers moving into the embedded realm as well as developers already working with embedded systems.*

*Prepare for the new Certified Ethical Hacker version 8 exam with this Sybex guide Security professionals remain in high demand. The Certified Ethical Hacker is a one-of-a-kind certification designed to give the candidate a look inside the mind of a hacker. This study guide provides a concise, easy-to-follow approach that covers all of the exam objectives and includes numerous examples and hands-on exercises. Coverage includes cryptography, footprinting and reconnaissance, scanning networks, enumeration of services, gaining access to a system, Trojans, viruses, worms, covert channels, and much more. A companion website includes additional study tools, Including practice exam and chapter review questions and electronic flashcards. Security remains the fastest growing segment of IT, and CEH certification provides unique skills The CEH also satisfies the Department of Defense's 8570 Directive, which requires all Information Assurance government positions to hold one of the approved certifications This Sybex study guide is perfect for candidates studying on their own as well as those who are taking the CEHv8 course Covers all the exam objectives with an easy-to-follow approach Companion website includes practice exam questions, flashcards, and a searchable Glossary of key terms CEHv8: Certified Ethical Hacker Version 8 Study Guide is the book you need when you're ready to tackle this challenging exam Also available as a set, Ethical Hacking and Web Hacking Set, 9781119072171 with The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, 2nd Edition. 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*

*Hacking Exposed Wireless*

*A Practical Guide to Implementing 802.11n and 802.11ac Wireless Networks For Enterprise-Based Applications*

*Certified Ethical Hacker Version 9 Study Guide*

*802.11 Wireless Networks: The Definitive Guide*

*Wireshark for Security Professionals*

*Identify and assess vulnerabilities present in your wireless network, Wi-Fi, and Bluetooth enabled devices to improve your wireless security*

This is the eBook version of the print title. Note that the eBook does not provide access to the practice test software that accompanies the print book. Learn, prepare, and practice for CEH v8 exam success with this cert guide from Pearson IT Certification, a leader in IT certification learning. Master CEH exam topics Assess your knowledge with chapter-ending quizzes Review key concepts with exam preparation tasks Certified Ethical Hacker (CEH) Cert Guide is a best-of-breed exam study guide. Leading security consultant and certification expert Michael Gregg shares preparation hints and test-taking tips, helping you identify areas of weakness and improve both your conceptual knowledge and hands-on skills. Material is presented in a concise manner, focusing on increasing your understanding and retention of exam topics. You'll get a complete test preparation routine organized around proven series elements and techniques. Exam topic lists make referencing easy. Chapter-ending Exam Preparation Tasks help you drill on key concepts you must know thoroughly. Review questions help you assess your knowledge, and a final preparation chapter guides you through tools and resources to help you craft your final study plan. This EC-Council authorized study guide helps you master all the topics on the CEH v8 (312-50) exam, including: Ethical hacking basics Technical foundations of hacking Footprinting and scanning Enumeration and system hacking Linux and automated assessment tools Trojans and backdoors Sniffers, session hijacking, and denial of service Web server hacking, web applications, and database attacks Wireless technologies, mobile security, and mobile attacks IDS, firewalls, and honeypots Buffer overflows, viruses, and worms Cryptographic attacks and defenses Physical security and social engineering

The ultimate preparation guide for the unique CEH exam. The CEH v10: Certified Ethical Hacker Version 10 Study Guide is your ideal companion for CEH v10 exam preparation. This comprehensive, in-depth review of CEH certification requirements is designed to help you internalize critical information using concise, to-the-point explanations and an easy-to-follow approach to the material. Covering all sections of

the exam, the discussion highlights essential topics like intrusion detection, DDoS attacks, buffer overflows, and malware creation in detail, and puts the concepts into the context of real-world scenarios. Each chapter is mapped to the corresponding exam objective for easy reference, and the Exam Essentials feature helps you identify areas in need of further study. You also get access to online study tools including chapter review questions, full-length practice exams, hundreds of electronic flashcards, and a glossary of key terms to help you ensure full mastery of the exam material. The Certified Ethical Hacker is one-of-a-kind in the cybersecurity sphere, allowing you to delve into the mind of a hacker for a unique perspective into penetration testing. This guide is your ideal exam preparation resource, with specific coverage of all CEH objectives and plenty of practice material. Review all CEH v10 topics systematically Reinforce critical skills with hands-on exercises Learn how concepts apply in real-world scenarios Identify key proficiencies prior to the exam The CEH certification puts you in professional demand, and satisfies the Department of Defense's 8570 Directive for all Information Assurance government positions. Not only is it a highly-regarded credential, but it's also an expensive exam—making the stakes even higher on exam day. The CEH v10: Certified Ethical Hacker Version 10 Study Guide gives you the intense preparation you need to pass with flying colors.

The perfect introduction to pen testing for all IT professionals and students · Clearly explains key concepts, terminology, challenges, tools, and skills · Covers the latest penetration testing standards from NSA, PCI, and NIST Welcome to today ' s most useful and practical introduction to penetration testing. Chuck Easttom brings together up-to-the-minute coverage of all the concepts, terminology, challenges, and skills you ' ll need to be effective. Drawing on decades of experience in cybersecurity and related IT fields, Easttom integrates theory and practice, covering the entire penetration testing life cycle from planning to reporting. You ' ll gain practical experience through a start-to-finish sample project relying on free open source tools. Throughout, quizzes, projects, and review sections deepen your understanding and help you apply what you ' ve learned. Including essential pen testing standards from NSA, PCI, and NIST, Penetration Testing Fundamentals will help you protect your assets—and expand your career options. LEARN HOW TO · Understand what pen testing is and how it ' s used · Meet modern standards for comprehensive and effective testing · Review cryptography essentials every pen tester must know · Perform reconnaissance with Nmap, Google searches, and ShodanHq · Use malware as part of your pen testing toolkit · Test for vulnerabilities in Windows shares, scripts, WMI, and the Registry · Pen test websites and web communication · Recognize SQL injection and cross-site scripting attacks · Scan for vulnerabilities with OWASP ZAP, Vega, Nessus, and MBSA · Identify Linux vulnerabilities and password cracks · Use Kali Linux for advanced pen testing · Apply general hacking technique ssuch as fake Wi-Fi hotspots and social engineering · Systematically test your environment with Metasploit · Write or customize sophisticated Metasploit exploits

Exam CWNA-106

Embedded Software for the IoT

SSCP Systems Security Certified Practitioner All-in-One Exam Guide, Third Edition

Using Wireshark to Solve Real-world Network Problems

Designing and Deploying 802.11 Wireless Networks