

Giac Network Penetration Testing And Ethical Hacking

The practical guide to simulating, detecting, and responding to network attacks Create step-by-step testing plans Learn to perform social engineering and host reconnaissance Evaluate session hijacking methods Exploit web server vulnerabilities Detect attempts to breach database security Use password crackers to obtain access information Circumvent Intrusion Prevention Systems (IPS) and firewall protections and disrupt the service of routers and switches Scan and penetrate wireless networks Understand the inner workings of Trojan Horses, viruses, and other backdoor applications Test UNIX, Microsoft, and Novell servers for vulnerabilities Learn the root cause of buffer overflows and how to prevent them Perform and prevent Denial of Service attacks Penetration testing is a growing field but there has yet to be a definitive resource that instructs ethical hackers on how to perform a penetration test with the ethics and responsibilities of testing in mind. Penetration Testing and Network Defense offers detailed steps on how to emulate an outside attacker in order to assess the security of a network. Unlike other books on hacking, this book is specifically geared towards penetration testing. It includes important information about liability issues and ethics as well as procedures and documentation. Using popular open-source and commercial applications, the book shows you how to perform a penetration test on an organization's network, from creating a test plan to performing social engineering and host reconnaissance to performing simulated attacks on both wired and wireless networks. Penetration Testing and Network Defense also goes a step further than other books on hacking, as it demonstrates how to detect an attack on a live network. By detailing the method of an attack and how to spot an attack on your network, this book better prepares you to guard against hackers. You will learn how to configure, record, and thwart these attacks and how to harden a system to protect it against future internal and external attacks. Full of real-world examples and step-by-step procedures, this book is both an enjoyable read and full of practical advice that will help you assess network security and develop a plan for locking down sensitive data and company resources. "This book goes to great lengths to explain the various testing approaches that are used today and gives excellent insight into how a responsible penetration testing specialist executes his trade." -Bruce Murphy, Vice President, World Wide Security Services, Cisco Systems

Target, test, analyze, and report on security vulnerabilities with pen testing Pen Testing is necessary for companies looking to target, test, analyze, and patch the security vulnerabilities from hackers attempting to break into and compromise their organizations data. It takes a person with hacking skills to look for the weaknesses that make an organization susceptible to hacking. Pen Testing For Dummies aims to equip IT enthusiasts at various levels with the basic knowledge of pen testing. It is the go-to book for those who have some IT experience but desire more knowledge of how to gather intelligence on a target, learn the steps for mapping out a test, and discover best practices for analyzing, solving, and reporting on vulnerabilities. The different phases of a pen test from pre-engagement to completion Threat modeling and understanding risk When to apply vulnerability management vs penetration testing Ways to keep your pen testing skills sharp, relevant, and at the top of the game Get ready to gather intelligence, discover the steps for mapping out tests, and analyze and report results!

Cyber-terrorism and corporate espionage are increasingly common and devastating threats, making trained network security professionals more important than ever. This timely text helps you gain the knowledge and skills to protect networks using the tools and techniques of an ethical hacker. The authors begin by exploring the concept of ethical hacking and its practitioners, explaining their importance in protecting corporate and government data from cyber attacks. The text then provides an in-depth guide to performing security testing against computer networks, covering current tools and penetration testing methodologies. Updated for today's cyber security environment, the Third Edition of this trusted text features new computer security resources, coverage of emerging vulnerabilities and innovative methods to protect networks, a new discussion of mobile security, and information on current federal and state computer crime laws, including penalties for illegal computer hacking. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

- This is the latest practice test to pass the GPEN GIAC Penetration Tester Exam. - It contains 385 Questions and Answers. - All the questions are 100% valid and stable. - You can rely on this practice test to pass the exam with a good mark and in the first attempt.

Over 100 practical recipes that leverage custom scripts and integrated tools in Kali Linux to help you effectively master network scanning About This Book Learn the fundamentals behind commonly used scanning techniques Deploy powerful scanning tools that are integrated into the Kali Linux testing platform The practical recipes will help you automate menial tasks and build your own script library Who This Book Is For This book is for information security professionals and casual security enthusiasts alike. It provides foundational principles if you're a novice, but will also introduce scripting techniques and in-depth analysis if you're more advanced. Whether you are brand new to Kali Linux or a seasoned veteran, this book will help you both understand and ultimately master many of the most powerful and useful scanning techniques in the industry. It is assumed that you have some basic security testing experience. What You Will Learn Develop a network-testing environment to test scanning tools and techniques Understand the principles of network-scanning tools by building scripts and tools Identify distinct vulnerabilities in web apps and remote services and learn how they are exploited Perform comprehensive scans to identify listening on TCP and UDP sockets Get started with different Kali desktop environments--KDE, MATE, LXDE, and Xfce Use Sparta for information gathering, port scanning, fingerprinting, vulnerability scanning, and more Evaluate DoS threats and learn how common DoS attacks are performed Learn how to use Burp Suite to evaluate web applications In Detail With the ever-increasing amount of data flowing in today's world, information security has become vital to any application. This is

where Kali Linux comes in. Kali Linux focuses mainly on security auditing and penetration testing. This step-by-step cookbook on network scanning trains you in important scanning concepts based on version 2016.2. It will enable you to conquer any network environment through a range of network scanning techniques and will also equip you to script your very own tools. Starting with the fundamentals of installing and managing Kali Linux, this book will help you map your target with a wide range of network scanning tasks, including discovery, port scanning, fingerprinting, and more. You will learn how to utilize the arsenal of tools available in Kali Linux to conquer any network environment. The book offers expanded coverage of the popular Burp Suite and has new and updated scripts for automating scanning and target exploitation. You will also be shown how to identify remote services, how to assess security risks, and how various attacks are performed. You will cover the latest features of Kali Linux 2016.2, which includes the enhanced Sparta tool and many other exciting updates. This immersive guide will also encourage the creation of personally scripted tools and the skills required to create them. Style and approach This step-by-step guide is full of recipes that will help you use integrated scanning tools in Kali Linux and develop custom scripts to make new and unique tools of your own.

Today, society is faced with numerous internet schemes, fraudulent scams, and means of identity theft that threaten our safety and our peace of mind. Computer Security: Protecting Digital Resources provides a broad approach to computer-related crime, electronic commerce, corporate networking, and Internet security, topics that have become increasingly important as more and more threats are made on our internet environment. This book is oriented toward the average computer user, business professional, government worker, and those within the education community, with the expectation that readers can learn to use the network with some degree of safety and security. The author places emphasis on the numerous vulnerabilities and threats that are inherent in the Internet environment. Efforts are made to present techniques and suggestions to avoid identity theft and fraud. Readers will gain a clear insight into the many security issues facing the e-commerce, networking, web, and internet environments, as well as what can be done to keep personal and business information secure.

Kali Linux Network Scanning Cookbook is intended for information security professionals and casual security enthusiasts alike. It will provide the foundational principles for the novice reader but will also introduce scripting techniques and in-depth analysis for the more advanced audience. Whether you are brand new to Kali Linux or a seasoned veteran, this book will aid in both understanding and ultimately mastering many of the most powerful and useful scanning techniques in the industry. It is assumed that the reader has some basic security testing experience.

- This is the latest practice test to pass the GIAC GSLC GIAC Security Leadership Exam. - It contains 566 Questions and Answers. - All the questions are 100% valid and stable. - You can reply on this practice test to pass the exam with a good mark and in the first attempt.

- This is the latest practice test to pass the GIAC GISP GIAC Information Security Professional Exam. - It contains 654 Questions and Answers. - All the questions are 100% valid and stable. - You can reply on this practice test to pass the exam with a good mark and in the first attempt.

Get hands-on experience on concepts of Bug Bounty Hunting Key Features Get well-versed with the fundamentals of Bug Bounty Hunting Hands-on experience on using different tools for bug hunting Learn to write a bug bounty report according to the different vulnerabilities and its analysis Book Description Bug bounty programs are the deals offered by prominent companies where-in any white-hat hacker can find bugs in the applications and they will have a recognition for the same. The number of prominent organizations having this program has increased gradually leading to a lot of opportunity for Ethical Hackers. This book will initially start with introducing you to the concept of Bug Bounty hunting. Then we will dig deeper into concepts of vulnerabilities and analysis such as HTML injection, CRLF injection and so on. Towards the end of the book, we will get hands-on experience working with different tools used for bug hunting and various blogs and communities to be followed. This book will get you started with bug bounty hunting and its fundamentals. What you will learn Learn the basics of bug bounty hunting Hunt bugs in web applications Hunt bugs in Android applications Analyze the top 300 bug reports Discover bug bounty hunting research methodologies Explore different tools used for Bug Hunting Who this book is for This book is targeted towards white-hat hackers, or anyone who wants to understand the concept behind bug bounty hunting and understand this brilliant way of penetration testing. This book does not require any knowledge on bug bounty hunting.

This book shows what IT in organizations need to accomplish to implement The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets and The National Strategy to Secure Cyberspace which were developed by the Department of Homeland Security after the terrorist attacks of September 2001. The September 11, 2001, attacks illustrated the immense vulnerability to terrorist threats. Since then there have been considerable efforts to develop plans and methods to protect critical infrastructures and key assets. The government at all levels, private sector organizations, as well as concerned citizens have begun to establish partnerships and to develop action plans. But there are many questions yet to be answered about what organizations should actual do to protect their assets and their people while participating in national efforts to improve security. This book provides practical steps that IT managers in all organizations and sectors can take to move security from the planning process into practice. *A one-minute manager approach to issuesp provides background and explanations in all areas *Step-by-step instructions on how to accomplish objectives guide readers through processes *Easy to implement advice allows readers to take quick action

- This is the latest practice test to pass the GSNA GIAC Systems and Network Auditor Exam. - It contains 413 Questions and Answers. - All the questions are 100% valid and stable. - You can reply on this practice test to pass the exam with a good mark and in the first attempt.

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

Eleventh Hour CISSP provides you with a study guide keyed directly to the most current version of the CISSP exam. This book is streamlined to include only core certification information and is presented for ease of last minute studying. Main objectives of the exam are covered concisely with key concepts highlighted. The CISSP certification is the most prestigious, globally recognized, vendor neutral exam for information security professionals. Over 67,000 professionals are certified worldwide with many more joining their ranks. This new Second Edition is aligned to cover all of the material in the most current version of the exam's Common Body of Knowledge. All 10 domains are covered as completely and as concisely as possible, giving you the best possible chance of acing the exam. All-new Second Edition updated for the most current version of the exam's Common Body of Knowledge The only guide you need for last minute studying Answers the toughest questions and highlights core topics No fluff - streamlined for maximum efficiency of study – perfect for professionals who are updating their certification or taking the test for the first time

Your one-stop guide to using Python, creating your own hacking tools, and making the most out of resources available for this programming language Key Features Comprehensive information on building a web application penetration testing framework using Python Master web application penetration testing using the multi-paradigm programming language Python Detect vulnerabilities in a system or application by writing your own Python scripts Book Description Python is an easy-to-learn and cross-platform programming language that has unlimited third-party libraries. Plenty of open source hacking tools are written in Python, which can be easily integrated within your script. This book is packed with step-by-step instructions and working examples to make you a skilled penetration tester. It is divided into clear bite-sized chunks, so you can learn at your own pace and focus on the areas of most interest to you. This book will teach you how to code a reverse shell and build an anonymous shell. You will also learn how to hack passwords and perform a privilege escalation on Windows with practical examples. You will set up your own virtual hacking environment in VirtualBox, which will help you run multiple operating systems for your testing environment. By the end of this book, you will have learned how to code your own scripts and mastered ethical hacking from scratch. What you will learn Code your own reverse shell (TCP and HTTP) Create your own anonymous shell by interacting with Twitter, Google Forms, and SourceForge Replicate Metasploit features and build an advanced shell Hack passwords using multiple techniques (API hooking, keyloggers, and clipboard hijacking) Exfiltrate data from your target Add encryption (AES, RSA, and XOR) to your shell to learn how cryptography is being abused by malware Discover privilege escalation on Windows with practical examples Countermeasures against most attacks Who this book is for This book is for ethical hackers; penetration testers; students preparing for OSCP, OSCE, GPEN, GXPN, and CEH; information security professionals; cybersecurity consultants; system and network security administrators; and programmers who are keen on learning all about penetration testing.

Get up to speed with various penetration testing techniques and resolve security threats of varying complexity Key Features Enhance your penetration testing skills to tackle security threats Learn to gather information, find vulnerabilities, and exploit enterprise defenses Navigate secured systems with the most up-to-date version of Kali Linux (2019.1) and Metasploit (5.0.0) Book Description Sending information via the internet is not entirely private, as evidenced by the rise in hacking, malware attacks, and security threats. With the help of this book, you'll learn crucial penetration testing techniques to help you evaluate enterprise defenses. You'll start by understanding each stage of pentesting and deploying target virtual machines, including Linux and Windows. Next, the book will guide you through performing intermediate penetration testing in a controlled environment. With the help of practical use cases, you'll also be able to implement your learning in real-world scenarios. By studying everything from setting up your lab, information gathering and password attacks, through to social engineering and post exploitation, you'll be able to successfully overcome security threats. The book will even help you leverage the best tools, such as Kali Linux, Metasploit, Burp Suite, and other open source pentesting tools to perform these techniques. Toward the later chapters, you'll focus on best practices to quickly resolve security threats. By the end of this book, you'll be well versed with various penetration testing techniques so as to be able to tackle security threats effectively What you will learn Perform entry-level penetration tests by learning various concepts and techniques Understand both common and not-so-common vulnerabilities from an attacker's perspective Get familiar with intermediate attack methods that can be used in real-world scenarios Understand how vulnerabilities are created by developers and how to fix some of them at source code level Become well versed with basic tools for ethical hacking purposes Exploit known vulnerable services with tools such as Metasploit Who this book is for If you're just getting started with penetration testing and want to explore various security domains, this book is for you. Security professionals, network engineers, and amateur ethical hackers will also find this book useful. Prior knowledge of penetration testing and ethical hacking is not necessary.

- This is the latest practice test to pass the GCFA GIAC Certified Forensic Analyst Exam. - It contains 318 Questions and Answers. - All the questions are 100% valid and stable. - You can reply on this practice test to pass the exam with a good mark and in the first attempt.

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 classicalSQL, 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.

JUMPSTART YOUR NEW AND EXCITING CAREER AS A PENETRATION TESTER The Pentester BluePrint: Your Guide to Being a Pentester offers readers a chance to delve deeply into the world of the ethical, or "white-hat" hacker. Accomplished pentester and author Phillip L. Wylie and cybersecurity researcher Kim Crawley walk you through the basic and advanced topics necessary to understand how to make a career out of finding vulnerabilities in systems, networks, and applications. You'll learn about the role of a penetration tester, what a pentest involves, and the prerequisite knowledge you'll need to start the educational journey of becoming a pentester. Discover how to develop a plan by assessing your current skillset and finding a starting place to begin growing your knowledge and skills. Finally, find

out how to become employed as a pentester by using social media, networking strategies, and community involvement. Perfect for IT workers and entry-level information security professionals, *The Pentester BluePrint* also belongs on the bookshelves of anyone seeking to transition to the exciting and in-demand field of penetration testing. Written in a highly approachable and accessible style, *The Pentester BluePrint* avoids unnecessarily technical lingo in favor of concrete advice and practical strategies to help you get your start in pentesting. This book will teach you: The foundations of pentesting, including basic IT skills like operating systems, networking, and security systems The development of hacking skills and a hacker mindset Where to find educational options, including college and university classes, security training providers, volunteer work, and self-study Which certifications and degrees are most useful for gaining employment as a pentester How to get experience in the pentesting field, including labs, CTFs, and bug bounties

Discover the latest trends, developments and technology in information security today with Whitman/Mattord's market-leading *PRINCIPLES OF INFORMATION SECURITY*, 7th Edition. Designed specifically to meet the needs of those studying information systems, this edition's balanced focus addresses all aspects of information security, rather than simply offering a technical control perspective. This overview explores important terms and examines what is needed to manage an effective information security program. A new module details incident response and detection strategies. In addition, current, relevant updates highlight the latest practices in security operations as well as legislative issues, information management toolsets and digital forensics. Coverage of the most recent policies and guidelines that correspond to federal and international standards further prepare you for success both in information systems and as a business decision-maker. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

The Art of Network Penetration Testing is a guide to simulating an internal security breach. You'll take on the role of the attacker and work through every stage of a professional pentest, from information gathering to seizing control of a system and owning the network. Summary Penetration testing is about more than just getting through a perimeter firewall. The biggest security threats are inside the network, where attackers can rampage through sensitive data by exploiting weak access controls and poorly patched software. Designed for up-and-coming security professionals, *The Art of Network Penetration Testing* teaches you how to take over an enterprise network from the inside. It lays out every stage of an internal security assessment step-by-step, showing you how to identify weaknesses before a malicious invader can do real damage. Purchase of the print book includes a free eBook in PDF, Kindle, and ePub formats from Manning Publications. About the technology Penetration testers uncover security gaps by attacking networks exactly like malicious intruders do. To become a world-class pentester, you need to master offensive security concepts, leverage a proven methodology, and practice, practice, practice. This book delivers insights from security expert Royce Davis, along with a virtual testing environment you can use to hone your skills. About the book *The Art of Network Penetration Testing* is a guide to simulating an internal security breach. You'll take on the role of the attacker and work through every stage of a professional pentest, from information gathering to seizing control of a system and owning the network. As you brute force passwords, exploit unpatched services, and elevate network level privileges, you'll learn where the weaknesses are—and how to take advantage of them. What's inside Set up a virtual pentest lab Exploit Windows and Linux network vulnerabilities Establish persistent re-entry to compromised targets Detail your findings in an engagement report About the reader For tech professionals. No security experience required. About the author Royce Davis has orchestrated hundreds of penetration tests, helping to secure many of the largest companies in the world. Table of Contents 1 Network Penetration Testing PHASE 1 - INFORMATION GATHERING 2 Discovering network hosts 3 Discovering network services 4 Discovering network vulnerabilities PHASE 2 - FOCUSED PENETRATION 5 Attacking vulnerable web services 6 Attacking vulnerable database services 7 Attacking unpatched services PHASE 3 - POST-EXPLOITATION AND PRIVILEGE ESCALATION 8 Windows post-exploitation 9 Linux or UNIX post-exploitation 10 Controlling the entire network PHASE 4 - DOCUMENTATION 11 Post-engagement cleanup 12 Writing a solid pentest deliverable

CISSP Study Guide, Third Edition provides readers with information on the CISSP certification, the most prestigious, globally-recognized, vendor-neutral exam for information security professionals. With over 100,000 professionals certified worldwide, and many more joining their ranks, this new third edition presents everything a reader needs to know on the newest version of the exam's Common Body of Knowledge. The eight domains are covered completely and as concisely as possible, allowing users to ace the exam. Each domain has its own chapter that includes a specially-designed pedagogy to help users pass the exam, including clearly-stated exam objectives, unique terms and definitions, exam warnings, "learning by example" modules, hands-on exercises, and chapter ending questions. Provides the most complete and effective study guide to prepare users for passing the CISSP exam, giving them exactly what they need to pass the test Authored by Eric Conrad who has prepared hundreds of professionals for passing the CISSP exam through SANS, a popular and well-known organization for information security professionals Covers all of the new information in the Common Body of Knowledge updated in January 2015, and also provides two exams, tiered end-of-chapter questions for a gradual learning curve, and a complete self-test appendix

Get prepared for your Information Security job search! Do you want to equip yourself with the knowledge necessary to succeed in the Information Security job market? If so, you've come to the right place. Packed with the latest and most effective strategies for landing a lucrative job in this popular and quickly-growing field, *Getting an Information Security Job For Dummies* provides no-nonsense guidance on everything you need to get ahead of the competition and launch yourself into your dream job as an Information Security (IS) guru. Inside, you'll discover the fascinating history, projected future, and current applications/issues in the IS field. Next, you'll get up to speed on the general educational concepts you'll be exposed to while earning your analyst certification and the technical requirements for obtaining an IS position. Finally, learn how to set yourself up for job hunting success with trusted and supportive guidance on creating a winning resume, gaining attention with your cover letter, following up after an initial interview, and much more. Covers the certifications needed for various jobs in the Information Security field Offers guidance on writing an attention-getting resume Provides access to helpful videos, along with other online bonus materials Offers advice on branding yourself and securing your future in Information Security If you're a student, recent graduate, or professional looking to break into the field of Information Security, this hands-on, friendly guide has you covered.

- This is the latest practice test to pass the GIAC GISF GIAC Information Security Fundamentals Exam. - It contains 316 Questions and Answers. - All the questions are 100% valid and stable. - You can reply on this practice test to pass the exam with a good mark and in the first attempt.

GPEN GIAC Certified Penetration Tester All-in-One Exam Guide McGraw Hill Professional

Most organizations place a high priority on keeping data secure, but not every organization invests in training its engineers or employees in understanding the security risks involved when using or developing technology. Designed for the non-security professional, *What Every Engineer Should Know About Cyber Security and Digital Forensics* is an overview of the field of cyber security. Exploring the cyber security topics that every engineer should understand, the book discusses: Network security Personal data security Cloud computing Mobile computing Preparing for an incident Incident response Evidence handling Internet usage Law and compliance Security and forensic certifications Application of the concepts is demonstrated through short case studies of real-world incidents chronologically delineating related events. The book also discusses certifications and reference manuals in the area of cyber security and digital forensics. By

mastering the principles in this volume, engineering professionals will not only better understand how to mitigate the risk of security incidents and keep their data secure, but also understand how to break into this expanding profession.

- This is the latest practice test to pass the GCIH GIAC Certified Incident Handler Exam. - It contains 328 Questions and Answers. - All the questions are 100% valid and stable. - You can reply on this practice test to pass the exam with a good mark and in the first attempt.

A practical guide to deploying digital forensic techniques in response to cyber security incidents About This Book Learn incident response fundamentals and create an effective incident response framework Master forensics investigation utilizing digital investigative techniques Contains real-life scenarios that effectively use threat intelligence and modeling techniques Who This Book Is For This book is targeted at Information Security professionals, forensics practitioners, and students with knowledge and experience in the use of software applications and basic command-line experience. It will also help professionals who are new to the incident response/digital forensics role within their organization. What You Will Learn Create and deploy incident response capabilities within your organization Build a solid foundation for acquiring and handling suitable evidence for later analysis Analyze collected evidence and determine the root cause of a security incident Learn to integrate digital forensic techniques and procedures into the overall incident response process Integrate threat intelligence in digital evidence analysis Prepare written documentation for use internally or with external parties such as regulators or law enforcement agencies In Detail Digital Forensics and Incident Response will guide you through the entire spectrum of tasks associated with incident response, starting with preparatory activities associated with creating an incident response plan and creating a digital forensics capability within your own organization. You will then begin a detailed examination of digital forensic techniques including acquiring evidence, examining volatile memory, hard drive assessment, and network-based evidence. You will also explore the role that threat intelligence plays in the incident response process. Finally, a detailed section on preparing reports will help you prepare a written report for use either internally or in a courtroom. By the end of the book, you will have mastered forensic techniques and incident response and you will have a solid foundation on which to increase your ability to investigate such incidents in your organization. Style and approach The book covers practical scenarios and examples in an enterprise setting to give you an understanding of how digital forensics integrates with the overall response to cyber security incidents. You will also learn the proper use of tools and techniques to investigate common cyber security incidents such as malware infestation, memory analysis, disk analysis, and network analysis.

Professional Penetration Testing walks you through the entire process of setting up and running a pen test lab. Penetration testing—the act of testing a computer network to find security vulnerabilities before they are maliciously exploited—is a crucial component of information security in any organization. With this book, you will find out how to turn hacking skills into a professional career. Chapters cover planning, metrics, and methodologies; the details of running a pen test, including identifying and verifying vulnerabilities; and archiving, reporting and management practices. Author Thomas Wilhelm has delivered penetration testing training to countless security professionals, and now through the pages of this book you can benefit from his years of experience as a professional penetration tester and educator. After reading this book, you will be able to create a personal penetration test lab that can deal with real-world vulnerability scenarios. All disc-based content for this title is now available on the Web. Find out how to turn hacking and pen testing skills into a professional career Understand how to conduct controlled attacks on a network through real-world examples of vulnerable and exploitable servers Master project management skills necessary for running a formal penetration test and setting up a professional ethical hacking business Discover metrics and reporting methodologies that provide experience crucial to a professional penetration tester Master the tools of the network security trade with the official book from SANS Press! You need more than a hammer to build a house, and you need more than one tool to secure your network. Security Essentials Toolkit covers the critical tools that you need to secure your site, showing you why, when, and how to use them. Based on the SANS Institute's renowned Global Information Assurance Certification (GIAC) program, this book takes a workbook-style approach that gives you hands-on experience and teaches you how to install, configure, and run the best security tools of the trade.

Fundamentals of Information Systems Security, Fourth Edition provides a comprehensive overview of the essential concepts readers must know as they pursue careers in information systems security.

This comprehensive exam guide offers 100% coverage of every topic on the CompTIA PenTest+ exam Get complete coverage of all the objectives included on the CompTIA PenTest+ certification exam PT0-001 from this comprehensive resource. Written by an expert penetration tester, the book provides learning objectives at the beginning of each chapter, hands-on exercises, exam tips, and practice questions with in-depth answer explanations. Designed to help you pass the exam with ease, this definitive volume also serves as an essential on-the-job reference. Covers all exam topics, including: •Pre-engagement activities •Getting to know your targets •Network scanning and enumeration •Vulnerability scanning and analysis •Mobile device and application testing •Social engineering •Network-based attacks •Wireless and RF attacks •Web and database attacks •Attacking local operating systems •Physical penetration testing •Writing the pen test report •And more Online content includes: •Interactive performance-based questions •Test engine that provides full-length practice exams or customized quizzes by chapter or by exam domain

Readers discover a managerially-focused overview of information security with a thorough treatment of how to most effectively administer it with MANAGEMENT OF INFORMATION SECURITY, 5E. Information throughout helps readers become information security management practitioners able to secure systems and networks in a world where continuously emerging threats, ever-present attacks, and the success of criminals illustrate the weaknesses in current information technologies. Current and future professional managers complete this book with the exceptional blend of skills and experiences to develop and manage the more secure computing environments that today's organizations need. This edition offers a tightened focus on key executive and managerial aspects of information security while still emphasizing the important foundational material to reinforce key concepts. Updated content reflects the most recent developments in the field, including NIST, ISO, and security governance. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

This effective study guide provides 100% coverage of every topic on the GPEN GIAC Penetration Tester exam. This effective self-study guide fully prepares you for the Global Information Assurance Certification's challenging Penetration Tester exam, which validates advanced IT security skills. The book features exam-focused coverage of penetration testing methodologies, legal issues, and best practices. GPEN GIAC Certified Penetration Tester All-in-One Exam Guide contains useful tips and tricks, real-world examples, and case studies drawn from authors' extensive experience. Beyond exam preparation, the book also serves as a valuable on-the-job reference. Covers every topic on the exam, including: Pre-engagement and planning activities Reconnaissance and open source intelligence gathering Scanning, enumerating targets, and identifying vulnerabilities Exploiting targets and privilege escalation Password attacks Post-exploitation activities, including data exfiltration and pivoting PowerShell for penetration testing Web application injection attacks Tools of the trade: Metasploit, proxies, and more Online content includes: 230 accurate practice exam questions Test engine containing full-length practice exams and customizable quizzes

This self-study guide delivers complete coverage of every topic on the GIAC Certified Incident Handler exam. Prepare for the challenging GIAC Certified Incident Handler exam using the detailed information contained in this effective exam preparation guide. Written by a recognized cybersecurity expert and seasoned author, GCIH GIAC Certified Incident Handler All-in-One Exam Guide clearly explains all of the advanced security incident handling skills covered on the test. Detailed examples and chapter summaries throughout demonstrate real-world threats and aid in retention. You will get online access to 300 practice questions that match those on the live test in style, format, and tone. Designed to help you prepare for the exam, this resource also serves as an ideal on-the-job reference. Covers all exam topics, including: Intrusion analysis and incident handling Information gathering Scanning, enumeration, and vulnerability identification Vulnerability exploitation Infrastructure and endpoint attacks Network, DoS, and Web application attacks Maintaining access Evading detection and covering tracks Worms, bots, and botnets Online content includes: 300 practice exam questions Test engine that provides full-length practice exams and customizable quizzes

Over 100 practical recipes that leverage custom scripts and integrated tools in Kali Linux to help you effectively master network scanning. About This Book* Learn the fundamentals behind commonly used scanning techniques* Deploy powerful scanning tools that are integrated into the Kali Linux testing platform* The practical recipes will help you automate menial tasks and build your own script library. Who This Book Is For* This book is for information security professionals and casual security enthusiasts alike. It provides foundational principles if you're a novice, but will also introduce scripting techniques and in-depth analysis if you're more advanced. Whether you are brand new to Kali Linux or a seasoned veteran, this book will help you both understand and ultimately master many of the most powerful and useful scanning techniques in the industry. It is assumed that you have some basic security testing experience. What You Will Learn* Develop a network-testing environment to test scanning tools and techniques* Understand the principles of network-scanning tools by building scripts and tools* Identify distinct vulnerabilities in web apps and remote services and learn how they are exploited* Perform comprehensive scans to identify listening on TCP and UDP sockets* Get started with different Kali desktop environments--KDE, MATE, LXDE, and Xfce* Use Sparta for information gathering, port scanning, fingerprinting, vulnerability scanning, and more* Evaluate DoS threats and learn how common DoS attacks are performed* Learn how to use Burp Suite to evaluate web applications. In Detail* With the ever-increasing amount of data flowing in today's world, information security has become vital to any application. This is where Kali Linux comes in. Kali Linux focuses mainly on security auditing and penetration testing. This step-by-step cookbook on network scanning trains you in important scanning concepts based on version 2016.2. It will enable you to conquer any network environment through a range of network scanning techniques and will also equip you to script your very own tools. Starting with the fundamentals of installing and managing Kali Linux, this book will help you map your target with a wide range of network scanning tasks, including discovery, port scanning, fingerprinting, and more. You will learn how to utilize the arsenal of tools available in Kali Linux to conquer any network environment. The book offers expanded coverage of the popular Burp Suite and has new and updated scripts for automating scanning and target exploitation. You will also be shown how to identify remote services, how to assess security risks, and how various attacks are performed. You will cover the latest features of Kali Linux 2016.2, which includes the enhanced Sparta tool and many other exciting updates. This immersive guide will also encourage the creation of personally scripted tools and the skills required to create them. Style and approach* This step-by-step guide is full of recipes that will help you use integrated scanning tools in Kali Linux and develop custom scripts to make new and unique tools of your own.

Cyber Warfare, Second Edition, takes a comprehensive look at how and why digital warfare is waged. The book explores the participants, battlefields, and the tools and techniques used in today's digital conflicts. The concepts discussed gives students of information security a better idea of how cyber conflicts are carried out now, how they will change in the future, and how to detect and defend against espionage, hacktivism, insider threats and non-state actors such as organized criminals and terrorists. This book provides concrete examples and real-world guidance on how to identify and defend a network against malicious attacks. It probes relevant technical and factual information from an insider's point of view, as well as the ethics, laws and consequences of cyber war and how computer criminal law may change as a result. Logical, physical, and psychological weapons used in cyber warfare are discussed. This text will appeal to information security practitioners, network security administrators, computer system administrators, and security analysts. Provides concrete examples and real-world guidance on how to identify and defend your network against malicious attacks Dives deeply into relevant technical and factual information from an insider's point of view Details the ethics, laws and consequences of cyber war and how computer criminal law may change as a result

CompTIA Network+ Certification Guide makes the most complex Network+ concepts easy to understand despite having no prior knowledge. It offers exam tips in every chapter along with access to practical exercises and exam checklist that map to the exam objectives and it is the perfect study guide to help you pass CompTIA Network+ exam. Delivering up-to-the-minute coverage, COMPUTER SECURITY AND PENETRATION TESTING, Second Edition offers readers of all backgrounds and experience levels a well-researched and engaging introduction to the fascinating realm of network security. Spotlighting the latest threats and vulnerabilities, this cutting-edge text is packed with real-world examples that showcase today's most important and relevant security topics. It addresses how and why people attack computers and networks--equipping readers with the knowledge and techniques to successfully combat hackers. This edition also includes new emphasis on ethics and legal issues. The world of information security is changing every day - readers are provided with a clear differentiation between hacking myths and hacking facts. Straightforward in its approach, this comprehensive resource teaches the skills needed to go from hoping a system is secure to knowing that it is. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

Annotation ""All-in-One Is All You Need.""Get complete coverage of all the objectives on Global Information Assurance Certification's Security Essentials (GSEC) exam inside this comprehensive resource. "GSEC GIAC Security Essentials Certification All-in-One Exam Guide" provides learning objectives at the beginning of each chapter, exam tips, practice exam questions, and in-depth explanations. Designed to help you pass the exam with ease, this authoritative resource also serves as an essential on-the-job reference. COVERS ALL EXAM TOPICS, INCLUDING: Networking fundamentals Network design Authentication and access control Network security Linux and Windows Encryption Risk management Virtual machines Vulnerability control Malware Physical security Wireless technologies VoIPELECTRONIC CONTENT FEATURES: TWO PRACTICE EXAMS AUTHOR VIDEOS PDF eBook.

[Copyright: ac610deb4fcab7dfa8790b558a4ec53d](#)