

Giac Network Penetration Testing And Ethical Hacking

Recognizing the habit ways to acquire this books **Giac Network Penetration Testing And Ethical Hacking** is additionally useful. You have remained in right site to start getting this info. get the Giac Network Penetration Testing And Ethical Hacking partner that we allow here and check out the link.

You could buy guide Giac Network Penetration Testing And Ethical Hacking or acquire it as soon as feasible. You could quickly download this Giac Network Penetration Testing And Ethical Hacking after getting deal. So, afterward you require the ebook swiftly, you can straight acquire it. Its hence utterly easy and appropriately fats, isnt it? You have to favor to in this freshen

Penetration Testing for Jobseekers -

Debasish Mandal 2022-04-19

Understand and Conduct Ethical Hacking and Security Assessments **KEY FEATURES** ●

Practical guidance on discovering, assessing, and mitigating web, network, mobile, and wireless vulnerabilities. ● Experimentation with Kali Linux, Burp Suite, MobSF, Metasploit and Aircrack-suite. ● In-depth explanation of topics focusing on how to crack ethical hacking interviews. **DESCRIPTION** Penetration Testing for Job Seekers is an attempt to discover the way to a spectacular career in cyber security, specifically penetration testing. This book offers a practical approach by discussing several computer and network fundamentals before delving into various penetration testing approaches, tools, and techniques. Written by a veteran security professional, this book provides a detailed look at the dynamics that form a person's career as a penetration tester. This book is divided into ten chapters and covers numerous facets of penetration testing, including web application, network, Android application, wireless penetration testing, and creating excellent penetration test reports. This book also shows how to set up an in-house hacking lab from scratch to improve your skills. A penetration tester's professional path, possibilities, average day, and day-to-day obstacles are all outlined to help readers better grasp what they may anticipate from a cybersecurity career. Using this book, readers will be able to boost their employability and job market relevance, allowing them to sprint

towards a lucrative career as a penetration tester. **WHAT YOU WILL LEARN** ● Perform penetration testing on web apps, networks, android apps, and wireless networks. ● Access to the most widely used penetration testing methodologies and standards in the industry. ● Use an artistic approach to find security holes in source code. ● Learn how to put together a high-quality penetration test report. ● Popular technical interview questions on ethical hacker and pen tester job roles. ● Exploration of different career options, paths, and possibilities in cyber security. **WHO THIS BOOK IS FOR** This book is for aspiring security analysts, pen testers, ethical hackers, anyone who wants to learn how to become a successful pen tester. A fundamental understanding of network principles and workings is helpful but not required. **TABLE OF CONTENTS** 1. Cybersecurity, Career Path, and Prospects 2. Introduction to Penetration Testing 3. Setting Up Your Lab for Penetration Testing 4. Web Application and API Penetration Testing 5. The Art of Secure Source Code Review 6. Penetration Testing Android Mobile Applications 7. Network Penetration Testing 8. Wireless Penetration Testing 9. Report Preparation and Documentation 10. A Day in the Life of a Pen Tester

Eleventh Hour CISSP® - Eric Conrad

2022-12-15

Eleventh Hour CISSP®: Study Guide 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 exams for information security professionals. Over 100,000 professionals are certified worldwide with many more joining their ranks. This new Fourth Edition is aligned to cover all of the material in the most current version of the exam's Common Body of Knowledge. All eight domains are covered completely and as concisely as possible, giving you the best possible chance of acing the exam. All new Fourth 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

Official (ISC)2® Guide to the CISSP®-

ISSEP® CBK® - Susan Hansche 2005-09-29

The Official (ISC)2® Guide to the CISSP®-ISSEP® CBK® provides an inclusive analysis of all of the topics covered on the newly created CISSP-ISSEP Common Body of Knowledge. The first fully comprehensive guide to the CISSP-ISSEP CBK, this book promotes understanding of the four ISSEP domains: Information Systems Security Engineering (ISSE); Certification and Accreditation; Technical Management; and an Introduction to United States Government Information Assurance Regulations. This volume explains ISSE by comparing it to a traditional Systems Engineering model, enabling you to see the correlation of how security fits into the design and development process for information systems. It also details key points of more than 50 U.S. government policies and procedures that need to be understood in order to understand the CBK and protect U.S. government information. About the Author Susan Hansche, CISSP-ISSEP is the training director for information assurance at Nortel PEC Solutions in Fairfax, Virginia. She has more than 15 years of experience in the field and since 1998 has served as the contractor program manager of the information assurance training program for the U.S. Department of State.

Computer Security and Penetration Testing -

Alfred Basta 2013-08-15

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.

Violent Python - TJ O'Connor 2012-12-28

Violent Python shows you how to move from a theoretical understanding of offensive computing concepts to a practical implementation. Instead of relying on another attacker's tools, this book will teach you to forge your own weapons using the Python programming language. This book demonstrates how to write Python scripts to automate large-scale network attacks, extract metadata, and investigate forensic artifacts. It also shows how to write code to intercept and analyze network traffic using Python, craft and spoof wireless frames to attack wireless and Bluetooth devices, and how to data-mine popular social media websites and evade modern anti-virus. Demonstrates how to write Python scripts to automate large-scale network attacks, extract metadata, and investigate forensic artifacts Write code to intercept and analyze network traffic using Python. Craft and spoof wireless frames to attack wireless and Bluetooth devices Data-mine popular social media websites and evade modern anti-virus

CompTIA PenTest+ Certification All-in-One Exam Guide (Exam PT0-001) - Raymond Nutting
2018-12-14

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

The Art of Network Penetration Testing - Royce Davis
2020-11-19

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

Eleventh Hour CISSP - Eric Conrad
2016-11-08

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 *CompTIA Network+ Certification Guide* - Glen D. Singh 2018-12-19

This is a practical certification guide covering all the exam topics in an easy-to-follow manner backed with self-assessment scenarios for better preparation. Key Features A step-by-step guide to give you a clear understanding of the Network+ Certification Learn about network architecture, protocols, security, and network troubleshooting Confidently ace the N10-007 exam with the help of practice tests Book Description CompTIA certified professionals have always had the upper hand in the information technology industry. This book will be your ideal guide to efficiently passing and achieving this certification. Learn from industry experts and implement their practices to resolve complex IT issues. This book revolves around networking concepts where readers will learn topics like network architecture, security, network monitoring, and troubleshooting. This book will not only prepare the readers conceptually but will also help them pass the N10-007 exam. This guide will also provide practice exercise after every chapter where readers can ensure their concepts are clear. By the end of this book, readers will leverage this guide and the included practice questions to boost their confidence in appearing for the actual certificate. What you will learn Explain the purpose of a variety of networking concepts and implement them appropriately Understand physical security and common attacks while

securing wired and wireless networks Understand the fundamentals of IPv4 and IPv6 Determine and explain the appropriate cabling, device, and storage technologies Understand network troubleshooting methodology and appropriate tools to support connectivity and performance Use best practices to manage the network, determine policies, and ensure business continuity Who this book is for This book is ideal for readers wanting to pass the CompTIA Network+ certificate. Rookie network engineers and system administrators interested in enhancing their networking skills would also benefit from this book. No Prior knowledge on networking would be needed.

Improving Your Penetration Testing Skills - Gilberto Najera-Gutierrez 2019-06-18

Penetration Testing For Dummies - Robert Shimonski 2020-03-27

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!

Cybersecurity Career Master Plan - Dr. Gerald Auger 2021-09-13

Start your Cybersecurity career with expert advice on how to get certified, find your first job, and progress Key Features Learn how to follow

your desired career path that results in a well-paid, rewarding job in cybersecurity

Explore expert tips relating to career growth and certification options

Access informative content from a panel of experienced cybersecurity experts

Book Description Cybersecurity is an emerging career trend and will continue to become increasingly important. Despite the lucrative pay and significant career growth opportunities, many people are unsure of how to get started. This book is designed by leading industry experts to help you enter the world of cybersecurity with confidence, covering everything from gaining the right certification to tips and tools for finding your first job. The book starts by helping you gain a foundational understanding of cybersecurity, covering cyber law, cyber policy, and frameworks. Next, you'll focus on how to choose the career field best suited to you from options such as security operations, penetration testing, and risk analysis. The book also guides you through the different certification options as well as the pros and cons of a formal college education versus formal certificate courses. Later, you'll discover the importance of defining and understanding your brand. Finally, you'll get up to speed with different career paths and learning opportunities. By the end of this cyber book, you will have gained the knowledge you need to clearly define your career path and develop goals relating to career progression. What you will learn

Gain an understanding of cybersecurity essentials, including the different frameworks and laws, and specialties

Find out how to land your first job in the cybersecurity industry

Understand the difference between college education and certificate courses

Build goals and timelines to encourage a work/life balance while delivering value in your job

Understand the different types of cybersecurity jobs available and what it means to be entry-level

Build affordable, practical labs to develop your technical skills

Discover how to set goals and maintain momentum after landing your first cybersecurity job

Who this book is for

This book is for college graduates, military veterans transitioning from active service, individuals looking to make a mid-career switch, and aspiring IT professionals. Anyone who considers cybersecurity as a potential career

field but feels intimidated, overwhelmed, or unsure of where to get started will also find this book useful. No experience or cybersecurity knowledge is needed to get started.

Professional Penetration Testing - Thomas Wilhelm 2013-06-27

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

Hacking For Dummies - Kevin Beaver 2022-04-26

Learn to think like a hacker to secure your own systems and data

Your smartphone, laptop, and desktop computer are more important to your life and business than ever before. On top of making your life easier and more productive, they hold sensitive information that should remain private. Luckily for all of us, anyone can learn powerful data privacy and security techniques to keep the bad guys on the outside where they belong. Hacking For Dummies takes

you on an easy-to-follow cybersecurity voyage that will teach you the essentials of vulnerability and penetration testing so that you can find the holes in your network before the bad guys exploit them. You will learn to secure your Wi-Fi networks, lock down your latest Windows 11 installation, understand the security implications of remote work, and much more. You'll find out how to: Stay on top of the latest security weaknesses that could affect your business's security setup Use freely available testing tools to "penetration test" your network's security Use ongoing security checkups to continually ensure that your data is safe from hackers Perfect for small business owners, IT and security professionals, and employees who work remotely, *Hacking For Dummies* is a must-have resource for anyone who wants to keep their data safe.

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

Build your defense against web attacks with Kali Linux, including command injection flaws, crypto implementation layers, and web application security holes Key Features Know how to set up your lab with Kali Linux Discover the core concepts of web penetration testing Get the tools and techniques you need with Kali Linux Book Description *Web Penetration Testing with Kali Linux - Third Edition* shows you how to set up a lab, helps you understand the nature and mechanics of attacking websites, and explains classical attacks in great depth. This edition is heavily updated for the latest Kali Linux changes and the most recent attacks. Kali Linux shines when it comes to client-side attacks and fuzzing in particular. From the start of the book, you'll be given a thorough grounding in the concepts of hacking and penetration testing, and you'll see the tools used in Kali Linux that relate to web application hacking. You'll gain a deep understanding of classical SQL, command-injection flaws, and the many ways to exploit these flaws. Web penetration testing also needs a general overview of client-side attacks, which is rounded out by a long discussion of scripting and input validation flaws. There is also an important chapter on cryptographic implementation flaws, where we discuss the most recent problems with cryptographic layers in the networking stack. The importance of these

attacks cannot be overstated, and defending against them is relevant to most internet users and, of course, penetration testers. At the end of the book, you'll use an automated technique called fuzzing to identify flaws in a web application. Finally, you'll gain an understanding of web application vulnerabilities and the ways they can be exploited using the tools in Kali Linux. What you will learn Learn how to set up your lab with Kali Linux Understand the core concepts of web penetration testing Get to know the tools and techniques you need to use with Kali Linux Identify the difference between hacking a web application and network hacking Expose vulnerabilities present in web servers and their applications using server-side attacks Understand the different techniques used to identify the flavor of web applications See standard attacks such as exploiting cross-site request forgery and cross-site scripting flaws Get an overview of the art of client-side attacks Explore automated attacks such as fuzzing web applications Who this book is for Since this book sets out to cover a large number of tools and security fields, it can work as an introduction to practical security skills for beginners in security. In addition, web programmers and also system administrators would benefit from this rigorous introduction to web penetration testing. Basic system administration skills are necessary, and the ability to read code is a must.

Hands-On Ethical Hacking and Network Defense - Michael T. Simpson 2016-10-10

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.

Bug Bounty Hunting Essentials - Carlos A. Lozano 2018-11-30

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.

CISSP® Study Guide - Eric Conrad 2022-12-01
CISSP® Study Guide, Fourth Edition provides the latest updates on CISSP® certification, the most prestigious, globally-recognized, vendor neutral exam for information security professionals. In this new edition, readers will learn about what's included in the newest

version of the exam's Common Body of Knowledge. The eight domains are covered completely and as concisely as possible. Each domain has its own chapter, including specially designed pedagogy to help readers pass the exam. Clearly stated exam objectives, unique terms/definitions, exam warnings, learning by example, hands-on exercises, and chapter ending questions help readers fully comprehend the material. Provides the most complete and effective study guide to prepare you for passing the CISSP® exam--contains only what you need to pass the test, with no fluff! Eric Conrad 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 May 2021, and also provides tiered end-of-chapter questions for a gradual learning curve, and a complete self-test appendix

CISSP Study Guide - Eric Conrad 2015-12-08
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

The Pentester BluePrint - Phillip L. Wylie
2020-11-24

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 [Penetration Testing and Network Defense](#) - Andrew Whitaker 2006

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(R)

[Hands-On Penetration Testing with Kali NetHunter](#) - Glen D. Singh 2019-02-28

Convert Android to a powerful pentesting platform. Key Features Get up and running with Kali Linux NetHunter Connect your Android device and gain full control over Windows, OSX, or Linux devices Crack Wi-Fi passwords and gain access to devices connected over the same network collecting intellectual data Book Description Kali NetHunter is a version of the popular and powerful Kali Linux pentesting platform, designed to be installed on mobile devices. Hands-On Penetration Testing with Kali NetHunter will teach you the components of NetHunter and how to install the software. You'll also learn about the different tools included and how to optimize and use a package, obtain desired results, perform tests, and make your environment more secure. Starting with an introduction to Kali NetHunter, you will delve into different phases of the pentesting process. This book will show you how to build your penetration testing environment and set up your lab. You will gain insight into gathering intellectual data, exploiting vulnerable areas, and gaining control over target systems. As you progress through the book, you will explore the NetHunter tools available for exploiting wired and wireless devices. You will work through new ways to deploy existing tools designed to reduce the chances of detection. In the concluding chapters, you will discover tips and best practices for integrating security hardening into your Android ecosystem. By the end of this book, you will have learned to successfully use a mobile penetration testing device based on Kali NetHunter and Android to accomplish the same tasks you would traditionally, but in a smaller and more mobile form factor. What you will learn Choose and configure a hardware device to use Kali NetHunter Use various tools during pentests Understand NetHunter suite components Discover tips to effectively use a compact mobile platform Create your own Kali NetHunter-enabled device and configure it for optimal results Learn to scan and gather information from a target Explore hardware adapters for testing and auditing wireless networks and Bluetooth devices Who this book is

for Hands-On Penetration Testing with Kali NetHunter is for pentesters, ethical hackers, and security professionals who want to learn to use Kali NetHunter for complete mobile penetration testing and are interested in venturing into the mobile domain. Some prior understanding of networking assessment and Kali Linux will be helpful.

[GPEN GIAC Certified Penetration Tester All-in-One Exam Guide](#) - Raymond Nutting 2020-11-05

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 **Hands-On Ethical Hacking and Network Defense** - Michael T. Simpson 2010-03-17 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.

Hands-On Ethical Hacking and Network Defense - Nicholas Antill 2022-02-24

Cyber-terrorism and corporate espionage are increasingly common and devastating threats, making trained network security professionals more important than ever.

Wilson/Simpson/Antill's HANDS-ON ETHICAL HACKING AND NETWORK DEFENSE, 4th edition, equips you with the knowledge and skills to protect networks using the tools and techniques of an ethical hacker. The authors explore the concept of ethical hacking and its practitioners -- explaining their importance in protecting corporate and government data -- and then deliver an in-depth guide to performing security testing. Thoroughly updated, the text covers new security resources, emerging vulnerabilities and innovative methods to protect networks, mobile security considerations, computer crime laws and penalties for illegal computer hacking. A final project brings many of the concepts together in a penetration testing exercise and report. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

The Official CompTIA Security+ Self-Paced Study Guide (Exam SY0-601) - CompTIA 2020-11-12

CompTIA Security+ Study Guide (Exam SY0-601)

GSEC GIAC Security Essentials Certification All-in-One Exam Guide - Ric Messier 2013-10-30
Providing learning objectives at the beginning of each chapter; exam tips; practice exam

questions; and in-depth explanations; this comprehensive resource will help you prepare for - and pass - the Global Information Assurance Certification's Security Essentials (GSEC) exam.

--

[Kali Linux Network Scanning Cookbook](#) - Michael Hixon 2017-05-26

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.

Learn Ethical Hacking - Satish Jha 2021-04-28

About the book: This help book contains mainly non-copyright matter which is solely and exclusively larger public interest . We acknowledge the copyright of the Original Author and are grateful for their historical contribution towards educational awareness. Ethical Hacking - Overview - Hacking has been a part of computing for almost five decades and it is a very broad discipline, which covers a wide range of topics. Learn how to become an elite ethical hacker and easily hack networks, computer systems, web apps and so much ... Cybersecurity & Ethical Hacking About the author: This help book Ethical Hacking - Overview - Hacking has been a part of computing for almost five decades and it is a very broad discipline, which covers a wide range of topics.

GSEC GIAC Security Essentials Certification All-in-One Exam Guide - Ric Messier 2013-11-01

"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

Kali Linux Network Scanning Cookbook - Michael Hixon 2017-05-26

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
DetailWith 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.

Eleventh Hour CISSP - Eric Conrad 2013

This study study guide is keyed directly to the most current version of the CISSP certification exam for information security professionals. Streamlined to include only core certification information and presented for ease of last-minute studying, it highlights key concepts covered on the exam.

CISSP Study Guide - Eric Conrad 2012-08-29

Annotation This study guide is aligned to cover all of the material included in the CISSP certification exam. Each of the 10 domains has its own chapter that includes specially designed pedagogy to aid the test-taker in passing the

exam.

Advanced Penetration Testing - Wil Allsopp 2017-02-27

Build a better defense against motivated, organized, professional attacks
Advanced Penetration Testing: Hacking the World's Most Secure Networks takes hacking far beyond Kali linux and Metasploit to provide a more complex attack simulation. Featuring techniques not taught in any certification prep or covered by common defensive scanners, this book integrates social engineering, programming, and vulnerability exploits into a multidisciplinary approach for targeting and compromising high security environments. From discovering and creating attack vectors, and moving unseen through a target enterprise, to establishing command and exfiltrating data—even from organizations without a direct Internet connection—this guide contains the crucial techniques that provide a more accurate picture of your system's defense. Custom coding examples use VBA, Windows Scripting Host, C, Java, JavaScript, Flash, and more, with coverage of standard library applications and the use of scanning tools to bypass common defensive measures. Typical penetration testing consists of low-level hackers attacking a system with a list of known vulnerabilities, and defenders preventing those hacks using an equally well-known list of defensive scans. The professional hackers and nation states on the forefront of today's threats operate at a much more complex level—and this book shows you how to defend your high security network. Use targeted social engineering pretexts to create the initial compromise Leave a command and control structure in place for long-term access Escalate privilege and breach networks, operating systems, and trust structures Infiltrate further using harvested credentials while expanding control Today's threats are organized, professionally-run, and very much for-profit. Financial institutions, health care organizations, law enforcement, government agencies, and other high-value targets need to harden their IT infrastructure and human capital against targeted advanced attacks from motivated professionals. Advanced Penetration Testing goes beyond Kali linux and Metasploit and to provide you advanced pen testing for high

security networks.

The Pentester BluePrint - Phillip L. Wylie
2020-10-27

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

Cyber Weaponry - Henry Prunckun 2018-04-04

There is little doubt that cyber-space has become the battle space for confrontations. However, to conduct cyber operations, a new armory of weapons needs to be employed. No matter how many, or how sophisticated an aggressor's kinetic weapons are, they are

useless in cyber-space. This book looks at the milieu of the cyber weapons industry, as well as the belligerents who use cyber weapons. It discusses what distinguishes these hardware devices and software programs from computer science in general. It does this by focusing on specific aspects of the topic—contextual issues of why cyber-space is the new battleground, defensive cyber weapons, offensive cyber weapons, dual-use weapons, and the implications these weapons systems have for practice. Contrary to popular opinion, the use of cyber weapons is not limited to nation states; though this is where the bulk of news reporting focuses. The reality is that there isn't a sector of the political-economy that is immune to cyber skirmishes. So, this book looks at cyber weapons not only by national security agencies and the military, but also by law enforcement, and the business sector—the latter includes administrations termed non-government organisations (NGOs). This book offers study material suitable for a wide-ranging audience—students, professionals, researchers, policy officers, and ICT specialists.

Penetration Testing For Dummies - Robert Shimonski 2020-04-01

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!

Management of Information Security -

Michael E. Whitman 2018-10-03

Whitman/Mattord's **MANAGEMENT OF INFORMATION SECURITY**, Sixth Edition, equips you with an executive-level overview of information security -- as well as the tools to effectively administer it. This book offers an exceptional blend of skills and experiences to staff and manage the more secure computing environments that today's organizations need. Reflecting the latest developments from the field, it includes updated coverage of NIST, ISO and security governance along with emerging concerns like Ransomware, Cloud Computing, the Internet of Things and much more. In addition, coverage of Certified Information Systems Security Professionals (CISSP) and Certified Information Security Managers (CISM) is integrated throughout to prepare you for certification. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

Python for Offensive PenTest -

Hussam Khrais 2018-04-26

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.

Principles of Information Security -

Michael E. Whitman 2021-07-06

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.