Penetration Testing And Network Defense Pearsoncmg

Cyber Security
Cyber Security
Mastering Kali Linux for Advanced Penetration Testing
A Beginner's Guide to Learn Penetration Testing to Protect Your Family and Business from Cyber Attacks Building a Home Security System for Wireless Network Security
Penetration Testing
Penetration Testing For Dummies
Hands-On Ethical Hacking and Network Defense
Quick Start to HACKING
Web Penetration Testing with Kali Linux
Testing and Analyzing Using Open Source and Low-Cost Tools
Guide to Network Defense and Countermeasures
A Beginner's Guide to Computer and Wireless Networks Defense Strategies, Penetration Testing and Information Security Risk Assessment
Leveraging Big Data for Predictive Analysis
Penetration Testing and Cisco Network Defense
Building Virtual Pentesting Labs for Advanced Penetration Testing
Building Virtual Pentesting Labs for Advanced Penetration Testing - Second Edition
Penetration Testing Fundamentals
Build your defense against complex attacks
Attack and Defense with Python 3
Hacking with Kali Linux
This Book Includes: Hacking with Kali Linux, Ethical Hacking. Learn How to Manage Cyber Risks Using Defense Strategies and Penetration Testing for Information Systems Security
A Hands-On Guide to Reliable Security Audits
Understanding Network Hacks
A Step-by-Step Guide
The Complete Guide to Understanding Wireless Technology, Network Security and Mastering Communication Systems. Includes Simples Approach to Learn Hacking Basics and Kali Linux.
Infrastructure security with Red Team and Blue Team tactics
Cybersecurity ??? Attack and Defense Strategies
Hands-On Ethical Hacking and Network Defense
Red Team Testing
Applied Network Security
Metasploit Revealed: Secrets of the Expert Pentester
Ethical Hacking
Hands-On Ethical Hacking and Network Defense, Loose-leaf Version
Implementing Cisco IOS Network Security (IINS)
Hacking with Kali Linux
The Network Security Test Lab
Offensive Security Techniques for Network Defense
Hands-On Ethical Hacking and Network Defense

A Practical Guide to Hacking, Wireless Network, Penetration Testing and Network Defense (CCNA Security exam 640-553) (Authorized Self-Study Guide)

HEATH HINES

Cyber Security Pearson IT Certification
Network Performance Security: Testing and Analyzing Using Open Source and Low-Cost Tools gives mid-level IT engineers the practical tips and tricks they need to use the best open source or low cost tools available to harden their IT infrastructure. The book details how to use the tools and how to interpret them. Network Performance Security: Testing and Analyzing Using Open Source and Low-Cost Tools begins with an overview of best practices for testing security and performance across devices and the network. It then shows how to document assets—such as servers, switches, hypervisor hosts, routers, and firewalls—using publicly available tools for network inventory. The book explores security zoning the network, with an emphasis on isolated entry points for various classes of access. It shows how to use open source tools to test network configurations for malware attacks, DDoS, botnet, rootkit and worm attacks, and concludes with tactics on how to prepare and execute a mediation schedule of the who, what, where, when, and how, when an attack hits. Network security is a requirement for any modern IT infrastructure. Using Network Performance Security: Testing and Analyzing Using Open Source and Low-Cost Tools makes the network stronger by using a layered approach of practical advice and good testing practices. Offers coherent, consistent guidance for those tasked with securing the network within an organization and ensuring that it is appropriately tested Focuses on practical, real world implementation and testing Employs a vetted "security testing by example" style to demonstrate best practices and minimize false positive testing Gives practical advice for securing BYOD devices on the network, how to test and defend against internal threats, and how to continuously validate a firewall device, software, and configuration Provides analysis in addition to step by step methodologies
Cyber Security Syngress
Master the art of detecting and averting advanced network security attacks and techniques About This Book Deep dive into the advanced network security attacks and techniques by leveraging tools such as Kali Linux 2, MetaSploit, Nmap, and Wireshark Become an expert in cracking WiFi passwords, penetrating anti-virus networks, sniffing the network, and USB hacks This step-by-step guide shows you how to confidently and quickly detect vulnerabilities for your network before the hacker does Who This Book Is For This book is for network security professionals, cyber security professionals, and Pentesters who are well versed with fundamentals of network security and now want to master it. So whether you're a cyber security professional, hobbyist, business manager, or student aspiring to becoming an ethical hacker or just want to learn more about the cyber security aspect of the IT industry, then this book is definitely for you. What You Will Learn Use SET to clone webpages including the login page Understand the concept of Wi-Fi cracking and use PCAP file to obtain passwords Attack using a USB as payload injector Familiarize yourself with the process of trojan attacks Use Shodan to identify honeypots, rogue access points, vulnerable webcams, and other exploits found in the database Explore various tools for wireless penetration testing and auditing Create an evil twin to intercept network traffic Identify human patterns in networks attacks In Detail Computer networks are increasing at an exponential rate and the most challenging factor organisations are currently facing is network security. Breaching a network is not considered an ingenious effort anymore, so it is very important to gain expertise in securing your network. The book begins by showing you how to identify malicious network behaviour and improve your wireless security. We will teach you what network sniffing is, the various tools associated with it, and how to scan for vulnerable wireless networks. Then we'll show you how attackers hide the payloads and bypass the victim's antivirus. Furthermore, we'll teach you how to spoof IP / MAC address and perform an SQL injection attack and prevent it on your website. We will create an evil twin and demonstrate how to intercept network traffic. Later, you will get familiar with Shodan and Intrusion Detection and will explore the features and tools associated with it. Toward the end, we cover tools such as Yardstick, Ubertooth, Wifi Pineapple, and Alfa used for wireless penetration testing and auditing. This book will show the tools and platform to ethically hack your own network whether it is for your business or for your personal home Wi-Fi. Style and approach This mastering-level guide is for all the security professionals who are eagerly waiting to master network security skills and protecting their organization with ease. It contains practical scenarios on various network security attacks and will teach you how to avert these attacks.
Mastering Kali Linux for Advanced Penetration Testing Cengage Learning
Do you feel that informatics is indispensable in today's increasingly digital world? Do you want to introduce yourself to the world of hacking? Do you want to have a head start in the job market by learning some of the most important future skills? If the answer to these questions is yes, then keep reading... Maybe you feel that Ethical Hacking will be a very valuable skill in the future, or maybe you simply think you'll have fun. If you want to teach yourself actual hacking (not just copy pasting a virus or a similar non-industry kind of hacking), then this is the book for you! First of all, we'll need to look at what an ethical hacker actually is. This book is filled with reasons why you should learn ethical hacking, as well as a few helpful tutorials to help you learn in the quickest way. This book assumes no programming knowledge at the start, so we'll be teaching you from the ground up. After all, you can't really teach yourself all that well if you don't have the fundamentals set. Ethical hacking can be, and for many people is, an extremely lucrative career to be enjoyed. The first thing you probably think of when you hear the word hackers is a criminal that works via the Internet. However, this book is here to teach you that there's more to it than meets the eye. Within these pages, you'll find a true trove of information and learn not only the raw theory, but also some practical applications. Here's a sneak peek of what you'll learn with this book: - What Ethical Hacking is (roles and responsibilities of an Ethical Hacker) - Hacking as a career - Making money freelance - Most common security tools - The three ways to scan your system - The seven proven penetration testing strategies ...and much more. Arm yourself with all this knowledge! Scroll to the top of the page and select the BUY NOW button!

A Beginner's Guide to Learn Penetration Testing to Protect Your Family and Business from Cyber Attacks Building a Home Security System for Wireless Network Security Springer Nature
Exploit the secrets of Metasploit to master the art of penetration testing. About This Book Discover techniques to integrate Metasploit with the industry's leading tools Carry out penetration testing in highly-secured environments with Metasploit and acquire skills to build your defense against organized and complex attacks Using the Metasploit framework, develop exploits and generate modules for a variety of real-world scenarios Who This Book Is For This course is for penetration testers, ethical hackers, and security professionals who'd like to master the Metasploit framework and explore approaches to carrying out advanced penetration testing to build highly secure networks. Some familiarity with networking and security concepts is expected, although no familiarity of Metasploit is required. What You Will Learn Get to know the absolute basics of the Metasploit framework so you have a strong foundation for advanced attacks Integrate and use various supporting tools to make Metasploit even more powerful and precise Test services such as databases, SCADA, and many more Attack the client side with highly advanced techniques Test mobile and tablet devices with Metasploit Understand how to Customize Metasploit modules and modify existing exploits Write simple yet powerful Metasploit automation scripts Explore steps involved in post-exploitation on Android and mobile platforms In Detail Metasploit is a popular penetration testing framework that has one of the largest exploit databases around. This book will show you exactly how to prepare yourself against the attacks you will face every day by simulating real-world possibilities. This learning path will begin by introducing you to Metasploit and its functionalities. You will learn how to set up and configure Metasploit on various platforms to create a virtual test environment. You will also get your hands on various tools and components and get hands-on experience with carrying out client-side attacks. In the next part of this learning path, you'll develop the ability to perform testing on various services such as SCADA, databases, IoT, mobile, tablets, and many more services. After this training, we jump into real-world sophisticated scenarios where performing penetration tests are a challenge. With real-life case studies, we take you on a journey through client-side attacks using Metasploit and various scripts built on the Metasploit framework. The final instalment of your learning journey will be covered through a bootcamp approach. You will be able to bring together the learning together and speed up and integrate Metasploit with leading industry tools for penetration testing. You'll finish by working on challenges based on user's preparation and work towards solving the challenge. The course provides you with highly practical content explaining Metasploit from the following Packt books: Metasploit for Beginners Mastering Metasploit, Second Edition Metasploit Bootcamp Style and approach This pragmatic learning path is packed with start-to-end instructions from getting started with Metasploit to effectively building new things and solving real-world examples. All the key concepts are explained with the help of examples and demonstrations that will help you understand everything to use this essential IT power tool.
Penetration Testing John Wiley & Sons
Penetration testers simulate cyber attacks to find security weaknesses in networks, operating systems, and applications. Information security experts worldwide use penetration techniques to evaluate enterprise defenses. In Penetration Testing, security expert, researcher, and trainer Georgia Weidman introduces you to the core skills and techniques that every pentester needs. Using a virtual machine–based lab that includes Kali Linux and vulnerable operating systems, you'll run through a series of practical lessons with tools like Wireshark, Nmap, and Burp Suite. As you follow along with the labs and launch attacks, you'll experience the key stages of an actual assessment—including information gathering, finding exploitable vulnerabilities, gaining access to systems, post exploitation, and more. Learn how to: –Crack passwords and wireless network keys with brute-forcing and wordlists –Test web applications for vulnerabilities –Use the Metasploit Framework to launch exploits and write your own Metasploit modules –Automate social-engineering attacks –Bypass antivirus software –Turn access to one machine into total control of the enterprise in the post exploitation phase You'll even explore writing your own exploits. Then it's on to mobile hacking—Weidman's particular area of research—with her tool, the Smartphone Pentest Framework. With its collection of hands-on lessons that cover key tools and strategies, Penetration Testing is the introduction that every aspiring hacker needs.
Penetration Testing For Dummies Zach Codings
How do I secure my computer? What is malware and how do I get rid of it? Do I only need to worry about Phishing attacks via email? What if my personal email account, bank account, or other accounts were compromised? Sounds familiar? Keep reading... Cybersecurity has changed significantly in the past decade, we've moved away from the days when basic virus protection and security controls were sufficient to deter threats, to the need for advanced security analytics tools to prevent advanced persistent threats (APTs) and tackle malicious insiders. This book includes: Hacking with Kali Linux: A Beginner's Guide to Learn Penetration Testing to Protect Your Family and Business from Cyber Attacks Building a Home Security System for Wireless Network Security Here's a sneak peek of what you'll learn with this book: What is hacking The importance of cybersecurity How malware and cyber-attacks operate How to install Kali Linux on a virtual box How to scan networks VPNs & Firewalls An introduction to Digital Signatures and Cryptography and much more... Ethical Hacking: A Beginner's Guide to Computer and Wireless Networks Defense Strategies, Penetration Testing and Information Security Risk Assessment Throughout these pages, you will learn: Roles and responsibilities of an Ethical Hacker Hacking as a career Making money freelance Most common security tools The three ways to scan your system The seven proven penetration testing strategies and much more... Even if you aren't a security expert, there are a few basic steps you can take to secure your computer. Arm yourself with all this knowledge! Scroll up and click the BUY NOW BUTTON!
Hands-On Ethical Hacking and Network Defense Cengage Learning
Do you have a big interest in computers and how they work?Are you interested in learning how to become a hacker?Would you like to learn all of this in a safe and secure manner that can make life easier? If your answer is yes, then look no further. This book will take you down that road! ''Computer Networking - All in One '' Includes the 4 best computer guides of recent years: Computer Networking First-Step (Book 1)An Introductory Guide to Understanding Wireless and Cloud Technology, Basic Communications Services and Network Security for Beginners Here is a summarized version of all the key points which have been mentioned in this book: Different aspects of wireless networks, their applications, and importance A brief introduction to the world of internet

Ways in which you can deal with the common security threats and troubleshooting your Wi-Fi connection Strategies to secure your network from all types of breaches Some common types of wireless networks And Much More... Computer Networking First-Step (Book 2)A Beginner's Guide to Understanding Computer Architecture and Mastering Communications System Including Cisco, CCNA, CCENT, and the OSI Model Some of the topics that we are going to explain will include: A look at some of the different types of certifications that you can use when it is time to handle this process and gain a deep understanding of computer networking. A look at some of the basics of the OSI method, and how we are able to use this for our own needs as well. A discussion on why network security is so important, especially when you are working with a rather large network in the first place. And Much More.. Hacking For Beginners A Step-By-Step Guide to Learn the Concept of Ethical Hacking; How to Use the Essential Hacking Command-Line, Penetration Testing and Basic Security for Your First Hack The book covers the following topics: The essentials of hacking. The role of programming and the various programming languages that play a crucial role in hacking have been appreciably examined, particularly Python. Protection of oneself while undertaking a hacking routine has also been given significant consideration. And Much More... Hacking with Kali Linux A Beginner's Guide to Learning All the Basics of Kali Linux and Cyber Security: Includes Network Defense Strategies, Penetration Testing, and Hacking Tools for Computer. Additionally, you can expect the following from this book: Introduction to Kali Linux Kali Tools Penetration Testing The basics of cybersecurity Wireless network hacking Analyzing and managing networks And Much More... "Computer Networking - All in One" contains all the knowledge you need to achieve your goals in the computer world. All you have to do is scroll up and click on the Buy Now button!

Quick Start to HACKING Packt Publishing Ltd

Drawing upon years of practical experience and using numerous examples and illustrative case studies, Threat Forecasting: Leveraging Big Data for Predictive Analysis discusses important topics, including the danger of using historic data as the basis for predicting future breaches, how to use security intelligence as a tool to develop threat forecasting techniques, and how to use threat data visualization techniques and threat simulation tools. Readers will gain valuable security insights into unstructured big data, along with tactics on how to use the data to their advantage to reduce risk. Presents case studies and actual data to demonstrate threat data visualization techniques and threat simulation tools Explores the usage of kill chain modelling to inform actionable security intelligence Demonstrates a methodology that can be used to create a full threat forecast analysis for enterprise networks of any size

Web Penetration Testing with Kali Linux Independently Published

Penetration Testing and Network DefensePearson Education

Testing and Analyzing Using Open Source and Low-Cost Tools Packt Pub Limited

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.

Guide to Network Defense and Countermeasures Packt Publishing Ltd

Implementing Cisco IOS Network Security (IINS) is a Cisco-authorized, self-paced learning tool for CCNA® Security foundation learning. This book provides you with the knowledge needed to secure Cisco® routers and switches and their associated networks. By reading this book, you will gain a thorough understanding of how to troubleshoot and monitor network devices to maintain integrity, confidentiality, and availability of data and devices, as well as the technologies that Cisco uses in its security infrastructure. This book focuses on the necessity of a comprehensive security policy and how it affects the posture of the network. You will learn how to perform basic tasks to secure a small branch type office network using Cisco IOS® security features available through the Cisco Router and Security Device Manager (SDM) web-based graphical user interface (GUI) and through the command-line interface (CLI) on Cisco routers and switches. The author also provides, when appropriate, parallels with Cisco ASA appliances. Whether you are preparing for CCNA Security certification or simply want to gain a better understanding of Cisco IOS security fundamentals, you will benefit from the information provided in this book. Implementing Cisco IOS Network Security (IINS) is part of a recommended learning path from Cisco that includes simulation and hands-on training from authorized Cisco Learning Partners and self-study products from Cisco Press. To find out more about instructor-led training, e-learning, and hands-on instruction offered by authorized Cisco Learning Partners worldwide, please visit www.cisco.com/go/authorizedtraining. Develop a comprehensive network security policy to counter threats against information security Configure routers on the network perimeter with Cisco IOS Software security features Configure firewall features including ACLs and Cisco IOS zone-based policy firewalls to perform basic security operations on a network Configure site-to-site VPNs using Cisco IOS features Configure IPS on Cisco network routers Configure LAN devices to control access, resist attacks, shield other network devices and systems, and protect the integrity and confidentiality of network traffic This volume is in the Certification Self-Study Series offered by Cisco Press®. Books in this series provide officially developed self-study solutions to help networking professionals understand technology implementations and prepare for the Cisco Career Certifications examinations.

A Beginner's Guide to Computer and Wireless Networks Defense Strategies, Penetration Testing and Information Security Risk Assessment Simon and Schuster

Are you interested in learning how to become a hacker? If your answer is yes, then look no further. This book will take you down that road. This book is going to teach you how hackers reason. Besides understanding the reasons why a hacker would target your computer, you will also get to know how they are able to do it and even how you can safeguard your systems, equipment, and network against hacking attacks. Keen readers will, by the end of this book, understand how their systems work, how to scan, and how to gain access to your computer. The book has been structured in 11

chapters that will each teach you something new in matters hacking with Kali Linux. Concepts have been simplified. By the time you come to the end of this book, you will have mastered the basics of computer hacking alongside a number of advanced concepts in social engineering attack mechanisms. The book is truly a template for everyone who intends to understand hacking. Additionally, you can expect the following from this book: Introduction to Kali Linux The Basics of Hacking and Using Kali Linux Kali Tools Penetration Testing The process of ethical hacking How to scanning devices in a network What are cyber attacks The basics of cybersecurity Vulnerability assessments Wireless network hacking Analyzing and managing networks Penetration Testing Plenty of books about Hacking with Kali Linux do not cover crucial concepts in a satisfactory fashion. Let me say again that nothing has been left out by this book. Grab yourself a copy of this book, and you will get to discover interesting stuff about hacking using Kali Linux. The book will provide you a platform to be better student, security administrator, or penetration tester. You will also find out how you can protect your computer from all the hacker's attacks!Scroll up and click BUY NOW button!

Leveraging Big Data for Predictive Analysis Syngress

Social engineering attacks target the weakest link in an organization's security human beings. Everyone knows these attacks are effective, and everyone knows they are on the rise. Now, Social Engineering Penetration Testing gives you the practical methodology and everything you need to plan and execute a social engineering penetration test and assessment. You will gain fascinating insights into how social engineering techniques including email phishing, telephone pretexting, and physical vectors can be used to elicit information or manipulate individuals into performing actions that may aid in an attack. Using the book's easy-to-understand models and examples, you will have a much better understanding of how best to defend against these attacks. The authors of Social Engineering Penetration Testing show you hands-on techniques they have used at RandomStorm to provide clients with valuable results that make a real difference to the security of their businesses. You will learn about the differences between social engineering pen tests lasting anywhere from a few days to several months. The book shows you how to use widely available open-source tools to conduct your pen tests, then walks you through the practical steps to improve defense measures in response to test results. Understand how to plan and execute an effective social engineering assessment Learn how to configure and use the open-source tools available for the social engineer Identify parts of an assessment that will most benefit time-critical engagements Learn how to design target scenarios, create plausible attack situations, and support various attack vectors with technology Create an assessment report, then improve defense measures in response to test results

Penetration Testing and Cisco Network Defense Course Technology

Have You Ever Wanted To Be A Hacker? Or Do You Simply Crave To Keep Yourself Updated With The Latest Technologies And Penetrating Techniques? If yes, then, Quick Start to HACKING is the right book. This book presents proven and practical step-by-step guides on... * Computers and Smartphones hacking * How to use Kali Linux * Penetration Testing * How to attack networks, corrupt systems and evade anti-viruses * How to Identify Vulnerabilities in websites and Applications * Simple Vulnerability Assessment and Exploitation tools This book provides you with detailed basic hacking resources and gets you exposed to the latest secret techniques of professional hackers.Enjoy limitless opportunities and benefits that this book offers by simply clicking on the DOWNLOAD Button

Building Virtual Pentesting Labs for Advanced Penetration Testing Cengage Learning

Learn how to build complex virtual architectures that allow you to perform virtually any required testing methodology and perfect itAbout This Book- Explore and build intricate architectures that allow you to emulate an enterprise network- Test and enhance your security skills against complex and hardened virtual architecture- Learn methods to bypass common enterprise defenses and leverage them to test the most secure environments.Who This Book Is ForWhile the book targets advanced penetration testing, the process is systematic and as such will provide even beginners with a solid methodology and approach to testing.You are expected to have network and security knowledge. The book is intended for anyone who wants to build and enhance their existing professional security and penetration testing methods and skills.What You Will Learn - Learning proven security testing and penetration testing techniques- Building multi-layered complex architectures to test the latest network designs- Applying a professional testing methodology- Determining whether there are filters between you and the target and how to penetrate them- Deploying and finding weaknesses in common firewall architectures.- Learning advanced techniques to deploy against hardened environments- Learning methods to circumvent endpoint protection controls In DetailSecurity flaws and new hacking techniques emerge overnight - security professionals need to make sure they always have a way to keep . With this practical guide, learn how to build your own virtual pentesting lab environments to practice and develop your security skills. Create challenging environments to test your abilities, and overcome them with proven processes and methodologies used by global penetration testing teams.Get to grips with the techniques needed to build complete virtual machines perfect for pentest training. Construct and attack layered architectures, and plan specific attacks based on the platforms you're going up against. Find new vulnerabilities for different kinds of systems and networks, and what these mean for your clients.Driven by a proven penetration testing methodology that has trained thousands of testers, Building Virtual Labs for Advanced Penetration Testing, Second Edition will prepare you for participation in professional security teams. Style and approach The book is written in an easy-to-follow format that provides a step-by-step, process-centric approach. Additionally, there are numerous hands-on examples and additional references for readers who might want to learn even more. The process developed throughout the book has been used to train and build teams all around the world as professional security and penetration testers.

Building Virtual Pentesting Labs for Advanced Penetration Testing - Second Edition Syngress

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.

Penetration Testing Fundamentals Packt Publishing Ltd

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.

Build your defense against complex attacks Packt Publishing Ltd

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.

Attack and Defense with Python 3 Elsevier

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

Hacking with Kali Linux Syngress

Employ the most advanced pentesting techniques and tools to build highly-secured systems and environments About This Book Learn how to build your own pentesting lab environment to practice advanced techniques Customize your own scripts, and learn methods to exploit 32-bit and 64-bit programs Explore a vast variety of stealth techniques to bypass a number of protections when penetration testing Who This Book Is For This book is for anyone who wants to improve their skills in penetration testing. As it follows a step-by-step approach, anyone from a novice to an experienced security tester can learn effective techniques to deal with highly secured environments. Whether you are brand new or a seasoned expert, this book will provide you with the skills you need to successfully create, customize, and plan an advanced penetration test. What You Will Learn A step-by-step methodology to identify and penetrate secured environments Get to know the process to test network services across enterprise architecture when defences are in place Grasp different web application testing methods and how to identify web application protections that are deployed Understand a variety of concepts to exploit software Gain proven post-exploitation techniques to exfiltrate data from the target Get to grips with various stealth techniques to remain undetected and defeat the latest defences Be the first to find out the latest methods to bypass firewalls Follow proven approaches to record and save the data from tests for analysis In Detail The defences continue to improve and become more and more common, but this book will provide you with a number or proven techniques to defeat the latest defences on the networks. The methods and techniques contained will provide you with a powerful arsenal of best practices to increase your penetration testing successes. The processes and methodology will provide you techniques that will enable you to be successful, and the step by step instructions of information gathering and intelligence will allow you to gather the required information on the targets you are testing. The exploitation and post-exploitation sections will supply you with the tools you would need to go as far as the scope of work will allow you. The challenges at the end of each chapter are designed to challenge you and provide real-world situations that will hone and perfect your penetration testing skills. You will start with a review of several well respected penetration testing methodologies, and following this you will learn a step-by-step methodology of professional security testing, including stealth, methods of evasion, and obfuscation to perform your tests and not be detected! The final challenge will allow you to create your own complex layered architecture with defences and protections in place, and provide the ultimate testing range for you to practice the methods shown throughout the book. The challenge is as close to an actual penetration test assignment as you can get! Style and approach The book follows the standard penetration testing stages from start to finish with step-by-step examples. The book thoroughly covers penetration test expectations, proper scoping and planning, as well as enumeration and foot printing

Related with Penetration Testing And Network Defense Pearsoncmg:
• Organic Chemistry Crash Course : click here