Ethical Hacking And Penetration Testing Guide By Rafay Baloch

Mastering Kali Linux for Advanced Penetration Testing
Ethical Hacking and Penetration Testing Guide
Hacking
The Ethical Hack
Hacking with Kali Linux
Ethical Hacker’s Penetration Testing Guide
Hacking
Kali Linux - An Ethical Hacker's Cookbook
Kali Linux - An Ethical Hacker's Cookbook
Building a Pentesting Lab for Wireless Networks
Ethical Hacker's Certification Guide (CEHv11)
Ethical Hacking
Web Penetration Testing with Kali Linux
Einstieg in Kali Linux
AWS Penetration Testing

Ethical Hacking
Penetration Testing Azure for Ethical Hackers
Hacking and Penetration Testing with Low Power Devices
Hands-On Penetration Testing with Python
The Basics of Hacking and Penetration Testing
Penetration Testing For Dummies
Ethical Hacking for Beginners
Hands on Hacking
The Basics of Hacking and Penetration Testing
Hacking For Beginners
Ethical Hacking for Beginners
Python Ethical Hacking from Scratch
Python for Offensive PenTest
Hacking Essentials
Ethical Hacking
Ethical Hacking and Penetration, Step by Step with Kali Linux
Web Penetration Testing with Kali Linux - Third Edition
Python Penetration Testing Essentials
The Pentester BluePrint
The Advanced Penetrating Testing

Certified Ethical Hacker (CEH) Preparation Guide
Certified Ethical Hacker Complete Training Guide with Practice Questions & Labs:
The Hacker Ethos
Learn Ethical Hacking from Scratch

KEENAN KENDALL

Mastering Kali Linux for Advanced Penetration Testing CRC Press
This book is written for those people who want to hack systems to test identify the security holes and vulnerabilities of thosesystems. This book outlines different tricks and techniques that an ethical hacker can use to assess the security of the systems, identify vulnerabilities and fix those vulnerabilities. This is done to prevent any malicious attacks against the system.The hacking we talk about in this book is professional, above board and is a legal type of testing. It is for this reason that it is called ethical hacking. Network and computer security is a complex subject, which constantly changes. You have to stay on top of it to ensure that the information you own is secure from the crackers or criminal hackers.Ethical hacking, also called white-hat hacking or penetration testing, is a tool that will help you ensure that the information system you use is truly secure. Over the course of this book, you

will gather information on the different tools and software you can use to run an ethical hacking program. There are some programs in this book that you can use to start off the ethical hacking process.In this book you will learn: What exactly is Ethical HackingThe dangers that your system can face through attacksThe Ethical Hacking Process and what it meansUnderstanding a hackers mindsetAn introduction to PythonAnd much much more!

Ethical Hacking and Penetration Testing Guide John Wiley & Sons

This book is a complete guide for those who would like to become an Ethical hacker. In this book you will learn what the Ethical hacking and its procedure is. The first couple of chapters are the definitions, concepts and process of becoming an Ethical hacker while the next half of the book will show in detail how to use certain tools and techniques to initiate attacks and penetrate a system. After reading this book, you should be able to use these tools to do some testing and even working on penetration projects. You just need to remember not to use these techniques in a production environment without having a formal approval.

Hacking John Wiley & Sons

Dive into the world of securing digital networks, cloud, IoT, mobile infrastructure, and much more. KEY FEATURES ● Courseware and practice papers with solutions for C.E.H. v11. ● Includes hacking tools, social engineering techniques, and live exercises. ● Add on coverage on Web

apps, IoT, cloud, and mobile Penetration testing. DESCRIPTION The 'Certified Ethical Hacker's Guide' summarises all the ethical hacking and penetration testing fundamentals you'll need to get started professionally in the digital security landscape. The readers will be able to approach the objectives globally, and the knowledge will enable them to analyze and structure the hacks and their findings in a better way. The book begins by making you ready for the journey of a seasonal, ethical hacker. You will get introduced to very specific topics such as reconnaissance, social engineering, network intrusion, mobile and cloud hacking, and so on. Throughout the book, you will find many practical scenarios and get hands-on experience using tools such as Nmap, BurpSuite, OWASP ZAP, etc. Methodologies like brute-forcing, wardriving, evil twining, etc. are explored in detail. You will also gain a stronghold on theoretical concepts such as hashing, network protocols, architecture, and data encryption in real-world environments. In the end, the evergreen bug bounty programs and traditional career paths for safety professionals will be discussed. The reader will also have practical tasks and self-assessment exercises to plan further paths of learning and certification. WHAT YOU WILL LEARN ● Learn methodologies, tools, and techniques of penetration testing and ethical hacking. ● Expert-led practical demonstration of tools and tricks like nmap, BurpSuite, and OWASP ZAP. ● Learn how to

perform brute forcing, wardriving, and evil twinning. ● Learn to gain and maintain access to remote systems. ● Prepare detailed tests and execution plans for VAPT (vulnerability assessment and penetration testing) scenarios. WHO THIS BOOK IS FOR This book is intended for prospective and seasonal cybersecurity lovers who want to master cybersecurity and ethical hacking. It also assists software engineers, quality analysts, and penetration testing companies who want to keep up with changing cyber risks. TABLE OF CONTENTS 1. Cyber Security, Ethical Hacking, and Penetration Testing 2. CEH v11 Prerequisites and Syllabus 3. Self-Assessment 4. Reconnaissance 5. Social Engineering 6. Scanning Networks 7. Enumeration 8. Vulnerability Assessment 9. System Hacking 10. Session Hijacking 11. Web Server Hacking 12. Web Application Hacking 13. Hacking Wireless Networks 14. Hacking Mobile Platforms 15. Hacking Clout, IoT, and OT Platforms 16. Cryptography 17. Evading Security Measures 18. Practical Exercises on Penetration Testing and Malware Attacks 19. Roadmap for a Security Professional 20. Digital Compliances and Cyber Laws 21. Self-Assessment-1 22. Self-Assessment-2

The Ethical Hack BPB Publications Have you always been curious about hacking? Have you also had a misconception about the term Ethical Hacking? Would you like to learn more about ethical hacking using a powerful operating system called Kali Linux? Do you aspire to start an ethical hacking

career someday? Then this is the right book to help you get started. This book will prove to be a valuable source of knowledge, especially when you want to learn a lot about ethical hacking in a short amount of time. This treasure trove of knowledge will teach you about the power of Kali Linux and how its tools can help you during every stage of the penetration testing lifecycle. If you want to launch yourself into the world of ethical hacking and want to use Kali Linux as the most used tool in your toolkit, this book will definitely serve as your launchpad. The book is designed to consider first time Kali Linux users and will take you through a step by step guide on how to download and install Kali Linux. The book is also designed to help existing Kali Linux users learn advanced techniques concerning the use of Kali Linux in the penetration testing lifecycle and the ethical hacking domain. The tools surrounding the Kali Linux operating system in this course will help you get a first impression of the ethical hacking profile and will also serve as a platform to launch you into the world of information security. The book will take you through: An overview of hacking Terminologies of hacking Steps to download and install Kali Linux The penetration testing lifecycle Dedicated chapters on the five stages of the penetration testing lifecycle viz. Reconnaissance, Scanning, Exploitation, Maintaining Access, and Reporting And a bonus chapter on Email Hacking The book has been designed for you to understand hacking and Kali Linux from

its foundation. You will not need to complete the entire book to start with a practical performance on Kali Linux. Every chapter of the penetration testing life cycle is a module in itself, and you will be in a position to try out the tools listed in them as you finish each chapter. There are step-by-step instructions and code snippets throughout the book that will help you get your hands dirty on a real Kali Linux system with the completion of each chapter. So here's hoping that this book helps you find the appetite to become an ethical hacker someday soon! Click the Buy Now button to get started now.

Hacking with Kali Linux Packt Publishing Ltd

Do you want learn how to build a PenTest Lab but you don't know where to start?Do you want a practical book that explains step-by-step how to get going?Do you want to become an Ethical Hacker or PenTester?If the answer is yes to the above questions, this book is for you!Frequently Asked Questions-Question: I am new to IT, and I don't have any experience in the field of Hacking, should I get this book?-Answer: This book is designed to those interested in Penetration Testing aka Ethical Hacking, and having limited, or no experience in the realm of Cybersecurity.-Question: I am not a hacker. Are there any technical prerequisites for reading this book?-Answer: No. This book is written in everyday English, and no technical experience required.-Question: I have been reading similar books before, but I

am still not sure if I should buy this book. How do I know this book is any good?- Answer: This book is written by a Security Architect, having over a decade of experience on platforms such as: Cisco Systems, Checkpoint, Palo Alto, Brocade, Back Track / Kali Linux, RedHat Linux, CentOS, Orion, Prime, DLP, IPS, IDS, Nexus, and much more... Learning from someone with real life experience is extremely valuable. You will learn about real life technologies and methodologies used in today's IT Infrastructure, and Cybersecurity Division.BUY THIS BOOK NOW, AND GET STARTED TODAY!IN THIS BOOK YOU WILL LEARN: What are the Foundations of Penetration TestingWhat are the Benefits of Penetration TestingWhat are the Frameworks of Penetration TestingWhat Scanning Tools you should be AwareWhat Credential Testing Tools you must UtilizeWhat Debugging & Software Assurance Tools are AvailableIntroduction to OSINT & Wireless ToolsWhat is a Web Proxy, SET & RDPWhat Mobile Tools you should be familiar withHow Communication must take placeHow to Cover your BackHow to Setup a Lab in NPEHow to Setup Hyper-V on Windows 10How to Setup VMware on Windows 10How to Assemble the Required ResourcesHow to Install Windows Server in VMwareHow to Configure Windows Server in VMwareHow to Install Windows Server in Hyper-VHow to Configure Windows Server in Hyper-VHow to Install & Configure OWASP-BWA in VMwareHow to Install & Configure Metasploitable in VMwareHow to Install Kali Linux in

VMwareHow to Install BlackArch in Hyper-VWhat Categories of Penetration Tests existsWhat Software & Hardware you must have as a PenTesterUnderstanding ConfidentialityWhat are the Rules of EngagementHow to set Objectives & DeliverablesWhat Type of Targets you must deal withSpecialized Systems for Pen TestersHow to Identify & Response to RiskHow to Prepare your Pen Test Team for an EngagementWhat are the Best Practices before Going LiveBUY THIS BOOK NOW, AND GET STARTED TODAY

Ethical Hacker's Penetration Testing Guide Createspace Independent

Build your defense against web attacks with Kali Linux, including command injection flaws, crypto implementation layers, and web application security holes Key Features Know how to set up your lab with Kali Linux Discover the core concepts of web penetration testing Get the tools and techniques you need with Kali Linux Book Description Web Penetration Testing with Kali Linux - Third Edition shows you how to set up a lab, helps you understand the nature and mechanics of attacking websites, and explains classical attacks in great depth. This edition is heavily updated for the latest Kali Linux changes and the most recent attacks. Kali Linux shines when it comes to client-side attacks and fuzzing in particular. From the start of the book, you'll be given a thorough grounding in the concepts of hacking and penetration testing, and you'll see the tools used in Kali Linux that relate to

web application hacking. You'll gain a deep understanding of classicalSQL, command-injection flaws, and the many ways to exploit these flaws. Web penetration testing also needs a general overview of client-side attacks, which is rounded out by a long discussion of scripting and input validation flaws. There is also an important chapter on cryptographic implementation flaws, where we discuss the most recent problems with cryptographic layers in the networking stack. The importance of these attacks cannot be overstated, and defending against them is relevant to most internet users and, of course, penetration testers. At the end of the book, you'll use an automated technique called fuzzing to identify flaws in a web application. Finally, you'll gain an understanding of web application vulnerabilities and the ways they can be exploited using the tools in Kali Linux. What you will learn Learn how to set up your lab with Kali Linux Understand the core concepts of web penetration testing Get to know the tools and techniques you need to use with Kali Linux Identify the difference between hacking a web application and network hacking Expose vulnerabilities present in web servers and their applications using server-side attacks Understand the different techniques used to identify the flavor of web applications See standard attacks such as exploiting cross-site request forgery and cross-site scripting flaws Get an overview of the art of client-side attacks Explore automated attacks such as fuzzing web applications Who this

book is for Since this book sets out to cover a large number of tools and security fields, it can work as an introduction to practical security skills for beginners in security. In addition, web programmers and also system administrators would benefit from this rigorous introduction to web penetration testing. Basic system administration skills are necessary, and the ability to read code is a must.

Hacking Independently Published Simulate real-world attacks using tactics, techniques, and procedures that adversaries use during cloud breaches Key FeaturesUnderstand the different Azure attack techniques and methodologies used by hackersFind out how you can ensure end-to-end cybersecurity in the Azure ecosystemDiscover various tools and techniques to perform successful penetration tests on your Azure infrastructureBook Description “If you're looking for this book, you need it.” — 5* Amazon Review Curious about how safe Azure really is? Put your knowledge to work with this practical guide to penetration testing. This book offers a no-faff, hands-on approach to exploring Azure penetration testing methodologies, which will get up and running in no time with the help of real-world examples, scripts, and ready-to-use source code. As you learn about the Microsoft Azure platform and understand how hackers can attack resources hosted in the Azure cloud, you'll find out how to protect your environment by identifying vulnerabilities, along with

extending your pentesting tools and capabilities. First, you'll be taken through the prerequisites for pentesting Azure and shown how to set up a pentesting lab. You'll then simulate attacks on Azure assets such as web applications and virtual machines from anonymous and authenticated perspectives. In the later chapters, you'll learn about the opportunities for privilege escalation in Azure tenants and ways in which an attacker can create persistent access to an environment. By the end of this book, you'll be able to leverage your ethical hacking skills to identify and implement different tools and techniques to perform successful penetration tests on your own Azure infrastructure. What you will learnIdentify how administrators misconfigure Azure services, leaving them open to exploitationUnderstand how to detect cloud infrastructure, service, and application misconfigurationsExplore processes and techniques for exploiting common Azure security issuesUse on-premises networks to pivot and escalate access within AzureDiagnose gaps and weaknesses in Azure security implementationsUnderstand how attackers can escalate privileges in Azure ADWho this book is for This book is for new and experienced infosec enthusiasts who want to learn how to simulate real-world Azure attacks using tactics, techniques, and procedures (TTPs) that adversaries use in cloud breaches. Any technology professional working with the Azure platform

(including Azure administrators, developers, and DevOps engineers) interested in learning how attackers exploit vulnerabilities in Azure hosted infrastructure, applications, and services will find this book useful.

Kali Linux - An Ethical Hacker's Cookbook
Packt Publishing Ltd
There are many books that detail tools and techniques of penetration testing, but none of these effectively communicate how the information gathered from tests should be analyzed and implemented. Until recently, there was very little strategic information available to explain the value of ethical hacking and how tests should be performed in order t

Kali Linux - An Ethical Hacker's Cookbook
John Wiley & Sons
Implement defensive techniques in your ecosystem successfully with Python Key FeaturesIdentify and expose vulnerabilities in your infrastructure with PythonLearn custom exploit development .Make robust and powerful cybersecurity tools with PythonBook Description With the current technological and infrastructural shift, penetration testing is no longer a process-oriented activity. Modern-day penetration testing demands lots of automation and innovation; the only language that dominates all its peers is Python. Given the huge number of tools written in Python, and its popularity in the penetration testing space, this language has always been the first choice for penetration testers. Hands-On Penetration Testing with Python walks

you through advanced Python programming constructs. Once you are familiar with the core concepts, you'll explore the advanced uses of Python in the domain of penetration testing and optimization. You'll then move on to understanding how Python, data science, and the cybersecurity ecosystem communicate with one another. In the concluding chapters, you'll study exploit development, reverse engineering, and cybersecurity use cases that can be automated with Python. By the end of this book, you'll have acquired adequate skills to leverage Python as a helpful tool to pentest and secure infrastructure, while also creating your own custom exploits. What you will learnGet to grips with Custom vulnerability scanner developmentFamiliarize yourself with web application scanning automation and exploit developmentWalk through day-to-day cybersecurity scenarios that can be automated with PythonDiscover enterprise-or organization-specific use cases and threat-hunting automationUnderstand reverse engineering, fuzzing, buffer overflows , key-logger development, and exploit development for buffer overflows.Understand web scraping in Python and use it for processing web responsesExplore Security Operations Centre (SOC) use casesGet to understand Data Science, Python, and cybersecurity all under one hoodWho this book is for If you are a security consultant , developer or a cyber security enthusiast with little or no knowledge of Python and want in-depth

insight into how the pen-testing ecosystem and python combine to create offensive tools , exploits , automate cyber security use-cases and much more then this book is for you. Hands-On Penetration Testing with Python guides you through the advanced uses of Python for cybersecurity and pen-testing, helping you to better understand security loopholes within your infrastructure .

Building a Pentesting Lab for Wireless Networks Syngress

Explore the world of practical ethical hacking by developing custom network scanning and remote access tools that will help you test the system security of your organization Key Features Get hands-on with ethical hacking and learn to think like a real-life hacker Build practical ethical hacking tools from scratch with the help of real-world examples Leverage Python 3 to develop malware and modify its complexities Book DescriptionPenetration testing enables you to evaluate the security or strength of a computer system, network, or web application that an attacker can exploit. With this book, you'll understand why Python is one of the fastest-growing programming languages for penetration testing. You'll find out how to harness the power of Python and pentesting to enhance your system security. Developers working with Python will be able to put their knowledge and experience to work with this practical guide. Complete with step-by-step explanations of essential concepts and practical examples, this book takes a

hands-on approach to help you build your own pentesting tools for testing the security level of systems and networks. You'll learn how to develop your own ethical hacking tools using Python and explore hacking techniques to exploit vulnerabilities in networks and systems. Finally, you'll be able to get remote access to target systems and networks using the tools you develop and modify as per your own requirements. By the end of this ethical hacking book, you'll have developed the skills needed for building cybersecurity tools and learned how to secure your systems by thinking like a hacker.What you will learn Understand the core concepts of ethical hacking Develop custom hacking tools from scratch to be used for ethical hacking purposes Discover ways to test the cybersecurity of an organization by bypassing protection schemes Develop attack vectors used in real cybersecurity tests Test the system security of an organization or subject by identifying and exploiting its weaknesses Gain and maintain remote access to target systems Find ways to stay undetected on target systems and local networks Who this book is forIf you want to learn ethical hacking by developing your own tools instead of just using the prebuilt tools, this book is for you. A solid understanding of fundamental Python concepts is expected. Some complex Python concepts are explained in the book, but the goal is to teach ethical hacking, not Python.

Ethical Hacker's Certification Guide (CEHv11) Independently Published

The Basics of Hacking and Penetration TestingElsevier
Ethical Hacking Apress
Master key approaches used by real attackers to perform advanced pentesting in tightly secured infrastructure, cloud and virtualized environments, and devices, and learn the latest phishing and hacking techniques Key FeaturesExplore red teaming and play the hackers game to proactively defend your infrastructureUse OSINT, Google dorks, Nmap, recon-nag, and other tools for passive and active reconnaissanceLearn about the latest email, Wi-Fi, and mobile-based phishing techniquesBook Description Remote working has given hackers plenty of opportunities as more confidential information is shared over the internet than ever before. In this new edition of Mastering Kali Linux for Advanced Penetration Testing, you'll learn an offensive approach to enhance your penetration testing skills by testing the sophisticated tactics employed by real hackers. You'll go through laboratory integration to cloud services so that you learn another dimension of exploitation that is typically forgotten during a penetration test. You'll explore different ways of installing and running Kali Linux in a VM and containerized environment and deploying vulnerable cloud services on AWS using containers, exploiting misconfigured S3 buckets to gain access to EC2 instances. This book delves into passive and active reconnaissance, from obtaining user information to large-scale port scanning.

Building on this, different vulnerability assessments are explored, including threat modeling. See how hackers use lateral movement, privilege escalation, and command and control (C2) on compromised systems. By the end of this book, you'll have explored many advanced pentesting approaches and hacking techniques employed on networks, IoT, embedded peripheral devices, and radio frequencies. What you will learnExploit networks using wired/wireless networks, cloud infrastructure, and web servicesLearn embedded peripheral device, Bluetooth, RFID, and IoT hacking techniquesMaster the art of bypassing traditional antivirus and endpoint detection and response (EDR) toolsTest for data system exploits using Metasploit, PowerShell Empire, and CrackMapExecPerform cloud security vulnerability assessment and exploitation of security misconfigurationsUse bettercap and Wireshark for network sniffingImplement complex attacks with Metasploit, Burp Suite, and OWASP ZAPWho this book is for This fourth edition is for security analysts, pentesters, ethical hackers, red team operators, and security consultants wanting to learn and optimize infrastructure/application/cloud security using advanced Kali Linux features. Prior penetration testing experience and basic knowledge of ethical hacking will help you make the most of this book.

Web Penetration Testing with Kali Linux
Packt Publishing Ltd

Do you want to keep your personal data safe from prying eyes? Do you want to

look behind the scenes of major attacks and hacking incidents? Do you want to keep your own computer and the network safe from hacking attacks? The world of hacking has often gotten a bad reputation thanks to the individuals who are unscrupulous with the work they do. But there are many ethical hackers out there, those who use it to keep their own personal information safe and sound and will ensure that they can keep others safe as well. If you fit into this final group, then this guidebook is for you. It is going to contain all of the information, techniques, and methods that you need to use in order to start your own ethical hacking adventure today. Whether you want to create some of these projects for your own needs or use it to further your career in cybersecurity, this guidebook is going to have all of the information that you need to get started. Some of the different topics that we are going to explore when it comes to working in this guidebook include: The essence and key concepts behind penetration testing and ethical hacking How to map out some of the hacks that you would like to do and get a better idea of your own network or the network you would like to target How to crack passwords and why this is so important to learn more about Insidious spoofing attacks that are used to fool potential targets How penetration testers handle various network connections and what they do to get onto some, even if they don't have access How they hide and find IP addresses Other attacks that hackers like to work with including denial of

service, malware, social engineering, phishing, and more How keyloggers are created and why screenshot tools play a crucial role in it Some of the best tips and tricks that you are able to follow to ensure that your network will always remain safe and easy to use And much, much more. The world of cybersecurity is quickly changing. And being able to understand how hacking works will make it easier for you to protect your own computer network and stand out as a "cyber-savvy" employee, executive or company owner. So, if you want to deep-dive into the world of hacking and learn how to protect your information systems, then click "add to cart" now!

Einstieg in Kali Linux Packt Publishing Ltd

Over 120 recipes to perform advanced penetration testing with Kali Linux About This Book Practical recipes to conduct effective penetration testing using the powerful Kali Linux Leverage tools like Metasploit, Wireshark, Nmap, and many more to detect vulnerabilities with ease Confidently perform networking and application attacks using task-oriented recipes Who This Book Is For This book is aimed at IT security professionals, pentesters, and security analysts who have basic knowledge of Kali Linux and want to conduct advanced penetration testing techniques. What You Will Learn Installing, setting up and customizing Kali for pentesting on multiple platforms Pentesting routers and embedded devices Bug hunting 2017 Pwning and escalating through corporate network Buffer overflows 101 Auditing wireless

networks Fiddling around with software-defned radio Hacking on the run with NetHunter Writing good quality reports In Detail With the current rate of hacking, it is very important to pentest your environment in order to ensure advanced-level security. This book is packed with practical recipes that will quickly get you started with Kali Linux (version 2016.2) according to your needs, and move on to core functionalities. This book will start with the installation and configuration of Kali Linux so that you can perform your tests. You will learn how to plan attack strategies and perform web application exploitation using tools such as Burp, and Jexboss. You will also learn how to perform network exploitation using Metasploit, Sparta, and Wireshark. Next, you will perform wireless and password attacks using tools such as Patator, John the Ripper, and airoscript-ng. Lastly, you will learn how to create an optimum quality pentest report! By the end of this book, you will know how to conduct advanced penetration testing thanks to the book's crisp and task-oriented recipes. Style and approach This is a recipe-based book that allows you to venture into some of the most cutting-edge practices and techniques to perform penetration testing with Kali Linux.

AWS Penetration Testing Packt Publishing Ltd

A fast, hands-on introduction to offensive hacking techniques Hands-On Hacking teaches readers to see through the eyes of their adversary and apply hacking

techniques to better understand real-world risks to computer networks and data. Readers will benefit from the author's years of experience in the field hacking into computer networks and ultimately training others in the art of cyber-attacks. This book holds no punches and explains the tools, tactics and procedures used by ethical hackers and criminal crackers alike. We will take you on a journey through a hacker’s perspective when focused on the computer infrastructure of a target company, exploring how to access the servers and data. Once the information gathering stage is complete, you’ll look for flaws and their known exploits—including tools developed by real-world government financed state-actors. An introduction to the same hacking techniques that malicious hackers will use against an organization Written by infosec experts with proven history of publishing vulnerabilities and highlighting security flaws Based on the tried and tested material used to train hackers all over the world in the art of breaching networks Covers the fundamental basics of how computer networks are inherently vulnerable to attack, teaching the student how to apply hacking skills to uncover vulnerabilities We cover topics of breaching a company from the external network perimeter, hacking internal enterprise systems and web application vulnerabilities. Delving into the basics of exploitation with real-world practical examples, you won't find any hypothetical academic only attacks here.

From start to finish this book will take the student through the steps necessary to breach an organization to improve its security. Written by world-renowned cybersecurity experts and educators, Hands-On Hacking teaches entry-level professionals seeking to learn ethical hacking techniques. If you are looking to understand penetration testing and ethical hacking, this book takes you from basic methods to advanced techniques in a structured learning format.

Ethical Hacking Primedia E-launch LLC

The Hacker Ethos is a condensed, easy-to-read guidebook on the subject of Ethical Hacking and Penetration Testing, the legal procedure for testing computer security by simulating real cyber attacks. Written by an expert in Computer Science and Information Security with ten years of experience in his field at the time of writing, The Hacker Ethos was specifically designed to be put in the hands of the beginner-level hacker, IT professional, and hopeful IT security researcher. This book covers the fundamental concepts of computer science and introduces the core knowledge that is required by all security professionals in the IT industry. The primary goal of the book is to instill what is known as the "Hacker Ethic" into the reader, a philosophy based on the ideal of free information, knowledge, and speech. Its very foundation is the principle of what it means to be a true hacker, an expert in computers at the most primal level, ready to explore new concepts and techniques without ever losing the hunger for knowledge. The

reader is encouraged to understand that Hacking is not easy, not is it a singular concept. It encompasses a vast library, covering every field of technology that includes programming, exploitation, web security and design, application security, viruses and malware, networking, wireless technology, telecommunication, phone technology, cellular technology, robotics, and everything that can be classified under the school of computing. Hackers are jacks of all trades, masters of none, but always striving to become so. Contained in this book are the topics of hacker ethics, and details the unwritten law of the Hacker Underground. It casts a bright spotlight on the Hacker Mythos, the subculture of hacking, and dispels the mystique of the Deep Web. It teaches the core techniques of hacking, and what is known as the Hacker Methodology, the list of techniques used my professional security testers and cyber-criminals alike to attack their targets. It teaches critical research techniques, heavily emphasizing self-study, and provides dozens of free resources on the various subjects and schools of hacking, including: programming, web hacking, service and application exploitation, malware development, password cracking, Denial-of-Service, Wireless and physical network penetration, cryptography. Lastly, the book provides a massive toolkit of professional and privately used hacking tools, all completely free, and teaches the reader how to acquire new tools for themselves. This book has been hailed by readers as

"the best and easiest beginner's guide to hacking of the millennium," meticulously having collected and organized every necessary tool, technique, and tutorial that beginners of the IT Security field absolutely must know. Its primary lesson is "teach you how to teach yourself," an invaluable skill that drives the field of technology and security more than any other. That a hacker who cannot learn on his own will never last. This book requires strong dedication and an insatiable desire to learn. Make no mistake, its contents will not be simple by any means, as much as it strives to make them easy to understand. There is no "hacking tools that does it all" and there is no magic trick to learning everything. Should you choose to continue, be prepared to adopt the true meaning of The Hacker Ethos, our creed: Information is meant to be free for everyone. Privacy is a right, hard earned; not a commodity, cheaply bought. Censorship is a tyranny delivered by silence. The Internet embodies freedom. Immerse yourself in it. Never stop learning; never stop teaching. Don't learn to hack; hack to learn. "We Are All Alike" Good luck on your Journey, - True Demon

Penetration Testing Azure for Ethical Hackers Packt Publishing Ltd

JUST FOR BOOKSTORES...55% DISCOUNT!!! Your customers will really appreciate this helpful guide! If you want to learn the art of Hacking and find out how a Hacker thinks then keep reading... Most every home and business office now has a firewall that separates your

internal computer network from the wild west of the world wide internet. The good news is that firewalls have become increasingly more sophisticated and properly configured can do an excellent job in securing your internal computer network devices. Modern firewalls now include intrusion detection and prevention, email spam filtering, website blocking and most are able to generate reports on who did what and when. They not only block evil doers from outside your network, but they police the users on the inside from accessing inappropriate resources on the outside internet. Employees can be blocked from visiting sites that can rob your business of valuable productivity time or violate some security compliance requirement. Prime business hours is really not the time to update your Facebook page! Nor do we want our medical and financial service folks using an instant messaging service to chat with and outsider! Chances are your Internet browser is worst enemy when it comes to securing your privacy. Every website you visit, every email you send and every link you follow is being tracked by hundreds of companies. Don't believe me? If you are using Firefox, install an add in extension named DoNotTrackme and study what happens. Assuming you are an average internet surfer, in less that 72 hours you will have a list of over 100 companies that have been tracking your every move on the internet! What you will learn: Meaning of Ethical Hacking. You will learn the primary benefits of Ethical Hacking How to install and use Kali Linux

Why choose Linux over Windows? How the process of Hacking works and how to use it for good How to do penetration testing with Kali Linux Cyber Security: The 5 best tips to prevent the cyber threat Types of Network and how to hack a Wireless Network Bash and Python Scripting. You will find recipes for writing real applications! Even if you are a completely beginner, with this guide, you will learn it easily! Don't miss the opportunity to sell so many copies of this amazing book, get it NOW !!!

Hacking and Penetration Testing with Low Power Devices Packt Publishing Ltd

• Von der Installation über die Konfiguration bis hin zum Einsatz der wichtigsten Tools • Detaillierter Ablauf von Security Assessments und Durchführung von Penetrationstests mit praktischer Checkliste • Schwachstellenanalyse mit OpenVAS, Angriffe mit WebScarab und Metasploit, IT-Forensik mit Autopsy, Reporting mit Faraday und viele weitere Tools Die Distribution Kali Linux ist auf Sicherheits- und Penetrationstests spezialisiert. Sie enthält mehrere Hundert Pakete zur Informationssammlung und Schwachstellenanalyse und jede Menge Tools für Angriffe und Exploitation sowie Forensik und Reporting, sodass Penetration Tester aus einem beinahe endlosen Fundus kostenloser Tools schöpfen können. Dieses Buch ermöglicht IT-Sicherheitsexperten und allen, die es werden wollen, einen einfachen Einstieg in Kali Linux. Erfahrung im Umgang mit anderen Linux-Distributionen setzt der Autor

dabei nicht voraus. Im ersten Teil des Buches erfahren Sie, wie Sie Kali Linux installieren und an Ihre Bedürfnisse anpassen. Darüber hinaus gibt Ihnen der Autor grundlegende Linux-Kenntnisse an die Hand, die Sie für das Penetration Testing mit Kali Linux brauchen. Der zweite Teil erläutert verschiedene Security Assessments sowie die grundlegende Vorgehensweise bei der Durchführung von Penetrationstests. So vorbereitet können Sie im nächsten Schritt gezielt die für Ihren Einsatzzweck passenden Tools für das Penetration Testing auswählen. Aus der Fülle der bei Kali Linux mitgelieferten Tools stellt der Autor im dritten Teil des Buches die wichtigsten vor und zeigt Schritt für Schritt, wie und wofür sie eingesetzt werden, darunter bekannte Tools wie Nmap, OpenVAS, Metasploit und John the Ripper. Nach der Lektüre sind Sie bereit, Kali Linux sowie die wichtigsten mitgelieferten Tools für Penetrationstests einzusetzen und IT-Systeme auf Schwachstellen zu prüfen. Aus dem Inhalt: • Hauptfeatures und Richt-linien von Kali Linux • Installation und Konfiguration • Linux-Dateisystem, Kommandozeile und nützliche Linux-Befehle • Sicherheitsrichtlinien • Einführung in Security Assessments • Durchführung von Pentests • Informationssammlung • mit Nmap, TheHarvester, HTTrack u.v.m. • Schwachstellenanalyse mit OpenVAS, Nikto und Siege • Sniffing und Spoofing mit Dsniff, Ettercap und Wireshark • Tools für Attacken: Wireless-Attacken (aircrack-ng, Ghost Phisher, Kismet) •

Pentesting von Webseiten (WebScarab, Skipfish, ZAP) • Exploitation (Metasploit, Armitage u.v.m.) • Passwort-Angriffe (Medusa, JtR u.v.m.) • IT-Forensik mit Autopsy, Binwalk und mehr • Reporting mit Cutycapt, Faraday und mehr • Checkliste für Penetrationstests • Praktisches Glossar

Hands-On Penetration Testing with Python Packt Publishing Ltd

The Basics of Hacking and Penetration Testing serves as an introduction to the steps required to complete a penetration test or perform an ethical hack from beginning to end. This book makes ethical hacking and penetration testing easy - no prior hacking experience is required. It shows how to properly utilize and interpret the results of the modern-day hacking tools required to complete a penetration test. With a simple and clean explanation of how to effectively utilize these tools - as well as the introduction to a four-step methodology for conducting a penetration test or hack - the book provides students with the know-how required to jump start their careers and gain a better understanding of offensive security. The book is organized into 7 chapters that cover hacking tools such as Backtrack Linux, Google reconnaissance, MetaGooFil, dig, Nmap, Nessus, Metasploit, Fast Track Autopwn, Netcat, and Hacker Defender rootkit. Each chapter contains hands-on examples and exercises that are designed to teach learners how to interpret results and utilize those results in later phases. PowerPoint slides are available for use in class. This book is an

ideal reference for security consultants, beginning InfoSec professionals, and students. Named a 2011 Best Hacking and Pen Testing Book by InfoSec Reviews Each chapter contains hands-on examples and exercises that are designed to teach you how to interpret the results and utilize those results in later phases. Writen by an author who works in the field as a Penetration Tester and who teaches Offensive Security, Penetration Testing, and Ethical Hacking, and Exploitation classes at Dakota State University. Utilizes the Backtrack Linus distribution and focuses on the seminal tools required to complete a penetration test.

The Basics of Hacking and Penetration Testing Packt Publishing Ltd

The Basics of Hacking and Penetration Testing, Second Edition, serves as an introduction to the steps required to complete a penetration test or perform an ethical hack from beginning to end. The book teaches students how to properly utilize and interpret the results of the modern-day hacking tools required to complete a penetration test. It provides a simple and clean explanation of how to effectively utilize these tools, along with a four-step methodology for conducting a penetration test or hack, thus equipping students with the know-how required to jump start their careers and gain a better understanding of offensive security. Each chapter contains hands-on examples and exercises that are designed to teach learners how to interpret results and utilize those results

in later phases. Tool coverage includes: Backtrack Linux, Google reconnaissance, MetaGooFil, dig, Nmap, Nessus, Metasploit, Fast Track Autopwn, Netcat, and Hacker Defender rootkit. This is complemented by PowerPoint slides for use in class. This book is an ideal resource for security consultants, beginning InfoSec professionals, and students. Each chapter contains hands-on examples and exercises that are designed to teach you how to interpret the results and utilize those results in later phases. Written by an author who works in the field as a Penetration Tester and who teaches Offensive Security, Penetration Testing, and Ethical Hacking, and Exploitation classes at Dakota State University. Utilizes the Kali Linux distribution and focuses on the seminal tools required to complete a penetration test.