Ethical Hacking And Penetration Testing Guide By Rafay Baloch

Ethical Hacking
Python Ethical Hacking from Scratch
Certified Ethical Hacker (CEH) Preparation Guide
Kali Linux Penetration Testing Bible
Penetration Testing
Ethical Hacker's Certification Guide (CEHv11)
Advanced Penetration Testing
Hacking and Penetration Testing
Web Penetration Testing with Kali Linux
The Basics of Hacking and Penetration Testing
CEH Certified Ethical Hacker Study Guide
Ethical Hacking
The Hacker Ethos
The Ethical Hack
Hacking With Kali Linux
Penetration Testing for Jobseekers
The Advanced Penetrating Testing
Linux Basics for Hackers
The Basics of Hacking and Penetration Testing
The Pentester BluePrint
Penetration Testing Azure for Ethical Hackers
Professional Penetration Testing
Ethical Hacking

DURHAM BRIGHT

Ethical Hacking Createspace Independent Publishing Platform 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

Python Ethical Hacking from Scratch John Wiley & Sons 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

Certified Ethical Hacker (CEH) Preparation Guide CRC Press

A hands-on guide to hacking computer systems from the ground up, from capturing traffic to crafting sneaky, successful trojans. A crash course in modern hacking techniques, Ethical Hacking is already being used to prepare the next generation of offensive security experts. In its many hands-on labs, you'll explore crucial skills for any aspiring penetration tester, security researcher, or malware analyst. You'll begin with the basics: capturing a victim's network traffic with an ARP spoofing attack and then viewing it in

Wireshark. From there, you'll deploy reverse shells that let you remotely run commands on a victim's computer, encrypt files by writing your own ransomware in Python, and fake emails like the ones used in phishing attacks. In advanced chapters, you'll learn how to fuzz for new vulnerabilities, craft trojans and rootkits, exploit websites with SQL injection, and escalate your privileges to extract credentials, which you'll use to traverse a private network. You'll work with a wide range of professional penetration testing tools—and learn to write your own tools in Python—as you practice tasks like: • Deploying the Metasploit framework's reverse shells and embedding them in innocent-seeming files • Capturing passwords in a corporate Windows network using Mimikatz • Scanning (almost) every device on the internet to find potential victims • Installing Linux rootkits that modify a victim's operating system • Performing advanced Cross-Site Scripting (XSS) attacks that execute sophisticated JavaScript payloads Along the way, you'll gain a foundation in the relevant computing technologies. Discover how advanced fuzzers work behind the scenes, learn how internet traffic gets encrypted, explore the inner mechanisms of nation-state malware like Drovorub, and much more. Developed with feedback from cybersecurity students, Ethical Hacking addresses contemporary issues in the field not often covered in other books and will prepare you for a career in penetration testing. Most importantly, you'll be able to think like an ethical hacker: someone who can carefully analyze systems and creatively gain access to them.
Kali Linux Penetration Testing Bible Packt Publishing Ltd
Became an Ethical Hacker that can hack computer systems like Black Hat Hackers and secure them like security expertsTopics CoveredSetting up a Hacking Lab-Lab overview and needed software-Install and configure VirtualBox-Installing Kali Linux as a Virtual Machine-Creating and Using SnapshotNetwork Hacking-Introduction to Network Penetration Testing / Hacking-Connecting a Wireless Adapter to Kali-What is MAC address and How to change it?-Wireless Modes (Managed and Monitor)Network Hacking: Pre-Connection Attacks-Packet Sniffing Basics-Wi-Fi Bands - 2.4 Ghz & 5 Ghz Frequencies-Targeted Packet Sniffing - Deauthentication Attack (Disconnecting Any Device From The Network)Network Hacking: Gaining Access - WEP Cracking-Theory Behind Cracking WEP Encryption-WEP Cracking Basics-Fake Authentication Attack-ARP Request Reply AttackNetwork Hacking: Gaining Access - WPA/WPA2/ Cracking-Introduction to WPA and WPA2 Cracking-Hacking WPA & WPA2 Without a Wordlist-Capturing The Handshake-Creating a Wordlist-Cracking WPA & WPA2 Using a Wordlist AttackNetwork Hacking: Post Connection Attacks-Introduction to Post Connection Attacks-Discovering Devices Connected to the Same Network-Gathering Sensitive Info About Connected Devices-Gathering More Sensitive Info(Running Services, Operating System.... etc.)Network Hacking: Post Connection Attacks - MITM attacks-ARP (Address Resolution Protocol) Poisoning-Intercepting Network Traffic-Bettercap Basics-ARP Spoofing Using Bettercap-Spying on Network Devices (Capturing Passwords, Visited websites etc.)-Creating Custom Spoofing Script-Understanding HTTPS & How to Bypass it-Bypassing HTTPS-Bypass HSTS (HTTP Strict Transport Security)-DNS Spoofing - Controlling DNS Requests on the Network-Injecting JavaScript Code-Wireshark- Basic Overview & How to Use it with MITM attacks-Wireshark - Using Filters, Tracing &

Dissecting Packets-Wireshark - Capturing Passwords & Anything Send by Any Device In the network.-Creating a Fake Access Point (Honeypot) - Theory-Creating a Fake Access Point (Honeypot) - PracticalGaining Access to Computers: Server-Side Attacks-Installing Metasploitable As a Virtual Machine-Basic Information Gathering & Exploitation-Hacking a Remote Server Using a Basic Metasploite Exploite-Exploiting a Code Execution Vulnerability to Hack into a Remote Server-Nexpose - Installing Nexpose-Nexpose - Scanning a Target Server for Vulnerabilities-Nexpose - Analyzing Scan Results & Generating ReportsGaining Access: Client-Side Attacks-Installing Veil Framework-Veil Overview and Payloads Basics-Generating an Undetectable Backdoor-Listening for Incoming Connections-Using a Basic Delivery Method to Test the Backdoor & Hack Windows 10-Hacking Windows 10 Using Fake Update-Backdooring Downloads on the Fly to Hack windows 10Gaining Access: Client-Side Attacks-Backdooring Any File Types (Images, PDF's ...etc.)-Compiling and Changing Trojan's Icon-Spoofing .exe Extension to any Extension-Spoofing Emails - Setting Up an SMTP Server-Email Spoofing - Sending Emails as any Email Account-BeEF Overview & Basic Hook Method-BeEF - Running Basic Commands on Target-BeEF - Stealing Password Using a Fake Login Prompt-BeEF - Hacking Windows 10 Using a Fake Update PromptGaining Access: Using the Above Attacks Outside the Local Network-Overview of the Setup-Example 1 - Generating a Backdoor that Works Outside the Network-Configuring the Router to Forward Connections to Kali-Example 2 - Using BeEF Outside the NetworkPost Exploitation-Meterpreter Basics-File System Commands-Maintaining Access - Basic Method-Maintaining Access - Using a Reliable & Undetectable Method-Spying - Capturing Key Strikes & Taking Screenshots-Pivoting - Using a Hacked System to Hack into other SystemsWebsite Hacking

Penetration Testing No Starch Press

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 Hacker's Certification Guide (CEHv11) Packt Publishing Ltd
Ever feel like you don't even own the hardware and software you paid dearly for? Ever get the impression that you have to ask for permission before installing or changing a program on your device? Ever feel like Facebook and Instagram are listening to your conversations to show you relevant ads? You're not alone.

Advanced Penetration Testing John Wiley & Sons
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.

Hacking and Penetration Testing Createspace Independent Publishing Platform
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.

Web Penetration Testing with Kali Linux BPB Publications

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 FeaturesGet hands-on with ethical hacking and learn to think like a real-life hackerBuild practical ethical hacking tools from scratch with the help of real-world examplesLeverage Python 3 to develop malware and modify its complexitiesBook Description Penetration 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 learnUnderstand the core concepts of ethical hackingDevelop custom hacking tools from scratch to be used for ethical hacking purposesDiscover ways to test the cybersecurity of an organization by bypassing protection schemesDevelop attack vectors used in real cybersecurity testsTest the system security of an organization or subject by identifying and exploiting its weaknessesGain and maintain remote access to target systemsFind ways to stay undetected on target systems and local networksWho this book is for If 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.

The Basics of Hacking and Penetration Testing John Wiley & Sons

Full Coverage of All Exam Objectives for the CEH Exams 312-50 and EC0-350 Thoroughly prepare for the challenging CEH Certified Ethical Hackers exam with this comprehensive study guide. The book provides full coverage of exam topics, real-world examples, and includes a CD with chapter review questions, two full-length practice exams, electronic flashcards, a glossary of key terms, and the entire book in a searchable pdf e-book. What's Inside: Covers ethics and legal issues, footprinting, scanning, enumeration, system hacking, trojans and backdoors, sniffers, denial of service, social engineering, session hijacking, hacking Web servers, Web application vulnerabilities, and more Walks you through exam topics and includes plenty of real-world scenarios to help reinforce concepts Includes a CD with an assessment test, review questions, practice exams, electronic flashcards, and the entire book in a searchable pdf

CEH Certified Ethical Hacker Study Guide Newnes

To crack passwords or to steal data? No, it is much more than that. Ethical hacking is to scan vulnerabilities and to find potential threats on a computer or networks. An ethical hacker finds the weak points or loopholes in a computer, web applications or network and reports them to the organization. So, let's explore more about Ethical Hacking step-by-step.

Ethical Hacking Elsevier

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 Hacker Ethos Packt Publishing Ltd

Herein, you will find a comprehensive, beginner-friendly book designed to teach you the basics of hacking. Learn the mindset, the tools, the techniques, and the ETHOS of hackers. The book is written so that anyone can understand the material and grasp the fundamental techniques of hacking. Its content is tailored specifically for the beginner, pointing you in the right direction, to show you the path to becoming an elite and powerful hacker. You will gain access and instructions to tools used by industry professionals in the field of penetration testing and ethical hacking and by some of the best hackers in the world. ---------- ---------- If you are curious about the FREE version of this book, you can reed the original, first-draft of this book for free on Google Drive! https://drive.google.com/open?id=0B78IWlY3bU_8RnZmOXczTUFEM1U

The Ethical Hack CRC Press

Giving an available prologue to infiltration testing and hacking, the book supplies you with a key comprehension of hostile security. In the wake of finishing the book you will be set up to go up against top to bottom and propelled subjects in hacking and entrance testing.The book strolls you through each of the means and apparatuses in an organized, systematic way enabling you to see how the yield from each instrument can be completely used in the ensuing periods of the infiltration test. This procedure will enable you to obviously perceive how the different instruments

and stages identify with each other.
Hacking With Kali Linux Createspace Independent Publishing Platform
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.
Penetration Testing for Jobseekers Independently Published
Requiring no prior hacking experience, Advance Ethical Hacking and Penetration Testing Guide supplies a complete introduction to the steps required to complete a penetration test, or ethical hack, from beginning to end. You will learn how to properly utilize and interpret the results of modern-day hacking tools, which are required to complete a penetration test. The book covers a wide range of tools, including Backtrack Linux, Google reconnaissance, MetaGooFil, dig, Nmap, Nessus, Metasploit, Fast Track Autopwn, Netcat, and Hacker Defender rootkit. Supplying a simple and clean explanation of how to effectively utilize these tools, it details a four-step methodology for conducting an effective penetration test or hack.Providing an accessible introduction to penetration testing and hacking, the book supplies you with a fundamental understanding of offensive security. After completing the book you will be prepared to take on in-depth and advanced topics in hacking and penetration testing. The book walks you through each of the steps and tools in a structured, orderly manner allowing you to understand how the output from each tool can be fully utilized in the subsequent phases of the penetration test. This process will allow you to clearly see how the various tools and phases relate to each other. An ideal resource for those who want to learn about ethical hacking but dont know where to start, this book will help take your hacking skills to the next level. The topics described in this book comply with international standards and with what is being taught in

international certifications

The Advanced Penetrating Testing Packt Publishing Ltd

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

Linux Basics for Hackers Ethical Hacking and Penetration Testing Guide

Learn how to hack systems like black hat hackers and secure them like security experts Key Features Understand how computer systems work and their vulnerabilities Exploit weaknesses and hack into machines to test their security Learn how to secure systems from hackers Book Description This book starts with the basics of ethical hacking, how to practice hacking safely and legally, and how to install and interact with Kali Linux and the Linux terminal. You will explore network hacking, where you will see how to test the security of wired and wireless networks. You'll also learn how to crack the password for any Wi-Fi network (whether it uses WEP, WPA, or WPA2) and spy on the connected devices. Moving on, you will discover how to gain access to remote computer systems using client-side and server-side attacks. You will also get the hang of post-exploitation techniques, including remotely controlling and interacting with the systems that you compromised. Towards the end of the book, you will be able to pick up web application hacking techniques. You'll see how to discover, exploit, and prevent a number of website vulnerabilities, such as XSS and SQL injections. The attacks covered are practical techniques that work against real systems and are purely for educational purposes. At the end of each section, you will learn how to detect, prevent, and secure systems from these attacks. What you will learn Understand ethical hacking and the different fields and types of hackers Set up a penetration testing lab to practice safe and legal hacking Explore Linux basics, commands, and how to interact with the terminal Access password-protected networks and spy on connected clients Use server and client-side attacks to hack and control remote computers Control a hacked system remotely and use it to hack other systems Discover, exploit, and prevent a

number of web application vulnerabilities such as XSS and SQL injections Who this book is for Learning Ethical Hacking from Scratch is for anyone interested in learning how to hack and test the security of systems like professional hackers and security experts.

The Basics of Hacking and Penetration Testing Lulu Press, Inc

If you want to lean advanced ethical hacking and penetration testing concepts, then keep reading... Does the concept of ethical hacking fascinate you?Do you know what penetration testing means?Do you want to learn about ethical hacking and penetration testing?Do you want to learn all this, but aren't sure where to begin? If YES, then this is the perfect book for you! Welcome to the advanced guide on ethical hacking and penetration testing with Kali Linux guide. Ethical Hacking is essentially the art of protecting a system and its resources and what you will be going through in this book is the techniques, tactics and strategies which will help you understand and execute ethical hacking in a controlled environment as well as the real world. You will also be learning about Kali Linux which the choice of an operating system that is preferred by ethical hackers all over the world. You will also get exposure to tools that are a part of Kali Linux and how you can combine this operating system and its tools with the Raspberry Pi to turn into a complete toolkit for ethical hacking. You will be getting your hands dirty with all these tools and will be using the tools practically to understand how ethical hackers and security admins work together in an organization to make their systems attack proof. As an ethical hacker, hacking tools are your priority and we will be covering tools such as NMap and Proxychains which are readily available in the Kali Linux setup. These two tools together will help us setup a system wherein we will target another system and not allow the target system to understand the source IP from where the attack is originating. We will write some basic scripts and automate those scripts to attack on a network at regular intervals to fetch us data describing the vulnerabilities of that network such as open ports, DNS server details. We will also be working with techniques and strategies for Web Application Firewall testing. This will include topics such as Cross Site Scripting and SQL injections. Then comes Social Engineering. This focuses more on the technical aspect of gathering information which will help us to prepare for an attack and not social engineering concerned with making fraudulent phone calls or pretending to be a person to get the password from an individual. We will also talk about Virtual Private Networks (VPN) and how it is important in the domain of ethical hacking. We will discuss how virtual private networks are used by employees of an organization to protect their connection to their corporate network from attackers who might try to steal their data by using man in the middle attacks. We will also understand cryptography in brief and how it plays a role in hacking operations. How various cryptography puzzles can train an ethical hacker to improve their thought process and help them in the technical aspects of hacking. In this book, you will learn about: Various hacking tools, Writing and automating scripts, Techniques used for firewall testing, Basics of social engineering, Virtual private networks, Cryptography and its role in hacking, and much more! So, what are you waiting for? Grab your copy today CLICKING BUY NOW BUTTON!

The Pentester BluePrint No Starch Press

Your ultimate guide to pentesting with Kali Linux Kali is a popular and powerful Linux distribution used by cybersecurity professionals around the world. Penetration testers must master Kali's varied library of tools to be effective at their work. The Kali Linux Penetration Testing Bible is the hands-on and methodology guide for pentesting with Kali. You'll discover everything you need to know about the tools and techniques hackers use to gain access to systems like yours so you can erect reliable defenses for your virtual assets. Whether you're new to the field or an established pentester, you'll find what you need in this comprehensive guide. Build a modern dockerized environment Discover the fundamentals of the bash language in Linux Use a variety of effective techniques to find vulnerabilities (OSINT, Network Scan, and more) Analyze your findings and identify false positives and uncover advanced subjects, like buffer overflow, lateral movement, and privilege escalation Apply practical and efficient pentesting workflows Learn about Modern Web Application Security Secure SDLC Automate your penetration testing with Python

Related with Ethical Hacking And Penetration Testing Guide By Rafay Baloch:
• Charlie Dead Poets Society : click here