

Kali Linux Windows Penetration Testing Free Ebooks

[Penetration Testing The Basics of Hacking and Penetration Testing BackTrack 4 Practical Web Penetration Testing The Basics of Hacking and Penetration Testing Hands on Hacking Advanced Penetration Testing](#) [Penetration Testing for Jobseekers](#) [Cone Penetration Testing 2022 Mastering Kali Linux for Advanced Penetration Testing Ethical Hacking and Penetration Testing Guide](#) [The Art of Network Penetration Testing](#) [Ethical Hacker's Penetration Testing Guide](#) [The Pen Tester BluePrint Hands-On Penetration Testing with Python](#) [Professional Penetration Testing](#) [Penetration Testing Azure for Ethical Hackers](#) [The Hacker Playbook 2](#) [CISO's Guide to Penetration Testing](#) [Hands-On Application Penetration Testing with Burp Suite](#) [Mobile Application Penetration Testing](#) [Unauthorised Access](#) [The Hacker Playbook Hacking](#) [Mastering Kali Linux for Advanced Penetration Testing, Third Edition](#) [Kali Linux Hacking IoT Penetration Testing Cookbook](#) [AWS Penetration Testing](#) [WarDriving and Wireless Penetration Testing](#) [Metasploit Learn Penetration Testing Hacking For Dummies](#) [Mastering Kali Linux for Advanced Penetration Testing - Second Edition](#) [Metasploit Penetration Testing Cookbook](#) [Windows and Linux Penetration Testing from Scratch](#) [Secure Your Network for Free](#) [Advanced Infrastructure Penetration Testing](#) [Penetration Testing For Dummies](#) [Penetration Testers Open Source Toolkit](#) [Penetration Testing Basics](#)

Right here, we have countless books [Kali Linux Windows Penetration Testing Free Ebooks](#) and collections to check out. We additionally meet the expense of variant types and also type of the books to browse. The usual book, fiction, history, novel, scientific research, as with ease as various supplementary sorts of books are readily handy here.

As this [Kali Linux Windows Penetration Testing Free Ebooks](#), it ends occurring best one of the favored book [Kali Linux Windows Penetration Testing Free Ebooks](#) collections that we have. This is why you remain in the best website to see the incredible book to have.

[Mastering Kali Linux for Advanced Penetration Testing, Third Edition](#) Oct 10 2020 A practical guide to testing your infrastructure security with Kali Linux, the preferred choice of pentesters and hackers Key Features Employ advanced pentesting techniques with Kali Linux to build highly secured systems Discover various stealth techniques to remain undetected and defeat modern infrastructures Explore red teaming techniques to exploit secured environment Book Description This book takes you, as a tester or security practitioner, through the reconnaissance, vulnerability assessment, exploitation, privilege escalation, and post-exploitation activities used by pentesters. To start with, you'll use a laboratory environment to validate tools and techniques, along with an application that supports a collaborative approach for pentesting. You'll then progress to passive reconnaissance with open source intelligence and active reconnaissance of the external and internal infrastructure. You'll also focus on how to select, use, customize, and interpret the results from different vulnerability scanners, followed by examining specific routes to the target, which include bypassing physical security and the exfiltration of data using a variety of techniques. You'll discover concepts such as social engineering, attacking wireless networks, web services, and embedded devices. Once you are confident with these topics, you'll learn the practical aspects of attacking user client systems by backdooring with fileless techniques, followed by focusing on the most vulnerable part of the network - directly attacking the end user. By the end of this book, you'll have explored approaches for carrying out advanced pentesting in tightly secured environments, understood pentesting and hacking techniques employed on embedded peripheral devices. What you will learn Configure the most effective Kali Linux tools to test infrastructure security Employ stealth to avoid detection in the infrastructure being tested Recognize when stealth attacks are being used against your infrastructure Exploit networks and data systems using wired and wireless networks as well as web services Identify and download valuable data from target systems Maintain access to compromised systems Use social engineering to compromise the weakest part of the network - the end users Who this book is for This third edition of Mastering Kali Linux for Advanced Penetration Testing is for you if you are a security analyst, pentester, ethical hacker, IT professional, or security consultant wanting to maximize the success of your infrastructure testing using some of the advanced features of Kali Linux. Prior exposure of penetration testing and ethical hacking basics will be helpful in making the most out of this book.

The Hacker Playbook 2 May 17 2021 Just as a professional athlete doesn't show up without a solid game plan, ethical hackers, IT professionals, and security researchers should not be unprepared, either. The Hacker Playbook provides them their own game plans. Written by a longtime security professional and CEO of Secure Planet, LLC, this step-by-step guide to the "game" of penetration hacking features hands-on examples and helpful advice from the top of the field. Through a series of football-style "plays," this straightforward guide gets to the root of many of the roadblocks people may face while penetration testing-including attacking different types of networks, pivoting through security controls, privilege escalation, and evading antivirus software. From "Pregame" research to "The Drive" and "The Lateral Pass," the practical plays listed can be read in order or referenced as needed. Either way, the valuable advice within will put you in the mindset of a penetration tester of a Fortune 500 company, regardless of your career or level of experience. This second version of The Hacker Playbook takes all the best "plays" from the original book and incorporates the latest attacks, tools, and lessons learned. Double the content compared to its predecessor, this guide further outlines building a lab, walks through test cases for attacks, and provides more customized code. Whether you're downing energy drinks while desperately looking for an exploit, or preparing for an exciting new job in IT security, this guide is an essential part of any ethical hacker's library-so there's no reason not to get in the game.

Hands on Hacking May 29 2022 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.

Advanced Penetration Testing Apr 27 2022 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.

Mastering Kali Linux for Advanced Penetration Testing Jan 25 2022 This book provides an overview of the kill chain approach to penetration testing, and then focuses on using Kali Linux to provide examples of how this methodology is applied in the real world. After describing the underlying concepts, step-by-step examples are provided that use selected tools to demonstrate the techniques. If you are an IT professional or a security consultant who wants to maximize the success of your network testing using some of the advanced features of Kali Linux, then this book is for you. This book will teach you how to become an expert in the pre-engagement, management, and documentation of penetration testing by building on your understanding of Kali Linux and wireless concepts.

Secure Your Network for Free Oct 29 2019 This is the only book to clearly demonstrate how to get big dollar security for your network using freely available tools. This is a must have book for any company or person with a limited budget. Network security is in a constant struggle for budget to get things done. Upper management wants thing to be secure but doesn't want to pay for it. With this book as a guide, everyone can get what they want. The examples and information will be of immense value to every small business. It will explain security principles and then demonstrate how to achieve them using only freely available software. Teachers you how to implement best of breed security using tools for free ideal for anyone recommending and implementing new technologies within the company

The Basics of Hacking and Penetration Testing Oct 02 2022 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.

WarDriving and Wireless Penetration Testing Jun 05 2020 Provides information on analyzing wireless networks through wardriving and penetration testing.

Hacking Now 10 2020 Would You Like To Learn Exactly How To Take Your Hacking Skills To The Next Level? - NOW INCLUDES FREE GIFTS! (see below for details) Do you want to learn how to make money with hacking legally? Do you want to delve even deeper into the art of hacking? Do you love solving puzzles and seeing how computer systems work? If the answer to any of these questions is yes, this book will make you with the answers you've been looking for! While some hackers use their skills to commit crimes, others use their skills for less nefarious means. Just about everything that we do is online now. There is a huge need for ethical hackers to test applications, system security, etc, and with the right skills, you can make some serious money as a penetration tester while staying on the right side of the law! In this book we will look at: The basics of coding and programming that you, as a hacker, need to know in order to be successful. We look at important concepts such as compiling code and ensuring that the code works. We also look at shortcuts when it comes to planning out your code so that you don't end up writing pages and pages of code only to find that it doesn't work as it should, thereby saving you valuable time. We look at the free systems that will enable you to perform penetration testing and that can easily be run alongside your normal operating system. This system is opensource, free, easy to edit and, best of all, very light on resources, and we'll show you how to get it as well as how it works! We will show you how to make your life as a hacker easier by finding exploits that are ready to go - all you'll need to do is to match up the right code to the right system and execute the code. Having a database of exploits at your fingertips can save you a HUGE amount of time and effort in the long run! We'll also go into exactly what penetration testing is and how it works. We walk you step by step through your first pen testing exercise so that you can get your toes wet without any issues. We also go through what a career in pen testing might entail and some of the options available. Next, we go through more in-depth information on concepts that are very important to any hacker - like networking and how it works; detecting hacking attempts; counter-measures that you might need to deal with, and how to deal with them; and how you can stay in the shadows during and after an attack. We will go through how you can remove the evidence of the attack as a whole. We then give a rundown of the most popular tools that hackers use to get information and how they work. We also go over how to protect yourself if someone tries to use these tools on you! Finally, we look into the exciting world of cryptography and why you as a hacker should be considering learning more about it. We go over the importance of encryption and when it is important for you to encrypt your own files. This serves as an interesting introduction that should whet your appetite to learn more about cryptography. Who knows, maybe it will inspire you to begin a career as a code-breaker yourself? ...and much more! Also included for a limited time only are 2 FREE GIFTS, including a full length, surprise FREE BOOK! Take the first step towards mastering hacking today. Click the buy now button above for instant access. Also included are 2 FREE GIFTS! - A sample from one of my other best-selling books, and full length, FREE BOOKS included with your purchase!

Ethical Hacker's Penetration Testing Guide Oct 22 2021 Discover security posture, vulnerabilities, and blind spots ahead of the threat actor KEY FEATURES ? Includes illustrations and real-world examples of pentesting web applications, REST APIs, thick clients, mobile applications, and wireless networks. ? Covers numerous techniques such as Fuzzing (FFuF), Dynamic Scanning, Secure Code Review, and bypass testing. ? Practical application of Nmap, Metasploit, SQLmap, OWASP ZAP, Wireshark, and Kali Linux. DESCRIPTION The 'Ethical Hacker's Penetration Testing Guide' is a hands-on guide that will take you from the fundamentals of pen testing to advanced security testing techniques. This book extensively uses popular pen testing tools such as Nmap, Burp Suite, Metasploit, SQLMap, OWASP ZAP, and Kali Linux. A detailed analysis of pentesting strategies for discovering OWASP top 10 vulnerabilities, such as cross-site scripting (XSS), SQL Injection, XXE, file upload vulnerabilities, etc., are explained. It provides a hands-on demonstration of pentest approaches for thick client applications, mobile applications (Android), network services, and wireless networks. Other techniques such as Fuzzing, Dynamic Scanning (DAST), and so on are also demonstrated. Security logging, harmful activity monitoring, and pentesting for sensitive data are also included in the book. The book also covers web security automation with the help of writing effective python scripts. Through a series of live demonstrations and real-world use cases, you will learn how to break applications to expose security flaws, detect the vulnerability, and exploit it appropriately. Throughout the book, you will learn how to identify security risks, as well as a few modern cybersecurity approaches and popular pentesting tools. WHAT YOU WILL LEARN ? Expose the OWASP top ten vulnerabilities, fuzzing, and dynamic scanning. ? Get well versed with various pentesting tools for web, mobile, and wireless pentesting. ? Investigate hidden vulnerabilities to safeguard critical data and application components. ? Implement security logging, application monitoring, and secure coding. ? Learn about various protocols, pentesting tools, and ethical hacking methods. WHO THIS BOOK IS FOR This book is intended for pen testers, ethical hackers, security analysts, cyber professionals, security consultants, and anybody interested in learning about penetration testing, tools, and methodologies. Knowing concepts of penetration testing is preferable but not required. TABLE OF CONTENTS 1. Overview of Web and Related Technologies and Understanding the Application 2. Web Penetration Testing- Through Code Review 3. Web Penetration Testing- Injection Attacks 4. Fuzzing, Dynamic scanning of REST API and Web Application 5. Web Penetration Testing- Unvalidated Redirects/Forwards, SSRF 6. Pentesting for Authentication, Authorization Bypass, and Business Logic Flaws 7. Pentesting for Sensitive Data, Vulnerable Components, Security Monitoring 8. Exploiting File Upload Functionality and XXE Attack 9. Web Penetration Testing: Thick Client 10. Introduction to Network Pentesting 11. Introduction to Wireless Penetration 12. Penetration Testing-Mobile App 13. Security Automation for Web Pentest 14. Setting up Pentest Lab Mobile Application Penetration Testing Feb 11 2021 Explore real-world threat scenarios, attacks on mobile applications, and ways to counter them>About This Book- Gain insights into the current threat landscape of mobile

applications in particular- Explore the different options that are available on mobile platforms and prevent circumventions made by attackers- This is a step-by-step guide to setting up your own mobile penetration testing environment Who This Book Is For You are a mobile application evangelist, mobile application developer, information security practitioner, penetration tester on infrastructure web applications, an application security professional, or someone who wants to learn mobile application security as a career, then this book is for you. This book will provide you with all the skills you need to get started with Android and iOS pen-testing. What You Will Learn- Gain an in-depth understanding of Android and iOS architecture and the latest changes- Discover how to work with different tool suites to assess any application- Develop different strategies and techniques to connect to a mobile device- Create a foundation for mobile application security principles- Grasp techniques to attack different components of an Android device and the different functionalities of an iOS device- Get to know secure development strategies for both iOS and Android applications- Gain an understanding of threat modeling mobile applications- Get an in-depth understanding of both Android and iOS implementation vulnerabilities and how to provide counter-measures while developing a mobile app Detail Mobile security has come a long way over the last few years. It has transitioned from "should it be done?" to "it must be done!" Alongside the growing number of devices and applications, there is also a growth in the volume of Personally identifiable information (PII), Financial Data, and much more. This data needs to be secured. This is why Pen-testing is so important to modern application developers. You need to know how to secure user data, and find vulnerabilities and loopholes in your application that might lead to security breaches. This book gives you the necessary skills to security test your mobile applications as a beginner, developer, or security practitioner. You'll start by discovering the internal components of an Android and an iOS application. Moving ahead, you'll understand the inter-process working of these applications. Then you'll set up a test environment for this application using various tools to identify the loopholes and vulnerabilities in the structure of the applications. Finally, after collecting all information about these security loop holes, we'll start securing our applications from these threats. Style and approach This is an easy-to-follow guide full of hands-on examples of real-world attack simulations. Each topic is explained in context with respect to testing, and for the more inquisitive, there are more details on the concepts and techniques used for different platforms.

BackTrack 4 Sep 01 2022 Master the art of penetration testing with BackTrack.

Practical Web Penetration Testing Jul 31 2022 Learn how to execute web application penetration testing end-to-end Key Features Build an end-to-end threat model landscape for web application security Learn both web application vulnerabilities and web intrusion testing Associate network vulnerabilities with a web application infrastructure Book Description Companies all over the world want to hire professionals dedicated to application security. Practical Web Penetration Testing focuses on this very trend, teaching you how to conduct application security testing using real-life scenarios. To start with, you'll set up an environment to perform web application penetration testing. You will then explore different penetration testing concepts such as threat modeling, intrusion test, infrastructure security threat, and more, in combination with advanced concepts such as Python scripting for automation. Once you are done learning the basics, you will discover end-to-end implementation of tools such as Metasploit, Burp Suite, and Kali Linux. Many companies deliver projects into production by using either Agile or Waterfall methodology. This book shows you how to assist any company with their SDLC approach and helps you on your journey to becoming an application security specialist. By the end of this book, you will have hands-on knowledge of using different tools for penetration testing. What you will learn Learn how to use Burp Suite effectively Use Nmap, Metasploit, and more tools for network infrastructure tests Practice using all web application hacking tools for intrusion tests using Kali Linux Learn how to analyze a web application using application threat modeling Know how to conduct web intrusion tests Understand how to execute network infrastructure tests Master automation of penetration testing functions for maximum efficiency using Python Who this book is for Practical Web Penetration Testing is for you if you are a security professional, penetration tester, or stakeholder who wants to execute penetration testing using the latest and most popular tools. Basic knowledge of ethical hacking would be an added advantage.

Ethical Hacking and Penetration Testing Guide Dec 24 2021 Requiring no prior hacking experience, 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, MetaGooFII, 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 don't 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.

Penetration Testing For Dummies Aug 27 2019 Target, test, analyze, and report on security vulnerabilities with pen testing Pen Testing is necessary for companies looking to target, test, analyze, and patch the security vulnerabilities from hackers attempting to break into and compromise their organizations data. It takes a person with hacking skills to look for the weaknesses that make an organization susceptible to hacking. Pen Testing For Dummies aims to equip IT enthusiasts at various levels with the basic knowledge of pen testing. It is the go-to book for those who have some IT experience but desire more knowledge of how to gather intelligence on a target, learn the steps for mapping out a test, and discover best practices for analyzing, solving, and reporting on vulnerabilities. The different phases of a pen test from pre-engagement to completion Threat modeling and understanding risk When to apply vulnerability management vs penetration testing Ways to keep your pen testing skills sharp, relevant, and at the top of the game Get ready to gather intelligence, discover the steps for mapping out tests, and analyze and report results!

Metasploit May 05 2020 The Metasploit Framework makes discovering, exploiting, and sharing vulnerabilities quick and relatively painless. But while Metasploit is used by security professionals everywhere, the tool can be hard to grasp for first-time users. Metasploit: The Penetration Tester's Guide fills this gap by teaching you how to harness the Framework and interact with the vibrant community of Metasploit contributors. Once you've built your foundation for penetration testing, you'll learn the Framework's conventions, interfaces, and module system as you launch simulated attacks. You'll move on to advanced penetration testing techniques, including network reconnaissance and enumeration, client-side attacks, wireless attacks, and targeted social-engineering attacks. Learn how to: -Find and exploit unmaintained, misconfigured, and unpatched systems -Perform reconnaissance and find valuable information about your target -Bypass anti-virus technologies and circumvent security controls -Integrate Nmap, Nexpose, and Nessus with Metasploit to automate discovery -Use the Meterpreter shell to launch further attacks from inside the network -Harness standalone Metasploit utilities, third-party tools, and plug-ins -Learn how to write your own Meterpreter post exploitation modules and scripts You'll even touch on exploit discovery for zero-day research, write a fuzzer, port existing exploits into the Framework, and learn how to cover your tracks. Whether your goal is to secure your own networks or to put someone else's to the test, Metasploit: The Penetration Tester's Guide will take you there and beyond.

Penetration Tester's Open Source Toolkit Jul 27 2019 Penetration Tester's Open Source Toolkit, Third Edition, discusses the open source tools available to penetration testers, the ways to use them, and the situations in which they apply. Great commercial penetration testing tools can be very expensive and sometimes hard to use or of questionable accuracy. This book helps solve both of these problems. The open source, no-cost penetration testing tools presented do a great job and can be modified by the student for each situation. This edition offers instruction on how and in which situations the penetration tester can best use them. Real-life scenarios support and expand upon explanations throughout. It also presents core technologies for each type of testing and the best tools for the job. The book consists of 10 chapters that covers a wide range of topics such as reconnaissance; scanning and enumeration; client-side attacks and human weaknesses; hacking database services; Web server and Web application testing; enterprise application testing; wireless penetrating testing; and building penetration test labs. The chapters also include case studies where the tools that are discussed are applied. New to this edition: enterprise application testing, client-side attacks and updates on Metasploit and Backtrack. This book is for people who are interested in penetration testing or professionals engaged in penetration testing. Those working in the areas of database, network, system, or application administration, as well as architects, can gain insights into how penetration testers perform testing in their specific areas of expertise and learn what to expect from a penetration test. This book can also serve as a reference for security or audit professionals. Details current open source penetration testing tools Presents core technologies for each type of testing and the best tools for the job New to this edition: Enterprise application testing, client-side attacks and updates on Metasploit and Backtrack

IoT Penetration Testing Cookbook Aug 08 2020 Over 80 recipes to master IoT security techniques. About This Book Identify vulnerabilities in IoT device architectures and firmware using software and hardware pentesting techniques Understand radio communication analysis with concepts such as sniffing the air and capturing radio signals A recipe based guide that will teach you to pentest new and unique set of IoT devices. Who This Book Is For This book targets IoT developers, IoT enthusiasts, pentesters, and security professionals who are interested in learning about IoT security. Prior knowledge of basic pentesting would be beneficial. What You Will Learn Set up an IoT pentesting lab Explore various threat modeling concepts Exhibit the ability to analyze and exploit firmware vulnerabilities Demonstrate the automation of application binary analysis for iOS and Android using MobSF Set up a Burp Suite and use it for web app testing Identify UART and JTAG pinouts, solder headers, and hardware debugging Get solutions to common wireless protocols Explore the mobile security and firmware best practices Master various advanced IoT exploitation techniques and security automation In Detail IoT is an upcoming trend in the IT industry today; there are a lot of IoT devices on the market, but there is a minimal understanding of how to safeguard them. If you are a security enthusiast or pentester, this book will help you understand how to exploit and secure IoT devices. This book follows a recipe-based approach, giving you practical experience in securing upcoming smart devices. It starts with practical recipes on how to analyze IoT device architectures and identify vulnerabilities. Then, it focuses on enhancing your pentesting skill set, teaching you how to exploit a vulnerable IoT device, along with identifying vulnerabilities in IoT device firmware. Next, this book teaches you how to secure embedded devices and exploit smart devices with hardware techniques. Moving forward, this book reveals advanced hardware pentesting techniques, along with software-defined, radio-based IoT pentesting with Zigbee and Z-Wave. Finally, this book also covers how to use new and unique pentesting techniques for different IoT devices, along with smart devices connected to the cloud. By the end of this book, you will have a fair understanding of how to use different pentesting techniques to exploit and secure various IoT devices. Style and approach This recipe-based book will teach you how to use advanced IoT exploitation and security automation.

The Hacker Playbook Dec 12 2020 Just as a professional athlete doesn't show up without a solid game plan, ethical hackers, IT professionals, and security researchers should not be unprepared. either. The Hacker Playbook provides them their own game plans. Written by a longtime security professional and CEO of Secure Planet, LLC, this step-by-step guide to the "game" of penetration hacking features hands-on examples and helpful advice from the top of the field. Through a series of football-style "plays," this straightforward guide gets to the root of many of the roadblocks people may face while penetration testing—including attacking different types of networks, pivoting through security controls, and evading antivirus software. From "Pregame" research to "The Drive" and "The Lateral Pass," the practical plays listed can be read in order or referenced as needed. Either way, the valuable advice within will put you in the mindset of a penetration tester of a Fortune 500 company, regardless of your career or level of experience. Whether you're downing energy drinks while desperately looking for an exploit, or preparing for an exciting new job in IT security, this guide is an essential part of any ethical hacker's library—so there's no reason not to get in the game.

CISO's Guide to Penetration Testing Apr 15 2021 CISO's Guide to Penetration Testing: A Framework to Plan, Manage, and Maximize Benefits details the methodologies, framework, and unwritten conventions penetration testers should cover to provide the most value to your organization and your customers. Discussing the process from both a consultative and technical perspective, it provides an overview o

The Pentester BluePrint Sep 20 2021 JUMPSTART YOUR NEW AND EXCITING CAREER AS A PENETRATION TESTER The Pentester BluePrint: Your Guide to Being a Pentester offers readers a chance to delve deeply into the world of the ethical, or "white-hat" hacker. Accomplished pentester and author Phillip L. Wylie and cybersecurity researcher Kim Crawley walk you through the basic and advanced topics necessary to understand how to make a career out of finding vulnerabilities in systems, networks, and applications. You'll learn about the role of a penetration tester, what a pentest involves, and the prerequisite knowledge you'll need to start the educational journey of becoming a pentester. Discover how to develop a plan by assessing your current skillset and finding a starting place to begin growing your knowledge and skills. Finally, find out how to become employed as a pentester by using social media, networking strategies, and community involvement. Perfect for IT workers and entry-level information security professionals, The Pentester BluePrint also belongs on the bookshelves of anyone seeking to transition to the exciting and in-demand field of penetration testing. Written in a highly approachable and accessible style, The Pentester BluePrint avoids unnecessarily technical lingo in favor of concrete advice and practical strategies to help you get your start in pentesting. This book will teach you: The foundations of pentesting, including basic IT skills like operating systems, networking, and security systems The development of hacking skills and a hacker mindset Where to find educational options, including college and university classes, security training providers, volunteer work, and self-study Which certifications and degrees are most useful for gaining employment as a pentester How to get experience in the pentesting field, including labs, CTFs, and bug bounties

The Art of Network Penetration Testing Nov 22 2021 The Art of Network Penetration Testing is a guide to simulating an internal security breach. You'll take on the role of the attacker and work through every stage of a professional pentest, from information gathering to seizing control of a system and owning the network. Summary Penetration testing is about more than just getting through a perimeter firewall. The biggest security threats are inside the network, where attackers can rampage through sensitive data by exploiting weak access controls and poorly patched software. Designed for up-and-coming security professionals, The Art of Network Penetration Testing teaches you how to take over an enterprise network from the inside. It lays out every stage of an internal security assessment step-by-step, showing you how to identify weaknesses before a malicious invader can do real damage. Purchase of the print book includes a free eBook in PDF, Kindle, and ePub formats from Manning Publications. About the technology Penetration testers uncover security gaps by attacking networks exactly like malicious intruders do. To become a world-class pentester, you need to master offensive security concepts, leverage a proven methodology, and practice, practice, practice. This book delivers insights from security expert Royce Davis, along with a virtual testing environment you can use to hone your skills. About the book The Art of Network Penetration Testing is a guide to simulating an internal security breach. You'll take on the role of the attacker and work through every stage of a professional pentest, from information gathering to seizing control of a system and owning the network. As you brute force passwords, exploit unpatched services, and elevate network level privileges, you'll learn where the weaknesses are—and how to take advantage of them. What's inside Set up a virtual pentest lab Exploit Windows and Linux network vulnerabilities Establish persistent re-entry to compromised targets Detail your findings in an engagement report About the reader For tech professionals. No security experience required. About the author Royce Davis has orchestrated hundreds of penetration tests, helping to secure many of the largest companies in the world. Table of Contents 1 Network Penetration Testing PHASE 1 - INFORMATION GATHERING 2 Discovering network hosts 3 Discovering network services 4 Discovering network vulnerabilities PHASE 2 - FOCUSED PENETRATION 5 Attacking vulnerable web services 6 Attacking vulnerable database services 7 Attacking unpatched services PHASE 3 - POST-EXPLOITATION AND PRIVILEGE ESCALATION 8 Windows post-exploitation 9 Linux or UNIX post-exploitation 10 Controlling the entire network PHASE 4 - DOCUMENTATION 11 Post-engagement cleanup 12 Writing a solid pentest deliverable

Mastering Kali Linux for Advanced Penetration Testing - Second Edition Jan 31 2020 A practical guide to testing your network's security with Kali Linux, the preferred choice of penetration testers and hackers. About This Book* Employ advanced pentesting techniques with Kali Linux to build highly-secured systems* Get to grips with various stealth techniques to remain undetected and defeat the latest defenses and follow proven approaches* Select and configure the most effective tools from Kali Linux to test network security and prepare your business against malicious threats and save costs Who This Book Is For* Penetration Testers, IT professional or a security consultant who wants to maximize the success of your network testing using some of the advanced features of Kali Linux, then this book is for you. Some prior exposure to basics of penetration testing/ethical hacking would be helpful in making the most out of this title. What You Will Learn* Select and configure the most effective tools from Kali Linux to test network security* Employ stealth to avoid detection in the network being tested* Recognize when stealth attacks are being used against your network* Exploit networks and data systems using wired and wireless networks as well as web services* Identify and download valuable data from target systems* Maintain access to compromised systems* Use social engineering to compromise the weakest part of the network—the end users In Detail* This book will take you, as a tester or security practitioner through the journey of reconnaissance, vulnerability assessment, exploitation, and post-exploitation activities used by penetration testers and hackers. We will start off by using a laboratory environment to validate tools and techniques, and using an application that supports a collaborative approach to penetration testing. Further we will get acquainted with passive reconnaissance with open source intelligence and active reconnaissance of the external and internal networks. We will also focus on how to select, use, customize, and interpret the results from a variety of different vulnerability scanners. Specific routes to the target will also be examined, including bypassing physical security and exfiltration of data using different techniques. You will also get to grips with concepts such as social engineering, attacking wireless networks, exploitation of web applications and remote access connections. Later you will learn the practical aspects of attacking user client systems by backdooring executable files. You will focus on the most vulnerable part of the network—directly and bypassing the controls, attacking the end user and maintaining persistence across through social media. You will also explore approaches to carrying out advanced penetration testing in tightly secured environments, and the book's hands-on approach will help you understand everything you need to know during a Red teaming exercise or penetration testing Style and approach An advanced level tutorial that follows a practical approach and proven methods to maintain top notch security of your networks.

Unauthorised Access Jan 13 2021 The first guide to planning and performing a physical penetration test on your computer's security Most IT security teams concentrate on keeping networks and systems safe from attacks from the outside-but what if your attacker was on the inside? While nearly all IT teams perform a variety of network and application penetration testing procedures, an audit and test of the physical location has not been as prevalent. IT teams are now increasingly requesting physical penetration tests, but there is little available in terms of training. The goal of the test is to demonstrate any deficiencies in operating procedures concerning physical security. Featuring a Foreword written by world-renowned hacker Kevin D. Mitnick and lead author of The Art of Intrusion and The Art of Deception, this book is the first guide to planning and performing a physical penetration test. Inside, IT security expert Wil Allsopp guides you through the entire process from gathering intelligence, getting inside, dealing with threats, staying hidden (often in plain sight), and getting access to networks and data. Teaches IT security teams how to break into their own facility in order to defend against such attacks, which is often overlooked by IT security teams but is of critical importance Deals with intelligence gathering, such as getting access building blueprints and satellite imagery, hacking security cameras, planting bugs, and eavesdropping on security channels Includes safeguards for consultants paid to probe facilities unbeknownst to staff Covers preparing the network and presenting it to management In order to defend data, you need to think like a thief-let Unauthorised Access show you how to get inside.

Hands-On Application Penetration Testing with Burp Suite Mar 15 2021 Test, fuzz, and break web applications and services using Burp Suite's powerful capabilities Key Features Master the skills to perform various types of security tests on your web applications Get hands-on experience working with components like scanner, proxy, intruder and much more Discover the best-way to penetrate and test web applications Book Description Burp suite is a set of graphic tools focused towards penetration testing of web applications. Burp suite is widely used for web penetration testing by many security professionals for performing different web-level security tasks. The book starts by setting up the environment to begin an application penetration test. You will be able to configure the client and apply target whitelisting. You will also learn to setup and configure Android and IOS devices to work with Burp Suite. The book will explain how various features of Burp Suite can be used to detect various vulnerabilities as part of an application penetration test. Once detection is completed and the vulnerability is confirmed, you will be able to exploit a detected vulnerability using Burp Suite. The book will also cover advanced concepts like writing extensions and macros for Burp suite. Finally, you will discover various steps that are taken to identify the target, discover weaknesses in the authentication mechanism, and finally break the authentication implementation to gain access to the administrative console of the application. By the end of this book, you will be able to effectively perform end-to-end penetration testing with Burp Suite. What you will learn Set up Burp Suite and its configurations for an application penetration test Proxy application traffic from browsers and mobile devices to the server Discover and identify application security issues in various scenarios Exploit discovered vulnerabilities to execute commands Exploit discovered vulnerabilities to gain access to data in various datastores Write your own Burp Suite plugin and explore the Infiltrator module Write macros to automate tasks in Burp Suite Who this book is for If you are interested in learning how to test web applications and the web part of mobile applications using Burp, then this is the book for you. It is specifically designed to meet your needs if you have basic experience in using Burp and are now aiming to become a professional Burp user.

Advanced Infrastructure Penetration Testing Sep 28 2019 A highly detailed guide to performing powerful attack vectors in many hands-on scenarios and defending significant security flaws in your company's infrastructure Key Features Advanced exploitation techniques to breach modern operating systems and complex network devices Learn about Docker breakouts, Active Directory delegation, and CRON jobs Practical use cases to deliver an intelligent endpoint-protected system Book Description It has always been difficult to gain hands-on experience and a comprehensive understanding of advanced penetration testing techniques and vulnerability assessment and management. This book will be your one-stop solution to compromising complex network devices and modern operating systems. This book provides you with advanced penetration testing techniques that will help you exploit databases, web and application servers, switches or routers, Docker, VLAN, VoIP, and VPN. With this book, you will explore exploitation abilities such as offensive PowerShell tools and techniques, CI servers, database exploitation, Active Directory delegation, kernel exploits, cron jobs, VLAN hopping, and Docker breakouts. Moving on, this book will not only walk you through managing vulnerabilities, but will also teach you how to ensure endpoint protection. Toward the end of this book, you will also discover post-exploitation tips, tools, and methodologies to help your organization build an intelligent security system. By the end of this book, you will have mastered the skills and methodologies needed to breach infrastructures and provide complete endpoint protection for your system. What you will learn Exposure to advanced infrastructure penetration testing techniques and methodologies Gain hands-on experience of penetration testing in Linux system vulnerabilities and memory exploitation Understand what it takes to break into enterprise networks Learn to secure the configuration management environment and continuous delivery pipeline Gain an understanding of how to exploit networks and IoT devices Discover real-world, post-exploitation techniques and countermeasures Who this book is for If you are a system administrator, SOC analyst, penetration tester, or a network engineer and want to take your penetration testing skills and security knowledge to the next level, then this book is for you. Some prior experience with penetration testing tools and knowledge of Linux and Windows command-line syntax is beneficial.

Penetration Testing Azure for Ethical Hackers Jun 17 2021 Simulate real-world attacks using tactics, techniques, and procedures that adversaries use during cloud breaches Key Features Understand the different Azure attack techniques and methodologies used by hackers Find out how you can ensure end-to-end cybersecurity in the Azure ecosystem Discover various tools and techniques to perform successful penetration tests on your Azure infrastructure Book 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-fault, 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 learn Identify how administrators misconfigure Azure services, leaving them open to exploitation Understand how to detect cloud infrastructure, service, and application misconfigurations Explore processes and techniques for exploiting common Azure security issues Use on-premises networks to pivot and escalate access within Azure Diagnose gaps and weaknesses in Azure security implementations Understand how attackers can escalate privileges in Azure AD Who 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.

The Basics of Hacking and Penetration Testing Jun 29 2022 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. You learn how to properly utilize and interpret the results of modern day hacking tools, which are required to complete a penetration test. Tool coverage will include, Backtrack Linux, Google, Whois, Nmap, Nessus, Metasploit, Netcat, Netbus, and more. A simple and clean explanation of how to utilize these tools will allow you to gain a solid understanding of each of the four phases and prepare them to take on more in-depth texts and topics. This book includes the use of a single example (pen test target) all the way through the book which allows you to clearly see how the tools and phases relate. 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. 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 Backtrack Linux distribution and focuses on the seminal tools required to complete a penetration test.

Cone Penetration Testing 2022 Feb 23 2022 This volume contains the proceedings of the 5th International Symposium on Cone Penetration Testing (CPT'22), held in Bologna, Italy, 8-10 June 2022. More than 500 authors - academics, researchers, practitioners and manufacturers - contributed to the peer-reviewed papers included in this book, which includes three keynote lectures, four invited lectures and 169 technical papers. The contributions provide a full picture of the current knowledge and major trends in CPT research and development, with respect to innovations in instrumentation, latest advances in data interpretation, and emerging fields of CPT application. The paper topics encompass three well-established topic categories typically addressed in CPT events: - Equipment and Procedures - Data Interpretation - Applications. Emphasis is placed on the use of statistical approaches and innovative numerical strategies for CPT data interpretation, liquefaction studies, application of CPT to offshore engineering, comparative studies between CPT and other in-situ tests. Cone Penetration Testing 2022 contains a wealth of information that could be useful for researchers, practitioners and all those working in the broad and dynamic field of cone penetration testing.

Kali Linux Hacking Sep 08 2020 Do you want to become a proficient specialist in cybersecurity and you want to learn the fundamentals of ethical hacking? Do you want to have a detailed overview of all the basic tools provided by the best Linux distribution for ethical hacking? Have you scoured the internet looking for the perfect resource to help you get started with hacking, but became overwhelmed by the amount of disjointed information available on the topic of hacking and cybersecurity? If you answered yes to any of these questions, then this is the book for you. Hacking is becoming more complex and sophisticated, and companies are scrambling to protect their digital assets against threats by setting up cybersecurity systems. These systems need to be routinely checked to ensure that these systems do the jobs they're designed to do. The people who can do these checks are penetration testers and ethical hackers, programs who are trained to find and exploit vulnerabilities in networks and proffer ways to cover them up. Now more than ever, companies are looking for penetration testers and cybersecurity professionals who have practical, hands-on experience with Kali Linux and other open-source hacking tools. In this powerful book, you're going to learn how to master the industry-standard platform for hacking, penetration and security testing—Kali Linux. This book assumes you know nothing about Kali Linux and hacking and will start from scratch and build up your practical knowledge on how to use Kali Linux and other open-source tools to become a hacker as well as understand the processes behind a successful penetration test. Here's a preview of what you're going to learn in Kali Linux Hacking: A concise introduction to the concept of "hacking" and Kali Linux Everything you need to know about the different types of hacking, from session hijacking and SQL injection to phishing and DOS attacks Why hackers aren't always bad guys as well as the 8 hacker types in today's cyberspace Why Kali Linux is the platform of choice for many amateur and professional hackers Step-by-step instructions to set up and install Kali Linux on your computer How to master the Linux terminal as well as fundamental Linux commands you absolutely need to know about A complete guide to using Nmap to understand, detect and exploit vulnerabilities How to effectively stay anonymous while carrying out hacking attacks or penetration testing How to use Bash and Python scripting to become a better hacker...and tons more! Designed with complete beginners in mind, this book is packed with practical examples and real-world hacking techniques explained in plain, simple English. This book is for the new generation of 21st-century hackers and cyber defenders and will help you level up your skills in cybersecurity and pen-testing. Whether you're just getting started with hacking or you're preparing for a career change into the field of cybersecurity, or are simply looking to buff up your resume and become more attractive to employers, Kali Linux Hacking is the book that you need! Would You Like To Know More? Click Buy Now With 1-Click or Buy Now to get started!

Penetration Testing for Jobseekers Mar 27 2022 Understand and Conduct Ethical Hacking and Security Assessments KEY FEATURES ? Practical guidance on discovering, assessing, and mitigating web, network, mobile, and wireless vulnerabilities. ? Experimentation with Kali Linux, Burp Suite, MobSF, Metasploit and Aircrack-suite. ? In-depth explanation of topics focusing on how to crack ethical hacking interviews. DESCRIPTION Penetration Testing for Job Seekers is an attempt to discover the way to a spectacular career in cyber security, specifically penetration testing. This book offers a practical approach by discussing several computer and network fundamentals before delving into various penetration testing approaches, tools, and techniques. Written by a veteran security professional, this book provides a detailed look at the dynamics that form a person's career as a penetration tester. This book is divided into ten chapters and covers numerous facets of penetration testing, including web application, network, Android application, wireless penetration testing, and creating excellent penetration test reports. This book also shows how to set up an in-house hacking lab from scratch to improve your skills. A penetration tester's professional path, possibilities, average day, and day-to-day obstacles are all outlined to help readers better grasp what you may anticipate from a cybersecurity career. Using this book, readers will be able to boost their employability and job market relevance, allowing them to sprint towards a lucrative career as a penetration tester. WHAT YOU WILL LEARN ? Perform penetration testing on web apps, networks, android apps, and wireless networks. ? Access to the most widely used penetration testing methodologies and standards in the industry. ? Use an artistic approach to find security holes in source code. ? Learn how to put together a high-quality penetration test report. ? Popular technical interview questions on ethical hacker and pen tester job roles. ? Exploration of different career options, paths, and possibilities in cyber security. WHO THIS BOOK IS FOR This book is for aspiring security analysts, pen testers, ethical hackers, anyone who wants to learn how to become a successful pen tester. A fundamental understanding of network principles and workings is helpful but not required. TABLE OF CONTENTS 1. Cybersecurity, Career Path, and Prospects 2. Introduction to Penetration Testing 3. Setting Up Your Lab for Penetration Testing 4. Web Application and API Penetration Testing 5. The Art of Secure Source Code Review 6. Penetration Testing Android Mobile Applications 7. Network Penetration Testing 8. Wireless Penetration Testing 9. Report Preparation and Documentation 10. A Day in the Life of a Pen Tester

AWS Penetration Testing Jul 07 2020 Get to grips with security assessment, vulnerability exploitation, workload security, and encryption with this guide to ethical hacking and learn to secure your AWS environment Key Features Perform cybersecurity events such as red or blue team activities and functional testing Gain an overview and understanding of AWS penetration testing and security Make the most of your AWS cloud infrastructure by learning about AWS fundamentals and exploring pentesting best practices Book Description Cloud security has always been treated as the highest priority by AWS while designing a robust cloud infrastructure. AWS has now extended its support to allow users and security experts to perform penetration tests on its environment. This has not only revealed a number of loopholes and brought vulnerable points in their existing system to the fore, but has also opened up opportunities for organizations to build a secure cloud environment. This book teaches you how to perform penetration tests in a controlled AWS environment. You'll begin by performing security assessments of major AWS resources such as Amazon EC2 instances, Amazon S3, Amazon API Gateway, and AWS Lambda. Throughout the course of this book, you'll also learn about specific tests such as exploiting applications, testing permissions flaws, and discovering weak policies. Moving on, you'll discover how to establish private-cloud access through backdoor Lambda functions. As you advance, you'll explore the no-go areas where users can't make changes due to vendor restrictions and find out how you can avoid being flagged to AWS in these cases. Finally, this book will take you through tips and tricks for securing your cloud environment in a professional way. By the end of this penetration testing book, you'll have become well-versed in a variety of ethical hacking techniques for securing your AWS environment against modern cyber threats. What you will learn Set up your AWS account and get well-versed in various pentesting services Delve into a variety of cloud pentesting tools and methodologies Discover how to exploit vulnerabilities in both AWS and applications Understand the legality of pentesting and learn how to stay in scope Explore cloud pentesting best practices, tips, and tricks Become competent at using tools such as Kali Linux, Metasploit, and Nmap Get to grips with post-exploitation procedures and find out how to write pen testing reports Who this book is for If you are a network engineer, system administrator, or system operator looking to secure your AWS environment against external cyberattacks, then this book is for you. Ethical hackers, penetration testers, and security consultants who want to enhance their cloud security skills will also find this book useful. No prior experience in penetration testing is required; however, some understanding of cloud computing or AWS cloud is recommended.

Metasploit Penetration Testing Cookbook Jan 01 2020 Over 80 recipes to master the most widely used penetration testing framework. Penetration Testing Basics Jun 25 2019 Learn how to break systems, networks, and software in order to determine where the bad guys might get in. Once the holes have been determined, this short book discusses how they can be fixed. Until they have been located, they are exposures to your organization. By reading Penetration Testing Basics, you'll gain the foundations of a simple methodology used to perform penetration testing on systems and networks for which you are responsible. What You Will Learn Identify security vulnerabilities Use some of the top security tools to identify holes Read reports from testing tools Spot and negate common attacks Identify common Web-based attacks and exposures as well as recommendations for closing those holes Who This Book Is For Anyone who has some familiarity with computers and an interest in information security and penetration testing. Windows and Linux Penetration Testing from Scratch Nov 30 2019 Master the art of identifying and exploiting vulnerabilities with Metasploit, Empire, PowerShell, and Python, turning Kali Linux into your fighter cockpit Key Features Map your client's attack surface with Kali Linux Discover the craft of shellcode injection and managing multiple compromises in the environment Understand both the attacker and the defender mindset Book Description Let's be honest—security testing can get repetitive. If you're ready to break out of the routine and embrace the art of penetration testing, this book will help you to distinguish yourself to your clients. This pen testing book is your guide to learning advanced techniques to attack Windows and Linux environments from the indispensable platform, Kali Linux. You'll work through core network hacking concepts and advanced exploitation techniques that leverage both technical and human factors to maximize success. You'll also explore how to leverage public resources to learn more about your target, discover potential targets, analyze them, and gain a foothold using a variety of exploitation techniques while dodging defenses like antivirus and firewalls. The book focuses on leveraging target resources, such as PowerShell, to execute powerful and difficult-to-detect attacks. Along the way, you'll enjoy reading about how these methods work so that you walk away with the necessary knowledge to explain your findings to clients from all backgrounds. Wrapping up with post-exploitation strategies, you'll be able to go deeper and

keep your access. By the end of this book, you'll be well-versed in identifying vulnerabilities within your clients' environments and providing the necessary insight for proper remediation. What you will learn Get to know advanced pen testing techniques with Kali Linux Gain an understanding of Kali Linux tools and methods from behind the scenes Get to grips with the exploitation of Windows and Linux clients and servers Understand advanced Windows concepts and protection and bypass them with Kali and living-off-the-land methods Get the hang of sophisticated attack frameworks such as Metasploit and Empire Become adept in generating and analyzing shellcode Build and tweak attack scripts and modules Who this book is for This book is for penetration testers, information technology professionals, cybersecurity professionals and students, and individuals breaking into a pentesting role after demonstrating advanced skills in boot camps. Prior experience with Windows, Linux, and networking is necessary.

Penetration Testing Nov 03 2022 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.

Professional Penetration Testing Jul 19 2021 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

Learn Penetration Testing Apr 03 2020 Get up to speed with various penetration testing techniques and resolve security threats of varying complexity Key Features Enhance your penetration testing skills to tackle security threats Learn to gather information, find vulnerabilities, and exploit enterprise defenses Navigate secured systems with the most up-to-date version of Kali Linux (2019.1) and Metasploit (5.0.0) Book Description Sending information via the internet is not entirely private, as evidenced by the rise in hacking, malware attacks, and security threats. With the help of this book, you'll learn crucial penetration testing techniques to help you evaluate enterprise defenses. You'll start by understanding each stage of pentesting and deploying target virtual machines, including Linux and Windows. Next, the book will guide you through performing intermediate penetration testing in a controlled environment. With the help of practical use cases, you'll also be able to implement your learning in real-world scenarios. By studying everything from setting up your lab, information gathering and password attacks, through to social engineering and post exploitation, you'll be able to successfully overcome security threats. The book will even help you leverage the best tools, such as Kali Linux, Metasploit, Burp Suite, and other open source pentesting tools to perform these techniques. Toward the later chapters, you'll focus on best practices to quickly resolve security threats. By the end of this book, you'll be well versed with various penetration testing techniques so as to be able to tackle security threats effectively What you will learn Perform entry-level penetration tests by learning various concepts and techniques Understand both common and not-so-common vulnerabilities from an attacker's perspective Get familiar with intermediate attack methods that can be used in real-world scenarios Understand how vulnerabilities are created by developers and how to fix some of them at source code level Become well versed with basic tools for ethical hacking purposes Exploit known vulnerable services with tools such as Metasploit Who this book is for If you're just getting started with penetration testing and want to explore various security domains, this book is for you. Security professionals, network engineers, and amateur ethical hackers will also find this book useful. Prior knowledge of penetration testing and ethical hacking is not necessary.

Hacking For Dummies Mar 03 2020 Stop hackers before they hack you! In order to outsmart a would-be hacker, you need to get into the hacker's mindset. And with this book, thinking like a bad guy has never been easier. In Hacking For Dummies, expert author Kevin Beaver shares his knowledge on penetration testing, vulnerability assessments, security best practices, and every aspect of ethical hacking that is essential in order to stop a hacker in their tracks. Whether you're worried about your laptop, smartphone, or desktop computer being compromised, this no-nonsense book helps you learn how to recognize the vulnerabilities in your systems so you can safeguard them more diligently—with confidence and ease. Get up to speed on Windows 10 hacks Learn about the latest mobile computing hacks Get free testing tools Find out about new system updates and improvements There's no such thing as being too safe—and this resourceful guide helps ensure you're protected.

Hands-On Penetration Testing with Python Aug 20 2021 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.