# Penetration Testing A Hands On Introduction To Hacking

"Metasploit is the best and most widely used tool for penetration testing, providing powerful attack simulations, security assessment management, and more. Metasploit is used by White Hat, and by Black Hat, hackers. Metasploit is a playground for hackers where they demonstrate their skill by protecting or damaging the target. In this course, you'll learn how to use Metasploit to enumerate services, identify potential weaknesses, test vulnerabilities through exploitation, and gather evidence for reporting. First, you'll explore several supporting tools on Kali Linux. Next, you'll explore how exploits and payloads work together to gain access to systems. Finally, you'll learn how Metasploit Framework works. By the end of this course, you'll have a better understanding of how to use Metasploit to quickly assess the security posture of systems and networks to reduce the risk of attack."--Resource description page.

Identify, exploit, and test web application security with ease Key Features Get up to speed with Metasploit and discover how to use it for pentesting Understand how to exploit and protect your web environment effectively Learn how an exploit works and what causes vulnerabilities Book Description Metasploit has been a crucial security tool for many years. However, there are only a few modules that Metasploit has made available to the public for pentesting web applications. In this book, you'll explore another aspect of the framework – web applications – which is not commonly used. You'll also discover how Metasploit, when used with its inbuilt GUI, simplifies web application penetration testing. The book starts by focusing on the Metasploit setup, along with covering the life cycle of the penetration testing process. Then, you will explore Metasploit terminology and the web GUI, which is available in the Metasploit Community Edition. Next, the book will take you through pentesting popular content management systems such as Drupal, WordPress, and Joomla, which will also include studying the latest CVEs and understanding the root cause of vulnerability in detail. Later, you'll gain insights into the vulnerability assessment and exploitation of technological platforms such as JBoss, Jenkins, and Tomcat. Finally, you'll learn how to fuzz web applications to find logical security vulnerabilities using third-party tools. By the end of this book, you'll have a solid understanding of how to exploit and validate vulnerabilities by working with various tools and techniques. What you will learn Get up to speed with setting up and installing the Metasploit framework Gain first-hand experience of the Metasploit web interface Use Metasploit for web-application reconnaissance Understand how to pentest various content management systems Pentest platforms such as JBoss, Tomcat, and Jenkins Become well-versed with fuzzing web applications Write and automate penetration testing reports Who this book is for This book is for web security analysts, bug bounty hunters, security professionals, or any stakeholder in the security sector who wants to delve into web application security testing. Professionals who are not experts with command line tools or Kali Linux and prefer Metasploit’s graphical user interface (GUI) will also find this book useful. No experience with Metasploit is required, but basic knowledge of Linux and web application pentesting will be helpful.

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.

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.

Fourth Edition (Traditional Chinese Translation) Sheds New Light on Open Source Intelligence Collection and Analysis. Author Michael Bazzell has been well known and respected in government circles for his ability to locate personal information about any target through Open Source Intelligence (OSINT). In this book, he shares his methods in great detail. Each step of his process is explained throughout sixteen chapters of specialized websites, application programming interfaces, and software solutions. Based on his live and online video training at IntelTechniques.com, over 250 resources are identified with narrative tutorials and screen captures. This book will serve as a reference guide for anyone that is responsible for the collection of online content. It is written in a hands-on style that encourages the reader to execute the tutorials as they go. The search techniques offered will inspire analysts to "think outside the box" when scouring the internet for personal information. Much of the content of this book has never been discussed in any publication. Always thinking like a hacker, the author has identified new ways to use various technologies for an unintended purpose. This book will improve anyone's online investigative skills. Among other techniques, you will learn how to locate: Hidden Social Network Content Cell Phone Owner Information Twitter GPS & Account Data Hidden Photo GPS & Metadata Deleted Websites & Posts Website Owner Information Alias Social Network Profiles Additional User Accounts Sensitive Documents & Photos Live Streaming Social Content IP Addresses of Users Newspaper Archives & Scans Social Content by Location Private Email Addresses Hidden Personal Videos Duplicate Copies of Photos Personal Radio Communications Compromised Email Information Wireless Routers by Location Hidden Mapping Applications Complete Facebook Data Free Investigative Software Alternative Search Engines Mobile App Network Data Unlisted Addresses Unlisted Phone Numbers Useful Browser Extensions Public Government Records Document Metadata Rental Vehicle Contracts Online Criminal Activity

You are about to discover how to start hacking with the #1 hacking/penetration testing tool, Kali Linux, in no time, even if you've never hacked before! Kali Linux is the king of all penetration testing tools out there. But while its 600+ pre-installed tools and utilities are meant to make penetration testing and forensics easy, at first, it can be overwhelming for experienced and aspiring security professionals to decide which tool to use to conduct a specific penetration test. That's where this book comes in to streamline your learning experience! If you are uncertain about where to begin even after reading and watching tons of free information online, this book will give you the much needed structure to go all in into the world of ethical hacking into secure computer systems with the best tool for the job. Since its introduction in 2012 as a successor to the previous version, Back Track Linux, Kali Linux has grown in popularity and capabilities to become the go-to open source security tool for information security professionals around the world. And this book will show you how to use it like the pros use it even if you've never stepped into a formal Kali Linux class before! In this book, we are going to cover the major features & tools provided by Kali Linux, including: Downloading, installation and set up Information gathering tools Vulnerability assessment Wireless attacks Web application attacks Exploitation tools Forensics tools

Sniffing and spoofing Password cracking Maintaining access Social engineering tools Reverse engineering tools Hardware hacking tools Reporting tools Denial of service attacks And much more! We shall cover each of these features & tools individually so that after reading this guide, you have hands-on experience with using Kali Linux and can use what you learn when completing the hands-on Kali Linux practice project found in the part 17 of this guide. To make the learning experience faster and easier for you, for this hands-on, Kali Linux guide, we may have to install some other tools needed to make it easier to learn how to use Kali Linux for penetration testing and cyber security forensics. Everything is laid out with easy to follow examples and illustrations to help you to follow through, practice and ultimately remember whatever you are learning! What are you waiting for? Click Buy Now In 1-Click or Buy Now at the top of this page to get started!

Perform effective and efficient penetration testing in an enterprise scenario KEY FEATURES ? Understand the penetration testing process using a highly customizable modular framework. ? Exciting use-cases demonstrating every action of penetration testing on target systems. ? Equipped with proven techniques and best practices from seasoned pen-testing practitioners. ? Experience-driven from actual penetration testing activities from multiple MNCs. ? Covers a distinguished approach to assess vulnerabilities and extract insights for further investigation. DESCRIPTION This book is designed to introduce the topic of penetration testing using a structured and easy-to-learn process-driven framework. Understand the theoretical aspects of penetration testing and create a penetration testing lab environment consisting of various targets to learn and practice your skills. Learn to comfortably navigate the Kali Linux and perform administrative activities, get to know shell scripting, and write simple scripts to effortlessly run complex commands and automate repetitive testing tasks. Explore the various phases of the testing framework while practically demonstrating the numerous tools and techniques available within Kali Linux. Starting your journey from gathering initial information about the targets and performing enumeration to identify potential weaknesses and sequentially building upon this knowledge to refine the attacks and utilize weaknesses to fully compromise the target machines. The authors of the book lay a particularly strong emphasis on documentation and the importance of generating crisp and concise reports which keep the various stakeholders' requirements at the center stage. WHAT YOU WILL LEARN ? Understand the Penetration Testing Process and its various phases. ? Perform practical penetration testing using the various tools available in Kali Linux. ? Get to know the process of Penetration Testing and set up the Kali Linux virtual environment. ? Perform active and passive reconnaissance. ? Learn to execute deeper analysis of vulnerabilities and extract exploit codes. ? Learn to solve challenges while performing penetration testing with expert tips. WHO THIS BOOK IS FOR This book caters to all IT professionals with a basic understanding of operating systems, networking, and Linux can use this book to build a skill set for performing real-world penetration testing. TABLE OF CONTENTS 1. The Basics of Penetration Testing 2. Penetration Testing Lab 3. Finding Your Way Around Kali Linux 4. Understanding the PT Process and Stages 5. Planning and Reconnaissance 6. Service Enumeration and Scanning 7. Vulnerability Research 8. Exploitation 9. Post Exploitation 10. Reporting 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.

Identify vulnerabilities across applications, network and systems using simplified cybersecurity scripting KEY FEATURES ? Exciting coverage on red teaming methodologies and penetration testing techniques. ? Explore the exploitation development environment and process of creating exploit scripts. ? Includes powerful Python libraries to analyze the web and helps identifying critical vulnerabilities. ? Conduct wireless attacks and identify potential threats using Python. DESCRIPTION This book starts with an understanding of penetration testing and red teaming methodologies and teaches Python 3.x from scratch for those who are not familiar with programming. The book gives the skills of how to create scripts for cracking, and brute force attacks. The second part of this book focuses on the network and wireless level. The book teaches you the skills of how to create an offensive tool using Python 3.x to identify different services and ports using different Python network modules and conducting network attacks. In the network monitoring section, you will be able to monitor layers 3 and 4. And finally, you will be able to conduct different attacks on wireless. The last part of this book focuses on web applications and exploitation developments. It focuses on how to create scripts to extract web information such as links, images, documents, etc. It also focuses on how to create scripts to identify and exploit web vulnerabilities and how to bypass WAF. The last chapter of this book focuses on exploitation development starting with how to play with the stack and then moving on to how to use Python in fuzzing and creating exploitation scripts. WHAT YOU WILL LEARN ? Learn to code Python scripts from scratch to identify web vulnerabilities. ? Conduct network attacks, create offensive tools, and identify vulnerable services and ports. ? Perform deep monitoring of network up to layers 3 and 4. ? Execute web scraping scripts to extract images, documents, and links. WHO THIS BOOK IS FOR This book is for Penetration Testers, Security Researchers, Red Teams, Security Auditors and IT Administrators who want to start with an action plan in protecting their IT systems. All you need is

some basic understanding of programming concepts and working of IT systems. Hands-on experience with python will be more beneficial but not required. TABLE OF CONTENTS 1. Start with Penetration Testing and Basic Python 2. Cracking with Python 3. Service and Applications Brute Forcing with Python 4. Python Services Identifications - Ports and Banner 5. Python Network Modules and Nmap 6. Network Monitoring with Python 7. Attacking Wireless with Python 8. Analyze Web Applications with Python 9. Attack Web Application with Python 10. Exploitation Development with Python

Implement defensive techniques in your ecosystem successfully with Python Key Features Identify and expose vulnerabilities in your infrastructure with Python Learn custom exploit development . Make robust and powerful cybersecurity tools with Python Book 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 learn Get to grips with Custom vulnerability scanner development Familiarize yourself with web application scanning automation and exploit development Walk through day-to-day cybersecurity scenarios that can be automated with Python Discover enterprise-or organization-specific use cases and threat-hunting automation Understand 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 responses Explore Security Operations Centre (SOC) use cases Get to understand Data Science, Python, and cybersecurity all under one hood Who 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 .

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.

A simultaneous Traditional Chinese translation of the much talked about book No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State by Glenn Greenwald. The book is the winner of the 2014 Pulitzer Prize for Public Service. In Traditional Chinese. Annotation copyright Tsai Fong Books, Inc. Distributed by Tsai Fong Books, Inc.

Penetration TestingA Hands-On Introduction to HackingNo Starch Press

Master the art of identifying vulnerabilities within the Windows OS and develop the desired solutions for it using Kali Linux. Key Features Identify the vulnerabilities in your system using Kali Linux 2018.02 Discover the art of exploiting Windows kernel drivers Get to know several bypassing techniques to gain control of your Windows environment Book Description Windows has always been the go-to platform for users around the globe to perform administration and ad hoc tasks, in settings that range from small offices to global enterprises, and this massive footprint makes securing Windows a unique challenge. This book will enable you to distinguish yourself to your clients. In this book, you'll learn advanced techniques to attack Windows environments from the indispensable toolkit that is Kali Linux. We'll work through core network hacking concepts and advanced Windows exploitation techniques, such as stack and heap overflows, precision heap spraying, and kernel exploitation, using coding principles that allow you to leverage powerful Python scripts and shellcode. We'll wrap up with post-exploitation strategies that enable you to go deeper and keep your access. Finally, we'll introduce kernel hacking fundamentals and fuzzing testing, so you can discover vulnerabilities and write custom exploits. By the end of this book, you'll be well-versed in identifying vulnerabilities within the Windows OS and developing the desired solutions for them. 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 See how to use Kali Linux at an advanced level Understand the exploitation of Windows kernel drivers

Understand advanced Windows concepts and protections, and how to bypass them using Kali Linux Discover Windows exploitation techniques, such as stack and heap overflows and kernel exploitation, through coding principles Who this book is for This book is for penetration testers, ethical hackers, and individuals breaking into the pentesting role after demonstrating an advanced skill in boot camps. Prior experience with Windows exploitation, Kali Linux, and some Windows debugging tools is necessary

Thousands of organizations are recognizing the crucial role of penetration testing in protecting their networks and digital assets. In some industries, "pentesting" is now an absolute requirement. This is the first systematic guidebook for the growing number of security professionals and students who want to master the discipline and techniques of penetration testing. Leading security expert, researcher, instructor, and author Chuck Easttom II has brought together all the essential knowledge in a single comprehensive guide that covers the entire penetration testing lifecycle. Easttom integrates concepts, terminology, challenges, and theory, and walks you through every step, from planning to effective post-test reporting. He presents a start-to-finish sample project relying on free open source tools, as well as quizzes, labs, and review sections throughout. Penetration Testing Fundamentals is also the only book to cover pentesting standards from NSA, PCI, and NIST. You don't need any prior pentesting knowledge to succeed with this practical guide: by the time you're finished, you'll have all the skills you need to conduct reliable, professional penetration tests.

Learn how to build an end-to-end Web application security testing framework KEY FEATURES ? Exciting coverage on vulnerabilities and security loopholes in modern web applications. ? Practical exercises and case scenarios on performing pentesting and identifying security breaches. ? Cutting-edge offerings on implementation of tools including nmap, burp suite and wireshark. DESCRIPTION Hands-on Penetration Testing for Web Applications offers readers with knowledge and skillset to identify, exploit and control the security vulnerabilities present in commercial web applications including online banking, mobile payments and e-commerce applications. We begin with exposure to modern application vulnerabilities present in web applications. You will learn and gradually practice the core concepts of penetration testing and OWASP Top Ten vulnerabilities including injection, broken authentication and access control, security misconfigurations and cross-site scripting (XSS). You will then gain advanced skillset by exploring the methodology of security testing and how to work around security testing as a true security professional. This book also brings cutting-edge coverage on exploiting and detecting vulnerabilities such as authentication flaws, session flaws, access control flaws, input validation flaws etc. You will discover an end-to-end implementation of tools such as nmap, burp suite, and wireshark. You will then learn to practice how to execute web application intrusion testing in automated testing tools and also to analyze

vulnerabilities and threats present in the source codes. By the end of this book, you will gain in-depth knowledge of web application testing framework and strong proficiency in exploring and building high secured web applications. WHAT YOU WILL LEARN ? Complete overview of concepts of web penetration testing. ? Learn to secure against OWASP TOP 10 web vulnerabilities. ? Practice different techniques and signatures for identifying vulnerabilities in the source code of the web application. ? Discover security flaws in your web application using most popular tools like nmap and wireshark. ? Learn to respond modern automated cyber attacks with the help of expert-led tips and tricks. ? Exposure to analysis of vulnerability codes, security automation tools and common security flaws. WHO THIS BOOK IS FOR This book is for Penetration Testers, ethical hackers, and web application developers. People who are new to security testing will also find this book useful. Basic knowledge of HTML, JavaScript would be an added advantage. TABLE OF CONTENTS 1. Why Application Security? 2. Modern application Vulnerabilities 3. Web Pentesting Methodology 4. Testing Authentication 5. Testing Session Management 6. Testing Secure Channels 7. Testing Secure Access Control 8. Sensitive Data and Information disclosure 9. Testing Secure Data validation 10. Attacking Application Users: Other Techniques 11. Attacking Application Users: Other Techniques 12. Automating Custom Attacks 13. Pentesting Tools 14. Static Code Analysis 15. Mitigations and Core Defense Mechanisms

Welcome to this comprehensive course on Ethical Hacking. This course assumes you have NO prior knowledge in hacking and by the end of it, you should be able to hack systems like black-hat hackers and secure them like security experts. This course is highly practical, but it will not neglect the theory, so we will begin with ethical hacking basics and the different fields in penetration testing, installing the needed and then we will start hacking systems straight away. From here onwards you will learn everything by example, by analysing and exploiting computer systems such as networks, servers, clients, websites and more.The course is divided into a number of sections, each section covers a penetration testing / hacking field, in each of these sections you'll first learn how the target system works, the weaknesses of this system, and how to practically exploit theses weaknesses and hack into it, not only that but you will also learn how to secure this system from the discussed attacks. This course will take you from a beginner to a more advanced level by the time you finish, you will have knowledge about most penetration testing fields. This book will ultimately enable you to become an Ethical Hacker that can Hack Computer Systems like Black Hat Hackers and Secure them like Security Experts.All the techniques in this course are practical and work against real systems, you will understand the whole mechanism of each technique first, then you will learn how to use it to hack into the target system, so by the end of the course you will be able to modify the these techniques to launch more powerful attacks, and adopt them to different situations and different scenarios.You will learn the following: -Start from scratch

up to a high-intermediate level-Learn what is ethical hacking, its fields and the different types of hackers-Install hacking lab & needed software-Hack & secure both WiFi & wired networks-Discover vulnerabilities & exploit them hack into servers-Hack secure systems using client-side and social engineering attacks-Use 40+ hacking tools such as Metasploit, Aircrack-ng, SQLmap.....etc-Understand how websites work, how to discover & exploit web vulnerabilities to gain control over websites-Secure systems from all the attacks shown-Install Kali Linux - a penetration testing operating system-Install Windows & vulnerable operating systems as virtual machines for testing-Learn linux basics-Learn Learn linux commands and how to interact with the terminal-Learn Network Penetration Testing-Network basics & how devices interact inside a network-Perform several practical attacks that can be used without knowing the key to the target network-Control connections of clients around you without knowing the password.-Gather detailed information about clients and networks like their OS, opened ports ...etc.-Crack WEP/WPA/WPA2 encryptions using several methods.-ARP Spoofing/ARP Poisoning-Launch Various Man In The Middle attacks.-Gain access to any account accessed by any client in your network.-Sniff packets from clients and analyse them to extract info such as: passwords, cookies, urls, videos, images.-Discover open ports, installed services and vulnerabilities on computer systems-Gain control over computer systems using server-side attacks-Exploit buffer overflows and code execution vulnerabilities to gain control over systems-Gain control over computer systems using client-side attacks-Gain control over computer systems using fake updates-Gain control over computer systems by backdooring downloads on the fly-Create undetectable backdoors-Backdoor normal programs-Backdoor any file type such as pictures, pdf's ...etc.-Gather information about people, such as emails, social media accounts, emails and friends-Use social engineering to gain full control over target systems

"Prepare yourself for common attacks, simulate real-world possibilities, and learn from test scenarios and case studies. You'll carry out exploitations, build/port exploits of various kinds in Metasploit, find weaknesses in target systems, and hunt for vulnerabilities using Metasploit and its supporting tools. You'll master the latest security techniques and methods that can be directly applied to scan, test, hack, and secure networks and systems with Metasploit. Towards the end of the course, you will implement time-saving techniques using Metasploit. By the end of the course, you will know how to fully protect your system using Metasploit, and will have gained the skills to carry out penetration testing in complex and highly-secured environments."--Resource description page.

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.

A complete pentesting guide facilitating smooth backtracking for working hackers About This Book Conduct network testing, surveillance, pen testing and forensics on MS Windows using Kali Linux Gain a deep understanding of the flaws in web applications and exploit them in a practical manner Pentest Android apps and perform various attacks in the real world using real case studies Who This Book Is For This course is for anyone who wants to learn about security. Basic knowledge of Android programming would be a plus. What You Will Learn Exploit several common Windows network vulnerabilities Recover lost files, investigate successful hacks, and discover hidden data in innocent-looking files Expose vulnerabilities present in web servers and their applications using server-side attacks Use SQL and cross-site scripting (XSS) attacks Check for XSS flaws using the burp suite proxy Acquaint yourself with the fundamental building blocks of Android Apps in the right way Take a look at how your personal data can be stolen by malicious attackers See how developers make mistakes that allow attackers to steal data from phones In Detail The need for penetration testers has grown well over what the IT industry ever anticipated. Running just a vulnerability scanner is no longer an effective method to determine whether a business is truly secure. This learning path will help you develop the most effective penetration testing skills to protect your Windows, web applications, and Android devices. The first module focuses on the Windows platform, which is one of the most common OSes, and managing its security spawned the discipline of IT security. Kali Linux is the premier platform for testing and maintaining Windows security. Employs the most advanced tools and techniques to reproduce the methods used by sophisticated hackers. In this module first,you'll be introduced to Kali's top ten tools and other useful reporting tools. Then, you will find your way around your target network and determine known vulnerabilities so you can exploit a system remotely. You'll not only learn to penetrate in the machine, but will also learn to work with Windows privilege escalations. The second module will help

you get to grips with the tools used in Kali Linux 2.0 that relate to web application hacking. You will get to know about scripting and input validation flaws, AJAX, and security issues related to AJAX. You will also use an automated technique called fuzzing so you can identify flaws in a web application. Finally, you'll understand the web application vulnerabilities and the ways they can be exploited. In the last module, you'll get started with Android security. Android, being the platform with the largest consumer base, is the obvious primary target for attackers. You'll begin this journey with the absolute basics and will then slowly gear up to the concepts of Android rooting, application security assessments, malware, infecting APK files, and fuzzing. You'll gain the skills necessary to perform Android application vulnerability assessments and to create an Android pentesting lab. This Learning Path is a blend of content from the following Packt products: Kali Linux 2: Windows Penetration Testing by Wolf Halton and Bo Weaver Web Penetration Testing with Kali Linux, Second Edition by Juned Ahmed Ansari Hacking Android by Srinivasa Rao Kotipalli and Mohammed A. Imran Style and approach This course uses easy-to-understand yet professional language for explaining concepts to test your network's security. Testing web security is best done through simulating an attack. Kali Linux lets you do this to professional standards and this is the book you need to be fully up-to-speed with this powerful open-source toolkit. Overview Learn key reconnaissance concepts needed as a penetration tester Attack and exploit key features, authentication, and sessions on web applications Learn how to protect systems, write reports, and sell web penetration testing services In Detail Kali Linux is built for professional penetration testing and security auditing. It is the next-generation of BackTrack, the most popular open-source penetration toolkit in the world. Readers will learn how to think like real attackers, exploit systems, and expose vulnerabilities. Even though web applications are developed in a very secure environment and have an intrusion detection system and firewall in place to detect and prevent any malicious activity, open ports are a pre-requisite for conducting online business. These ports serve as an open door for attackers to attack these applications. As a result, penetration testing becomes essential to test the integrity of web-applications. Web Penetration Testing with Kali Linux is a hands-on guide that will give you step-by-step methods on finding vulnerabilities and exploiting web applications. "Web Penetration Testing with Kali Linux" looks at the aspects of web penetration testing from the mind of an attacker. It provides real-world, practical step-by-step instructions on how to perform web penetration testing exercises. You will learn how to use network reconnaissance to pick your targets and gather information. Then, you will use server-side attacks to expose vulnerabilities in web servers and their applications. Client attacks will exploit the way end users use web applications and their workstations. You will also learn how to use open source tools to write reports and get tips on how to sell penetration tests and look out for common pitfalls. On the completion of this book, you will have the skills needed to use Kali Linux for web penetration tests

and expose vulnerabilities on web applications and clients that access them. What you will learn from this book Perform vulnerability reconnaissance to gather information on your targets Expose server vulnerabilities and take advantage of them to gain privileged access Exploit client-based systems using web application protocols Learn how to use SQL and cross-site scripting (XSS) attacks Steal authentications through session hijacking techniques Harden systems so other attackers do not exploit them easily Generate reports for penetration testers Learn tips and trade secrets from real world penetration testers Approach "Web Penetration Testing with Kali Linux" contains various penetration testing methods using BackTrack that will be used by the reader. It contains clear step-by-step instructions with lot of screenshots. It is written in an easy to understand language which will further simplify the understanding for the user."

Leading security expert, researcher, instructor, and author Chuck Easttom II has brought together all the essential knowledge in a single comprehensive guide that covers the entire penetration testing lifecycle. Easttom integrates concepts, terminology, challenges, and theory, and walks you through every step, from planning to effective post-test reporting. He presents a start-to-finish sample project relying on free open source tools, as well as quizzes, labs, and review sections throughout. Penetration Testing Fundamentals is also the only book to cover pentesting standards from NSA, PCI, and NIST.

Learn the art of building a low-cost, portable hacking arsenal using Raspberry Pi 3 and Kali Linux 2 About This Book Quickly turn your Raspberry Pi 3 into a low-cost hacking tool using Kali Linux 2 Protect your confidential data by deftly preventing various network security attacks Use Raspberry Pi 3 as honeypots to warn you that hackers are on your wire Who This Book Is For If you are a computer enthusiast who wants to learn advanced hacking techniques using the Raspberry Pi 3 as your pentesting toolbox, then this book is for you. Prior knowledge of networking and Linux would be an advantage. What You Will Learn Install and tune Kali Linux 2 on a Raspberry Pi 3 for hacking Learn how to store and offload pentest data from the Raspberry Pi 3 Plan and perform man-in-the-middle attacks and bypass advanced encryption techniques Compromise systems using various exploits and tools using Kali Linux 2 Bypass security defenses and remove data off a target network Develop a command and control system to manage remotely placed Raspberry Pis Turn a Raspberry Pi 3 into a honeypot to capture sensitive information In Detail This book will show you how to utilize the latest credit card sized Raspberry Pi 3 and create a portable, low-cost hacking tool using Kali Linux 2. You'll begin by installing and tuning Kali Linux 2 on Raspberry Pi 3 and then get started with penetration testing. You will be exposed to various network security scenarios such as wireless security, scanning network packets in order to detect any issues in the network, and capturing sensitive data. You will also learn how to plan and perform various attacks such as man-in-the-middle, password cracking, bypassing SSL

encryption, compromising systems using various toolkits, and many more. Finally, you'll see how to bypass security defenses and avoid detection, turn your Pi 3 into a honeypot, and develop a command and control system to manage a remotely-placed Raspberry Pi 3. By the end of this book you will be able to turn Raspberry Pi 3 into a hacking arsenal to leverage the most popular open source toolkit, Kali Linux 2.0. Style and approach This concise and fast-paced guide will ensure you get hands-on with penetration testing right from the start. You will quickly install the powerful Kali Linux 2 on your Raspberry Pi 3 and then learn how to use and conduct fundamental penetration techniques and attacks.
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 costsWho This Book Is ForPenetration 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 usersIn DetailThis 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 access 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 testingStyle and approachAn advanced level tutorial that follows a practical approach and proven methods to maintain top notch security of your networks.

This book will help you in Learning the Basics of Penetration Testing. It will cover the main features of Penetration Testing and will help you better understand the flaws in a network system and how to resolve them. It has been designed in such a way that it does not require any prior experience of testing or hacking. It will cover all the details completely from start to end. You will learn the objectives of Penetrating Testing, steps to conduct a pen test, elements, and phases of Penetrating Testing. The book also covers the techniques used in Penetration Testing and how to test the standard security protocols in network systems. This book guides you on how to use vulnerability assessment, types of security breaches, and the role of Penetrating Testing in enterprises. You will also learn how to keep your systems safe and secure. You will learn about the top ten security risks and how to fix them using Penetration Testing. You will learn how to use Penetration tools like Nmap, Burp Suite Intruder, IBM Appscan, HP Webinspect, and Hack Bar. Once you finish reading the book, you will be ready to make your own pen tests and tackle the advanced topics related to Penetration Testing. This book will guide you step by step in a structured and efficient manner so that you can fully utilize it in your practical experience. It is an excellent book for those who want to learn Penetration Testing but don't know where or how to start.

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

target Explore hardware adapters for testing and auditing wireless networks and Bluetooth devices Who this book is for Hands-On Penetration Testing with Kali NetHunter is for pentesters, ethical hackers, and security professionals who want to learn to use Kali NetHunter for complete mobile penetration testing and are interested in venturing into the mobile domain. Some prior understanding of networking assessment and Kali Linux will be helpful.

Testing web security is best done through simulating an attack. Kali Linux lets you do this to professional standards and this is the book you need to be fully up-to-speed with this powerful open-source toolkit. Overview Learn key reconnaissance concepts needed as a penetration tester Attack and exploit key features, authentication, and sessions on web applications Learn how to protect systems, write reports, and sell web penetration testing services In Detail Kali Linux is built for professional penetration testing and security auditing. It is the next-generation of BackTrack, the most popular open-source penetration toolkit in the world. Readers will learn how to think like real attackers, exploit systems, and expose vulnerabilities. Even though web applications are developed in a very secure environment and have an intrusion detection system and firewall in place to detect and prevent any malicious activity, open ports are a pre-requisite for conducting online business. These ports serve as an open door for attackers to attack these applications. As a result, penetration testing becomes essential to test the integrity of web-applications. Web Penetration Testing with Kali Linux is a hands-on guide that will give you step-by-step methods on finding vulnerabilities and exploiting web applications. "Penetration Testing with Kali Linux" looks at the aspects of web penetration testing from the mind of an attacker. It provides real-world, practical step-by-step instructions on how to perform web penetration testing exercises. You will learn how to use network reconnaissance to pick your targets and gather information. Then, you will use server-side attacks to expose vulnerabilities in web servers and their applications. Client attacks will exploit the way end users use web applications and their workstations. You will also learn how to use open source tools to write reports and get tips on how to sell penetration tests and look out for common pitfalls. On the completion of this book, you will have the skills needed to use Kali Linux for web penetration tests and expose vulnerabilities on web applications and clients that access them. What you will learn from this book Perform vulnerability reconnaissance to gather information on your targets Expose server vulnerabilities and take advantage of them to gain privileged access Exploit client-based systems using web application protocols Learn how to use SQL and cross-site scripting (XSS) attacks Steal authentications through session hijacking techniques Harden systems so other attackers do not exploit them easily Generate reports for penetration testers Learn tips and trade secrets from real world penetration testers Approach "Penetration Testing with Kali Linux" contains various penetration testing methods using BackTrack that will be used by the reader. It contains clear step-by-step instructions with lot of screenshots. It is written in an easy to understand language which will further simplify the understanding for the user.

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.

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 covers 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.

You will learn how to properly utilize and interpret the results of modern day hacking tools, which are required to complete a penetration test. Tool coverage includes Backtrack and Kali Linux, Google reconnaissance, MetaGooFil, DNS interrogation,

Nmap, Nessus, Metasploit, the Social Engineer Toolkit (SET), w3af, Netcat, post exploitation tactics, the Hacker Defender rootkit, and more. The book provides a simple and clean explanation of how to effectively utilize the tools and introduces a four-step methodology for conducting a penetration test or hack. You will be provided with the know-how required to jump start your career or gain a better understanding of offensive security. The book walks through each of the steps and tools in a structured, orderly manner, allowing readers to understand how the output from each tool can be fully utilized in the subsequent phases of the penetration test. This process allows readers to clearly see how the tools and phases function and relate.-The second edition includes updated information covering Kali Linux as well as focusing on the seminal tools required to complete a penetration test New tools added including the Social Engineer Toolkit, Meterpreter, w3af and more!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

Learn everything you need to know to become a professional security and penetration tester. It simplifies hands-on security and penetration testing by breaking down each step of the process so that finding vulnerabilities and misconfigurations becomes easy. The book explains how to methodically locate, exploit, and professionally report security weaknesses using techniques such as SQL-injection, denial-of-service attacks, and password hacking. Although From Hacking to Report Writing will give you the technical know-how needed to carry out advanced security tests, it also offers insight into crafting professional looking reports describing your work and how your customers can benefit from it. The book will give you the tools you need to clearly communicate the benefits of high-quality security and penetration testing to IT-management, executives and other stakeholders. Embedded in the book are a number of on-the-job stories that will give you a good understanding of how you can apply what you have learned to real-world situations. We live in a time where computer security is more important than ever. Staying one step ahead of hackers has never been a bigger challenge. From Hacking to Report Writing clarifies how you can sleep better at night knowing that your network has been thoroughly tested. What you'll learn Clearly understand why security and penetration testing is important Find vulnerabilities in any system using the same techniques as hackers do Write professional looking reports Know which security and penetration testing method to apply for any given situation Successfully hold together a security and penetration test project Who This Book Is For Aspiring security and penetration testers, security consultants, security and penetration testers, IT managers, and security researchers.

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, 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.

Defend your systems from methodical and proficient attackers About This Video Hands-on experience with advanced penetration testing techniques to protect modern operating systems and complex network devices from potential attacks. Explore penetration testing with fully up-to-date techniques and enhance your device and network security. A detailed course that will provide you with practical use cases so you can deliver an intelligent endpoint protection system. In Detail Are you a system administrator, penetration tester, or network engineer and do you want to take your penetration testing skills to the next level? Then this course is for you. It is your one-stop solution to safeguarding complex network devices and modern operating systems from external threats using Kali Linux. This course will provide you with advanced penetration testing techniques with Kali Linux that will help you exploit databases and web/applications servers and perform network penetration. With this course, you will prevent your system from being exploited by using techniques such as reverse shells. Moving on, this course will not only walk you through managing vulnerabilities but will also show you how to protect endpoints. You will explore web pentesting, learn how to set up your LAB environment, and explore the various vulnerabilities that exist nowadays. Towards the end of this course, you will also perform wireless penetration testing to defend against the wireless assets. Finally, you will have mastered the skills and methodologies you need to breach infrastructures and provide complete endpoint protection for your system via Kali Linux. All the code and supporting files for this course are available from Github at https://github.com/PacktPublishing/Hands-On-Infrastructure-Penetration-Testing Downloading the example code for this course: You can download the example code files for all Packt video courses you have purchased from your account at http://www.PacktPub.com . If you purchased this course elsewhere, you can visit http://www.PacktPub.com/support and register to have the files e-mailed directly to you.

Hacking with Kali introduces you the most current distribution of the de facto standard tool for Linux pen testing. Starting with use of the Kali live CD and progressing through installation on hard drives, thumb drives and SD cards, author James Broad walks you through creating a custom version of the Kali live distribution. You'll learn how to configure networking components, storage devices and system services such as DHCP and web services. Once you're familiar with the basic components of the software, you'll learn how to use Kali through the phases of the penetration testing lifecycle; one major tool from each phase is explained. The book culminates with a chapter on reporting that will provide examples of documents used prior to, during and after the pen test. This guide will benefit information security professionals of all levels, hackers, systems administrators, network administrators, and beginning and intermediate professional pen testers, as well as students majoring in information security. Provides detailed explanations of the complete penetration testing lifecycle Complete linkage of the Kali information, resources and distribution downloads Hands-on exercises reinforce topics

Written in an easy-to-follow approach using hands-on examples, this book helps you create virtual environments for advanced penetration testing, enabling you to build a multi-layered

architecture to include firewalls, IDS/IPS, web application firewalls, and endpoint protection, which is essential in the penetration testing world.If you are a penetration tester, security consultant, security test engineer, or analyst who wants to practice and perfect penetration testing skills by building virtual pentesting labs in varying industry scenarios, this is the book for you. This book is ideal if you want to build and enhance your existing pentesting methods and skills. Basic knowledge of network security features is expected along with web application testing experience.

An intensive hands-on guide to perform professional penetration testing for highly-secured environments from start to finish. You will learn to provide penetration testing services to clients with mature security infrastructure. Understand how to perform each stage of the penetration test by gaining hands-on experience in performing attacks that mimic those seen in the wild. In the end, take the challenge and perform a virtual penetration test against a fictional corporation. If you are looking for guidance and detailed instructions on how to perform a penetration test from start to finish, are looking to build out your own penetration testing lab, or are looking to improve on your existing penetration testing skills, this book is for you. Although the books attempts to accommodate those that are still new to the penetration testing field, experienced testers should be able to gain knowledge and hands-on experience as well. The book does assume that you have some experience in web application testing and as such the chapter regarding this subject may require you to understand the basic concepts of web security. The reader should also be familiar with basic IT concepts, and commonly used protocols such as TCP/IP.

Identify tools and techniques to secure and perform a penetration test on an AWS infrastructure using Kali Linux Key Features Efficiently perform penetration testing techniques on your public cloud instances Learn not only to cover loopholes but also to automate security monitoring and alerting within your cloud-based deployment pipelines A step-by-step guide that will help you leverage the most widely used security platform to secure your AWS Cloud environment Book Description The cloud is taking over the IT industry. Any organization housing a large amount of data or a large infrastructure has started moving cloud-ward -- and AWS rules the roost when it comes to cloud service providers, with its closest competitor having less than half of its market share. This highlights the importance of security on the cloud, especially on AWS. While a lot has been said (and written) about how cloud environments can be secured, performing external security assessments in the form of pentests on AWS is still seen as a dark art. This book aims to help pentesters as well as seasoned system administrators with a hands-on approach to pentesting the various cloud services provided by Amazon through AWS using Kali Linux. To make things easier for novice pentesters, the book focuses on building a practice lab and refining penetration testing with Kali Linux on the cloud. This is helpful not only for beginners but also for pentesters who want to set up a pentesting environment in their private cloud, using Kali Linux to perform a white-box assessment of their own cloud resources. Besides this, there is a lot of in-depth coverage of the large variety of AWS services that are often overlooked during a pentest -- from serverless infrastructure to automated deployment pipelines. By the end of this book, you will be able to identify possible vulnerable areas efficiently and secure your AWS cloud environment. What you will learn Familiarize yourself with and pentest the most common external-facing AWS services Audit your own infrastructure and identify flaws, weaknesses, and loopholes Demonstrate the process of lateral and vertical movement through a partially compromised AWS account Maintain stealth and persistence within a compromised AWS account Master a hands-on approach to pentesting Discover a number of automated tools to ease the process of continuously assessing and improving the security stance of an AWS infrastructure Who this book is for If you are a security analyst or a penetration tester and are interested in exploiting Cloud environments to reveal vulnerable areas and secure them, then

this book is for you. A basic understanding of penetration testing, cloud computing, and its security concepts is mandatory.

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 If 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 In 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 devises 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.

"Have you ever wondered how to test web applications security? This course will teach you about web application vulnerabilities and how to use Kali Linux tools to perform web penetration testing to professional standards. You will start with application security and learn about the process of web penetration testing. Then you'll create a test lab with Oracle VirtualBox and Kali Linux. Next, you'll learn about common vulnerabilities in web applications with practical examples, which will help you understand the process of penetration testing and the importance of security. Now you'll be introduced to different tools to assess and analyze web application vulnerabilities. In the end, you'll learn to secure web applications. By the end of the course, you'll be able to perform web penetration testing using Kali Linux."--Resource description page.