

# Mastering Kali Linux For Advanced Penetration Testing

Thank you very much for reading **Mastering Kali Linux For Advanced Penetration Testing** . As you may know, people have search hundreds times for their favorite readings like this Mastering Kali Linux For Advanced Penetration Testing , but end up in infectious downloads.

Rather than enjoying a good book with a cup of coffee in the afternoon, instead they juggled with some harmful bugs inside their computer.

Mastering Kali Linux For Advanced Penetration Testing is available in our digital library an online access to it is set as public so you can get it instantly.

Our book servers saves in multiple countries, allowing you to get the most less latency time to download any of our books like this one.

Kindly say, the Mastering Kali Linux For Advanced Penetration Testing is universally compatible with any devices to read

## **Mastering Kali Linux for Web Penetration Testing** - Michael McPhee 2017-06-28

Master the art of exploiting advanced web penetration techniques with Kali Linux 2016.2 About This Book Make the most out of advanced web pen-testing techniques using Kali Linux 2016.2 Explore how Stored (a.k.a. Persistent) XSS attacks work and how to take advantage of them Learn to secure your application by performing advanced web based attacks. Bypass internet security to traverse from the web to a private network. Who This Book Is For This book targets IT pen testers, security consultants, and ethical hackers who want to expand their knowledge and gain expertise on advanced web penetration techniques. Prior knowledge of penetration testing would be beneficial. What You Will Learn Establish a fully-featured sandbox for test rehearsal and risk-free investigation of applications Enlist open-source information to get a head-start on enumerating account credentials, mapping potential dependencies, and discovering unintended backdoors and exposed information Map, scan, and spider web applications using nmap/zenmap, nikto, arachni, webscarab, w3af, and NetCat for more accurate characterization Proxy web transactions through tools such as Burp Suite, OWASP's ZAP tool, and Vega to uncover application weaknesses and manipulate responses Deploy SQL injection, cross-site scripting, Java vulnerabilities, and overflow attacks using Burp Suite, websploit, and SQLMap to test application robustness Evaluate and test identity, authentication, and authorization schemes and sniff out weak cryptography before the black hats do In Detail You will start by delving into some common web application architectures in use, both in private and public cloud instances. You will also learn about the most common frameworks for testing, such as OWASP OGT version 4, and how to use them to guide your efforts. In the next section, you will be introduced to web pentesting with core tools and you will also see how to make web applications more secure through rigorous penetration tests using advanced features in open source tools. The book will then show you how to better hone your web pentesting skills in safe environments that can ensure low-risk experimentation with the powerful tools and features in Kali Linux that go beyond a typical script-kiddie approach. After establishing how to test these powerful tools safely, you will understand how to better identify vulnerabilities, position and deploy exploits, compromise authentication and authorization, and test the resilience and exposure applications possess. By the end of this book, you will be well-versed with the web service architecture to identify and evade various protection mechanisms that are used on the Web today. You will leave this book with a greater mastery of essential test techniques needed to verify the secure design, development, and operation of your customers' web applications. Style and approach An advanced-level guide filled with real-world examples that will help you take your web application's security to the next level by using Kali Linux 2016.2.

## *Mastering Kali Linux for Advanced Penetration Testing* - Vijay Kumar Velu 2022-02-28

Master key approaches used by real attackers to perform advanced pentesting in tightly secured infrastructure, cloud and virtualized environments, and devices, and learn the latest phishing and hacking techniques Key FeaturesExplore red teaming and play the hackers game to proactively defend your infrastructureUse OSINT, Google dorks, Nmap, recon-nag, and other tools for passive and active reconnaissanceLearn about the latest email, Wi-Fi, and mobile-based phishing techniquesBook Description Remote working has given hackers plenty of opportunities as more confidential information is shared over

the internet than ever before. In this new edition of Mastering Kali Linux for Advanced Penetration Testing, you'll learn an offensive approach to enhance your penetration testing skills by testing the sophisticated tactics employed by real hackers. You'll go through laboratory integration to cloud services so that you learn another dimension of exploitation that is typically forgotten during a penetration test. You'll explore different ways of installing and running Kali Linux in a VM and containerized environment and deploying vulnerable cloud services on AWS using containers, exploiting misconfigured S3 buckets to gain access to EC2 instances. This book delves into passive and active reconnaissance, from obtaining user information to large-scale port scanning. Building on this, different vulnerability assessments are explored, including threat modeling. See how hackers use lateral movement, privilege escalation, and command and control (C2) on compromised systems. By the end of this book, you'll have explored many advanced pentesting approaches and hacking techniques employed on networks, IoT, embedded peripheral devices, and radio frequencies. What you will learnExploit networks using wired/wireless networks, cloud infrastructure, and web servicesLearn embedded peripheral device, Bluetooth, RFID, and IoT hacking techniquesMaster the art of bypassing traditional antivirus and endpoint detection and response (EDR) toolsTest for data system exploits using Metasploit, PowerShell Empire, and CrackMapExecPerform cloud security vulnerability assessment and exploitation of security misconfigurationsUse bettercap and Wireshark for network sniffingImplement complex attacks with Metasploit, Burp Suite, and OWASP ZAPWho this book is for This fourth edition is for security analysts, pentesters, ethical hackers, red team operators, and security consultants wanting to learn and optimize infrastructure/application/cloud security using advanced Kali Linux features. Prior penetration testing experience and basic knowledge of ethical hacking will help you make the most of this book.

## Mastering Modern Web Penetration Testing - Prakhar Prasad 2016-10-28

Master the art of conducting modern pen testing attacks and techniques on your web application before the hacker does! About This Book This book covers the latest technologies such as Advance XSS, XSRF, SQL Injection, Web API testing, XML attack vectors, OAuth 2.0 Security, and more involved in today's web applications Penetrate and secure your web application using various techniques Get this comprehensive reference guide that provides advanced tricks and tools of the trade for seasoned penetration testers Who This Book Is For This book is for security professionals and penetration testers who want to speed up their modern web application penetrating testing. It will also benefit those at an intermediate level and web developers who need to be aware of the latest application hacking techniques. What You Will Learn Get to know the new and less-publicized techniques such PHP Object Injection and XML-based vectors Work with different security tools to automate most of the redundant tasks See different kinds of newly-designed security headers and how they help to provide security Exploit and detect different kinds of XSS vulnerabilities Protect your web application using filtering mechanisms Understand old school and classic web hacking in depth using SQL Injection, XSS, and CSRF Grasp XML-related vulnerabilities and attack vectors such as XXE and DoS techniques Get to know how to test REST APIs to discover security issues in them In Detail Web penetration testing is a growing, fast-moving, and absolutely critical field in information security. This book executes modern web application attacks and utilises cutting-edge hacking techniques

with an enhanced knowledge of web application security. We will cover web hacking techniques so you can explore the attack vectors during penetration tests. The book encompasses the latest technologies such as OAuth 2.0, Web API testing methodologies and XML vectors used by hackers. Some lesser discussed attack vectors such as RPO (relative path overwrite), DOM clobbering, PHP Object Injection and etc. has been covered in this book. We'll explain various old school techniques in depth such as XSS, CSRF, SQL Injection through the ever-dependable SQLMap and reconnaissance. Websites nowadays provide APIs to allow integration with third party applications, thereby exposing a lot of attack surface, we cover testing of these APIs using real-life examples. This pragmatic guide will be a great benefit and will help you prepare fully secure applications. Style and approach This master-level guide covers various techniques serially. It is power-packed with real-world examples that focus more on the practical aspects of implementing the techniques rather going into detailed theory.

#### **Hands-On AWS Penetration Testing with Kali Linux** - Karl Gilbert 2019-04-30

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.

#### **AWS Penetration Testing** - Jonathan Helmus 2020-12-04

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 pentesting 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.

#### **Mastering Kali Linux for Advanced Penetration Testing** - Vijay Kumar Velu 2017-06-30

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 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 testing Style and approach An advanced level tutorial that follows a practical approach and proven methods to maintain top notch security of your networks.

#### **Kali Linux - An Ethical Hacker's Cookbook** - Himanshu Sharma 2017-10-17

Over 120 recipes to perform advanced penetration testing with Kali Linux About This Book Practical recipes to conduct effective penetration testing using the powerful Kali Linux Leverage tools like Metasploit,

Wireshark, Nmap, and many more to detect vulnerabilities with ease Confidently perform networking and application attacks using task-oriented recipes Who This Book Is For This book is aimed at IT security professionals, pentesters, and security analysts who have basic knowledge of Kali Linux and want to conduct advanced penetration testing techniques. What You Will Learn Installing, setting up and customizing Kali for pentesting on multiple platforms Pentesting routers and embedded devices Bug hunting 2017 Pwning and escalating through corporate network Buffer overflows 101 Auditing wireless networks Fiddling around with software-defined radio Hacking on the run with NetHunter Writing good quality reports In Detail With the current rate of hacking, it is very important to pentest your environment in order to ensure advanced-level security. This book is packed with practical recipes that will quickly get you started with Kali Linux (version 2016.2) according to your needs, and move on to core functionalities. This book will start with the installation and configuration of Kali Linux so that you can perform your tests. You will learn how to plan attack strategies and perform web application exploitation using tools such as Burp, and Jexboss. You will also learn how to perform network exploitation using Metasploit, Sparta, and Wireshark. Next, you will perform wireless and password attacks using tools such as Patator, John the Ripper, and airoscript-ng. Lastly, you will learn how to create an optimum quality pentest report! By the end of this book, you will know how to conduct advanced penetration testing thanks to the book's crisp and task-oriented recipes. Style and approach This is a recipe-based book that allows you to venture into some of the most cutting-edge practices and techniques to perform penetration testing with Kali Linux.

**Mastering Kali Linux** - Nelson Saxton 2017-08

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. This book will take you, as a tester or security practitioner through the journey of reconnaissance, vulnerability assessment, exploitation, and post-exploitation.

**Penetration Testing** - Georgia Weidman 2014-06-14

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.

[Python Ethical Hacking from Scratch](#) - Fahad Ali Sarwar 2021-06-25

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

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

*Linux Basics for Hackers* - OccupyTheWeb 2018-12-04

This practical, tutorial-style book uses the Kali Linux distribution to teach Linux basics with a focus on how hackers would use them. Topics include Linux command line basics, filesystems, networking, BASH basics, package management, logging, and the Linux kernel and drivers. If you're getting started along the exciting path of hacking, cybersecurity, and pentesting, Linux Basics for Hackers is an excellent first step. Using Kali Linux, an advanced penetration testing distribution of Linux, you'll learn the basics of using the Linux operating system and acquire the tools and techniques you'll need to take control of a Linux environment. First, you'll learn how to install Kali on a virtual machine and get an introduction to basic Linux concepts. Next, you'll tackle broader Linux topics like manipulating text, controlling file and directory permissions, and managing user environment variables. You'll then focus in on foundational hacking concepts like security and anonymity and learn scripting skills with bash and Python. Practical tutorials and exercises throughout will reinforce and test your skills as you learn how to: - Cover your tracks by changing your network information and manipulating the rsyslog logging utility - Write a tool to scan for network connections, and connect and listen to wireless networks - Keep your internet activity stealthy using Tor, proxy servers, VPNs, and encrypted email - Write a bash script to scan open ports for potential targets - Use and abuse services like MySQL, Apache web server, and OpenSSH - Build your own hacking tools, such as a remote video spy camera and a password cracker Hacking is complex, and there is no single way in. Why not start at the beginning with Linux Basics for Hackers?

[Kali Linux Wireless Penetration Testing: Beginner's Guide](#) - Vivek Ramachandran 2015-03-30

If you are a security professional, pentester, or anyone interested in getting to grips with wireless penetration testing, this is the book for you. Some familiarity with Kali Linux and wireless concepts is beneficial.

**The Basics of Hacking and Penetration Testing** - Patrick Engebretson 2013-06-24

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.

*Advanced Infrastructure Penetration Testing* - Chiheb Chebbi 2018-02-26

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.

**Mastering Kali Linux for Advanced Penetration Testing** - Vijay Kumar Velu 2019

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.

**The Ultimate Kali Linux Book** - Glen D. Singh 2022-02-24

Explore the latest ethical hacking tools and techniques to perform penetration testing from scratch Purchase of the print or Kindle book includes a free eBook in the PDF format Key Features Learn to compromise enterprise networks with Kali Linux Gain comprehensive insights into security concepts using advanced real-life hacker techniques Use Kali Linux in the same way ethical hackers and penetration testers do to gain control of your environment Book Description Kali Linux is the most popular and advanced penetration testing Linux distribution within the cybersecurity industry. Using Kali Linux, a cybersecurity professional will be able to discover and exploit various vulnerabilities and perform advanced penetration testing on both enterprise wired and wireless networks. This book is a comprehensive guide for those who are new to Kali Linux and penetration testing that will have you up to speed in no time. Using

real-world scenarios, you'll understand how to set up a lab and explore core penetration testing concepts. Throughout this book, you'll focus on information gathering and even discover different vulnerability assessment tools bundled in Kali Linux. You'll learn to discover target systems on a network, identify security flaws on devices, exploit security weaknesses and gain access to networks, set up Command and Control (C2) operations, and perform web application penetration testing. In this updated second edition, you'll be able to compromise Active Directory and exploit enterprise networks. Finally, this book covers best practices for performing complex web penetration testing techniques in a highly secured environment. By the end of this Kali Linux book, you'll have gained the skills to perform advanced penetration testing on enterprise networks using Kali Linux. What you will learn Explore the fundamentals of ethical hacking Understand how to install and configure Kali Linux Perform asset and network discovery techniques Focus on how to perform vulnerability assessments Exploit the trust in Active Directory domain services Perform advanced exploitation with Command and Control (C2) techniques Implement advanced wireless hacking techniques Become well-versed with exploiting vulnerable web applications Who this book is for This pentesting book is for students, trainers, cybersecurity professionals, cyber enthusiasts, network security professionals, ethical hackers, penetration testers, and security engineers. If you do not have any prior knowledge and are looking to become an expert in penetration testing using the Kali Linux operating system (OS), then this book is for you.

**Mastering Kali Linux for Advanced Penetration Testing** - Robert W. Beggs 2014-06-24

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.

**Mastering Machine Learning for Penetration Testing** - Chiheb Chebbi 2018-06-27

Become a master at penetration testing using machine learning with Python Key Features Identify ambiguities and breach intelligent security systems Perform unique cyber attacks to breach robust systems Learn to leverage machine learning algorithms Book Description Cyber security is crucial for both businesses and individuals. As systems are getting smarter, we now see machine learning interrupting computer security. With the adoption of machine learning in upcoming security products, it's important for pentesters and security researchers to understand how these systems work, and to breach them for testing purposes. This book begins with the basics of machine learning and the algorithms used to build robust systems. Once you've gained a fair understanding of how security products leverage machine learning, you'll dive into the core concepts of breaching such systems. Through practical use cases, you'll see how to find loopholes and surpass a self-learning security system. As you make your way through the chapters, you'll focus on topics such as network intrusion detection and AV and IDS evasion. We'll also cover the best practices when identifying ambiguities, and extensive techniques to breach an intelligent system. By the end of this book, you will be well-versed with identifying loopholes in a self-learning security system and will be able to efficiently breach a machine learning system. What you will learn Take an in-depth look at machine learning Get to know natural language processing (NLP) Understand malware feature engineering Build generative adversarial networks using Python libraries Work on threat hunting with machine learning and the ELK stack Explore the best practices for machine learning Who this book is for This book is for pen testers and security professionals who are interested in learning techniques to break an intelligent security system. Basic knowledge of Python is needed, but no prior knowledge of machine learning is necessary.

**Advanced Penetration Testing** - Wil Allsopp 2017-02-27

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.

*Ethical Hacking and Penetration, Step by Step with Kali Linux* - Rassoul Ghaznavi-zadeh 2014-11-16

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

[KALI LINUX FOR BEGINNERS](#) - Michael Clark 2021-05-28

*Kali Linux - An Ethical Hacker's Cookbook* - Himanshu Sharma 2019-03-29

Discover end-to-end penetration testing solutions to enhance your ethical hacking skills Key Features Practical recipes to conduct effective penetration testing using the latest version of Kali Linux Leverage tools like Metasploit, Wireshark, Nmap, and more to detect vulnerabilities with ease Confidently perform networking and application attacks using task-oriented recipes Book Description Many organizations have been affected by recent cyber events. At the current rate of hacking, it has become more important than ever to pentest your environment in order to ensure advanced-level security. This book is packed with practical recipes that will quickly get you started with Kali Linux (version 2018.4 / 2019), in addition to covering the core functionalities. The book will get you off to a strong start by introducing you to the installation and configuration of Kali Linux, which will help you to perform your tests. You will also learn how to plan attack strategies and perform web application exploitation using tools such as Burp and JexBoss. As you progress, you will get to grips with performing network exploitation using Metasploit, Sparta, and Wireshark. The book will also help you delve into the technique of carrying out wireless and password attacks using tools such as Patator, John the Ripper, and airoscript-ng. Later chapters will draw focus to the wide range of tools that help in forensics investigations and incident response mechanisms. As you wrap up the concluding chapters, you will learn to create an optimum quality pentest report. By the end of this book, you will be equipped with the knowledge you need to conduct advanced penetration testing, thanks to the book's crisp and task-oriented recipes. What you will learn Learn how to install, set up and customize Kali for pentesting on multiple platforms Pentest routers and embedded devices Get insights into fiddling around with software-defined radio Pwn and escalate through a corporate network Write good quality security reports Explore digital forensics and memory analysis with Kali Linux Who this book is for If you are an IT security professional, pentester, or security analyst who wants to conduct advanced penetration testing techniques, then this book is for you. Basic knowledge of Kali Linux is assumed.

[Metasploit Penetration Testing Cookbook](#) - Abhinav Singh 2018-02-26

Over 100 recipes for penetration testing using Metasploit and virtual machines Key Features Special focus on the latest operating systems, exploits, and penetration testing techniques Learn new anti-virus evasion techniques and use Metasploit to evade countermeasures Automate post exploitation with AutoRunScript Exploit Android devices, record audio and video, send and read SMS, read call logs, and much more Build and analyze Metasploit modules in Ruby Integrate Metasploit with other penetration testing tools Book Description Metasploit is the world's leading penetration testing tool and helps security and IT professionals find, exploit, and validate vulnerabilities. Metasploit allows penetration testing automation, password auditing, web application scanning, social engineering, post exploitation, evidence collection, and reporting. Metasploit's integration with InsightVM (or Nexpose), Nessus, OpenVas, and other vulnerability scanners provides a validation solution that simplifies vulnerability prioritization and remediation reporting. Teams can collaborate in Metasploit and present their findings in consolidated reports. In this book, you will go through great recipes that will allow you to start using Metasploit effectively. With an ever increasing level of complexity, and covering everything from the fundamentals to more advanced features in Metasploit, this book is not just for beginners but also for professionals keen to master this awesome tool. You will begin by building your lab environment, setting up Metasploit, and learning how to perform intelligence gathering, threat modeling, vulnerability analysis, exploitation, and post exploitation—all inside Metasploit. You will learn how to create and customize payloads to evade anti-virus software and bypass an organization's defenses, exploit server vulnerabilities, attack client systems, compromise mobile phones, automate post exploitation, install backdoors, run keyloggers, hijack webcams, port public exploits to the framework, create your own modules, and much more. What you will learn Set up a complete penetration testing environment using Metasploit and virtual machines Master the world's leading penetration testing tool and use it in professional penetration testing Make the most of Metasploit with PostgreSQL, importing scan results, using workspaces, hosts, loot, notes, services, vulnerabilities, and exploit results Use Metasploit with the Penetration Testing Execution Standard methodology Use MSFvenom efficiently to generate payloads and backdoor files, and create shellcode Leverage Metasploit's advanced options, upgrade sessions, use proxies, use Meterpreter sleep control, and change timeouts to be stealthy Who this book is for If you are a Security professional or pentester and want to get into vulnerability exploitation and make the most of the Metasploit framework, then this book is for you. Some prior understanding of penetration testing and Metasploit is required.

**Learn Ethical Hacking from Scratch** - Zaid Sabih 2018-07-31

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

security of systems like professional hackers and security experts.

**Mastering Kali Linux for Advanced Penetration Testing** - Vijay Kumar Velu 2019-01-30

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.

**Web Penetration Testing with Kali Linux** - Joseph Muniz 2013-09-25

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. "Web Penetration Testing with Kali Linux" is ideal for anyone who is interested in learning how to become a penetration tester. It will also help the users who are new to Kali Linux and want to learn the features and differences in Kali versus Backtrack, and seasoned penetration testers who may need a refresher or reference on new tools and techniques. Basic familiarity with web-based programming languages such as PHP, JavaScript and MySQL will also prove helpful.

**Mastering Kali Linux for Advanced Penetration Testing** - Shailesh kori 2018-03-02

this book Mastering Kali Linux for. Advanced Penetration Testing. A practical guide to testing your network's security with. Kali Linux, the preferred choice of penetration testers and hackers Kali Linux has not only become the information security professional's platform of choice, but evolved into an industrial-grade, and world-class operating system distribution--mature, secure, and enterprise-ready. Through the decade-long development process, Muts and his team, along with countless volunteers from the hacker community, have taken on the burden of streamlining and organizing our work environment, freeing us from much of the drudgery. They provided a secure and reliable foundation, allowing us to concentrate on securing our digital world. An amazing community has built up around Kali Linux. Every month, more than 300,000 of us download a version of Kali. We come together in online and real-world training rooms and grind through the sprawling Offensive Security Penetration Testing Labs, pursuing the near-legendary Offensive Security certifications. We come together on the Kali forums, some 40,000 strong, and hundreds of us at a time can be found on the Kali IRC channel. We gather at conferences and attend Kali Dojos to learn from the developers themselves how to best leverage Kali. However, the Kali team has never released

an official Kali Linux manual, until now. In this book, we'll focus on the Kali Linux platform itself, and help you understand and maximize Kali from the ground up. The developers will walk you through Kali Linux features and fundamentals, provide a crash course in basic Linux commands and concepts, and then walk you through the most common Kali Linux installation scenarios. You'll learn how to configure, troubleshoot and secure Kali Linux and then dive into the powerful Debian package manager. Throughout this expansive section, you'll learn how to install and configure packages, how to update and upgrade your Kali installation, and how to create your own custom packages. Then you'll learn how to deploy your custom installation across massive enterprise networks. Finally, you'll be guided through advanced topics such as kernel compilation, custom ISO creation, industrial-strength encryption, and even how to install crypto kill switches to safeguard your sensitive information. Whether you're a veteran or an absolute n00b, this is the best place to start with Kali Linux, the security professional's platform of choice

**Hands-On Penetration Testing on Windows** - Phil Bramwell 2018-07-30

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

**Learn Kali Linux 2019** - Glen D. Singh 2019-11-14

Explore the latest ethical hacking tools and techniques in Kali Linux 2019 to perform penetration testing from scratch

**Key Features** Get up and running with Kali Linux 2019.2 Gain comprehensive insights into security concepts such as social engineering, wireless network exploitation, and web application attacks Learn to use Linux commands in the way ethical hackers do to gain control of your environment

**Book Description** The current rise in hacking and security breaches makes it more important than ever to effectively pentest your environment, ensuring endpoint protection. This book will take you through the latest version of Kali Linux and help you use various tools and techniques to efficiently deal with crucial security aspects. Through real-world examples, you'll understand how to set up a lab and later explore core penetration testing concepts. Throughout the course of this book, you'll get up to speed with gathering sensitive information and even discover different vulnerability assessment tools bundled in Kali Linux 2019. In later chapters, you'll gain insights into concepts such as social engineering, attacking wireless networks, exploitation of web applications and remote access connections to further build on your pentesting skills. You'll also focus on techniques such as bypassing controls, attacking the end user and maintaining persistence access through social media. Finally, this pentesting book covers best practices for performing complex penetration testing techniques in a highly secured environment. By the end of this book, you'll be able to use Kali Linux to detect vulnerabilities and secure your system by applying penetration testing

techniques of varying complexity. What you will learn Explore the fundamentals of ethical hacking Learn how to install and configure Kali Linux Get up to speed with performing wireless network pentesting Gain insights into passive and active information gathering Understand web application pentesting Decode WEP, WPA, and WPA2 encryptions using a variety of methods, such as the fake authentication attack, the ARP request replay attack, and the dictionary attack Who this book is for If you are an IT security professional or a security consultant who wants to get started with penetration testing using Kali Linux 2019.2, then this book is for you. The book will also help if you're simply looking to learn more about ethical hacking and various security breaches. Although prior knowledge of Kali Linux is not necessary, some understanding of cybersecurity will be useful.

**Mastering Linux** - Paul S. Wang 2010-09-22

Encouraging hands-on practice, Mastering Linux provides a comprehensive, up-to-date guide to Linux concepts, usage, and programming. Through a set of carefully selected topics and practical examples, the book imparts a sound understanding of operating system concepts and shows how to use Linux effectively. Ready-to-Use Examples Offer Immediate Access

**Mastering Kali Linux for Advanced Penetration Testing - Second Edition** - Vijay Kumar Velu 2017-06-30

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 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 testing. Style and approach An advanced level tutorial that follows a practical approach and proven methods to maintain top notch security of your networks.

**Mastering Kali Linux Wireless Pentesting** - Jilumudi Raghu Ram 2016-02-25

Test your wireless network's security and master advanced wireless penetration techniques using Kali Linux About This Book Develop your skills using attacks such as wireless cracking, Man-in-the-Middle, and Denial of Service (DOS), as well as extracting sensitive information from wireless networks Perform advanced wireless assessment and penetration tests Use Embedded Platforms, Raspberry PI, and Android in wireless penetration testing with Kali Linux Who This Book Is For If you are an intermediate-level

wireless security consultant in Kali Linux and want to be the go-to person for Kali Linux wireless security in your organisation, then this is the book for you. Basic understanding of the core Kali Linux concepts is expected. What You Will Learn Fingerprint wireless networks with the various tools available in Kali Linux Learn various techniques to exploit wireless access points using CSRF Crack WPA/WPA2/WPS and crack wireless encryption using Rainbow tables more quickly Perform man-in-the-middle attack on wireless clients Understand client-side attacks, browser exploits, Java vulnerabilities, and social engineering Develop advanced sniffing and PCAP analysis skills to extract sensitive information such as DOC, XLS, and PDF documents from wireless networks Use Raspberry PI and OpenWrt to perform advanced wireless attacks Perform a DOS test using various techniques and tools In Detail Kali Linux is a Debian-based Linux distribution designed for digital forensics and penetration testing. It gives access to a large collection of security-related tools for professional security testing - some of the major ones being Nmap, Aircrack-ng, Wireshark, and Metasploit. This book will take you on a journey where you will learn to master advanced tools and techniques to conduct wireless penetration testing with Kali Linux. You will begin by gaining an understanding of setting up and optimizing your penetration testing environment for wireless assessments. Then, the book will take you through a typical assessment from reconnaissance, information gathering, and scanning the network through exploitation and data extraction from your target. You will get to know various ways to compromise the wireless network using browser exploits, vulnerabilities in firmware, web-based attacks, client-side exploits, and many other hacking methods. You will also discover how to crack wireless networks with speed, perform man-in-the-middle and DOS attacks, and use Raspberry Pi and Android to expand your assessment methodology. By the end of this book, you will have mastered using Kali Linux for wireless security assessments and become a more effective penetration tester and consultant. Style and approach This book uses a step-by-step approach using real-world attack scenarios to help you master the wireless penetration testing techniques.

**The Complete Metasploit Guide** - Sagar Rahalkar 2019-06-25

Master the Metasploit Framework and become an expert in penetration testing. Key Features Gain a thorough understanding of the Metasploit Framework Develop the skills to perform penetration testing in complex and highly secure environments Learn techniques to integrate Metasploit with the industry's leading tools Book Description Most businesses today are driven by their IT infrastructure, and the tiniest crack in this IT network can bring down the entire business. Metasploit is a pentesting network that can validate your system by performing elaborate penetration tests using the Metasploit Framework to secure your infrastructure. This Learning Path introduces you to the basic functionalities and applications of Metasploit. Throughout this book, you'll learn different techniques for programming Metasploit modules to validate services such as databases, fingerprinting, and scanning. You'll get to grips with post exploitation and write quick scripts to gather information from exploited systems. As you progress, you'll delve into real-world scenarios where performing penetration tests are a challenge. With the help of these case studies, you'll explore client-side attacks using Metasploit and a variety of scripts built on the Metasploit Framework. By the end of this Learning Path, you'll have the skills required to identify system vulnerabilities by using thorough testing. This Learning Path includes content from the following Packt products: Metasploit for Beginners by Sagar Rahalkar Mastering Metasploit - Third Edition by Nipun Jaswal What you will learn Develop advanced and sophisticated auxiliary modules Port exploits from Perl, Python, and many other programming languages Bypass modern protections such as antivirus and IDS with Metasploit Script attacks in Armitage using the Cortana scripting language Customize Metasploit modules to modify existing exploits Explore the steps involved in post-exploitation on Android and mobile platforms Who this book is for This Learning Path is ideal for security professionals, web programmers, and pentesters who want to master vulnerability exploitation and get the most of the Metasploit Framework. Basic knowledge of Ruby programming and Cortana scripting language is required.

**Mobile Application Penetration Testing** - Vijay Kumar Velu 2016-03-11

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 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.

#### **Learning Kali Linux** - Ric Messier 2018-07-17

With more than 600 security tools in its arsenal, the Kali Linux distribution can be overwhelming. Experienced and aspiring security professionals alike may find it challenging to select the most appropriate tool for conducting a given test. This practical book covers Kali's expansive security capabilities and helps you identify the tools you need to conduct a wide range of security tests and penetration tests. You'll also explore the vulnerabilities that make those tests necessary. Author Ric Messier takes you through the foundations of Kali Linux and explains methods for conducting tests on networks, web applications, wireless security, password vulnerability, and more. You'll discover different techniques for extending Kali tools and creating your own toolset. Learn tools for stress testing network stacks and applications Perform network reconnaissance to determine what's available to attackers Execute penetration tests using automated exploit tools such as Metasploit Use cracking tools to see if passwords meet complexity requirements Test wireless capabilities by injecting frames and cracking passwords Assess web application vulnerabilities with automated or proxy-based tools Create advanced attack techniques by extending Kali tools or developing your own Use Kali Linux to generate reports once testing is complete

#### **Kali Linux Penetration Testing Bible** - Gus Khawaja 2021-04-26

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

#### **Kali Linux Revealed** - Raphaël Hertzog 2017-06-05

Whether you're a veteran or an absolute n00b, this is the best place to start with Kali Linux, the security professional's platform of choice, and a truly industrial-grade, and world-class operating system distribution-mature, secure, and enterprise-ready.

#### **Kali Linux Web Penetration Testing Cookbook** - Gilberto Nájera-Gutiérrez 2016-02-29

Over 80 recipes on how to identify, exploit, and test web application security with Kali Linux 2 About This Book Familiarize yourself with the most common web vulnerabilities a web application faces, and understand how attackers take advantage of them Set up a penetration testing lab to conduct a preliminary assessment of attack surfaces and run exploits Learn how to prevent vulnerabilities in web applications before an attacker can make the most of it Who This Book Is For This book is for IT professionals, web developers, security enthusiasts, and security professionals who want an accessible reference on how to find, exploit, and prevent security vulnerabilities in web applications. You should know the basics of operating a Linux environment and have some exposure to security technologies and tools. What You Will Learn Set up a penetration testing laboratory in a secure way Find out what information is useful to gather when performing penetration tests and where to look for it Use crawlers and spiders to investigate an entire website in minutes Discover security vulnerabilities in web applications in the web browser and using command-line tools Improve your testing efficiency with the use of automated vulnerability scanners Exploit vulnerabilities that require a complex setup, run custom-made exploits, and prepare for extraordinary scenarios Set up Man in the Middle attacks and use them to identify and exploit security flaws within the communication between users and the web server Create a malicious site that will find and exploit vulnerabilities in the user's web browser Repair the most common web vulnerabilities and understand how to prevent them becoming a threat to a site's security In Detail Web applications are a huge point of attack for malicious hackers and a critical area for security professionals and penetration testers to lock down and secure. Kali Linux is a Linux-based penetration testing platform and operating system that provides a huge array of testing tools, many of which can be used specifically to execute web penetration testing. This book will teach you, in the form step-by-step recipes, how to detect a wide array of vulnerabilities, exploit them to analyze their consequences, and ultimately buffer attackable surfaces so applications are more secure, for you and your users. Starting from the setup of a testing laboratory, this book will give you the skills you need to cover every stage of a penetration test: from gathering information about the system and the application to identifying vulnerabilities through manual testing and the use of vulnerability scanners to both basic and advanced exploitation techniques that may lead to a full system compromise. Finally, we will put this into the context of OWASP and the top 10 web application vulnerabilities you are most likely to encounter, equipping you with the ability to combat them effectively. By the end of the book, you will have the required skills to identify, exploit, and prevent web application vulnerabilities. Style and approach Taking a recipe-based approach to web security, this book has been designed to cover each stage of a penetration test, with descriptions on how tools work and why certain programming or configuration practices can become security vulnerabilities that may put a whole system, or network, at risk. Each topic is presented as a sequence of tasks and contains a proper explanation of why each task is performed and what it accomplishes.

#### **Hacking Mastery with Kali Linux** - Vidya Basant 2021-05-14

Do you want to become a professional hacker? If answer to that question is yes, then you need to learn Kali Linux. It is the most world famous and the best operating system for hacking and penetration testing. This book will not only be teaching you hacking with kali linux, but will also teach you all the things you need to be successful in the career of hacking and penetration testing. Even if you're a complete beginner and have never used kali linux before, don't worry, because we will start you off with the very basic until you reach the advance level. In the first 5 chapters, we will be covering some basic things like setting up a lab, linux basic internet protocol and more to make you comfortable with kali linux. From chapters 5 to 10 you will be learning intermediate concepts like Trojan, viruses and worms, password cracking, and network sniffing. Here you will be introduced to the real world of hacking. In the last 5 chapters we will be covering few more advance concepts like gaining access, post exploitation, anti-virus evasions and much more. All the chapters in this book have a theoretical and a practical portion. This book also contains more than 150+



screenshots that makes complex attack easy to follow. Table of content Introduction Setting up a lab Linux basic Internet protocol Port number Trojan, viruses and worms Password attack & cracking Network sniffing & spoofing Staying anonymous online Information gathering Gaining access Post exploitation Anti-viurs evasion File Transfer Bonus Section Book a Copy Now, and get started hacking with kali linux.

Python for Offensive PenTest - Hussam Khrais 2018-04-26

Your one-stop guide to using Python, creating your own hacking tools, and making the most out of resources available for this programming language Key Features Comprehensive information on building a web application penetration testing framework using Python Master web application penetration testing using the multi-paradigm programming language Python Detect vulnerabilities in a system or application by writing your own Python scripts Book Description Python is an easy-to-learn and cross-platform programming language that has unlimited third-party libraries. Plenty of open source hacking tools are written in Python, which can be easily integrated within your script. This book is packed with step-by-step instructions and working examples to make you a skilled penetration tester. It is divided into clear bite-

sized chunks, so you can learn at your own pace and focus on the areas of most interest to you. This book will teach you how to code a reverse shell and build an anonymous shell. You will also learn how to hack passwords and perform a privilege escalation on Windows with practical examples. You will set up your own virtual hacking environment in VirtualBox, which will help you run multiple operating systems for your testing environment. By the end of this book, you will have learned how to code your own scripts and mastered ethical hacking from scratch. What you will learn Code your own reverse shell (TCP and HTTP) Create your own anonymous shell by interacting with Twitter, Google Forms, and SourceForge Replicate Metasploit features and build an advanced shell Hack passwords using multiple techniques (API hooking, keyloggers, and clipboard hijacking) Exfiltrate data from your target Add encryption (AES, RSA, and XOR) to your shell to learn how cryptography is being abused by malware Discover privilege escalation on Windows with practical examples Countermeasures against most attacks Who this book is for This book is for ethical hackers; penetration testers; students preparing for OSCP, OSCE, GPEN, GXPN, and CEH; information security professionals; cybersecurity consultants; system and network security administrators; and programmers who are keen on learning all about penetration testing.