Sql Injection Kali Tutorial

Kali Linux Intrusion and Exploitation Cookbook
Ethical Hacking and Penetration, Step by Step with Kali Linux
Mastering Modern Web Penetration Testing
Kali Linux Hacking
Mastering Kali Linux for Web Penetration Testing
Kali Linux
Hacking with Kali Linux
Kali Linux CTF Blueprints
Mastering Kali Linux for Advanced Penetration Testing
Web Penetration Testing with Kali Linux
Kali Linux Web Penetration Testing Cookbook
SQL Injection Strategies
Hacking: Penetration Testing with Kali Linux
Kali Linux 2 – Assuring Security by Penetration Testing
Sql Injection Attack and Countermeasures
SQL Hacks
SQL Injection Attack and Defense
SQL injection attacks and mitigations
Kali Linux
Kali Linux Cookbook
Kali Linux – Assuring Security by Penetration Testing
Kali Linux for Dummies
Burp Suite Cookbook
Kali Linux Web Penetration Testing Cookbook
Hacking with Kali Linux: Step by Step Guide to Hacking and Penetration Test with Kali Linux
Kali Linux 2: Windows Penetration Testing
Learning Kali Linux
OUTLINE for ADVANCED KALI LINUX
Hands-On Penetration Testing with Kali NetHunter
Metasploit for Beginners
Web Penetration Testing with Kali Linux - Second Edition
The Big Book Of Kali Linux Hacking
SQL Injection
Mastering SQL Injection
Sql Injection Best Method For Begineers
Web Penetration Testing with Kali Linux
Kali Linux Hacking Official
SQL Injection Attacks and Defense
Basics of SQL Injection Analysis, Detection and Prevention
Hacking with Kali Linux - When you don't know sh#t

YULIANA BRADY

Kali Linux Intrusion and Exploitation Cookbook Packt Publishing Ltd
Embark on a journey through the digital labyrinth of cybersecurity with Kali Linux. This essential handbook serves as your trusted companion, offering a profound exploration into the tools and techniques of today’s cybersecurity experts. Inside these pages lies the key to unlocking the potential of Kali Linux, the premier operating system for ethical hackers, penetration testers, and security aficionados. You will begin by laying the groundwork—understanding the installation process, navigation, and fundamental Linux commands—before advancing to the strategic principles of penetration testing and the ethical considerations that underpin the cybersecurity profession. Each chapter delves deeper into the tactical execution of cybersecurity, from mastering command line tools to the meticulous art of network scanning, from exploiting vulnerabilities to fortifying defenses. With this guide, you will: Harness the extensive toolkit of Kali Linux to uncover weaknesses within secure environments. Develop proficiency in web application penetration testing to identify and mitigate common security flaws. Learn advanced penetration techniques and strategies used in real-world cybersecurity assessments. Explore the development of custom security tools and the intricacies of scripting to automate your security tasks. Prepare for the future with insights into advanced topics and the roadmap for continuing education and certifications in the ever-evolving domain of cybersecurity. Whether you are venturing into the field for the first time or seeking to refine your expertise, Kali Linux empowers you with practical, hands-on knowledge and a clear path forward in the cybersecurity landscape. The threats may be advancing, but your ability to counter them will be too. Step beyond the basics, transcend challenges, and transform into an adept practitioner ready to tackle the cybersecurity threats of tomorrow. Kali Linux is more than a book—it’s your guide to a future in securing the digital world.
Ethical Hacking and Penetration, Step by Step with Kali Linux smashwords.inc
"Mastering Cybersecurity with Kali Linux: An Advanced Guide" provides an in-depth exploration of advanced cybersecurity concepts and techniques using Kali Linux, a powerful and versatile penetration testing platform. The book covers a wide range of topics, from the basics of setting up Kali Linux to sophisticated exploitation techniques and defensive strategies. Key chapters include: Introduction to Kali Linux: Learn the fundamentals of Kali Linux and its importance in cybersecurity. Network Scanning and Enumeration: Master the techniques and tools for discovering and mapping network resources. Vulnerability Assessment and Exploitation Techniques: Gain expertise in identifying and exploiting vulnerabilities. Wireless Network Security and Attacks: Understand wireless protocols and learn how to secure and attack wireless networks. Incident Response and Forensics: Develop skills in incident response and forensic analysis to manage and recover from security incidents. Ethical Hacking and Penetration Testing: Learn the principles and methodologies of ethical hacking and penetration testing. Future Trends in Cybersecurity: Stay informed about emerging threats and technologies shaping the future of cybersecurity. Legal and Ethical Considerations: Understand the legal and ethical aspects of cybersecurity

practices. Case Studies and Practical Examples: Explore real-world examples and case studies to gain practical insights into cybersecurity applications. Why You Should Read This Book Comprehensive Coverage: With over 1,000,000 words of detailed content, this book provides exhaustive coverage of advanced cybersecurity topics. Practical Guidance: Includes numerous practical examples, case studies, and hands-on tutorials to help readers apply their knowledge. Stay Ahead: Learn about the latest trends and technologies in cybersecurity to stay ahead of emerging threats. Ethical and Legal Awareness: Gain a thorough understanding of the ethical and legal considerations in cybersecurity practices.

Mastering Modern Web Penetration Testing Packt Publishing Ltd

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.

Kali Linux Hacking Packt Publishing Ltd

Over 80 recipes to effectively test your network and boost your career in security About This Book Learn how to scan networks to find vulnerable computers and servers Hack into devices to control them, steal their data, and make them yours Target wireless networks, databases, and web servers, and password cracking to make the most of Kali Linux Who This Book Is For If you are looking to expand your career into penetration testing, you will need a good understanding of Kali Linux and the variety of tools it includes. This book will work as a perfect guide for anyone who wants to have a practical approach in leveraging penetration testing mechanisms using Kali Linux What You Will Learn Acquire the key skills of ethical hacking to perform penetration testing Learn how to perform network reconnaissance Discover vulnerabilities in hosts Attack vulnerabilities to take control of workstations and servers Understand password cracking to bypass security Learn how to hack into wireless networks Attack web and database servers to exfiltrate data Obfuscate your command and control connections to avoid firewall and IPS detection In Detail Kali Linux is a Linux distribution designed for penetration testing and security auditing. It is the successor to BackTrack, the world's most popular penetration testing distribution. Kali Linux is the most widely used platform and toolkit for penetration testing. Security is currently the hottest field in technology with a projected need for millions of security professionals. This book focuses on enhancing your knowledge in Kali Linux for security by expanding your skills with toolkits and frameworks that can increase your value as a security professional. Kali Linux Cookbook, Second Edition starts by helping you install Kali Linux on different options available. You will also be able to understand the lab architecture and install a Windows host for use in the lab. Next, you will understand the concept of vulnerability analysis and look at the different types of exploits. The book will introduce you to the concept and psychology of Social Engineering and password cracking. You will then be able to use these skills to expand the scope of any breaches you create. Finally, the book will guide you in exploiting specific technologies and gaining access to other systems in the environment. By the end of this book, you will have gained the core knowledge and concepts of the penetration testing process. Style and approach This book teaches you everything you need to know about Kali Linux from the perspective of a penetration tester. It is filled with powerful recipes and practical examples that will help you gain in-depth knowledge of Kali Linux.

Mastering Kali Linux for Web Penetration Testing Createspace Independent Publishing Platform

This book is a guide on how to use Kali Linux for penetration testing. It begins by guiding you on how to use the "Sqlmap" tool to perform an SQL injection. This will help you seal any loopholes in your databases. The book then guides you on how to use a tool named "Fluxion" so as to hack networks which are protected by WPA/WPA2. Brute forcing has been used for carrying out this kind of attack. You will also learn how to check or know the location for a particular IP address in the world. You will learn how to get details about this location in terms of longitude, country, and other parameters. The process of hiding or spoofing MAC addresses for your devices is very important for penetration testing. This book guides you on how to spoof the MAC address of your devices. After developing a website or before you can hack a website, it is good for you to scan it and identify any loopholes or vulnerabilities within it. You can then go ahead and exploit these vulnerabilities, or seal them to prevent a disaster. This book guides you on how to scan a website and identify any vulnerability within it. You are guided on how to hack Android phones by the use of Kali Linux. HTP servers usually have an open FTP port. This book guides you on how to use this port and gain access to the server. You will also know how to carry out a mass mailer attack, as well as password cracking in Kali Linux. The following topics are discussed in this book: - Sqlmap for Website Hacking - How to Hack WPA/WPA2 without Brute Force - Checking for IP Address Location - MAC Address Spoofing - Scanning a Website for Vulnerability - Hacking Android Phones with Kali Linux -Hacking FTP Server in Kali Linux - Creating a Persistent Backdoor in Android - Mass Mailer Attack - Password Cracking

Kali Linux XinXii

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.

Hacking with Kali Linux Anonim

Do you want to become a skilled cybersecurity professional and master the foundations of ethical hacking? Do you want a full breakdown of all the fundamental tools supplied by the finest Linux distribution for ethical hacking? Have you combed the internet for the right resource to help you get started with hacking, only to be overwhelmed by the quantity of contradictory material available on the subject of hacking and cybersecurity? If you answered yes to any of these questions, this book is for you. Hacking is growing more sophisticated and complicated, and businesses are trying to secure their digital assets from dangers by implementing cybersecurity measures. These systems must be reviewed on a regular basis to verify that they are performing as intended. Penetration testers and ethical hackers, programmers who are educated to detect and exploit network flaws and suggest solutions to cover them up, are the individuals who can do these inspections. Companies are searching for penetration testers and cybersecurity specialists that have actual, hands-on expertise with Kali Linux and other open-source hacking tools now more than ever. This powerful book will teach you how to master the industry-standard platform for hacking, penetration testing, and security testing. This book assumes you know nothing about Kali Linux or hacking. It will teach you from the ground up how to utilize Kali Linux and other open-source tools to become a hacker and understand the procedures behind a successful penetration test. Here's a sneak peek at what you'll study in Kali Linux Hacking: A brief overview of the notion of "hacking" and Kali Linux. Everything you need to know about hacking, from session hijacking and SQL injection to phishing and denial-of-service assaults. Why hackers aren't necessarily terrible folks, as well as the eight different sorts of hackers in today's world Why is Kali Linux so popular among both amateur and professional hackers? Step-by-step instructions for installing and configuring Kali Linux on your PC. How to grasp the Linux terminal, as well as basic Linux commands you must be aware with An in-depth look at how to use Nmap to analyze, discover, and exploit vulnerabilities. How to remain anonymous when conducting hacking assaults or penetration testing How to Become a Better Hacker by Using Bash and Python Scripting ...and Much More!.... This book is intended for total novices and is jam-packed with practical examples and real-world hacking methods taught in clear, straightforward English. This book is for the next generation of 21st-century hackers and cyber defenders, and it will help you improve your cybersecurity and pen-testing abilities. Whether you're just starting with hacking, planning for a career transition into the realm of cybersecurity, or just trying to beef up your résumé and make yourself more appealing to recruiters, Kali Linux Hacking is the book for you! Do you want to learn more? To get started, click Buy Now With 1-Click or Buy Now.

Kali Linux CTF Blueprints Packt Publishing Ltd

Are you interested in learning more about hacking and how you can use these techniques to keep yourself and your network as safe as possible? Would you like to work with Kali Linux to protect your network and to make sure that hackers are not able to get onto your computer and cause trouble or steal your personal information? Have you ever been interested in learning more about the process of hacking, how to avoid being taken advantage of, and how you can use some of techniques for your own needs? In this Kali Linux For Hackers book, you will discover: - A concise introduction to the concept of "hacking" and Kali Linux - Everything you need to know about the different types of hacking, from session hijacking and SQL injection to phishing and DOS attacks - Why hackers aren't always bad guys as well as the 8 hacker types in today's cyberspace - Why Kali Linux is the platform of choice for many amateur and professional hackers - Step-by-step instructions to set up and install Kali Linux on your computer - How to master the Linux terminal as well as fundamental Linux commands you absolutely need to know about - A complete guide to using Nmap to understand, detect and exploit vulnerabilities - How to effectively stay anonymous while carrying out hacking attacks or penetration testing - How to use Bash and Python scripting to become a better hacker ...and tons more! When you are ready to learn more about hacking with Kali Linux and how this can benefit your own network and computer, make sure to check out this guidebook to get started!

Mastering Kali Linux for Advanced Penetration Testing Elsevier

Discover the most common web vulnerabilities and prevent them from becoming a threat to your site's security Key Features Familiarize yourself with

the most common web vulnerabilities Conduct a preliminary assessment of attack surfaces and run exploits in your lab Explore new tools in the Kali Linux ecosystem for web penetration testing Book Description 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 that provides a broad array of testing tools, many of which can be used to execute web penetration testing. Kali Linux Web Penetration Testing Cookbook gives you the skills you need to cover every stage of a penetration test – from gathering information about the system and application, to identifying vulnerabilities through manual testing. You will also cover the use of vulnerability scanners and look at basic and advanced exploitation techniques that may lead to a full system compromise. You will start by setting up a testing laboratory, exploring the latest features of tools included in Kali Linux and performing a wide range of tasks with OWASP ZAP, Burp Suite and other web proxies and security testing tools. As you make your way through the book, you will learn how to use automated scanners to find security flaws in web applications and understand how to bypass basic security controls. In the concluding chapters, you will look at what you have learned in the context of the Open Web Application Security Project (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 this book, you will have acquired the skills you need to identify, exploit, and prevent web application vulnerabilities. What you will learn Set up a secure penetration testing laboratory Use proxies, crawlers, and spiders to investigate an entire website Identify cross-site scripting and client-side vulnerabilities Exploit vulnerabilities that allow the insertion of code into web applications Exploit vulnerabilities that require complex setups Improve testing efficiency using automated vulnerability scanners Learn how to circumvent security controls put in place to prevent attacks Who this book is for Kali Linux Web Penetration Testing Cookbook 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. The basics of operating a Linux environment and prior exposure to security technologies and tools are necessary.

Web Penetration Testing with Kali Linux Packt Publishing Ltd

Get hands-on experience in using Burp Suite to execute attacks and perform web assessments Key FeaturesExplore the tools in Burp Suite to meet your web infrastructure security demandsConfigure Burp to fine-tune the suite of tools specific to the targetUse Burp extensions to assist with different technologies commonly found in application stacksBook Description Burp Suite is a Java-based platform for testing the security of your web applications, and has been adopted widely by professional enterprise testers. The Burp Suite Cookbook contains recipes to tackle challenges in determining and exploring vulnerabilities in web applications. You will learn how to uncover security flaws with various test cases for complex environments. After you have configured Burp for your environment, you will use Burp tools such as Spider, Scanner, Intruder, Repeater, and Decoder, among others, to resolve specific problems faced by pentesters. You will also explore working with various modes of Burp and then perform operations on the web. Toward the end, you will cover recipes that target specific test scenarios and resolve them using best practices. By the end of the book, you will be up and running with deploying Burp for securing web applications. What you will learnConfigure Burp Suite for your web applicationsPerform authentication, authorization, business logic, and data validation testingExplore session management and client-side testingUnderstand unrestricted file uploads and server-side request forgeryExecute XML external entity attacks with BurpPerform remote code execution with BurpWho this book is for If you are a security professional, web pentester, or software developer who wants to adopt Burp Suite for applications security, this book is for you.

Kali Linux Web Penetration Testing Cookbook Packt Publishing Ltd

Taking a highly practical approach and a playful tone, Kali Linux CTF Blueprints provides step-by-step guides to setting up vulnerabilities, in-depth guidance to exploiting them, and a variety of advice and ideas to build and customising your own challenges. If you are a penetration testing team leader or individual who wishes to challenge yourself or your friends in the creation of penetration testing assault courses, this is the book for you. The book assumes a basic level of penetration skills and familiarity with the Kali Linux operating system.

SQL Injection Strategies Packt Publishing Ltd

Over 70 recipes for system administrators or DevOps to master Kali Linux 2 and perform effective security assessments About This Book Set up a penetration testing lab to conduct a preliminary assessment of attack surfaces and run exploits Improve your testing efficiency with the use of automated vulnerability scanners Work through step-by-step recipes to detect a wide array of vulnerabilities, exploit them to analyze their consequences, and identify security anomalies Who This Book Is For This book is intended for those who want to know more about information security. In particular, it's ideal for system administrators and system architects who want to ensure that the infrastructure and systems they are creating and managing are secure. This book helps both beginners and intermediates by allowing them to use it as a reference book and to gain in-depth knowledge. What You Will Learn Understand the importance of security assessments over merely setting up and managing systems/processes Familiarize yourself with tools such as OPENVAS to locate system and network vulnerabilities Discover multiple solutions to escalate privileges on a compromised machine Identify security anomalies in order to make your infrastructure secure and further strengthen it Acquire the skills to prevent infrastructure and application vulnerabilities Exploit vulnerabilities that require a complex setup with the help of Metasploit In Detail With the increasing threats of breaches and attacks on critical infrastructure, system administrators and architects can use Kali Linux 2.0 to ensure their infrastructure is secure by finding out known vulnerabilities and safeguarding their infrastructure against unknown vulnerabilities. This practical cookbook-style guide contains chapters carefully structured in three phases – information gathering, vulnerability assessment, and penetration testing for the web, and wired and wireless networks. It's an ideal reference guide if you're looking for a solution to a specific problem or learning how to use a tool. We provide hands-on examples of powerful tools/scripts designed for exploitation. In the final section, we cover various tools you can use during testing, and we help you create in-depth reports to impress management. We provide system engineers with steps to reproduce issues and fix them. Style and approach This practical book is full of easy-to-follow recipes with based on real-world problems faced by the authors. Each recipe is divided into three sections, clearly defining what the recipe does, what you need, and how to do it. The carefully structured recipes allow you to go directly to your topic of interest.

Hacking: Penetration Testing with Kali Linux Packt Publishing Ltd

Would you like to become an ace in cybersecurity systems and learn about ethical hacking? If you answered yes, this book is ideal. Hacking is an increasingly complex skill to develop, the system is complicated, and companies are rushing to protect their digital assets from threats by setting up cybersecurity systems. These systems must be checked regularly to ensure that these systems perform the jobs for which they are designed. The people who can perform these checks are penetration testers and ethical hackers, programmers who are trained to find and exploit vulnerabilities in networks and offer ways to cover them. Now more than ever, companies are looking for penetration testers and cybersecurity professionals who have hands-on and hands-on experience with Kali Linux and other open-source hacking tools. In this powerful book, you will learn how to master the industry-standard platform for hacking, penetration, and security testing: Kali Linux. This book assumes that you know nothing about Kali Linux and hacking. It will start from scratch and develop your practical knowledge on using Kali Linux and other open-source tools to become a hacker and understand the processes behind a penetration test. Success. Here is a preview of what you will learn about Kali Linux Hacking: A brief introduction to the concept of "hacking" and Kali Linux Everything you need to know about the different types of hacking, from session hijacking and SQL injection to phishing and DOS attacks Because hackers aren't always bad as are the 8 types of hackers in cyberspace today Because Kali Linux is the platform of choice for many amateur and professional hackers Detailed instructions to set up and install Kali Linux on your computer How to master the Linux terminal and basic Linux commands you absolutely must know. A comprehensive guide to using Nmap to understand, detect and exploit vulnerabilities How to effectively remain anonymous while performing hacking attacks or penetration tests How to use Bash and Python scripts to become a better hacker ... and much more! Designed with absolute beginners in mind, this book is packed with practical examples and real-world hacking techniques explained in plain, simple English. This book is for the new generation of hackers and cyber defenders of the 21st century and will help you improve your cybersecurity and pen testing skills. Whether you're just getting started with hacking or preparing for a career change in cybersecurity, or just looking to improve your resume and become more attractive to employers, Kali Linux Hacking is the book you need! Would you like to know more?

Kali Linux 2 – Assuring Security by Penetration Testing Independently Published

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.

Sql Injection Attack and Countermeasures Packt Publishing Ltd

Learn to exploit vulnerable database applications using SQL injection tools and techniques, while understanding how to effectively prevent attacks Key FeaturesUnderstand SQL injection and its effects on websites and other systemsGet hands-on with SQL injection using both manual and automated toolsExplore practical tips for various attack and defense strategies relating to SQL injectionBook Description SQL injection (SQLi) is probably the most infamous attack that can be unleashed against applications on the internet. SQL Injection Strategies is an end-to-end guide for beginners looking to learn how to perform SQL injection and test the security of web applications, websites, or databases, using both manual and automated techniques. The book serves as both a theoretical and practical guide to take you through the important aspects of SQL injection, both from an attack and a defense perspective. You'll start with a thorough introduction to SQL injection and its impact on websites and systems. Later, the book features steps to configure a virtual environment, so you can try SQL injection techniques safely on your own computer. These tests can be performed not only on web applications but also on web services and mobile applications that can be used for managing IoT environments. Tools such as sqlmap and others are then covered, helping you understand how to use them effectively to perform SQL injection attacks. By the end of this book, you will be well-versed with SQL injection, from both the attack and defense perspective. What you will learnFocus on how to defend against SQL injection attacksUnderstand web application securityGet up and running with a variety of SQL injection conceptsBecome well-versed with different SQL injection scenariosDiscover SQL injection manual attack techniquesDelve into SQL injection automated techniquesWho this book is for This book is ideal for penetration testers, ethical hackers, or anyone who wants to learn about SQL injection and the various attack and defense strategies against this web security vulnerability. No prior knowledge of SQL injection is needed to get started with this book.

SQL Hacks Independently Published

Achieve the gold standard in penetration testing with Kali using this masterpiece, now in its third edition! About This Book Get a rock-solid insight into penetration testing techniques and test your corporate network against threats like never before Formulate your pentesting strategies by relying on the most up-to-date and feature-rich Kali version in town—Kali Linux 2 (aka Sana). Experience this journey with new cutting-edge wireless penetration tools and a variety of new features to make your pentesting experience smoother Who This Book Is For If you are an IT security professional or a student with basic knowledge of Unix/Linux operating systems, including an awareness of information security factors, and you want to use Kali Linux for penetration testing, this book is for you. What You Will Learn Find out to download and install your own copy of Kali Linux Properly scope and conduct the initial stages of a penetration test Conduct reconnaissance and enumeration of target networks Exploit and gain a foothold on a target system or network Obtain and crack passwords Use the Kali Linux NetHunter install to conduct wireless penetration testing Create proper penetration testing reports In Detail Kali Linux is a comprehensive penetration testing platform with advanced tools to identify, detect, and exploit the vulnerabilities uncovered in the target network environment. With Kali Linux, you can apply appropriate testing methodology with defined business objectives and a scheduled test plan, resulting in a successful penetration testing project engagement. Kali Linux – Assuring Security by Penetration Testing is a fully focused, structured book providing guidance on developing practical penetration testing skills by demonstrating cutting-edge hacker tools and techniques with a coherent, step-by-step approach. This book offers you all of the essential lab preparation and testing procedures that reflect real-world attack scenarios from a business perspective, in today's digital age. Style and approach This practical guide will showcase penetration testing through cutting-edge tools and techniques using a coherent, step-by-step approach.

SQL Injection Attack and Defense Packt Publishing

Hacking with Kali Linux - When you don't know sh#t is a comprehensive guide to ethical hacking using the Kali Linux operating system. The book provides a detailed introduction to the basics of hacking and covers the tools and techniques used in ethical hacking. The book is written for individuals who are interested in learning about ethical hacking and have little to no experience with Kali Linux. It is also suitable for individuals who have experience with other operating systems and are interested in learning about Kali Linux. The book is divided into eight chapters, with each chapter focusing on a specific aspect of ethical hacking. The first chapter provides an introduction to hacking, its types, ethics, and legal implications, as well as an overview of Kali Linux tools for ethical hacking. The second chapter covers the downloading and installation of Kali Linux, as well as setting up virtual environments for hacking and basic configuration of Kali Linux. Chapters three and four cover information gathering, scanning for open ports and services, vulnerability scanning and exploitation using Kali Linux tools. Chapter five focuses on password cracking and wireless network hacking, including techniques for wireless network penetration testing. Chapter six covers advanced hacking techniques, including exploiting web applications, social engineering, evading detection, and staying anonymous. Chapter seven delves into forensics and analysis, including techniques for forensic analysis, using Kali Linux tools for forensic analysis, recovering data from a compromised system, and analysis of logs and event data. Finally, chapter eight covers building a secure network using Kali Linux tools, monitoring and protecting a network from attacks, and techniques for securing web applications and databases. Throughout the book, readers are provided with examples and hypothetical scenarios to help them understand and apply the concepts covered. By the end of the book, readers will have gained a comprehensive understanding of ethical hacking using Kali Linux and will be able to apply their knowledge in real-world situations.

SQL injection attacks and mitigations Packt Publishing Ltd

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 "O'Reilly Media, Inc."

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.

Kali Linux Cookbook "O'Reilly Media, Inc."

In today's world, SQL Injection is a serious security threat over the Internet for the various dynamic web applications residing over the internet. These Web applications conduct many vital processes in various web-based businesses. As the use of internet for various online services is rising, so is the security threats present in the web increasing. There is a universal need present for all dynamic web applications and this universal need is the need to store, retrieve or manipulate information from a database. Most of systems which manage the databases and its requirements such as MySQL Server and PostgreSQL use SQL as their language. Flexibility of SQL makes it a powerful language. It allows its users to ask what he/she wants without leaking any information about how the data will be fetched. However the vast use of SQL based databases has made it the center of attention of hackers. They take advantage of the poorly coded Web applications to attack the databases. They introduce an apparent SQL query, through an unauthorized user input, into the legitimate query statement. In this paper, we have tried to present a comprehensive review of all the different types of SQL injection attacks present, as well as detection of such attacks and preventive measure used. We have highlighted their individual strengths and weaknesses. Such a classification would help other researchers to choose the right technique for further studies.

Related with Sql Injection Kali Tutorial:

• Name That Angle Pair Color Worksheet Answer Key : click here