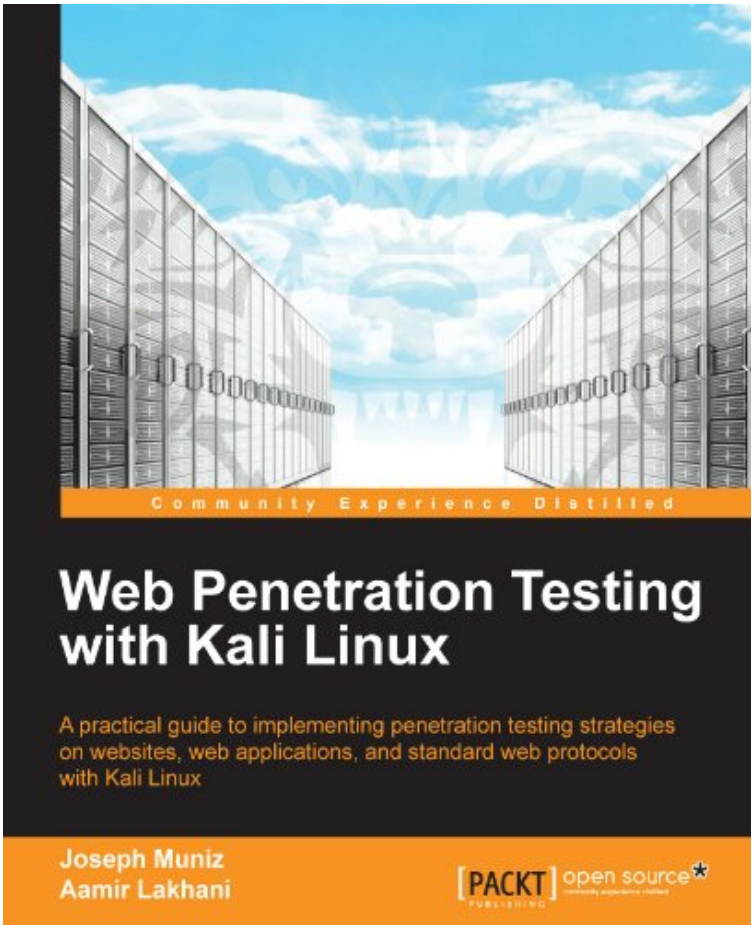
Web Penetration Testing with Kali Linux

Von Joseph Muniz, Aamir Lakhani
*ebooks | Download PDF | *ePub | DOC | audiobook*



Produktinformation -Verkaufsrang: #400271 in eBooksVerffentlicht am: 2013-09-25Erscheinungsdatum: 2013-09-25File Name: B00FF8OK12 | File size: 74.Mb

Von Joseph Muniz, Aamir Lakhani : Web Penetration Testing with Kali Linux before purchasing it in order to gage whether or not it would be worth my time, and all praised Web Penetration Testing with Kali Linux:

KundenrezensionenHilfreichste Kundenrezensionen0 von 2 Kunden fanden die folgende Rezension hilfreich. Fr NeulingeVon MajestixFr jemanden der sich auf dem Gebiet Linux nicht sicher ist, jedoch verstanden hat das es mit Windows nicht mglich ist vernftig zu testen wird dieses Buch wrmstens empfohlen.Voraussetzung: Englisch lesen ;)Das Buch beginnt wirklich am Anfang mit Grundlagen und fhrt an das Thema heran. Es gibt dann Beispiele und Anleitungen wie Systeme getestet werden mit Kali.Ein Buch gefllt mit Wissen! PERFEKT!Wer sich unsicher ist blttern einfach in der Vorschau durch das Inhaltsverzeichnis ;)

KurzbeschreibungIn DetailKali Linux is built for professional penetration testing and security auditing. It is the next-

generation of BackTrack, the most popular open-source penetration toolkit in the world. Readers will learn how to think like real attackers, exploit systems, and expose vulnerabilities.Even though web applications are developed in a very secure environment and have an intrusion detection system and firewall in place to detect and prevent any malicious activity, open ports are a pre-requisite for conducting online business. These ports serve as an open door for attackers to attack these applications. As a result, penetration testing becomes essential to test the integrity of web-applications. Web Penetration Testing with Kali Linux is a hands-on guide that will give you step-by-step methods on finding vulnerabilities and exploiting web applications."Web Penetration Testing with Kali Linux" looks at the aspects of web penetration testing from the mind of an attacker. It provides real-world, practical step-by-step instructions on how to perform web penetration testing exercises.You will learn how to use network reconnaissance to pick your targets and gather information. Then, you will use server-side attacks to expose vulnerabilities in web servers and their applications. Client attacks will exploit the way end users use web applications and their workstations. You will also learn how to use open source tools to write reports and get tips on how to sell penetration tests and look out for common pitfalls.On the completion of this book, you will have the skills needed to use Kali Linux for web penetration tests and expose vulnerabilities on web applications and clients that access them.Approach"Web Penetration Testing with Kali Linux" contains various penetration testing methods using BackTrack that will be used by the reader. It contains clear step-by-step instructions with lot of screenshots. It is written in an easy to understand language which will further simplify the understanding for the user.Who this book is for"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.KurzbeschreibungIn DetailKali Linux is built for professional penetration testing and security auditing. It is the next-generation of BackTrack, the most popular open-source penetration toolkit in the world. Readers will learn how to think like real attackers, exploit systems, and expose vulnerabilities.Even though web applications are developed in a very secure environment and have an intrusion detection system and firewall in place to detect and prevent any malicious activity, open ports are a pre-requisite for conducting online business. These ports serve as an open door for attackers to attack these applications. As a result, penetration testing becomes essential to test the integrity of web-applications. Web Penetration Testing with Kali Linux is a hands-on guide that will give you step-by-step methods on finding vulnerabilities and exploiting web applications."Web Penetration Testing with Kali Linux" looks at the aspects of web penetration testing from the mind of an attacker. It provides real-world, practical step-by-step instructions on how to perform web penetration testing exercises.You will learn how to use network reconnaissance to pick your targets and gather information. Then, you will use server-side attacks to expose vulnerabilities in web servers and their applications. Client attacks will exploit the way end users use web applications and their workstations. You will also learn how to use open source tools to write reports and get tips on how to sell penetration tests and look out for common pitfalls.On the completion of this book, you will have the skills needed to use Kali Linux for web penetration tests and expose vulnerabilities on web applications and clients that access them.Approach"Web Penetration Testing with Kali Linux" contains various penetration testing methods using BackTrack that will be used by the reader. It contains clear step-by-step instructions with lot of screenshots. It is written in an easy to understand language which will further simplify the understanding for the user.Who this book is for"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.ber den Autor und weitere MitwirkendeJoseph Muniz Joseph Muniz is a technical solutions architect and security researcher. He started his career in software development and later managed networks as a contracted technical resource. Joseph moved into consulting and found a passion for security while meeting with a variety of customers. He has been involved with the design and implementation of multiple projects ranging from Fortune 500 corporations to large federal network. Joseph runs TheSecurityBlogger.com website, a popular resources regarding security and product implementation. You can also find Joseph speaking at live events as well as involved with other publications. Recent events include speaker for Social Media Deception at the 2013 ASIS International conference, speaker for Eliminate Network Blind Spots with Data Center Security webinar, speaker for Making Bring Your Own Device (BYOD) Work at the Government Solutions Forum, Washington DC, and an article on Compromising Passwords in PenTest Magazine - Backtrack Compendium, July 2013. Outside of work, he can be found behind turntables scratching classic vinyl or on the soccer pitch hacking away at the local club teams.Aamir Lakhani Aamir Lakhani is a leading Cyber Security and Cyber Counterintelligence architect. He is responsible for providing IT security solutions to major commercial and federal enterprise organizations. Lakhani leads projects that implement security postures for Fortune 500 companies, the US Department of Defense, major healthcare providers, educational institutions, and financial and media organizations. Lakhani has designed offensive counter defense measures for defense and intelligence agencies, and has

assisted organizations in defending themselves from active strike back attacks perpetrated by underground cyber groups. Lakhani is considered an industry leader in support of detailed architectural engagements and projects on topics related to cyber defense, mobile application threats, malware, and Advanced Persistent Threat (APT) research, and Dark Security. Lakhani is the author and contributor of several books, and has appeared on National Public Radio as an expert on Cyber Security. Writing under the pseudonym Dr. Chaos, Lakhani also operates the DrChaos.com blog. In their recent list of 46 Federal Technology Experts to Follow on Twitter, Forbes magazine described Aamir Lakhani as "a blogger, infosec specialist, superhero..., and all around good guy."