Backtrack 5r3 Reaver

PRATT ROWAN

Web Penetration Testing with Kali Linux Packt Publishing Ltd
Nasıl hackleneceğini bilmeden, hacker'lardan korunamazsınız! Linux'un getirmiş olduğu özgürlüklerin sınırının olmadığı su götürmez bir gerçektir. Bu özgürlüğün içerisinde Penetration Tester ve Ethical Hacker ünvanına sahip ya da sahip olmak isteyen kişilere hitap eden kitabımız, Backtrack 5 R3 ve Penetrasyon Testleri'ne dair teknik özellikler ve uygulamaları barındırmaktadır. Örnekler, açıklamalar ve görsel yapı ile incelenen Backtrack 5 ve Penetrasyon Testleri hususu, kitapta detaylar ve pratikler ile sizlere sunulmuştur. Tüm kullanıcılara hitap eden kitap, yazılımsal güvenlik mekanizmalarının mimarları olan Ethical Hacker'ların bu işi nasıl yaptıklarına dair sizlere eğitici bilgiler sunmaktadır. • Black Box, Gray Box, White Box Penetrasyon Testleri • Ortam Dinlemeleri Nasıl Yapılmaktadır? • SQL Enjeksiyonları, XSS Betik Saldırıları, Servis Durdurma Saldırıları ve İlişkileri • Flash Bellek ile Backtrack Booting • Backtrack Erişim Yetkileri • Backtrack ve Trafik İzleme • Clickjacking Saldırıları • Frequancy Damping • Kablosuz Ağlara Nasıl Sızılır? • SQL Enjeksiyon ile Web Sistemlerine Saldırı İşlemleri ve daha fazlası...

Ethical Hacking and Penetration Testing Guide Albert Whitman & Company
Honor Book - 2011 Paterson Prize for Books for Young People 2013 Grand Canyon Reader Award Nominee The Green Prize for Sustainable Literature, Youth Picture Book, 2011 Counting and nature combine in this tree-rific tale. If you listen closely, the lone tree behind Oak Lane School has a story to tell. It starts with one owl, two spiders, and goes all the way up to ten earthworms using the tree as their home! So what does this tree need? Learn about the importance of trees and count from one to ten in this tale about going green.

Rtfm Packt Publishing Ltd
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.

Packt Publishing Ltd

Hacking Wireless Access Points: Cracking, Tracking, and Signal Jacking provides readers with a deeper understanding of the hacking threats that exist with mobile phones, laptops, routers, and navigation systems. In addition, applications for Bluetooth and near field communication (NFC) technology continue to multiply, with athletic shoes, heart rate monitors, fitness sensors, cameras, printers, headsets, fitness trackers, household appliances, and the number and types of wireless devices all continuing to increase dramatically. The book demonstrates a variety of ways that these vulnerabilities can be—and have been—exploited, and how the unfortunate consequences of such exploitations can be mitigated through the responsible use of technology. - Explains how the wireless access points in common, everyday devices can expose us to hacks and threats - Teaches how wireless access points can be hacked, also providing the techniques necessary to protect and defend data - Presents concrete examples and real-world guidance on how to protect against wireless access point attacks

Linux Forensics BACKTRACK 5 R3 VE PENETRASYON TESTLERİ

Requiring no prior hacking experience, Ethical Hacking and Penetration Testing Guide supplies a complete introduction to the steps required to complete a penetration test, or ethical hack, from beginning to end. You will learn how to properly utilize and interpret the results of modern-day hacking tools, which are required to complete a penetration test. The book covers a wide range of tools, including Backtrack Linux, Google reconnaissance, MetaGooFil, dig, Nmap, Nessus, Metasploit, Fast Track Autopwn, Netcat, and Hacker Defender rootkit. Supplying a simple and clean explanation of how to effectively utilize these tools, it details a four-step methodology for conducting an effective penetration test or hack.Providing an accessible introduction to penetration testing and hacking, the book supplies you with a fundamental understanding of offensive security. After completing the book you will be prepared to take on in-depth and advanced topics in hacking and penetration testing. The book walks you through each of the steps and tools in a structured, orderly manner allowing you to understand how the output from each tool can be fully utilized in the subsequent phases of the penetration test. This process will allow you to clearly see how the various tools and phases relate to each other. An ideal resource for those who want to learn about ethical hacking but don‘t know where to start, this book will help take your hacking skills to the next level. The topics described in this book comply with international standards and with what is being taught in international certifications.

Rapid BeagleBoard Prototyping with MATLAB and Simulink Ujjwal Sahay

The state of California votes on secession in the wake of a divisive presidential election in this gripping, prescient novel of marriage, family, and the profound moments that shape our lives. Doctor Julie Walker has just signed her divorce papers when she receives news that her younger sister, Heather, has gone into labor. Though theirs is a strained relationship, Julie sets out for the hospital to be at her sister’s side—no easy task since the streets of San Francisco are filled with tension and strife. Today is also the day that Julie will find herself at the epicenter of a violent standoff in which she is forced to examine both the promising and the painful parts of her past—her Southern childhood; her romance with her husband, Tom; her estrangement from Heather; and the shattering incident that led to her greatest heartbreak. Infused with emotional depth and poignancy, Golden State takes readers on a journey over the course of a single, unforgettable day—through an extraordinary landscape of love, loss, and hope. Praise for Golden State “A stirring look at the ties that bind husband-wife, mother-child and even sisters, and what happens when they’re torn asunder. Set in a San Francisco chafing with unrest both political and personal, the world Richmond creates is exquisitely charged with regret and hope.”—Family Circle “[A] riveting read that can be recommended to fans of Jodi Picoult and Jacquelyn Mitchard . . . Mesmerizing and intricate, Richmond’s dissection of a California on the violent brink of secession from the nation provides the backdrop to her deeper inspection of the uneasy, fragile relationship between siblings.”—Booklist (starred review) “[An] amazing, turbulent novel woven of disparate threads . . . Nearly every feature of this mesmerizing novel is provocative, as Richmond explores the fragmented, hopeful lives of complex characters. This is gripping, multilayered must-read fiction.”—Library Journal (starred review) “An exciting premise . . . skillfully written . . . Julie’s past and her relationship with the other characters are scrutinized as the clock ticks. It’s an interesting and sometimes-disturbing study.”—Kirkus Reviews “Richmond takes readers through a bittersweet, heartwarming tale of a woman on the cusp of life-changing events in both her personal and professional lives. . . . Once invested, the reader is carried away by this action-packed, poignant story, making this a tale that will live in the heart of the reader once the last page is read.”—RT Book Reviews “This is a thoughtful book about how past circumstances change us into the people we are today, for the good or bad. Julie is a sympathetic and relatable character, and readers will definitely feel for her as she goes through her life-changing day.”—The Parkersburg News and Sentinel “Richmond . . . delivers a page-turner.”—San Jose Mercury News “A breathtaking read and one I’ll not soon forget.”—Melanie Benjamin, author of The Aviator’s Wife Look for special features inside. Join the Random House Reader’s Circle for author chats and more.

Mobile Devices John Wiley & Sons

This Book is written by keeping one object in mind that a beginner, who is not much familiar regarding computer hacking, can easily, attempts these hacks and recognize what we are trying to demonstrate. After Reading this book you will come to recognize that how Hacking is affecting our everyday routine work and can be very hazardous in many fields.

This Tree Counts! John Wiley & Sons

Wireless and mobile communications have grown exponentially. The average individual now possesses a minimum of two smart mobile devices. The consistent advancement of mobile devices feeds the ever-growing appetite for faster bandwidth,

uninterrupted connectivity, applications to fulfill the needs of consumers and businesses, and security for all of
Mastering Kali Linux for Advanced Penetration Testing KODLAB YAYIN DAĞITIM YAZILIM LTD.ŞTİ.
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.
Golden State CRC Press
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.
CEH: Certified Ethical Hacker Version 8 Study Guide Syngress
This book is a fast-paced guide with practical, hands-on recipes which will show you how to prototype Beagleboard-based audio/video applications using Matlab/Simlink and Sourcery Codebench on a Windows host.Beagleboard Embedded Projects is great for students and academic researchers who have practical ideas and who want to build a proof-of-concept system on an embedded hardware platform quickly and efficiently. It is also useful for product design engineers who want to ratify their applications and reduce the time-to-market. It is assumed that you are familiar with Matlab/Simulink and have some basic knowledge of computer hardware. Experience in Linux is favoured but not necessary, as our software development is purely on a Windows host.
Advanced Penetration Testing Createspace Independent Publishing Platform
Prepare for the new Certified Ethical Hacker version 8 exam with this Sybex guide Security professionals remain in high demand. The Certified Ethical Hacker is a one-of-a-kind certification designed to give the candidate a look inside the mind of a hacker. This study guide provides a concise, easy-to-follow approach that covers all of the exam objectives and includes numerous examples and hands-on exercises. Coverage includes cryptography, footprinting and reconnaissance, scanning networks, enumeration of services, gaining access to a system, Trojans, viruses, worms, covert channels, and much more. A companion website includes additional study tools, Including practice exam and chapter review questions and electronic flashcards. Security remains the fastest growing segment of IT, and CEH certification provides unique skills The CEH also satisfies the Department of Defense’s 8570 Directive, which requires all Information Assurance government positions to hold one of the approved certifications This Sybex study guide is perfect for candidates studying on their own as well as those who are taking the CEHv8 course Covers all the exam objectives with an easy-to-follow approach Companion website includes practice exam questions, flashcards, and a searchable Glossary of key terms CEHv8: Certified Ethical Hacker Version 8 Study Guide is the book you need when you're ready to tackle this challenging exam Also available as a set, Ethical Hacking and Web Hacking Set, 9781119072171 with The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, 2nd Edition.
Mastering Kali Linux for Advanced Penetration Testing CreateSpace
Wireless Hacking 101 - How to hack wireless networks easily! This book is perfect for computer enthusiasts that want to gain expertise in the interesting world of ethical hacking and that wish to start conducting wireless pentesting. Inside you will find step-by-step instructions about how to exploit WiFi networks using the tools within the known Kali Linux distro as the famous aircrack-ng suite. Topics covered: •Introduction to WiFi Hacking •What is Wardriving •WiFi Hacking Methodology •WiFi Mapping •Attacks to WiFi clients and networks •Defeating MAC control •Attacks to WEP, WPA, and WPA2 •Attacks to WPS •Creating Rogue AP's •MITM attacks to WiFi clients and data capture •Defeating WiFi clients and evading SSL encryption •Kidnapping sessions from

WiFi clients •Defensive mechanisms

HACK-X-CRYPT Bantam

Linux Forensics is the most comprehensive and up-to-date resource for those wishing to quickly and efficiently perform forensicson Linux systems. It is also a great asset for anyone that would like to better understand Linux internals. Linux Forensics will guide you step by step through the process of investigating a computer running Linux. Everything you need to know from the moment you receive the call from someone who thinks they have been attacked until the final report is written is covered in this book. All of the tools discussed in this book are free and most are also open source. Dr. Philip Polstra shows how to leverage numerous tools such as Python, shell scripting, and MySQL to quickly, easily, and accurately analyze Linux systems. While readers will have a strong grasp of Python and shell scripting by the time they complete this book, no priorknowledge of either of these scripting languages is assumed. Linux Forensics begins by showing you how to determine if there was an incident with minimally invasive techniques. Once it appears likely that an incident has occurred, Dr. Polstra shows you how to collect data from a live system before shutting it down for the creation of filesystem images. Linux Forensics contains extensive coverage of Linux ext2, ext3, and ext4 filesystems. A large collection of Python and shell scripts for creating, mounting, and analyzing filesystem images are presented in this book. Dr. Polstra introduces readers to the exciting new field of memory analysis using the Volatility framework. Discussions of advanced attacks and malware analysis round out the book. Book Highlights 370 pages in large, easy-to-read 8.5 x 11 inch format Over 9000 lines of Python scripts with explanations Over 800 lines of shell scripts with explanations A 102 page chapter containing up-to-date information on the ext4 filesystem Two scenarios described in detail with images available from the book website All scripts and other support files are available from the book website Chapter Contents First Steps General Principles Phases of Investigation High-level Process Building a Toolkit Determining If There Was an Incident Opening a Case Talking to Users Documenation Mounting Known-good Binaries Minimizing Disturbance to the Subject Automation With Scripting Live Analysis Getting Metadata Using Spreadsheets Getting Command Histories Getting Logs Using Hashes Dumping RAM Creating Images Shutting Down the System Image Formats DD DCFLDD Write Blocking Imaging Virtual Machines Imaging Physical Drives Mounting Images Master Boot Record Based Partions GUID Partition Tables Mounting Partitions In Linux Automating With Python Analyzing Mounted Images Getting Timestamps Using LibreOffice Using MySQL Creating Timelines Extended Filesystems Basics Superblocks Features Using Python Finding Things That Are Out Of Place Inodes Journaling Memory Analysis Volatility Creating Profiles Linux Commands Dealing With More Advanced Attackers Malware Is It Malware? Malware Analysis Tools Static Analysis Dynamic Analysis Obfuscation The Road Ahead Learning More Communities Conferences Certifications

Network analysis Babelcube Inc.

A practical guide to testing your infrastructure security with Kali Linux, the preferred choice of pentesters and hackers Key FeaturesEmploy advanced pentesting techniques with Kali Linux to build highly secured systemsDiscover various stealth techniques to remain undetected and defeat modern infrastructuresExplore red teaming techniques to exploit secured environmentBook 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 learnConfigure the most effective Kali Linux tools to test infrastructure securityEmploy stealth to avoid detection in the infrastructure being testedRecognize when stealth attacks are being used against your infrastructureExploit networks and data systems using wired and wireless networks as well as web servicesIdentify and download valuable data from target systemsMaintain access to compromised systemsUse social engineering to compromise the weakest part of the network - the end usersWho 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.

Mastering Kali Linux for Web Penetration Testing Packt Publishing Ltd

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.

Wireless Hacking 101 Packt Publishing Ltd

BACKTRACK 5 R3 VE PENETRASYON TESTLERİKODLAB YAYIN DAĞITIM YAZILIM LTD.ŞTİ.

BACKTRACK 5 R3 VE PENETRASYON TESTLERİ CRC Press

The Red Team Field Manual (RTFM) is a no fluff, but thorough reference guide for serious Red Team members who routinely find themselves on a mission without Google or the time to scan through a man page. The RTFM contains the basic syntax for commonly used Linux and Windows command line tools, but it also encapsulates unique use cases for powerful tools such as Python and Windows PowerShell. The RTFM will repeatedly save you time looking up the hard to remember Windows nuances such as Windows wmic and dsquery command line tools, key registry values, scheduled tasks syntax, startup locations and Windows scripting. More importantly, it should teach you some new red team techniques.

Hacking Wireless Access Points