
Hacking Mit Metasploit Das Umfassende Handbuch Zu

The Phoenix Project

Hacking

Hacking- The art Of Exploitation

Mastering Kali Linux for Advanced Penetration Testing

Black Hat Python, 2nd Edition

Hacking mit Metasploit

Ubuntu 22.04 Schnelleinstieg

Social Engineering

Kali Linux Revealed

Learn Kali Linux 2019

CompTIA Security+

Advanced Penetration Testing

Einstieg in Kali Linux

The Ultimate Kali Linux Book

Real-World Bug Hunting

WLAN Hacking

Security für Data-Warehouse- und Business-Intelligence-Systeme

Hacking mit Metasploit

Hacking im Web 2.0

The Hacker Playbook 2

Metasploit

c't Admin (2020)

Hacking Tools For Computers

Learning Kali Linux

Linux für Anfänger - der leichte Einstieg / Mit praktischen Anleitungen für Anfänger +
140 Terminal-Befehle

Cybersecurity For Dummies

Hacking Your Education

USB Rubber Ducky

The Basics of Hacking and Penetration Testing

Click Here to Kill Everybody: Security and Survival in a Hyper-connected World

Hacking For Dummies

The Web Application Hacker's Handbook

Violent Python

Mastering Metasploit

The Book of Postfix
Hands-On Web Penetration Testing with Metasploit
Penetration Testing
Mobile Hacking
Einstieg in Kali Linux

*Hacking Mit Metasploit
Das Umfassende
Handbuch Zu*

Downloaded from
intra.itu.edu by guest

INGRID NEAL

The Phoenix Project dpunkt.verlag
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

Hacking Packt Publishing Ltd

When it comes to creating powerful and effective hacking tools, Python is the language of choice for most security analysts. But just how does the magic happen? In *Black Hat Python*, the latest from Justin Seitz (author of the best-

selling *Gray Hat Python*), you'll explore the darker side of Python's capabilities—writing network sniffers, manipulating packets, infecting virtual machines, creating stealthy trojans, and more. You'll learn how to:

- Create a trojan command-and-control using GitHub
- Detect sandboxing and automate common malware tasks, like keylogging and screenshotting
- Escalate Windows privileges with creative process control
- Use offensive memory forensics tricks to retrieve password hashes and inject shellcode into a virtual machine
- Extend the popular Burp Suite web-hacking tool
- Abuse Windows COM automation to perform a man-in-the-browser attack
- Exfiltrate data from a network most sneakily

Insider techniques and creative challenges

throughout show you how to extend the hacks and how to write your own exploits. When it comes to offensive security, your ability to create powerful tools on the fly is indispensable. Learn how in Black Hat Python. Uses Python 2

Hacking- The art Of Exploitation

MITP-Verlags GmbH & Co. KG

This book is a practical guide to discovering and exploiting security flaws in web applications. The authors explain each category of vulnerability using real-world examples, screen shots and code extracts. The book is extremely practical in focus, and describes in detail the steps involved in detecting and exploiting each kind of security weakness found within a variety of applications such as online banking, e-commerce and other web applications.

The topics covered include bypassing login mechanisms, injecting code, exploiting logic flaws and compromising other users. Because every web application is different, attacking them entails bringing to bear various general principles, techniques and experience in an imaginative way. The most successful hackers go beyond this, and find ways to automate their bespoke attacks. This handbook describes a proven methodology that combines the virtues of human intelligence and computerized brute force, often with devastating results. The authors are professional penetration testers who have been involved in web application security for nearly a decade. They have presented training courses at the Black Hat security conferences throughout the world. Under

the alias "PortSwigger", Dafydd developed the popular Burp Suite of web application hack tools.

Mastering Kali Linux for Advanced Penetration Testing Createspace Independent Publishing Platform Fully-updated for Python 3, the second edition of this worldwide bestseller (over 100,000 copies sold) explores the stealthier side of programming and brings you all new strategies for your hacking projects. When it comes to creating powerful and effective hacking tools, Python is the language of choice for most security analysts. In *Black Hat Python, 2nd Edition*, you'll explore the darker side of Python's capabilities—writing network sniffers, stealing email credentials, brute forcing directories, crafting mutation fuzzers,

infecting virtual machines, creating stealthy trojans, and more. The second edition of this bestselling hacking book contains code updated for the latest version of Python 3, as well as new techniques that reflect current industry best practices. You'll also find expanded explanations of Python libraries such as ctypes, struct, lxml, and BeautifulSoup, and dig deeper into strategies, from splitting bytes to leveraging computer-vision libraries, that you can apply to future hacking projects. You'll learn how to:

- Create a trojan command-and-control using GitHub
- Detect sandboxing and automate common malware tasks, like keylogging and screenshotting
- Escalate Windows privileges with creative process control
- Use offensive memory forensics tricks to

retrieve password hashes and inject shellcode into a virtual machine • Extend the popular Burp Suite web-hacking tool • Abuse Windows COM automation to perform a man-in-the-browser attack • Exfiltrate data from a network most sneakily When it comes to offensive security, your ability to create powerful tools on the fly is indispensable. Learn how with the second edition of Black Hat Python. New to this edition: All Python code has been updated to cover Python 3 and includes updated libraries used in current Python applications. Additionally, there are more in-depth explanations of the code and the programming techniques have been updated to current, common tactics. Examples of new material that you'll learn include how to sniff network traffic, evade anti-

virus software, brute-force web applications, and set up a command-and-control (C2) system using GitHub. [Black Hat Python, 2nd Edition](#) Heise Medien

A world of "smart" devices means the Internet can kill people. We need to act. Now. Everything is a computer. Ovens are computers that make things hot; refrigerators are computers that keep things cold. These computers—from home thermostats to chemical plants—are all online. The Internet, once a virtual abstraction, can now sense and touch the physical world. As we open our lives to this future, often called the Internet of Things, we are beginning to see its enormous potential in ideas like driverless cars, smart cities, and personal agents equipped with their own

behavioral algorithms. But every knife cuts two ways. All computers can be hacked. And Internet-connected computers are the most vulnerable. Forget data theft: cutting-edge digital attackers can now crash your car, your pacemaker, and the nation's power grid. In [Click Here to Kill Everybody](#), renowned expert and best-selling author Bruce Schneier examines the hidden risks of this new reality. After exploring the full implications of a world populated by hyperconnected devices, Schneier reveals the hidden web of technical, political, and market forces that underpin the pervasive insecurities of today. He then offers common-sense choices for companies, governments, and individuals that can allow us to enjoy the benefits of this omnipotent age

without falling prey to its vulnerabilities. From principles for a more resilient Internet of Things, to a recipe for sane government regulation and oversight, to a better way to understand a truly new environment, Schneier's vision is required reading for anyone invested in human flourishing.

[Hacking mit Metasploit](#) MITP-Verlags GmbH & Co. KG

Metasploit ist ein Penetration-Testing-Werkzeug, das in der Toolbox eines jeden Pentesters zu finden ist. Dieses Buch stellt das Framework detailliert vor und zeigt, wie Sie es im Rahmen unterschiedlichster Penetrationstests einsetzen. Am Beispiel von Metasploit erhalten Sie einen umfassenden Einblick ins Penetration Testing. Sie lernen typische Pentesting-Tätigkeiten kennen

und können nach der Lektüre komplexe, mehrstufige Angriffe vorbereiten, durchführen und protokollieren. Jeder dargestellte Exploit bzw. jedes dargestellte Modul wird anhand eines praktischen Anwendungsbeispiels in einer gesicherten Laborumgebung vorgeführt. Behandelt werden u.a. folgende Themen: • Komplexe, mehrstufige Penetrationstests • Post-Exploitation-Tätigkeiten • Metasploit-Erweiterungen • Webapplikationen, Datenbanken, Client-Side-Angriffe, IPv6 • Automatisierung mit Ruby-Skripten • Entwicklung eigener Exploits inkl. SEHExploits • Exploits für Embedded Devices entwickeln • Umgehung unterschiedlichster Sicherheitsumgebungen Die dritte Auflage wurde überarbeitet und

aktualisiert. Neu dabei: • Post-Exploitation-Tätigkeiten mit Railgun vereinfachen • Bad-Characters bei der Entwicklung von Exploits berücksichtigen • Den Vulnerable Service Emulator nutzen Vorausgesetzt werden fundierte Kenntnisse der Systemtechnik (Linux und Windows) sowie der Netzwerktechnik.

Ubuntu 22.04 Schnelleinstieg John Wiley & Sons

Learn to think like a hacker to secure your own systems and data Your smartphone, laptop, and desktop computer are more important to your life and business than ever before. On top of making your life easier and more productive, they hold sensitive information that should remain private. Luckily for all of us, anyone can learn

powerful data privacy and security techniques to keep the bad guys on the outside where they belong. **Hacking For Dummies** takes you on an easy-to-follow cybersecurity voyage that will teach you the essentials of vulnerability and penetration testing so that you can find the holes in your network before the bad guys exploit them. You will learn to secure your Wi-Fi networks, lock down your latest Windows 11 installation, understand the security implications of remote work, and much more. You'll find out how to: Stay on top of the latest security weaknesses that could affect your business's security setup Use freely available testing tools to "penetration test" your network's security Use ongoing security checkups to continually ensure that your data is safe from

hackers **Perfect for small business owners, IT and security professionals, and employees who work remotely, Hacking For Dummies is a must-have resource for anyone who wants to keep their data safe.**

Social Engineering No Starch Press

The USB Rubber Ducky is a keystroke injection tool disguised as a generic flash drive. Computers recognize it as a regular keyboard and accept its pre-programmed keystroke payloads at over 1000 words per minute.

Kali Linux Revealed John Wiley & Sons

The first book to reveal and dissect the technical aspect of many social engineering maneuvers From elicitation, pretexting, influence and manipulation all aspects of social engineering are picked apart, discussed and explained

by using real world examples, personal experience and the science behind them to unraveled the mystery in social engineering. Kevin Mitnick—one of the most famous social engineers in the world—popularized the term “social engineering.” He explained that it is much easier to trick someone into revealing a password for a system than to exert the effort of hacking into the system. Mitnick claims that this social engineering tactic was the single-most effective method in his arsenal. This indispensable book examines a variety of maneuvers that are aimed at deceiving unsuspecting victims, while it also addresses ways to prevent social engineering threats. Examines social engineering, the science of influencing a target to perform a desired task or

divulge information Arms you with invaluable information about the many methods of trickery that hackers use in order to gather information with the intent of executing identity theft, fraud, or gaining computer system access Reveals vital steps for preventing social engineering threats Social Engineering: The Art of Human Hacking does its part to prepare you against nefarious hackers—now you can do your part by putting to good use the critical information within its pages.

Eugen Keterling

Just as a professional athlete doesn't show up without a solid game plan, ethical hackers, IT professionals, and security researchers should not be unprepared, either. The Hacker Playbook provides them their own game plans.

Written by a longtime security professional and CEO of Secure Planet, LLC, this step-by-step guide to the "game" of penetration hacking features hands-on examples and helpful advice from the top of the field. Through a series of football-style "plays," this straightforward guide gets to the root of many of the roadblocks people may face while penetration testing—including attacking different types of networks, pivoting through security controls, privilege escalation, and evading antivirus software. From "Pregame" research to "The Drive" and "The Lateral Pass," the practical plays listed can be read in order or referenced as needed. Either way, the valuable advice within will put you in the mindset of a penetration tester of a Fortune 500

company, regardless of your career or level of experience. This second version of The Hacker Playbook takes all the best "plays" from the original book and incorporates the latest attacks, tools, and lessons learned. Double the content compared to its predecessor, this guide further outlines building a lab, walks through test cases for attacks, and provides more customized code. Whether you're downing energy drinks while desperately looking for an exploit, or preparing for an exciting new job in IT security, this guide is an essential part of any ethical hacker's library—so there's no reason not to get in the game.

Learn Kali Linux 2019 John Wiley & Sons

Drahtlose Netzwerke sind heute allgegenwärtig und werden im Zuge von

Entwicklungen wie dem "Smart Home" und dem "Internet of Things" in Zukunft eine noch wichtigere Schlüsselrolle bei der Informationsvermittlung spielen. Folglich steht und fällt die Zuverlässigkeit unserer Infrastruktur nicht zuletzt mit der Sicherheit von WLAN-Technologien. Das Buch vermittelt seinen Leserinnen und Lesern das nötige Wissen, um WLAN-Umgebungen wirksam gegen Angriffe abzusichern. Zahlreiche praxisnahe Beispiele helfen sowohl Anfängern als auch Fortgeschrittenen dabei, verschiedene Angriffsszenarien nachzuvollziehen, um sich effektiv vor Hackern schützen zu können. Vom Auskundschaften einer WLAN-Umgebung bis zur Umgehung von Authentifizierungsverfahren geben die Autoren einen umfassenden Einblick in

alle gängigen Angriffswege auf drahtlose Datenübertragungstechnologien. Rechtliche und gesellschaftliche Aspekte wie Störerhaftung und Freifunk runden das Buch ab und machen es zu einem unverzichtbaren Lern- und Nachschlagewerk für alle, denen die Sicherheit ihrer Funknetze am Herzen liegt.

CompTIA Security+ MITP-Verlags GmbH & Co. KG

Do you want to Be a Hacker?Great! Learn to Hack! Hacking is the best way to learn how not to build things. Programmers master programming languages but often leave traces of code that hackers can master to create backdoors. This book explains hacking in an interesting way that will help you master it easily. Hackers often use Linux

and Kali for their operations. This book explains everything with command line code in layman terms. Often people get misinformation about hacking from websites and blogs. To master hacking, you need to master tools that does the job. This book exactly deals in this way to help you understand the process of hacking. This book explains about the Installation procedures of kali Linux and Linux. A detailed description on Linux commands is given along with many examples that will help us understand the techniques we need to master. Along with a brief introduction of kali Linux, this book will explain us about tools like Nmap an information-gathering tool and Metasploit an exploit creation tool. People often live in workplaces and are surrounded by wireless networks in this

generation. A chapter in this book deals solely about Wireless Hacking with a lot of examples. Below we explain the most exciting parts of the book. Introduction to Linux Operating System Installation of Linux Mint and Kali Linux Installation of Linux Distributions using a virtual machine Introduction to Linux Commands Explaining about hacking tools in Kali Linux Information gathering of the target using Nmap Automatic vulnerability assessment using Nessus Getting introduced to Netcat utility with a lot of examples Notes on using password cracking tools Introduction to John the Ripper Introduction to Snort tool A whole chapter dealing about wireless hacking with a lot of examples Every concept in the book is followed by a command line

code that will help you understand the process of hacking further. Buy this to get a great introduction to hacking and this book is followed by another book ("Hacking with Kali Linux" - ICT SCHOOL) that will further expand your skills. Even if you've never make a hack in your life, you can easily learn how to do it. So what are you waiting for? Scroll up and click BUY NOW button!

Advanced Penetration Testing

Newnes

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.

Einstieg in Kali Linux No Starch Press
Protect your business and family against cyber attacks Cybersecurity is the protection against the unauthorized or criminal use of electronic data and the practice of ensuring the integrity, confidentiality, and availability of information. Being "cyber-secure" means that a person or organization has both protected itself against attacks by cyber criminals and other online scoundrels, and ensured that it has the ability to recover if it is attacked. If keeping your business or your family safe from cybersecurity threats is on your to-do list, Cybersecurity For Dummies will introduce you to the basics of becoming cyber-secure! You'll learn what threats exist, and how to identify, protect against, detect, and respond to these

threats, as well as how to recover if you have been breached! The who and why of cybersecurity threats Basic cybersecurity concepts What to do to be cyber-secure Cybersecurity careers What to think about to stay cybersecure in the future Now is the time to identify vulnerabilities that may make you a victim of cyber-crime — and to defend yourself before it is too late.

The Ultimate Kali Linux Book John Wiley & Sons

- Methoden und Tools der Hacker, Cyberkriminellen und Penetration Tester
- Mit zahlreichen Schritt-für-Schritt-Anleitungen und Praxis-Workshops -
Inklusive Vorbereitung auf den Certified Ethical Hacker (CEHv12) mit
Beispielfragen zum Lernen
Schwachstellen erkennen und

Gegenmaßnahmen durchführen Dies ist ein praxisorientierter Leitfaden für angehende Hacker, Penetration Tester, IT-Systembeauftragte, Sicherheitsspezialisten und interessierte Poweruser. Der Fokus liegt auf der Perspektive des Angreifers und auf den Angriffstechniken, die jeder Penetration Tester kennen muss. Darüber hinaus erläutern die Autoren für alle Angriffe effektive Gegenmaßnahmen. So gibt dieses Buch Ihnen alle Mittel und Informationen an die Hand, um Ihre Systeme auf Herz und Nieren zu prüfen und effektiv vor Angriffen zu schützen. Zahlreiche Praxis-Workshops und Schritt-für-Schritt-Anleitungen Mithilfe vieler Workshops, Schritt-für-Schritt-Anleitungen sowie Tipps und Tricks lernen Sie die Werkzeuge der Hacker

und Penetration Tester sowie die Vorgehensweise eines professionellen Hacking-Angriffs kennen. Sie finden zahlreiche Beispiele, die anhand konkreter Szenarien direkt zum Mitmachen gezeigt werden. So haben Sie die Möglichkeit, die Angriffstechniken selbst zu erleben und zu üben. Prüfungsvorbereitung für die Zertifizierung CEHv12 Sowohl der Inhalt als auch die Methodik orientieren sich an der Zertifizierung zum Certified Ethical Hacker (CEHv12) des EC-Council. Testfragen am Ende jedes Kapitels helfen dabei, das eigene Wissen zu überprüfen und für die CEH-Prüfung zu trainieren. Damit eignet sich das Buch hervorragend als ergänzendes Material zur Prüfungsvorbereitung. Real-World Bug Hunting Hacking mit

MetasploitHacking mit Metasploit
Der Erfolg des E-Commerce hat auch seine Schattenseiten: Hackerangriffe im Web gehören inzwischen zum Alltag. Es geht dabei nicht nur um unsichere Firewalls oder Fehler in Betriebssystemen, häufig stellt die selbst programmierte Webapplikation das größte Einfallstor dar. Um sich vor Hackern zu schützen, ist es wichtig, wie ein Hacker zu denken. In diesem Buch lernen Sie die häufigsten Angriffsmethoden kennen und erhalten Tipps, wie Sie sich dagegen schützen können. Analysieren Sie Ihren Programmcode auf Schwachstellen und schließen Sie die Lücken gleich in der Implementierungsphase. Die wichtigsten Angriffsvektoren Durch die Kombination verschiedenster Technologien wie

Browser, HTML, JavaScript, PHP, Java und SQL in Webanwendungen sind die potenziellen Schwachstellen quasi unzählbar. Ob SQL-Injection, Cross-Site-Scripting oder Session-Hijacking: Lernen Sie die Funktionsweise dieser Angriffe kennen, stellen Sie Ihr Können beim Angreifen der Testumgebung unter Beweis und schützen Sie sich mit den aufgeführten Tipps erfolgreich vor Angriffen. Werkzeuge kennen und nutzen Entwickler sind keine Sicherheitsexperten und können nicht jede Schwachstelle der eingesetzten Programmiersprache und Bibliotheken kennen. Umso wichtiger ist es, die entstandene Webanwendung auf ihre Schwachpunkte zu testen. Schäfers stellt in einem ausführlichen Anhang zahlreiche Werkzeuge vor, mit denen Sie

effektiv nach Schwachstellen suchen können.

WLAN Hacking Penguin

It's no secret that college doesn't prepare students for the real world. Student loan debt recently eclipsed credit card debt for the first time in history and now tops one trillion dollars. And the throngs of unemployed graduates chasing the same jobs makes us wonder whether there's a better way to "make it" in today's marketplace. There is—and Dale Stephens is proof of that. In *Hacking Your Education*, Stephens speaks to a new culture of "hackademics" who think college diplomas are antiquated. Stephens shows how he and dozens of others have hacked their education, and how you can, too. You don't need to be a genius

or especially motivated to succeed outside school. The real requirements are much simpler: curiosity, confidence, and grit. *Hacking Your Education* offers valuable advice to current students as well as those who decided to skip college. Stephens teaches you to create opportunities for yourself and design your curriculum—inside or outside the classroom. Whether your dream is to travel the world, build a startup, or climb the corporate ladder, Stephens proves you can do it now, rather than waiting for life to start after "graduation" day. Security für Data-Warehouse- und Business-Intelligence-Systeme Franzis Verlag

The most comprehensive guide to ethical hacking and penetration testing with Kali Linux, from beginner to

professional 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 Purchase of the print or Kindle book includes a free eBook in the PDF format Book DescriptionKali 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.

Hacking mit Metasploit No Starch Press

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.

Hacking im Web 2.0 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.

Best Sellers - Books :

- [The Four Agreements: A Practical Guide To Personal Freedom \(a Toltec Wisdom Book\) By Don Miguel Ruiz](#)
- [Heart Bones: A Novel](#)
- [The 48 Laws Of Power](#)
- [Are You There God? It's Me, Margaret. By Judy Blume](#)
- [Little Blue Truck's Springtime: An Easter And Springtime Book For Kids By Alice Schertle](#)
- [A Court Of Frost And Starlight \(a Court Of Thorns And Roses, 4\)](#)
- [Can't Hurt Me: Master Your Mind And Defy The Odds By David Goggins](#)
- [It's Not Summer Without You By Jenny Han](#)

- [The Boy, The Mole, The Fox And The Horse By Charlie Mackesy](#)
- [Blowback: A Warning To Save Democracy From The Next Trump](#)