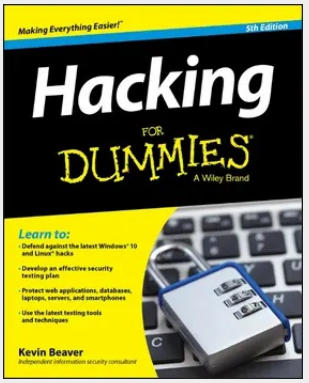
Beaver

Hacking For Dummies



26,90 €
25,14 € (zzgl. MwSt.)

Nicht mehr lieferbar

Learn to hack your own system to protect against malicious attacks from outside Is hacking something left up to the bad guys? Certainly not! Hacking For Dummies, 5th Edition is a fully updated resource that guides you in hacking your system to better protect your network against malicious attacks. This revised text helps you recognize any vulnerabilities that are lurking in your system, allowing you to fix them before someone else finds them. Penetration testing, vulnerability assessments, security best practices, and other aspects of ethical hacking are covered in this book, including Windows 10 hacks, Linux hacks, web application hacks, database hacks, VoIP hacks, and mobile computing hacks. Additionally, you have access to free testing tools and an appendix detailing valuable tools and resources. Ethical hacking entails thinking like the bad guys to identify any vulnerabilities that they might find in your system--and fixing them before they do. Also called penetration testing, ethical hacking is essential to keeping your system, and all of its data, secure. Understanding how to perform effective ethical hacking can improve the safety of your network. * Defend your system--and all of the data it holds--against the latest Windows 10 and Linux hacks * Develop an effective ethical hacking plan that keeps your system safe * Protect your web applications, databases, laptops, and smartphones by going beyond simple hacking strategies * Leverage the latest testing tools and techniques when using ethical hacking to keep your system secure Hacking For Dummies, 5th Edition is a fully updated resource that guides you in hacking your own system to protect it--and it will become your go-to reference when ethical hacking is on your to-do list.

Learn to: * Defend against the latest Windows (r) 10 and Linux(r) hacks * Develop an effective security testing plan * Protect web applications, databases, laptops, servers, and smartphones * Use the latest testing tools and techniques Protect your network against malicious attacks Is hacking something left to the bad guys? Certainly not! If security assessments are on your to-do list, this book helps you identify vulnerabilities in your system and stay on top of the security game. Here's just what you need to defend your network environment-and all of the data it holds-against hacks, including the latest Windows 10 and Linux hacks. * Know your enemy - get in the malicious mindset and discover how to plan your security testing efforts throughout the security assessment process * Put your plan into motion - get familiar with several well-known and widely used hack attacks, like information gathering, social engineering, and cracking passwords * Improve communications - find out how networks are compromised by using specific methods of flawed network communications * Find your flaws - exploit well-known vulnerabilities in Windows, Mac OS X(r), and Linux operating systems, take over operating systems remotely, and implement countermeasures to make your operating systems more secure * App attack - find the latest on hacking messaging systems, web applications, mobile apps, and databases Open the book and find: * The fundamentals of vulnerability assessments and penetration testing * Common weak links in most security programs * How smartphones, tablets, and the Internet of Things can be exploited * Tips and tricks to perform common security tests against your business systems * How to develop reports on the information you gather to get management interested * Guidance on correcting the flaws you find-and how to keep looking for more

Artikelnummer: 9781119154686
Medium: Buch
ISBN: 978-1-119-15468-6
Verlag: Wiley
Erscheinungstermin: 19.01.2016
Sprache(n): Englisch
Auflage: 5. Auflage 2016
Produktform: Kartoniert
Gewicht: 608 g
Seiten: 408
Format (B x H): 188 x 233 mm

Kundenservice Verlag Dr. Otto Schmidt KG
Neumannstraße 10, 40235 Düsseldorf | kundenservice@otto-schmidt.de | 0221-93738-997 (Inland)