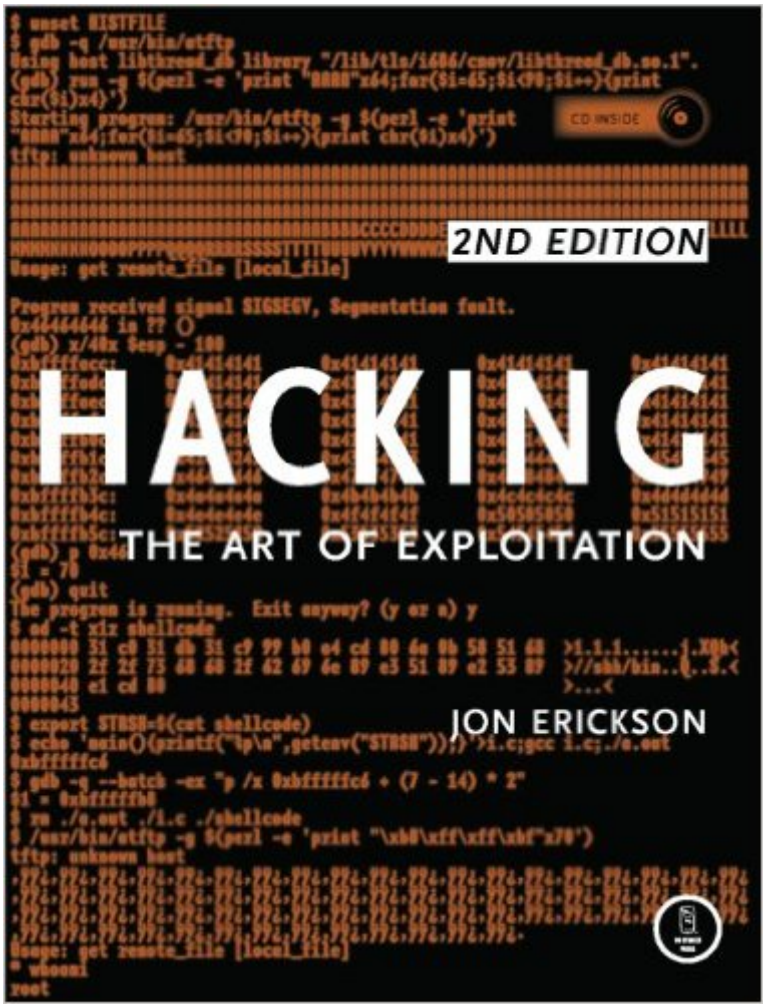
Hacking: The Art Of Exploitation: The Art Of Exploitation



Synopsis

Hacking is the art of creative problem solving, whether that means finding an unconventional solution to a difficult problem or exploiting holes in sloppy programming. Many people call themselves hackers, but few have the strong technical foundation needed to really push the envelope.Rather than merely showing how to run existing exploits, author Jon Erickson explains how arcane hacking techniques actually work. To share the art and science of hacking in a way that is accessible to everyone, Hacking: The Art of Exploitation, 2nd Edition introduces the fundamentals of C programming from a hacker's perspective. Use it to follow along with the book's examples as you fill gaps in your knowledge and explore hacking techniques on your own. Get your hands dirty debugging code, overflowing buffers, hijacking network communications, bypassing protections, exploiting cryptographic weaknesses, and perhaps even inventing new exploits. This book will teach you how to:Program computers using C, assembly language, and shell scripts Corrupt system memory to run arbitrary code using buffer overflows and format strings Inspect processor registers and system memory with a debugger to gain a real understanding of what is happening Outsmart common security measures like nonexecutable stacks and intrusion detection systems Gain access to a remote server using port-binding or connect-back shellcode, and alter a server's logging behavior to hide your presenceRedirect network traffic, conceal open ports, and hijack TCP connections Crack encrypted wireless traffic using the FMS attack, and speed up brute-force attacks using a password probability matrix Hackers are always pushing the boundaries, investigating the unknown, and evolving their art. Even if you don't already know how to program, Hacking: The Art of Exploitation, 2nd Edition will give you a complete picture of programming, machine architecture, network communications, and existing hacking techniques. Combine this knowledge with the accompanying Linux environment, and all you need is your own creativity.

Book Information

File Size: 1318 KB
Print Length: 488 pages
Simultaneous Device Usage: Unlimited
Publisher: No Starch Press; 2 edition (January 28, 2008)
Publication Date: August 12, 2010
Sold by:Â Digital Services LLC
Language: English
ASIN: B004OEJN3I

Text-to-Speech: Enabled

X-Ray: Enabled

Word Wise: Not Enabled

Lending: Not Enabled

Enhanced Typesetting: Not Enabled

Best Sellers Rank: #33,217 Paid in Kindle Store (See Top 100 Paid in Kindle Store) #33 inÂ Books > Computers & Technology > Internet & Social Media > Hacking #45 inÂ Kindle Store > Kindle eBooks > Computers & Technology > Programming #78 inÂ Books > Computers & Technology > Security & Encryption

Customer Reviews

ContentsThis is the second edition of a well known book about hacking and contains a lot about hacking. Jon Erickson has expanded the book from the first edition doubling the number of pages to 450 pages and a Linux based Live-CD is also included.I don’t own the first edition, since I had to choose between Hacking by Jon Erickson and The Shellcoders Handbook (first edition, it is also in 2nd ed. now). I choose the Shellcoders handbook, which I have considered my bible for buffer overflows and hacking.Now that I have read Jon Ericksons book about hacking I have two bibles, both excellent and well written, both covering some of the same stuff - but in very different ways.This book details the steps done to perform buffer overflows on Linux on the x86 architecture. So detailed that any computer science student can do it, and they should. Every computer science student or aspiring programmer should be forced to read this book along with another book called 19 deadly sins of software programming.That alone would improve internet security and program reliability in the future. Why you may ask, because this book teaches hacking, and how you can get started hacking.Not hacking as doing criminal computer break ins, but thinking like an old-school hacker - doing clever stuff, seeing the things others don’t. This book contains the missing link back to the old days, where hackers were not necessarily bad guys. Unfortunately today the term hacker IS dead in the public eye, it HAS been maimed, mutilated and the war about changing it back to the old meaning is over. (Actually this war was fought in the 1990’s but some youngsters new to hacking still think it can be won, don’t waste your time.

This is the last in a recent collection of reviews on "hacking" books. Jon Erickson’s Hacking, 2nd Ed (H2E) is one of the most remarkable books in the group I just read. H2E is in some senses amazing because the author takes the reader on a journey through programming, exploitation, shellcode,

and so forth, yet helps the reader climb each mountain. While the material is sufficiently technical to scare some readers away, those that remain will definitely learn more about the craft.H2E accomplishes a very difficult task. The book strives to take readers with little to no real "hacking" knowledge to a level where they can at least understand, if not perform, fairly complicated digital security tasks. Other books aren't as successful, e.g., "Gray Hat Hacking," which features material on C, assembly, Python, etc. into one short chapter. In contrast, H2E, in my opinion, does a credible job leading the reader from pseudo-code to C and assembly. Now, I would not recommend this book as a reader's sole introduction to programming, let alone C or assembly. Please see my older reviews for recommendations on books devoted to those topics. Still, H2E credibly integrates programming into the hacker narrative in a compelling and educational manner.The author also has a great eye for consistency and style. I welcomed reading his examples using gdb, where he presented code, explained it, stepped through execution, showed memory, transitioned from displaying source, then assembly, and so on. This was a compelling teaching method that technical authors should try to emulate.Overall I really liked H2E, hence the 5 star review. My only main gripe was the author seems to believe that it's in society's benefit for black hats to test and exploit defenses.

(Hacking Freedom and Data Driven Book 2) Hacking: The Beginners Guide to Master The Art of Hacking In No Time - Become a Hacking GENIUS HACKING: Beginner's Crash Course - Essential Guide to Practical: Computer Hacking, Hacking for Beginners, & Penetration Testing (Computer Systems, Computer Programming, Computer Science Book 1) Hacking: How to Computer Hack: An Ultimate Beginner's Guide to Hacking (Programming, Penetration Testing, Network Security) (Cyber Hacking with Virus, Malware and Trojan Testing) Wireless Hacking: How To Hack Wireless Network (How to Hack, Wireless Hacking, Penetration Testing, Social ... Security, Computer Hacking, Kali Linux) C++: C++ and Hacking for dummies. A smart way to learn C plus plus and beginners guide to computer hacking (C++ programming, C++ for Beginners, hacking, ... language, coding, web developing Book 2) Hacking: Tapping into the Matrix Tips, Secrets, steps, hints, and hidden traps to hacking: Hacker, Computer, Programming, Security & Encryption Hacking: Beginner to Expert Guide to Computer Hacking, Basic Security, and Penetration Testing (Computer Science Series) Hacking: Hacking Made Easy 1: Beginners: Python: Python Programming For Beginners, Computer Science, Computer Programming Hacking: Basic Security, Penetration Testing and How to Hack (hacking, how to hack, penetration testing, basic security, arduino, python, engineering) Hacking: Computer Hacking for beginners, how to hack, and understanding computer security!