

## Larte Dellhacking

L'ebook che non si limita a mostrare come funzionano le tecniche di exploit, ma spiega come svilupparle, ritorna in due ebook. Jon Erickson guida il lettore in un percorso di iniziazione alle tecniche hacker. Ancora una volta il presupposto è che conoscere i metodi, le logiche, la teoria e i fondamenti scientifici che stanno alla base dell'hacking stesso, rappresenta l'unica via per costruire sistemi sicuri. Se la prima edizione di questo libro, pubblicata sul finire del 2003 e tradotta in undici lingue, aveva ottenuto vasti consensi confermati da ampie vendite, la seconda, ora disponibile in formato EPUB, porta la conoscenza delle tecniche dell'hacking a un nuovo livello. Volume 1: argomenti in breve- Introduzione all'hacking- Programmazione in C e Assembly- Tecniche di exploit- Vulnerabilità buffer overflow- Exploit da stringa di formato- Introduzione alle reti: modello OSI e socket- Sniffing di rete

Sebbene le reti senza fili (wireless) promettano, e permettano oggi, di portare l'uso e l'esperienza di Internet sempre più vicina alle persone, muovere i primi passi in questo mondo non è semplice, soprattutto per i non addetti ai lavori. Ecco lo scopo e il senso di questo libro: insegnare come servirsi con profitto di una soluzione di rete senza fili. Che si tratti di una rete domestica (abitazione o ufficio) o di una rete pubblica, i problemi sono sempre gli stessi: funzionalità e sicurezza. La configurazione e la messa in sicurezza, la scelta dell'hardware e del software, ma anche del provider, gli standard delle reti wireless e i costi di connessione: tutto questo viene affrontato e discusso capitolo dopo capitolo, per soddisfare le esigenze di ogni tipo di utente, da Windows a Linux, senza dimenticare Mac e i telefoni cellulari di ultima generazione.

In this "intriguing, insightful and extremely educational" novel, the world's most famous hacker teaches you easy cloaking and counter-measures for citizens and consumers in the age of Big Brother and Big Data (Frank W. Abagnale). Kevin Mitnick was the most elusive computer break-in artist in history. He accessed computers and networks at the world's biggest companies -- and no matter how fast the authorities were, Mitnick was faster, sprinting through phone switches, computer systems, and cellular networks. As the FBI's net finally began to tighten, Mitnick went on the run, engaging in an increasingly sophisticated game of hide-and-seek that escalated through false identities, a host of cities, and plenty of close shaves, to an ultimate showdown with the Feds, who would stop at nothing to bring him down. Ghost in the Wires is a thrilling true story of intrigue, suspense, and unbelievable escapes -- and a portrait of a visionary who forced the authorities to rethink the way they pursued him, and forced companies to rethink the way they protect their most sensitive information. "Mitnick manages to make breaking computer code sound as action-packed as robbing a bank." -- NPR

L'ebook che non si limita a mostrare come funzionano le tecniche di exploit, ma spiega come svilupparle, ritorna in due ebook. Jon Erickson guida il lettore in un

percorso di iniziazione alle tecniche hacker. Ancora una volta il presupposto è che conoscere i metodi, le logiche, la teoria e i fondamenti scientifici che stanno alla base dell'hacking stesso, rappresenta l'unica via per costruire sistemi sicuri. Se la prima edizione di questo libro, pubblicata sul finire del 2003 e tradotta in undici lingue, aveva ottenuto vasti consensi confermati da ampie vendite, la seconda, ora disponibile in formato EPUB, porta la conoscenza delle tecniche dell'hacking a un nuovo livello. Volume 2: argomenti in breve- Attacchi DoS (Denial of Service)- Dirottamento TCP/IP- Scansione di porte- Programmi shellcode- Crittografia e crittoanalisi- Violazione di sistemi cifrati- Cracking di password- Attacchi e contromisure

"If I had this book 10 years ago, the FBI would never have found me!" -- Kevin Mitnick This book has something for everyone---from the beginner hobbyist with no electronics or coding experience to the self-proclaimed "gadget geek." Take an ordinary piece of equipment and turn it into a personal work of art. Build upon an existing idea to create something better. Have fun while voiding your warranty! Some of the hardware hacks in this book include: \* Don't toss your iPod away when the battery dies! Don't pay Apple the \$99 to replace it! Install a new iPod battery yourself without Apple's "help" \* An Apple a day! Modify a standard Apple USB Mouse into a glowing UFO Mouse or build a FireWire terabyte hard drive and custom case \* Have you played Atari today? Create an arcade-style Atari 5200 paddle controller for your favorite retro videogames or transform the Atari 2600 joystick into one that can be used by left-handed players \* Modern game systems, too! Hack your PlayStation 2 to boot code from the memory card or modify your PlayStation 2 for homebrew game development \* Videophiles unite! Design, build, and configure your own Windows- or Linux-based Home Theater PC \* Ride the airwaves! Modify a wireless PCMCIA NIC to include an external antenna connector or load Linux onto your Access Point \* Stick it to The Man! Remove the proprietary barcode encoding from your CueCat and turn it into a regular barcode reader \* Hack your Palm! Upgrade the available RAM on your Palm m505 from 8MB to 16MB · Includes hacks of today's most popular gaming systems like Xbox and PS/2. · Teaches readers to unlock the full entertainment potential of their desktop PC. · Frees iMac owners to enhance the features they love and get rid of the ones they hate.

L'arte dell'hacking. Le idee, gli strumenti, le tecniche degli hacker Apogeo Editore L'arte dell'hacking. Con CD-ROM Apogeo Editore L'arte dell'hacking - Apogeo Editore

A text for high school and general readers on the natural and human-made forces that influence the shape of the planet. Topics include arctic, desert, and coastal geography; the formation of continents; erosion; tectonic processes; and mountain ranges, river courses, and unique landforms such as monoliths and arches. Erickson, a geologist in Colorado, is the author of several Facts on Files books on Earth science and geology.

Describes the techniques of computer hacking, covering such topics as stack-based overflows, format string exploits, and shellcode.

Praise for the previous edition: ...refreshingly clear...will entertain the reader with the wonders of the rock world, and will enhance an understanding of the natural environment... Recommended for all audiences, from high school upward. -- CHOICE Clearly written and illustrated

Real-world advice on how to be invisible online from "the FBI's most-wanted hacker" (Wired) Your every step online is being tracked and stored, and your identity easily stolen. Big companies and big governments want to know and exploit what you do, and privacy is a luxury few can afford or understand. In this explosive yet practical book, computer-security expert Kevin Mitnick uses true-life stories to show exactly what is

happening without your knowledge, and teaches you "the art of invisibility": online and everyday tactics to protect you and your family, using easy step-by-step instructions. Reading this book, you will learn everything from password protection and smart Wi-Fi usage to advanced techniques designed to maximize your anonymity. Invisibility isn't just for superheroes--privacy is a power you deserve and need in the age of Big Brother and Big Data.

Vi siete mai domandati cosa succede nel momento esatto in cui cominciate a premere i tasti del computer? Sapete cosa accade all'interno di un PC prima che un carattere venga visualizzato sullo schermo? In quel momento siete già esposti ai pericoli degli attacchi informatici...Il rumore dell'hacking è un ebook sulla sicurezza informatica. Ma non è l'ennesimo testo sulla sicurezza informatica. Questo libro parla di hacker e hacking da una prospettiva diversa. Oggetto della trattazione non sono tanto concetti tecnici, che pur non mancano, quanto il giusto approccio metodologico, conoscitivo prima che pratico, ai problemi di sicurezza. L'autore vuole far acquisire prima di tutto la sensibilità ai pericoli della Rete, requisito fondamentale affinché una possibile minaccia sia riconosciuta come tale e le tecniche di difesa siano conseguentemente attivate. Per fare questo tratteggia una panoramica dei percorsi dell'informazione sulle silenziose strade della Rete, nella quale concetti di sicurezza, formule matematiche, elementi di elettronica si succedono a un ritmo serrato, avvincente, che caratterizza il libro più come un racconto tecnologico che come un manuale di informatica. Michal Zalewski si augura che i suoi lettori possano dormire sonni tranquilli, perché per un momento sono riusciti a entrare in sintonia con il silenzio della Rete, riconoscendo in sottofondo il rumore dell'hacking?

This text introduces the spirit and theory of hacking as well as the science behind it all; it also provides some core techniques and tricks of hacking so you can think like a hacker, write your own hacks or thwart potential system attacks.

La storia di un genio eccentrico del software, a partire dalle sue esperienze scolastiche e universitarie, fino alle battaglie combattute contro le grandi corporation. Idealista e rivoluzionario, Stallman ha dato il via al movimento free software che sta scuotendo le fondamenta di tutto il mercato informatico, rappresentando un inevitabile punto di confronto per colossi come Microsoft. Secondo Stallman, il prodotto dell'ingegno deve restare libero: il codice sorgente di qualunque programma rappresenta un bene comune e, proteggerlo con brevetti e copyright, andrebbe considerato un crimine contro l'umanità. Un saggio illuminante che, dipingendo il ritratto di una delle figure più importanti nella storia dell'informatica, mostra i retroscena di una battaglia occulta tra il movimento per il software libero e i grandi interessi commerciali. Per tutti coloro che vogliono capire come funziona il mercato del software nel mondo, come si è arrivati alla situazione attuale e quali sono le possibilità che ci riserva il futuro.

Hacker extraordinaire Kevin Mitnick delivers the explosive encore to his bestselling *The Art of Deception*. Kevin Mitnick, the world's most celebrated hacker, now devotes his life to helping businesses and governments combat data thieves, cybervandals, and other malicious computer intruders. In his bestselling *The Art of Deception*, Mitnick presented fictionalized case studies that illustrated how savvy computer crackers use "social engineering" to compromise even the most technically secure computer systems. Now, in his new book, Mitnick goes one step further, offering hair-raising stories of real-life computer break-ins-and showing how the victims could have prevented them. Mitnick's reputation within the hacker community gave him unique credibility with the perpetrators of these crimes, who freely shared their stories with him-and whose exploits Mitnick now reveals in detail for the first time, including: A group of friends

who won nearly a million dollars in Las Vegas by reverse-engineering slot machines Two teenagers who were persuaded by terrorists to hack into the Lockheed Martin computer systems Two convicts who joined forces to become hackers inside a Texas prison A "Robin Hood" hacker who penetrated the computer systems of many prominent companies-and then told them how he gained access With riveting "you are there" descriptions of real computer break-ins, indispensable tips on countermeasures security professionals need to implement now, and Mitnick's own acerbic commentary on the crimes he describes, this book is sure to reach a wide audience-and attract the attention of both law enforcement agencies and the media.

Examines the effects of population growth on the environment, discussing global pollution, resource depletion, and habitat destruction and their impact on the earth's natural cycles. Disasters happen. Be prepared. Here's how. As a leading security engineer, Michal Zalewski has spent his career methodically anticipating and planning for cyberattacks. In *Practical Doomsday*, Zalewski applies the same thoughtful, rational approach to preparing for disasters of all kinds. By sharing his research, advice, and a healthy dose of common sense, he'll help you rest easy knowing you have a plan for the worst—even if the worst never comes. The book outlines a level-headed model for evaluating risks, one that weighs the probability of scenarios against the cost of preparing for them. You'll learn to apply that model to the whole spectrum of potential crises, from personal hardships like job loss or a kitchen fire, to large-scale natural disasters and industrial accidents, to recurring pop-culture fears like all-out nuclear war. You'll then explore how basic lifestyle adjustments, such as maintaining a robust rainy-day fund, protecting yourself online, and fostering good relationships with your neighbors, can boost your readiness for a wide range of situations. You'll also take a no-nonsense look at the supplies and equipment essential to surviving sudden catastrophes, like prolonged power outages or devastating storms, and examine the merits and legal implications of different self-defense strategies. You'll learn:

- How to identify and meaningfully assess risks in your life, then develop strategies for managing them
- Ways to build up and diversify a robust financial safety net—a key component of nearly all effective preparedness strategies
- How to adapt your prep plans to a variety of situations, from shelter-in-place scenarios to evacuations by car or on foot
- Sensible approaches to stockpiling food, water, and other essentials, along with recommendations on what supplies are actually worth having

Disasters happen, but they don't have to dominate your life. *Practical Doomsday* will help you plan ahead, so you can stop worrying about what tomorrow may bring and start enjoying your life today.

Networking means to create nets of relations, where the publisher and the reader, the artist and the audience, act on the same level. The book is a first tentative reconstruction of the history of artistic networking in Italy, through an analysis of media and art projects which during the past twenty years have given way to a creative, shared and aware use of technologies, from video to computers, contributing to the creation of Italian hacker communities. The Italian network proposes a form of critical information, disseminated through independent and collective projects where the idea of freedom of expression is a central theme. In Italy, thanks to the alternative use of Internet, during the past twenty years a vast national network of people who share political, cultural and artistic views has been formed. The book describes the evolution of the Italian hacktivism and net culture from the 1980s till today. It builds a reflection on the new role of the artist and author who becomes a networker, operating in collective nets, reconnecting to Neoavant-garde practices of the 1960s (first and

foremost Fluxus), but also Mail Art, Neoism and Luther Blissett. A path which began in BBSes, alternative web platforms spread in Italy through the 1980s even before the Internet even existed, and then moved on to Hackmeetings, to Telestreet and networking art by different artists such as 0100101110101101.ORG, [epidemiC], Jaromil, Giacomo Verde, Giovanotti Mondani Meccanici, Correnti Magnetiche, Candida TV, Tommaso Tozzi, Federico Bucalossi, Massimo Contrasto, Mariano Equizzi, Pigreca, Molleindustria, Guerriglia Marketing, Sexyshock, Phag Off and many others. The world's most infamous hacker offers an insider's view of the low-tech threats to high-tech security Kevin Mitnick's exploits as a cyber-desperado and fugitive form one of the most exhaustive FBI manhunts in history and have spawned dozens of articles, books, films, and documentaries. Since his release from federal prison, in 1998, Mitnick has turned his life around and established himself as one of the most sought-after computer security experts worldwide. Now, in *The Art of Deception*, the world's most notorious hacker gives new meaning to the old adage, "It takes a thief to catch a thief." Focusing on the human factors involved with information security, Mitnick explains why all the firewalls and encryption protocols in the world will never be enough to stop a savvy grifter intent on rifling a corporate database or an irate employee determined to crash a system. With the help of many fascinating true stories of successful attacks on business and government, he illustrates just how susceptible even the most locked-down information systems are to a slick con artist impersonating an IRS agent. Narrating from the points of view of both the attacker and the victims, he explains why each attack was so successful and how it could have been prevented in an engaging and highly readable style reminiscent of a true-crime novel. And, perhaps most importantly, Mitnick offers advice for preventing these types of social engineering hacks through security protocols, training programs, and manuals that address the human element of security.

Johnny Long's last book sold 12,000 units worldwide. Kevin Mitnick's last book sold 40,000 units in North America. As the cliché goes, information is power. In this age of technology, an increasing majority of the world's information is stored electronically. It makes sense then that we rely on high-tech electronic protection systems to guard that information. As professional hackers, Johnny Long and Kevin Mitnick get paid to uncover weaknesses in those systems and exploit them. Whether breaking into buildings or slipping past industrial-grade firewalls, their goal has always been the same: extract the information using any means necessary. After hundreds of jobs, they have discovered the secrets to bypassing every conceivable high-tech security system. This book reveals those secrets; as the title suggests, it has nothing to do with high technology. • Dumpster Diving Be a good sport and don't read the two "D" words written in big bold letters above, and act surprised when I tell you hackers can accomplish this without relying on a single bit of technology (punny). • Tailgating Hackers and ninja both like wearing black, and they do share the ability to slip inside a building and blend

with the shadows. • **Shoulder Surfing** If you like having a screen on your laptop so you can see what you're working on, don't read this chapter. • **Physical Security Locks** are serious business and lock technicians are true engineers, most backed with years of hands-on experience. But what happens when you take the age-old respected profession of the locksmith and sprinkle it with hacker ingenuity? • **Social Engineering with Jack Wiles** Jack has trained hundreds of federal agents, corporate attorneys, CEOs and internal auditors on computer crime and security-related topics. His unforgettable presentations are filled with three decades of personal "war stories" from the trenches of Information Security and Physical Security. • **Google Hacking** A hacker doesn't even need his own computer to do the necessary research. If he can make it to a public library, Kinko's or Internet cafe, he can use Google to process all that data into something useful. • **P2P Hacking** Let's assume a guy has no budget, no commercial hacking software, no support from organized crime and no fancy gear. With all those restrictions, is this guy still a threat to you? Have a look at this chapter and judge for yourself. • **People Watching** Skilled people watchers can learn a whole lot in just a few quick glances. In this chapter we'll take a look at a few examples of the types of things that draws a no-tech hacker's eye. • **Kiosks** What happens when a kiosk is more than a kiosk? What happens when the kiosk holds airline passenger information? What if the kiosk holds confidential patient information? What if the kiosk holds cash? • **Vehicle Surveillance** Most people don't realize that some of the most thrilling vehicular espionage happens when the cars aren't moving at all!

[Copyright: e1b3bf38623b745e52f43eb99ea60c77](http://e1b3bf38623b745e52f43eb99ea60c77)