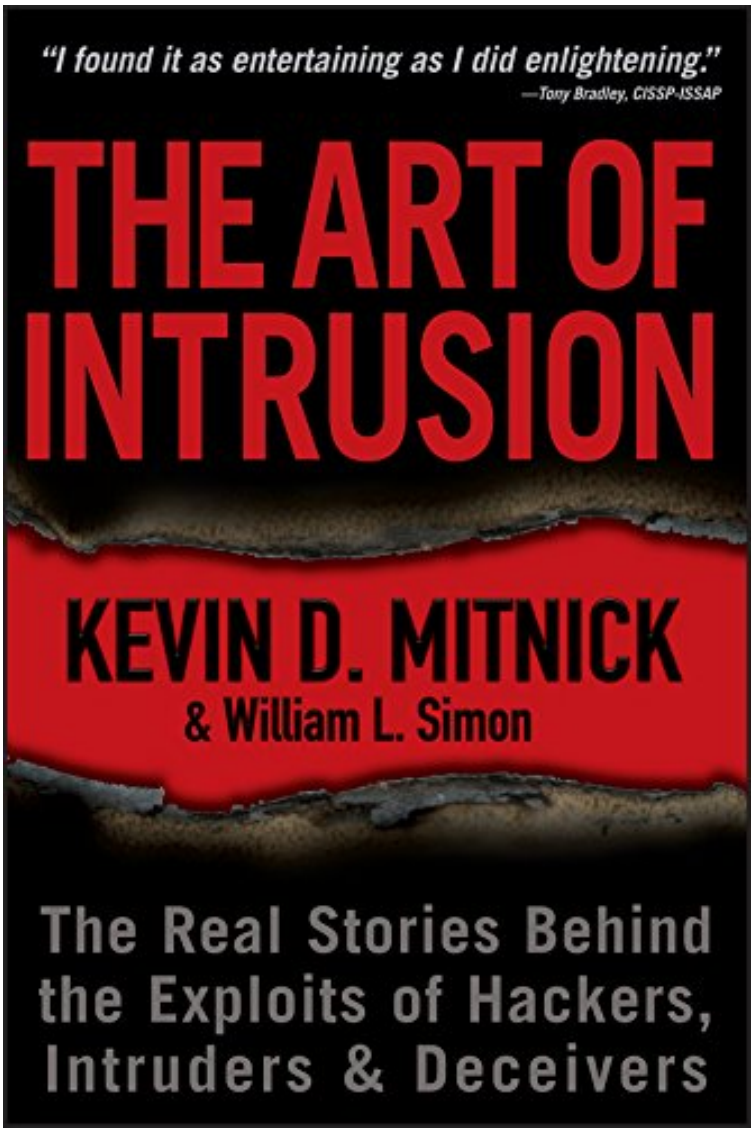
The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders and Deceivers

Von William L. Simon, Kevin D. Mitnick
*audiobook | *ebooks | Download PDF | ePub | DOC*



Produktinformation -Verkaufsrang: #308978 in eBooksVerffentlicht am: 2009-03-17Erscheinungsdatum: 2009-03-17File Name: B000S1M0DG | File size: 23.Mb

Von William L. Simon, Kevin D. Mitnick : The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders and Deceivers before purchasing it in order to gage whether or not it would be worth my time, and all praised The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders and Deceivers:

KundenrezensionenHilfreichste Kundenrezensionen1 von 1 Kunden fanden die folgende Rezension hilfreich. Ramblings of an aging computer buff well out of the game.Von Dave WilfordAfter the exhilerating and insightful

experience of reading 'Kingpin' I thought this would give me more insight. Not so, unfortunately.The story writeups are ok, a good cybercrime story is a good cybercrime story after all, even if it appears to have been written down by a teenager or a highschool dropout (wait a minute...). The book is full of typos and dropped words, it's very inconsistent in its explanations (typically, the more mundane, the more likely it is to be explained... RAS? Reverse DNS lookup? come on.). The authors also can't seem to be able to decide whether they want to just tell the story themselves or quote the perpetrators about it, in both cases it comes out very tedious reading.The bottom line is I can't help but feel that Mitnick is old now and well out of the game. He could teach my mom something about cyber security with this book but anybody under 50 will be left wondering where the meat is.Similarly, his view of "hackers" seems anachronistic and thus very romanticized, the only really bad thing he can say about "them" is that "they" are often childish and foolish and don't realize or care about the potential damage they may be causing. This illustrates how he keeps talking about "a hacker" in a sort of sociological way rather than purely empirically. Surely he must realize that there is not "a hacker" like there is "a plumber" or "a mason", and yet he keeps talking about "them" like it's some sort of homogenous demographic. He seems to feel all these people are hackers first and foremost, and then sometimes stray from the path of virtue to some degree ot other. Criminals that do some hacking as well appear as aberrations, impostors or intruders into his round table of 'true' hackers that "perform a valuable service" (Sic! Seriously. I'm quoting.).His whole view of "the Hackers" as a sort of underground 'Community' with certain universal personality traits and motives is extremely naive and very 1998. It doesn't cover but the most innoctuous of cybercrimes and cybercriminals, i.e. the ones that hardly deserve the title. It's like someone doing a writeup on the drug trade based on a 1971 view of the problem.Finally, a particularly painful part of the book is the so-called "insight", that ranges from the trivial to the plain ridiculous. To share one quote, under the title "THE BOTTOM LINE":"Let's wake up, people. Changing default settings and using strong passwords might stop your business from being victimized."At least he didn't use any exclamation marks. That's some shocking insight halfway through this book. Others include tips like glueing your ICs to the PCB if you're a slot machine manufacturer and regularly changing your passwords (I hope I'm not giving anything away here).Finally, yes, as mentioned elsewhere, he does have the annoying habit of trying to refer everything to himself. Every single story includes at least one, sometimes many, passages along the lines of "that reminded me a lot of how I, back when I was the greatest hacker of all times,..." or how he inspired this or that guy to take up hacking. I'll just share another quote:"[...] their son got involved in hacking because hae had several facvorite hackers who inspired him. It wasn't mentioned, but I get the impression from Adrian that one of those individuals might have been me."And that was on the one "Hacker" that wasn't directly quoted saying that Mitnick was a great inspiration to them.Overall, the book is like the script from a lengthy speech by Mitnick on the topic, and 'live' you would forgive him its shortcomings. As a book it's safe to say it's pretty bad and should at least be priced at half of what it currently is. This is a light $5 read for the porch or the subway commute. If you feel you're learning a lot from this, good for you, but you should give that some thought.Finally, if you want useful facts and insight - on the how, the why, the 'scene' and the perpetrators, get 'Kingpin'.1 von 1 Kunden fanden die folgende Rezension hilfreich. extrem spannend, die Hexenjagd auf den ersten Hacker!Von Hella WahnsinnExtrem spannend geschrieben und eine sehr interessante Geschichte, ber den ersten, berhmtesten und aufsssigsten Hacker der USA, der nie wirklich was gestohlen hat, sondern eher die Herausforderung gesucht hat, in Systeme einzubrechen und sich auch nie persnlich bereichert hat,a ber dafr von geltungsschtigen Journalisten und Polizisten gejagt und fr 5 Jahre ins Gefngnis verfrachtet wurde. Eine Geschichte, sie sie wohl nur in den USA passieren kann, hat etwas von einem Outlaw an sich, der Kevin Mitnick! Sehr empfehlenswert und das Englisch ist so gehalten, dass man (frau) es verstehen kann!0 von 0 Kunden fanden die folgende Rezension hilfreich. Makes you realise how insecure a lot of computers areVon Mark O'NeillThis author was recommended to me by a geek friend and after I did some research on Mitnick, I realised this was a guy I wanted to read. I was a bit amazed to read all the reviews who accused Mitnick of putting his ego all over the book. I didn't see any evidence of that at all. Yes he talks quite a bit about his own experiences in relation to what he is talking about in that chapter but that is to be expected. After all, he IS a convicted computer hacker! So he does have some knowledge in this area! Is this egotism? I don't think so. He is just giving us the benefit of his own experiences.Where this book slightly falls down is that Mitnick makes it WAY too complicated and technical for people like me who are not that techie and geeky. So he talks about computer languages and hacking procedures that are just way too complicated to follow. So if you are not fluent in the lingo, you'll find yourself page flipping. This book is ideally for geeks and nerds who talk computer languages that normal people wouldn't even begin to comprehend! Not me unfortunately.Nevertheless, this is a fascinating insight into the world of hacking and it is also frightening - it makes you realise how insecure a lot of computer systems are all over the world and how a teenager with a PC can easily gain access. Remember that the next time you're entering your password into your online banking.

KurzbeschreibungHacker 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-andthen 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.Pressestimmen"...a valuable investment..." (AccountingWeb UK, 30th August 2005)"...he retells stories provided by his other hackers of how they managed, often with pitiful ease, to break supposedly secure companies all over the world." (Director, May 2005)"...a compilation of real hacking stories told to Mitnick by fellow hackers..." (VNUnet.com, March 2005)It would be difficult to find an author with more credibility than Mitnick to write about the art of hacking. In 1995, he was arrested for illegal computer snooping, convicted and held without bail for two years before being released in 2002. He clearly inspires unusual fear in the authorities and unusual dedication in the legions of computer security dabblers, legal and otherwise. Renowned for his use of "social engineering," the art of tricking people into revealing secure information such as passwords, Mitnick (The Art of Deception) introduces readers to a fascinating array of pseudonymous hackers. One group of friends bilks Las Vegas casinos out of more than a million dollars by mastering the patterns inherent in slot machines; another fellow, less fortunate, gets mixed up with a presumed al-Qaeda-style terrorist; and a prison convict leverages his computer skills to communicate with the outside world, unbeknownst to his keepers. Mitnick's handling of these engrossing tales is exemplary, for which credit presumably goes to his coauthor, writing pro Simon. Given the complexity (some would say obscurity) of the material, the authors avoid the pitfall of drowning readers in minutiae. Uniformly readable, the stories--some are quite exciting--will impart familiar lessons to security pros while introducing lay readers to an enthralling field of inquiry. Agent, David Fugate. (Mar.) (Publishers Weekly, February 14, 2005)Infamous criminal hacker turned computer security consultant Mitnick offers an expert sequel to his best-selling The Art of Deception, this time supplying real-life rather than fictionalized stories of contemporary hackers sneaking into corporate servers worldwide. Each chapter begins with a computer crime story that reads like a suspense novel; it is a little unnerving to learn how one's bank account is vulnerable to digital thieves or how hackers with an interest in gambling can rake in thousands of dollars in just minutes at a compromised slot machine. The hack revealed, Mitnick then walks readers step by step through a prevention method. Much like Deception, this book illustrates that hacking techniques can penetrate corporate and government systems protected by state-of-the-art security.Mitnick's engaging writing style combines intrigue, entertainment, and education. As with Deception, information technology professionals can learn how to detect and prevent security breaches, while informed readers can sit back and enjoy the stories of cybercrime. Recommended for most public and academic libraries. --Joe Accardi, William Rainey Harper Coll. Lib., Palatine, IL (Library Journal, January 15, 2005)"...a compilation of real hacking stories told to Mitnick by fellow hackers..." (VNUnet.com, March 2005)"Uniformly readable, some quite exciting...will impart familiar lessons to security pros while introducing lay readers to an enthralling field of inquiry." (Publishers Weekly, February 14, 2005)"...engaging writing style combines intrigue, entertainment, and education". (Library Journal, January 15, 2005)KurzbeschreibungHacker 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-andthen 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.