

---

## Hacking Exposed 7 Network Security Secrets Pdf

### BOOK DETAIL

Amazon Business : For business-only pricing, quantity discounts and FREE Shipping. Register a free business account Series: Hacking Exposed Paperback: 768 pages Publisher: McGraw-Hill Education; 7 edition (August 1, 2012) Language: English ISBN-10: 0071780289 ISBN-13: 978-0071780285 Product Dimensions: 7.4 x 1.5 x 9.1 inches

### Book Description

Publisher's Note: Products purchased from Third Party sellers are not guaranteed by the publisher for quality, authenticity, or access to any online entitlements included with the product. The latest tactics for thwarting digital attacks "Our new reality is zero-day, APT, and state-sponsored attacks. Today, more than ever, security professionals need to get into the hacker's mind, methods, and toolbox to successfully deter such relentless assaults. This edition brings readers abreast with the latest attack vectors and arms them for these continually evolving threats." --Brett Wahlin, CSO, Sony Network Entertainment "Stop taking punches--let's change the game; it's time for a paradigm shift in the way we secure our networks, and Hacking Exposed 7 is the playbook for bringing pain to our adversaries." --Shawn Henry, former Executive Assistant Director, FBI Bolster your system's security and defeat the tools and tactics of cyber-criminals with expert advice and defense strategies from the world-renowned Hacking Exposed team. Case studies expose the hacker's latest devious methods and illustrate field-tested remedies. Find out how to block infrastructure hacks, minimize advanced persistent threats, neutralize malicious code, secure web and database applications, and fortify UNIX networks. Hacking Exposed 7: Network Security Secrets & Solutions contains all-new visual maps and a comprehensive "countermeasures cookbook." Obstruct APTs and web-based meta-exploits Defend against UNIX-based root access and buffer overflow hacks Block SQL injection, spear phishing, and embedded-code attacks Detect and terminate rootkits, Trojans, bots, worms, and malware Lock down remote access using smartcards and hardware tokens Protect 802.11 WLANs with multilayered encryption and gateways Plug holes in VoIP, social networking, cloud, and Web 2.0 services Learn about the latest iPhone and Android attacks and how to protect yourself

**DOWNLOAD:** <https://tinurli.com/2ilzme>



View the complete transcript: Rob: Hello, my name is Rob Wietfeldt and welcome to the Fluke Hacking Exposed. I'm really excited to have Stuart McClure on today. He is a senior vice president at Fluke Networks and he is a well-respected expert in the field of security. He has published many of the best books on hacking as a software engineer and author. Rob: He is also the coauthor of Hacking Exposed with many of the professionals who are currently in the field of penetration testing and cyber

---

security and he joins us on the show today. Stuart, I'd like to start off by having you talk a little bit about what the course of this book will be. Stuart: Sure. My goal is to give the layman an overview of hacking so that they understand the steps that an attacker takes. I want to address the skill levels of a hacker. I want to give them the knowledge of what they can do to get in so that they can protect their network from people trying to attack their networks. Rob: Stuart, your background is in the area of software engineering and you've worked with the very highest level of security. How did you get into this field? I've read your book Hacking Exposed and I've read Hackers at Play in the 20th Century and I'm very interested in your opinion of the field and the changing of how we approach this. How did you get into the field of cybersecurity? Stuart: Well, I was a software engineer for 25 years. I built operating systems for many companies. My first time working with the government was at the Central Intelligence Agency. I was writing code for the CIA for their viruses. I worked for them for a while, and I became a risk assessment engineer. Rob: And how did that lead you into this field? Stuart: Right. I saw the needs in the government and I wanted to build the same kind of product. I wanted to have a product that they could buy and help them secure their networks. I wanted to learn all of the things that I could and work as a penetration test engineer. That's how I got into the security field. Rob: You mention in your book that you did some work with the CIA, which I find really interesting and I'm curious, how many people have done work with the CIA 82157476af

[bela kovacs hommages pdf 30](#)  
[AnyTrans 6.3.0 Crack Serial Key](#)  
[Recovery Toolbox For Pdf Full Crack](#)