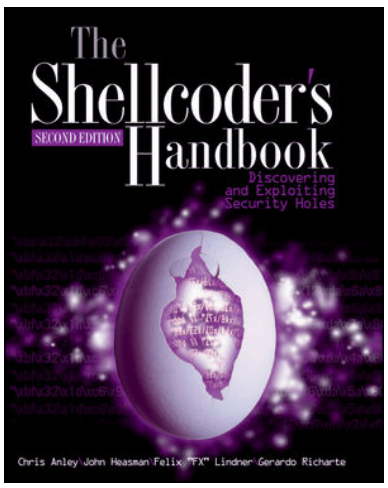

The Shellcoder's Handbook: Discovering and Exploiting Security Holes, 2nd Edition

Chris Anley, John Heasman, Felix Lindner, Gerardo Richarte

E-Book	978-0-470-19882-7	October 2007	**£23.99**
E-Book	978-1-118-07912-6	February 2011	**£23.99**
Paperback	978-0-470-08023-8	August 2007	**£31.99**

DESCRIPTION

• This much-anticipated revision, written by the ultimate group of top security experts in the world, features 40 percent new content on how to find security holes in any operating system or application

• New material addresses the many new exploitation techniques that have been discovered since the first edition, including attacking "unbreakable" software packages such as McAfee's Entercept, Mac OS X, XP, Office 2003, and Vista

• Also features the first-ever published information on exploiting Cisco's IOS, with content that has never before been explored

• The companion Web site features downloadable code files

ABOUT THE AUTHOR

Chris Anley is a founder and director of NGSSoftware, a security software, consultancy, and research company based in London, England. He is actively involved in vulnerability research and has discovered security flaws in a wide variety of platforms including Microsoft Windows, Oracle, SQL Server, IBM DB2, Sybase ASE, MySQL, and PGP.

John Heasman is the Director of Research at NGSSoftware. He is a prolific security researcher and has published many security advisories in enterprise level software. He has a particular interest in rootkits and has authored papers on malware persistence via device firmware and the BIOS. He is also a co-author of *The Database Hacker's Handbook: Defending Database Servers* (Wiley 2005).

Felix “FX” Linder leads SABRE Labs GmbH, a Berlin-based professional consulting company specializing in security analysis, system design creation, and verification work. Felix looks back at 18 years of programming and over a decade of computer security consulting for enterprise, carrier, and software vendor clients. This experience allows him to rapidly dive into complex systems and evaluate them from a security and robustness point of view, even in atypical scenarios and on arcane platforms. In his spare time, FX works with his friends from the Phenoelit hacking group on different topics, which have included Cisco IOS, SAP, HP printers, and RIM BlackBerry in the past.

Gerardo Richarte has been doing reverse engineering and exploit development for more than 15 years non-stop. In the past 10 years he helped build the technical arm of Core Security Technologies, where he works today. His current duties include developing exploits for Core IMPACT, researching new exploitation techniques and other low-level subjects, helping other exploit writers when things get hairy, and teaching internal and external classes on assembly and exploit writing. As result of his research and as a humble thank you to the community, he has published some technical papers and open source projects, presented in a few conferences, and released part of his training material. He really enjoys solving tough problems and reverse engineering any piece of code that falls in his reach just for the fun of doing it.