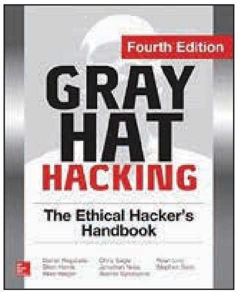
Book Review

Gray Hat Hacking: The Ethical Hacker's Handbook



By Allen Harper, Shon Harris, Jonathan Ness, Chris Eagle, Gideon Lenkey, Terron Williams

Reviewed by Ibe Etea, CISA, CRISC, CA, CFE, CIA, CRMA, a corporate governance, internal controls, fraud and enterprise risk assurance professional. Etea also serves as a member on the advisory council of the Association of Certified Fraud Examiners (ACFE).

The rise of hacking exploits and their potential to cause havoc to enterprises, nations, industries and individuals has led to a need for more information on hacking. *Gray Hat Hacking: The Ethical Hacker's Handbook* is written by a team of experts with advanced knowledge in gray hat hacking and penetration testing, and the book includes proven strategies and techniques meant to fortify user networks and help prevent current and emerging digital catastrophes.

The book offers a variety of hacking tools and weapons, case studies, mitigating remedies against attacks, and ready-to-deploy models. It gives an overview of modern hacking tools and techniques such as Android-based exploits and reverse-engineering techniques. It also outlines the ethical considerations of hacking, including existing cyberlaws. The book was compiled by a team of experts with years of experience in the field, demonstrated by the depth and accuracy of this book. *Gray Hat Hacking* highlights important points in its note bookmarks and lists useful links and references in each chapter. Additionally, practical codes and command structures bring theory to real-life scenarios, which are included in the book as engaging illustrations, graphics and tables.

The book succeeds in giving a holistic guide to the subject of gray hat hacking by addressing the different facets of the subject, from definitions to legal developments in the area. It also provides up-to-date granular threat profiles, processes, techniques, commands and tools that are utilized in modern-day hacking. All of this is achieved while keeping to the key theme of the gray hat—responsible and truly ethical in its intentions and the materials prescribed. A key aspect of the book's coverage is a focus on programming, which is needed in order to be able to create exploits or review source code. Fuzzing techniques and shellcode creation are also reviewed, as are advanced penetration methods and exploits.

The benefits derived from the book are numerous and readers will be able to:

- Build and launch spoofing exploits with Ettercap and Evilgrade
- Hack Cisco routers, switches and network hardware
- Bypass Windows Access Control and memory-protection schemes
- Use advanced reverse-engineering to exploit Windows and Linux software and learn the use-after-free technique in recent zero-day exploits
- Neutralize ransomware before it takes control of their desktop
- Find one-day vulnerabilities with binary diffing and other similar techniques

The book itself is broken into three parts and has 23 chapters. The first part prepares the readers with essential tools and techniques, such as programming and reverse engineering. It describes the distinctions between black, gray and white hat hackers and their respective characteristics. The second part delves deep into advanced penetration techniques and exploits, with hands-on testing labs, covered beyond what is available in print and other materials on the subject. The final part covers Android malware, ransomware, 64-bit malware and next-generation reverse engineering.

The book delivers a comprehensive and up-to-date compilation of the gray hat hacker's tools and materials, with downloadable hands-on labs that can be replicated by readers. Since the last edition, 12 new chapters have been added and many of the gaps from the previous edition have been addressed.

EDITOR'S NOTE

Gray Hat Hacking: The Ethical Hacker's Handbook is available from the ISACA® Bookstore. For information, see the ISACA Bookstore Supplement in this issue of the *Journal*, visit *www.isaca.org/bookstore*, *contact support at https://support.isaca.org/* or telephone +1.847.660.5650.

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA web site *(www.isaca.org/journal)*, find the article and choose the Comments tab to share your thoughts.

Go directly to the article: