<<黑客免杀攻防>>

图书基本信息

书名：<<黑客免杀攻防>>

13位ISBN编号：9787111440420

10位ISBN编号：7111440420

出版时间：2013-9-1

出版时间：机械工业出版社

作者：任晓珲

<<黑客免杀攻防>>

内容概要

《黑客免杀攻防》国内首部关于黑客免杀技术的专著，旨在为反病毒工程师剖析各种恶意软件和应对各种安全威胁提供全面指导。
不仅从攻击者（黑客）的视角全方位揭示了黑客免杀技术的常用方法、常用技术和思想原理，还从防御者（反病毒工程师）的视角深入讲解了遏制免杀技术的具体方法策略。
从纯技术的角度讲，本书不仅详细讲解了免杀技术的各种细节和方法，还详细讲解了PE文件、逆向工程、C++壳的编写、免杀壳的打造、脱壳、Rootkit等安全技术的细节。

《黑客免杀攻防》共20章，分为三大部分：基础篇（第1~6章）详细介绍了黑客免杀技术的初级技巧，包括查找（修改）特征码、常见特征码绕过技巧、壳在免杀中的应用、花指令和其他免杀基础知识；高级篇（第7~16章）深入讲解了PE文件、逆向工程、C++壳的编写、免杀壳的打造、脱壳、Rootkit等常用安全技术的原理和细节，以及黑客免杀技术是如何应用它们的，为反病毒工程师应对各种恶意软件提供了原理性指导；扩展篇（第17~20章）为遏制黑客免杀技术提供了思路和具体的方案。

作者简介

任晓珲，资深安全技术工程师，华章“信息安全技术丛书”专家顾问，致力于免杀技术和反病毒技术的实践。
对软件安全、逆向工程、Rootkit、加壳与脱壳等技术有较深入的研究和理解，积累了丰富的经验。
北京蓝森科技有限公司创始人，黑客反病毒论坛创始人，邪恶八进制团队成员，资深培训讲师，国内知名信息安全培训品牌15PB的创始人。
目前专注于计算机安全的中高端培训。

<<黑客免杀攻防>>

书籍目录

附录A　80x86汇编基础知识

版权说明