《Rootkit：系统灰色地带的潜》

图书基本信息

书名：《Rootkit：系统灰色地带的潜伏者》

13位ISBN编号：9787111441786

10位ISBN编号：7111441788

出版时间：2013-10-1

出版社：机械工业出版社

作者：Bill Blunden

页数：600

译者：姚领田,蒋蓓,刘安,李潇

《Rootkit：系统灰色地带的潜》

内容概要

《Rootkit：系统灰色地带的潜伏者》共分四部分。第一部分（第1～6章），全新阐释rootkit本质、rootkit与反取证关系、安全领域态势，以及反取证技术的策略、应对建议和攻击优势。之后，从硬件、软件（系统）、行业工具和内核空间方面介绍rootkit调查过程和利用反取证技术破坏调查过程的策略，使你对取证和反取证有全新了解。第二部分（第7～8章），主要介绍rootkit如何阻止磁盘分析和可执行文件的分析，而调查人员如何利用有效的工具和策略来分析辅助存储器（例如磁盘分析、卷分析、文件系统分析以及未知二进制分析）中可能留下的rootkit痕迹，并对内存驻留和多级释放器技术及用户态Exec（UserlandExec）理念进行了深入剖析。第三部分（第9～15章）主要详解攻击者利用rootkit破坏数据收集过程和造成“一切安好”的假象的前沿实用策略：阻止在线取证、内核模式策略、更改调用表、更改代码、更改内核对象、创建隐秘通道和部署带外rootkit。第四部分（第16章），高屋建瓴地重新总结了rootkit的核心策略，以及如何识别隐藏的rootkit、注意事项和如何处理感染等。

《Rootkit：系统灰色地带的潜》

作者简介

Bill Blunden，资深计算机安全专家，从事相关研究10余年，对rootkit有非常深入的研究。目前从事网络安全设备代码和ERP中间件的相关工作。活跃于计算机安全类社区，常与计算机安全领域多名世界级安全专家交流探讨。在学术生涯中走过不少弯路，因此对计算机安全有异于常人的观察角度和体会。

《Rootkit：系统灰色地带的潜》

书籍目录

《Rootkit：系统灰色地带的潜》

精彩短评

1、有史以来翻译的最烂的一本书
2、难得的一本关于rootkit的专业书籍，几年前利用它的英文版走入rootkit的世界，终于有了英文版，而且还是新版，翻译的也不错。赞一个。
3、很不错的一本书。不过在看的时候得结合一些个人的理解，死抠字面意义是很难懂的。
4、力荐
5、不错入门

《Rootkit：系统灰色地带的潜》

精彩书评

1、首先，我不是说这本书是本烂书。作者也许功力深厚，作者也许是个大牛，可惜选错了译者！从目录和大概看，作者的本意是给入门的rootkit编写者看的，内容也不错，还介绍了一些rootkit的前沿发展，可惜选错了译者！翻译文字极尽晦涩拗口之能事，甚至还不如谷歌翻译的好不好！再看看译者就明白了，群译啊！群译啊！群译啊！群译啊！16章的书有姚领田，蒋蓓，刘安，李潇，张振项等共计24人分包翻译，翻译不好谁也不担责任，果然是三个和尚没水喝啊！评价：极差。性价比极低，极度不建议购买。如果英文能力不错还是建议去看原版吧！

《Rootkit：系统灰色地带的潜》

版权说明