吉首大学学报自然科学版 » 2010, **Vol. 31** » Issue (3): 43-46 DOI:

基于文件系统过滤驱动的内核Rootkit隐藏技术

（吉首大学物理科学与信息工程学院，湖南 吉首 416000）

Research on Occultation Techniques of Kernel Rootkit Based on File System Filter Driver

(College of Physics Science and Information Engineering，Jishou University，Jishou 416000,Hunan China)

全文: PDF (253 KB) HTML (1 KB) **输出:** BibTeX | EndNote (RIS) **背景资料**

摘要 Rootkit是能够持久或可靠地、无法检测的存在于计算机上的一组程序和代码.研究了基于文件系统过滤驱动技术的内核Rootkit，阐述了文件系统过滤驱动的工作原理、过滤驱动的实现、基于文件系统过滤驱动的内核Rootkit对文件隐藏的实现，并讨论了针对Rootkit隐藏的检测技术.

关键词： 文件系统 Rootkit 过滤驱动 隐藏

Abstract: A Rootkit is a set of programs and code that allows a permanent or consistent，undetectable presence on a computer.Windows kernel Rootkit based on file system filter driver has been researched.The work principle of file system filter driver and the realization of filter driver and occultation techniques of kernel Rootkit based on file system filter driver have been introduced.The techniques of Rootkit detection have been discussed.

Key words: file system Rootkit filter driver occultation

服务
- 把本文推荐给朋友
- 加入我的书架
- 加入引用管理器
- E-mail Alert
- RSS

作者相关文章
- 侯春明
- 刘林

基金资助:

吉首大学校级科研课题（09JD015）

作者简介：侯春明（1979-），男，湖南桑植人，吉首大学物理科学与信息工程学院讲师，硕士，主要从事计算机应用与信息安全研究.

引用本文:

侯春明,刘林. 基于文件系统过滤驱动的内核Rootkit隐藏技术[J]. 吉首大学学报自然科学版, 2010, 31(3): 43-46.

HOU Chun-Ming,LIU Lin. Research on Occultation Techniques of Kernel Rootkit Based on File System Filter Driver[J]. Journal of Jishou University(Natural Sciences Edit, 2010, 31(3): 43-46.

[1] GREG HOGLUND，JAMES BUTLER.Rootkit：Windows 内核的安全防护 [M].北京：清华大学出版社，2007.

[2] 杨平，罗红，乔向东． Windows Rootkit隐藏技术研究 [J].计算机与信息技术，2009（3）:73-74.

[3] NAGAR R.Windows NT File System Internals [EB/OL].[2007-04-01].http://download.csdn.net/source/168266.

[4] 张帆，史彩成．Windows驱动开发技术详解 [M].北京：电子工业出版社，2008.

[5] WALTER ONEY．Programming the Microsoft Windows Driver Mode [EB/OL].[2008-02-15].http://download.csdn.net/source/353955.

[1] 侯春明, 王灵. **基于过滤驱动的图书馆网络系统安全监控**[J]. 吉首大学学报自然科学版, 2011, 32(4): 46-49.

通讯地址：湖南省吉首市人民南路120号《吉首大学学报》编辑部 邮编：416000
电话传真：0743-8563684 E-mail：xb8563684@163.com 办公QQ：1944107525