

图书基本信息

书名：<<《黑客防线》2009精华奉献本（上、下册）>>

13位ISBN编号：9787115195043

10位ISBN编号：7115195048

出版时间：2009-1

出版时间：人民邮电出版社

作者：《黑客防线》编辑部 编

页数：全2册

字数：1440000

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

## 内容概要

《黑客防线2009精华奉献本》是国内最早创刊的网络安全技术媒体之一《黑客防线》总第85期至第96期的精华文章摘要。

《黑客防线》一直秉承“在攻与防的对立统一中寻找突破”的核心理念，关注网络安全技术的相关发展，并一直保持在国内网络安全技术发展前列。

从2001年创刊至今，已经成为国内网络安全技术的顶尖媒体。

《黑客防线2009精华奉献本》选取了包括黑客攻防、安全编程、漏洞发掘、入侵渗透、安全防护等方面的精华文章，配合两张包含1200MB安全技术工具、代码和录像的光盘，为读者方便阅读、理解提供了非常便捷的途径。

本书分为上、下两册（本册为上册），适合高校在校生、网络管理员、网络安全公司从业人员、黑客技术爱好者阅读。

## 书籍目录

上册 编程解析 植入执行文件穿越软件防火墙 穿透还原卡原理以及实现 NAT穿透之NAT  
 类型检测 内核方法实现进程保护 无进程式线程插入穿墙技术实现 感染PE文件加载DLL  
 霸王卸甲之击溃nProtect保护体系 在内核驱动中检测隐藏进程 利用BMP图片水印技术写入加  
 密信息 RootKit文件隐藏技术实现 RingO钩子防网页挂马 编程打造自己的SSDT恢复工具  
 基于NTFS的数据流创建与检测 LSP的遍历与修复 Ring3下实现进程之间的跳转 基于线程  
 的隐藏进程检测 使用过滤驱动打造防火墙 用户模式下突破ICESword进程保护 东方微点注  
 册表保护绕过及反绕过实现 打造自己的程序行为监视器 映像劫持Vs启动杀软 Ring3下强行  
 删除文件的攻与防 再谈内核及进程保护 用开源反汇编引擎检测inline hook B / dS结构远程  
 控制的构想与实现 “摧毁”还原精灵保护系统 Rootkit端口隐藏实现 RingO中强行结束进  
 程 直接调用NTFS文件驱动检测隐藏文件 Ringo中Hook SSDT防止进程被结束 RingO突  
 破360自我保护 探秘系统内核表SSDT Shadow RingO下恢复SSDT Shadow 另类绕过Ring3  
 下inline hook Inline hook KeyboardClassServiceCallback实现键盘记录 恢复RingO下的fAT与EAT  
 hook RingO中hook SSDT实现注册表监控 托管注入深入研究 修改函数一个字节实现新  
 型hook 黑器攻防 逆向工程打造木马过360监控 sYs与DLL文件的大范围免杀——黑防系列远  
 控工具免杀全集 让二代远控轻松对抗主动防御 实战突破微点主动防御 Spji函数黑客化 .  
 轻松免杀ASP木马 “拿来主义”对抗微点主动防御 对PHP免杀的思考 数字化脚本免杀法  
 网吧冰点还原终极破解 Au3干掉360实时保护 使用代码混淆技术免杀脚本后门 网管之  
 家 也谈PHP程序SQL . 注入防范 用Linux下的代理服务器保护主干网 Linux下绕过多网卡实  
 现双网络 基于符号链接的防盗链功能实现 一个隔离网络的安全加固方案 初探Ubuntu内置  
 防火墙之netfilter/iptables 密界寻踪 破除Hide The IP的网络验证 Flash也玩破解——去除Flash文  
 件网络验证 修改OillyDBG插件成为ImmDBG插件 百度QQ号码搜索算法分析 Therrtida脚本  
 编写详解 Armadillo5 . 00标准保护的简单脱法 初探国内某个人杀毒软件内部原理 利  
 用Decornpi ler辅助分析IceSword端口枚举功能 . 猎剑文件与磁盘过滤驱动遍历和删除功能全逆向  
 软件代码“窃取”技术——逆向你想要的代码 打造文曲星NC3000模拟器白金存档补丁  
 Ring3下逆向TCPView端口枚举机制 攻破DomLinux邮件服务系统下册 首发漏洞 零点爆破  
 ——零点站点管理系统3 . 2 1版漏洞分析 虚拟机也不安全——VMWare critical Bug浅析 捷派风  
 波——捷派网站管理系统 . net V2 . 0漏洞分析 Dedecms V5又一个任意代码执行漏洞 双字节编  
 码：PHP的隐形杀手 拿下DVBBBS PHP官网 发掘CMS001程序漏洞 特别专题 浅析Microsoft  
 Jet Engine MDB File溢出漏洞 手机入侵与入侵手机 MS08—011 Office WPS文件转换栈溢出漏洞分  
 析与利用 NDIs过滤驱动在广域网络会话劫持防范技术中的应用研究 PHP的后注入时代—  
 —DeDe、PHPCMS, PHPI 68三款PHP系统漏洞分析 . . 漏洞攻防 迅雷PPLAYER . DLL ActiveX  
 控件溢出漏洞剖析及利用 免杀迅雷PPLAYER . DLL ActiveX控件溢出漏洞 Linux内核vmspl ice提  
 权漏洞利用与分析 VoIP安全体系下的全面BreakThrough Linux xfs服务漏洞利用与分析 蓝牙  
 攻击——手机、PDA, 蓝牙耳机尽在囊中 PowerPoint漏洞经典案例分析 从MS08—025看本地  
 提权漏洞的分析与利用 借助IE崩溃实现另类自启动 Surf-Jacking攻击的原理与实现 飘忽在  
 办公室里的暗影——打印机攻击 密界寻踪 利用Session验证做后门 高贝文章系统最新版ODay  
 分析 发掘MaosinCMS网站系统漏洞 JSP提权再品DOS刀耕火种年代 c—Blog注入漏洞再现  
 构造并修复后台登录页面注入漏洞 利用xss在猫扑网“盗”Cookie挂马 活用SQL注入中的  
 “绕” 科讯的软肋——科讯最新漏洞深度分析与利用 注入Discuz!NT 2 . 5 从DedeCMS  
 谈PHP本地文件包含漏洞的利用方式 ODay极速秒杀FTBBS 6 . x DVBBBS 2 . 0 PHP++再现多  
 个ODay 绕过的注入——XuAs、MYPHP最新漏洞分析 Hidden下的注入攻击 溢出研究 菜  
 鸟版Exploit编写指南之四十三隔山打牛之RealPlayer栈溢出 菜鸟版Exploit编写指南之四十四：安全  
 搜索进程内存空间 菜鸟版Exploit编写指南之四十五再谈全字母数字的ShellCode的编写 菜鸟  
 版Exploit编写指南之四十六重温MDB File文件漏洞 菜鸟版Exploit编写指南之四十七The shorter, the  
 better——精简你的数字字母Shell Code 黑客漏洞发掘技术内幕系列之一：磨刀不误砍柴功——迈

出第一步的准备工作 黑客漏洞发掘技术内幕系列之二：搭建一个测试平台 黑客漏洞发掘技术内幕系列之三：xss脚本漏洞发掘技术 黑客漏洞发掘技术内幕系列之四：SQL Injection注入漏洞的发掘方法 黑客漏洞发掘技术内幕系列之五：上传漏洞的发掘技术 黑客漏洞发掘技术内幕系列之六：包含式&信息泄漏式漏洞的发掘技术 黑客漏洞发掘技术内幕系列之七：Fuzzing技术的魅力 黑客漏洞发掘技术内幕系列之八：给程序号脉的调试技术 黑客漏洞发掘技术内幕系列之九：代码中的指航灯逆向技术 黑客漏洞发掘技术内幕系列之十：监视技术&补丁比较技术 黑客漏洞发掘技术内幕系列之十一：最有效的漏洞发掘技术：代码审计 渗透与提权 误打误撞进入电信、网通，移动 校园网渗透技术解析 ASP和PHP双马连用直接提权 入侵Linux系统 社工渗透张家界信息港

## 章节摘录

若采用LBA方式寻址，则没有磁头和磁道的转换操作，当进行连续的多扇区读写时，速度比CHS方式要快。

硬盘的这两种工作方式可由用户在BIOS中设置，但一般都采用LBA方式。

有了以上知识，我们就很容易编写出一个通过IDE控制器访问磁盘的驱动程序了，相关代码如下

。

编辑推荐

《黑客防线(2009精华奉献本)(套装上下册)》分为上、下两册(本册为上册),适合高校在校生、网络管理员、网络安全公司从业人员、黑客技术爱好者阅读。

透视黑客技术发展焦点,把握黑客攻防技术跳动脉搏,全面收录流行黑客技术。

黑客编程实战大演练,黑器免杀与入侵进阶,加密与破解经典实例,网络安全与加固精讲。

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>