

图书基本信息

书名：<<《黑客防线》2010精华奉献本（上、下册）>>

13位ISBN编号：9787115222558

10位ISBN编号：711522255X

出版时间：2010-4

出版时间：人民邮电出版社

作者：《黑客防线》编辑部 编

页数：500

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 2010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97期至第108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求突破”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，经过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 2010精华奉献本》上册选取了包括编程解析、工具与免杀、网络安全顾问以及密界追踪等方面的精华文章，配合两张包含1200MB安全技术工具、代码和录像的光盘，为读者阅读、理解提供了非常便捷的途径。

《黑客防线2010精华奉献本》下册选取了包括首发漏洞、特别专题、漏洞攻防、脚本攻防、溢出研究以及渗透与提取等方面的精华文章，配合两张包含1200MB安全技术工具、代码和录像的光盘，为读者阅读、理解提供了非常便捷的途径。

本书分为上、下两册，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	LKM方式下实现RootKit常见隐藏功能	基于进程行为的Linux反病毒软件
	对抗微点的思路与实现	NDIS协议驱动发送原始以太帧	NDIS中间层过滤驱动修改封装
	枚举CPU的全局描述符表	内核清零杀进程	内核模式简单实现进程监控
	程序注入实现System权限	一种获取Shadow SSDT服务函数原始地址的思路	一种基于内存搜索的进程检测方法
	基于NTFS文件系统的数据恢复程序设计	内核级驱动对抗Hook	
	ZwSetInformationFile反删除技术	Ring3下Hook ZwQueryDirectoryFile实现文件隐藏	基于混合模型的远程控制软件客户端编写
	Kerberos安全协议解析与编程实现	PE格式分析取得ICO图标	自主研发基于文件系统的计算机反取证软件
	基于混合模型的远程控制软件服务端编写	Hook全局描述符表GDT实现进程隐藏	Linux下拦截系统调用实现Root权限的新思路
	Ring0中Inline Hook Shadow SSDT实现窗体保护	Ring3下全局Inline Hook实现HIPS和Rootkit功能	Ring0下注册表键值的枚举与隐藏
	使用通告例程监控驱动及DLL加载	Ring3下实现恶意代码注入Linux内核	拦截Linux内核缺页异常实现System权限
	工具与免杀	VBS玩“进程相互守护”	打造404自定义增强后台扫描工具
	编写删除BHO插件的程序	打造手机通话记录获取木马	编写插件管理程序之注册表快速定位
	对几种驱动防火墙的简单绕过	测试	禁止360安全卫士v5.0运行
	获取Windows XP登录密码	编写批量在线破解MD5程序	通过还原Hive文件分析木马功能
	Ring0下结束KV2009	进程嵌入式木马的分析及查杀	另类下载者轻松突破瑞星2010主动防御及ESET高启发
	计算机病毒行为特征分析	网络安全顾问	利用ext2文件属性和Linux内核能力约束加固系统
	循序渐进巧解IFEO映像劫持	就“一些网民喜欢广告插件”谈IEBHO的双刃性	TCP/IP堆栈指纹识别技术浅析
	轻松玩转Samba服务器安全维护	点面结合轻松阻止Linux非法进程	Linux桌面安全应用一点通
	IPv6 过渡技术浅析	Linux系统远程管理完全攻略	利用“爬虫”技术进行网络漏洞安全检测
	Linux内核编译一点通	中小型企业Web后台安全的实现	密界寻踪
	Windows Vista下动态开启Local kernel Debug的实现与分析	破解分析蝗虫军团病毒	用Debug API踩点
	正确注册码	网络验证的Keygen编写探讨	BT3+Spoonwep2+卡王破解WEP密码
	深入剖析百度空间互踩漫游大师2008的加密体系	破解BB FlashBack2.0	Easy Screensaver Maker算法分析及注册机的编写
	逆向Mail PassView编写自己的Outlook密码恢复工具	从单一到通用，内存补丁的开发过程	利用动态调试器绕过网维大师还原保护
	易SiteWeaver6.6最新漏洞分析与利用	Notepad++之CSS文件无效指针缺陷	搜狗拼音皮肤文件本地溢出漏洞分析及利用
	Mozilla核心浏览器URL编码缺陷	搜狗浏览器特殊URI欺骗漏洞	国内OA安全现状初探——破解华天、金和OA系统
	安全浏览器最新本地XSS跨域0Day分析及其利用	腾讯TT浏览器任意代码注入执行漏洞	曲折入侵网站智能管理MyWeb系统
	腾讯浏览器任意COM文件加载漏洞	揭示Safari3.2.3多个拒绝服务漏洞	飞天总动员——飞天论坛、飞天下载系统ASP、PHP版最新漏洞分析
	特别专题	VOIP安全之微软LCS高级服务器攻防	突破腾讯Tencent Traveler浏览器网址黑名单限制
	Windows驱动漏洞的发现与利用	破解分析犇牛病毒	淘宝用户登录缺陷分析
	指纹识别在办公环境下的安全及渗透技术分析	从XSS到校内网的多个跨站	GPU，密码破解技术应用新时代
	你的聊天我能看到——蓝牙键盘安全	SSL协议的安全性及其安全缺陷分析	QQ登录窗口键盘保护原理分析
	漏洞攻防	浅析Clickjacking技术的利用	淘宝跨站脚本漏洞
	ECShop V2.6.2后台获取WebShell	Comersus Cart漏洞分析与利用	利用Mysql load_file()函数列目录
	Microsoft IIS 6.0 WebDAV远程验证绕过漏洞利用	QQ邮箱也跨站	腾讯浏览器地址栏欺骗漏洞
	网页欺骗技术之劫持超级链接	浅谈Google跳转漏洞	图片验证漏洞的社工利用
	揭开Facebook用户信息泄露的神秘面纱	Cisco IOS路由器的漏洞利用	基于JavaScript的堆溢出利用工程
	浅议安防系统中潜在的安全漏洞	让360的实时监控形同虚设	PHPStat 2.0远程代码执行漏洞
	解析Read8书网程序安全漏洞	再谈手机攻防	脚本攻防
	老Y文章管理系统分析与利用	老Y文章管理系统V2.4最新漏洞分析	搜狐博客跨站之行
	尘月网		

站智能管理系统V2009漏洞分析      浅析LxBlog V6变量未初始化漏洞      微尔文章管理系统漏洞  
 简析      四通政府CMS管理系统漏洞分析      鼎峰ASP版v0.3.6漏洞分析及利用  
 AspProductCatalog漏洞分析与利用      SDCMS 1.1sp1的XSS漏洞挖掘与利用      先锋文章管理系  
 统v1.2漏洞分析      从CCVMS 2009漏洞看Web应用程序API接口安全性      Oracle搜索型注入  
 及NBSI3.0的两个疏忽      PHPCMS漏洞的二次利用      视频点播系统的末日——剖析远古视频点  
 播系统、Supe 1.0漏洞      HTML+TIME下的网页欺骗技术      Dedecms变量未初始化漏洞的深入  
 利用      溢出研究      七禧舞曲CMS入侵思路及漏洞分析      菜鸟版Exploit编写指南之四十八: IE 7  
 XML漏洞分析      菜鸟版Exploit编写指南之四十九: Thinking in MS09-002——IE7内存破坏漏洞原理  
 分析      菜鸟版Exploit编写指南之五十: 缓冲区溢出初探——ShellCode的编写      菜鸟版Exploit编  
 写指南之五十一: Linux下巧妙构造ShellCode实现远程控制      菜鸟版Exploit编写指南之五十二:  
 MPEG2 0Day漏洞揭秘——微软视频ActiveX Control远程执行漏洞分析      菜鸟版Exploit编写指南之  
 五十三: Microsoft Office 0Day漏洞分析——Office Web Components OWC10.dll远程执行漏洞分析  
 菜鸟版Exploit编写指南之五十四: TIFF格式DotRange缓冲区溢出漏洞研究与实例      菜鸟版Exploit编  
 写指南之五十五: 缓冲区溢出攻击和ShellCode实验      菜鸟版Exploit编写指南之五十六: 突  
 破Windows 2003基于硬件的DEP      菜鸟版Exploit编写指南之五十七: MS08-078启示录——IE7 XML  
 远程代码执行漏洞分析与利用      菜鸟版Exploit编写指南之五十八: 打造简单的ShelloCode解码器  
 渗透与提取      入侵威盾IIS防火墙官方网站      Cisco渗透系列之基础知识      Cisco渗透系列  
 之暴力破解      Cisco渗透系列之AS自治系统      Cisco渗透系列之BGP详细分析      网站入侵  
 提权之路      内网渗透嗅探术      一次Resin服务器测试实例      基于Linux的渗透检测平  
 台Backtrack      巧妙渗透:从注入点直接到root      复制Discuz!管理员实现提权      一个巧合的  
 渗透提权      一次由投票引发的入侵及思考

## 章节摘录

插图：看了黑防2008年10期（《即时Patch Linux内核——脱离LK M的实现方法》一文，让我有了学习Linux内核编程的想法。

无奈限于水平，劫持Linux还是没有脱离LKM.只完成了Rootkit常见的隐藏文件、进程和模块信息的功能。

我的开发环境为Fedora 8 i386版操作系统，默认安装了大部分的开发工具和开发库，内核也是默认的2.6.23.1DE是KDevelop.2GB内存，单核P4 3.0G。

这里之所以提到内存和CPU是有原因的。

因为我的CPU是单核的，没有考虑内核抢占的问题.所以如果代码在SMP上运行不稳定.就需要在关键步骤，如替换系统调用的地方加锁（个人觉得替换过程中修改了CRO寄存器，如果内核此时被抢占.恐怕会因为修改了CRO的值出问题）。

至于内存大小的影响，体现在是否注意到了用户空间和内核空间的差别。

如果直接使用用户空间的指针.可能因为指针指向的用户页面已被换出而导致指针失效。

编辑推荐

《2010精华奉献本(套装上下册)》：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

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>