<<《黑客防线》2010精华奉献 >

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

<<《黑客防线》2010精华奉献 >

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寻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。

<<《黑客防线》2010精华奉献 >

书籍目录

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 Lil3UX内核——脱离L K 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