

图书基本信息

书名：<<黑客防线2011合订本（下半年）>>

13位ISBN编号：9787121161209

10位ISBN编号：7121161206

出版时间：2012-3

出版时间：《黑客防线》编辑部 电子工业出版社 (2012-03出版)

作者：《黑客防线》编辑部 编

页数：402

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

《黑客防线系列：黑客防线（2011合订本）（下半年）》为《黑客防线》杂志2011年第7期至第12期杂志所刊登文章的合集，内容涉及当前操作系统与应用软件最新漏洞的攻击原理与防护、脚本攻防、渗透与提权、溢出研究，以及网络安全软件的编写、网管工具的使用等。

《黑客防线系列：黑客防线（2011合订本）（下半年）》涉猎范围广，涵盖目前网络安全领域的各个方面，其中不乏代表着国内网络安全的顶级技术研究，0day漏洞的发布，以及最新的安全技术研究趋势，具有极高的收藏与阅读价值。

本书适用于网络安全从业者、网络管理员、软件测试人员，以及在校大学生等诸多网络安全爱好者阅读。

## 书籍目录

《黑客防线》2011合订本(下半年)目录  
 目录  
 1 彻底废除Win64上360的进程自我保护  
 2 详解Win64上的SSDT  
 3 完美突破Win7 UAC  
 4 CVE-2011-2140 Flash漏洞分析  
 5 Ring3下穿透磁盘还原技术的揭秘  
 6 Stuxnet蠕虫攻击原理分析  
 7 漏洞攻防揭秘ChinaExcel Chart 图表控件远程溢出  
 8 Oday  
 9 另类的珊瑚浏览器XSS Oday漏洞  
 10 The Bat!  
 11 远程命令注入执行漏洞  
 12 再论CVE-2011-0073 Firefox漏洞  
 13 不得不说的QQ浏览器  
 14 无处不在的Dllhijack漏洞  
 15 首发超速浏览器XSS Oday漏洞  
 16 百密一疏的宝贝儿拍卖系统  
 17 乐彼网店系统致命的SQL注入漏洞  
 18 百度游戏用户登录漏洞  
 19 隐藏在超级链接下的罪恶  
 20 H3C iMC Portal ARP欺骗及数据库后门hash验证漏洞  
 21 Kangle Error Message XSS代码注入漏洞  
 22 危险的网趣网上购物系统  
 23 支付宝密码安全控件明文漏洞  
 24 来自金山毒霸的欺骗  
 25 揭秘Remote Files Server文件信息泄露漏洞  
 26 首发微软IIS 7.5 Express拒绝服务漏洞  
 27 脚本攻防利用msvcr71.dll与mona.py实现通用绕过DEP/ASLR  
 28 打造程序自身MemoryWatcher  
 29 Format String攻击再谈  
 30 博客园博客跨站漏洞及利用  
 31 Discuz!6.0管理员权限插件导入获取Webshell  
 32 工具测试利用堆空间突破启发式  
 33 协议包构造工具——scapy  
 34 SSL DOS攻击测试  
 35 渗透与提权对国外某站点的一次安全检测  
 36 利用Art2008cms系统管理员获取Webshell  
 37 Microsoft SQL Server 2005提权  
 38 Mysql数据库提权  
 39 Serv-U提权  
 40 Access注入获取Webshell  
 41 密码绕过获取某国外站点Webshell  
 42 1033389攻击与防范实用技巧  
 43 为VPN而渗透学校校园网  
 44 Pr提权渗透国外某高速服务器  
 45 Windows 2008中Magic Winmail Server提权  
 46 使用Discuz!NT3.5.2文件编辑Oday获取Webshell  
 47 JBoss Application Server获取Webshell  
 48 JBoss信息查看获取Webshell  
 49 Discuz!6.0管理员编辑模板文件获取Webshell  
 50 Discuz!7.2管理员权限插件导入获取Webshell  
 51 渗透数据库之某欺骗的绝妙应用  
 52 133溢出研究MS11-046本地权限提升漏洞分析  
 53 VMware UDF文件缓冲区溢出  
 54 网络安全顾问利用OSSEC构建自己的入侵检测系统  
 55 Android手机上来电防火墙的设计与实现  
 56 ARP欺骗攻击及其检测与防御  
 57 一种防御僵尸网络攻击的编码方式  
 58 一种新的Linux内核劫持方法分析  
 59 谁在遥控我的电视(下)——中兴机顶盒引发的IPTV安全问题  
 60 Serv-U密码破解  
 61 利用NDIS中间层驱动实施通信拦截与自阻塞  
 62 深度剖析Windows句柄分配  
 63 程序动态分析与软件漏洞利用  
 64 利用INT 2D检测调试器和代码混淆  
 65 Android操作系统安全研究系列——通话录音  
 66 远程终端攻防技术完全攻略专题——远程终端的安装使用  
 67 Metasploit下的高级武器——Armitage  
 68 Android操作系统安全研究系列——手机变窃听器  
 69 垃圾的安全——碎纸机安全剖析  
 70 利用Windows用户模式回调机制实施内核攻击  
 71 物理内存取证之文件与缓存分析  
 72 Radmin网络攻防全面接触  
 73 Android操作系统安全研究系列——文件下载  
 74 手机动态口令文件保护系统  
 75 Hardware Hack之NFC系列IC卡数据读取  
 76 一种使PatchGuard失效的简单方法  
 77 编程解析HAL层直接端口I/O  
 78 绕过IceSword1.22来隐藏文件  
 79 241在Ring 3调用内核函数  
 80 VB识别倾斜验证码方法讨论  
 81 252在x86程序里混合x64代码  
 82 256利用缺页异常中断主动拦截Api Hook  
 83 260编写NdisRegisterProtocol  
 84 262针对Python bytecode混淆技术的内存级反汇编  
 85 267一个魔兽争霸外挂的实现  
 86 271挂钩xxxKeyEvent实现安全键盘输入  
 87 275由HOOK引发同步安全之谈  
 88 278使用kprobes进行内核修改  
 89 281另类过文件主动防御  
 90 287VB伸缩图像之插值算法  
 91 289Win64上实现摄像头开启防护  
 92 292对某Crackme的分析及其注册机的写法  
 93 296过滤IRP突破冰刃文件检测  
 94 299Android操作系统安全研究系列——短信窃听器  
 95 303再谈在Win64上反蓝屏  
 96 308在Win64上动态枚举SSDT  
 97 311挂钩KeUsermodeCallback函数来实现自己的“财产保镖”  
 98 316利用MmCheckSystemImage拦截驱动加载  
 99 321indy组件idhttp 500 错误时获取网页内容  
 100 324Android远程监控技术之——Android系统概述  
 101 326破坏PE与拆分功能突破启发式  
 102 335通过手机短信控制电脑  
 103 336在Win64上实现内核级Inline Hook  
 104 340杂谈兼容模式与WOW64  
 105 342在Win64上实现强制读/写进程内存  
 106 347在Win64上实现代码注入  
 107 351在Win64上内核模块的枚举和隐藏  
 108 356摸清中文输入原理截汉字  
 109 359调研Handwritten Password  
 110 361DLL劫持检测  
 111 363高效使用和管理程序内存  
 112 368Android程序开发之Whereyouare  
 113 370进程防火墙开发的再次挖掘  
 114 374无驱动记录QQ2011密码  
 115 379清空CMOS的几种方法  
 116 383密界寻踪对一个键盘过滤驱动的逆向  
 117 388一款游戏资源解包工具的开发始末  
 118 390反程序破解的一种方法  
 119 396记一个有趣的CrackMe  
 120 397慧炬虚拟操作系统探秘(一)  
 400



## 章节摘录

版权页:破解360密盘的加密之谜360密盘是360公司最新推出的一款保护用户资料不外泄的加密工具，在黑客防线2010年第12期的文章上我提到绕过文件透明加密机制的方法，其中提到过360密盘加密机制，它就是利用一个文件虚拟成磁盘，也就是FileDisk的原理。

了解到这一步，大家就可以明白360密盘的工作原理是，通过网络验证来打开加密盘符。

大家再仔细想一想，是不是验证成功，就马上解密出原先加过密的镜像文件（也就是虚拟磁盘360密盘x），解密的结果如图1所示。

由于360密盘是内嵌入360安全卫士的，所以4要安装360安全卫士才能安装360密盘，其实可以将360密盘直接剥离出360安全卫士。

在360安装目录下建一个360sofe文件夹，这个其实就是安装360安全卫士产生的目录。

里面建一个文件夹，名为mipan的目录，还R要一个36OCommon.dll的公用通信的动态链接库文件，如图2所示。

编辑推荐

《黑客防线(2011合订本)(下半年)》是一本涉及网络信息安全的纯技术月刊，创刊于2001年，至今已经历时10年。

10年来，《黑客防线》坚持“在攻与防的对立统一中寻找技术突破”的理念、积极倡导技术创新和突破，成为国内网络信息安全技术人员和相关专业在校学生不可缺少的技术月刊。

《黑客防线(2011合订本)(下半年)》适用于网络安全业者、网络管理员、软件测试人员，以及在校大学生等诸多网络安全爱好者阅读。

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>