

<<黑客防线2011精华奉献本（上）>>

图书基本信息

书名：<<黑客防线2011精华奉献本（上下册）>>

13位ISBN编号：9787115247957

10位ISBN编号：7115247951

出版时间：2011-3

出版时间：人民邮电

作者：《黑客防线》编辑部 编

页数：596

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>

## <<黑客防线2011精华奉献本（上）>>

### 内容概要

《黑客防线》是国内最早创刊的网络安全技术媒体之一。本书收录了《黑客防线》总第109期至第120期的精华文章。

《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，并一直跟踪国内网络安全技术的发展，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。

本书选取了编程解析、工具与免杀、网络安全顾问、密界寻踪、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权等方面的精华文章，并配有两张CD光盘，其中包含安全技术工具、代码和录像，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

- AV对抗技术之数据编码
- Hook NDIS实现MAC过滤
- Hook ObCreateObject实时监控进程创建
- Linux下利用调试寄存器Hook系统调用
- Ring0级Rootkit进程隐藏与检测技术
- Ring3下通过查询GDI句柄表来检测进程
- VB验证码识别方法之数据分类?匹配
- Windows内核bugcheck和shutdown回调的检测
- WS方法结束线程
- 保护文件不被360文件粉碎机删除
- 编写文件粉碎机
- 防止直接切换CR3读写进程内存
- 构造自己的SSDT绕过主动防御
- 绕过360驱动防火墙加载驱动研究
- 后门程序的“安全”之路
- 基于Intel VT-x检测隐藏进程
- 基于分层的键盘监听驱动程序的编写
- 模拟实现NT系统通用PspTerminateProcess
- 江民2010 KiFastCallEntry Hook保护原理分析
- 禁用Copy-On-Write机制实现全局Hook
- 决战反外挂系统之秘密通信原理
- 利用Delphi玩转ShellCode
- 利用Fltmgr加载驱动绕过瑞星剖析
- 利用GINA实现U盘开机锁
- 内核编写CMOS维护工具
- 浅谈枚举DPC定时器的思路
- 图片验证码的随机实现详解
- 实现在Windows Mobile手机中彩信的后台收发
- 无模块DLL的进程注入剖析
- 冰刃下实现无驱动隐藏自身
- 让句柄可写——修改正在被使用文件的方法探索
- 在C++中嵌入汇编实现DLL注入剖析
- 支付宝转接安全应用全接触
- 自己开发内核漏洞挖掘工具IoControlFuzzer
- 特殊方法实现读写进程内存

工具与免杀

- VBS实现通用定位autorun.inf中病毒体的路径
- U盘打造开机锁
- 基于硬件虚拟化的HIPS
- 利用EFS提高文件系统的安全性
- 文件夹加密超级大师的脆弱加密分析
- 探寻“秒杀”技术背后的猫腻
- PE文件图标修改原理详?

<<黑客防线2011精华奉献本 (上)>>

Python编写Post注入脚本剖析  
Windows启动驱动加载顺序修改  
编写反启发式免杀下载者剖析  
动态污点分析系统TEMU  
反高启发与反主动防御之路——基于源码的免杀技术(上)  
反高启发与反主动防御之路——基于源码的免杀技术(中)  
反高启发与反主动防御之路——基于源码的免杀技术(下)  
利用强迫超时规避JavaScript Exploit特征码检测  
卡斯基虚拟机启发式扫描技术突破剖析

网络安全顾问

Linux下LDAP统一认证的实现  
巧用Linux实现局域网安全访问  
数字证书原理及应用  
用VXE保护Linux系统安全  
利用日志进行MySQL数据库实时恢复  
Paros 3.2.13在Windows平台下的使用指南  
安全SSL访问的实现方法详解  
二层安全的解析与防护  
基于文件系统的移动存储设备安全管理  
肉鸡还是陷阱：巧借VMWare逆向分析入侵过程  
修改数据库用户权限防范SQL注入  
无线网络设备指纹识别

下?

密界寻踪

利用Shell SDK保护程序  
WEP加密算法的实现原理与破解  
Anti-debug Crackme算法分析  
游戏外挂软件破解剖析  
WPS破解无线WPA/WPA2密钥攻防  
窗口破解万能招  
分析木马以寻找攻击者  
极虎病毒破解分析  
雅虎通聊天记录解密攻防  
逆向工程：打造了不起的签名  
文件夹病毒破解分析  
浅析“内存不能为read/written”

首发漏洞

Kerio MailServer远程管理访问服务器任意文件漏洞  
KooMail安全警告机制绕过漏洞  
SparkMail Mail Server用户权限越界漏洞  
动易SiteWeaver 6.8短消息0day跨站漏洞  
揭密Safari 4 Remote Crash漏洞  
绕过限制的KooMail XSS 0Day漏洞  
淘特CMS最新0Day漏洞攻防分析  
我家我设计6.5 cell32.ocx控件本地文件信息泄露0day  
千博企业网站管理系统0day跨站漏洞攻防剖析  
Kangle Web Server源代码信息泄露0day剖析

## <<黑客防线2011精华奉献本 (上)>>

### 特别专题

- 东方微点主动防御Mp110013.sys本地特权提升漏洞攻防剖析
- 网络打印机攻防
- 基于Minifilter进程衍生物跟踪技术
- 基于WiFi通信的攻击与劫持攻防剖析
- 解释器漏洞利用：指针推断与JIT喷射技术
- 在Windows 7 x64下隐藏进程和保护进程

### 漏洞攻防

- Discuz! 7.1 & 7.2远程代码执行漏洞解析
- 构建守护进程：FreeBSD操作系统内核栈利用
- Windows内核描述符表GDT及LDT漏洞利用
- IE下绕过同源策略限制的方法
- 基于智能手机设备的中间人攻击技术
- 手机漏洞与恶意攻击防范
- ActiveX控件引发的泄密
- CMailServer远程任意文件下载漏洞
- dBpowerAMP Audio Player 2 ActiveX控件溢出漏洞
- Detour补丁技术攻击Windows组策略
- DreamMail通讯录跨域脚本执行漏洞攻防剖析
- FCkeditor上传漏洞与IIS6解析漏洞的利用和修补
- ICMPv6中异常NS消息探析
- IE极光漏洞分析与利用防范
- TurboMail 4.3邮件系统XSS 0Day漏洞剖析
- 不安全的搜狗浏览器ActiveX控件函数剖析
- 超级巡警ASTDriver.sys本地特权提升漏洞攻防剖析
- 金笛邮件系统3.10版本用户权限越权漏洞攻防剖析
- 搜狗浏览器clickjacking漏洞剖析
- 无线网络设备攻击技术白皮书

### 脚本攻防

- 一个Oracle注入点引发的检测剖析
- 动态跨站请求伪造攻击剖析
- 绕过单引号继续注入攻防
- 浅析跨站请求伪造
- 黑客防线脚本实验室第二期基础入侵篇通关攻略
- 保险箱保护的程序攻防剖析
- iframe脚本攻防完全接触
- IncrediMail邮件脚本跨域执行漏洞
- W-SVD数字水印系统性能分析
- 高级命令行注入研究
- 基于混沌细胞自动机数字水印的嵌入及检测
- 揭示DreamMail安全限制绕过与邮件跨域执行双重漏洞剖析
- 跨站脚本攻击攻防解析
- 浅谈Local File Disclosure漏洞的利用剖析
- 浅析路径遍历漏洞
- 新挂马方式单击劫持漏洞剖析
- 由Apache Server-Status引?的旁注入攻击剖析

### 溢出研究

<<黑客防线2011精华奉献本 (上)>>

Wireshark溢出漏洞分析与利用剖析  
阻止缓冲区溢出攻击研究  
Fat Player 0.6b视频播放软件栈溢出漏洞分析  
失败的堆栈溢出之旅  
Muse v4.9.0.006(.m3u)本地溢出漏洞的分析和利用  
Winamp 本地栈溢出漏洞分析Windows XP SP3  
SAP Player 0.9本地缓冲区溢出  
Windows溢出保护绕过方法概览  
不改变程序执行流实现缓冲区溢出攻击剖析  
探秘Excel对象堆栈溢出漏洞  
Free CD to MP3 Converter v3.1栈溢出漏洞分析

渗透与提权

\*nix操作系统入侵攻防剖析  
Windows访问令牌窃取提升进程权限剖析  
对于iGENUS邮件系统的一次安全检测  
对办公内网的一次安全检测  
对一台Linux服务器的入侵安全检测  
一次计算机系统安全检测全程笔记  
简单渗透IBM AIX 5.3 (JSP+DB2)剖析  
利用FCKeditor漏洞渗透Linux服务器剖析  
巧用G6FTP Server渗透服务器剖析  
渗透局域网新模式研究  
利用栈回溯来编写驱动防火墙

## 章节摘录

插图：在电子数据四处乱飞的年代里，如何保护自己的文件不被外泄，如何做到文件真正地销毁，是当前亟待解决的问题。

用户一方面担心自己的重要电子数据丢失，一方面又担心自己的数据被窃取。

当前，很多人为了保护自己的数据不被丢失，对数据进行分散管理，即在多个位置备份自己的文件，这种方式必然带来大量数据的冗余存放，极大地降低文件系统存储效率，同时也给文件使用者带来极大不便，每次更新文件内容都需要对已存在的多个备份进行更新，且安全性能也必然随之下降。

这些问题的出现，也使得数据恢复技术得到快速发展。

数据恢复技术即在面对计算机系统遭受误操作、病毒侵袭、硬件故障、黑客攻击等事件后，能够将用户数据从各种“无法读取”的存储设备中拯救出来，从而将损失减到最小的技术。

当前，大多数人都希望数据的丢失能够借助数据恢复软件重现找回数据。

当前国际上数据恢复技术主要有：软恢复（文件系统问题）、硬恢复（硬件问题）、大型数据库系统、异型系统的数据恢复、数据覆盖后的恢复。

在软件上，主要有Easy Recovery、Final Data等。

硬件恢复主要是针对磁盘片损坏、磁道坏、硬盘内部系统区坏的修复。

在数据恢复技术高速发展的今天，大家又开始担心起如何彻底地销毁不需要的数据，但又不希望电子数据被别人利用各种工具挖掘出来。

本文将介绍一种新方法，即采用软件方式实现文件数据的永久擦除。

<<黑客防线2011精华奉献本(上)>>

编辑推荐

《黑客防线2011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>