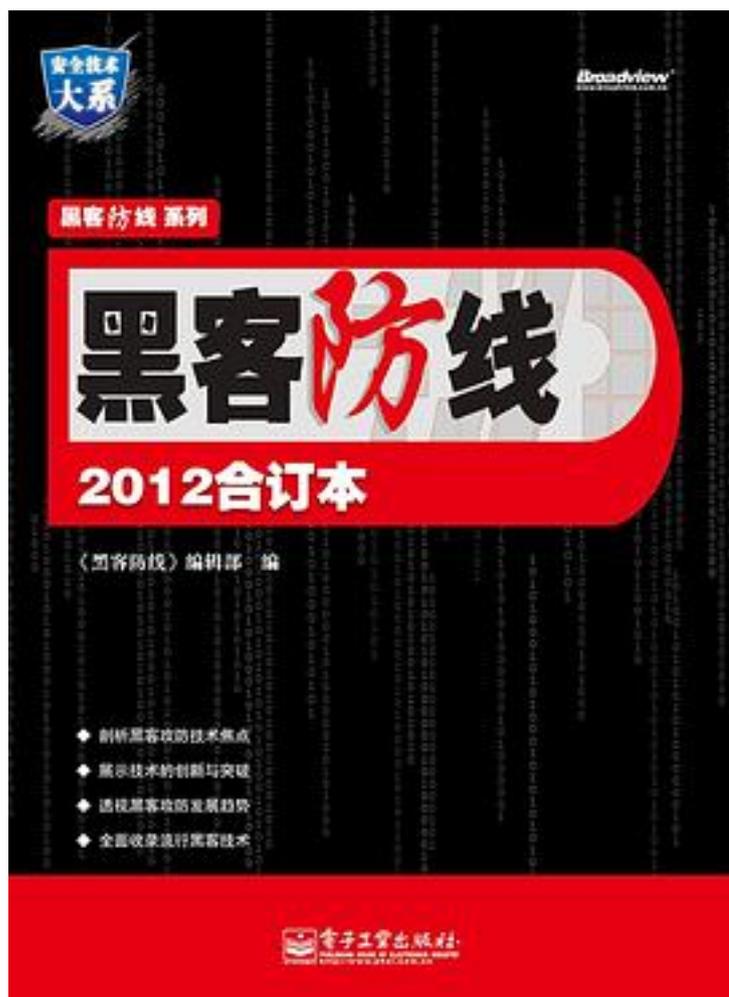


黑客防线2012合订本



[黑客防线2012合订本_下载链接1](#)

著者:《黑客防线》编辑部

出版者:电子工业出版社

出版时间:2013-6

装帧:平装

isbn:9787121202902

本书为《黑客防线》杂志2012年杂志所刊登文章的合集，内容涉及当前系统与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。本书涉猎范围广，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。

作者介绍:

目录: 本月焦点

一次艰难的渗透纪实 1

漏洞攻防

解密百度阅读器远程执行任意文件漏洞 14

危机四伏的iWeb Mall多用户商城系统 16

DeDeCMS v5.7最新漏洞分析 18

如履薄冰的新为在线0Day漏洞分析 29

解密56ican远程执行任意程序漏洞 43

计算机网络安全之DLL劫持漏洞详解 45

潜伏在办公室里的攻击 48

优看PDF在线阅读控件远程代码执行漏洞 50

Web Office控件漏洞大曝光 53

巧妙破解YesLab联网认证视频 56

基于组件对象模型 (COM) 的劫持攻击技术 58

手机支付宝密码存储机制分析 62

UUSee2012漏洞六连发 71

IE浏览器数组越界漏洞利用方法 75

NOTES邮件系统漏洞发掘 77

RPC漏洞挖掘 79

Struts2远程执行漏洞分析 之CVE-2012-0392篇 83

HTML5十大威胁：隐秘攻击与漏洞潜伏 86

A-PDF All to MP3基于SEH的漏洞利用 91

危机重重的Office Anywhere 96

惊爆UUSee网络电视2012远程溢出漏洞 98

关于DarkCometRAT531的逆向分析 100

AXMAN工具原理解析 103

利用pvefindaddr编写飞秋漏洞利用程序 107

挖掘AcReport报表远程植入命令漏洞 110

Android远程监控技术

击溃360手机卫士的三大防护 112

Android下访问Web服务器上传文件 125

Android系统shellcode编写 127

Android应用程序的补丁方法 131

安卓WiFi密码破解工具编写初探 141

Android 环境窃听器的实现 151

Android蓝牙安全通信 153

Android手机一键Root原理分析 160

伸向Android的核心解析NDK 165

Android Gamex木马分析报告 169

Android平台下ARP欺骗的分析与实现 174

Android木马分析与编写 180

Android API Hook之LD_PRELOAD 182

Android下APK及DEX文件解析 185

移植Linux源码到Android系统环境搭建 187

工具与免杀

- 自己动手打造APK安装器 190
- 搜索Kernel32.dll：TEB与PEB之旅 197
- Windows内核调试命令利器分析 199

渗透与提权

- Burp Suite——SQLINJECTION渗透 203
- 老树开花：一个js函数引发的命案 210
- Linux下的MySQL提权 212
- PHPDISK header bypass & getShell 215
- Linux环境下的防火墙绕过技巧 217
- 浅谈Linux下ARP入侵 220
- MetInfo 全局变量覆盖另类突破防注入 224
- XSS黑盒入侵实例 227
- 暴力破解一个ASP加密算法 228
- 另类思路检测webshell 230
- 由Tencent://Message协议联想到的“协议劫持” 233

外文精粹

- Stealth Rootkits攻击技术发展趋势分析 236
- 基于Linux内核2.6.x/3.0.x可加载内核模块的注射技术 240

网络安全顾问

- 来自移动终端的新一代 245
- 信息威胁技术探讨 245
- Hardware Hack 之NFC系列——门禁卡攻击 248
- 电子渠道身份认证系统安全性分析 251
- 摩托罗拉XOOM 提权和安装backtrack5 254
- 企业内网ISA安全认证环境搭建详解 258
- 浅谈Windows和Linux下的嗅探攻击及防范 267
- 揭示主流内网管控系统的脆弱性 273
- Linux LKM注入攻击 275
- 编程实现Linux环境的二进制文件反调试 281

编程解析

- 编程实现突破Win64内核保护机制 285
- Linux下内核漏洞利用的几种方式 290
- 在Win64上实现SSDT HOOK 294
- 初步探索PE32+格式文件 298
- 深入跟踪Hello World执行 303
- PHP Hashtable collisions简要算法分析 310
- 远程同步CMD SHELL 程序的实现 312
- 实现Win64上的内核级 Inline Hook引擎 316
- 恢复在Win64上的SSDT钩子 318
- Windows 7注册表之SAM文件取证分析 321
- 安博士V3 Lite 的一些问题 324
- 编程实现使安博士无法访问被保护文件 328
- Returnil影子系统1.2的逆向分析 331
- 对卡巴斯基安全键盘的研究 337
- 详解Win64上的 Shadow SSDT 339
- Linux ELF运行时内存详解 343
- 细解使用Native API编程 347
- 利用Glibc Hook打造Linux程序防火墙 352
- Win64上使用标准方法监控进程创建 354

Win64下使用标准方法监视文件访问 356
浅议 MDL 359
小议csrss与smss 363
新思路注入DLL并绕过杀毒软件 370
利用Detours实现API Hook 374
在Win64上枚举消息钩子 377
木马核心功能研究 380
Pass TrojanCut突破研究 385
Windows异常处理机制 387
使用Libnet实现ARP数据包发送 391
Shellcode In X64 Find kernel32.dll 394
Shellcode In X64-2Search Function using hash 397
Windows编程之对象与句柄 402
用pcap编写网络嗅探器 407
TLS反调试的前世今生 411

密界寻踪

Android应用程序破解入门 416
手写指令对抗IDA 422
一个平板软键盘的算法分析与注册机编写 428
AvKiller病毒分析 432
分析一个DLL劫持下载者 439
• • • • • ([收起](#))

[黑客防线2012合订本_下载链接1](#)

标签

hack

os

lol

VPN

看见了

评论

挺好的，原理讲解也比较详细。

[黑客防线2012合订本 下载链接1](#)

书评

[黑客防线2012合订本 下载链接1](#)