<<黑客防线2011合订本（上半年 >

图书基本信息

书名：<<黑客防线2011合订本（上半年）>>

13位ISBN编号：9787121143274

10位ISBN编号：7121143275

出版时间：2011-8

出版时间：电子工业

作者：《黑客防线》编辑部 编

页数：422

内容概要

本书为《黑客防线》杂志2011年第1期至第6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。
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，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。

<<黑客防线2011合订本（上半年 >

书籍目录

mp3-nator漏洞挖掘
mp3-nator漏洞挖掘 （续bypass dep）
coolplayer 2.18缓冲区溢出漏洞利用分析
ms10-081漏洞从补丁比对到生成poc
rop——一种非传统栈上攻击 方法分析与防御方法介绍
皮皮播放器溢出漏洞挖掘
win2003活动目录堆溢出漏洞分析手记
一步步分析最新flash player 0day漏洞溢出
网络安全顾问
kerberos协议登录服务的漏洞攻击与防御
攻击下一代web开发标准html5
打造rtx登录安全审计系统
windows服务器安全加固之组策略篇
google android平台下编写内核级rootkit
防御浏览器遭受跨源css攻击策略
offensive security exploit weekend赛题详解
windows服务器安全加固之账户设置和服务管理篇
谋杀时间——ntp攻击技术浅析
upnp hacking攻防技术初探
针对智能手机和路由器的tapjacking与物理定位攻击
sap web应用程序攻击技术
gprs/edge/umts/hspa移动数据通信攻击技术
无须注入shellcode实现对rop程序的攻击
adobe reader 'cooltype.dll' ttf字体溢出漏洞分析
exim"string_vforat()"溢出漏洞分析
win32k.sys键盘布局文件提权漏洞分析
某校园网站的安全性分析
谈谈区域传送的威胁和防御
sql server数据库系统日志安全体系
隐藏实现交换网络的qq号
连接字符串参数污染攻击技术
应用程序级拒绝服务攻击与防御
zeroaccess：内核模式下的一个高级rootkit分析
银行支付网关协议安全性分析
简单构建linux操作审计系统
攻击wdm驱动
ntp反射型ddos攻击
android应用的破解初探
谁在遥控我的电视（上）——中兴机顶盒引发的iptv安全问题
编程解析
编程打造ime输入法启动程序
读取本地已登录的qq号及应用
在win64上实现ring3 inline hook
在win64上实现文件保护
编程实现简易winobj
编写自身带病毒警告的程序
windows mobile手机病毒研究系列之“ 牛刀小试 ”

章节摘录

版权页：插图：键盘记录技术可谓缤纷繁杂，毕竟键盘记录是任何一个远控程序所必需的组件。
简单地实现有Ring3层的全局钩子，虽然很简单，但是笔者清楚地记得，在2010年的这个时候所得到的测试结果是，大部分的安全产品默认配置下都不能阻止键盘全局钩子。
到了RingO层，实现键盘记录的方法非常多，比如安装一个键盘过滤驱动、Hookkbdclass类驱动的分发函数、Hook I of Compiete Request，再比如黑防杂志之前相关的两篇文章，（编写调用门键盘记录程序）和（直接访问键盘控制芯片获取键盘记录）等。
但是这些技术或多或少都有缺陷，比如安装键盘过滤驱动，很容易被摘掉；Hook类驱动的分发函数以及一些其他的函数，由于这些Hook点是固定的，很容易被检测到。
相对而言，动态的Hook点则往往很难被安全软件所关注，甚至这些动态的Hook点并不是常驻在内存中的，而是有生命周期的，周期结束后也就不存在Hook了，这时安全软件根本无法检测。
而本文就是介绍这样一种技术，希望对安全软件的关注点扩展有所帮助。

编辑推荐

《黑客防线(2011合订本)(上半年)》：焦点关注：针对热点网络安全技术问题展开讨论，或发表技术观点、研究成果，或针对某一技术事件做分析、评测。
漏洞攻防：探讨如何利用系统漏洞、网络协议漏洞进行渗透／反渗透、入侵／反入侵。
脚本攻防：探讨如何利用脚本系统漏洞进行注入、提权、渗透；国内外使用率高的脚本系统的O-day攻击以及相关防护代码。
工具测试：讨论巧妙的免杀技术，针对最新杀毒软件、HIPS等安全防护软件技术进行讨论。
渗透与提权：对主流的Windows系统、SQL数据库，以及其他操作系统的渗透、提权技术进行讨论。
溢出研究：详细分析各种系统，包括应用软件漏洞，以及底层触发、Shellcode编写、漏洞模式等。
网络安全顾问：讨论局域网和广域网整体网络防／杀病毒、防渗透体系的建立；ARP系统的整体防护，较有效地防范DDoS攻击的技术等。
编程解析：探讨各种安全软件和黑客软件的编程技术，底层驱动、网络协议、进程的加载与控制技术和Virus高级应用技术编写，以及漏洞利用的关键代码解析和测试。
密界寻踪：关于算法、完全破解、硬件级加解密的技术讨论和病毒分析、虚拟机设计、外壳开发、调试及逆向分析技术的深入研究。
剖析黑客攻防技术焦点，展示技术的创新与突破，透视黑客攻防发展趋势，全面收录流行黑客技术。

版权说明