第一图书网, tushu007.com

<<《黑客防线》2010合订本（>>

图书基本信息

书名：<<《黑客防线》2010合订本（上半年）>>

13位ISBN编号：9787121116520

10位ISBN编号：7121116529

出版时间：2010-8

出版时间：电子工业出版社

作者：《黑客防线》编辑部

页数：612

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

第一图书网, tushu007.com

前言

《黑客防线》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，坚持在攻与防的对立统一中寻求技术突破的理念、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。
随着时代的发展，为了使读者更加及时、便捷地阅读这本技术月刊，从2010年7月开始，月刊采用了电子版网络传播形式、不再出版纸张版的月刊。
但是由于广大读者在得到快捷电子版的同时，还是希望作为技术资料收藏纸张版，为了满足这一要求，每半年将会出版这样一本合订本。
合订本将全面收录半年的文章，偶尔也会删除极少部分技术含量不足文章。
总体还是体现技术创新和突破。
关于《黑客防线》半年合订本的出版周期半年合订本一般会在每年的8月出版上半年的，每年的2月出版前一年上半年的。
由于编印发涉及诸多环节，希望读者能够容忍这个延时。
及时阅读，还是建议到黑客防线官网订阅电子版月刊。
关于文章中涉及代码的下载由于强调纯粹技术性的研究，很多文章涉及的技术阐述需要代码实现，本来应该收录在光盘中随书配赠。
但是，光盘审读一般依赖杀毒软件扫描结果，对于本技术领域很多代码都会误报，澄清需要拖延出版周期。
所以，我们只能在黑客防线官网提供相关代码的下载。
由此带来的不便希望得到读者的理解和谅解。
关于购买合订本的途径电子工业出版社所有的销售终端都是极好的购买途径，包括但不限与各大新华书店、科技书店、计算机书店以及网络书城。
同时黑客防线编辑部的淘宝店也会有便捷服务。

第一图书网, tushu007.com

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一，一直秉承“ 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发展，并且在国内一直处于网络安全技术的前沿。
从2001年创刊至今，《黑客防线》已经成为国内网络安全技术的顶尖媒体。
《2010合订本（上半年）》是《黑客防线》2010年上半年（总第109期至第114期）的合订本，将6期杂志的文章整合入“ 编程解析 ”“ 工具测试 ”“ 脚本攻防 ”“ 漏洞攻防 ”“ 密界追踪 ”“ 渗透与提权 ”“ 网管之家 ”“ 溢出研究 ”几个栏目中。
文章涉及的代码，读者可到《黑客防线》的官方网站上载。
本书适合高校在校生、网络管理人员、网络安全公司从业人员、黑客技术爱好者阅读。

第一图书网, tushu007.com

<<《黑客防线》2010合订本（>>

书籍目录

编程解析 模拟实现NT系统通用PspTerminateProcess 绕过360驱动防火墙加载驱动结束360 浅析手机来电防火墙的实现原理 SSDT及SSDT Shadow完全解析（二） AV对抗技术之数据编码 VC实现木马服务端自动更新 VC实现用户克隆和登录信息擦除 端口转发3389数据 打造Linux下无线PPPoE攻击工具 Linux下基于日志文件的Ext3数据恢复程序设计 强制类型转换之谜 添加Section全攻略补遗 使用GRETA正则表达式扫描网马 编程实现定制系统安装盘 Ring 下阻止ARK启动 API Hook反屏幕截图 论BIOS感染的持久化之道 基于.NET框架的驱动加载模块的设计与实现 Windows内核bugcheck和shutdown回调的检测 .WinIo驱动级模拟按键的实现 基于进程行为的检测技术 利用CPU序列号保护自己的软件 江民2010 KiFastCall Entry Hook保护原理分析 函数CALL地址替换实现深度钩子 基于SPI的网络行为监视器 浅谈枚举DPC定时器的思路 新思路打造Loader程序——编写木马加载程序 编写简单代理程序 Linux下利用调试寄存器Hook系统调用 Inline Hook IoCallDriver保护文件 机密文件的图片隐藏法 巧用ASP.NET实现验证码安全登录 简单代码打造无敌内存清零和过NP内存读写 利用fltmgr加载驱动绕过瑞星 后门程序的“安全”之路 钩子的另类用法 WS方法结束线程 另类思路解决自动连接VPN问题 浅谈Kernel EAT Hook的检测与绕过 浅谈HTTP代理环境下的两种通信方式 一个简单dump工具的实现 支付宝转接安全应用全接触 利用BHO获取当前光标信息 编程解析数字证书 TDL3 Rootkit深入分析 Windows Vista/2008网络编程接口的应用及挂钩（一） Windows Vista/2008网络编程接口的应用及挂钩（二） JMP大法对抗Call Hook 防止直接切换CR3读写进程内存 利用Hook IRP隐藏磁盘分区 绕过Head Inline Hook 服务的编程实现 清理AT命令使用痕迹 无模块DLL的进程注入 自己实现插APC结束线程 VB识别简单规则验证码 验证VB破解宽带账号的两种思路 Ring3下模拟NtSystemDebugControl实现驱动功能 Ring0级Rootkit进程隐藏与检测技术 利用FSD Hook IRP分发例程保护文件 基于BlueZ接口开发蓝牙扫描程序 VC实现远程关机 游戏木马面面观 简单获取所有内核对象类型 浅谈64位环境下的编程 浅谈用户空间内存管理 浅议Windows Session ID 图片验证码的随机实现详解 FSD Hook实现文件行为取证 保护文件不被360文件粉碎机删除 利用GINA实现U盘开机锁 在WM手机中实现来电防火墙 无驱动隐藏DLL 检测虚拟机 突破UAC获取System权限 SSDT Hook与DKOM实现反杀 基于分层的键盘监听驱动程序的编写 利用LSB位信息实现隐藏与隐写 远程文件捆绑器的原理与实现 Delphi实现邮件SMTP与POP3 Hook NDIS实现MAC过滤 编写Nessus扫描插件 禁用Copy-On-Write机制实现全局Hook 冰刃下实现无驱动隐藏自身 修改QQ群发器 打造绕过XueTr的注册表项隐藏 底层函数的文件防删除 恢复Inline Hook结束冰刃进程 内核编写CMOS维护工具 让句柄可写——修改正在被使用文件的方法探索 Ring0检测中断及KiFastCallEntry钩子 工具测试 VBS实现通用定位autorun.inf中病毒体路径 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） 一个bash door的简单分析 主动防御AutoRun病毒 解密Ability FTP Server用户信息数据 蓝屏的调试艺术 编程免杀Poison Ivy远控 对国外垃圾邮件的分析 FTP服务器的传输模式实战剖析 Ajax实现网页Sniffer研究 U盘打造开机锁 基于Linux系统WINE虚拟机技术的研究 实战网页盗链攻与防 基于硬件虚拟化的HIPS 探寻秒杀技术背后的猫腻 利用配置文件生成可执行文件 打造最小化PE文件 利用EFS提高文件系统的安全性 脚本攻防 动态跨站请求伪造攻击 浅析跨站请求伪造 iframe脚本攻防完全接触 绕过单引号继续注入 轻松注入360保险箱保护的程序 浅谈Local File Disclosure漏洞的利用 由Apache server- status引发的旁注入侵 一个Oracle注入点引发的检测 黑客防线脚本实验室第二期基础入侵篇通关攻略 揭示绕过DreamMail安全限制与邮件跨域执行双重漏洞 IncrediMail邮件脚本跨域执行漏洞 浅析路径遍历漏洞 高级命令行注入研究 漏洞攻防 Detour补丁技术攻击Windows组策略 FCKeditor上传漏洞与IIS 解析漏洞的利用和修补 .NET FrameWork Rootkit：Framework框架中的后门技术 揭密Safari Remote Crash漏洞 无线网络设备攻击技术白皮书 Discuz! .1 & .2远程代码执行漏洞解析 TurboMail .3邮件系统XSS -Day漏洞 绕过限制的KooMail XSS -Day漏洞 Rootkit技术：智能手机的攻击与启示 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 “IE极光”漏洞的分析与利用 KooMail安全警告机制绕过漏洞 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 网络合法监听的漏洞利用 SparkMail Mail Server用户权限越界漏洞 ICMPv6中异常NS消息探析 CmailServer远程任意文件下载漏洞 不安全的搜狗

第一图书网, tushu007.com

浏览器ActiveX控件函数 Kerio MailServer远程管理访问服务器任意文件漏洞 构建守护进程：FreeBSD操作系统内核栈利用 Java串口通信攻击技术 CAPTCHA攻防作战 教育之忧——Edoas（教育行政办公系统）安全检测 密界寻踪 XML文档加密解密一点通 AntiESP定律 WPS——破解无线WPA/WPA2密钥的捷径 极虎病毒破解分析 WEP加密算法的实现原理与破解 一个Crackme的破解 利用Shell SDK保护程序 xfpack不能不说的秘密 xfpack不能不说的秘密（续） 一个图片Crackme的简单算法分析 Anti-debug Crackme算法分析 彻底分析盗号木马 Apple固件更新机制的逆向与利用 文件夹病毒破解分析 逆向文件捆绑程序编写思路 逆向工程：打造了不起的签名 渗透与提权 对一台Linux服务器的艰难入侵 利用FCKeditor漏洞渗透Linux服务器 窃取Windows访问令牌提升进程权限 对Discuz!的漏洞分析 巧用G6FTP Server渗透服务器 对于iGENUS邮件系统的一次安全检测 渗透局域网的新模式研究 对母校的“友情检测”社会工程学在入侵中的作用 对办公内网的一次安全检测 网管之家 几种恶意程序搞破坏的新伎俩 肉鸡还是陷阱：巧借VMWare逆向分析入侵过程 数字证书原理及应用 Windows 的系统安全与病毒防护 二层安全的解析与防护 取证调查中的BitLocker驱动级加密技术 Linux下LDAP统一认证的实现 巧用jQuery插件进行密码安全校验 应对分布式拒绝服务攻击 利用日志进行MySQL数据库实时恢复 Biologger——生物特征记录程序 DNS Flood Detector让DNS更安全 用djbdns为DNS保驾护航 打造安全强大的网页快照 安全SSL访问的实现方法详解 走进安全的Java脚本世界 用VXE保护Linux系统安全 RPM另类用法加固Linux安全 用Stunnel加密保护邮件服务器 解析安全电子交易协议SET 借助虚拟内存快照检测恶意Shellcode 巧用Linux实现局域网安全访问 强悍的完整性检查工具Nabou 溢出研究 菜鸟版Exploit编写指南之五十九：迅雷5.9任意内核地址覆盖漏洞及利用方法 菜鸟版Exploit编写指南之六十：Wireshark溢出漏洞分析与利用 菜鸟版Exploit编写指南之六十一：阻止缓冲区溢出攻击研究 高效编写JIT-Spray Shellcode

第一图书网, tushu007.com

章节摘录

插图：

第一图书网, tushu007.com

编辑推荐

《2010合订本(上半年)》：透视黑客技术发展焦点把握黑客攻防技术脉搏全面收录流行黑客技术编程解析 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。
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。
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、Shelleode编写、漏洞模式等。
渗透与提权对主流的Windows系统、SQL数据库，以及其他的操作系统的渗透、提权技术进行讨论。
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。
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。
网管之家 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，较有效的防范DDOS攻击的技术等。

第一图书网, tushu007.com

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