

<<暗战亮剑>>

图书基本信息

书名：<<暗战亮剑>>

13位ISBN编号：9787115230461

10位ISBN编号：7115230463

出版时间：2010-7

出版时间：人民邮电

作者：朱锡华//刘月铎//侯伟

页数：441

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>

## 前言

本书以讲解渗透攻防技术为主线，用实例剖析了黑客的渗透手法，揭示了黑客的渗透内幕，由浅入深、循序渐进地介绍了网络渗透攻防的核心技术。

渗透攻防是一项综合性很强的技术，以往的有关安全的书籍讲解这方面的知识显得理论多于实战，且观念陈旧，无法跟上高速发展的网络技术。

很多内容都停留在几年前的黑客攻防水平，使得新型安全技术无法在书籍中再现，这样也阻碍了新技术的普及，而黑客一旦掌握了最新的攻击技术，就可以肆意破坏整个网络，正是由于这些原因，笔者决定撰写一本技术新颖、实战性和扩展性强的网络渗透攻防书籍。

书中讲解了最流行的渗透攻防技术，每章都精选经典渗透攻防案例，从案例出发再现真实攻防场景，将真实攻防环境“搬”到书中。

在本书的编写过程中，随时关注最新的安全技术，将国内外最新的攻防技术吸收到本书中，这样读者不仅可以掌握国内黑客的攻防秘籍，更重要的是可以了解到国外高端安全攻防的前沿技术。

本书包括黑客攻防入门、高级缓冲区溢出技术、各类高级web渗透攻防技术、主流数据库攻防技术、最新服务器提权渗透攻防技术、专业网络渗透工具剖析、内网高级渗透攻防等。

在了解了黑客渗透技术后，本书还提供了专业性、针对性极强的安全防御方案，让读者学以致用地管理好自己的网站、计算机系统、服务器等免受黑客渗透攻击，打造更加坚固的安全防御遁甲。

## &lt;&lt;暗战亮剑&gt;&gt;

## 内容概要

《暗战亮剑：黑客渗透与防御全程实录》是一本全面剖析黑客渗透攻防技术的书籍，剖析了黑客对网络系统进行渗透的技术，帮助读者了解计算机系统的脆弱环节及安全缺陷，教给读者有针对性地采取安全措施，堵住黑客入侵的通道，加固系统安全。

《暗战亮剑：黑客渗透与防御全程实录》包括黑客攻防入门、高级缓冲区溢出技术、高级Web渗透攻防技术、主流数据库攻防技术、最新服务器提权渗透攻防技术、专业网络渗透工具剖析、内网高级渗透攻防等。

在了解了黑客渗透技术后，《暗战亮剑：黑客渗透与防御全程实录》还提供了专业性、针对性极强的安全防御方案，让读者知己知彼地管理自己的服务器及计算机系统免受黑客渗透，打造更加坚固的安全防御盾甲。

《暗战亮剑：黑客渗透与防御全程实录》可作为网络安全评估人员、网络安全开发人员、黑客攻防研究人员、企业和电子商务网络安全维护人员，以及网络安全机构认证培训等机构的辅助学习教材，同时也可作为计算机院校师生的网络安全教学参考书。

## <<暗战亮剑>>

### 作者简介

侯伟，笔名“猪猪”，2004年创办 [ 岁月联盟 ] 网络安全团队与网站。担任多家企事业单位安全顾问，多次应邀参加国内安全峰会，参与国家电网公司多项安全检查工作。现参与西安交通大学多个安全合作项目。

朱锡华，笔名“晓华”，精通多种网络安全技术，尤其热衷于研究网络渗透与安全防御技术。拥有丰富的安全实战攻防经验以及安全项目实施经验，曾在国内著名黑客杂志《黑客手册》发表过若干网络攻防类技术文章，现为国内著名黑客组织“岁月联盟”核心成员，参与团队内部技术研究与管理工

作。酷爱摩托车越野极限运动，曾多次穿越川西高原。

## 书籍目录

第1章 渗透攻防实践技术11.1 命令行下的黑色艺术11.2 扫描器下的黑色艺术81.2.1 扫描器基本概述81.2.2 国产黑客扫描利器——X-Scan91.2.3 著名黑客工具——SuperScan111.2.4 SuperScan扫描使用技巧111.2.5 SuperScan实战利用111.2.6 超速S扫描器使用技巧131.2.7 暴力破解利器——HSCAN141.3 黑客远程控制技术剖析151.3.1 远程控制软件结构151.3.2 高级远程控制软件——Pcshare161.3.3 Pcshare客户端设置161.3.4 Pcshare上线方式161.3.5 Pcshare服务端配置171.3.6 Pcshare更新IP181.3.7 远程控制软件——VNC181.3.8 黑客的忠实守护者——随意门剖析191.4 黑软上传技术剖析211.4.1 TFTP上传211.4.2 FTP上传221.4.3 VBS脚本上传231.4.4 超短VBS上传241.5 黑客常见攻击手法揭秘251.5.1 端口扫描251.5.2 口令破解251.5.3 缓冲区溢出271.5.4 拒绝服务271.5.5 网络嗅探281.5.6 SQ、注射攻击281.5.7 会话劫持291.5.8 网页挂马攻击301.5.9 网络钓鱼301.6 社会工程学欺骗剖析311.7 域名劫持321.8 常见系统端口渗透实战剖析321.8.1 网络端口概述321.8.2 21端口渗透剖析331.8.3 23端口渗透剖析351.8.4 53端口渗透剖析351.8.5 80端口渗透剖析361.8.6 135端口渗透剖析381.8.7 139/445端口渗透剖析391.8.8 1433端口渗透剖析401.8.9 1521端口渗透剖析411.8.10 306端口渗透剖析411.8.11 389端口渗透剖析421.8.12 899端口渗透剖析431.8.13 631端口渗透剖析441.8.14 900端口渗透剖析441.8.15 080端口渗透剖析451.9 常见加密算法破解技术剖析461.9.1 MD5密码破解剖析461.9.2 CFS编码加密破解481.9.3 电子邮件客户端软件密码破解剖析481.9.4 RDP远程桌面密码破解剖析491.9.5 FlashFXP密码破解剖析491.9.6 本地破解VPN客户端登录密码剖析501.9.7 常见JS加、解密501.9.8 雷池新闻系统加、解密501.9.9 RAR压缩软件密码破解剖析511.9.1 常见文字类文档加密破解521.9.1 其他加密算法的破解531.10 黑客反取证之痕迹擦除剖析531.10.1 操作系统常见日志531.10.2 服务器日志剖析541.10.3 系统防火墙日志551.10.4 系统终端登录日志561.10.5 其他日志561.10.6 系统日志的擦除571.10.7 数据库日志擦除591.11 WindowsNT系统渗透演练剖析591.11.1 WindowsNT系统入侵概述591.11.2 目标扫描601.11.3 渗透方案制定611.11.4 实施方案A611.11.5 实施方案B631.11.6 获得权限641.12 WindowsXP安全加固641.12.1 物理安全很重要641.12.2 勿用盗版系统641.12.3 文件系统安全651.12.4 关闭危险服务651.12.5 账户密码安全671.12.6 系统补丁安全681.12.7 系统自带防火墙681.12.8 ESETSmartSecurity与360安全卫士构筑安全防线691.13 网络攻防环境搭建711.13.1 VMwareWorkstation的安装711.13.2 创建虚拟机以及安装操作系统731.14 IIS6.0与Serv-U7.3 构建稳定服务器771.14.1 IIS6.0概述771.14.2 IIS6.0安装过程771.14.3 IIS6.0配置791.14.4 Serv-U7.3 安装821.14.5 Serv-U7.3 域配置841.14.6 Serv-U账户建立851.14.7 使用FlashFXP管理服务器861.15 Apache+PHP5+MySQL+PHPMyAdmin环境构建与DZ论坛架设871.15.1 AppServ2.5.6安装与配置881.15.2 DZ论坛架设901.16 Apache-Tomcat+JSP环境构建941.16.1 安装SDK941.16.2 Apache\_Tomcat6.0安装与配置961.17 VPN服务器搭建与应用971.17.1 VPN基础概述981.17.2 VPN服务器配置981.17.3 VPN客户端应用101第2章 缓冲区溢出和漏洞挖掘攻防实战1032.1 缓冲区溢入门1032.1.1 从人类思维到计算机1032.1.2 计算机内存分布1042.1.3 操作系统函数调用过程1062.2 Win32栈溢出1072.2.1 Win32栈溢入门1072.2.2 溢出报错原因分析1082.2.3 常见栈溢方式1102.3 Win32堆溢出1162.3.1 Win32堆基础知识1162.3.2 堆的运行过程1172.3.3 堆溢出点的定位1202.3.4 堆溢出的SEH利用法1232.4 ShellCode编写技术1252.4.1 本地ShellCode编写技术1252.4.2 远程ShellCode编写技术1292.4.3 通用ShellCode编写1382.5 软件漏洞挖掘技术1442.5.1 软件漏洞挖掘入门1442.5.2 Python简介1452.5.3 Python探测warFTP漏洞1462.6 Foxmail5.0溢出实战1512.6.1 Foxmail5.0漏洞公布信息1522.6.2 精确定位溢出点1522.6.3 Foxmail5.0溢出1582.7 最新溢出漏洞获取及编写相应exploit1652.7.1 公布exploit的网站1652.7.2 轻松编写exploit1672.7.3 验证修改的exploit1712.8 缓冲区溢出的防范1712.8.1 防火墙防范溢出策略1712.8.2 操作系统防护设置1722.8.3 编写安全的代码173第3章 漏洞攻防实战1753.1 WindowsServer2003IIS6.0安全性解析1753.1.1 利用默认网站目录渗透1753.1.2 上传漏洞的偏门剖析——应用程序扩展1763.1.3 错误信息与盲注1763.1.4 权限设置成拦路虎1763.1.5 目录浏览泄露网站数据1773.1.6 Web服务扩展与提权渗透1773.1.7 IIS写权限渗透网站1783.1.8 特殊目录暗藏杀机1793.2 Apache安全性解析1793.2.1 权限至高无上1803.2.2 文件名解析漏洞1803.2.3 站点配置文件泄漏路径1803.3 Apache\_Tomcat安全性解析1813.3.1 获取机密信息的绝招剖析1813.3.2 弱口令的不安全性1813.3.3 Tomcat也泄密1833.4 ASP程序常见漏洞剖析1833.4.1 上传漏洞1833.4.2 默认数据库入侵剖析1843.4.3 暴库漏洞1853.4.4 SQLInjection (SQL注入) 1853.4.5 Cookie注射1863.4.6 Cookies欺骗1863.5 PHP程序常见漏洞剖析1883.5.1

## &lt;&lt;暗战亮剑&gt;&gt;

php.ini安全性解析1883.5.2 远程文件包含漏洞1893.5.3 PHP注射攻击剖析1903.6 NET程序常见漏洞剖析1913.6.1 上传组件1913.6.2 SQLInjection (SQL注入) 1923.6.3 XSS攻击剖析1933.7 XSS跨站高级利用方式剖析1933.7.1 XSS截取管理员cookies信息剖析1933.7.2 跨站备份WebShell1953.7.3 跨站挂马渗透管理员剖析1983.8 Googlehacker渗透开路1983.8.1 精通Googlehacker语法1983.8.2 Googlehacker批量SQL检测1993.8.3 Googlehacker获取敏感信息剖析2003.8.4 Googlehacker查找管理后台2023.8.5 Googlehacker搜索脚本后门剖析2023.8.6 Googlehacker防御2023.8.7 搜索渗透利器GoogleHacker1.2 2033.8.8 搜索渗透利器GoolagScanner2033.8.9 搜索渗透利器SimpleGoogleV1.02033.9 常见Web渗透利器2043.10 高级Web渗透测试软件剖析2043.10.1 国产王牌注入工具Pangolin穿山甲2043.10.2 黑帽子大会最佳评估工具MatriXay2053.10.3 商业渗透工具Vulnerability62053.11 幕后的入侵揭秘2073.11.1 ASP一句话木马2073.11.2 PHP一句话木马2083.11.3 新型.NET一句话木马2103.11.4 JSP一句话木马2123.12网站编辑器带来的安全问题2143.12.1 判断Web是否使用eWebEditor2143.12.2 eWebEditor默认数据库与路径猜解剖析2153.12.3 eWebEditor新增样式上传WebShell2163.12.4 利用eWebEditor\_.NET版渗透网站剖析2183.12.5 利用eWebEditor\_.JSP版渗透网站剖析2193.12.6 利用Fckeditor击溃坚固网站攻防剖析2213.13后台权限攻防争夺战剖析2253.13.1 数据库备份恢复得到WebShell2253.13.2 IIS6.0路径解析漏洞得到WebShell剖析2273.13.3 数据库插马得到WebShell2273.13.4 系统配置文件得到WebShell2283.13.5 利用模板得到Discuz后台WebShell2283.13.6 直接上传JSP木马2283.14脚本渗透剖析2283.14.1 突破防注入系统继续注射剖析2283.14.2 防注入系统成帮凶2293.14.3 搜索型注射剖析2303.14.4 上传SHTML渗透网站剖析230第4章 数据库渗透安全攻防2314.1 数据库基础知识入门2314.1.1 关系型数据库标准语言——SQL概述2314.1.2 数据库的操作2324.1.3 数据库表的操作2334.1.4 数据表的查询操作2344.1.5 数据更新操作2354.2 数据库的安装2374.2.1 MicrosoftSQLServer2000安装2374.2.2 MySQL安装2404.2.3 ORacle10g安装2454.3 Access手工注射攻防技术剖析2494.3.1 注射点的判断剖析2504.3.2 实际手工注射2514.4 MicrosoftJetDB引擎溢出漏洞剖析攻防2534.5 脚本木马控制Access数据库2554.6 MSSQL账户信息与查询分析器2574.6.1 MSSQL账户信息2574.6.2 查询分析器的使用2584.7 SA账户无cmdshell存储过程渗透剖析2604.8 存储过程添加渗透剖析2614.9 反弹注射技术剖析2614.9.1 opendir函数语法2624.9.2 本地环境配置2634.9.3 反弹注射之目录2634.9.4 反弹注射之爆敏感数据2654.9.5 反弹注射之回显系统命令2674.10 沙盒模式 (SandboxMode) 渗透剖析2674.11 MySQL数据库安全知识2694.11.1 MySQL的部署2694.11.2 Winmysqladmin自动启动2704.11.3 MySQL默认用户名2704.11.4 root密码修改2704.11.5 远程管理用户的建立2714.11.6 MySQL的发现2714.12 MySQL渗透经典函数以及语句剖析2724.12.1 MySQL版本识别2724.12.2 字段数目和类型的确定2734.12.3 Load\_file ( ) 函数2734.12.4 char ( ) 函数2744.12.5 Substring ( ) 函数2744.12.6 Replace ( ) 函数2744.12.7 Loaddatainfile语句2754.12.8 concat\_ws ( ) 函数2754.12.9 Select...intooutfile语句2764.12.10 时间延迟与漏洞剖析2764.12.11 UDF用户自定义函数2774.13 利用MySQL自定义函数执行系统命令剖析2784.13.1 脆弱主机的寻找2784.13.2 文件上传及工具应用2784.13.3 函数的注册及使用2824.14 MySQL5渗透之高级注射剖析2834.15 MySQL导出文件高级利用剖析2854.15.1 原理分析2864.15.2 模拟实战应用2864.15.3 MySQL普通账户渗透剖析2884.16 Linux下MySQL高级渗透剖析2904.17 Oracle渗透之基本命令攻防介绍2934.18 Oracle渗透之账户密码破解攻防剖析2944.19 Oracle渗透之执行操作系统命令剖析2964.20 Oracle普通账户权限提升2994.21 Oracle写入WebShell剖析3014.22 Oracle渗透之WebSQL注射技术攻防剖析3024.23 Access数据库安全加固3054.23.1 修改数据库名3054.23.2 修改数据库连接文件3064.23.3 设置IIS再次加固3064.23.4 修改后台管理认证码3074.23.5 修改后台管理路径3074.23.6 设置严格的权限3074.23.7 及时更新补丁文件3074.24 SQLServer数据库安全加固3084.24.1 SQLServer降权3084.24.2 数据库账户安全管理3094.24.3 删除恶意的存储过程3104.24.4 修改默认TCP/IP端口号3114.24.5 使用SSL加密数据3114.24.6 用补丁增加数据库安全3124.24.7 制定安全容灾备份计划3124.25 MySQL安全加固3124.25.1 降低权限运行3124.25.2 口令安全3144.25.3 修改MySQL监听端口3144.25.4 补丁安全加固3144.26 Oracle安全加固3154.26.1 系统安全加固3154.26.2 Oracle账户安全3164.26.3 设置监听器密码3164.26.4 修改1521端口3164.26.5 使用SSL网络加密3174.26.6 应用最新安全补丁317.....第5章 抢占权限的制高点318第6章 精通常见网络安全工具及技术369第7章 内网渗透防御攻略411

## 章节摘录

黑客在实施渗透的时候，很少会用到图形化操作界面，一般是用系统命令实现的。为了真实地剖析黑客的渗透行为，我们所讲的整个操作过程都将在命令行下完成，以便剖析出黑客渗透并控制远程计算机的踪迹。

学习系统命令不仅可以了解黑客用来实施渗透攻击的秘密，而且对维护操作系统的安全也有特别的意义。

通常黑客在攻击过程中，一般会进行创建用户、上传黑客工具、开启远程桌面服务等操作，这些操作在图形化界面下很难完成，利用系统命令实施对系统的控制是最佳途径。

了解系统命令可以更深入地了解系统的底层，是安全高手必备知识。

本节主要讲解在渗透过程中比较常用的系统命令。

1. 打开命令提示符打开DOS命令提示符有很多种方法，比较常用的就是依次单击“开始”-“运行”项，在弹出的窗口中输入cmd命令即可，如图1.1所示。

另外，也可以建立一个批处理文件用以打开DOS命令提示符，值得注意的是，批处理文件所在的路径是打开cmd后所处的路径，如图1-2所示。

通过这种方式省略了目录切换的麻烦，也非常实用。

## <<暗战亮剑>>

### 媒体关注与评论

面对困难永远不要放弃，你的下一次单击回车键也许就有奇迹发生，感谢作者让我们能有机会亲自见证这些奇迹。

——goodwell（龚巍） 关于书中的内容，只有仔细看过的人才能真正体会到她的价值，希望每个人拥有这本书的朋友，只要你想在黑客安全技术方面有所突破，一定要认真细致地学一学、练一练，真正把里面的知识吃透，练实，再深入学习就不是什么难事了。

——逆风飞扬（周剑） 网络安全管理一直是整个网络管理的难点，特别是在当前开放的网络环境中，本书集中介绍了各种操作系统，应用软件和设备安全弱点及解决方案，使你做到真正有的放矢。

——网络实战专家 王达（茶乡浪子） 黑客技术，羚羊挂角，照书索骥，有迹可求，故其妙处，透澈玲珑。

——著名黑客LCX（李春晓）



## <<暗战亮剑>>

### 编辑推荐

27个核心渗透攻防技术案例，100个疑难解答，寻踪攻击原理，解析渗透安全核心问题，120个实战技巧，提升读者的实战能力，400个安全实例，涵盖操作系统，网站应用程序，主流数据库、内部网络的渗透安全攻防技术。

<<暗战亮剑>>

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>