

信息安全 大系

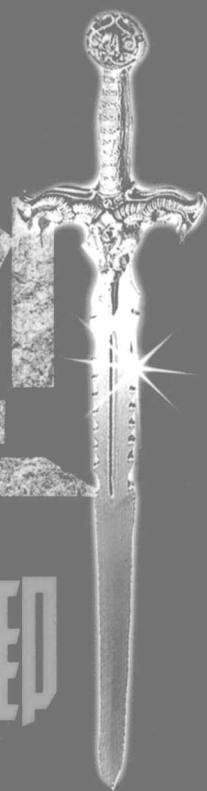


“岁月联盟”鼎力推荐

暗战亮剑

——黑客渗透与防御

全程实录



朱锡华 刘月铨 侯伟 编著

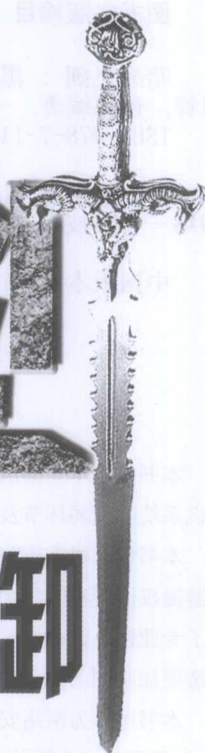
- 27个核心渗透攻防技术案例
- 100个疑难解答，寻踪攻击原理，解析渗透安全核心问题
- 120个实战技巧，提升读者的实战能力
- 400个安全实例，涵盖操作系统、网站应用程序、主流数据库、内部网络的渗透安全攻防技术



人民邮电出版社
POSTS & TELECOM PRESS

信息安全 大系

暗战亮剑



—黑客渗透与防御 全程实录

朱锡华 刘月铨 侯伟 编著

人民邮电出版社
北京

图书在版编目 (C I P) 数据

暗战亮剑：黑客渗透与防御全程实录 / 朱锡华，刘月铎，侯伟编著. — 北京：人民邮电出版社，2010.7
ISBN 978-7-115-23046-1

I. ①暗… II. ①朱… ②刘… ③侯… III. ①计算机网络—安全技术 IV. ①TP393.08

中国版本图书馆CIP数据核字(2010)第082735号

内 容 提 要

本书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薄弱环节及安全缺陷，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。

本书包括黑客攻防入门、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，本书还提供了专业性、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遁甲。

本书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。

书中讲解的工具可在相应的网站搜索下载，也可在岁月联盟 (www.syue.com) 官方站点下载获取。

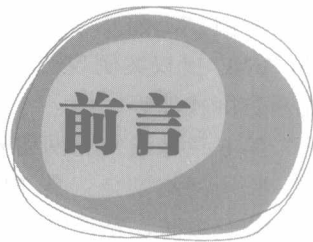
暗战亮剑——黑客渗透与防御全程实录

- ◆ 编 著 朱锡华 刘月铎 侯 伟
责任编辑 张 涛
- ◆ 人民邮电出版社出版发行 北京市崇文区夕照寺街 14 号
邮编 100061 电子函件 315@ptpress.com.cn
网址 <http://www.ptpress.com.cn>
北京隆昌伟业印刷有限公司印刷
- ◆ 开本：787×1092 1/16
印张：28.25
字数：673 千字 2010 年 7 月第 1 版
印数：1—3 000 册 2010 年 7 月北京第 1 次印刷

ISBN 978-7-115-23046-1

定价：55.00 元

读者服务热线：(010)67132692 印装质量热线：(010)67129223
反盗版热线：(010)67171154



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、实战性和可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。

本书分为 7 章，主要内容如下。

第 1 章渗透攻防实践技术，主要包括命令行下的黑色艺术、黑客远程控制技术、黑客常见攻击手法揭秘、常见系统端口渗透实战集锦、常见加密算法破解技术、黑客反取证之痕迹擦除、Windows NT 系统渗透演练、Windows XP 安全加固、网络攻防环境搭建等。

第 2 章缓冲区溢出和漏洞挖掘实战，主要讲解了缓冲区溢出入门、Win32 栈溢出、Win32 堆溢出、ShellCode 编写技术、软件漏洞挖掘技术、最新溢出漏洞获取及编写相应 exploit、缓冲区溢出的防范等。

第 3 章漏洞攻防实战，主要阐述了 Windows Server 2003 IIS6.0 安全性解析、Apache 安全性解析、Apache_Tomcat 安全性解析、ASP 程序常见漏洞剖析、PHP 程序常见漏洞剖析、NET 程序常见漏洞剖析、XSS 跨站高级利用方式、常见 Web 渗透利器、后台权限争夺战等。

第 4 章数据库渗透安全攻防，主要讲解了 Access 手工注射技术、脚本木马控制 Access 数据库、MSSQL 账户信息与查询分析器、存储过程添加渗透剖析、高级 SandboxMode 渗透技巧、MySQL 普通账户渗透、Oracle 普通账户权限提升、Access 数据库安全加固、修改后台管理路径、SQL Server 数据库安全加固、MySQL 安全加固、Oracle 安全加固等。

第 5 章抢占权限的制高点，主要包括 pcAnywhere 提权案例、Serv-U 提权案例、MSSQL

提权案例、MySQL 自定义函数提权案例、Apache_TOMCAT 提权案例、Apache 提权案例攻防、VNC 提权案例攻防、常规安全加固、磁盘权限安全设置、防止木马袭击、部署网警 110 安全防御软件等

第 6 章精通常见网络安全工具及技术，主要讲解了精通网络安全工具 NC、蜜罐欺骗攻防、精通网络安全工具 MT、Windows 远程终端渗透攻防、系统密码破解攻防技术、系统密码截获攻防、精通网络安全工具 hijack、精通网络安全工具 PsTools 等。

第 7 章内网渗透防御攻略，主要包括了内网拓扑结构介绍、内网设备配置与路由渗透测试、利用 XSS 跨站漏洞进内网剖析、无线网络渗透剖析、内网渗透攻防作战方案研究、ARP 的漏洞剖析、内网安全防御战之拒绝 ARP 攻击、Ethereal 准确定位攻击源、安全通甲 ARP 防火墙、铁血通甲 AntiARP-DNS 防火墙、内网安全解决方案经验谈、各安全域安全措施等。

本书由朱锡华、候伟、刘月铎主编，参与编写的还有黄俊然、刘志、王振宇、吴骁、颜有城、郑舒文、余航、杨智伟、杨攀、徐粤川、王常远、范桥。

本书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。

书中讲解的工具可在相应的网站搜索下载，也可在岁月联盟（www.syue.com）官方站点下载获取和本书有关的视频。

编者



第1章 渗透攻防实践技术.....1

1.1 命令行下的黑色艺术.....1	1.5.8 网页挂马攻击.....30
1.2 扫描器下的黑色艺术.....8	1.5.9 网络钓鱼.....30
1.2.1 扫描器基本概述.....8	1.6 社会工程学欺骗剖析.....31
1.2.2 国产黑客扫描利器——X-Scan.....9	1.7 域名劫持.....32
1.2.3 著名黑客工具——SuperScan.....11	1.8 常见系统端口渗透实战剖析.....32
1.2.4 SuperScan 扫描使用技巧.....11	1.8.1 网络端口概述.....32
1.2.5 SuperScan 实战利用.....11	1.8.2 21 端口渗透剖析.....33
1.2.6 超速 S 扫描器使用技巧.....13	1.8.3 23 端口渗透剖析.....35
1.2.7 暴力破解利器——HSCAN.....14	1.8.4 53 端口渗透剖析.....35
1.3 黑客远程控制技术剖析.....15	1.8.5 80 端口渗透剖析.....36
1.3.1 远程控制软件结构.....15	1.8.6 135 端口渗透剖析.....38
1.3.2 高级远程控制软件——Pcshare.....16	1.8.7 139/445 端口渗透剖析.....39
1.3.3 Pcshare 客户端设置.....16	1.8.8 1433 端口渗透剖析.....40
1.3.4 Pcshare 上线方式.....16	1.8.9 1521 端口渗透剖析.....41
1.3.5 Pcshare 服务端配置.....17	1.8.10 3306 端口渗透剖析.....41
1.3.6 Pcshare 更新 IP.....18	1.8.11 3389 端口渗透剖析.....42
1.3.7 远程控制软件——VNC.....18	1.8.12 4899 端口渗透剖析.....43
1.3.8 黑客的忠实守护者——随意门 剖析.....19	1.8.13 5631 端口渗透剖析.....44
1.4 黑软上传技术剖析.....21	1.8.14 5900 端口渗透剖析.....44
1.4.1 TFTP 上传.....21	1.8.15 8080 端口渗透剖析.....45
1.4.2 FTP 上传.....22	1.9 常见加密算法破解技术剖析.....46
1.4.3 VBS 脚本上传.....23	1.9.1 MD5 密码破解剖析.....46
1.4.4 超短 VBS 上传.....24	1.9.2 CFS 编码加密破解.....48
1.5 黑客常见攻击手法揭秘.....25	1.9.3 电子邮件客户端软件密码破解 剖析.....48
1.5.1 端口扫描.....25	1.9.4 RDP 远程桌面密码破解剖析.....49
1.5.2 口令破解.....25	1.9.5 FlashFXP 密码破解剖析.....49
1.5.3 缓冲区溢出.....27	1.9.6 本地破解 VPN 客户端登录密码 剖析.....50
1.5.4 拒绝服务.....27	1.9.7 常见 JS 加、解密.....50
1.5.5 网络嗅探.....28	1.9.8 雷池新闻系统加、解密.....50
1.5.6 SQL 注射攻击.....28	1.9.9 RAR 压缩软件密码破解剖析.....51
1.5.7 会话劫持.....29	1.9.10 常见文字类文档加密破解.....52

1.9.11 其他加密算法的破解	53	1.15.1 AppServ 2.56 安装与配置	88
1.10 黑客反取证之痕迹擦除剖析	53	1.15.2 DZ 论坛架设	90
1.10.1 操作系统常见日志	53	1.16 Apache_Tomcat+JSP 环境构建	94
1.10.2 服务器日志剖析	54	1.16.1 安装 SDK	94
1.10.3 系统防火墙日志	55	1.16.2 Apache_Tomcat 6.0 安装与配置	96
1.10.4 系统终端登录日志	56	1.17 VPN 服务器搭建与应用	97
1.10.5 其他日志	56	1.17.1 VPN 基础概述	98
1.10.6 系统日志的擦除	57	1.17.2 VPN 服务器配置	98
1.10.7 数据库日志擦除	59	1.17.3 VPN 客户端应用	101
1.11 Windows NT 系统渗透演练剖析	59	第2章 缓冲区溢出和漏洞挖掘攻防实战	103
1.11.1 Windows NT 系统入侵概述	59	2.1 缓冲区溢出入门	103
1.11.2 目标扫描	60	2.1.1 从人类思维到计算机	103
1.11.3 渗透方案制定	61	2.1.2 计算机内存分布	104
1.11.4 实施方案 A	61	2.1.3 操作系统函数调用过程	106
1.11.5 实施方案 B	63	2.2 Win32 栈溢出	107
1.11.6 获得权限	64	2.2.1 Win32 栈溢出入门	107
1.12 Windows XP 安全加固	64	2.2.2 溢出报错原因分析	108
1.12.1 物理安全很重要	64	2.2.3 常见栈溢方式	110
1.12.2 勿用盗版系统	64	2.3 Win32 堆溢出	116
1.12.3 文件系统安全	65	2.3.1 Win32 堆基础知识	116
1.12.4 关闭危险服务	65	2.3.2 堆的运行过程	117
1.12.5 账户密码安全	67	2.3.3 堆溢出点的定位	120
1.12.6 系统补丁安全	68	2.3.4 堆溢出的 SEH 利用法	123
1.12.7 系统自带防火墙	68	2.4 ShellCode 编写技术	125
1.12.8 ESET Smart Security 与 360 安全卫士构筑安全防线	69	2.4.1 本地 ShellCode 编写技术	125
1.13 网络攻防环境搭建	71	2.4.2 远程 ShellCode 编写技术	129
1.13.1 VMware Workstation 的安装	71	2.4.3 通用 ShellCode 编写	138
1.13.2 创建虚拟机以及安装操作系统	73	2.5 软件漏洞挖掘技术	144
1.14 IIS 6.0 与 Serv_U 7.3 构建稳定服务器	77	2.5.1 软件漏洞挖掘入门	144
1.14.1 IIS6.0 概述	77	2.5.2 Python 简介	145
1.14.2 IIS 6.0 安装过程	77	2.5.3 Python 探测 warFTP 漏洞	146
1.14.3 IIS 6.0 配置	79	2.6 Foxmail 5.0 溢出实战	151
1.14.4 Serv-U 7.3 安装	82	2.6.1 Foxmail 5.0 漏洞公布信息	152
1.14.5 Serv-U 7.3 域配置	84	2.6.2 精确定位溢出点	152
1.14.6 Serv-U 账户建立	85	2.6.3 Foxmail 5.0 溢出	158
1.14.7 使用 FlashFXP 管理服务器	86	2.7 最新溢出漏洞获取及编写相应 exploit	165
1.15 Apache+PHP5+MySQL+PHPMyAdmin 环境构建与 DZ 论坛架设	87	2.7.1 公布 exploit 的网站	165
		2.7.2 轻松编写 exploit	167
		2.7.3 验证修改的 exploit	171
		2.8 缓冲区溢出的防范	171

2.8.1 防火墙防范溢出策略·····	171
2.8.2 操作系统防护设置·····	172
2.8.3 编写安全的代码·····	173

第3章 漏洞攻防实战····· 175

3.1 Windows Server 2003 IIS6.0 安全性解析·····	175
3.1.1 利用默认网站目录渗透·····	175
3.1.2 上传漏洞的偏门剖析——应用程序 扩展·····	176
3.1.3 错误信息与盲注·····	176
3.1.4 权限设置成拦路虎·····	176
3.1.5 目录浏览泄露网站数据·····	177
3.1.6 Web 服务扩展与提权渗透·····	177
3.1.7 IIS 写权限渗透网站·····	178
3.1.8 特殊目录暗藏杀机·····	179
3.2 Apache 安全性解析·····	179
3.2.1 权限至高无上·····	180
3.2.2 文件名解析漏洞·····	180
3.2.3 站点配置文件泄漏路径·····	180
3.3 Apache_Tomcat 安全性解析·····	181
3.3.1 获取机密信息的绝招剖析·····	181
3.3.2 弱口令的不安全性·····	181
3.3.3 Tomcat 也泄密·····	183
3.4 ASP 程序常见漏洞剖析·····	183
3.4.1 上传漏洞·····	183
3.4.2 默认数据库入侵剖析·····	184
3.4.3 暴库漏洞·····	185
3.4.4 SQL Injection (SQL 注入)·····	185
3.4.5 Cookie 注射·····	186
3.4.6 Cookies 欺骗·····	186
3.5 PHP 程序常见漏洞剖析·····	188
3.5.1 php.ini 安全性解析·····	188
3.5.2 远程文件包含漏洞·····	189
3.5.3 PHP 注射攻击剖析·····	190
3.6 NET 程序常见漏洞剖析·····	191
3.6.1 上传组件·····	191
3.6.2 SQL Injection (SQL 注入)·····	192
3.6.3 XSS 攻击剖析·····	193
3.7 XSS 跨站高级利用方式剖析·····	193
3.7.1 XSS 截取管理员 cookies 信息 剖析·····	193
3.7.2 跨站备份 WebShell·····	195

3.7.3 跨站挂马渗透管理员剖析·····	198
3.8 Google hacker 渗透开路·····	198
3.8.1 精通 Google hacker 语法·····	198
3.8.2 Google hacker 批量 SQL 检测·····	199
3.8.3 Google hacker 获取敏感信息剖析·····	200
3.8.4 Google hacker 查找管理后台·····	202
3.8.5 Google hacker 搜索脚本后门剖析·····	202
3.8.6 Google hacker 防御·····	202
3.8.7 搜索渗透利器 Google Hacker 1.2·····	203
3.8.8 搜索渗透利器 GoolagScanner·····	203
3.8.9 搜索渗透利器 SimpleGoogle V1.0·····	203
3.9 常见 Web 渗透利器·····	204
3.10 高级 Web 渗透测试软件剖析·····	204
3.10.1 国产王牌注入工具 Pangolin 穿山甲·····	204
3.10.2 黑帽子大会最佳评估工具 MatriXay·····	205
3.10.3 商业渗透工具 Vulnerability6·····	205
3.11 幕后的入侵揭秘·····	207
3.11.1 ASP 一句话木马·····	207
3.11.2 PHP 一句话木马·····	208
3.11.3 新型.NET 一句话木马·····	210
3.11.4 JSP 一句话木马·····	212
3.12 网站编辑器带来的安全问题·····	214
3.12.1 判断 Web 是否使用 eWebEditor·····	214
3.12.2 eWebEditor 默认数据库与路径 猜解剖析·····	215
3.12.3 eWebEditor 新增样式上传 WebShell·····	216
3.12.4 利用 eWebEditor_.NET 版渗透 网站剖析·····	218
3.12.5 利用 eWebEditor_JSP 版渗透网站 剖析·····	219
3.12.6 利用 Fckeditor 击溃坚固网站攻防 剖析·····	221
3.13 后台权限攻防争夺战剖析·····	225
3.13.1 数据库备份恢复得到 WebShell·····	225
3.13.2 IIS 6.0 路径解析漏洞得到 WebShell 剖析·····	227
3.13.3 数据库插马得到 WebShell·····	227
3.13.4 系统配置文件得到 WebShell·····	228
3.13.5 利用模板得到 Discuz 后台 WebShell·····	228

3.13.6 直接上传 JSP 木马	228
3.14 脚本渗透剖析	228
3.14.1 突破防注入系统继续注射剖析	228
3.14.2 防注入系统成帮凶	229
3.14.3 搜索型注射剖析	230
3.14.4 上传 SHTML 渗透网站剖析	230

第4章 数据库渗透安全攻防 231

4.1 数据库基础知识入门	231
4.1.1 关系型数据库标准语言——SQL 概述	231
4.1.2 数据库的操作	232
4.1.3 数据库表的操作	233
4.1.4 数据表的查询操作	234
4.1.5 数据更新操作	235
4.2 数据库的安装	237
4.2.1 Microsoft SQL Server 2000 安装	237
4.2.2 MySQL 安装	240
4.2.3 ORacle10g 安装	245
4.3 Access 手工注射攻防技术剖析	249
4.3.1 注射点的判断剖析	250
4.3.2 实际手工注射	251
4.4 Microsoft Jet DB 引擎溢出漏洞 剖析攻防	253
4.5 脚本木马控制 Access 数据库	255
4.6 MSSQL 账户信息与查询 分析器	257
4.6.1 MSSQL 账户信息	257
4.6.2 查询分析器的使用	258
4.7 SA 账户无 cmdshell 存储过程 渗透剖析	260
4.8 存储过程添加渗透剖析	261
4.9 反弹注射技术剖析	261
4.9.1 opendatasource 函数语法	262
4.9.2 本地环境配置	263
4.9.3 反弹注射之列目录	263
4.9.4 反弹注射之爆敏感数据	265
4.9.5 反弹注射之回显系统命令	267
4.10 沙盒模式 (SandboxMode) 渗透 剖析	267
4.11 MySQL 数据库安全知识	269
4.11.1 MySQL 的部署	269
4.11.2 Winmysqladmin 自动启动	270
4.11.3 MySQL 默认用户名	270
4.11.4 root 密码修改	270
4.11.5 远程管理用户的建立	271
4.11.6 MySQL 的发现	271
4.12 MySQL 渗透经典函数以及 语句剖析	272
4.12.1 MySQL 版本识别	272
4.12.2 字段数目和类型的确定	273
4.12.3 Load_file()函数	273
4.12.4 char()函数	274
4.12.5 Substring()函数	274
4.12.6 Replace()函数	274
4.12.7 Load data infile 语句	275
4.12.8 concat_ws()函数	275
4.12.9 Select ...into outfile 语句	276
4.12.10 时间延迟与漏洞剖析	276
4.12.11 UDF 用户自定义函数	277
4.13 利用 MySQL 自定义函数执行 系统命令剖析	278
4.13.1 脆弱主机的寻找	278
4.13.2 文件上传及工具应用	278
4.13.3 函数的注册及使用	282
4.14 MySQL 5 渗透之高级注射 剖析	283
4.15 MySQL 导出文件高级利用 剖析	285
4.15.1 原理分析	286
4.15.2 模拟实战应用	286
4.15.3 MySQL 普通账户渗透剖析	288
4.16 Linux 下 MySQL 高级渗透 剖析	290
4.17 Oracle 渗透之基本命令 攻防介绍	293
4.18 Oracle 渗透之账户密码破解 攻防剖析	294
4.19 Oracle 渗透之执行操作系统 命令剖析	296
4.20 Oracle 普通账户权限提升	299
4.21 Oracle 写入 WebShell 剖析	301
4.22 Oracle 渗透之 Web SQL 注射技术攻防剖析	302
4.23 Access 数据库安全加固	305
4.23.1 修改数据库名	305

4.23.2	修改数据库连接文件	306
4.23.3	设置 IIS 再次加固	306
4.23.4	修改后台管理认证码	307
4.23.5	修改后台管理路径	307
4.23.6	设置严格的权限	307
4.23.7	及时更新补丁文件	307
4.24	SQL Server 数据库安全加固	308
4.24.1	SQL Server 降权	308
4.24.2	数据库账户安全管理	309
4.24.3	删除恶意的存储过程	310
4.24.4	修改默认 TCP/IP 端口号	311
4.24.5	使用 SSL 加密数据	311
4.24.6	用补丁增加数据库安全	312
4.24.7	制定安全容灾备份计划	312
4.25	MySQL 安全加固	312
4.25.1	降低权限运行	312
4.25.2	口令安全	314
4.25.3	修改 MySQL 监听端口	314
4.25.4	补丁安全加固	314
4.26	Oracle 安全加固	315
4.26.1	系统安全加固	315
4.26.2	Oracle 账户安全	316
4.26.3	设置监听器密码	316
4.26.4	修改 1521 端口	316
4.26.5	使用 SSL 网络加密	317
4.26.6	应用最新安全补丁	317

第 5 章 抢占权限的制高点 318

5.1	Windows 2003 基础知识	318
5.1.1	Windows 2003 内置用户组	318
5.1.2	Windows 2003 NTFS 特性	319
5.1.3	权限设置工具 CACLS 与权限复制工具 ROBOCOPY	322
5.1.4	Windows 2003 默认敏感目录及敏感程序路径	324
5.2	pcAnywhere 提权案例剖析	326
5.3	Serv-U 提权案例剖析	328
5.3.1	Serv-U 核心文件详解	329
5.3.2	Serv-U 加密原理分析与破解提权	329
5.3.3	使用 Serv-U 脚本提权剖析	332
5.3.4	使用 .NET 脚本进行提权剖析	333
5.4	SQL Server 提权案例剖析	335
5.4.1	SA 角色权限提升	335

5.4.2	DB_owner 角色权限提升技术	337
5.4.3	Public 角色提权技术	339
5.5	MySQL 自定义函数提权案例	341
5.6	Apache_Tomcat 提权案例剖析	343
5.7	Apache 提权案例攻防剖析	345
5.8	VNC 提权案例剖析	348
5.9	无法添加账户的攻防案例剖析	350
5.9.1	运用 DLLCACHE 进行攻防	350
5.9.2	利用 WSH 脚本宿主添加用户	352
5.9.3	通过账户“克隆”添加账户	353
5.9.4	密码策略对添加用户的影响	354
5.10	拒绝提权——拦住攻击者的黑手	355
5.10.1	常规安全加固	355
5.10.2	磁盘权限安全设置	356
5.10.3	系统敏感文件安全设置	357
5.10.4	修改终端端口号	358
5.10.5	启用 TCP/IP 筛选	358
5.10.6	IIS6.0 安全设置	359
5.10.7	防止木马袭击	360
5.10.8	为 IIS 单独配置一个账户	362
5.10.9	安全使用第三方软件	363
5.10.10	部署网警 110 安全防御软件	363

第 6 章 精通常见网络安全工具及技术 369

6.1	精通网络安全工具 NC	369
6.1.1	Netcat 简介与参数介绍	369
6.1.2	端口的监听与连接	369
6.1.3	端口扫描	370
6.1.4	绑定 CMD 发送	370
6.1.5	蜜罐欺骗攻防	371
6.1.6	NC 渗透网站案例攻防剖析	371
6.2	精通网络安全工具 MT	374
6.2.1	MT 简介与参数介绍	374
6.2.2	列出系统的详细信息	375
6.2.3	关闭 TCP/IP 筛选	375
6.2.4	查杀进程	376
6.2.5	查看程序调用哪些动态连接库	376
6.2.6	终端的检测安装与更改端口号	377
6.2.7	清除日志信息	377
6.2.8	下载功能	377
6.2.9	强制关机与注销和重新启动	377

6.2.10 查找本地管理密码	378
6.3 Windows 远程终端渗透攻防剖析	378
6.3.1 Windows XP 双开技术	378
6.3.2 Windows 2000 Server 终端开启技术	380
6.3.3 Windows Server 2003 终端开启	381
6.4 系统密码攻防技术剖析	383
6.4.1 Hash 基本知识介绍	383
6.4.2 Windows 系统 Hash 密码值的提取	384
6.4.3 使用 SAMInside 破解系统密码	385
6.4.4 使用 LC5 破解系统密码	386
6.4.5 彩虹表破解系统密码攻防	387
6.5 系统密码截获攻防	388
6.5.1 NTPass 显奇效	388
6.5.2 Tylogin 密码攻防利器	389
6.6 内网的攻防工具	391
6.6.1 内网端口转发攻防	391
6.6.2 美国黑帽子大会 reDuh 应用案例	392
6.7 精通网络安全工具 hijack	395
6.7.1 hijack 嗅探环境配置	395
6.7.2 hijack 参数详解	396
6.7.3 网络环境探测	396
6.7.4 实战之双向嗅探	397
6.7.5 实战之跨网段嗅探	398
6.7.6 实战之子网网速限制	398
6.7.7 实战之突破 IP 限制	398
6.7.8 实战之 http 数据包修改攻防	399
6.7.9 实战之 DNS 欺骗挂马攻防剖析	400
6.8 精通网络安全工具 PsTools	401
6.8.1 psexec.exe 远程命令执行	401
6.8.2 Psinfo 获取远程系统信息	402
6.8.3 pslist 远程进程查看	403
6.8.4 pskill 远程杀进程	403
6.8.5 psloggedon 查看用户正在使用计算 机资源的情况	404
6.8.6 psservice 控制服务	404
6.8.7 Pspasswd 更改账户密码	405
6.9 精通内网安全渗透工具 Metasploit Framework	406
6.9.1 安全渗透工具 Metasploit Framework	406
6.9.2 Metasploit Framework 安装与更新	406
6.9.3 Metasploit Framework 图形化界面 应用	407
6.9.4 Metasploit Framework 之命令行环境 应用	409
第 7 章 内网渗透防御攻略	411
7.1 内网拓扑结构介绍	411
7.1.1 拓扑结构	411
7.1.2 典型的内网拓扑结构	412
7.2 内网设备配置与路由渗透测试	413
7.2.1 路由器和交换机	413
7.2.2 内网设备配置案例	414
7.2.3 网络管理工具 SolarWinds 渗透 网络设备攻防	416
7.3 内网入口渗透攻防	417
7.3.1 利用 XSS 跨站漏洞进内网剖析	417
7.3.2 渗透 Citrix 服务器进内网剖析	418
7.3.3 渗透邮件系统进内网剖析	418
7.3.4 利用 VPN 进内网剖析	419
7.3.5 无线网络渗透	420
7.4 内网渗透攻防剖析	421
7.4.1 网络结构分析	421
7.4.2 内网扫描虚实	423
7.4.3 内网方案研究与渗透攻击剖析	423
7.5 内网渗透之 ARP sniffer 劫持嗅 探攻击剖析	427
7.5.1 ARP 的漏洞	427
7.5.2 ARP 欺骗的原理	427
7.5.3 驰骋疆场的 Cain 简介	427
7.5.4 当前网络环境判断	428
7.5.5 WinPcap_4_0 驱动包的安装	428
7.5.6 Cain 实际渗透应用剖析	429
7.6 内网渗透之 ARP 挂马攻击剖析	430
7.6.1 欺骗环境配置	430
7.6.2 模拟利用 zxarps 实施 ARP 欺骗 挂马	431
7.7 内网安全防御战之拒绝 ARP 攻击	432
7.7.1 准确定位攻击源	433
7.7.2 安全通甲 ARP 防火墙	434
7.7.3 铁血通甲 AntiARP-DNS 防火墙	437
7.8 内网安全解决方案经验谈	438
7.8.1 内网安全建设	438
7.8.2 安全域划分	439
7.8.3 各安全域安全措施	440



第1章 渗透攻防实践技术

1.1 命令行下的黑色艺术

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”，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。

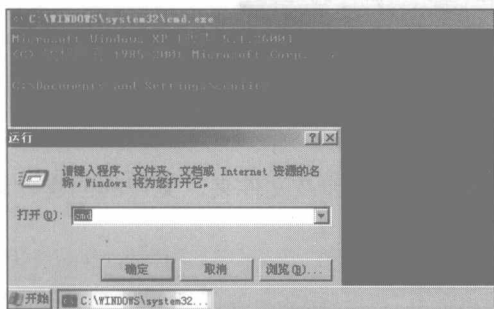


图 1-1 打开 DOS 操作界面 (1)

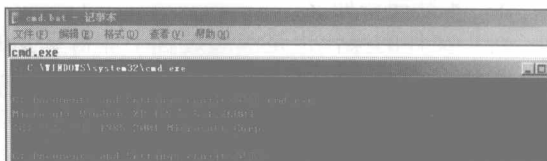


图 1-2 打开 DOS 操作界面 (2)

2. 目录转换命令

黑客入侵的过程中通常会在目标机上上传一些小工具，在 DOS 命令提示符下必须切换到

这里演示使用管道命令查看 boot.ini 文件信息，如图 1-6 所示。

这类命令在提权渗透中显得十分重要。

5. 查看和停掉系统服务

在提权过程中会反复查看系统服务的开启状态，利用服务名判断当前计算机运行了哪些应用软件，比如安装了什么杀毒软件、防火墙、数据库软件等。查看和停掉系统服务都要使用功能强大的 Net 命令，其基本使用格式如下：

Net start 查看所有系统服务
Net stop xxservice 停掉某个系统服务

显示当前系统服务列表，如图 1-7 所示。



由图 1-7 所示，发现当前系统运行了数据库软件 MySQL，如何将其停止呢？执行如下命令：

```
Net stop mysql
```

这样就成功停止了 MySQL 数据库服务器，如图 1-8 所示。

Windows XP 系统启动开始，系统都默认集合了 ICF 状态防火墙，这类防火墙有时候就会成为黑客们入侵的拦路虎，所以黑客必须将其关掉，关闭命令如下：

Net stop sharedaccess

这样就成功停止了防火墙，这时就可以登录远程桌面了，如图 1-9 所示。



Net 命令功能强大，后面还会继续介绍它的其他用法。

6. 网络连接查看

使用网络连接命令可查看到当前计算机开放的端口，常见的就是判断目标主机是否开启了 21、43958、3389 等端口，这些都是黑客在提权前要收集的信息。网络连接查看的命令是 Netstat，下面列出几种常见渗透用法：

```
Netstat -an 查看本地端口开放情况
Netstat -anb 查看本地端口开放情况及其可执行组件
Netstat -ano 查看本地端口开放情况及其连接相关的进程 id 号
```

现在查看本地端口开放情况及其可执行组件，如图 1-10 所示。

(1) Ping 192.168.1.1 判断网络是否畅通, 主要是根据返回的 TTL 值大致判断操作系统类型

(2) Ping www.syue.com 得到目标站点的 IP 地址

下面我们利用 Ping 命令测试“岁月联盟”官方主站的 IP 地址, 执行命令后成功地得到其 IP 地址, 如图 1-13 所示。

```
C:\>ping www.syue.com

Pinging www.syue.com [117.29.29.19] with 32 bytes of data:

Reply from 117.29.29.19: bytes=32 time=26ms TTL=62
Reply from 117.29.29.19: bytes=32 time=34ms TTL=62
Reply from 117.29.29.19: bytes=32 time=26ms TTL=62
Reply from 117.29.29.19: bytes=32 time=34ms TTL=62

Ping statistics for 117.29.29.19:
    Packets: Sent = 4, Received = 4, Loss = 0.0%, Time = 114ms
    Approximate round trip times in milliseconds:
        Minimum = 26ms, Maximum = 34ms, Average = 29ms
```

图 1-13 得到的 IP 地址

9. 网络环境查看

在得到一定权限后可对目标主机所处的网络环境进行查看, 搞清楚是内网还是外网, 网关和 DNS 服务器 IP 地址等。这些都非常重要, 对于内网服务器可使用端口转发技术连接目标主机的远程桌面或者其他端口。网络环境查看的命令:

Ipconfig /all

当前网络环境如图 1-14 所示。

```
C:\>ipconfig /all

Windows IP Configuration

Ethernet adapter Local Area Connection 2:
    Media State . . . . . : Media disconnected
    . . . . .
    IP Address . . . . . : 192.168.1.100
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . : 192.168.1.1
    DNS Servers . . . . . : 192.168.1.1
    NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter Local Area Connection:
    Media State . . . . . : Media disconnected
    . . . . .
    IP Address . . . . . : 192.168.1.101
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . : 192.168.1.1
    DNS Servers . . . . . : 192.168.1.1
    NetBIOS over Tcpip. . . . . : Enabled

Wireless LAN adapter Wireless Network Connection:
    Media State . . . . . : Media disconnected
    . . . . .
    IP Address . . . . . : 192.168.1.102
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . : 192.168.1.1
    DNS Servers . . . . . : 192.168.1.1
    NetBIOS over Tcpip. . . . . : Enabled
```

图 1-14 当前网络环境

10. 内网渗透命令 Net View

Net View 显示正由指定的计算机共享的域、计算机或资源的列表。如果在没有参数的情况下使用, 则 Net View 显示当前域中的计算机列表。这个命令在内网渗透过程中用得很多, 它可以列出一些当前计算机的资源列表。可以查看到哪些共享计算机在线, 如图 1-15 所示。

11. 网络命令 Telnet

Telnet 是微软公司提供给系统管理员维护远程计算机使用的命令, Telnet 所使用的通信端口是 23。用这种方式远程登录计算机, 在网络中数据的传输是明文的形式, 也就是口令没有经过加密, 因此很容易受到黑客的攻击。如果一个黑客在中间监听, 你的密码很轻松地被黑客获得。所以它及其不安全, 除非把它做加密传输。现在很多系统维护管理员都放弃使用 Telnet 了, 一般都用 SSH 远程登录, 因为它是加密传输的。在 Windows VISTA 系统中, 都已

经取消了这条命令。虽然使用得少，但是对黑客来说还是很有用的，使用它可以手工探测目标主机的端口开放情况，这也是个技巧。在有些网络环境下不适合用大型扫描软件，因为容易被管理员发现。

使用 Telnet 命令登录远程系统，命令格式如下：

```
Telnet 10.4.31.96
```

正确输入完密码后即可成功登录，执行任意系统命令，如图 1-16 所示。



图 1-15 在线共享计算机

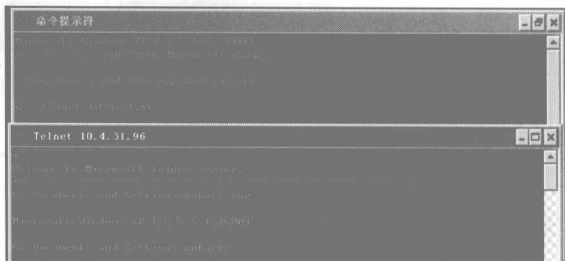


图 1-16 登录远程系统

利用 Telnet 探测端口开放其实就是以 Telnet 方式去请求一个端口，如果该端口没有开放，返回信息会显示“XX 端口无法打开”，如果能够连接则说明该端口开放，使用格式如下所示：

```
Telnet 218.XX.XX.255 Portnumber
```

另外，如果计算机中有防火墙的阻挡，也是不能请求目标端口。

12. 渗透命令中用户权限查看

判断当前用户权限在渗透提权中是非常重要的，如果当前用户是系统权限，那么黑客将很快攻陷这台主机。有的管理员对操作系统不熟悉，配置计算机管理权限不得方法，这就给黑客留下了可乘之机。查看当前用户权限主要使用命令 `whoami`，如图 1-17 所示。

由图 1-17 所示可知，当前用户属于管理员权限。另外，一般黑客拿到 WebShell 后会查找第三方软件漏洞来提权，但是很多攻击者都忽略了系统本身权限，这也是渗透的技巧。

13. 渗透命令中路由跟踪

`tracert` 这个命令检测你的计算机经几个路由中转到目的地 IP 的命令，也就是实现路由跟踪。这个命令在嗅探渗透的时候用得最多，用它来判断本机和目标机是否处在同一交换机下，如果是就可以用来发起嗅探和 ARP 攻击，截取敏感的数据，比如嗅探 FTP MSSQL MySQL 等密码口令，使用格式如下所示：

```
tracert 192.x.x.1
```

查看某台主机是否与当前主机位于同一网关下，执行 `tracert` 命令，如图 1-18 所示。



图 1-17 用户权限查看



图 1-18 路由跟踪命令

这样就可以利用 ARP 嗅探攻击了。