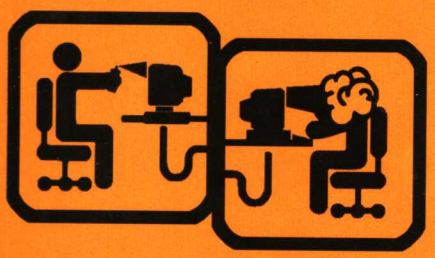
电脑迷 荣誉出品

网安天才少年 王胤辰（台湾）
信息安全资深作者 CC_long
联合编著

黑客招数大PK
任务实战



查找、锁定目标计算机的IP、开放端口及漏洞

寻找、判断、歼灭木马、恶意/间谍程序、傀儡/僵尸程序、后门、跳板、蠕虫、病毒

账户、文件有效破解·邮件、IM攻防大作战

真实记录黑客任务，场景再现系统入侵、密码破解、木马攻陷.....

资深黑客踩点、隐藏IP，探询目标主机

Cookie欺骗、IE炸弹、恶意网页……制作与防护

木马加壳、加花免杀捆绑、潜入、引爆

Telnet、FTP、终端机服务打开后门自由操纵

139、145、3389……端口直接入侵实战演练

局域网监听、嗅探、伪IP、ARP攻击……

远程溢出入侵的技巧与盲点

WEP与WPA加密保护，黑客使用无线基地台方法大曝光

网页钓鱼法和蜜罐手法之攻与防，弱者和强盗的陷阱之战

完美消除入侵痕迹5大方式

齐鲁電子音像出版社

网安天才少年 王胤辰（台湾）
信息安全资深作者 CC_LONG 联合编著

黑客招数大PK

任务实战

齐鲁電子音像出版社

名　　称：黑客招数大PK——任务实战
策　　划：彭　葵
编　　著：王胤辰 CC_long
责任编辑：于　溪
监　　制：林国刚
组版编辑：卓　娟
光盘制作：史　祺
封面设计：汤　立

出版单位：齐鲁电子音像出版社
技术支持：（023）63658888-13101

发　　行：重庆中科普传媒发展股份有限公司发行部
电　　话：（023）63658888-13138
传　　真：（023）63659779
经　　销：各地新华书店、报刊亭
邮购地址：400013
邮购询问：（023）63658888-13126
光盘生产：苏州新海博数码科技有限公司
文本印刷：重庆升光电力印务有限公司
开本规格：787×1092毫米 1/16　18印张 250千字

版本号：ISBN 978-7-900433-43-5
版　　次：2008年1月第1版
定　　价：29.80元（1CD＋手册）

光盘导读

特别说明

本光盘提供的黑客软件演示仅供研究使用，切勿利用来破坏他人的计算机或数据，否则一切后果自负。

点击任意视频按钮，即可直接播放界面列表中的黑客教学视频。

为什么购买

首先声明

全书从技术分析角度出发，对黑客的每个攻击入侵方法和所有实例都进行了测试，全部可以实现和做到，但，害人之心不可有，读者诸君切勿将本书内容用于任何违法行为，否则一切法律责任自负！

2000年，年仅**15**岁的**MafiaBoy**在**2**月**6**日到**2**月**14**日情人节期间成功侵入包括**eBay**，**Amazon**和**Yahoo**在内的大型网站服务器，成功阻止了服务器向用户提供服务，同年被捕。

很多我们认为不可思议的技术正被越来越年轻的黑客所掌握。你知道上网时，有多少黑客正在浏览你计算机里的重要数据吗？随着黑客工具的传播，稍微有点计算机知识的人，就能对你进行攻击，而我们的目的就在于完全从技术角度出发再现黑客各种入侵的思路和操作方法，让你能知己知彼，把控好自己的电脑“大门”。

本书由台湾网安天才兼网安图书策划人王胤辰和实战经验丰富的黑客雇佣军**CC_long**联合编写。

适用读者：

懂一点网络知识的电脑用户。

目录

Part 1
黑客攻击手法大公开

黑客如何收集目标系统信息 2
如何分析和挖掘弱点信息 4
黑客如何获取目标使用权限 5
黑客如何开辟后门 6
如何进行简单的黑客攻击防范 7
黑客攻击类型有哪些 15
什么是入侵系统类攻击 15
如何实施欺骗类攻击 16
如何实施拒绝服务攻击 18
如何攻击防火墙 18

Part 2
查找、锁定目标计算机的IP、开放端口及漏洞

如何由网址查找IP地址 22
黑客如何通过电子邮件查看发送者的IP 24
黑客如何查找远程局域网用户的IP 25
黑客如何用珊瑚虫版QQ得到聊天用户IP 28
如何定位对方的真实地理地址 29
如何利用Angry IP Scanner检测IP状态 30
如何由IP得到目标主机的地理位置 32
如何进行网站基本信息查询 33
如何进行结构探测 34
什么是代理服务器 36
如何获得免费的代理服务器 37
如何验证匿名代理的等级 41
如何使用代理超人验证代理的等级 42
如何使用代理隐藏IP 43
什么是端口 46
Windows系统常用端口有哪些 47
如何关闭Windows常见开放端口 49
如何查找开放端口 57
Windows系统常见漏洞有哪些 60
如何扫描目标计算机的漏洞 64

Part 3
Windows攻防之无孔不入

哪些目标最适合使用Windows直接入侵 74
Windows直接入侵的详细流程与步骤 74
直接入侵遇到的问题与解决方法 78
还有哪些方法可以入侵Windows电脑 79

怎样将没有共享的电脑磁盘共享出来 82
利用注册表把电脑磁盘共享出来 84
将需要输密码的磁盘改为点击即可进入 84
防止黑客利用注册表将磁盘设置为共享 84
利用默认共享漏洞入侵 86
对方已将默认共享彻底关闭，如何打开 88

NT/2K/XP的用户名与密码所藏地及破解 89
如何快速猜到磁盘共享用户名和密码 93
如何有效防止黑客猜中磁盘共享密码 94

目标机的磁盘只能读，如何更改为可读写 96

如何在别人的系统中获取最高权限账户 96

如何找出有FTP服务的电脑 100
如何让Win2K/XP电脑提供Telnet服务 102
如何防止黑客利用Telnet服务入侵 103

如何向网络上任一Windows电脑发恐吓信 104
如何假冒他人给任一Windows电脑发消息105

如何让自己的电脑不再收到垃圾信息 106

黑客在别人的电脑中通常会有哪些操作 108
防范黑客在你的电脑中建账户与开Telnet 108

如何查看、修改与删除他人电脑的注册表111
如何防止黑客查看、更改或删除我的注册表 112

哪些方法可以获取别人的上网密码 113

Cookies文件中可能包含哪些信息 114

如何获取Cookies中进入某些网站的账户 114
如何有效防止黑客获取我的Cookies文件 117

如何破解压缩文件的密码 118
如何尽可能防止压缩文件的密码被破解 118
如何破译各版本Office文件的密码 118
找出与使用CuteFTP的所有FTP账户 125
如何有效防范FTP账户被黑客窃取使用 127

如何在连接网络时将重要文件夹隐藏 128
防止黑客利用at命令运行你电脑中的程序 129

Part 4

全新木马、恶意或间谍程序、傀儡或僵尸程序、后门程序、跳板程序、蠕虫、病毒……寻找、判断、歼灭

什么是木马文件 132
木马是怎样启动的 132
如何利用共享和Autorun文件植入木马 135
如何把木马文件转换为BMP格式 136
如何在Office文档中加入木马文件 138
如何给木马服务端程序更名 138
如何把木马程序和其它文件捆绑 138
如何查找已经安装有木马的电脑 141
如何建立目标计算机木马的连接 143
如何利用端口型BO2K木马控制电脑 144
如何检测和清除BO2K 146
黑客如何利用网络公牛实现木马攻击 146
如何检测和清除网络公牛 152
如何利用冰河查看对方屏幕 153
如何利用冰河查看对方任务管理器 155
如何清除及防范冰河木马 155
如何创建“黑洞”服务端安装程序 156
如何使用黑洞2007的Telnet功能 157
如何清除黑洞 158
利用灰鸽子通过3389端口入侵 158
如何清除灰鸽子 164
如何利用进程查看端口号 166
如何根据端口号查进程 167
如何防范ICMP被利用 167
如何防范IE执行恶意程序 168
什么是IE炸弹 170
如何制作死循环炸弹 170
如何制作超大图片炸弹 171
如何制作格式化硬盘的炸弹 171
如何防范IE炸弹 172
如何实现Cookie欺骗 173
实现本地可执行程序漏洞的利用 179
如何利用CHM文件进行攻击 180
防范chm帮助文件执行任意程序 183
如何管理IE插件 185
什么是恶意网页修改 187
浏览器不能打开新窗口 188
如何恢复IE默认首页 189
防止儿童看到网页上的不健康信息 190
如何设定安全等级防止恶意网站 191
如何屏蔽特定网页 191
如何利用网页中的代码修改注册表 192
如何消除网页恶意代码的影响 194
如何利用网络资源查找病毒 195

Part 5
电子邮件、IM攻防大战

破解或窃取电子邮件账户（含Web-Mail） 198
破解或获取Outlook的用户名与密码 202
如何防止邮件账户的密码被黑客获取 209
如何对某个电子信箱进行邮件炸弹攻击 209
如何发黑信，并让对方无法知晓 211
如何将窗口炸弹送到对方电脑中 212
窗口炸弹对Windows系统的破坏与影响 212
如何避免受到窗口炸弹的攻击 213
如何解决打开信件程序后不断冒出的窗口 214

Part 6
服务器入侵攻防

服务器Unicode漏洞攻防 216
怎么扫描Unicode漏洞 216
黑客们是怎么利用Unicode漏洞攻击的 220
如何防范Unicode漏洞攻击 224
IIS写权限攻击及防范 226
缓冲区溢出攻防 231
什么是DDoS攻击 236
利用MS SQL入侵 236
入侵者在入侵成功后都会做些什么 242
怎么利用SQL注入攻击 243
怎么进行SQL注入攻击 244
怎么发送电子邮件来钓鱼 246

Part 7
另类安全防黑手法

黑客为什么会对日志文件感兴趣 250
怎么在Windows系统中利用安全日志 250
天网日志分析实例 258
如何拒绝笔记本ad-hoc方式接入 263
如何设置WEP及WPA加密保护 269
怎么隐藏无线基地台（SSID） 275
怎么利用DHCP的IP地址策略进行防范 275
用AirCrack进行WEP加密破解 277

PART 1
黑客攻击手法大公开

黑客在进行攻击时通常有个习惯性的流程：首先搜寻到目标信息系统，然后找到目标信息系统的弱点，并利用弱点获得权限开辟后门，最后对痕迹进行清除。

信息的收集并不对目标系统产生危害，只是为进一步的入侵提供有用信息。这些信息主要包括目标的操作系统类型及版本，目标提供哪些服务，各服务器程序的类型与版本以及相关的信息等。

要攻击一台机器，首先要确定它正在运行的操作系统版本。因为不同类型的操作系统其系统漏洞有很大区别，攻击的方法也完全不同，甚至同一种操作系统的不同版本的系统漏洞也不一样。要确定一台服务器的操作系统一般是靠经验，有些服务器的某些服务显示信息会泄露其操作系统。

方法1：利用Telnet命令

【案例】利用Telnet登录一台IP地址为202.115.30.134的Linux服务器。

如果用户是在Windows的环境下，想对远程的Linux系统进行操作，推荐选择“telnet”的方式进行登录，具体步骤如下：

第1步 启动Windows操作系统，单击执行“开始”→“运行”命令。

第2步 在弹出的“运行”对话框中输入“telnet+远程Linux系统IP地址”，例如：telnet 202.115.30.134。

第3步 弹出“**Red Hat Linux**”界面，输入用户名和密码后，即可像在本机一样进行命令行的操作了。从图中可以得知该版本为**Red Hat Linux release 9**。

```
Red Hat Linux release 9 (Shrike)
Kernel 2.4.20-8 on an i686
login: chen
Password:
Last login: Tue Apr  3 03:01:16 from 202.115.30.135
[chen@localhost chen]$
```

注意

这样确定操作系统类型是不准确的，因为有些网站管理员为了迷惑攻击者会故意更改显示信息，造成假象。

方法2：查询DNS的主机信息

还有一种不是很有效的方法，诸如查询DNS的主机信息（不是很可靠）来看登记域名时的申请机器类型和操作系统类型，或者利用某些主机开放的SNMP的公共组来查询。

小知识

SNMP是专门用于管理网络节点（服务器、工作站、路由器、交换机及 HUBS 等）的一种标准协议，它是一种应用层协议。SNMP能让网络管理员管理网络，发现并解决网络问题以及规划网络增长。通过SNMP接收随机消息（及事件报告）网络管理系统获知网络出现的问题。

获知目标提供哪些服务及各服务的daemon类型、版本同样重要，因为已知的漏洞一般都是针对某一服务的。

小知识

这里说的服务就是指通常提到的端口，例如Telnet对应23端口，FTP对应21端口，WWW对应80端口或8080端口，这只是一般情况，网站管理员完全可以按自己的意愿修改服务所监听的端口号。在不同服务器上提供同一种服务的软件也可以不同，我们管这种软件叫daemon，例如同样是提供FTP服务，可以使用wuftp、proftp，ncftp等许多不同种类的daemon。确定daemon的类型版本也有助于黑客利用系统漏洞攻破网站。

另外需要获得的关于系统的信息就是一些与计算机本身没有关系的社会信息，例如网站所属公司的名称、规模，网络管理员的生活习惯、电话号码等。这些信息看起来与攻击一个网站没有关系，实际上很多黑客都是利用了这类信息攻破网站的。例如有些网站管理员用自己的电话号码做系统密码，如果掌握了该电话号码，就等于掌握了管理员权限。进行信息收集可以用手工进行，也可以利用工具来完成，完成信息收集的工具叫做扫描器。用扫描器收集信息的优点是速度快，可以一次对多个目标进行扫描。

在收集到一些准备要攻击目标的信息后，黑客们会探测目标网络上的每台主机，来寻求系统内部的安全漏洞，这些信息即所谓的弱点信息，主要探测的方式如下：

自编程序

往往网上会发布一些操作系统的新安全漏洞，一旦用户不重视或一时疏忽未打上该系统的“补丁”程序，那么黑客就可以自己编写一段程序进入到该系统进行破坏。

慢速扫描

由于一般扫描侦测器的实现是通过监控某个时间段内一台特定主机发起的连接数来判断是否被扫描，这样黑客可以通过使用扫描速度慢的扫描软件进行扫描。

体系结构探测

黑客利用一些特殊的数据包传送给目标主机，使其做出相对应的响应。由于每种操作系统的响应时间和方式都是不一样的，黑客利用这种特征把得到的结果与准备好的数据库中的资料相对照，从中便可轻而易举地判断出目标主机操作系统所用的版本及其他相关信息。

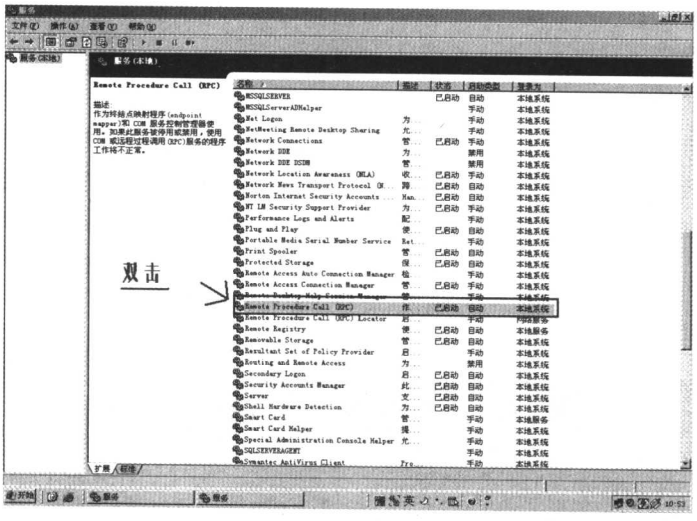
获得权限

TIPS： **当收集到足够的信息之后，攻击者就要开始实施攻击行动了。如果是破坏性攻击，只需利用工具发动攻击即可。如果是入侵性攻击，则往往要利用收集到的信息，找到其系统漏洞，然后利用该漏洞获取一定的权限。**

有时获得了一般用户的权限就足以达到修改主页等目的了，但作为一次完整的攻击是要获得系统最高权限的，这不仅是为了达到一定的目的，更重要的是证明攻击者的能力，这也符合黑客的追求。

能够被攻击者所利用的漏洞不仅包括系统软件设计上的安全漏洞，也包括由于管理配置不当而造成的漏洞。

当然大多数攻击成功的范例还是利用了系统软件本身的漏洞。造成软件漏洞的主要原因在于编制该软件的程序员缺乏安全意识。当攻击者对软件进行非正常的调用请求时造成缓冲区溢出或者对文件的非法访问。其中利用缓冲区溢出进行的攻击最为普遍，如下图所示为针对微软的RPC漏洞进行病毒攻击。



无论作为一个黑客还是一个网络管理员，都需要掌握尽量多的系统漏洞。黑客需要用它来完成攻击，而管理员需要根据不同的漏洞来采取不同的防御措施。

㊑ 权限的扩大

系统漏洞分为远程漏洞和本地漏洞两种，如采用Norton杀毒软件漏洞扫描功能获取的系统安全漏洞的信息。远程漏洞是指黑客可以在别的机器上直接利用该漏洞进行攻击并获取一定的权限。这种漏洞的威胁性相当大，黑客的攻击一般都是从远程漏洞开始的。但是利用远程漏洞获取的不一定是最高权限，而往往只是一个普通用户的权限，这样常常没有办法做黑客们想要做的事。这时就需要配合本地漏洞来把获得的权限进行扩大，常常是扩大至系统的管理员权限。

只有获得了最高的管理员权限之后，才可以做诸如网络监听、打扫痕迹之类的事情。完成权限的扩大，不但可以利用已获得的权限在系统上执行利用本地漏洞的程序，还可以放一些木马之类的欺骗程序来套取管理员密码，这种木马是放在本地套取最高权限用的，而不能进行远程控制。

通常对主机进行了分析后，对它的弱点已经了如指掌，选一个适合这台主机的后门，然

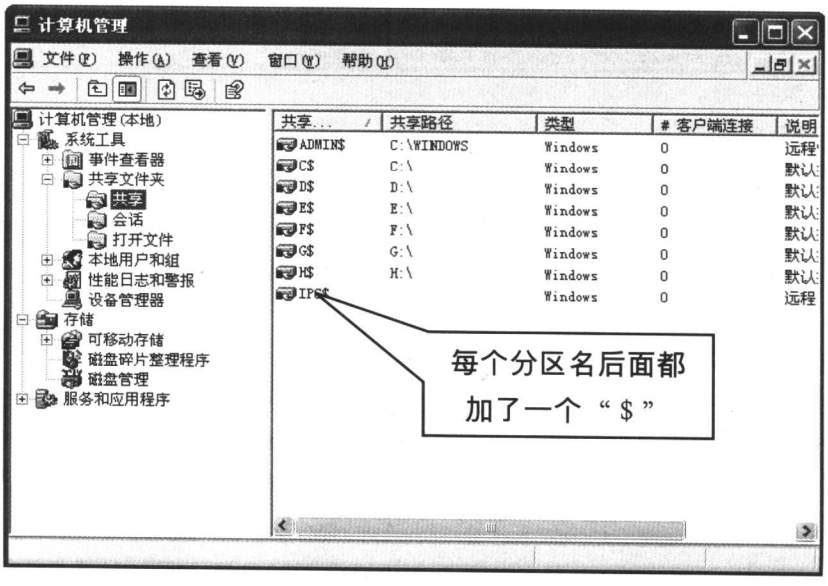
后上传，这里要注意后门的取名和开口（或ping后门）。在主机上装上后门后，一定要与主机断开ipc连接，不然会在会话中留下记录。

再通过后门上传你要用到的程序，比如做代理的、扫描的、sniffer的软件等，放这些程序目录最好是放深一点，名字取得好听一些，也可用软件把它隐藏了。假设我们发现这台主机上没有查杀sniffer的软件，那么就可以给它装上一个sniffer，来监听FTP/POP3等明文传输密码。如果主机还开着web服务，还可以给它装上一个脚本木马，脚本木马如果放得好的话，检测难度非常大，而管理员在做web备份的时候，也会把它备份进去，一个好的asp木马可以完全接管一台NT操作系统。然后把主机上有用的文件全部下载下来，如web程序的数据库连接代码里会有数据库用户名和口令信息。

既然黑客攻击如此危险且具有隐蔽性，应该“防患于未然”，清除所有的隐患，这里介绍几个简单的办法：

㊀ 取消文件夹隐藏共享

在默认状态下，Windows 2000/XP会开启所有分区的隐藏共享，从“控制面板”→“管理工具”→“计算机管理”窗口下展开选择“系统工具”→“共享文件夹”→“共享”命令，就可以看到硬盘上的每个分区名后面都加了一个“$”。

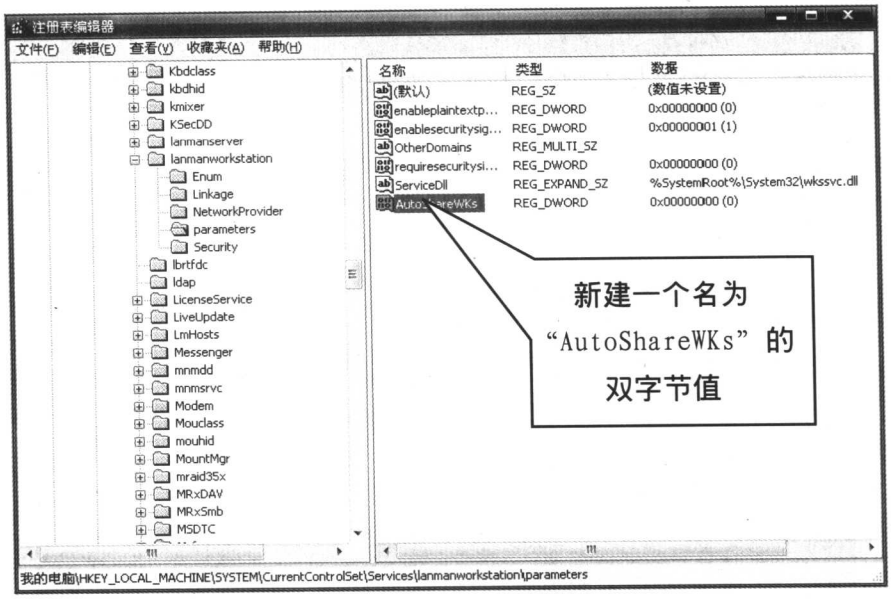


只要键入“计算机名或者IPC$”，系统就会询问用户名和密码，但是由于大多数个人用户系统Administrator的密码都为空，入侵者可以轻易看到C盘的内容，这就给网络安全带来了极大的隐患。

消除默认共享的具体方法如下：

第1步 单击执行“开始”→“运行”命令，打开“运行”对话框，在方框中输入“regedit”，打开“注册表编辑器”窗口。

第2步 展开“HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Sevices/Lanmanworkstation/parameters”，新建一个名为“AutoShareWKs”的双字节值，并将其值设为“0”，然后重新启动电脑，这样共享就取消了。



④ 拒绝恶意代码

一般恶意网页都是因为加入了恶意代码才有破坏力的。这些恶意代码就相当于一些小程序，只要打开该网页就会被运行。所以要避免恶意网页的攻击只要禁止这些恶意代码的运行就可以了。

第1步 运行IE浏览器。

第2步 单击执行“工具→Internet选项”命令，打开“Internet选项”对话框，选择“安全”选项卡，并单击“自定义级别”按钮，弹出“安全设置”对话框，将安全级别定义为“安全级-高”，将“ActiveX控件和插件”中第1、3项设置为“禁用”，其它项设置为“提示”。