随手查

电脑迷 荣誉出品

黑客攻击秘技

罗盘工作室 著

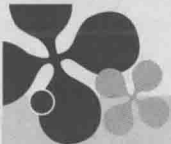
- 最完整的密码破解教程
- 最全面的入侵必用命令
- 最详实的网络攻击实例
- 光盘具互动教学功能

山东电子音像出版社出版

随手查

黑客攻击秘技

山东电子音像出版社出版



书　　名：黑客攻击秘技随手查
策　　划：《电脑迷》张 洁 蒲 涛
编　　著：罗盘工作室
责任编辑：刁 戈
执行编辑：刘 恒 胡小茜 彭 葵 王 莹
封面设计：刘 勤
组版编辑：唐荣檥

出版单位：山东电子音像出版社
地　　址：济南市胜利大街39号
邮　　编：250001
电　　话：（0531）2060055－7616
技术支持：（023）63658888－10112

发　　行：山东电子音像出版社
经　　销：各地新华书店、报刊亭
CD 生产：苏州新海博数码科技有限公司
文本印刷：重庆华林天美印务有限公司
开本规格：787×1092毫米 1/32 印张8

版本号：ISBN 978 7-89491-926-7
版次：2007年3月第1版
定价：10元（1CD+手册）

为什么购买此书

首先声明：本书从技术角度出发，对黑客的攻击入侵方法和所有实例都进行了详细剖析与分解。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！

上网大家都会，但对网络安全防护的认识却是相当的匮乏。QQ密码、游戏账号被盗，网上交易被偷窥，电脑文件被窃取这些不幸的事时常在我们周围发生。针对这些问题，本书披露了黑客攻击的全过程，在助你知己知彼的同时，还能给予攻击者有力的反击，以保个人电脑的安全。

光盘内容：

5大黑客主题教学视频
黑客常用攻击工具
精选网络安全防护工具
光盘独有启动查毒、杀毒功能

本书特色：

内容实用，通俗易懂，入门上手快
精致小开本，便于携带，随查随用

[光盘导读]

光盘使用说明

将本光盘放入电脑光驱中，光盘会自动运行。如没有自动运行，可以打开“我的电脑”，用鼠标右键单击光驱所在盘符，在弹出菜单中选择“自动播放”即可。

本光盘内置江民杀毒伴侣及电脑迷装机工具包，在光盘启动模式下具有查毒、杀毒、磁盘格式化、分区等功能。

光盘界面说明

黑客教学视频

该页面为教学视频导航界面。单击五个分类下的各个按钮，程序将弹出视频播放框，播放相对应的教学视频。

工具软件

在该页面中，左侧为软件浏览框，分为“黑客工具”与“安全工具”两大类。右侧分别为软件截图与软件说明。通过右下角的“浏览”与“安装”按钮，分别可以找到该软件在光盘中的位置和安装该软件。

光盘文件索引

黑客入门　　视频教学\黑客入门

文件上传终极方案.exe
net命令应用详解.exe
跳板的简单使用.exe
代理跳板的使用详解.exe
radmin服务端的设置.exe

端口扫描　　视频教学\端口扫描

sss演示.exe
流光.exe
X-scanner扫描器.exe
SuperScan 3.0使用教程.exe

破解技巧　　视频教学\破解技巧

暴力破解信箱.exe
使用x-way进行邮箱密码破解.exe

网络入侵　　视频教学\网络入侵

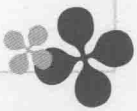
“完美”后门入侵生成视频.exe
ipc攻击演示.exe
IIS CGI文件名错误解码漏洞入侵.exe
通过Serv-u入侵.exe
sql2入侵实例.exe

木马技巧　　视频教学\木马技巧

对灰鸽子的详细解剖1.exe
对灰鸽子的详细解剖2.exe
对灰鸽子的详细解剖3.exe
木马新藏身处.exe

黑客常用工具　　黑客软件\黑客工具

溯雪 Beta7
HostScan
IP炸弹
Sqldict
QICQ密码轻松盗
ProxyHunter
Pspv



QQ万能发送精灵
QQ远控精灵
SuperScanV4.0-RHC
WinShell 5.0
阿拉丁UDP洪水攻击器v2.1
灰鸽子[牵手2004]
流光

安全工具　　黑客软件\安全工具

IE优化修复专家2006 v6.30豪华版
QQ密码防盗专家
Windows清理大师v0.12
超级兔子魔法设置v7.76
木马克星
木马猎手pclxavins
天网防火墙 Build 0808 试用版
文件加密器v8.4

声明：

本光盘所收录的黑客软件仅供研究使用，切勿利用来破坏他人的计算机或数据，否则一切后果自负！本光盘但因收录有黑客程序，所以在运行光盘时某些杀毒软件会报警。

[目　录]

第一章 黑客入门

第二章 密码破解

第四章 木马攻击

第五章 网络攻击

第一章 黑客入门

黑客又名hacker，是一群喜欢用智力通过创造性方法来挑战脑力极限的人，特别是他们所感兴趣的领域。本章我们来认识一下黑客，看看他们是怎样“黑”掉别人电脑的。

1.1 黑客攻击解密

Skill 1：黑客攻击流程解密

黑客们的性格千奇百怪，但是他们攻击别人的步骤无外乎就是那几样，下面我们来看黑客们最常用的攻击步骤。

（1）给自己隐身

普通攻击者都会利用别人的电脑隐藏他们真实的IP地址。老练的攻击者还会利用800电话的无人转接服务联接ISP，然后再盗用他人的账号上网。这也是一个最基本的手段，攻击别人，肯定先要隐藏自己，以免被别人发现。

（2）寻找目标主机

攻击者首先要寻找目标主机并分析目标主机。在Internet上能真正标识主机的是IP地址，域名是为了便于记忆主机的IP地址而另起的名字，只要利用域名和IP地址就可以顺利地找到目标主机。当然，知道了要攻击目标的位置还是远远不够的，还必须将主机的操作系统类型及其所提供服务等资料作个全面的了解。此时，攻击者们会使用一些扫描器工具，轻松获取目标主机运行的操作系统、系统账户、服务器程序是何种版本等资料，为入侵作好充分的准备。

（3）登录主机

攻击者要想入侵一台主机，首先要有该主机的一个账号和密码，否则连登录都无法进行。这样常迫使他们先设法盗窃账户文件，进行破解，从中获取某用户的账户和口令，再寻觅合适时机以此身份进入主机。当然，利用某些工具或系统漏洞登录主机也是攻击者常用的一种方法。

（4）控制目标主机

攻击者们用FTP、Telnet等工具通过系统漏洞进入目标主机系统获得控制权之后，就会做两件事：清除记录和留下后门。他会更改某些系统设置，在系统中置入特洛伊木马或其他一些远程操纵程序，以便日后可以不被觉察地再次进入系统。大多数后门程序是预先编译好的，只需要想办法修改时间和权限就可以使用了，甚至新文件的大小都和原文件一模一样。攻击者一般会使用rep传递这些文件，以便不留下FTB记录。通过清除日志，删除拷贝的文件等手段来隐藏自己的踪迹之后，攻击者就开始下一步的行动。

（5）夺取网络资源和特权

攻击者找到攻击目标后，会继续下一步的攻击。如：下载敏感信息；实施窃取账号密码、信用卡号等经济偷窃；使网络瘫痪等。

Skill 2：黑客攻击常用方法详解

上面我们简单的了解了黑客一般的攻击流程，下面我们来详细了解下黑客攻击的常用手段。

（1）口令入侵

所谓口令入侵是指使用某些合法用户的账号和口令登录到目的主机，然后再实施攻击活动。这种方法的前提是必须先得到该主机上的某个合法用户的账号，然后再进行合法用户口令的破译。获得合法用户账号的方法很多，如：

利用目标主机的Finger功能：当用Finger命令查询时，主机系统会将保存的用户资料（如用户名、登录时间等）显示在终端或计算机上。

利用目标主机的X.500服务：有些主机没有关闭X.500的目录查询服务，也给攻击者提供了获得信息的一条简易途径。

从电子邮件地址中收集：有些用户电子邮件地址常会透露其在目标主机上的账号。

查看主机是否有习惯性的账号：有经验的用户都知道，很多系统会使用一些习惯性的账号，造成账号的泄露。

（2）放置特洛伊木马程序

特洛伊木马程序可以直接侵入用户的电脑并进行破坏，它常被伪装成

工具程序或者游戏等，诱使用户打开带有特洛伊木马程序的邮件附件或从网上直接下载，一旦用户打开了这些邮件的附件或者执行了这些程序之后，它们就会像特洛伊人在敌人城外留下的藏满士兵的木马一样留在自己的电脑中，并在自己的计算机系统中隐藏一个可以在Windows启动时悄悄执行的程序。当用户连接到因特网上时，这个程序就会通知攻击者，报告IP地址以及预先设定的端口。攻击者在收到这些信息后，再利用这个潜伏在其中的程序，就可以任意地修改计算机的参数设定、复制文件、窥视你整个硬盘中的内容等，从而达到控制你的计算机的目的。

（3）WWW的欺骗技术

在网上，用户可以利用IE等浏览器进行各种各样的WEB站点的访问，如阅读新闻组、咨询产品价格、订阅报纸、电子商务等。然而一般的用户恐怕不会想到有这些问题存在：正在访问的网页已经被黑客篡改过，网页上的信息是虚假的！例如黑客将用户要浏览的网页的URL改写为指向黑客自己的服务器，当用户浏览目标网页的时候，实际上是向黑客服务器发出请求，那么黑客就可以达到欺骗的目的了。

一般Web欺骗使用两种技术手段，即URL地址重写技术和相关信息掩盖技术。利用URL地址，使这些地址都指向攻击者的Web服务器，即攻击者可以将自己的Web地址加在所有URL地址的前面。这样，当用户与站点进行安全链接时，就会毫不防备地进入攻击者的服务器，于是所有信息便处于攻击者的监视之中。但由于浏览器一般设有地址栏和状态栏，当浏览器与某个站点连接时，可以在地址栏和状态栏中获得连接中的Web站点地址及其相关的传输信息，用户由此可以发现问题，所以攻击者往往在URL地址重写的同时，利用相关信息技术，即一般用JavaScript程序来重写地址，以达到其欺骗的目的。

（4）电子邮件攻击

电子邮件是互联网上运用得十分广泛的一种通讯方式。攻击者可以使用一些邮件炸弹软件或CGI程序向目的邮箱发送大量内容重复、无用的垃圾邮件，从而使目的邮箱被撑爆而无法使用。当垃圾邮件的发送流量特别大时，还有可能造成邮件系统反应缓慢甚至瘫痪。相对于其他的攻击手段来说，这种攻击方法具有简单、见效快等优点。

电子邮件攻击主要表现为两种方式：

电子邮件轰炸和电子邮件“滚雪球”。也就是通常所说的邮件炸

弹，指的是用伪造的IP地址和电子邮件地址向同一信箱发送数以千计、万计甚至无穷多次的内容相同的垃圾邮件，致使受害人邮箱被“炸”，严重者可能会给电子邮件服务器操作系统带来危险，甚至瘫痪。

电子邮件欺骗。攻击者佯称自己为系统管理员（邮件地址和系统管理员完全相同），给用户发送邮件要求用户修改口令（口令可能为指定字符串）或在貌似正常的附件中加载病毒或其他木马程序。

（5）通过一个节点来攻击其他节点

攻击者在突破一台主机后，往往以此主机作为根据地，攻击其他主机(以隐蔽其入侵路径，避免留下蛛丝马迹)。他们可以使用网络监听方法，尝试攻破同一网络内的其他主机；也可以通过IP欺骗和主机信任关系，攻击其他主机。

这类攻击很狡猾，但由于某些技术很难掌握（如TCP／IP欺骗攻击），因此攻击者通过外部计算机伪装成另一台合法计算机来实现。它能破坏两台计算机之间通信链路上的数据，其伪装的目的在于哄骗网络中的其他计算机误将其攻击者作为合法计算机加以接受，诱使其他机器向它发送数据或允许它修改数据。TCP／IP欺骗可以发生TCP／IP系统的所有层次上，包括数据链路层、网络层、运输层及应用层均容易受到影响。如果底层受到损害，则应用层的所有协议都将处于危险之中。另外由于用户本身不直接与底层相互相交流，因而对底层的攻击更具有欺骗性。

（6）网络监听

网络监听是主机的一种工作模式，在这种模式下，主机可以接收到本网段在同一条物理通道上传输的所有信息，而不管这些信息的发送方和接收方是谁。因为系统在进行密码校验时，用户输入的密码需要从用户端传送到服务器端，而攻击者就能在两端之间进行数据监听。此时若两台主机进行通信的信息没有加密，只要使用某些网络监听工具(如NetXRay等)就可轻而易举地截取包括口令和账号在内的信息资料。虽然网络监听获得的用户账号和口令具有一定的局限性，但监听者往往能够获得其所在网段的所有用户账号及口令。

（7）利用黑客软件攻击

利用黑客软件攻击是互联网上比较多的一种攻击手法。Back Orifice2000、冰河等都是比较著名的木马软件，它们可以非法地取得用

户电脑的超级用户级权利，可以对其进行完全的控制，除了可以进行文件操作外，同时也可以进行对方桌面抓图、取得密码等操作。这些黑客软件分为服务器端和用户端，当黑客进行攻击时，会使用用户端程序登录已安装好服务器端程序的电脑，这些服务器端程序都比较小，一般会附带于某些软件上。有可能当用户下载了一个小游戏并运行时，黑客软件的服务器端就安装完成了，而且大部分黑客软件的重生能力比较强，会给用户进行清除造成一定的麻烦。如TXT文件欺骗手法，表面看上去是一个TXT文本文件，但实际上却是一个附带黑客程序的可执行程序，另外有些程序也会伪装成图片和其他格式的文件。

（8）安全漏洞攻击

许多系统都有这样那样的安全漏洞（Bugs）。其中一些是操作系统或应用软件本身具有的，如缓冲区溢出攻击。由于很多系统不检查程序与缓冲之间变化的情况，就任意接受任意长度的数据输入，把溢出的数据放在堆栈里，系统还照常执行命令。这样攻击者只要发送超出缓冲区所能处理的长度的指令，系统便进入不稳定状态。若攻击者特别配置一串准备用作攻击的字符，他甚至可以访问根目录，从而拥有对整个网络的绝对控制权。另一些是利用协议漏洞进行攻击。如攻击者利用POP3一定要在根目录下运行的这一漏洞发动攻击，从而获得超级用户的权限。又如，ICMP协议也经常被用于发动拒绝服务攻击。它的具体手法就是向目的服务器发送大量的数据包，几乎占取该服务器所有的网络宽带，从而使其无法对正常的服务请求进行处理，而导致网站无法进入、网站响应速度大大降低或服务器瘫痪。现在常见的蠕虫病毒或与其同类的病毒都可以对服务器进行拒绝服务攻击。它们的繁殖能力极强，一般通过Microsoft的Outlook软件向众多邮箱发出带有病毒的邮件，使邮件服务器无法承担如此庞大的数据处理量而瘫痪。对于个人上网用户而言，也有可能遭到大量数据包的攻击使其无法进行正常的网络操作。

（9）端口扫描攻击

所谓端口扫描，就是利用Socket编程与目标主机的某些端口建立TCP连接、进行传输协议的验证等，从而侦知目标主机的扫描端口是否是处于激活状态、主机提供了哪些服务、提供的服务中是否含有某些缺陷等等。

1.2 网络攻击基本知识

Skill 1：系统端口完全掌握

端口攻击是很重要的一种攻击手段，了解每个端口已成为一名黑客的必修课，下面我们来看看这些系统端口到底包含了些什么意义。

端口号	服务	说明
0	Reserved	通常用于分析操作系统。这一方法能够工作是因为在一些系统中“0”是无效端口，当你试图使用通常的闭合端口连接它时将产生不同的结果。一种典型的扫描，使用IP地址为0.0.0.0，设置ACK位并在以太网层广播。
1	tcpmux	这显示有人在寻找SGI Irix机器。Irix是实现tcpmux的主要提供者，默认情况下tcpmux在这种系统中被打开。
7	Echo	能看到许多人搜索Fraggle放大器时，发送到X.X.X.0和X.X.X.255的信息。
19	Character Generator	这是一种仅仅发送字符的服务。UDP版本将会在收到UDP包后回应含有垃圾字符的包。TCP连接时会发送含有垃圾字符的数据流直到连接关闭。黑客利用IP欺骗可以发动Dos攻击。伪造两个chargen服务器之间的UDP包。同样Fraggle DoS攻击向目标地址的这个端口广播一个带有伪造受害者IP的数据包，受害者为了回应这些数据而过载。
21	FTP	FTP服务器所开放的端口，用于上传、下载。最常见的攻击者用于寻找打开anonymous的FTP服务器的方法。这些服务器带有可读写的目录。木马DolyTrojan、Fore、Invisible FTP、WebEx、WinCrash和Blade Runner所开放的端口。