黑客攻防秘技大曝光

武新华　翟长霖　等编著

清华大学出版社

黑客攻防秘技大曝光

武新华　翟长霖　等编著

清华大学出版社
北　京

内 容 简 介

本书是为了使广大读者了解黑客的攻击手法并知道如何进行相应的防范而编写的，实用性强。全书共分为11章，通过在虚拟实验环境中进行技能训练的方式，详细讲解黑客实验环境的打造，剖析漏洞和木马的危害，并对攻击即时通信软件(QQ/MSN)/电子邮箱的手法进行揭秘和演示，及指出相应的防范措施。本书对时下流行的针对论坛/文章系统/博客系统的攻击、跨站攻击、注入攻击实例进行讲解，还通过黑客攻击与防范、电脑软件加密解密、远程溢出攻击实例讲解了电脑/服务器的安全防护。

本书内容丰富，深入浅出，图文并茂，可供对网络安全及对黑客攻防感兴趣的读者使用，同时可作为一本速查手册，供网络安全从业人员及网络管理员使用。

图书在版编目(CIP)数据

黑客攻防秘技大曝光/武新华，翟长霖等编著.—北京：清华大学出版社，2006.11
ISBN 7-302-14102-9

Ⅰ.黑…　Ⅱ.①武…②翟…　Ⅲ.计算机网络—安全技术　Ⅳ.TP393.08

中国版本图书馆CIP数据核字(2006)第127835号

出 版 者：清华大学出版社　　**地　　址**：北京清华大学学研大厦
http://www.tup.com.cn　　**邮　　编**：100084
社 总 机：010-62770175　　**客户服务**：010-62776969
组稿编辑：邹　杰
文稿编辑：宋延清
排版人员：王　杰
印 装 者：北京鑫海金澳胶印有限公司
发 行 者：新华书店总店北京发行所
开　　本：185×260　**印张**：23.5　**字数**：558千字
版　　次：2006年11月第1版　2006年11月第1次印刷
书　　号：ISBN 7-302-14102-9/TP·8471
印　　数：1～5000
定　　价：35.00元

前　言

或许大家都曾碰到过这样的情况，当自己正在为精彩的网页着迷时，突然硬盘吵闹不休，最后发现所有的程序都不能运行了；正在为网友写 E-mail 时，突然弹出一个对话框，上面写着“我是幽灵，我要毁了你的电脑！”；正在聊天室里与网友激情聊天时，突然弹出一堆对话框，无论怎么关都关不掉，最后只能无奈地重启计算机；在登录 QQ 时却突然提示密码错误，试遍所有可能的密码却依然不能通过，这时可以确定自己的 QQ 密码被盗了。

随着互联网的迅猛发展，一些“信息垃圾”、“邮件炸弹”、“病毒木马”、“网上黑客”等越来越多地威胁着网络的安全。本书紧密围绕黑客的攻与防来展开介绍，全书的主线就是围绕黑客的“攻与防”，告诉读者如何建立个人电脑的安全防护措施，从而使自己远离黑客攻击的困扰，确保自己电脑数据的安全。

本书的目标在于让读者了解黑客的攻击与防范技术，使读者在实际应用中碰到黑客攻击时，能够做到“胸有成竹”。我们不提倡那些肤浅的入侵、进攻以及破坏，那些都是为一个真正的黑客所鄙视的。本书最主要的精髓在于：希望读者能够通过书中介绍的黑客攻击和防守方法去了解黑客，进而防范黑客的攻击，使自己的网络更加安全。

本书在围绕“攻与防”来展开叙述的同时，特别注重实际例子的演示作用，针对每一种攻防手段，都结合实际的例子来进行介绍，以期使读者能够对这些黑客的攻防技术有更加感性的认识。

作者采用最为通俗易懂的图文解说，既使您是电脑新手，也能通读全书；任务驱动式的黑客软件讲解，揭秘出每一种黑客攻击的手法；对最新黑客技术的盘点，让您能够实现“先下手为强”；使用攻防互渗的防御方法，可以全面确保您的网络安全。

本书由众多经验丰富的高校教师编写，具体编写情况是：翟长霖负责第 1、2、3、4、8 章，武新华负责第 5、7、10 章，段玲华负责第 6 章，安向东负责第 9 章，陈芳负责第 11 章，最后由武新华统审全稿。本书在编写过程中还得到了许多热心网友的支持，并参考了大量来自网络的资料，对这些资料进行了再加工和深化处理，在此对这些资料的原作者表示衷心的感谢。

由于作者水平有限，书中的疏漏之处在所难免，恳请广大读者批评指正。

最后，需要提醒大家的是：

根据国家有关法律规定，任何利用黑客技术攻击他人的行为都属于违法行为，希望读者在阅读本书后一定不要使用本书中介绍的黑客技术对别人进行攻击，否则后果自负。

为便于读者阅读和理解，本书在写作中使用了如下图标约定：

对文章中所涉及到的一些内容进行特别描述，提醒读者**注意**操作到此处时切忌不要犯的一些常识性错误。

提示读者关于文中所述内容的一些相关信息，以及对文中表述复杂的内容做进一步的阐述。

对实际操作中的一些**小技巧**进行阐述，教给读者应该如何进行具体的操作。

目　录

1 实战黑客新手的入侵与防御

本章重点：

- 黑客新手的入侵与防御
- 新手入侵实战

案例目标：

在本章中将着重介绍黑客的一般入侵方法与步骤，让读者掌握一些防止黑客攻击的基本技巧，以及了解黑客如何利用百度搜索引擎偷窥别人的收藏夹，如何使用 Windows XP 的超强 syskey 命令等内容。

第 1 章　实战黑客新手的入侵与防御

对于刚刚掌握了一些黑客攻击手段的新手而言，由于他们年龄大多都比较小，因此做事容易冲动，往往是刚刚掌握了某些黑客技术之后，就会迫不急待地进行尝试，以验证自己所掌握技术的实用性，体验入侵别人计算机的快感。

这些人为了显示自己的成就，往往会对被攻击的计算机进行一些破坏，从而给被攻击者造成一定的损失。所以，新手的入侵最令人感觉到恐怖。

1.1　黑客新手的入侵与防御

在掌握了计算机基本知识的人看来，黑客是一个具有高超计算机技术的群体，他们能够随意进入别人的计算机内，了解其中的信息，并且在被入侵者不知不觉的情况下悄然退出。

这就使得那些梦想掌握计算机高级技术的人，特别是刚刚对计算机有了初步了解的年轻人，对黑客有着极其强烈的崇拜心理，千方百计地想了解有关黑客的知识，并且往往会不计后果地进行尝试。

1.1.1　新手热衷入侵的缘由

黑客一词，源于英文 Hacker，原意指热心于计算机技术，水平高超的电脑专家，尤其是程序设计人员，他们出现的真正原因是网络先天存在的安全漏洞。

但今天黑客一词已被用于泛指那些专门利用电脑搞破坏或恶作剧的人(其实对这些人，正确的英文称呼是 Cracker，有人翻译成“骇客”。黑客与骇客的根本区别是：黑客们建设，而骇客们破坏)。

黑客经常会侵入别人的计算机，并对系统进行修改或破坏。他们可能会怀有恶意地破坏计算机系统，并取得利益，或者可能只是为了显示自己的能力而制造计算机病毒，所以，现在比较确切的黑客定义是：在数据安全领域，一种未经授权、又企图躲过系统访问控制程序的检查而侵入计算机网络的用户。

黑客除了无法物理性地破坏别人的计算机或帮别人重新安装计算机系统外，其他的基本都能做到，包括把别人的计算机当跳板，盗取其他计算机内的文件(各种重要数据，如银行账号和密码、商业秘密、工作成果等)；造成别人的计算机崩溃、磁盘格式化；监视他人计算机或侵犯他人隐私，甚至远程控制他人的计算机等。如果入侵服务器则可能是替换网站的主页、下载用户数据库从而造成商业损失，或令服务器瘫痪等。

因为黑客一般都比较年轻，行为往往比较偏激。对于刚刚掌握了一些黑客技术的人，

更是如此。为了显示自己的能力，验证所掌握技术的可靠性，为了体验入侵别人的计算机时成功的快感，这些人往往不计后果；有些人在成功入侵后，还特意留下一些痕迹，以炫耀自己的本领。

1.1.2 黑客是如何入侵的

虽然黑客在入侵不同的计算机时，其实际操作会有所不同，但大体上，黑客入侵过程可概括为以下几个步骤。

1. 搜集信息

黑客在入侵其他计算机时，往往先用一些工具对网络上的一些主机进行整体扫描，然后确定攻击目标，再尽可能地搜集该计算机的相关信息，为以后的攻击行动打下基础。

2. 漏洞扫描

该阶段还是为了更准确地了解目标主机上的弱点，从而利用这些弱点来实施攻击。一般情况下，黑客会使用一些专门的扫描工具，如 X-Scan、X-way、流光、SuperScan 等，以获得攻击目标的系统数据，包括所使用的系统、开放的端口及弱口令等。

3. 弱点试探

在查找到攻击目标的漏洞之后，黑客已经掌握了攻击目标的比较详细的数据，并开始试探被攻击目标的服务漏洞。在这个过程中，黑客会去不断地猜测一些系统路径，测试用户账号和密码。

4. 取得初步权限

如果黑客找到了可以利用的漏洞，就可以获得攻击目标的初步权限。如果反复尝试后仍没有突破性进展，那么黑客就可能会利用暴力破解或者缓冲区溢出等技术，从而获得攻击目标的初步权限。

5. 提升权限

获得了初步权限以后，入侵就已经成功了一半，只要能登录目标计算机，对于黑客而言，提升权限将不会成为问题。为了提高成功率，他们有可能会借助于木马程序的帮助，如果一切顺利，此步骤花费的时间不会很长。

6. 破坏

取得用户权限的黑客已经完全控制了目标计算机，就可以像操作自己的计算机一样进行任何操作。如果其想要实施破坏，将可能造成非常严重的后果。

7. 建立后门

为了达到自己长期控制目标计算机或建立跳板的目的，黑客在取得足够的权限之后，

大多会马上在目标计算机中建立后门，如安装木马程序、设置定时任务等。

8. 消除痕迹

由于黑客的行为在许多国家都被视为犯罪行为，所以，黑客为了自保，在完成入侵之后，往往会删除目标计算机中的日志文件，及一些应用程序，如防火墙的日志文件等。

当清除完所有的入侵痕迹之后，再从目标计算机中退出，就完成了一次入侵的过程。

1.1.3 查看自己开放的端口

查看自己开放的端口，并了解其中的信息是需要掌握的最基本技术，黑客在攻击别人的计算机时，如果扫描到了攻击目标的开放端口，进行攻击就会比较有把握。为此，这里先从本地计算机开始，讲解如何查看自己计算机的开放端口，从中了解本地计算机的信息，以便防止黑客对自己的计算机进行攻击。

1. Windows 本身自带的 netstat 命令

该命令用于显示协议统计和当前的 TCP/IP 网络连接，只有在安装了 TCP/IP 协议之后才可以使用。

netstat 的命令格式：

netstat [-a] [-e] [-n] [-o] [-s] [-p protocol] [-r] [interval]

该命令的参数含义如下：

-a：显示所有连接和侦听端口。服务器连接通常不显示。

-e：显示以太网统计。该参数可以与 -s 选项结合使用。

-n：以数字格式显示地址和端口号(而不是尝试查找名称)。

-o：显示活动的 TCP 连接并包括每个连接的进程 ID(PID)。可以在 Windows 任务管理器中的【进程】选项卡中找到基于 PID(进程编号)的应用程序。该参数可以与-a、-n 和-p 结合使用。

-s：显示每个协议的统计。默认情况下，显示 TCP、UDP、ICMP 和 IP 的统计。-p 选项可以用来指定默认的子集。

-p protocol：显示由 protocol 指定的协议的连接；protocol 可以是 TCP 或 UDP。如果与-s 选项一同使用，则显示每个协议的统计，protocol 可以是 TCP、UDP、ICMP 和 IP。

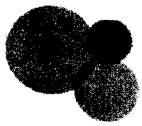
-r：显示路由表的内容。

interval：重新显示所选的统计，在每次显示之间暂停 interval 秒。按 Ctrl+B 键停止重新显示统计。如果省略该参数，netstat 将打印一次当前的配置信息。

明白 netstat 命令的使用方法后，现在就可以进行实际的操作。

(1) 选择【开始】|【运行】菜单命令，在打开的“运行”对话框中执行 CMD 命令，即可打开 MS-DOS(或命令提示符)窗口。

(2) 输入“netstat –an”命令并按 Enter 键，则显示如图 1.1 所示的端口信息。



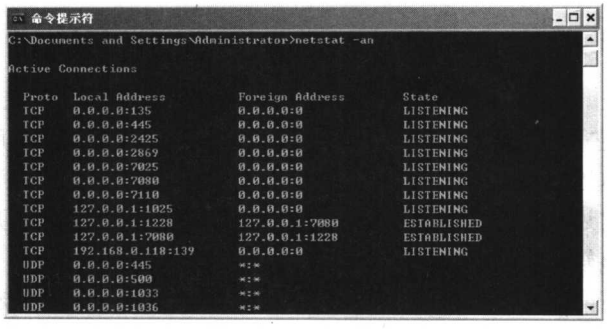


图 1.1　显示的端口信息

其中 Active Connections 是指当前的本机活动连接；Proto 是指连接使用的协议名称；Local Address 是本地计算机的 IP 地址和连接正在使用的端口号；Foreign Address 是连接该端口的远程计算机的 IP 地址和端口号；State 则是表明 TCP 连接的状态，LISTENING 表示是开放的端口，正在监听等待连接，开放的端口有可能会被黑客利用。

2. 命令行工具 fport

使用 Windows NT4\2000\XP 操作系统的读者，可以使用该 fport 程序来显示本机开放端口与进程的对应关系。

fport 是 FoundStone 公司出品的一个用来列出系统中所有打开 TCP/IP 和 UDP 端口、对应应用程序的完整路径、PID 标识以及进程名称等信息的软件。读者可到官方网站下载该工具，http://www.foundstone.com/knowledge/zips/fport.zip。

下载完毕之后，需要将其解压缩即可，不需要进行安装。

其操作方法如下。

(1) 在打开的【运行】对话框中执行 CMD 命令打开命令提示符窗口。

(2) 进入 fport 所在的目录。

(3) 输入“fport”命令，并按 Enter 键，即可查看自己计算机所打开的端口及使用该端口的程序，如图 1.2 所示。如果发现有某个可疑程序打开了某个可疑端口，千万不要大意，也许那就是一只狡猾的木马。

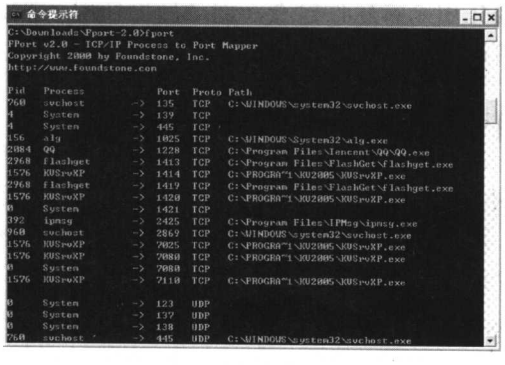


图 1.2　查看本地计算机端口信息

3. 图形化界面工具 Active Ports

Active Ports 是 SmartLine 公司出品的软件，用户可以用来监视电脑所有打开的 TCP/IP/UDP 端口。它不但可以将所有的端口显示出来，还可以显示出所有端口对应的程序所在的路径，以及本地 IP 和远端 IP(试图连接用户的电脑 IP)是否正在活动。

更重要的是，它还提供了一个关闭端口的功能，在用它发现木马开放的端口时，可以立即将端口关闭。该软件需要运行在 Windows NT/2000/XP 系统下。

用户可以在以下网站下载：http://www.smartline.ru/software/aports.zip。下载完毕并对其进行解压缩和安装之后，才能运行，其操作界面如图 1.3 所示。

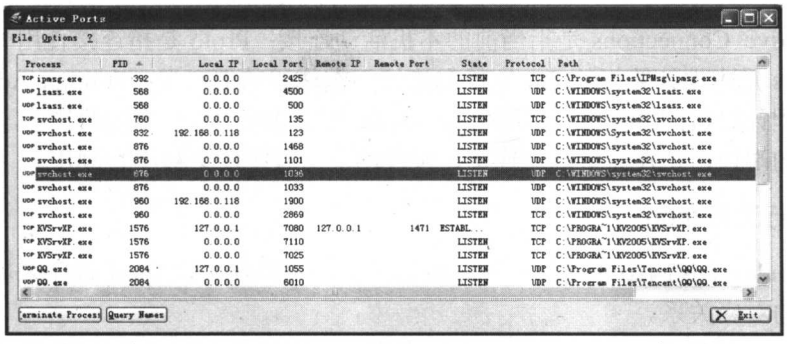


图 1.3 Active Ports 界面

【小技巧】

其实使用 Windows XP 的用户无须借助其他软件即可以得到端口与进程的对应关系，因为 Windows XP 所带的 netstat 命令比以前的版本多了一个“o”参数，使用这个参数就可以得到端口与进程的对应信息。

通过以上方法可以轻松地发现基于 TCP/UDP 协议的木马，但对于木马重在防范，而且如果碰上反弹端口木马，如利用驱动程序及动态链接库技术制作的新木马时，用上述方法就很难查出木马的痕迹了。所以一定要养成良好的上网习惯，不要随意运行邮件中的附件，最好安装一套杀毒软件。

从网上下载的软件要先用杀毒软件检查一遍之后再使用，在上网时应打开网络防火墙和病毒实时监控，保护自己的计算机不被木马侵入。

1.1.4 使用系统自带命令查看自己的 IP 信息

IP 信息是黑客攻击时所需要得到的第一信息资料，知道攻击目标的 IP 信息之后，黑客的攻击就变得简单多了，那么，如何查看自己的 IP 信息呢？其实查看 IP 信息的方法很多，下面就进行一些简单的介绍。

1. 使用 ipconfig 命令

先选择【开始】|【运行】菜单命令，并执行 CMD 命令打开“MS-DOS”(或命令提示

符)窗口，然后输入 ipconfig 命令并按 Enter 键，就可以看到自己的 IP 地址信息了，如图 1.4 所示(其中 IP Address 后面的“192.168.0.118”就是本地计算机的 IP 地址)。

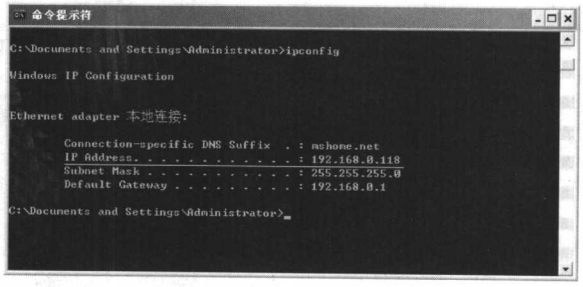


图 1.4　查看本地 IP 信息

2. 使用 Winipcfg 命令

该命令存在于 Windows Me/9X 操作系统中，它的功能与 ipconfig 相同。

通过【开始】|【运行】菜单命令，并执行 Winipcfg 命令，单击【确定】按钮，即可查看自己的 IP 地址信息。

3. 使用 Route 命令

选择【开始】|【运行】菜单命令，并执行 CMD 命令打开“MS-DOS”(或命令提示符)窗口，然后输入 route print 命令，并按 Enter 键，此时显示如图 1.5 所示的信息(其中 192.168.0.118 就是本地计算机的 IP 地址)。

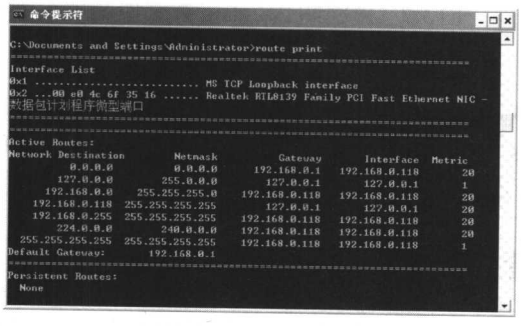


图 1.5　Route 命令显示的信息

4. 使用 Ping 命令

在【运行】对话框中执行 CMD 命令打开“MS-DOS”(或命令提示符)窗口之后，输入“Ping 自己计算机的名称”命令并按 Enter 键，即可查看自己的 IP 信息，如图 1.6 所示(计算机名称后方括号内就是本地计算机的地址)。

5. 使用 NetMeeting 程序

运行 NetMeeting 程序，选择【帮助】|【关于 Windows NetMeeting】菜单命令，在显示

的界面中即可看到本地计算机的 IP 地址，如图 1.7 所示。

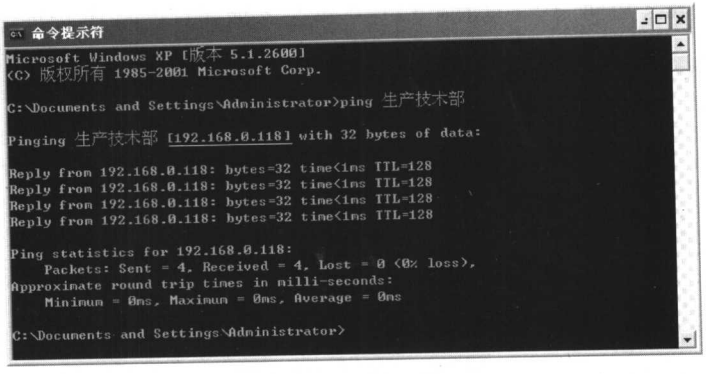


图 1.6　使用 Ping 命令

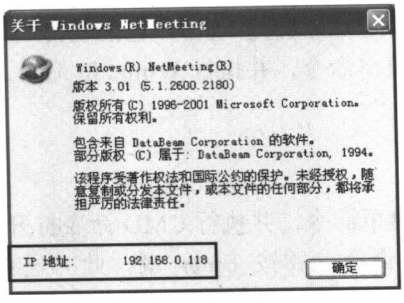


图 1.7　通过 NetMeeting 查看 IP 地址

【提示】

NetMeeting 是 Windows 系统自带的应用程序，用户可以通过控制面板进行安装，或进入 Windows 系统的“Program Files”文件夹中的“NetMeeting”子文件夹，双击 conf.exe 程序启动 NetMeeting(在 Windows 2000/XP 系统下)。

1.1.5　利用软件查看自己的 IP 信息

追捕是国产软件，它可以根据 IP/域名查询对方的所在地，还可以查询对方机器上提供的服务。只要用户处于在线状态，运行该软件即可显示自己的 IP 地址，如图 1.8 所示。

IP Hunter 是独孤剑客开发的软件，运行 IP Hunter 之后，在【自己的 IP 地址】栏中显示的就是自己的 IP 地址，如图 1.9 所示。

Icounter 是网络计时计费软件，运行 Icounter 之后，在其主界面中右击并在出现的菜单中选择【查看 IP 地址】命令即可显示自己的 IP 地址。

【注意】

只有通过电话线或 ISDN 拨号方式上网才能显示出本地计算机的 IP 地址。