黑客杀破狼

攻防秘技入门

武新华　陈 芳　段玲华　等编著

- 例说黑客入侵与防御
- Windows 系统漏洞攻防实战
- 木马的植入与防杀；远程控制技术大集合
- 伸向 QQ 和 MSN 的黑手
- 防范自己的邮箱被偷窥和轰炸
- 防不胜防的 IE 浏览器恶意攻击
- 必不可少的超级经典小工具
- 全面飚升网络控制的权限
- 防止 IIS 服务器被恶意攻击

机械工业出版社
CHINA MACHINE PRESS

来破狼——黑客攻防秘技入门

武新华　陈　芳　段玲华　等编著

机械工业出版社

本书紧紧围绕黑客的攻防来介绍，在详细介绍黑客攻击手段的同时，介绍了相应的防范方法，使读者对于攻防技术有系统的了解，能够更好地防范黑客的攻击。全书共分 11 章，包括黑客入侵与防御方法、Windows 系统漏洞攻防实战、木马的植入方法与防杀、远程控制技术大集合、QQ 和 MSN 黑客防御、防范自己的邮箱被偷窥和轰炸、如何防止浏览器被恶意攻击、常用超级小工具、全面飚升网络控制权力、如何防止 IIS 服务器被恶意攻击、打好网络安全防御战等。

本书内容丰富，图文并茂，深入浅出，适用于广大网络爱好者，同时可作为一本速查手册，适用于网络安全从业人员及网络管理员。

图书在版编目（CIP）数据

杀破狼——黑客攻防秘技入门/武新华，陈芳，段玲华等编著.

-北京：机械工业出版社，2006.4

ISBN 7-111-18870-5

I. 杀… II. ①武… ②陈… ③段… III. 计算机网络-安全技术-基本知识 IV. TP393.08

中国版本图书馆 CIP 数据核字（2006）第 031574 号

机械工业出版社（北京市百万庄大街 22 号 邮政编码 100037）

策划编辑：夏孟瑾　责任编辑：李虎斌　版式设计：崔俊利

三河市宏达印刷有限公司印刷

2006 年 5 月第 1 版第 1 次印刷

184mm × 260mm · 22 印张 · 489 千字

0001—5000 册

定价：32.00 元

凡购本图书，如有缺页、倒页、脱页，由本社发行部调换

本社购书热线电话：（010）68326294

封面无防伪标均为盗版

前　言

随着计算机技术的飞速发展，网络的安全问题也日益严重。也许仅仅是晚几天没有升级杀毒软件的病毒库或不小心点击了一个链接，都有可能带来巨大的损失。想必大家听说过“冰河”、“欢乐时光”、“漏洞攻击”吧，但这些只是黑客惯用伎俩中很小的一部分，黑客攻击的手段实在是太多了，因为每一台与互联网连接的计算机都可能成为黑客的攻击对象，当然其中也包括我们的计算机。

对于那些防范意识较差或对网络安全知识不甚了解的用户，常常极易成为黑客攻击的目标。因此，为了让所有计算机使用者能够防患于未然，对于书中几乎所有的内容，作者都在写作时直接用连接 Internet 的计算机进行了实践，并对黑客常用的一些攻击手段进行了详尽的分析，分析得到的结果便是使读者在实际应用中碰到黑客攻击时，能够做到“胸有成竹”，避免因遭受攻击与破坏而造成损失。

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，以使读者能够对这些黑客的攻防技术有更加感性的认识。

应该说，在黑客攻防方面历来都是“道高一尺，魔高一丈”，没有哪本书可以把黑客所有的攻击手段都剖析清楚，本书也只是讲述了一些最常见的黑客攻击手段，但与市面上种类繁多的黑客类图书相比，本书仍然具有如下几个方面的优点：

1．实用价值高。

2．通俗易懂，使枯燥的学习过程更轻松。

3．经验性强，能够把使用过程中的问题描绘得清清楚楚，便于分辨正误。

4．犹如老师在旁边亲自指导，有种亲临现场的感觉。

本书采用最为通俗易懂的图文解说，即使是计算机新手也可轻松通读；由浅入深的黑客软件讲解，详尽揭秘黑客攻击的手法；全新的黑客技术大盘点，让用户实现“先下手为强”；攻防互参的防御方法，全面确保用户的网络安全。

本书最主要的精髓在于：希望读者能够运用本书介绍的黑客攻击防御方法去了解黑客，进而构筑自己的“铜墙铁壁”，使自己的网络更加安全。

本书言简意赅，内容详实，能够使读者在学习有关黑客知识时而不觉得乏味，在轻松和趣味中不知不觉地学习到防杀黑客的基本知识，从而使自己在以后使用计算机时能够防止黑客的攻击与破坏，保护自己计算机中的资料不被黑客看到和破坏。

本书由众多经验丰富的高校教师编写，并得到了众多热心网友的支持，在此一并表示衷心的感谢。本书的编写情况是：武新华负责第 1、2、3、4、8 章，段玲华负责第 5、6 章，陈芳负责第 7、11 章，安向东负责第 9、10 章，最后由武新华统审全稿。由于作者水平有限，加之创作时间仓促，本书难免有疏漏之处，欢迎广大读者朋友批评指正。

最后，请读者一定要注意一点：不要迷信书，要相信自己的实践。由于软件的更新换代，任何一本书都不能保证书中的内容和实际应用中的软件完全一致，所以书中的疏漏和错误在所难免，当然本书也不例外。如果读者觉得本书中有不妥或需要改进之处，可以登录 www.newtop01.com 与笔者联系，笔者衷心感谢提供建议的读者，并真心希望在和广大读者互动的过程中能得到提高，在此致谢！

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，切记切记!

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：

对文中所涉及到的一些小知识进行描述，让读者在遇到类似问题时，能够理解应用，方便其操作。

设置问题，考察读者对操作的掌握情况。

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，以及对文中表述不清的内容进行进一步的阐述。

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操作。

编　者

目　　录

第 7 章 黑浪滔天话黑客

——例说黑客入侵与防御

本章重点：

- 功能强大的黑客工具——“冰河”2005
- 守好那扇进出的门——IPC$漏洞入侵与防御
- 黑客的常用伎俩——命令行下的远程控制 PsExec
- 一双偷窥的眼睛——远程开启视频木马初探
- 为你通风报信的灰鸽子

案例目标：

在本章中将着重介绍黑客的一些入侵方法与步骤，让读者掌握一些防止黑客攻击的基本技巧，以及 IPC$漏洞入侵与防御、命令行下的远程控制 PsExec 和如何远程开启视频木马等内容。

黑客在大多数人心里，往往是魔鬼的化身。由于他们掌握着最前沿的系统和网络技术，因此他们自称为网络时代的精英；但因为他们搞破坏的力量实在是太大，所以不得不把他们和魔鬼联系到一起。

下面就一起来看看黑客必知而又威力无穷的“秘技”，不过操作起来确实十分容易，看后大概能使大家有两种感觉：一种是蠢蠢欲动，自己想动手攻击一下别人；另一种就是会觉得黑客也不过如此。好了，闲话少说，请看实例。

1.1 功能强大的黑客工具——“冰河”2005

进行远程控制的工具很多，大多数都是称之为木马的软件。在国内影响最大的远程控制木马工具莫过于“冰河”。从某种意义上讲，“冰河”的开发者在设计之初，可能仅仅是想打造一款功能强大的远程控制软件，但十分不幸的是，“冰河”从一开始就远远偏离了这个目的，并且更为令人吃惊的是，它的诞生标志着“洋”木马一统天下局面的结束，并一度成为“木马”的代名词（国内受“冰河”木马感染的计算机多不胜数）。

【小知识】

木马，也称特洛伊木马，英文名称为 Trojan。其本身就是为了入侵个人计算机而做的，藏在计算机中和工作时是很隐蔽的，它的运行和黑客的入侵不会在计算机的屏幕上显示出任何痕迹。Windows 本身没有监视网络的软件，所以不借助其他工具软件，许多时候是很难知道木马的存在和黑客的入侵的。

1.1.1 揭开“冰河”木马的神秘面纱

“冰河”是一个基于 TCP/IP 协议和 Windows 操作系统的网络工具，所以首先应确保该协议已被安装且网络连接无误，然后配置服务器程序（如果不进行配置则取默认设置），并在欲监控的计算机上运行服务器端监控程序即可。在本节中将以经典的“冰河 v8.4”专版为例，来说明一下如何使用冰河木马，以及如何防御冰河木马。

从网上下载“冰河”软件并将其解压之后，将看到 3 个文件：G_Server.exe（服务器端程序）、G_Client.exe（客户端程序）和 Readme.txt（说明文件），如图 1-1 所示。要使用“冰河”木马，首先需要用客户端程序对服务器进行配置。

图 1-1 认清冰河的客户端与服务端

【提示】

G_Server.exe 是用来安装在别人计算机里的文件，可以任意更名，双击时没有任何反应，但其实已经悄悄地安装在计算机中了。G_Client.exe 则安装在自己的计算机中，用来监控别人的计算机。

1.1.2 配置“冰河”木马的被控端程序

服务端程序 G_Server.exe 用于被监控端后台监控程序（运行一次即自动安装，可任意改名），在安装前可以先通过 G_Client 的“配置本地服务器程序”功能进行一些特殊配置，例如是否将动态 IP 发送到指定信箱、改变监听端口、设置访问口令等。

在传输 G_Server.exe 文件前还需要对 G_Client.exe 文件进行一些配置。双击 G_Client.exe 文件，接着进行如下操作：

① 打开瑞士军刀图标的客户端 G_Client.exe，在如图 1-2 所示的主界面中单击【配置本地服务器程序】按钮。

② 在弹出的【服务器配置】对话框中选择【基本设置】选项卡，并在其中设定一个访问口令，如图 1-3 所示。

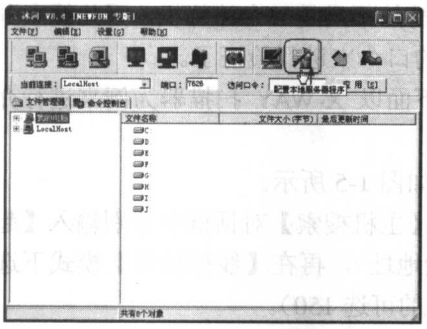

图 1-2 单击【配置本地服务器程序】按钮

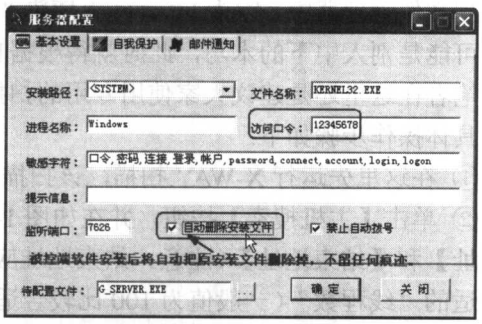

图 1-3 设定访问口令、选中“自动删除安装文件”复选框

这样，只有通过此口令才能访问到被控端的计算机，防止其他装有“冰河”控制端的用户访问。选中“自动删除安装文件”复选框，则被控端软件安装后将自动把原安装文件删除掉。

③ 选择【服务器配置】对话框中的【邮件通知】选项卡，然后输入 E-mail 地址和发送服务器，如图 1-4 所示。这样，被控端软件就可以将对方每次拨号后所产生的 IP 地址都发送到自己设定的 E-mail 中了（由于现在大多用户均采用拨号上网或动态 IP 的 ADSL 宽带上网，其每次拨号后的 IP 都不同。但进行该步设置之后，只要对方开机上网，就可以获得其 IP 并连接到其计算机上了）。

④ 在【服务器配置】对话框中还可以通过单击…按钮来选择待配置文件（一般取默认值即可），然后设置服务器端的安装路径、更改服务器的文件名、设置访问口令、进程名称、监听端口、是否写入注册表启动项、是否关联文件等。还可以设置是否将“肉鸡”的系统信息、开机口令、共享资源信息等发送到指定 E-mail。

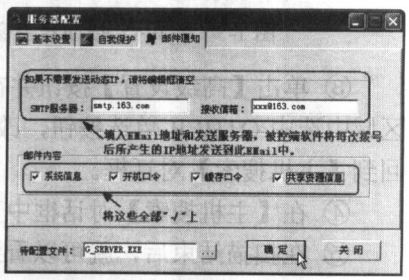

图 1-4 输入 E-mail 地址和发送服务器

⑤ 最后单击【确定】按钮，被控端软件就配置好了。当然，还有一些无关重要的选项，如果需要可以根据自己的实际情况酌情设置，如可以更改监听端口（范围在 1024~32768 之间）。

1.1.3 搜索、远控目标计算机

除从 E-mail 中得到 IP 地址外，还可以通过控制端软件进行自动搜索（当然也可以使用其他搜索工具），单击主界面中的【自动搜索】按钮，在弹出的对话框中输入起始域和起止地址，如搜索 192.168.0.1 到 192.168.0.255 之间的 IP 地址，则可以在【起始域】文本框中输入 192.168.0，在【起始地址】文本框中输入 1，【终止地址】文本框中输入 255，然后单击【开始搜索】按钮即可。

“搜索结果”框中以 OK 开头的 IP 就可能是自己要找的了，控制端软件将会自动将其添加到文件管理器中，因为 Internet 上感染“冰河”木马的不只是一台计算机，因此搜索到的很可能是别人中下的木马，此时就得根据自己设定的口令来进行验证了。

笔者在这里还是建议大家使用专用的扫描工具，下面以 X-WAY 扫描器为例来进行介绍，具体操作步骤如下：

① 在这里先运行 X-WAY 扫描，该扫描器主界面如图 1-5 所示。

② 单击【主机搜索】按钮，并在如图 1-6 所示的【主机搜索】对话框中分别输入【起始地址】和【结束地址】（注意：结束地址应大于起始地址），再在【线程设置】模式下选择合适的“线程数”（一般值为 100 比较合适，网速快的可选 150）。

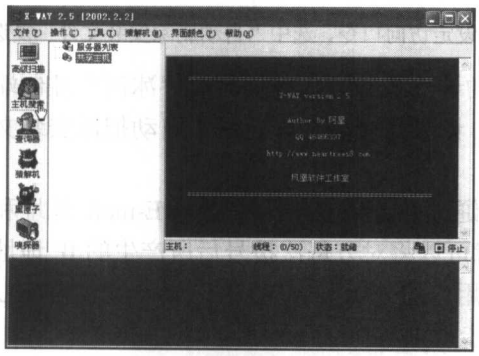

图 1-5 X-WAY 扫描器主窗口

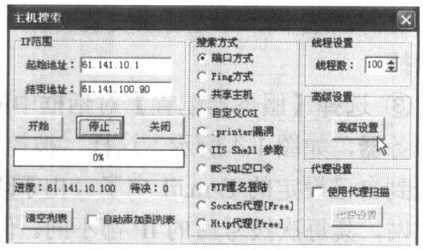

图 1-6 设置主机扫描

③ 单击【高级设置】按钮并在【主机搜索各参数设置】对话框中的【端口设置】选项区域中选中 OTHER 单选按钮，改变其值为 7626，如图 1-7 所示。然后单击【关闭】按钮回到【主机搜索】对话框。

④ 在【主机搜索】对话框中直接单击【开始】按钮即可开始扫描，如图 1-8 所示。

⑤ 在扫描结束后，就可以看到如图 1-9 所示的扫描结果了。

【提示】

为了某些特殊的缘故，笔者对本书中的个别图片会做一些技术上的处理，希