魔与道——黑客攻防鬼招拆招

武新华　陈恩波　段玲华　等编著

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

魔与道——
黑客攻防见招拆招

武新华　陈恩波　段玲华　等编著

電子工業出版社
Publishing House of Electronics Industry
北京·BEIJING

内 容 简 介

在现今这个科技发达的时代，网络在人们工作、学习中起着举足轻重的作用，但大多数人的网络安全知识还很匮乏，在遇到黑客入侵时不知道如何应对。而本书的目的就是让读者在尽可能短的时间内，了解黑客的起源、常用工具以及攻击方法，并在拥有基本网络知识的前提下，掌握反黑知识、工具和技巧，从而保护自己的电脑。

本书内容丰富，图文并茂，深入浅出，面向广大网络爱好者，同时可作为网络安全从业人员的一本速查手册。

图书在版编目(CIP)数据

魔与道——黑客攻防见招拆招 / 武新华等编著.—北京：电子工业出版社，2007.9
ISBN 978-7-121-04727-5

I. 魔… II.武… 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（2007）第 108895 号

责任编辑：严　力
印　　刷：北京市天竺颖华印刷厂
装　　订：三河市金马印装有限公司
出版发行：电子工业出版社出版
　　北京市海淀区万寿路 173 信箱　邮编：100036
开　　本：787×1092　1/16　印张：24　字数：584 千字
印　　次：2007 年 9 月第 1 次印刷
印　　数：6000 册　　定价：33.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

前言

PREFACE

古时候，人们谈虎色变。而在科技发达的今天，人们则谈“黑”色变，是因为在网络驰骋的千里马中有一些别样之马——黑客。同时，人们的网络安全意识淡薄，使这些黑客有机可乘。而本书就是给大家指引一条康庄大道，让读者在尽可能短的时间里了解黑客的起源、基本工具、攻击方式，并在拥有基本网络知识的前提下，掌握反黑知识、工具以及技巧，从而保护自己的电脑。

本书在写作过程中，始终本着让所有计算机使用者能够防患于未然的主旨，着重而详细地介绍了黑客的一些攻击方式，从而使读者在了解黑客攻击方法的基础上，能够最大限度地做到知己知彼，并在遭受黑客攻击时能尽量减少自己的损失。

本书紧紧围绕“攻”、“防”两个不同的角度，在讲解黑客攻击手段的同时，介绍了相应的防范方法，图文并茂地再现了网络入侵与防御的全过程。本书共分 13 章，系统地介绍了同黑客斗争的全部过程，以及相应的防御措施和方法，以方便读者了解入侵者常用的方式、方法，从而保卫网络安全。书中包括：信息安全基础知识，扫描、嗅探与欺骗，漏洞的攻击与防范，木马的植入与防范，QQ 和 MSN 的攻防，网络浏览器的攻防，服务器的攻防，远程控制技术，杀毒软件的使用等内容。

本书写作的目的在于让读者了解黑客的攻防技术，使读者在实际工作中碰到黑客攻击时，能够做到应对自如。同时，读者能够通过本书介绍的黑客技术去了解黑客，进而防范黑客的攻击，使自己的网络更加安全。

但不可避免的是，书中要涉及到一些具体的实例，因为只有这样才能够使本书的内容生动、翔实和具有可说服性。为此，考虑到大多数读者均是互联网用户，如果直接在互联网上进行实例模拟，不仅我们模拟的难度需要大大增加，而且容易引来一些操作失误和社会危害。因此，本书中的所有实例我们只是在一个模拟的局域网环境中调试通过的。

这样做的好处是：对于初级用户而言，一点也不妨碍他们学习这些工具软件的使用，且对于互联网用户几乎产生不了什么危害。对于高级用户而言，工具软件的使用仅仅是作为一种参考，他们一般都有更好的处理方法。

因此，本书尽管也是在讲实例，也是在教大家如何实现黑客技术的攻击与防御。由于所有的攻防技术都是在一个封闭的局域网环境中模拟的，因此，读者完全可以放心地对本书中所涉及的软件及其使用技术进行应用。从而使自己在以后使用计算机时，能够防范黑客的攻击与破坏，保护自己计算机中的资料不被黑客看到和破坏。

同时，为了使读者能够在学习和掌握这些新技术时做到“知其然，知其所以然”，本书在写作中还加入了相当篇幅的理论讲解，尽量做到“授人以渔而非授人以鱼”，使读者在全面掌握这些知识的同时，能够举一反三，更好地维护自己的系统，尽最大可能地为自己的网络打造出坚实的“铜墙铁壁”，最大限度地保护自己的信息安全。

PREFACE

本书由武新华、陈恩波、段玲华等编写，其中，陈恩波负责第1、2、3、4章，李防负责第5章，曹燕华负责第6、7章，段玲华负责第8、9章，安向东负责第10、11章，张慧娟负责第12章，武新华负责第13、14章，最后由武新华通审全稿。本书在编写过程中得到了许多热心网友的支持，参考了他们提供的一些资料，并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感谢。

我们虽满腔热情，但限于自己的水平，书中的疏漏之处在所难免，欢迎广大读者批评指正。

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不要使用本书中介绍的黑客技术对别人进行攻击，否则将会担负相应的法律责任。

编　者

2007年8月

目录

CONTENTS

第1章

黑客其实并不神秘

重点提示

常用的入侵攻击方式
一般常用的几个入侵命令
黑客必经之门——IP 和端口

学习目标：

本章所要实现的学习目标是使读者明白黑客是怎样攻击电脑的。学会黑客知识不仅可有效预防黑客的攻击，还可以让自己练练手，何乐而不为呢？在本章中将重点介绍黑客的一般入侵方法和步骤，让读者更好地掌握一些有效预防黑客攻击的基本技巧。

对掌握了计算机基本知识的人，“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，窃取他人的信息，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攻击和入侵的知识，并且不计后果地进行尝试。

1.1 黑客基础知识概述

黑客是一种技术，更是一种文化，已经在网络世界发展了几十年，并且根深蒂固，可以预料，在今后相当长的一段时期内，它还会继续发展下去。如果想要靠打击、封杀消灭黑客是不可能的，只有充分了解黑客、认识黑客，才能真正把黑客引向正途，让黑客技术为国家、为社会服务。

1.1.1 为什么会受到黑客攻击

在这个黑客攻击日益猖獗的年代，为什么会受到黑客攻击，遭到黑客入侵后应该采取哪些措施？在上网安全受到了极大威胁时，难道只能被迫挨打吗？当然不是，只要防范得好，这些黑客才攻击不了我们的计算机。

下面来简单了解一下为什么用户的网络总是容易受到黑客的侵入。

1. 隐藏 IP 地址

黑客经常利用一些网络探测技术来查看用户的主机信息，主要目的是得到网络中主机的 IP 地址。IP 地址在网络安全中是一个不容忽视的问题，如果攻击者知道了用户的 IP 地址，就等于为其攻击准备好了目标，就可以向这个 IP 地址发动各种进攻，如 DoS 攻击、Floop 溢出攻击等。隐藏 IP 地址的有效方法是使用代理服务器。

与直接连接到 Internet 相比，使用代理服务器可以有效地保护上网用户的 IP 地址，从而保障上网安全。代理服务器的原理是在客户机和远程服务器之间架设一个“中转站”，当客户机向远程服务器提出服务请求后，代理服务器先截取用户的请求，再将服务请求转交给远程服务器，从而实现客户机和远程服务器之间的联系。

显然，在使用代理服务器之后，其他用户只能探测到代理服务器的 IP 地址而不是用户的 IP 地址，这就实现了隐藏用户 IP 地址的目的，保障了用户上网安全。

提供免费代理服务器的网站有很多，用户也可以自己用代理猎手等工具来查找。

2. 关闭不必要的端口

黑客在入侵时常常会扫描用户的计算机端口，如果用户安装了端口监视程序，该监视程序则会有警告提示。在遇到这种入侵时，最好用工具软件关闭用不到的端口。

3. 更换管理员账户

Administrator 账户拥有最高的系统权限，如果该账户被人利用，后果将不堪设想。黑客入侵的常用手段就是试图获得 Administrator 账户和密码，因此最好重新配置 Administrator 账户。先为 Administrator 账户设置一个强大而复杂的密码之后，再重命名 Administrator 账

户，然后创建一个没有管理员权限的 Administrator 账户欺骗入侵者。这样，入侵者就很难搞清哪个账户才真正拥有管理员权限，所以在一定程度上减少了危险性。

4. 杜绝 Guest 账户的入侵

Guest 账户即所谓的来宾账户，它可以访问计算机，但受到限制。Guest 同时也为黑客入侵打开了方便之门。利用 Guest 用户得到管理员权限的方法很多，所以要杜绝基于 Guest 账户的系统入侵，最好对其进行一些必要的设置，如图 1-1 所示。

禁用或彻底删除 Guest 账户是最好的办法，不过在某些必须使用到 Guest 账户的情况下，就需要通过其他途径来做好防御工作了。首先给 Guest 设置一个强大而复杂的密码，然后详细设置 Guest 账户对物理路径的访问权限即可。

5. 封死黑客的“后门”

既然黑客能够轻松地入侵用户的计算机，该系统一定存在为其打开的“后门”，用户只要将其堵死，就会让黑客无处下手。

（1） 删掉不必要的协议

对于服务器和主机一般只安装 TCP/IP 协议就够了，具体的操作步骤如下。

步骤 1 使用鼠标右击“网络邻居”图标，并在弹出菜单中，选择“属性”菜单项，即可打开“网络连接”窗口。

步骤 2 用鼠标右击“本地连接”图标，并在弹出快捷菜单中选择“属性”菜单项，即可打开“本地连接 属性”对话框。

步骤 3 在“常规”选项卡的“此连接使用下列项目”列表框中，勾选不必要的协议之后，单击“卸载”按钮，即可卸载不需要的协议。

由于 NetBIOS 是很多安全缺陷的源泉，因此对于不需要提供 NetBIOS 功能的主机，可以考虑将绑定在 TCP/IP 协议上的 NetBIOS 关闭，以避免黑客针对 NetBIOS 的攻击，如图 1-2 所示。

图 1-1 禁用 Guest 账户

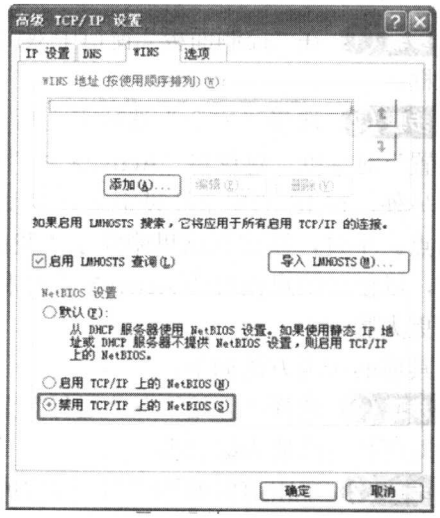

图 1-2 禁用 NetBIOS 功能

（2） 关闭“文件和打印共享”功能

“文件和打印共享”本来是一个非常便利的功能，但在使用时，却也是引发黑客入侵的漏洞。因此，在没有必要“文件和打印共享”功能的情况下，可以考虑将其关闭。即便需要使用共享，也应该为共享资源设置访问密码。

（3） 禁止建立空连接

由于在默认的情况下，所有用户均可通过空连接连上服务器，来实现枚举账号并猜测密码。因此，为了有效预防黑客入侵，就必须禁止建立空连接。

禁止建立空连接的方法如下。

方法一：修改注册表编辑器。

在注册表编辑器中，展开到 HKEY_LOCAL_MACHINE/System/Current/Control/SetControl LSA 子键下，将 DWORD 值 ResTrictAnonymous 的键值改为 1 即可。

方法二：修改本地安全策略

修改 Windows 2000/XP 系统的本地安全策略为“不允许 SAM 账户和共享的匿名枚举”即可。

（4） 关闭不必要的服务

为了方便管理的需要，网管员往往会开启很多的服务，服务开得多可以给管理带来方便，但也会给黑客留下可乘之机。因此，对于一些使用不到的服务，最好应该将其关掉。比如在不需要远程管理计算机时，最好将有关远程网络登录的服务关掉，将不必要的服务停止之后，不仅能保证系统的安全，同时还可以提高系统运行速度。

6. 做好 IE 的安全设置

虽然 ActiveX 控件和 Java Applets 有较强的功能，但也存在被人利用的隐患，网页中的恶意代码往往就是利用这些控件编写的小程序，只要打开网页就会被运行。因此，要想避免恶意网页的攻击，最好禁止这些恶意代码的运行。

IE 对此提供了多种选择，具体的设置步骤如下。

步骤 1 在“控制面板”窗口中双击“Internet 选项”图标项，即可打开“Internet 属性”对话框。

步骤 2 选择“安全”选项卡之后，单击其中的“自定义级别”按钮，即可打开“安全设置”对话框，建议将“ActiveX 控件和插件”与“Java”相关选项禁用，如图 1-3 所示。

另外，在 IE 的安全性设定中只能设定 Internet、本地 Intranet、受信任的站点、受限制的站点。不过，微软在这里隐藏了“我的电脑”的安全性设定，通过修改注册表把该选项打开，以便于用户在对待 ActiveX 控件和 Java Applets 时有更多的选择，并对本地电脑安全产生更大影响。

具体的实现方法如下。

步骤 1 选择“开始”→“运行”菜单项，在“运行”对话框中输入“Regedit.exe”命令，即可打开注册表编辑器。

步骤 2 单击前面的“+”号，顺次展开到 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\InternetSettings\Zones\0 子键之后，找到 DWORD 值“Flags”（默认键值为十六进制的 21），双击“Flags”将其键值改为“1”即可，如图 1-4 所示。