网络任我行系列

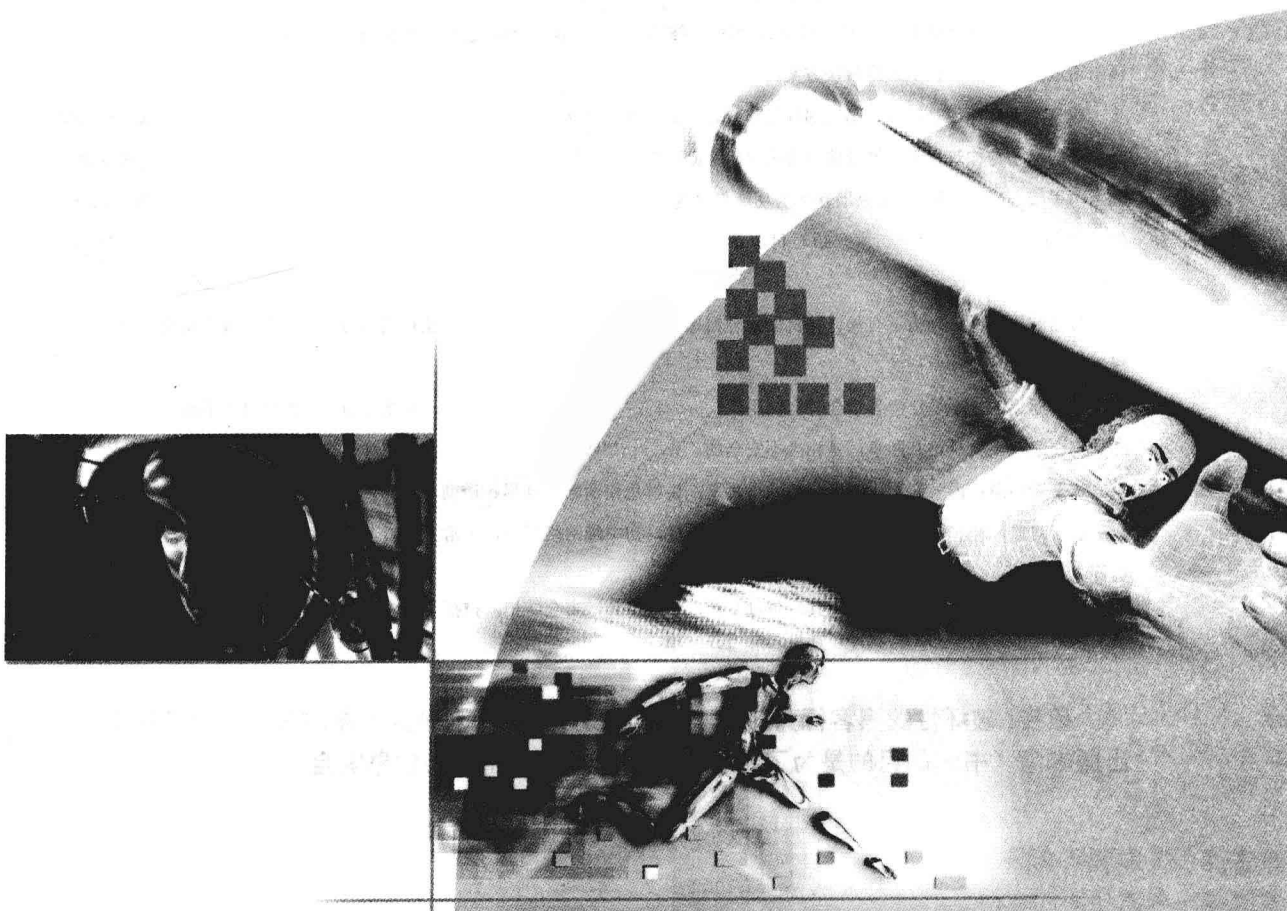
黑客 Hacker 防范宝典

魏继超 著

中国标准出版社

黑客防范宝典

黑客 Hacker 防范宝典



魏继超 著

中国标准出版社

黑客防范宝典

编　　著：魏继超
出版发行：中国标准出版社
责任编辑：王一力　张雪梅
执行编辑：秦　致
光盘制作：吴　松　魏继超
美术设计：孙志强
排　　版：余　菲
印　　刷：北京广益印刷有限公司
版　　号：ISBN 7-900032-44-4
零　　售：全国各地图书市场、报刊亭（摊）
定　　价：23 元（光盘+配套说明书）

中国标准出版社
地　　址：北京市复兴门外三里河北街 16 号
电　　话：（010）68522006
邮　　编：100045
出版日期：2001 年 6 月

邮购地址：北京海淀区复兴路 15 号
　　北京赛维波信息咨询有限公司
邮 购 价：23 元（光盘+配套说明书）
邮　　编：100038
咨询电话：（010）68514026　68515544-2901/2961

内 容 简 介

本手册是配合《黑客防范宝典》光盘，供网络与广大计算机用户防范黑客攻击的实用指南，通过大量的实例，详细解说黑客攻击计算机用户和服务器的惯用伎俩与手段，为用户介绍构筑安全网络的知识。

全书由三大部分、十二个章节和一个附录构成。

基础知识是根本。第一部分为核心知识篇，讲述不可或缺的黑客防范基础知识。第一章介绍两个基本概念——IP 地址与代理服务器。第二章详细介绍了 24 种常用命令及其使用方法。

要构筑安全的网络，必须了解黑客攻击的手段。第二部分为实战篇，是本书之中心所在，揭示黑客入侵计算机用户与网络的惯用伎俩。第三章通过实际操作方式，讲解两种扫描工具 SuperScan 与 IP-Tools 2000 的使用方法。第四章介绍黑客破解 FTP 服务器的三种破解方式——全自动破解、使用字典破解和暴力破解。第五章通过实例形式解析黑客怎样利用 NetBIOS 的漏洞，进行 NetBIOS 共享入侵，并以 NT 系统为例提供一个堵塞该漏洞的解决办法。第六章演示黑客对 Windows NT/2000 系统的详细入侵过程与隐藏手段，解说了 Windows NT 系统存在的 43 处漏洞，并提出了相应的解决办法。第七章揭示路由器本身存在的缺陷，详细披露黑客利用这些缺陷来获得非法访问权限的伎俩，并提出路由器的故障解决办法。第八章讲述虚拟网络计算机（VNC）和 WIN2KS 的终端服务（WBT）存在的安全性问题，通过问答形式揭示黑客的攻击伎俩与造成的危害，并提供最终解决方案。

黑客的最高境界是防守。第三部分是防守篇，讲述对付黑客攻击的策略，介绍构筑安全网络的手段。第九章简单介绍防火墙的概念与构筑原理，推荐选购防火墙的原则，解说设置防火墙过程中应注意的问题。第十章针对黑客进行网络攻击的常用手段，介绍三种个人防火墙软件的功能与设置方法。第十一章详细介绍了个人用户网络黑客防范软件 LockDown 2000 的功能与设置方法。第十二章介绍对付电子邮件炸弹的手段，推荐一款对付电子邮件炸弹的免费砍信软件——E-mail Remover 的使用方法。

最后的附录部分列出了有关计算机信息网络国际联网安全保护管理办法与法规的部分条款，提醒读者玩网不能玩火，侵犯他人是要负法律责任的。

本手册目的：不是让读者学会怎么使用黑客工具，怎样去进入别人的电脑，而是希望读者通过对本手册的学习，让你感觉到网络原来就是这么回事，是相当不安全的。只有时刻做好防范工作，才能拒黑客于门外。

本手册特点：内容新颖、丰富，技术含量高；讲解思路清晰、详尽、透彻，图文并茂。

读者对象：计算机个人用户，大中专学校在校生，初中级网络用户，经常上网者，网站管理与维护人员，系统开发人员等。

光盘内容：书内工具，邮箱工具，杀毒专栏，木马工具，安全防护，扫描工具，破解工具，聊天工具，补丁升级，其它工具等十多个系列的工具软件。详见光盘内容介绍。

敬告：破坏性的黑客行为违反我国有关法律规定，对他人实施攻击要承担法律责任。出版本盘（书）的目的是为了更有效地保障用户的系统与信息安全。

序　言

网络创造了神话，也带来了灾难。

入侵，反入侵，黑客，入侵者，安全专家顾问，形形色色的人物，最活跃最闪亮的可以说是黑客。他们是一种特殊的群体，真正的黑客不为名也不为利，只想探索计算机系统的奥妙所在。他们个个都是编程专家，系统分析专家，他们的知识最丰富最专业，他们乐于破解，渴望着进入。进入的那一刻是多么令人兴奋的时刻呀，它具有非凡的价值。

黑客们似乎都只对大网站、大公司的服务器感兴趣，他们利用一切可以利用的方法去破解，去入侵，去告知对方的网络不安全，要提高警惕。

现在的网络是资源共享的网络，没有文件共享，后果将不堪设想。小到二台三台的局域网，大到几十台上百台甚至上千万台的广域网，更大的就是互联网，共享无处不在。没有共享，简直无法想象。比如我需要一个文件，而硬盘中却没有，恰恰同事有这个文件，可是怎么取得这个文件呢？没有软驱，只有一个网卡。好！够了，就是一块网卡，这就够了。赶快共享你的资源吧，这样我就可以毫不费力地取得我所要的文件了，真方便呀，共享真好！

有得必有失，这话一点不假。为何这样说，在互联网上，你方便了自己，同时也方便了大家，是什么意思呢？只要你有共享，互联网上一些好事者，都会有兴趣去瞧瞧的，也就是说，可以轻易地得到你的文件。

其实你仔细想一想，几乎 80%~90%的计算机都设有共享资源，并且大多数都是连在网上的，安全措施做得好的很少。谁愿意绞尽脑汁地去设置长长的密码，弄不好自己也忘了，因此为了图省事，图方便，就不设密码，也没有什么防护措施，即使有一个软件保护，可有用的很少，不是长期没有产品升级，就是软件功能太差。一个好的网络安全工具也是很重要的。设共享就共享，这可是真正地共享，让全世界的人都共享了。其实本来就该这样。唉，我的隐私文件呀，和妹妹的聊天记录呀，说不定什么时间被登在某个比较热闹的 BBS 上，这下可丢脸了，怨谁呢？设共享是有级别的，只读，存取，完全访问，只读就只读吧，至少文件被看了，可丢不了。你可不要图方便，嫌硬盘太小了，把硬盘设置为可存取，这下，损失可不仅仅是几个聊天记录了，说不定，系统要重装了。开玩笑，不过也是，很危险的，只读本来就很危险，为什么这样说？你想呢，如果你的密码文件也在共享之列，那……就不说了！太恐怖，太可怕，这样一来，我的电脑和是别人的有什么两样呢？

给你举个小例子吧！比如呢，你把你的 OICQ 文件夹共享了，有人呢，不留意地进入到你的机器中，又不经意地发现了这个 OICQ 文件夹，他可以一边与你聊天，一边复制你的聊天记录，一边破你的 OICQ 密码。没想到被骗了，这次和人家聊得是很不可开

交，可下次再登录的时候就麻烦了，到什么地方去取密码呀！唉，我的“妹妹”全丢了，得不偿失呀！说不定想不开，没有“妹妹”不行，再寻个短见。唉！你看看，多可怕的后果。虽然说腾讯公司现在有要回密码的功能，可是，密码能被黑，能黑你的人都不是傻瓜，你能要回吗？看来网络安全还真是个问题呢。你别说了，再说下去，大家都不敢上网了。唉，你怕什么，只要你没有设共享。不可能，现在电脑这么便宜，上网又可以包月，哪家不是二台三台的，家庭网络呀，没有共享，可能吗？

再给你说一点，如果进了你的机器，或者没有进入你的机器，但如果通过一定的手段扫描到某主机所提供的服务和后门，这可不是闹着玩的，有了这个信息，就不单单是访问访问你，至少给你纪念一次，破了你的密码，呀，你完了。

不管什么事，要三思而行呀，共享还是不共享，要密码还是不要密码，这密码安全吗？可以这样说，密码很简单，大多数人的心理应该是一样的。你不会说登录一个密码，上网一个密码，OICQ 一个密码，ICQ 一个密码，我 5 个信箱再每个信箱一个密码，还有信用卡一大串密码，还有……行了，你记得住吗？根据经验，许多人可以说达到 90% 以上的人几乎用同样的密码，也就是说，破你一个，等于你就完了。真可怕，密码多吧，记不住；一个吧，好记但极不安全。敢问一句，读者你自己是怎么做的呢？密码，真是麻烦的东西，却也是令黑客们最兴奋的东西。再举个例子吧，大的不说，就说网易的个人主页吧。说句实话，谁的网站都是不堪一击的。为什么这样说，当然是有根有据的，申请过的人都知道，http://go.163.com/sunnygirl，其中的 sunnygirl 就是你自己的 username，有了这个东西，你的密码，还不是轻而一举就被 crack 了吗？不过对于个人网站呀，还是没兴趣，除非你做得好，引人起坏心眼了。好好设置你的密码吧！随时带个本子，把密码记下来。为什么，太长了。你看看我的 ftp 密码 Whla02n4fEng（当然没这么复杂），这么长，我自己常常要输入几遍才输对，有时自己破自己的网站，这密码还不够，一天半天就被破了。建议大家用“黑客字典”制作密码文件，很简单的，也比较安全。

编　者

2001 年 6 月

光 盘 主 要 内 容

1. 杀毒专栏

McAfee 杀毒之星
KILL98 for Win9x/NT/2000 病毒码
PC-Cillin 98/2000 病毒码
熊猫卫士
瑞星杀毒软件

2. 书内工具

黑客字典
网络密码探测器 2.0

3. 其它工具

猎鹿人 2.1 正式版
黑客字典 II
网路小刀之代理安全
万能钥匙

4. 木马工具

网络精灵 3.0
subseven2.1

5. 扫描工具

代理猎手 3.1
IP 搜索客 v1.70
追 捕
superscan3.0
portscan

6. 邮箱工具

FlashSendMail
邮箱终结者 1.0
EmailSearch

7. 安全防护

美萍电脑安全卫士
LockDown 2000
Trojan Remover
木马克星
Firewall
天网防火墙个人版
护猫专家
win95 98 nt 安全补丁

8. 破解工具

Zip 密码破解
流影 HTTP 远程扫描工具
Emailcrk
BrutusA2

9. 聊天工具

TraceIcqV1.5 正式版
Semot 聊天动作生成机
OICQ 魔道终结者 1.0
OICQ 聊天圣手
OICQ 浏览器清除器

10. 补丁工具

Office 2000 SR2 升级包
Outlook VCard Buffer Overflow 安全补丁
Windows 2000 补丁 SP1

目　录

第一部分　核心知识篇

第二部分 实战篇

第三部分　高级防守篇

第一部分

核心知识篇

不可不知的基础知识……

没有人能随随便便成功，防范黑客也是一样。本部分是最基础的知识，只有具备了这些基础，才能进入后面的实战……

第一章　基础知识

本章重点

本章主要介绍本手册中经常使用的两个基本概念——IP 与代理服务器，其中包括 IP 地址、IP 地址的组成与种类、与 IP 相关的一些问题和代理服务器的定义、设置与应用等。

1.1　IP 基础

1.1.1　IP 地址

IP 地址是一个 32 位二进制数，分为 4 个 8 位字节，是在使用 TCP/IP 协议的网络中用于识别计算机和网络设备的唯一标识，也就是说 IP 地址必须是唯一的——因特网上不能有两台计算机或其他网络设备的 IP 地址相同。如果两台计算机的 IP 地址相同，则其中一台计算机将无法在网络中进行通信。

得到 IP 地址的方法很多，这里介绍两种比较有效的。一是通过 OICQ，采用 OICQ SNIFFER 工具，随便给你的朋友说一句话就可以得到对方的 IP 地址。二是扫描工具，例如 SuperScan，该工具功能强大，可以查找某区域内的所有计算机的 IP 地址以及各台计算机所开放的端口（实战部分有详细介绍）。

1.1.2　动态 IP 地址

动态 IP 是对广大拨号上网用户而言的，每次上网由 ISP 自动分配一个 IP 地址。

1.1.3　静态 IP 地址

静态 IP 是对于常年连接在网上的计算机而言的，其 IP 地址是由 InterNIC 提供的。IP 地址的格式为***.***.***.***，例如 202.102.224.68 就是合法 IP 地址。

1.1.4　IP 地址的组成与种类

每一个 IP 地址都是由 4 个字节共 32 位的数字串组成，这 4 个字节通常用小数点分隔。每个字节可用十进制或十六进制表示，例如 168.180.17.200 或 0x8.0x43.0x10.0x26 就是用十

进制或十六进制表示的 IP 地址。IP 地址也可以用二进制表示。

每个 IP 地址包括两个标识码 ID，即网络 ID 和主机 ID。同一个物理网络上的所有主机都用同一个网络 ID，网络上的一个主机（包括网络上工作站、服务器和路由器等）有一个主机 ID 与其对应。据此把 IP 地址的 4 个字节划分为 2 个部分，一部分用以标明具体的网络段，即网络 ID；另一部分用以标明具体的节点，即宿主机 ID。在这 32 位地址信息内有五种定位的划分方式，这五种划分方法分别对应于 A 类、B 类、C 类、D 类和 E 类 IP 地址。

（1） A 类 IP 地址

一个 A 类 IP 地址由 1 字节的网络地址和 3 字节主机地址组成，网络地址的最高位必须是“0”，如图 1-1 所示。

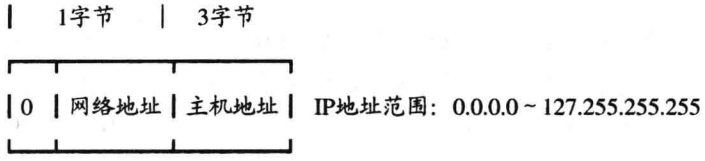


图1-1　A类网络IP描述

（2） B 类 IP 地址

一个 B 类 IP 地址由 2 个字节的网络地址和 2 个字节的主机地址组成，网络地址的最高位必须是“10”，如图 1-2 所示。

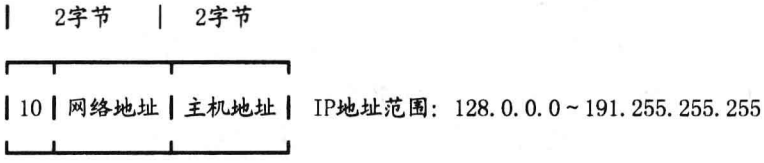


图1-2　B类网络IP描述

（3） C 类 IP 地址

一个 C 类地址是由 3 字节的网络地址和 1 字节的主机地址组成，网络地址的最高位必须是“110”，如图 1-3 所示。

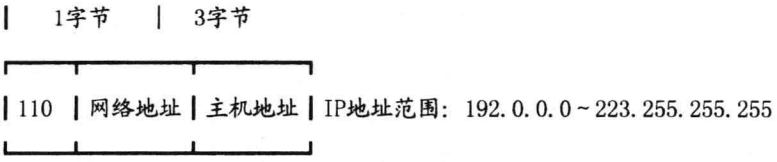


图1-3　C类网络IP描述

（4） D 类 IP 地址

D 类地址用于多点播送。第一个字节以“1110”开始。因此，任何第一个字节大于 223 小于 240 的 IP 地址是多点播送地址。全零（“0.0.0.0”）地址对应于当前主机。全“1”的 IP 地址（“255.255.255.255”）是当前子网的广播地址。范围是 224.0.0.0 到 239.255.255.255。

（5） E 类 IP 地址

E 类地址以“11110”开始，为将来使用保留。范围是 240.0.0.0 到 247.255.255.255。

（6） 几个用作特殊用途的 IP 地址

① 凡是主机段，即宿主机 ID 全部设为“0”的 IP 地址称之为网络地址，如 129.45.0.0 就是 B 类网络地址。

② 广播地址。凡是主机 ID 部分全部设为“1”的 IP 地址称之为广播地址，如 129.45.255.255 就是 B 类的广播地址。

③ 保留地址。网络 ID 不能以十进制“127”作为开头，在 A 类地址中数字 127 保留给诊断用。如 127.1.1.1 用于回路测试，同时网络 ID 的第一个 8 位组也不能全置为“0”，全“0”表示本地网络。网络 ID 部分全部为“0”和全部为“1”的 IP 地址被保留使用。

1.2 与 IP 有关的几个问题

问：任何一台电脑都有 IP 吗?

答：任何一台具备网络能力的电脑都有一个合法的 IP（这里的合法是指你的电脑能够确认的 IP），那个 IP 就是 127.0.0.1，请注意，其实 127.0.0.1 并不是你电脑的真正 IP，它只是一个系统默认的本机主机 IP，而且必须需要拥有网络适配器等条件才可拥有 127.0.0.1。

问：一台电脑可以拥有两个以上不同的 IP 吗?

答：当然，如果你的电脑装了两块网卡，并且在你的电脑里如果这两块网卡都工作正常的话，那么你的电脑就有 3 个 IP（加上默认的本机 IP：127.0.0.1），如果这时你再用 Modem 上网或用 ISDN 上网的话，那就再多加一个 IP，这时你的 ISP 给你分配了一个 IP 地址。在 NT 或 UNIX 系统下，可拥有更多的 IP，只要你改改 Windows 系统的注册表，同样可以拥有多个不同的 IP。

问：合法的 IP 是什么样的，什么样的 IP 是不合法的呢?

答：所谓合法 IP，就是被网络认可的 IP，合法的 IP 地址网络也分为许多种，比如你内部使用的对等网，全世界相连的因特网，像上面的双网卡的 IP，只有在内部网里这两个 IP 才是合法的，而对外的因特网来说，你这个 IP 就不是合法的了，因为在因特网网络中，它是无法识别你这两块网卡的 IP 的。而你用 Modem 拨号上去分配的那个 IP，才算是因特网上的合法 IP，而这个 IP 对于所支持那两块网卡 IP 的网络来说，将又是一个不合法的 IP，因为内部网是无法识别你这个由拨号网络分配的 IP。