防范黑客秘笈

精华本

■ 智联教育
甘立富 编著

你担心自己的电脑被黑客 **攻击** 吗？

你害怕自己的 **隐私**、机密的文件被黑客窃取、偷窥吗？

你是否希望在上网冲浪时不再为无孔不入的 **病毒** 而忧虑？

……

不用再苦于四处寻求保护电脑系统 **安全** 的良方，

翻开本书，你就可以找到 **锦囊妙计**！

人民邮电出版社
POSTS & TELECOM PRESS

防范黑客X秘笈

（精华本）

智联教育　甘立富　编著

人民邮电出版社

图书在版编目（CIP）数据

防范黑客X秘笈精华本 / 智联教育编著. —北京：人民邮电出版社，2006.6
ISBN 7-115-14795-7

Ⅰ. 防… Ⅱ. 智… 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051919号

内 容 提 要

本书是一本经过精心策划与组织，为初、中级读者量身制作的介绍防范黑客原理与防御的图书。在内容和结构的安排上，分为黑客攻防、加密解密、安全防范3个部分，对黑客行为、系统漏洞安全防范、清除木马、网络炸弹攻防、IE浏览器漏洞攻防、实战QQ/ICQ/MSN攻防、电子邮箱安全防范、网站安全与防御脚本攻击、IIS服务器漏洞安全防范、局域网管理安全防范、电脑加密解密、数据文件加密解密、系统安全加密限制、查杀病毒与安全防范等内容进行了详细讲解。

本书结构清晰，内容实用，适合对电脑网络安全有浓厚兴趣的读者，从事网络安全维护工作的技术人员，以及需要了解并掌握防范黑客入侵的个人电脑用户阅读参考。

防范黑客X秘笈精华本

◆ 编　　著　智联教育　甘立富
责任编辑　王　琳　陈　昇

◆ 人民邮电出版社出版发行　　北京市崇文区夕照寺街14号
邮编　100061　　电子函件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京顺义振华印刷厂印刷
新华书店总店北京发行所经销

◆ 开本：787×1092　1/16
印张：17.5
字数：417千字　　2006年6月第1版
印数：1－5 000册　　2006年6月北京第1次印刷

ISBN 7-115-14795-7/TP・5406

定价：25.00元

读者服务热线：(010)67132692　印装质量热线：(010)67129223

前 言

病毒破坏和黑客攻击是目前网络中危害电脑系统的两大不安全因素。而各种病毒、木马程序又基本上都是由黑客编写和散布的，常常给用户的电脑系统造成严重的破坏；恶意的黑客攻击，不仅会给电脑系统带来安全威胁，而且还会窃取、泄露电脑用户的个人隐私甚至重要的商业机密，造成各种严重的损失。可以说，黑客才是破坏网络安全的根源。由此可见，建立完善的保护系统，有效地防范黑客的恶意攻击，是维护电脑安全的根本所在。

本书正是针对防范黑客攻击这一主题，分别从防范黑客攻击，为文件数据加密，防御和清除病毒、木马等 3 个方面，循序渐进地为读者详细介绍如何有效地对付黑客的各种入侵行为，保护个人电脑系统的安全。

全书共 16 章，内容涵盖黑客防范、系统加密、安全防范三大热点。

第一部分：黑客防范（第 1 章至第 10 章）

主要讲述防范黑客的常识、系统漏洞的防范、木马的清除、IE 浏览器漏洞的防范、电子邮箱和 IM 通信软件的安全防范、网站服务器漏洞防范以及局域网安全防范等内容。读者可以从中了解和掌握各种防范黑客攻击的有效办法。

第二部分：系统加密（第 11 章至第 13 章）

主要介绍 BIOS 加密、Windows 系统加密、注册表加密、利用常用软件进行加密，以及对驱动器硬件进行加密设置等内容。读者在掌握这些知识之后，可以在对网络攻击进行有效防范的同时，及时地对电脑系统进行有效的加密控制。

第三部分：安全防范（第 14 章至第 16 章）

主要介绍通过卡巴斯基、Symantec Anti Virus 等专业的查杀病毒软件清除系统中的病毒，以及利用天网防火墙、网络安全特警、ZoneAlarm 个人网络防火墙等工具软件，建立科学、合理的电脑安全防御机制，更完善、全面地维护电脑系统的安全。

本书结构清晰，通俗易懂，能够带领读者轻松地掌握防范黑客攻击、清除病毒和木马的各种有效技能，以便更好地保护电脑系统的安全，适合初、中级读者阅读学习。

本书由“智联教育”组织编著，参与策划、编写、排版的主要人员有：甘立富、徐春红、曾全、覃明楔、赵乾伟、尹小港、叶俊、许明等。由于编者经验有限，书中难免有疏漏和不足之处，恳请专家和读者不吝赐教。

读者在使用本书过程中如有其他问题、意见或建议，可以通过下面的方式和我们联系：

Http://www.ChinaMook.com

E-mail:mook@vip.sina.com

QQ：35691532

智联教育

www.ChinaMook.com

目 录

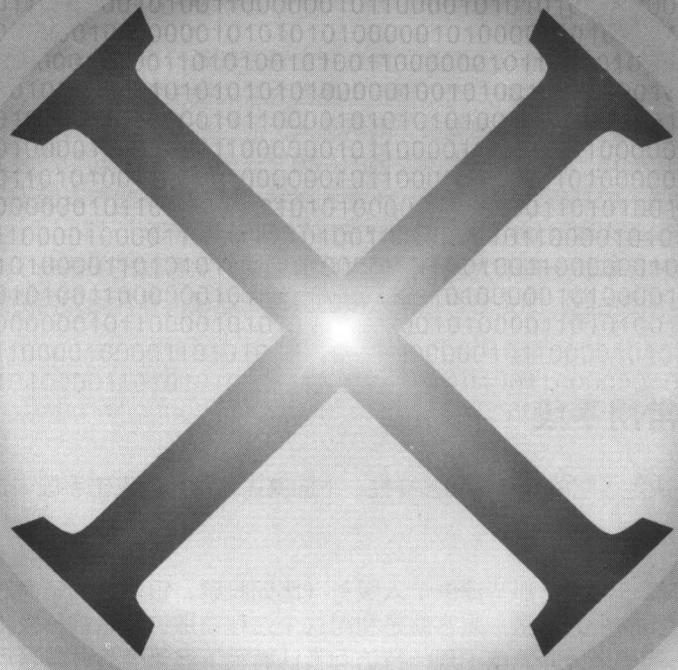
第一部分 黑客防范

第二部分 系统加密

第三部分 安全防范

防范黑客X秘笈

精华本



●第一部分 黑客防范

●第二部分 系统加密

●第三部分 安全防范

在许多人眼中，黑客往往是利用其掌握的计算机技术肆意进行攻击网络、盗取商业机密的人。因此，黑客以及黑客技术对于大多数的网民而言，蒙上了一层神秘的面纱。其实并非完全如此，本章将带你走进黑客世界，揭开黑客的神秘面纱。

第 1 章　初识黑客

- 关于黑客
- 黑客攻击流程
- 黑客常用工具

1.1　关于黑客

1.1.1　认识黑客

黑客，源于英语动词 hack，意为“劈、砍”，黑客即是 hacker 的译音，泛指所有利用高级技术手段，通过网络进入他人电脑系统的人。

他们通常具有硬件和软件的高级知识，并有能力通过创新的方法剖析系统，使更多的网络趋于完善和完全。他们以保护网络为目的，而以不正当侵入为手段找出网络漏洞。

另一种入侵者是那些利用网络漏洞破坏网络的人，他们也具备广泛的电脑知识，但与正规黑客不同的是，他们通常以破坏、窃取或恶作剧为目的。因为这些行为对电脑用户会造成各种程度的损害，所以人们通常对这些人或其行为高度警觉；一提到黑客，就会被联想为以侵犯为目的的对象。从技术角度来看，可以将这些人称为 cracker，或者“骇客”、非法黑客等。

所以，虽然黑客在本质上有很大区分，但大众普遍认为黑客就是那些为了个人目的而故意去破坏他人系统的人。本书的主题，即是分析这些入侵的原理和途径，并介绍如何防范各种恶意攻击的实用方法。

1.1.2　黑客常用手段

网络的开放性决定了它的复杂性和多样性。下面就黑客常用的攻击手段中选取几种加以介绍。

1. 以假乱真

在登录一些站点，特别是那些提供个人服务（比如股票、银行）的站点时，访问者往往会被要求填写一些密码之类的个人信息，黑客就是利用这个过程窃取访问者的秘密。黑客伪造一个登录页面，使其抢在真正的登录页面之前出现，待访问者认真写下登录信息并发送后，真正的登录页面才姗姗而来。

防范这种情况，最佳的解决之道就是防患于未然，经常查看服务器的运作日志，若发现疑点要及早处理，将隐患消灭在萌芽状态。

2. 声东击西

黑客利用某些防火墙漏洞，将自己的 IP 请求设置为指向防火墙的路径，而不是受防火墙保护的主机，畅通无阻地接近防火墙，此时再利用防火墙作跳板，便可轻松地入侵主机。如有这种情况发生，就得考虑是否应该更换防火墙，或升级原来的防火墙，为它打上补丁。

3. 单刀直入

黑客凭借自己高超的技术，通过分析 DNS（域名管理系统）而直接获取 Web 服务器等主机的 IP 地址，从而为入侵主机彻底扫除障碍。

对付这种黑客，除了不要接受免费域名服务，几乎没有更好的办法。因为正规的注册域名服务一般都会有有效的安全手段，可以保证少受攻击或不受攻击。

4. 旁敲侧击

电子邮件其实是一种很脆弱的通信手段。一方面电子邮件的安全性很差，传送的资料很可能丢失或被拦截；另一方面特洛伊木马等黑客程序大都通过电子邮件进驻用户的机器。

但电子邮件是网络上用得最多的东西，许多公众网站和大公司局域网，出于吸引访问者或工作的需要，提供免费邮件或内部邮件的服务，因此邮件服务器就成了黑客们攻击的对象。

防范这些黑客，可采用以下措施：邮件服务器专设专用，不与内部局域网发生关系；开启防火墙的邮件中转功能，让中转站过滤所有邮件等。

1.1.4 网络安全常识

1. 认识电脑病毒

电脑病毒是人为编制的一种特殊程序，能够搅乱、改变或摧毁电脑中的软件，能够进行复制并感染其他程序。电脑执行这些错误的命令后，将破坏用户数据，甚至使电脑停止工作。

电脑病毒有传染性，危害性很大。它是通过电脑的硬盘、软盘以及联网使用实现传染的电脑病毒交换信息有的是正常的、合法的，有的是不合法的，比如私自复制他人程序等。电脑病毒种类很多，主要表现为以下 4 类：

- 电脑的显示屏幕上出现异常，如出现蹦跳小球等；
- 破坏存储数据；
- 改变磁盘中的存储内容和数据；
- 干扰正常操作，使运算速度下降，甚至使电脑停止工作。

电脑病毒的特点如下。

潜伏性 ——电脑系统被传染上病毒后，并不马上发作。病毒可以潜伏几周或几个月之久，并继续传染而不会被发现。

激发性 ——电脑病毒并不是什么时候都发作，只有当外界条件满足病毒发生的条件时，病毒才开始破坏活动。例如“愚人节”病毒的发作条件是电脑系统日期为愚人节那天，即每年的 4 月 1 日。

传播性 ——在微型电脑系统中，病毒可迅速地在各个电脑之间通过软盘、硬盘（甚至光盘与硬盘）进行传染；在电脑网络中，病毒可很快地在网络中的各个电脑之间传播。

破坏性 ——电脑病毒发作时，会使电脑系统的运行出现各种故障。

2. 什么是 IP 地址

IP 是英语 Internet Protocol 的缩写，意为“互联网协议”。IP 地址构成了整个 Internet 的基础，每台电脑节点都依靠 IP 地址互相区分和相互联系。IP 地址和人的住址一样，是惟一的。

互联网上的计算机无权自行设定 IP 地址。有一个统一的机构 ——IANA 负责给申请组织（如中国电信、中国网通等）分配一个网络 IP 段，该组织可以对自己网络中的每一个主机分配一个惟一的主机 IP（如果通过中国电信 ADSL 上网，IP 地址就是由中国电信分配）。

IP 地址是一个 32 位二进制数的地址，由 4 个 8 位字段组成，每个字段之间用点号隔开，用于标识 TCP/IP 宿主机，比如 61.220.111.1。

3. IP 地址的作用

在 Internet 上，如果想访问别人的电脑，必须知道对方电脑的 IP 地址；如果别人想访问你的电脑，

也必须知道你的电脑的 IP 地址。

已知 IP 地址后，网络服务器将按照所输入的 IP 地址查找相应的电脑，并将信息传送到对方的电脑里。也就是说，主叫方只要获得被叫方的 IP 地址，即可发出呼叫、建立连接、实现应用，比如利用网络电话可以直接通话或者发送文件。

访问网站往往需要输入网址，比如在 IE 地址栏中输入“ http://www.sina.com.cn/ ”即可访问新浪网站。网址只是一个域名，要访问这个网站，网络上的 DNS 服务器会把这个域名翻译成 IP 地址，再查找相对应的服务器。

一般情况下，通过域名和 IP 地址都可以顺利地找到主机。因此，某台电脑被攻击时，其主机的域名或者 IP 地址是被最先确立的攻击目标，例如“www.******.com”或 124.18.65.1 等。

4．什么是端口

简单地说，端口就是计算机和外界连接的通道。不同的端口有不同的功能，例如，网页用的是 80 端口，而计算机上可开启的端口数值范围为 1～65535。常用端口及其解释如表 1-1 所示。

表 1-1

端　口	解　释	备　注
21 号端口	FTP	和 Telnet 服务一样，用户可以从 FTP 服务器上下载或上传资料等，还可匿名登录
23 号端口	Telnet	表明远程登录服务正在运行，从这里可以远程登录到该主机
25 号端口	SMTP	
53 号端口	DNS	
79 号端口	Finger	入侵者利用它获得目标用户信息，查看目标机器的运行情况等
80 号端口	HTTP	表明 WWW 服务在端口运行
110 号端口	POP	邮局协议
139 号端口	NetBIOS	共享服务

除了以上列表中的端口外，还有一些其他端口（如 135、445 等），有需要的读者可以自己去查资料。需要说明的是，并不是所有的端口都是有用的。

1.2　黑客攻击流程分析

下面就来看看黑客是如何攻击用户电脑的。一般来讲，黑客攻击的流程大致如图 1-1 所示。

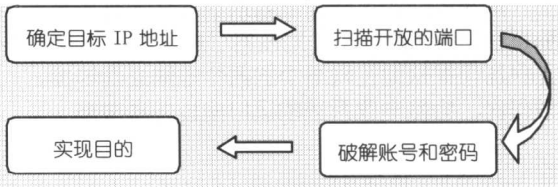


图 1-1　黑客攻击流程图

黑客在发动一场攻击之前，一般需要先选定攻击目标，就是要确定目标电脑的 IP 地址。

确定了目标 IP 地址以后，黑客还需要收集目标计算机的各种信息，比如操作系统版本、开放的服务端口、端口提供的服务类型及软件版本等。这些信息能帮助黑客发现目标的弱点，比如目标电脑开放的端口和漏洞，等等。

黑客查看对方机器 IP 地址的方法很多。要进行有效的安全防范措施，就必须先了解黑客 IP 探查工具。下面就简单介绍几款黑客常用的 IP 查探工具。

1．利用 QQ 补丁程序

QQ 每推出一个新版本，网络中都会出现相应的补丁程序。利用这种补丁，即可查看到在线用户

的 IP 地址、所在地及 QQ 版本等信息，如图 1-2 所示。

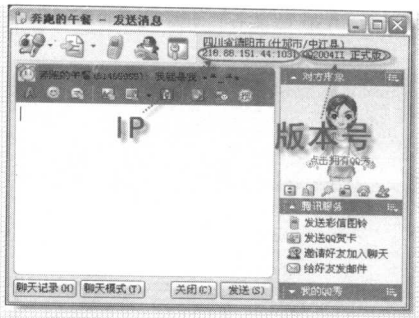


图 1-2　利用 QQ 补丁查看 IP

2. 利用 QQ 狙击手

在黑客获取 QQ 用户 IP 的软件中，最常用的是 QQ 狙击手，其工作界面如图 1-3 所示。

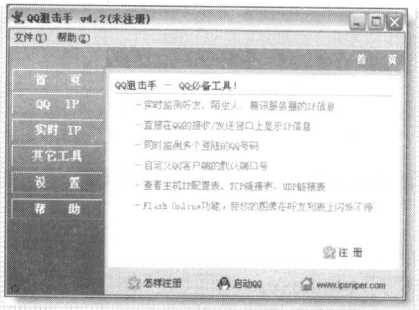


图 1-3　QQ 狙击手界面

该软件几乎支持 QQ 目前的所有版本，其主要功能如下：

- 实时监测好友、陌生人、腾讯服务器及腾讯广告服务器代理的 IP 地址及端口号；
- 直接在 QQ 的接收/发送窗口上显示 IP 以及地理位置信息；
- 可以同时监测多个登录的 QQ 号码，并且能够自定义 QQ 客户端的默认端口号；
- 独特的 IP 助手功能，可以让用户方便地查看主机 IP 配置信息、TCP 链接表以及 UDP 链接表；
- Flash Online 功能，能够使用户的 QQ 在自己的好友 QQ 列表上不停闪烁。

3. 利用 Iplocate

Iplocate 是一款用于查看 QQ 好友及陌生人 IP 地址的软件。不管对方是否在线，只要向对方发送信息或是对方向你发信息，都可以查出其 IP 地址及所处地区，其监听模式运行界面如图 1-4 所示

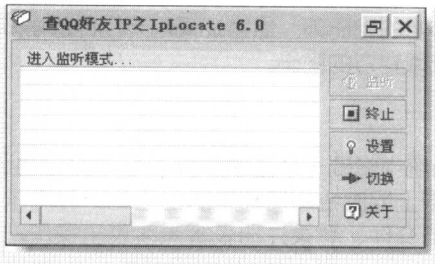


图 1-4　监听模式