个人用网安全与黑客防范技术

数字时代工作室　编著

人 民 邮 电 出 版 社

图书在版编目（CIP）数据

个人用网安全与黑客防范技术/数字时代工作室编著.—北京：人民邮电出版社，2001.8

ISBN 7-115-09528-0

I.**个**… II.**数**… 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（**2001**）第** 049216 **号**

内 容 提 要

本书对多种来自网络的威胁进行了分类，明确地将网络安全的原理和实用技巧放在了首位，从病毒和黑客的工作原理出发，围绕对网络病毒和网络黑客这两个主要方面的防范措施展开了深入的论述，并介绍了多种用于防范网络威胁的工具。本书的最大特色是书中配有大量非常实用的操作范例，综合性和实用性强。

本书所面对的对象主要是个人用户，对相关专业的大专院校师生、培训班学员也有一定的参考价值。

个人用网安全与黑客防范技术

◆ **编　　著　数字时代工作室**

责任编辑　张瑞喜　姚予疆

◆ **人民邮电出版社出版发行　　北京市崇文区夕照寺街** 14 **号**

北京汉魂图文设计有限公司制作

北京顺义向阳胶印厂印刷

新华书店总店北京发行所经销

◆ **开本：**787×1092　1/16

印张：20.5

字数：480 **千字**　　2001 **年** 8 **月第** 1 **版**

印数：1 –　000 **册**　　2001 **年** 8 **月北京第** 1 **次印刷**

ISBN 7-115-09528-0/TP.2381

定价：31.00 **元**

前　言

近两年来，国内的上网用户增长非常快。截止到目前，全国上网用户的数量已经接近了2000 万。同时，国内网络服务的类型正在日趋多样化。但是，在繁荣的背后，来自网络上的威胁也日益加剧。各种不请自来的非法访问者，驻留本地计算机内的暗探——特洛伊木马，大量经过电子邮件携带的各类病毒，以及在网上聊天时不经意就来到身边的 OICQ 炸弹等，时时威胁着用户计算机的安全。事实上，绝大部分网民在上网的过程中，网络安全意识淡薄，没有实施有效的网络安全保障措施。

现在，人们正在越来越多地依赖网络来改变自己的生活方式，例如网上购物、网上交易、网上投资和网上数据存储等。如果在访问 Internet 的过程中不注意网络安全，一旦重要的数据被破坏或被窃取，那么后果将不堪设想。为了能够引起人们对网络安全问题的足够重视，并为大众介绍实用的网络安全防护技巧，我们组织编写了这本书。本书的讲解详略得当，综合性、实用性都很强，适合具有一定 Internet 基础的广大读者，是广大商业和家庭用户不可多得的参考工具书籍。特别建议那些在个人电脑中存储有重要数据的用户阅读本书。

严正声明：本书中提到的“黑客”工具只是为了帮助用户更好地掌握防范黑客攻击的方法。任何人不得利用这些工具攻击他人或网站，否则将会受到法律的严惩！

参与本书编写工作的人员主要有水超、于纲、张岩和陈晓华等。由于作者本身的水平有限，再加上创作时间仓促，本书难免存在疏漏和错误之处，衷心希望各界专家和读者朋友不吝赐教。

数字时代工作室

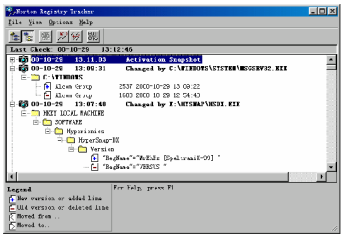
目　　录

第 1 章

来自网络的威胁

本章要点：

- 计算机的本地防护
- 计算机的网络防护



当今世界中没有一种工具能像 Internet 这样改变着世界，它以前所未有的速度改变全球用户的通信方式，这种新的大众传媒以其快速、方便和简单的特点受到人们的普遍欢迎。在过去的两年中，Internet 飞速增长，融入了大量的信息—— 从商品买卖到就业机会、从电子公告牌（BBS）到 E-mail、从新闻报道到电影预告、文学评论以及娱乐。不管是微不足道的小事，还是关系全球的大事，几乎人类有史以来的所有知识都可以在网上找到，人们享受到了巨大的便利。

但是，Internet 这个虚拟的世界就像现实世界一样，也有它的阴暗面。一方面，电脑病毒已经发展到网络病毒，它就像幽灵一样伺机破坏用户的电脑，摧毁用户的重要数据；另一方面，有一批人在网络中窥视他人的秘密、改变商业合同、盗窃机密，给用户造成巨大的损失，他们就是——“ 黑客 ”。

计算机的网络安全防护分为两个方面，一个是计算机的本地安全；一个是对黑客的防范。本章将概括介绍这两个方面的基本内容。

1.1 计算机的本地防护

很可能用户周围的某些人，出于某种目的，会利用一些计算机漏洞进入用户的电脑，窃取用户的重要数据，或者通过某种方式间接地将计算机病毒输入到用户的计算机中，给用户造成损失。当然用户在使用计算机的过程中，如果缺乏必要的安全防范意识，也会不经意间使计算机感染病毒。因此计算机的本地安全是至关重要的，是计算机网络安全的基础。计算机的本地防护包括对计算机本地登录的防护、对病毒的防范等等，这就要求用户综合利用我们介绍的内容。

1.1.1 防范病毒

1949 年，电脑的先驱者约翰·范纽曼（John Von Neumann）在他的一篇论文《复杂自动装置的理论及组织的进行》中勾勒出病毒程序的蓝图。从此，计算机病毒就像是一个魔王开始威胁着整个计算机世界的安全，使人们谈毒色变。

20 世纪 80 年代中期，美国一个计算机系研究生设计了一种“ 蠕虫 ”病毒，在短短几个月的时间内攻击了包括五角大楼、银行、学校在内的上百万台计算机，使它们的重要数据在瞬间被破坏，重要服务无法进行，整个网络处于瘫痪状态，造成了无法估量的损失。

1999 年 4 月 26 日，一种新型的 CIH 病毒爆发了，它不仅破坏用户的所有数据，更直接破坏用户的硬件，摧毁用户的硬盘和主板。CIH 病毒是中国台湾省大同工学院一位名叫陈盈豪的学生设计的，CIH 即“ 陈盈豪 ”三字的汉语拼音缩写。这个软件原本是他的一个小小恶作剧，但因特网巨大的威力将之传送到世界的每一个角落，并造成 1999 年全球大规模的 CIH 病毒发作。

按美国国家计算机安全协会发布的统计资料，当前的计算机病毒已经达到 18000 种，而且每个月又会产生 200 种新型病毒。可以这样说，在计算机世界中没有一台计算机可以对病毒免疫，对于经常上网的用户来说必须常规性、系统性地对付病毒。因此我们将在第三章详细介

绍病毒的原理，揭开它的神秘面纱；在第 4 章介绍病毒防范工具，使用户掌握保护自己的方法。

1.1.2 Windows 系统安全措施

操作系统可以说是计算机世界最重要，也是最难编写的软件。它是其他所有软件运行的平台和基础，可以控制计算机的一切软件和硬件，因此它的安全是计算机安全的首要目标。当前计算机操作系统主要包括 UNIX 系统和 Windows 系统。

UNIX 系统是世界上高端计算机广泛使用的操作系统，主要应用于工作站、服务器、巨型计算机等高性能计算机中，为用户提供一个高效、灵活的运行环境。但是对于个人用户来说，这个操作系统存在着使用复杂、维护困难等缺点，因此在个人计算机上使用得不多，本书将不做介绍。

Windows 操作系统是美国 Microsoft（微软）公司出品的一款新型操作系统，它分为个人操作系统和服务器操作系统两大类。其中个人操作系统包括 Windows 95、Windows 98 以及最新出现的 Windows Me。服务器类操作系统包括 Windows NT 和 Windows 2000。Windows 操作系统使用简单、维护方便，尤其是它的图形操作界面，更使用户倍感亲切。因此当 Windows 系统一出现，就很快风靡全球，成为个人用户操作系统的主流。

根据美国国防部（DOD）的技术标准，操作系统的安全等级分成了 D1、C1、C2、B1、B2、B3、A 级，其安全等级由低到高。目前主要的操作系统的安全等级都是 C2 级，其特征包括：

- ✧ 用户必须通过用户注册名和口令让系统识别。
- ✧ 系统可以根据用户注册名决定用户访问资源的权限。
- ✧ 系统可以对系统中产生的每一件事进行审核和记录。
- ✧ 可以创建其他具有系统管理权限的用户。
- ✧ B1 级操作系统除上述机制外，还不允许文件的拥有者改变其许可权限。
- ✧ B2 级操作系统要求计算机系统中所有对象都加标签，且给设备（如磁盘、磁带或终端）分配单个或多个安全级别。

对于 B 级的操作系统，美国是作为军火产品而严格控制的，即使是他的同盟国也难以取得。在我国，绝大多数的用户使用的是 C 类的操作系统，例如，Unix、Windows NT，因此我国的计算机安全问题就更加突出。

Windows 操作系统的安全主要包括注册表安全、Windows 口令的安全、Windows 的设计漏洞防护等。

Windows 为了保护用户的计算机安全，在许多地方使用了安全措施，本书将在第 2 章对 Windows 系统的安全做重点的介绍。其中，Windows NT 和 Windows 2000 更是为用户计算机的安全设计了许多保护措施。在第 14 章中，我们也将结合 IIS 服务器的安全，介绍 Windows 2000 在这些方面的具体措施。

1.1.3 防止用户密码被盗

用户密码是识辨用户身份的关键，如果用户密码丢失，就意味着用户网站的失控。用户可以使用加密技术把自己的密码文件加密，并记住密码注意事项。用户可以参考第 3 章的内容。

1.2 计算机的网络防护

计算机网络防护主要是防止黑客从网上利用操作系统的一些漏洞和计算机的安全设置的一些失误，入侵用户的计算机，达到控制用户计算机、获取计算机上的保密数据的目的。

1.2.1 “黑客”（Hacker）的兴起

夜深了，加尼福尼亚州一个小镇的一座小楼的灯却还闪着微光。房间内，计算机闪动着咒语般的符号，微弱的荧光照亮了一张只有十七、八岁的幼稚的脸，手指在键盘上飞快地闪动，炯炯的目光紧紧盯着屏幕，眼睛中闪烁着紧张和兴奋，甚至还带着疯狂的神情。忽然计算机上红光闪动，警报器叫响，但那个年轻人却露出了笑容，从容关闭了计算机。他知道那是美国联邦调查局的反黑客程序启动了，因为他就在刚才又一次成功地闯入了美国联邦调查局的内部网络，他不禁为自己的成就而骄傲，也为联邦调查局的疏忽而嘲笑，他有一个名字叫“黑客”。

1. 黑客的历史

“黑客”一词是英文 Hacker 的谐音，在英文中其意思是：“乱砍、劈”，另一个意思是指“受雇从事艰苦工作的人”。这一词在计算机领域的出现可以一直追溯到第一台计算机的发明，那时计算机非常复杂，只有一些最聪明的人才能用最简单的程序操纵计算机以达到极高的效率。因此在当时，Hacker 一词并不是指入侵计算机系统的人，而是指那些非常聪明、富有创造力的高级程序员或计算机设计人员，而那些计算机的破坏者就被称为 cracker（破坏者）。

到了 1969 年，计算机世界出现了一件大事—— UNIX 的发明。它是由贝尔实验室的 Ken Thompson 发明的，当时他只是想在自己的机器上编写一个适合玩游戏的系统，当他用汇编语言做完第一版 UNIX 后，它只能在 PDP－7 的机器上运行。但是，不久以后贝尔实验室的另一个天才人物 Dennis Ritchie 发明了一个里程碑式的程序设计语言——C 语言，于是 KenThompson 和 Dennis Ritchie 合作，用 C 语言把 UNIX 重新写了一遍，并把它移植到数种机器上。于是 UNIX 和 C 语言以它们的易用性、开放性开始在贝尔实验室流行起来，到了 1980 年，它已经传播到许多大学和研究机构，数以千计的个人用户也开始安装了 UNIX。

20 世纪 80 年代，Internet 的原型 ARPANET 开始出现，它最初是由美国国防部出资兴建的一个数字通信网络，但当它把美国的各个大学和研究机构联系起来以后，其史无前例的合作方式就在美国流行起来。它使得全世界的 Hacker 能聚集在一起，相互交流经验和资源，使得 Hacker 文化开始出现。

1992 年，芬兰的一个学生 Linus Torvalds 开始在一台 386 上编写了一个开放源码式的操作系统 Linux，他通过网络与其他人一起开发，这是软件编写的一个重要模式的开始，它没有严格的产品测试和开发的方针，靠的是大家使用软件，然后发现 bug，修改它或者告诉开发者，这样 Linux 就在不断的更新和完善中发展起来。

可以这样说，Linux 是一大群 Hacker 利用 Internet 完成的，这样 Hacker、Internet 和 Linux 就完美地结合在一起。到这时 Hacker 依然是褒义词，仍是指那些计算机编程高手。

但是在近年，出现了大量通过计算机和网络入侵他人计算机系统的事件，他们以入侵他人的系统为乐，随意修改他人的资料，新闻媒体往往称他们是“黑客”（Hacker），于是 Hacker

一词就成为了网络入侵者的代名词。对此，真正的 Hacker 是强烈反对的，因此读者必须分清 Hacker 和 Cracker 之间的区别。

2. 黑客的解释

现在，Hacker（黑客）的解释就成为了在数据安全领域，一种未经授权、又企图躲过计算机系统安全控制程序的检查而进入计算机网络的用户。黑客通常是一些高级程序员，他们同时掌握有操作系统和编程语言方面的高级知识。黑客们不停地探索新的知识，不停地探测未知世界，能发现系统中所存在的安全漏洞以及导致那些漏洞的原因，并自由地共享他们的发现。

Cracker 的解释是：一个未经许可“ 侵入 ”计算机程序系统的人。Cracker 们通过获取未授权的访问权限，破坏重要的数据，拒绝合法的用户服务，或只是使他们的目标产生些小问题。另外，对正版软件的破坏和对盗版的发展也是 Cracker 的一个重要“ 贡献 ”。

Cracker 和黑客是很容易被区分的，这是因为 Cracker 的行为具有恶意，他们总是在破坏；而黑客却有自己的活动方式，这就是遵守“ 黑客守则 ”。

3. 近年来的黑客大事记

国外计算机互联网出现的安全问题案例：

- ✧ 1994 年末，俄罗斯黑客弗拉基米尔·利文与其伙伴从圣彼得堡的一家小软件公司的联网计算机上，向美国 CITYBANK 银行发动了一连串攻击，通过电子转账方式，从 CITYBANK 银行在纽约的计算机主机里窃取了 1100 万美元。
- ✧ 1996 年初，据美国旧金山的计算机安全协会与联邦调查局的一次联合调查统计，有 53%的企业受到过计算机病毒的侵害，42%的企业的计算机系统在过去的 12 个月中被非法使用过。而五角大楼的一个研究小组称美国一年中遭受的攻击就达 25 万次之多。
- ✧ 1996 年 8 月 17 日，美国司法部的网络服务器遭到黑客入侵，主页被改为“ 美国不公正部 ”、司法部部长的照片被换成了阿道夫·希特勒、司法部的徽章被换成了纳粹党徽、并加上一幅色情女郎的图片作为所谓司法部部长的助手，此外还留下了很多攻击美国司法政策的文字。
- ✧ 1996 年 9 月 18 日，黑客又光顾美国中央情报局的网络服务器，将其主页由“ 中央情报局 ”改为“ 中央愚蠢局 ”。
- ✧ 1998 年 5 月，黑客向五角大楼发动了“ 有史以来最大规模、最系统的攻击行动 ”，打入了许多政府非保密的敏感电脑网络，查询并修改了工资表和人员名单。
- ✧ 1999 年 9 月 19 日出版的星期日时报报道说，英国银行正在被“ 黑客 ”勒索，这些“ 黑客 ”侵入了银行的安全系统并威胁要破坏银行的计算机或将窃取的文件公之于众。
- ✧ 2000 年 2 月 11 日最先是雅虎网站（Yahoo !）遭殃，然后电子零售商 Buy.com 网站在上市当天也挂彩，紧接着 eBay、亚马逊（A mazon.com）和 CNN.com 等顶尖网站也陆续遭遇所谓“ 拒绝服务 ”（denial of service）式攻击，导致系统暂时停摆。雅虎网站的网络系统停止运行 3 小时，这令它损失了几百

万美金的交易。据统计在这整个行动中美国经济共损失了十多亿美金。由于业界人心惶惶，亚马逊（Amazon.com）、AOL、雅虎（Yahoo!）、eBay 的股价均告下挫，以科技股为主的那斯达克指数（Nasdaq）打破过去连续三天创下新高的升势，下挫了 63 点，道琼斯工业平均指数周三收市时也跌了 258 点。遇袭的网站包括雅虎、亚马逊和 Buy.com、MSN.com、网上拍卖行 eBay 以及新闻网站 CNN.com，估计这些袭击把 Internet 交通拖慢了 20%。

我国计算机互联网出现的安全问题案例：

- ✧ 1996 年 2 月，刚开通不久的 Chinanet 受到攻击，且攻击得逞。
- ✧ 1997 年初，黑客成功侵入北京某 ISP，并在清华大学“水木清华”BBS 站的“黑客与解密”讨论区张贴有关如何免费通过该 ISP 进入 Internet 的文章。
- ✧ 1997 年 4 月 23 日，美国德克萨斯州内查德逊地区西南贝尔互联网络公司的某个 PPP 用户侵入中国互联网络信息中心的服务器，破译该系统的 shutdown 账户，把中国互联网信息中心的主页换成了一个笑嘻嘻的骷髅头。
- ✧ 2000 年 2 月 8 日下午，国内著名网站新浪网（www.sina.com.cn）的邮件系统由于被黑客的垃圾邮件塞满而导致崩溃。
- ✧ 2000 年 2 月 29 日，国内一个著名网站的主页被修改，中央是一个红色的圆形，在网页上还有一些意义不明的红字，网页的名称也被改为“HackedBy：Fall AnD Rep3nt———〉hey dog0.gimmie a shell！”。
- ✧ 2000 年 3 月 15 日，IT163 网站遭网上黑客袭击，站点页面被篡改，数据库遭到破坏，网站无法运作，攻击者还在页面上留言。

1.2.2 黑客攻击的主要途径和方法

黑客的进攻主要是寻找目标计算机的漏洞和用户在操作时造成的失误，黑客们拥有三条必胜的秘笈：

- ✧ “通往计算机的路不止一条”。
- ✧ “任何计算机系统都存在漏洞”。
- ✧ “70%的系统攻击成功是由于系统管理员的疏忽造成的”。

他们以此为基本进攻准则，对各种网络展开了进攻。由此可以看出影响计算机网络安全的因素主要包括人为因素和自然因素，其中人为因素的危害最大，包括以下几个方面。

- ➢ 人为的无意失误

主要是操作员安全配置不当而造成的安全漏洞。不合理地设置资源访问的权限控制、用户安全意识不强、用户口令选择不慎、用户将自己的账号随意转借他人或与别人共享等都会对网络安全带来威胁。

- ➢ 人为的恶意攻击

这是计算机网络所面临的最大威胁，黑客的攻击和计算机犯罪就属于这一类。这也是本

书要重点介绍的地方。

- 网络软件的漏洞和“后门”

网络软件不可能是百分之百的无缺陷和无漏洞的，这些漏洞和缺陷恰恰是黑客进行攻击的首选目标。曾经出现过的黑客攻入网络内部的事件，大部分就是因为网络软件有漏洞，导致安全措施不完善造成的。另外，软件的“后门”都是软件公司或黑客编写的一种程序，一般潜伏在计算机中不为用户所知，但一旦“后门”洞开，造成的后果将不堪设想。

1. 进攻的种类

黑客的攻击可以分为以下两种，这两种攻击均可对计算机网络造成极大的危害，并导致机密数据的泄漏。

一种是主动攻击。首先，黑客以各种方式收集网络的有效信息，从而找出用户的漏洞，通过漏洞进入系统，获得系统的最高权限，然后有选择地破坏信息的有效性和完整性，这就是纯粹的信息破坏，这样的网络侵犯者被称为积极侵犯者。积极侵犯者截取网上的信息包，并对其进行更改使它失效，或者故意添加一些有利于自己的信息，起到信息误导的作用，或者登录进入系统，使用并占用大量网络资源，造成资源的消耗，损害合法用户的利益，积极侵犯者的破坏性最大。他们获得用户信息的方法包括以下几种。

- DNS 服务器

可以访问主机的 IP 地址表和它们对应的主机名。

- Finger 协议

能够提供特定主机上用户们的详细信息（注册名、电话号码、最后一次注册的时间等）。

- Ping 实用程序

可以用来确定一个指定的主机的位置并确定其是否可达。把这个简单的工具用在扫描程序中，可以检查网络上每个可能的主机地址，从而可以构造出实际驻留在网络上的主机清单。

- TraceRoute 程序

得出到达目标主机所经过的网络数和路由器数。

这些程序的使用我们将在以后的章节中详细介绍。

另一类是被动攻击，它是在不影响网络正常工作的情况下，进行截获、窃取、破译以获得重要机密信息。这种仅窃听或只收集信息而不破坏网络中传输信息的侵犯者被称为消极侵犯者，它包括窃听和通信流量分析。窃听是指在通信线路上进行窃听，获得机密信息；通信流量分析是指通过分析通信流量获取被攻网络的安全弱点，从而便于实施进一步的攻击。

例如，sniffer（网络嗅觉器）可以将局域网上的任何数据包截获下来，从而分析出数据包中的敏感信息（如用户的账户和口令）从而达到攻击用户机器的目的。而 NetXray 应用程序可以分析局域网中的信息流量和它的网络拓扑结构，从而找到网络的弱点，然后再加以攻击。

2. 主要的进攻方式

以下是黑客进攻的一些主要方式。