“十五”国家重点电子出版物规划项目·计算机知识普及和软件开发系列

编程宝典
2002
2

北京希望电子出版社 总策划
刘庆（Sharpwiner） 编 写

解读红客内幕大曝光

翔实——经过实践检验
技巧——红客大联盟的集体智慧
专业——各种 WINDOWS NT/2000 系统漏洞
有趣——OICQ 及江湖游戏等热门软件攻防

中国科学出版集团
北京希望电子出版社

“十五”国家重点电子出版物规划项目·计算机知识普及和软件开发系列

编程宝典
2002
2

北京希望电子出版社 总策划
刘庆（Sharpwiner） 编 写

解读红客内幕大曝光

翔实——经过实践检验
技巧——红客大联盟的集体智慧
专业——各种 WINDOWS NT/2000 系统漏洞
有趣——OICQ 及江湖游戏等热门软件攻防

中国科学出版集团
北京希望电子出版社

内 容 简 介

本书是一本红客技术入门指导书，作者本人就是红客大联盟网站的站长。书中详实地介绍了各种红客的入门技、战术，以及各种技巧，这些技、战术以及各种技巧都是经过红客大联盟的各个成员在实践检验中总结出来的，着重讲解了红客对系统漏洞利用的技巧、防火墙和服务器的安全防范知识以及 OICQ、江湖游戏等一些网络上热门的交流工具攻防策略，具有相当的可靠性和实用性。

本书内容包括第 1 章网络安全基础；第 2 章红客攻击技巧；第 3 章 Windows 攻击技巧；第 4 章红客工具介绍；第 5 章电脑安全与病毒防范；第 6 章红客文化宣传等。对于从事网络安全的技术人员以及红客技术的爱好者来说，本书是一本很实用的学习和参考书籍。

本版 CD 内容包括多种工具软件，大量工具软件的介绍及链接。

盘书系列名：“十五”国家电子出版物规划项目　计算机知识普及和软件开发系列
编程宝典 2002（2）
盘　书　名：解读红客——内幕大曝光
总　策　划：北京希望电子出版社
文本著作者：刘庆
责任编辑：赵文博
CD 制作者：希望多媒体开发中心
CD 测试者：希望多媒体测试部
出版、发行者：北京希望电子出版社
地　　址：北京中关村大街 26 号，100080
网址：www.bhp.com.cn　E-mail: lwm@hope.com.cn
电话：010-62562329,62541992,62637101,62637102,62633308,62633309（发行部）
010-62613322-215（门市）　010-62547735（编辑部）
经　　销：各地新华书店、软件连锁店
排　　版：希望图书输出中心　董淑红　刘英
CD 生产者：北京中新联光盘有限责任公司
文本印刷者：北京双青印刷厂
开本 / 规格：787 毫米×1092 毫米　16 开本　16.5 印张　390 千字
版次 / 印次：2002 年 1 月第 1 版　2002 年 1 月第 1 次印刷
印　　数：1-5000 册
本 版 号：ISBN 7-900088-04-0
定　　价：30.00 元（本版 CD）

目　录

第 1 章　网络安全基础

1.1　“红客”备受媒体的关注

从今年 4 月中美撞机事件以来，一种情绪、一个人群引起了人们的注意，自称为“红客”的一群计算机安全爱好者在网上组织起来的团体以攻击美国网站的方式表达了国人的民族情绪，其规模之大甚至引起了国际媒体的争相报道。

4 月 30 日上海热线报道了红客大联盟攻击美军网站新闻（见图 1.1）。

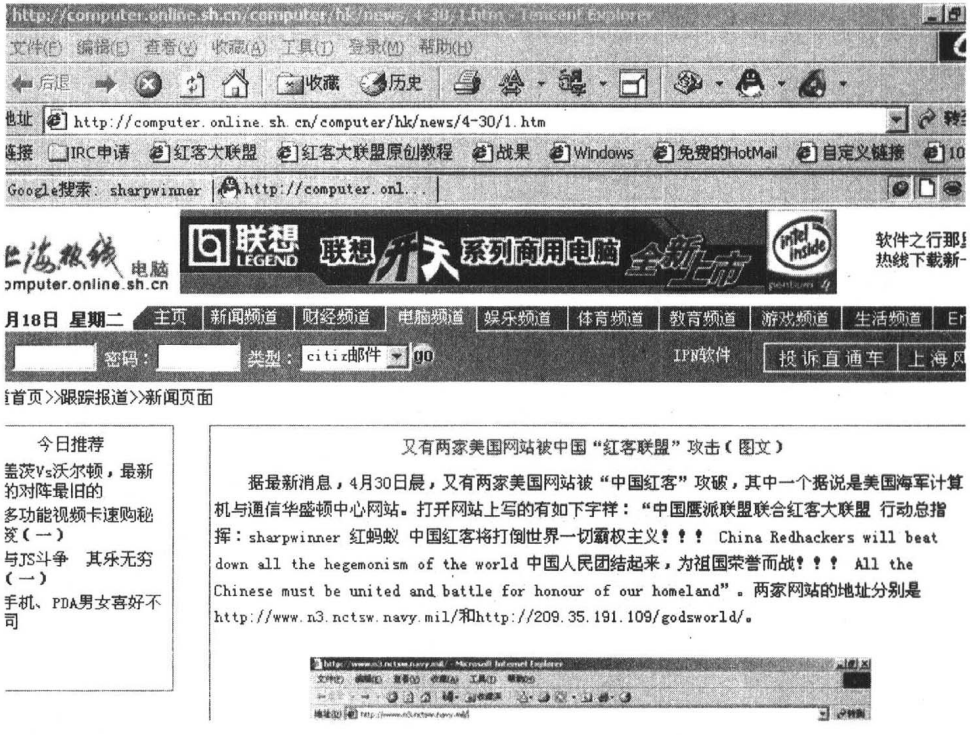

图 1.1　上海热线对红客联盟攻击美军网站的报道

5 月 2 日，中华网报道了红客大联盟攻击近百家美国网站的新闻（见图 1.2）。

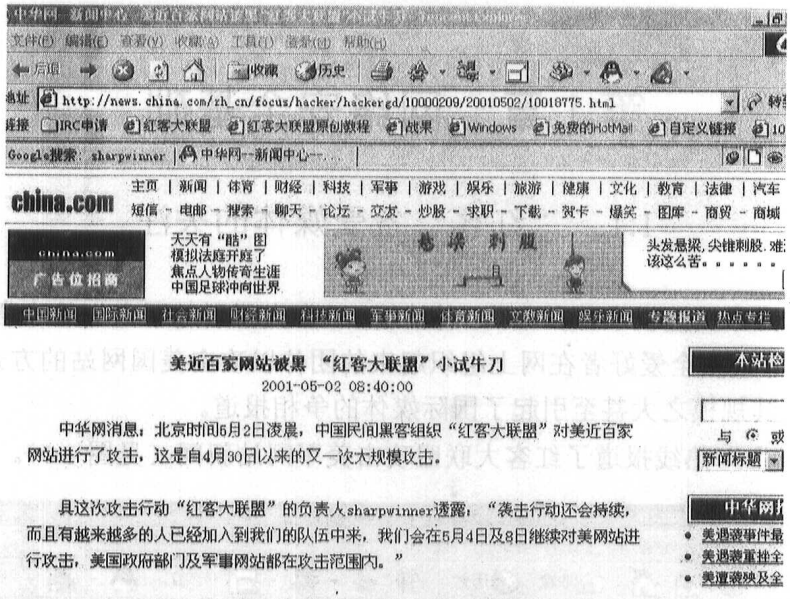

图 1.2　中华网对红客联盟攻击百家美国网站的报道

5 月 4 日，上海热线又报道了红客大联盟攻击美政府站点的 5.4 青年节特别行动（见图 1.3）。

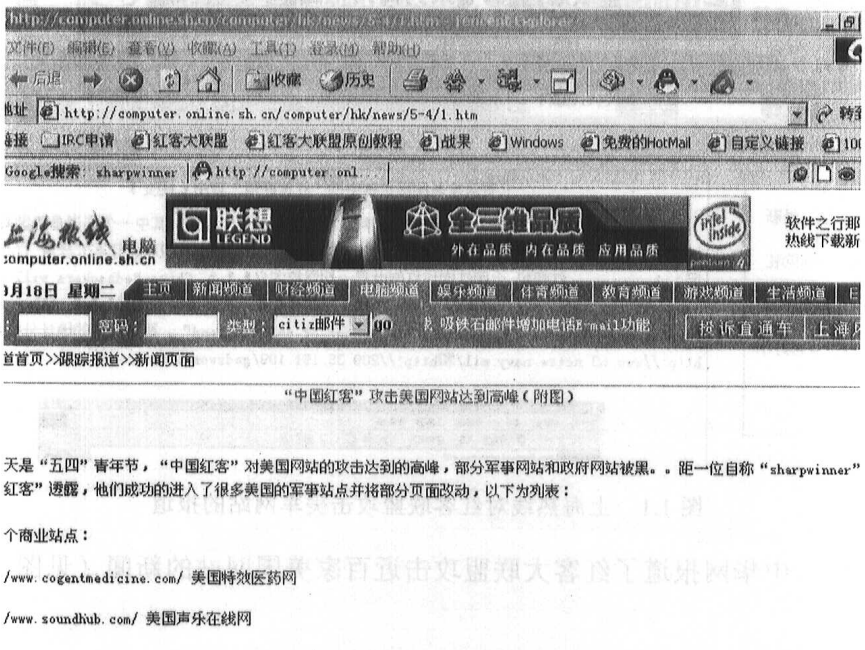

图 1.3　上海热线的报道

5 月 8 日，新浪、中华网、网易等近百家媒体争相报道了红客大联盟对美的 5.8 终

结站（见图 1.4）。

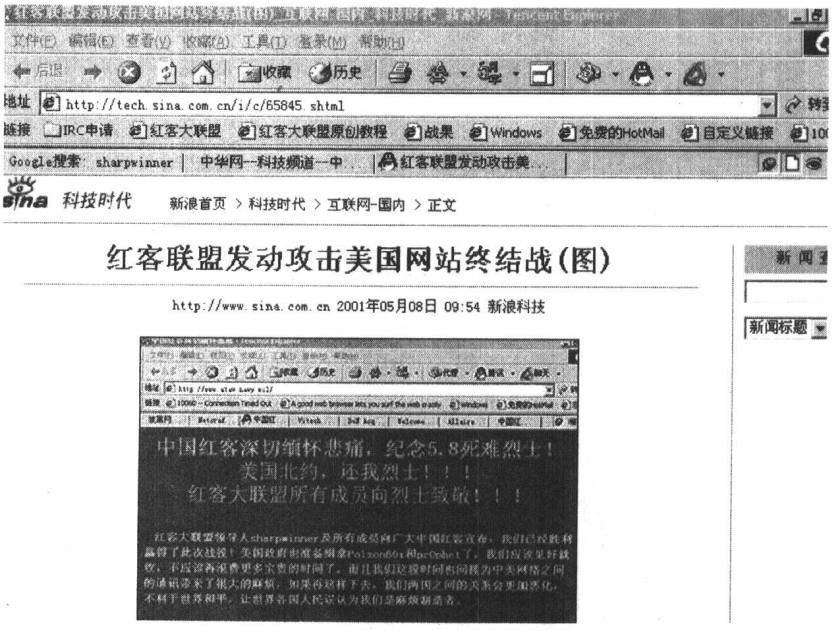

图 1.4　新浪网对红客联盟攻击美国网站的报道

红客逐渐开始成为媒体关注的对象、老百姓饭后的谈资。7 月，媒体又对我们红客大联盟攻击日本政府站点以纪念 7.7 历史事件进行了报道（见图 1.5）。

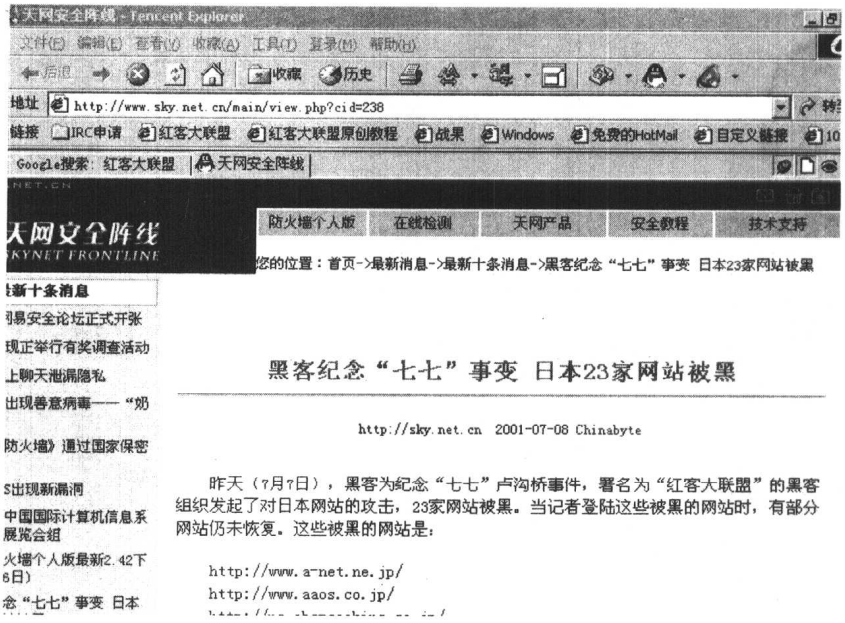

图 1.5　天网对红客联盟攻击日本政府站点以纪念 7.7 历史事件的报道

不久前，日本首相小泉纯一郎不顾各国反对公然参拜靖国神社，我们红客大联盟在第一时间给予日本政府网站以沉重的打击！国内各家媒体对此事件进行了大幅报道（见图 1.6）。

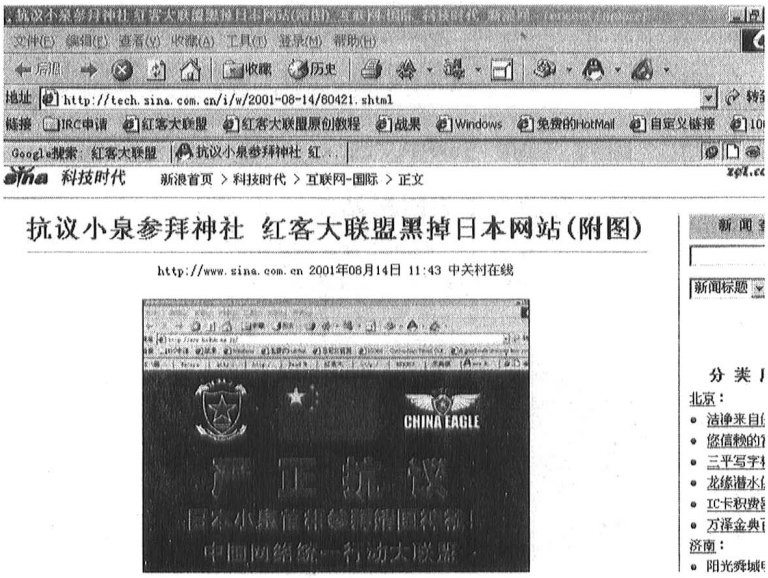

图 1.6　关于“抗议小泉参拜神社 红客大联盟黑掉日本网站”的报道

甚至连传统媒体——《北京青年报》也要对我们红客大联盟的负责人进行采访。以下为《北京青年报》的报道（见图 1.7）。

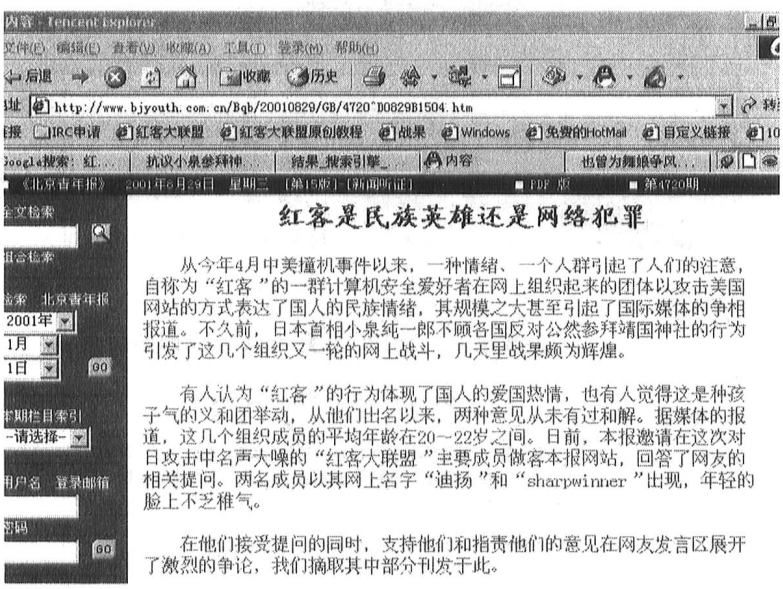

图 1.7　北京青年报的报道

从此，红客浮出了水面，成为曝光度高的一个网络群体。

1.2　红客、黑客与入侵者

所谓红客(RedHakcer)，在传统意义上说，是“一群热爱国家、团结、进取的崇尚网络安全技术研究”的有志青年。

红客产生的年代还不太久远，想要知道红客的历史，那还得追溯到红客的前身——黑客！

(1) 黑客

在个人电脑刚刚兴起的年代，“黑客”以“计算机为人人所用”为宗旨，在互联网时代，黑客们又提出信息共享。

也正是因为有这些理想主义色彩的主张，使得“黑客”这个名称成为一个褒贬不一的词。在虚幻的网络中，他们扮演着技艺高超的神秘人和罗宾汉式侠客的角色，享受着公众的崇拜。

虽然种种黑客行为闯下了不少弥天大祸，但他们利用那精湛的技术也创造了无数令人称服的记录，而且黑客的存在在客观上也促使网络安全技术有了很快的发展。很多网络安全技术人员也是黑客出身的，就连微软的创始人比尔·盖茨也曾经有过“黑客行为”，学生时代时，他利用黑客技术改动班上课程表，让自己周围坐的都是漂亮女生。

尽管很多人对黑客是赞赞称道，但各国政府均出台了相关的法律法规，对他们危害网络秩序的行为给予制裁，美国最负盛名的黑客——凯文·米特尼克在入侵北美空军防务指挥系统后，多次被判刑。在这以后，黑客内部也产生了不同的流派，一部分人标榜入侵系统但不从事破坏性活动，他们把从事各种破坏活动的黑客称为“挎客”(Cracker)，也就是入侵者。

(2) 入侵者

入侵者是指那些强行闯入远程系统或者以某种恶意的目的干扰远程系统完整性的人。入侵者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。这部分人通常入侵一个系统都是为了某种商业目的而做的，例如非法获取一个电子商务网站的会员资料，以勒索电子商务公司而获取巨额利润。因此，入侵者是各国政府坚决打击的目标。作为爱国红客团体也是非常痛恨这种行为的，并准备联合业界一些网络安全团体成立一个网络安全自律团体来配合政府对这些人予以坚决打击！

(3) 红客

黑客在中国产生的时间也不是很长，但是中国黑客们的一系列行动，的确让国外的

黑客刮目相看。

1998 年 8 月，印尼的大规模排华事件中印尼暴民的暴行引起国人的愤慨。由于中国网民的人数有限，和黑客手法较强的技术性，局限了被黑网站的数量和份量，早期红黑客团体由此受到国人的关注和对红黑客技术的探求欲。

1999 年 5 月，期间以美国为首的北约在南斯拉夫悍然轰炸我驻南使馆，促使义愤填膺的中国红黑客们的大举攻击。相隔一年，这次有分量的政府网站有很多能回想起的有美能源部、内政部、海军部空军基地，应该还有白宫。当时的美国国旗曾经被改换成骷髅海盗的标志。

1999 年 7 月，李登辉公然发表臭名一时的“两国论”。两岸局势从而提升至 1992 年共识后的最紧张的状态，国内的红黑客也正是在此时对台湾众多“政府”网站进行了“统一”，部分持鼓吹态度的台湾媒体也受到了攻击。

2000 年初，就日本的公然不顾中国及亚洲人民感受，企图篡改历史，否认侵略，推卸战争罪行进行了出击。此举一出，遭至亚洲人民的强烈不满，这次也是受到中国及中国以外的黑客就同一目标不约而同的相继攻击。

2001 年 2 月，中国消费者得不到日本企业（东芝笔记本、三菱、日航）相同对待，加之日本反华日渐嚣张，中国红黑客连续一个半月对日本右翼团体以及上述企业网站进行了网络攻击。

2001 年 5 月，导火索是撞机事件和美国黑客对中国的挑衅性的入侵，加之长假期和国内媒体的关注炒作，使得网络安全意识首次受到国内政府企业的重视。红黑客到底能在外交争端中起多大的作用等议题讨论得沸沸扬扬。

2001 年 8 月，红客大联盟已经在 8 月 10 日和国内部分合作的团体相约对日本进行大规模的网络打击。但最后是针对日本领导人参拜靖国神社。红客大联盟在第一时间对日本进行了网络打击，在随后的几天里，国内的其他网络安全团体也相继有所行动。由于红客大联盟联合了中国鹰派成功的入侵了美国 NAVY 和众多政府网站而受到了业界的关注和认可。红客大联盟的域名 www.cnredhacker.org 在五一期间得到加拿大华人的捐赠。

中国黑客与西方黑客的一个不同之处就是，中国黑客有一种泛政治化的倾向，如果说西方黑客的思想根源是自由主义的话，中国黑客的思想根源则是民族主义。在中国黑客组织“中国鹰派”网站的首页公然标榜着：“民族主义振兴中国。”

为了区别于崇尚自由主义、资源共享为目的的西方传统黑客，我们以表达政治情绪和立场为主要宗旨的中国黑客，给自己起了个有特色的名字——“红客”（RedHacker）。于是，“红客”诞生了。为了能够实现理想，红客成立了“红客大联盟”（The Redhacker's

Alliance)，号召以网络安全技术来维护国家的利益。

1.2.1　网络安全问题的初步了解

随着互联网的高速发展，网络安全问题也越来越受到人们的关注。主要是由于互联网的主导系统 UNIX 是一个开放的系统，所有的用户都能对系统进行分析并提出问题，安全性的问题尤其被用户所关注。在互联网上也发生过非常多的安全性的问题，这样让安全问题成为了被关注的焦点。但是基于此就对互联网失去信心是大可不必的，虽然互联网不是一个安全性非常高的网络系统，但也不是想象的那样不可信赖，主要是因为互联网的开放性，让很多安装方面的问题比较公开。但是只要正确的使用它，也是可以保证它的安全性的。

一般来说对待网络安全问题通常有两种不同的态度，第一种为保守的态度，认为应该将安全问题隐藏起来才是最好的解决办法。表面上看起来，隐藏就可以避免安全问题，但是人们也不能证明不会被人发现安全漏洞，特别是入侵者，也可以说他们不能阻止掌握了这种漏洞的人不去利用这些安全问题。现在世面上有很多商业软件都是采取的这种态度，事实上这些安全性很低的软件到了攻击者和网络安全专家面前，漏洞就很容易被发现。另外一种是比较积极的态度，认为安全问题不应该隐藏，只有不断地去发现和解决这些安全问题，才能让系统变得更安全。这种态度至少可以让用户了解到哪些是安全的，哪些还存在问题，从而可以避开安全问题，同样在开发软件时也采用这种方法，安全漏洞就能够很快的被发现并修补上，如果一个软件经受住了众多的使用者的考验，那么开发者以及使用者就不用担心严重的安全性问题了。

UNIX 用户中大多数人都是持后者的态度来对待安全性问题，不断的学习与研究是网络安全的一个非常重要的方面。尽管网络入侵者能够利用互联网上的安全漏洞的攻击方法，但是网管也是能够获取这些技术的，并能够及时的修补漏洞。

互联网上最享有盛名的网络安全团体是“安全策略中心”，它通过互联网提供一些网络安全方面的建议，各种操作系统所存在的网络安全性的问题和漏洞，以及相应的解决方案。它的互联网网址为：http://www.security-policy.org/。关心网络安全方面的用户可以来这里查阅他们所需要的与网络安全有关的内容，这个网站还是很丰富的。

事实上，很多系统漏洞被入侵者利用都是因为管理员没有及时的弥补上安全漏洞，也就是说是管理员疏于工作而导致的，而那些合格的管理员就能够利用各种方法找出自己系统所存在的安全漏洞，并在互联网上找到相关的解决办法，国外有很多大公司都聘用专业的网络安全顾问，这些顾问的任务之一就是及时发现系统的漏洞，并通知管理员来进行修补。

1.2.2 网络安全重要吗

随着计算机网络的广泛使用和网络之间信息传输量的急剧增长，一些机构和部门在得益于网络加快业务运作的同时，其上网的数据也遭到了不同程度的破坏，或被删除或被复制，数据的安全性和自身的利益受到了严重的威胁。

根据美国 FBI 的调查，美国每年因为网络安全造成的经济损失超过 1.70 亿美元。75%的公司报告财政损失是由于计算机系统的安全问题造成的。超过 50%的安全威胁来自内部；只有 17%的公司愿意报告黑客入侵，其他的由于担心负面影响而未声张。59%的损失可以定量估算。平均每个组织损失$402，000。

1998 年，一连串的网络非法入侵改变了中国网络安全犯罪“一片空白”的历史。

据公安部的资料，1998 年中国共破获电脑黑客案件近百起，利用计算机网络进行的各类违法行为在中国以每年 30%的速度递增。黑客的攻击方法已超过计算机病毒的种类，总数达近千种。公安部官员估计，目前已发现的黑客攻击案约占总数的 15%，多数事件由于没有造成严重危害或商家不愿透露而未被曝光。有媒介报道，中国 95%的与 Internet 相连的网络管理中心都遭到过境内外黑客的攻击或侵入，其中银行、金融和证券机构是黑客攻击的重点。在中国，针对银行、证券等金融领域的黑客犯罪案件总涉案金额已高达数亿元，针对其他行业的黑客犯罪案件也时有发生。

无论是有意的攻击，还是无意的误操作，都将会给系统带来不可估量的损失。攻击者可以窃听网络上的信息，窃取用户的口令、数据库的信息；还可以篡改数据库内容，伪造用户身份，否认自己的签名。更有甚者，攻击者可以删除数据库内容，摧毁网络节点，释放计算机病毒等等。

黑客的威胁见诸报道的已经屡见不鲜，像贵州省城热线、成都艺术节主页等都报道有黑客入侵，他们在主页上发布反动口号，或将主页修改成黄色画面。

内部工作人员的不小心甚至充当间谍。内部工作人员能较多地接触内部信息，工作中的任何不小心都可能给信息安全带来危险。这些都使信息安全问题越来越复杂。

竞争对手的非法入侵。现在社会竞争越来越激烈，竞争对手通过网络非法访问对方内部信息的事件屡见不鲜。

总之，网络必须有足够强的安全措施。无论是在局域网还是在广域网中，网络的安全措施应是能全方位地针对各种不同的威胁和脆弱性，这样才能确保网络信息的保密性、完整性和可用性。

1.2.3 入侵者的攻击手段

对计算机网络进行攻击的手段可以分为几个主要种类，它们的危害程度和检测防御

办法也各不相同：

1. 黑客发动攻击的主要过程

(1) 用扫描器发现对方目标系统的有关信息。兵书云：“知己知彼，百战不殆”，黑客深谙此道。不了解敌方军情贸然出兵必然会一败涂地，不熟悉目标对象的基本特征就发动攻击就像是“狗咬刺猬，没法儿下嘴”。网上各种各样的扫描器程序很多，利用它，黑客能发现攻击对象运行的是哪种操作系统的哪个版本，系统有哪些账户，WWW、FTP、Telnet、SMTP 等服务器程序是何种版本。

(2) 根据系统的具体弱点，寻找突破口。网上有许多黑客站点专门收集并分析各种操作系统及服务器程序的安全漏洞，如 Solaris、Windows 9X、Windows NT、Linux 等操作系统还有 Apache、NCSA、IIS 等多种服务器的弱点分析，利用这些弱点和漏洞，黑客就能够进入目标系统，获得较低级别的访问权限。

(3) 设法盗窃账户文件，然后破解获得超级用户账户和口令并寻匿合适时机以此身份进入。或者利用某些工具和系统漏洞转变成超级用户角色。

(4) 盗窃甚至篡改某些敏感信息，在系统中置入特洛伊木马或其他远程操纵程序。该要的东西拿到了，该放的“炸弹”放入了，黑客的目的达到了，以后，他就可以实现“远程办公”了。

2. 黑客的攻击手段

(1) 信息收集

经常使用的工具包括：NSS，Strobe，Netscan，SATAN（Security Aadministrator's Tool for Auditing Network），Jakal，IdentTCPscan，FTPScan 等以及各种 sniffer。广义上说，特洛依木马程序也是收集信息攻击的重要手段。收集信息攻击有时是其他攻击手段的前奏。对于简单的端口扫描，敏锐的安全管理员往往可以从异常的日志记录中发现攻击者的企图。但是对于隐秘的 sniffer 和 trojan 程序来说，检测就是件更高级和困难的任务了。

① 嗅探器。它们可以截获口令等非常秘密的或专用的信息，甚至还可以用来攻击相邻的网络，因此，网络中 sniffer 的存在，会带来很大的威胁。这里不包括安全管理员安装用来监视入侵者的 sniffer，它们本来是设计用来诊断网络的连接情况的。它可以是带有很强 debug 功能的普通的网络分析器，也可以是软件和硬件的联合形式。现在已有工作于各种平台上的 sniffer，例如：

- Gobbler(MS-DOS)
- ETHLOAD(MS-DOS)
- Netman(UNIX)

- Esniff.c(SunOS)
- Sunsniff(SunOS)
- Linux-sniffer.c(Linux)
- NitWit.c(SunOS)
- etc.

检测 sniffer 的存在是个非常困难的任务，因为 sniffer 本身完全只是被动地接收数据，而不发送什么。并且上面所列的 sniffer 程序都可以在 Internet 上下载到，其中有一些是以源码形式发布的(带有.c 扩展名的)。

一般来讲，真正需要保密的只是一些关键数据，例如用户名和口令等。使用 IP 包一级的加密技术，可以使 sniffer 即使得到数据包，也很难得到真正的数据本身。这样的工具包括 secure shell（ssh），以及 F-SSH，尤其是后者针对一般利用 TCP/IP 进行通信的公共传输提供了非常强有力的，多级别的加密算法。ssh 有免费版本和商业版本，可以工作在 UNIX 上，也可以工作在 Windows 3.1，Windows 9x 和 Windows NT。

另外，采用网络分段技术减少信任关系等手段可以将 sniffer 的危害控制在较小范围以内也为发现 sniffer 的主人提供了方便。

② 特洛伊木马。这是一种技术性攻击方式 RFC1244 中给出了 trojan 程序的经典定义：特洛依木马程序是这样一种程序，它提供了一些有用的、或仅仅是有意思的功能。但是通常要做一些用户不希望的事，诸如在你不了解的情况下拷贝文件或窃取你的密码，或直接将重要资料转送出去，或破坏系统等等。

特洛依程序带来一种很高级别的危险，因为它们很难被发现，在许多情况下，特洛依程序是在二进制代码中发现的，它们大多数无法直接阅读，并且特洛依程序可以作用在许许多多系统上，它的散播和病毒的散播非常相似。从 Internet 上下载的软件，尤其是免费软件和共享软件，从匿名服务器或者 usernet 新闻组中获得的程序等等都是十分可疑的。

所以作为关键网络中的用户有义务明白自己的责任，自觉做到不轻易安装使用来路不清楚的软件。

检测一个特洛依程序，需要一些比较深入的有关操作系统的知识。可以通过检查文件的更改时间，文件长度，校验等来检查文件是否进行过非预期的操作。另外，文件加密也是有效的检查特洛依程序的方法。可以使用的工具包括：

① trip wire。这是一个广泛应用的系统完整性工具。系统通过读取配置文件得到环境变量，在这个文件中包含着所有的文件标志(filemarks)使用者可以详尽地规定应该对哪些文件作出哪些改变作出报告等，它们的数字签名保存在数据库中，数字签名可以使

用的 hash 函数包括：

MD5 MD4 CRC32 MD2 Snc frn SHA 等。

TAMU 程序包可以检查许多项目，包括由 CERT 通知中定义的项目，以及最近的入侵事件中发现的项目，所有被改动的系统二进制流，以及要求保密的那些关键路径。

② Hobgoblin。

③ ATP(The Anti-Tampering Program)。

后面两种工具的使用没有前面两种那么普遍，但是它们都各有特点。

(2) 密码破解攻击

这种攻击者的目的很明确，窃取他人系统的账户和密码，然后待机侵入。根据目标系统种类的不同，窃取账户和密码也有很多方法：

① 中途截击。很多协议根本就没有采用任何加密或身份认证技术，比如 Telnet、FTP、HTTP、SMTP 等协议中，用户账户和密码信息都是以明文格式传输的，所以，如果攻击者利用数据包截取工具就很容易收集到你的 Telnet、FTP、Email 账户和密码以及你的会话内容。还有一种中途截击攻击方法更厉害，即使你的账户和密码是加密传输的，也“难逃此劫”，它在你同服务器端完成“三次握手”建立连接之后，在通信过程中扮演“第三者”的角色，假冒服务器身份欺骗你，再假冒你向服务器发出恶意请求，其造成的后果不堪设想。

② 利用目标系统的固有弱点获得超级用户的账户和密码。比如某些 Web 服务器存在很大的安全漏洞，客户端可以通过发送特定格式组合的 HTTP 请求，就能得到对方的超级用户的账户和密码；黑客站点上经常公布这样一些弱点，所以，发现系统存在安全漏洞以后，请尽快联系产品厂商获取补丁程序。

③ 攻击者先以较低权限用户身份访问，再设法转变为超级用户。一个大的系统往往不止一个用户，并且还有许多公用的账户和口令，如 pubic、everyone 等账户。对于一些 UNIX 系统而言，有的黑客先以此身份进入系统，然后取走 /etc/passwd 文件，回去之后将此文件解密就能得到该系统的所有账户和口令（包括超级用户账户和口令）。还有一些黑客工具，能使一个低权限用户获得超级用户的权限。也有些攻击不需要获取账户和密码，直接利用对方系统的某些设置漏洞就能发动攻击甚至远程操纵目标系统。例如有很多 WWW 服务器缺省安装一些脚本程序，实际上这些脚本并无多大用处，但却可能被黑客利用。有的 UNIX 系统启动时就将网络文件系统（NFS，Network File System）开放，这也很容易被别人远程操纵。

(3) 服务拒绝攻击

这是一类个人或多个人利用 Internet 协议组的某些方面妨碍甚至关闭其他用户对系