黑客与网络安全

主编 / 刘晨　张滨

东方卓越
航空工业出版社

黑客与网络安全

主编 刘 晨 张 滨

编委 易 鸿 刘庆红

刘 强 万 林

航空工业出版社

1999

内 容 提 要

本书对黑客与网络安全进行了比较全面的介绍。前三章详细地介绍了黑客的行为、黑客的手法和工具。第四到第七章讲述了密码技术、计算机操作系统的安全、电子邮件系统的安全和 WWW 的安全。鉴于计算机病毒凭借网络广泛传播并对计算机和网络安全产生了日益严重的威胁，本书第 8 章专门介绍了计算机病毒及其防治方法。本书的最后一章还简要地介绍了防火墙及其它一些 Internet 安全措施。

本书适合对黑客与计算机网络安全感兴趣的读者。

图书在版编目（CIP）数据

黑客与网络安全 / 刘晨，张滨编．－北京：航空工业出版社，1999.9

ISBN 7－80134－523－1

Ⅰ.黑… Ⅱ.①刘… ②张… Ⅲ.计算机网络－安全技术 Ⅳ.TP393

中国版本图书馆 CIP 数据核字（1999）第 39585 号

航空工业出版社出版发行

(北京市安定门外小关东里 14 号 100029)

北京云浩印刷厂印刷　　全国各地新华书店经售

1999 年 9 月第 1 版　　1999 年 9 月第 1 次印刷

开本：787×1092　1/16　　印张：19.875　　字数：458 千字

印数：1－12000　　定价：26.80 元

前　言

计算机安全是一个越来越引起世界各国关注的重要问题，也是一项十分复杂的课题。随着计算机在人类生活各领域中的广泛应用，计算机病毒也在不断产生和传播，计算机网络不断遭受黑客的攻击，重要情报资料被窃密，甚至造成网络系统瘫痪，给各个国家以及众多公司造成巨大的经济损失，甚至危害国家和地区的安全。因此计算机系统的安全问题是一个关系到人类生活与生存的大事情，必须给予充分的重视并设法加以解决。

TCP/IP 协议群在网际互联中的使用迅速崛起，导致了通常称为 Internet 的由主机和网络组成的全球网际互联系统。过去的十年，是 Internet 胜利大进军的十年。按它现在的发展速度预测，到本世纪末，将有超过一百万的计算机网络和超过十亿的用户加入 Internet。正因为如此，Internet 被看成是美国政府提出的国家信息基础设施（NII）的第一个具体体现。

但是，Internet 的开放性成了一把双刃剑。从 Internet 诞生之日起，特别是自 90 年代它向公众开放以来，它已经成为众矢之的。1988 年 11 月，小 Robert T. Morris 放出的 Internet 蠕虫攻击了数千台主机。从那时起，不断传出侵犯安全的事件报道。企图闯入系统的黑客有之，成功闯入系统的黑客有之，抓住 Internet 上主机的种种弱点和漏洞加以利用的黑客也有之。最近，成千成万的口令在 Internet 上被盗取，序列数猜测的攻击手段已经被用来冒充 IP。特别要指出的是：很早就有人知道这些易受攻击的弱点了。

如今 Internet 上的每一个人实际上都是脆弱的。Internet 的安全问题成了关注的焦点。计算机和通信界一片恐慌。对安全问题的考虑，对认为 Internet 已经完全胜任商务活动的过高期望泼了一盆冷水，可能还延缓或阻碍了作为国家信息基础设施或全球信息基础设施的 Internet 成为大众媒体。

尽管众说纷纭，有一点是大家都同意的，那就是 Internet 需要更多更好的安全机制。本书旨在对网络的安全作一些探讨。在讲述网络安全的同时，基于“知己知彼”的考虑，也对黑客的行为和攻击手法作了必要的讨论，这正是前面三章所作的努力。但有一点要声明：讲述黑客的行为和攻击手段并不是要教读者如何去作黑客，而是正好相反，希望读者能够更好地保护自己在网上的安全。在后面的六章中讲述了加强网络安全的几个方面，讨论了加密技术、操作系统的安全、电子邮件系统的安全、WWW 的安全。由于近几年计算机病毒借助于 Internet 的传播给众多的计算机用户带来了很大损失，在本书第 8 章对计算机病毒作了一些讲述。在本书的最后，概括讲述了防火墙及其他一些 Internet 安全措施。

在本书的写作过程中，参考了很多的网上的资料，在此谨向那些知名和不知名的作者表示感谢。希望本书能对您有所帮助。

编　者

1999 年 7 月

目 录

第 1 章　认识黑客与网络安全

在本章中用户将对网络安全现状和黑客的社会有一个初步的认识。首先用户将对现在网络上存在的安全问题作一了解，然后用户再对黑客的文化史、黑客守则以及黑客的活动规律等进行了解。

1.1　认识网络安全

现在没有人认为网络是安全的。用户可以不时地从各种媒体上读到关于黑客入侵、作案的新闻，从普通的篡改系统到对五角大楼的入侵，似乎用户快要对这些现象见怪不怪了。

1.1.1　网上漏洞何其多

在开始讲述网络安全之前，先让用户看一下最近的几则新闻。

1. 聊天室也遭袭击

1997 年 12 月 18 日

流行的聊天室共享软件 mIRC 本周被发现有一个漏洞。IBM 公司华盛顿研究实验室的反病毒专家们指出，在 mIRC 软件中存在安全漏洞，它使得在线交谈时恶意的脚本文件可以被传送给用户。这个安全漏洞允许用户文件与 mIRC 软件一起被传送。如果文件是脚本形式，那么它们将被执行，从而接管被攻击者的计算机。受控计算机可被攻击者用来响应其他通道的对话或退出聊天室等。更糟糕的是，它允许其他人来访问自身的硬盘。该脚本程序还能发送复制本给其他用户。到目前为止，已发现四种不同的脚本程序，其中罪大恶极的名为 SCRIPT.INI。上周末，mIRC 的出品人推出了更新版 v5.0。

摘自：www.zdnet.com

2. IE 4.0 中又发现新漏洞

1998 年 1 月 16 日文

自去年秋季微软发布了 IE 4.0 “res” 缺陷修补程序之后，日前在该浏览器中又发现一个类似缺陷，该缺陷对运行于 Win95 和 NT 上的 IE 4.0 及 IE 4.01 有影响。当浏览器访问前缀为 “mk” 的 URL 地址时，在 URL 长度超过 256 个字符时，超过的字符将被扔入系统内存中。其结果是使浏览器崩溃，如果多余字符为可执行代码，这些代码将在机器内自动执行。微软称该漏洞还没有对用户造成任何影响，并计划在本周发布修补程序。微软将继续研究，以使新的修补程序能防止其他类似缺陷出现。

摘自：www.news.com

3. IE 4 for Mac 有加密错误

1998 年 1 月 20 日

微软宣布，本月初发布的 IE 4.0 for Macintosh 存在加密缺陷，该缺陷使得用户不能访

问使用“安全套接字层”（SSL）的站点。

微软称，这个缺陷只出现在使用128位加密机制的IE 4 For Mac当用户使用这种有缺陷的浏览器访问使用SSL2或3版本协议的站点时，将被拒绝访问，原因是三层DES加密的实现出了问题。但是由于它根本拒绝用户浏览站点，因此不会泄漏任何个人信息或对数据有任何损害。该漏洞的修补程序将于周一在微软网站发布。

摘自：www.news.com以继夜

4. BUG作怪，Navigator竟成IE

1998年2月19日

CyberMedia公司日前正式向网景公司表示道歉。原因是CyberMedia公司的“急救”（FirstAid）软件中有“虫”（Bug）作怪，偷偷将用户缺省设置的Navigator浏览器换成了IE。“急救”虫惹恼了许多忠于网景的用户，因此CyberMedia不得不向网景公司及广大用户致歉，并随即在网站上公布其修补程序。“急救”软件是一种用来检测并解决常见PC问题的软件。

摘自：www.news.com

5. Ascend产品有漏洞

1998年3月19日

据Secure Networks报道，新漏洞会导致Ascend Communications公司的网络产品遭到恶意攻击，造成机器瘫痪、口令被盗等后果。黑客可以使远程接入和路由设备失灵。由于Ascend采用的“简单网络管理协议”（SNMP），网络口令和远程拨打号码也可能暴露给黑客。

然而Ascend的发言人却对Secure Networks的动机提出质疑，因为Secure Networks的主要业务是测试系统漏洞，同时销售安全监督软件来帮助修补漏洞。这位发言人说，“一个只有少数人知道的漏洞，经Secure Network宣传就有更多的人了解。这样，黑客就可以利用漏洞捣乱。对于Secure Network来说安全漏洞最好解决不了，这样才最有利于Secure Network，因为，它可以卖出更多的软件。”

Ascend发言人称：“用户尊重使人们建立安全意识的行为，并尽快作出反应。”Ascend已经在公司站点上公布了可以减轻问题后果的方法。

摘自：www.news.com

6. NT出了大漏洞

1998年6月4日

Counterpane系统公司在对Windows NT进行安全测试时发现，NT中存在一个很大的安全漏洞，外人可通过它截取口令、偷窥网络。同一天微软也确认了这一问题的存在。该缺陷影响基于NT和点到点通道协议（PPP）的虚拟专用网络（VPN）。VPN可将集团公司位于不同地点的网络联接起来。由于其成本低，因此该方案普及速度很快。该安全漏洞出在PPP身上。PPP是微软自家开发的一种通过公用Internet网安全发送与接收数据的协议。微软表示，将尽快提供修补方案。

摘自：www.zdnet.com

7. 微软发布“虫”情警报

1998 年 7 月 20 日

微软日前发布“虫”情警报：由于在微软 IIS4.0、RDS1.5 和 Visual Studio6.0 中存在的一个安全漏洞，一些恶意用户可能通过它闯入公司的 SQL 服务器及 Access 数据库，甚至摧毁整个 NT 服务器系统。

微软还表示，如果公司在安装了与 VS6.0 一同发售的 Data Shape Provider 和 JETOLEDB Provider 组件，则系统被侵入的可能性更大。漏洞出在 RDS 中的 Deta Factory，因此微软建议那些还没有使用 Deta Factory 功能的公司屏蔽其功能。微软表示，不会为此推出修补程序。

摘自：www.news.com

8. 微软网景 Email 软件有大漏洞

1998 年 7 月 29 日

芬兰的研究人员日前发现，在微软和网景的电子邮件软件中存在一个严重的安全漏洞。入侵者利用该漏洞，通过向受害者发送带有超长文件名的附加文件电子邮件，从而摧毁对方的电子邮件程序(包括微软 Outlook 98 和 Outlook Express 邮件程序及网景 Messenger 邮件程序）。然后，受害者的计算机就可能被迫运行邮件附加文件中的恶意代码程序。该漏洞几乎影响所有的 32 位 Windows 系统。微软日前已为 Outlook 98 和 Outlook Express 的邮件客户端提供了修补程序。网景表示也将于最近两周为 Communicator 4.05 和 4.5beta 版发布修补程序。微软和网景都要求受影响用户尽快安装修补程序。该漏洞的可怕之处在于用户根本不用打开附加文件就会被袭击。只要用户从邮件服务器下载了该邮件，就会出现邮件程序崩溃、恶意代码运行的恶果。

摘自：www.pcworld.com

9. NT 中发现严重漏洞

1998 年 7 月 29 日

据悉，在 NT 操作系统中存在的一个安全漏洞，可以使任何一个网络用户都当上系统管理员。据安全咨询人员 Mark Edwards 说，只要掌握了利用该漏洞的知识，任何一个在 NT 网络客户端工作的人都可以篡改他人的口令、增加新地址、改变机密信息访问权限，就象是该网络的系统管理员一样。微软是在上周获悉这一漏洞的，并表示即将在其 Security Advisor 网站上推出修补程序和安全建议。该漏洞影响服务器版和工作站版的 NT 4.0 及 3.51。

摘自：www.news.com

1.1.2　网络的安全问题

虽然网络的安全问题自网络的诞生之日起，便和网络自身一起形影不离，但事实上直到最近几年由于 Internet 的蓬勃发展，这一问题才有今天这样备受重视的地位。电子商务也是 1998 年 IT 行业的热门话题之一。全球的许多国家不管是风风火火，或是姗姗来迟的推进电子商务，但真要使网上购物、网上银行和网上交易深得人心，就不得不消除人们对网络安全的疑虑。然而，1998 年的 Bug 却是剪不断，理还乱，上面所列只是聊作代表而

已，偏偏 Hacker（黑客）是见缝就插针的，有了漏洞就会有黑客去加以利用。网络安全方面出了新闻，如果是黑色的，一般总和黑客联系在一起。进入 1999 年，先是 Intel 因在最新推出的 P III 中可能含带有跟踪设置 ID 芯片，闹得沸沸扬扬。接着，Microsoft 也坦言 Windows 98 中含有在电子邮件中产生一个用来查找用户身份的名为“全球特殊身份证”的特殊序号。这个“全球特殊身份证”可以让 Microsoft 在神不知鬼不觉的情况下获得用户电脑上的认证资料。这些资料理论上可以跟踪到单个文件的作者。在 Word 和 Excel 软件所建立的电子邮件的内码中，隐藏由一台电脑所特有的三十二位数字序号，Windows 98 用户在登记注册的时候会被强行传送一个特殊的硬件认证号码。这个号码会被直接传送到 Micrsoft 公司。Microsoft 公司通过此项技术来确认用户是否非法使用 Windows 操作系统，方法是把这个硬件序号与二十位的 Microsoft 产品序号相比较，如果 Microsoft 看到同一产品序列号出现不同的硬件序号，那么 Microsoft 就可以以此作为盗版软件的证据来控告。在个人隐私越来越高于一切的今天，不单是公司，个人也越来越对网络上的安全问题表现出极大的不安。

1996 年《信息周刊》Emst Young 调查结果表明，对安全的威胁正在持续上升，越来越多的企业身受其害。调查报告指出，近 78%的信息主管、信息安全官员及其他高级技术管理人员报告其企业已因泄密而遭受损失，超过 25%的企业报告其损失要高于 25 万美元。这些事件中，近 32%的事件由内部黑客所为。

1. 网络在安全方面存在的漏洞

- 操作系统在安全方面的漏洞

（1）操作系统的体系结构造成操作系统本身是不安全的，这是计算机系统不安全的根本原因。

操作系统的程序是可以动态连接的，包括 I/O 的驱动程序与服务系统，都可以用打补丁的方式进行动态连接。许多 UNIX 操作系统的版本升级开发都是采用打补丁的方式进行的。这种方法厂商可以使用，黑客也可以使用，而且这种动态连接也是计算机病毒产生的好环境。一个靠打补丁开发的操作系统是不可能从根本上解决安全问题的。

但操作系统支持程序动态连接与数据动态交换又是现代系统集成和系统扩充必备的功能，因此这是相互矛盾的。

（2）操作系统支持在网络上传输文件，包括可以执行的文件映像，即在网络上加载程序。

（3）操作系统不安全的另一个因素在于它可以创建进程，甚至支持在网络的节点上进行远程进程的创建与激活，更重要的是被创建的进程可以继承创建进程的权力。这一点与上一点（可在网络上加载程序）结合起来就构成了可以在远端服务器上安装“间谍”软件的条件。若再加上把这种间谍软件以打补丁的方式“打”在一个合法的用户上，尤其“打”在一个特权用户上，间谍软件就可以做到系统进程与作业的监视程序都检测不到它的存在。

（4）操作系统通常都提供 daemon 软件，这种软件实质上是一些系统进程。它们总在等待一些条件的出现，之后程序便继续运行下去。这样的软件都是黑客可以利用的。这里应该说明的是：关键不在于有没有 daemon，而在于这种 daemon 在 UNIX 以及 WINDOWS NT 操作系统上具有与操作系统核心层软件同等的权利。

（5）操作系统提供远程过程调用（RPC）服务。

（6）操作系统提供 Debug 与 Wizard。许多研制软件系统的人员，他们的基本技术就是 Patching 加上系统 Debug。具备了这两样技术，他们就有条件从事“黑客”可以从事的所有事情。

（7）操作系统安排的无口令入口是为系统开发人员提供的便捷入口，但它也是黑客的通道。另外，操作系统还有隐蔽通道，商户可以进去做任何事情；而且简单的密码设置也让黑客有可乘之机。

- 计算机网络安全的漏洞

Internet/Intranet 使用的 TCP/IP 协议以及 FTP、E-mail、RPC、NFS 等都包含许多不安全因素，存在许多漏洞。很多人都知道，1988 年一个叫 Rebert Morry 的人，在 VAX 机上用 C 语言编写了一个通过 GUESS 软件，引用根据搜索的用户名字来猜测机器密码口令的程序，结果自 1988 年 11 月开始在网络上传播以来，几乎每年都给 Internet 上的系统造成一亿美元的损失。

黑客通常采用 Source Porting、Source Routing、SOCKIT、TCP 序列预测或者使用远程访问（RPC）进行直接扫描等方法对防火墙进行攻击。

- 数据库管理系统安全漏洞

数据库管理系统的安全必须与操作系统的安全进行配套，例如 DBMS 的安全级别是 B2 级，那末操作系统的安全级别也应当是 B2 级。由于数据库的安全管理同样是建立在分级管理的概念之上的，因此 DBMS 的安全也是脆弱的。

- 应用系统安全的漏洞

路由器——错误的路由配置、隐蔽的 Modem、缺省的路由配置这些都可导致黑客的攻击。防火墙——它的出发点是防止外部黑客的攻击，从根本上说防外不防内，在美国的调查表明，32%的泄密是由内部作案，所有的防火墙都不同程度地被黑客攻击过。而且防火墙只能防一个口，并且不能对 IP 包进行分析。Web 服务器——又是非常容易利用的黑客工具。另外还有未知的安全间歇。

- 缺少安全管理

世界上现有的信息系统绝大多数都缺少管理人员，目前绝大多数企业负责网络安全管理的只有几个人，而且缺少信息系统安全管理的规范，缺少定期的安全测试与检查，更缺少安全监控。另外，安全要求与实际操作相脱离，因为安全策略经常会与用户方便性相矛盾，致使安全措施和实际执行之间存在很大的距离。我国许多的信息系统已经使用了很多年，但计算机的系统管理员与用户的注册还有很大一部分仍处于缺省状态，信息系统受到威胁。信息系统安全的隐患包括内部的安全隐患、黑客（外部的和内部的，内部黑客了解熟悉网络结构，更易下手）的攻击、计算机病毒以及拒绝服务攻击（Denial of Service Attack）。

计算机系统本身就存在着种种安全性问题，互联后的计算机系统的安全问题就更为复杂，因为互联的设计使得攻击者可以在它们的连接处进行破坏。计算机网络的安全性主要包括：网络服务的可用性（Availability）、网络信息的保密性（Confidentiality）和网络信息的完整性（Integrity）。

2. 计算机网络面临的安全性威胁

计算机网络作为一种技术是面向所有用户的，所有资源通过网络共享。对 Internet 来

说，则具有开放性和标准性的特点，过去 Internet 是用于科研和学术，现在商业用途是其最重要的组成部分。

用户把网络攻击和网络安全作一分类。从总体上来说用户可以分为两类。第一类为系统型攻击，它所对应的网络安全是系统安全，从比例上来讲，占到整个攻击的百分之三十，造成损失的比例也占到百分之三十。系统攻击的特点是：

- 它是在网络层进行的。
- 破坏系统的可用性，使系统不能正常工作。
- 留下明显的攻击痕迹，用户会发现系统不能正常工作。

第二类叫做数据型攻击，它所对应的安全称之为数据安全。这种攻击主要来源于系统内部，占到攻击总数的百分之七十，所造成的损失也占到百分之七十。数据型攻击的特点是：

- 在网络的应用层进行。
- 面向信息，主要目的是获得或修改数据。
- 数据型攻击不会留下明显的痕迹，因为攻击者需要多次的获取或修改。

上面是从总体上分类。从具体上来说，计算机互联网络面临的安全性威胁主要有以下几个方面：

（1）非法访问和破坏

操作系统总不免存在这样那样的漏洞，一些人就利用系统的漏洞，进行网络攻击，其主要目标就是对系统数据的非法访问和破坏。“黑客”攻击已有十几年的历史，黑客活动几乎覆盖了所有的操作系统，包括 UNIX、Linux、Windows NT、VM、VM2 以及 MV3。

（2）计算机病毒

计算机病毒程序很容易编制，有着巨大的破坏性，其危害已被人们所认识。单机病毒就已经让人们谈毒色变了，通过网络传播的病毒无论是在传播速度、破坏性及传播范围等方面都是单机病毒所不能比拟的。

（3）特洛伊木马（Trojan Horse）

特洛伊木马的名称来源于古希腊的历史故事。特洛伊程序一般是由编程人员所编制，它提供了用户所不希望的功能，这些额外的功能往往是有害的。它把预谋的功能隐藏在公开的功能中。

（4）蠕虫（Worms）

蠕虫是一个或一组程序，它可以从一台机器向另一台机器传播。它同病毒不一样，它不需要修改宿主程序就能传播。

（5）活板门（Trap Doors）

为攻击者提供“后门”的一段非法的操作系统程序。这一般是指一些内部程序人员为了特殊的目的，在所编制的程序中潜伏代码或保留漏洞。

（6）隐蔽通道

是一种允许违背合法安全策略方式进行操作系统进程间通信（IPC）的通道，又分隐蔽存储通道和隐蔽时间通道。隐蔽通道的重要参数是带宽。

（7）拒绝服务攻击（Denial of Service Attack）

一种破坏性攻击，最早的拒绝服务攻击是“电子邮件炸弹”，它能使用户在很短的时

间内收到大量电子邮件，使用户系统不能处理正常业务，严重时会使系统崩溃、网络瘫痪。

（8）泄露机密信息

包括两种情况：系统内部人员的泄露机密和外部人员通过非法手段截获机密信息。

在上述八种行为中，每一种都有黑客的参与。

在所有的操作系统中，由于 UNIX 系统的核心代码是公开的，这使其成为最易受攻击的目标。攻击者可能先设法登录到一合 UNIX 的主机上，通过操作系统的漏洞来取得特权，然后再以此为据点访问其余主机，这被称为“跳跃”（Island hooping）。攻击者在到达目的主机之前往往会先经过几次这种跳跃。这样，即使被攻击网络发现了攻击者从何处发起攻击，管理人员也很难顺次找到他们的最初据点，何况他们能在窃取某台主机的系统特权后，在退出时删掉系统日志。用户只要能登录到 UNIX 系统上，就能相对容易地成为超级用户。所以，如何检测系统自身的漏洞，保障网络的安全，已成为一个日益紧迫的问题。

3. 网络犯罪

互联网上的攻击与破坏事件不胜枚举。尽管我国的网络应用还远未普及，但涉及黑客的案件也时有发生。最典型的如 1995 年 12 月，在北京，有人对投币公用电话进行一番特殊操作后，花一角钱便可无限时地拨打长途电话。另外在金融证券行业里，也有黑客的足迹，如：有人登录到深圳市某证券营业部网络服务器，操纵自己的帐户吞吐股票，进行非法获利；在上海某银行，一名工作人员编了一套程序，用于截获银行储户利息等等；1998 年 12 月 24 日，全国首例利用电脑窃取银行巨款案在江苏省扬州市一审判决犯罪分子死刑。

相比而言，国外的“黑客”案件就多得多了。据美国军方的一份报告透露，去年，试图闯入五角大楼计算机网络的尝试达 25 万次之多，其中 60%的尝试达到了目的，而这些得逞的入侵中，每 150 起中只有 1 起被侦测到并被上报。可见，灾难性破坏的潜在危险是巨大的。五角大楼计算机网络的数据涉及到非常敏感的信息，如部队调动、武器的采购和维护等。那些并没有犯罪企图的年轻“黑客”当然不会带来实质性的危害，但只要有一起蓄意破坏国家安全的“入侵”，危害就是致命的。

1998 年，由于“黑客”的“造访”，在全球范围内，主要的银行和大公司损失了大约 8 亿美元，美国约占 4 亿。大多数案例中，受害企业因害怕市场形象受损和长时间卷入调查而并未将受损情况向法律部门报告。

每年，美国政府的计算机系统遭非法侵入（虽然并非全是恶意）的次数至少有 30 万次之多。17%的美国公司因计算机安全性有漏洞而导致损失，每年黑客犯罪引起的损失估计可达 15 亿美元。

今天，恐怖分子能够凭借电脑网络及卫星通信网络引爆放在另一个国家的爆炸物。由于正在出现的信息高速公路是没有边界的，恐怖分子可以从地球上任何地方向企业或政府机构的电脑信息系统投放电脑病毒以及其他能够摧毁信息系统的东西。说得严重一点，个别恐怖分子通过网络引发某国的导弹，进而引起一场战争，造成人类社会的一场灾难，也不是没有可能的。

以下是几个利用计算机网络犯罪的典型例子。

- 1989 年 3 月 2 日凌晨，3 名德国黑客因涉嫌向前苏联出售机密情报被捕，他们在两年多的时间内，闯入了许多北约和美国的计算机中，而这些计算机中储存着高度机密的信息。

- 法国国防部 1996 年证实，法国海军行动力量参谋部的计算机所存储的军事机密 1995 年 7 月底被人盗窃。这些军事机密包括几百艘盟军军舰的声音识别码，即海军情报部门分类保存的每艘军舰的特殊声音，它们可以保证情报部门准确地判定每艘军舰的航行方位。这些军事机密被窃，令法国政府和军事部门大为恐慌。
- 1996 年 1 月，一名俄罗斯侨民认罪。因为他参与了一项闯入花旗银行伦敦分行的计算机并将 280 多万美元转入另外 3 个国家的银行帐户的计划。
- 1996 年 9 月，美国中央情报局的主页被一名远在瑞典的少年黑客改为中央笨蛋局（Central Stupidity Agency）。此前，一名黑客闯入美国司法部网址，将主页上的“司法部”（Department of Justice）改为“非法部”（Department of Injustice），页面背景也被换成了德国纳粹党党徽的标志。

下面两条是 1998 年消息。

- 研究生入侵网络被捕

日前，上海市公安局刑侦总队和计算机管理处成功侦破一起本市首例、全国罕见的“黑客”攻击上海某信息网络案件。犯罪嫌疑人杨某被以破坏计算机信息系统的罪名依法逮捕。据悉，这是修订后的刑法实施以来，第一起以该罪名批捕的案件。

今年 22 岁的杨某系全国某著名大学数学研究所计算数学专业研究生，曾获国家软件高级程序员资格证书。经初步调查，杨某先后侵入某科技网和上海某信息网络，不仅破译过网络大部分工作人员和 500 多个合法用户，包括两台服务器上超级用户的帐号和密码，同时把攻击网络的技法在一定范围内传播和使用。

鉴于上海的电脑黑客犯罪趋向升级，对申城政治、经济等安全构成威胁，市公安局已加强研究、制订打击对策，并提请市人大及人大常委会尽快制订严格的惩罚电脑犯罪的法规，严厉打击有可能日益增多的电脑犯罪活动。（沪讯）

《计算机世界》1998.9.21

- 黑客做手脚，AOL 成禁区

近日，由于 Internet 域名系统出现错误，Internet 用户向美国在线（AOL）用户发送电子邮件或接入 AOL 站点时遇到了重重困难。

此前也曾有报道，部分 Internet 用户在向 AOL 的 1300 万用户发送电子邮件或准备接入该 AOL 的门户时，发现进入的是一家域名为 Autonet.net 的公司的服务器，而不是直接连通 AOL。

AOL 女发言人 Ann Brackbill 证实了这一消息。

问题发生的原因在于，用户向 NSI 公司运营的 InterNIC 发送电子邮件时会要求 NSI 修改 AOL 指定的域名服务器。AOL 为修改其 InterNIC 记录设定的是最低安全检查，因此黑客做手脚比较容易。

记录被修改了几个小时，现在已经纠正。由于不同的 ISP 更新其域名服务器时间不同，因此这个问题影响范围不得而知。但是系统管理员们已经开始注意到有些电子邮件被退回，接入 AOL 站点比较困难。

当 Internet 冲浪者希望接入一个 Internet 地址时，需要在他们的 Web 浏览器或电子邮件中键入这个地址。域名经过网络送至域名服务器，最后才会到目的地。如果服务器出现错误，冲浪者不会接入正确的目的地，电子邮件也不会正确送达。