策　　划／裴红义
责任编辑／夏君才
封面设计／肖　广

别碰我的电脑!——黑客攻防与网络安全

★介绍计算机与网络安全技术，特邀资深系统专家为您悉心介绍

★最合适的内容编排，最亲切易懂的语言表达，最直观的实战案例教学方式

★熟悉黑客攻防手法，保障网络安全，马上成为计算机应用高手！

电脑技能十全劲补系列

- 步入E时代——电脑快乐入门　18.8元(全彩)
- 运指如飞——轻松掌握五笔打字　14.8元
- 系统设置——轻松搞定BIOS与Windows注册表　16.8元
- **别碰我的电脑!——黑客攻防与网络安全**　15.8元
- Photo玩家——家庭数码照片处理技术　18.8元(全彩)
- 演讲自助——PowerPoint幻灯片轻松做　18.8元(全彩)
- 动感地带——Flash MX酷炫动画轻松做　18.8元(全彩)
- 文字处理——Word轻松学　18.8元(全彩)
- 电子表格——玩转Excel　18.8元(全彩)
- 数据库高手——Access数据库轻松做　18.8元(全彩)

ISBN 7-5083-1511-1
9 787508 315119 >

ISBN 7-5083-1511-1　定价：15.80元

电脑技能十全劲补系列

别碰我的电脑！——黑客攻防与网络安全

杨青 编著

中国电力出版社

图书在版编目（CIP）数据

别碰我的电脑！——黑客攻防与网络安全／杨青编著. 北京：中国电力出版社，2003
（电脑技能十全劲补系列）
ISBN 7-5083-1511-1
Ⅰ.别… Ⅱ.杨… 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（2003）第 028783 号

总 策 划: 宗 健
刘广峰
责任编辑: 夏君才
责任校对: 崔燕菊
责任印制: 邹树群

丛 书 名: 电脑技能十全劲补系列
书　　名: 别碰我的电脑！——黑客攻防与网络安全
编　　著: 杨青
出版发行: 中国电力出版社
地址：北京市三里河路 6 号　邮政编码：100044
电话：（010）88515918　传真：（010）88423191
印　　刷: 北京鑫丰华彩印有限公司
开　　本: 787 × 1092　1/16　　**印　张:** 13.25
版　　次: 2003 年 7 月北京第 1 版
印　　次: 2003 年 7 月第 1 次印刷
印　　数: 1~8000
标准书号: ISBN 7-5083-1511-1
定　　价: 15.80 元

有一天，当你打开电脑登录 QQ 时，发现密码错了。在试遍所有可能的密码后，发现还是不能通过，这时可以确定你的 QQ 密码被盗了。谁碰了我的电脑呢？

有一天，当你正在聊天室里与 MM 聊天的时候，突然窗口中弹出一堆对话框，无论怎么关都关不掉，最后只能无奈地重启计算机了。谁碰了我的电脑呢？

有一天，当你浏览网页的时候，突然硬盘狂响不止，最后发现所有的程序都不能运行了。“恭喜”你，你的电脑中病毒了。谁碰了我的电脑呢？

有一天，当你正在写 E-mail 的时候，突然桌面弹出一个对话框，上面写着“我是幽灵，我要毁了你的电脑！”，电脑里真的有幽灵吗？如果没有，这又是谁干的呢？

这些都是黑客做的！

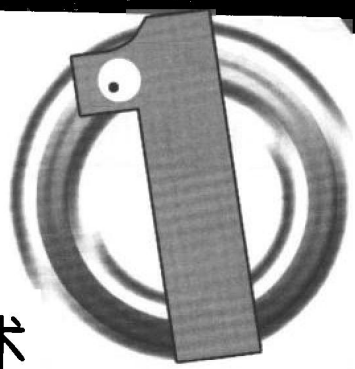
随着计算机技术的飞速发展，电脑的安全问题日益严重。也许只是升级病毒库晚了几天或者不小心点击了一个链接就可能造成巨大的损失。可能你听说过“冰河”、“欢乐时光”、“漏洞攻击”，但这些只是黑客惯用伎俩中很小的一部分，黑客攻击的手段实在是太多了。防范意识较差或者对网络安全知识不甚了解的用户，常常成为黑客攻击的目标。因此，提高自身的防范意识，掌握必要的网络安全知识就显得十分重要了，本书的写作目的也就是想让广大用户远离病毒、让黑客别碰我的电脑！本书对黑客常用的几种攻击手段进行了详尽的分析，分析得到的结果便是防范这些攻击的方法。第 3 章、第 4 章、第 5 章及第 6 章中分别分析了漏洞攻击、共享文件夹安全隐患、木马的危害、QQ 密码丢失等问题，同时给出了相应的解决办法。

应该说，在黑客攻防方面历来都是“道高一尺，魔高一丈”，没有哪本书可以把黑客所有的攻击手段都剖析清楚，本书也只是讲述了那些最常见的黑客攻击手段。因此，本书是一本黑客攻防与网络安全的入门书，适合电脑初级使用者阅读参考。本书很多章节的内容用户直接用连接了 Internet 的个人电脑进行实践，达到理论学习与实际操作的统一。另外，本书还涉及一些网络方面的基础知识，适合对网络知识感兴趣的读者参阅。

由于黑客攻防与网络安全方面的知识太多，加上笔者自身能力有限，书中难免会有不当之处，还望同行不吝赐教。

编　者

目录



黑客攻防与网络安全概述

相信很多使用电脑的人都有过类似的经历：感染病毒、QQ 密码被盗,甚至电脑被远程控制等。所有这些都给我们的工作和生活带来了极大的不便，以至于我们开始怀疑既然电脑这么不安全，我们到底该不该用？答案是肯定的。只要掌握了足够的黑客与网络安全的知识，便可以自由、安全地遨游于网络世界。

本章将会讲解黑客与网络安全的基础知识，揭开黑客的神秘面纱。其中涉及到的术语将会用通俗的语言表述，如果实在看不懂可以略过，在后续章节中将进一步讲解。另外，本书中提到的所有操作都是在 Windows XP 系统下完成的，这些操作与其他的 Windows 系统操作很类似，因此不作区分。对于因操作系统不同而有所不同的操作，本书都做了区分，请根据自己的操作系统选择合适的操作。另外，本书中用到的共享软件或免费软件均可到 http://www.chinesehack.org 网站下载。

本章内容包括：

- ◆ 初识黑客
- ◆ 网络基本术语
- ◆ 黑客常用的攻击手段
- ◆ 木马程序简要介绍

1.1 初识黑客

“黑客”是一个外来词，来自英语中的 hacker。hacker 有很多意思，简单地可以理解成为破坏者。黑客之所以能破坏我们的电脑，主要是利用了系统或软件的漏洞，还有就是利用了使用者的一些不安全操作。总之，黑客最善于钻空子。

黑客能做的事情很多，他可以在不知不觉中入侵你的电脑、盗取密码、破坏系统，甚至可以在服务器上破解你的邮箱（E-mail）密码等。当然，因为大多数服务器都有很可靠的安全机制，黑客的入侵和破解都有很大的难度；相对而言，个人电脑则没有那么完善的安全机制，大多数黑客（特别是一些初级的黑客）都会选择攻击个人电脑。

本书将会提到很多黑客常用的攻击手法，其中绝大部分都是针对个人电脑实施攻击的。但是，如何攻击个人电脑并不是本书的写作目的，所以每种攻击方法之后都给出了详细的解决和防备方案。黑客技术实在是太多了，而且有些技术非常复杂，本书只是勾勒出黑客技术的概貌，同时给出“以不变应万变”的防御方法。

1.2 网络基本术语

要了解黑客与网络安全的技术，首先就要理解一些基本的网络术语。

1. 拨号上网

用户通过电话线拨号连接到 Internet 上，常见的拨叫 163、169 等上网方式都属于拨号上网。

2. 局域网

多台电脑通过网络连接设备形成的一个小型的网络叫做局域网。连接设备可以有很多种：双绞线、光纤、同轴电缆等。当然一个局域网可以包括几台（如网吧）或者几百台（如校园网）计算机。另外，不仅计算机之间可以互连成局域网，几个小的局域网还可以连接成一个大的网络（如 Internet）。

3. IP 地址

所有连接到 Internet 上的计算机必须有一个惟一的地址，否则计算机之间将不能进行通信，就像如果不知道地址便无法邮信一样。该地址由国际上的专门组织进行分配和管理。IP 地址采取 x.x.x.x 的形式，其中 x 为 0～255 之间的数字，如 202.116.37.156。

拨号上网用户的 IP 地址是动态分配的，即每次上网的 IP 地址是不同的。

4. 域名

由于 IP 地址很不容易记忆，于是便出现了域名。例如，www.sohu.com 就是一个域名，与它对应的 IP 地址是 61.135.132.174。域名的分配和管理也是由专门的组织负责的。当然，在 Internet Explorer（以后简称 IE）地址栏中输入 www.sohu.com 或者 61.135.132.174 都可以连到“搜狐”的网站上。

由于从域名到 IP 地址需要一个解析过程，所以输入 IP 地址连接速度会快一些。

5. 计算机名

每台计算机必须有一个计算机名（即使这台计算机不在任何网络中），这个名字通常是方便记忆的字符串，例如 MyComputer。

6. MAC 地址

在局域网中的计算机要用到网卡，每张网卡的标识（也就是 MAC 地址）是不同的。

7. 端口

在完成繁重的网络活动时，只有 IP 地址是不够的。常常有这种情况：一边浏览网页，一边聊 QQ。当某一信息到来时，如何区分哪个信息是网页的，哪个信息是 QQ 的呢？这就要用到端口。端口值可以是 1～65535 中的任意数字，小于 1024 的端口由系统程序使用，所以大于 1024 的端口便常常被黑客利用，例如木马“冰河”利用的端口就是 7626。下面列出一些常用的端口及其用途：

21 端口：FTP（File Transfer Protocol 文件传输协议）服务所用端口。最常见的攻击手法是寻找打开 anonymous 账号的 FTP 服务器。

25 端口：SMTP（Simple Mail Transfer Protocol， 简单邮件传输协议）服务所用端口。

110 端口：POP（Post Office Protocol， 邮局协议）服务所用端口。POP 服务有许多公认的弱点，仅仅关于用户名和密码交换缓冲区溢出的弱点至少有 20 个。

139 端口：NetBIOS 服务所用端口。该端口的漏洞会在第 4 章中详细讲解。

8. 共享

上网的目的很大程度上是为了找到自己想要的信息，信息共享也正是网络的魅力所在。如何实现信息共享呢？方法很多，可以架设 Web 服务器、FTP 服务器等。

最简单的方法就是利用 Windows 提供的共享文件夹功能实现共享。

9．注册表

注册表中记录了计算机运行时所需的所有重要的信息。所以，不当的操作将会带来整个系统崩溃的危险。

1.3 黑客常用的攻击手法

兵法有云：知己知彼，百战不殆。了解黑客的常用手法是防黑的基础。黑客技术其实并不神秘，大多数黑客都使用一些软件来进行破坏活动。本节将对黑客惯用的“伎俩”进行介绍、分析，后面的章节将会介绍一些黑客软件的使用方法。

1．系统漏洞攻击

这种攻击方法应该说是黑客最常用的。如果目标计算机的系统确实存在漏洞，只要知道目标的 IP 地址以及系统的版本，便可以实施攻击。许多系统都有这样那样的安全漏洞，其中某些是操作系统或工具软件本身的缺陷。例如 Windows 98 中的共享目录密码验证漏洞，Microsoft Outlook 2002 E-mail 头处理远程拒绝服务攻击漏洞等，这些漏洞在补丁程序未被开发出来之前几乎是无法防御的，安装系统的升级补丁是解决这类问题的惟一办法。还有一些漏洞是由开发程序员的疏忽造成的。为了方便调试，程序员常常在某一模块中加入调试代码，当整个软件开发完成时再将这些代码删除。但由于疏忽可能留下某些调试代码，这就给了黑客以可乘之机。

2．通过电子邮件进行攻击

电子邮件（E-mail）是 Internet 上运用十分广泛的一种通信方式。黑客可以使用一些邮件炸弹或者 CGI 程序向目标邮箱发送大量垃圾邮件，从而将目标邮箱“炸”掉。当有多台计算机同时发送大量垃圾邮件时，还可能造成邮件系统对正常的工作反应缓慢，甚至瘫痪，这一点与“拒绝服务攻击（DoS）”比较类似。还有一种方法就是利用邮件的附件发送病毒和木马程序。因此，在打开 E-mail 中的附件时要格外慎重，建议同时开启病毒防火墙，确保安全。

3．安装木马程序

利用木马攻击一般要在目标计算机的系统中隐藏一个会在 Windows 启动时自动运行的程序；然后，采用服务器/客户机的运行方式，达到控制目标计算机的目的。通过木马程序几乎可以得到目标计算机的所有信息，对目标计算机进行任何操作。实际上，木马程序属于一种远程控制软件，只不过它的服务器端更加隐蔽，在未经授权的情况下远程控制目标计算机，因此是非法的。既然是远程控制，那么通过木马客户端便可以对目标计算机进行几乎所有的控制，如窃取密码口令、更改文件操

作、捕捉屏幕、修改注册表等。由于木马程序实在太强大了，而且操作简单，所以成为众多黑客的最爱。

4．解密攻击

说到密码，几乎所有上网的人都用到过。登录 E-mail 要用到密码，登录 QQ 要用到密码，登录论坛要密码……。现在的密码保护手段大都是只认密码不认人，只要有密码，系统就会通过认证，授权为正常用户。因此，非法获取密码便吸引了众多黑客的注意力。获取密码的手段很多，利用木马程序当然可以获取密码，另外有一种叫做“暴力破解”的方法。“暴力破解”的工作原理是：通过提取密码字典（通常是一个存有好多密码的文件）中的密码项，逐个尝试。理论上只要密码字典足够大，密码项足够多，总是可以试出来的。不过，需要的时间可能会比较长。

5．Web 攻击

很多在聊天室里聊天的人都遇到过这种情况：屏幕上不断弹出警告或者错误对话框，怎么也没办法把所有的对话框都关闭。这不是聊天室系统出了毛病，实际上是别人给你发了一段 HTML 语句，例如一个死循环语句。当然这样攻击的前提是聊天室系统允许用户使用 HTML 语言的功能。为了安全起见，可以禁止自己的 IE 中运行 Web 脚本。

禁止 IE 运行 Web 脚本

Step 1　右击桌面上的 IE 图标，将弹出快捷菜单，如图 1.1 所示。

Step 2　选择【属性】菜单命令，将弹出【Internet 属性】对话框，如图 1.2 所示。

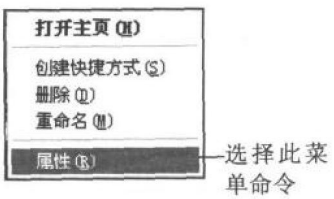


图 1.1　IE 快捷菜单

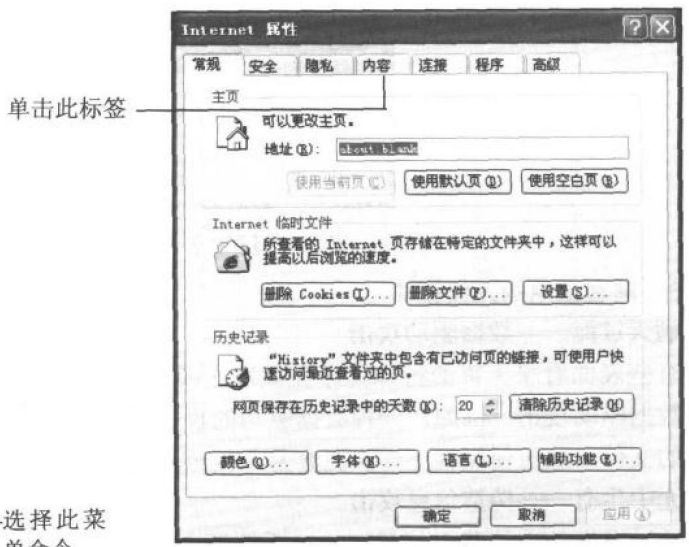


图 1.2　【Internet 属性】对话框

Step 3　单击【安全】标签，将出现【安全】选项卡，如图 1.3 所示。

Step 4　单击【自定义级别】按钮，将弹出【安全设置】对话框，如图 1.4 所示。

Step 5　向下拉动【设置】列表框，在【活动脚本】中单击【禁用】单选按钮；最好也在【Java 小程序脚本】中单击【禁用】单选按钮。

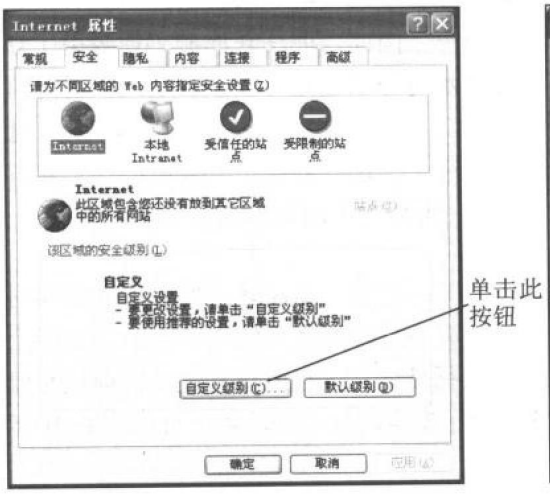


图 1.3　【安全】选项卡

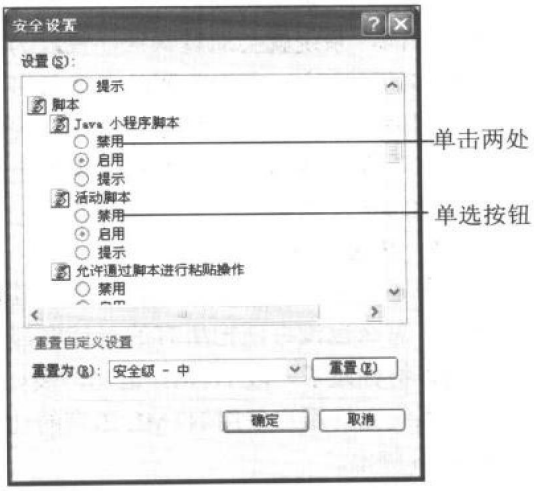


图 1.4　【安全设置】对话框

Step 6　单击【确定】按钮，将弹出【警告】对话框，如图 1.5 所示，请单击【是】按钮。

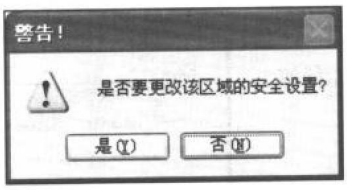


图 1.5　【警告】对话框

6. 黑客惯用的入侵策略

瞒天过海——数据驱动攻击

有些表面看来无害的特殊程序在被发送或复制到网络主机上并被执行时，就会发生数据驱动攻击。例如，一种数据驱动的攻击可以造成一台主机 修改与网络安全有关的文件，从而使黑客下一次更容易入侵该系统。

无中生有——伪造信息攻击

通过发送伪造的路由信息，构造系统源主机和目标主机的虚假路径，从而使流向目标主机的数据包均经过攻击者的系统主机，这样就可以截获敏感的信息和有用

的密码。

顺手牵羊——利用系统管理员失误攻击

网络安全的重要因素之一就是人!无数历史事实表明:“保垒最容易从内部攻破”。因而人为的失误，如 WWW 服务器系统的配置差错、普通用户使用权限扩大等，都会给黑客造成可趁之机。黑客常利用系统管理员的失误收集攻击信息。如用 finger、netstat、arp、w、who、ps、ls、mail、grep 命令和 SATAN 黑客工具软件进行攻击。

偷梁换柱——窃取 TCP 协议

TCP（Transfer Control Protocal，传输控制协议）最初的设计目的是为了更方便信息的交流，因此设计者对安全方面很少考虑甚至不去考虑。针对安全协议的分析成为攻击中最历害的一招。在几乎所有由 UNIX 实现的协议中，都存在着一个久为人知的漏洞，这个漏洞使得窃取 TCP 连接成为可能。当 TCP 连接正在建立时，服务器用一个含有初始序列号的应答报文来确认用户请求。这个序列号无特殊要求，只要是惟一的就可以了。客户端收到回答后，再对其确认一次，连接便成功建立了。TCP 协议规范要求每秒更换序列号 25 万次，但大多数的 UNIX 系统实际更换频率远小于此数量，而且下一个更换的数字往往是可以预知的。黑客正是有这种可预知服务器初始序列号的能力使得攻击可以完成。惟一可以防治这种攻击的方法是使初始序列号的产生更具有随机性。最安全的解决方法是用加密算法产生初始序列号，由此产生的额外的 CPU 运算负载对现在的硬件来说是可以忽略的。

暗渡陈仓——针对信息协议弱点攻击

IP 地址的源路径选项允许 IP 数据包自己选择一条通往系统目的主机的路径。设想攻击者试图与防火墙后面的一个不可到达主机 A 连接，他只需要在送出的请求报文中设置 IP 源路径选项，使报文有一个目的地址指向防火墙，而最终地址是主机 A。当报文到达防火墙时被允许通过，因为它指向防火墙而不是主机 A。防火墙的 IP 层处理该报文的源路径被改变，并发送到内部网上，报文就这样到达了不可到达的主机 A。

借尸还魂——重新发送（REP-LAY）攻击

收集特定的 IP 数据包，篡改其数据，然后再一一重新发送，欺骗接收的主机。

抛砖引玉——针对源路径选项的弱点攻击

强制报文通过一个特定的路径到达目的主机。这样的报文可以用来攻陷防火墙和欺骗主机。一个外部攻击者可以传送一个具有内部主机地址的源路径报文。服务器会相信这个报文并对攻击者发回答报文，因为这是 IP 的源路径选项要求的。对付这种攻击最好的办法是配置好路由器，使它抛弃那些由外部网进来的却声称是内部主机的报文。

调虎离山、声东击西——对 ICMP 报文的攻击

尽管比较困难，黑客们有时也使用 ICMP 报文进行攻击。重定向消息可以改变路由列表，路由器可以根据这些消息建议主机走另一条更好的路径。攻击者可以有效地利用重定向消息把连接转向一个不可靠的主机或路径，或使所有报文通过一个不可靠主机来转发。对付这种威胁的方法是对所有 ICMP 重定向报文进行过滤，有的路由软件可对此进行配置。单纯地抛弃所有重定向报文是不可取的：主机和路由器常常会用到它们，例如一个路由器发生故障时。

趁火打劫——系统文件非法利用

UNIX 系统可执行文件的目录，如/bin/who 可由所有的用户进行读访问。有些用户可以从可执行文件中得到其版本号，从而结合已公布的资料知道系统会具有什么样的漏洞，如通过 Telnet 指令操作就可以知道 Sendmail 的版本号。禁止对可执行文件的访问虽不能防止黑客对它们的攻击，但至少可以使这种攻击变得更困难。还有一些弱点是由配置文件、访问控制文件和默认初始化文件产生的。最出名的一个例子是：用来安装 SunOS Version 4 的软件，它创建了一个/rhosts 文件，这个文件允许局域网（因特网）上的任何人、从任何地方取得对该主机的超级用户特权。当然，最初这个文件的设置是为了“从网上方便地进行安装，而不需超级用户的允许和检查”。

“智者千虑、必有一失”，操作系统设计的漏洞为黑客开启了后门，最近针对 Win 95/Win NT 的一系列具体攻击就是很好的实例。

笑里藏刀——远端操纵

默认的登录界面（shell scripts）、配置和客户文件常常会引发这样一个问题：远端操纵。因为它们提供了一个简单的方法来配置一个程序的执行环境，这很容易在被攻击主机上启动一个可执行程序，该程序显示一个伪造的登录界面；当用户在这个伪装的界面上输入登录信息（用户名、密码等）后，该程序将用户输入的信息传送到攻击者主机，然后关闭界面给出提示信息说“系统故障”，要求用户重新登录；此后，才会出现真正的登录界面。在我们能够得到新一代更加完善的操作系统版本之前，类似的攻击仍会发生。防火墙的一个重要作用就是防止非法用户登录到受保护网站的主机上。例如，可以在进行报文过滤时，禁止外部主机 Telnet 登录到内部主机上。

混水摸鱼——以太网广播攻击

将以太网接口设置为乱模式（promiscuous），截获局部范围的所有数据包，为我所用。

远交近攻——“跳跃式”攻击

现在许多因特网上的站点使用 UNIX 操作系统。黑客们会设法先登录到一台

UNIX 的主机上，通过该操作系统的漏洞来取得系统特权，然后再以此为据点访问其余主机，这被称为“跳跃”（Island-hopping）。黑客们在达到目的主机之前往往会这样跳跃几次。例如，一个在美国的黑客在进入美联邦调查局的网络之前，可能会先登录到亚洲的一台主机上，再从那里登录到加拿大的一台主机，然后再跳到欧洲，最后从法国的一台主机向联邦调查局发起攻击。这样被攻击的网络即使发现了黑客是从何处向自己发起了攻击，管理人员也很难顺藤摸瓜找回去，更何况黑客在取得某台主机的系统特权后，可以在退出时删掉系统日志，把“藤”割断。你只要能够登录到 UNIX 系统上，就能相对容易成为超级用户，这使得它同时成为黑客和安全专家们的关注焦点。

反客为主——夺取系统控制权

在 UNIX 系统下，多数文件只能由超级用户拥有，少数可以由某一类用户所有，这使得管理员必须在 root 下进行各种操作，这种做法并不安全。黑客攻击的首要对象就是 root，最常受到攻击的目标是超级用户的 Password。严格来说，UNIX 下的用户密码是没有加密的，它只是作为 DES 算法加密一个常用字符串的密钥。现在出现了许多用来解密的软件工具，它们利用 CPU 的高速度来究尽式搜索密码。攻击一旦成功，黑客就会成为 UNIX 系统中的“皇帝”。因此，将系统中的权利进行“三权分立”，如果设定邮件系统邮件由管理员管理，那么邮件管理员可以在不具有超级用户特权的情况下很好地管理邮件系统，这会使系统安全很多。此外，攻击者攻破系统后，常使用金蝉脱壳之计——删除系统运行日志，使自己不被系统管理员发现，便于以后东山再起。故有“用兵之道，以计为首”之说，作为网络攻击者会竭尽一切可能的方法，使用各种计谋来攻击目标系统。

1.4 木马程序简要介绍

上一节简要讲解了黑客常用的攻击手法。漏洞攻击主要依赖于系统漏洞，然而系统漏洞并不是一般用户可以查到的，通常黑客只是利用别人编写好的漏洞攻击软件进行攻击。一旦漏洞被堵上，黑客便无法用此方法进行攻击。其他的几种攻击方法虽然可以实现某些功能，可是仅仅这些功能是不能满足黑客的好奇心理的。但是木马程序就不一样了，现在的木马程序越来越隐蔽，功能也越来越强大，使用的人也越来越多。因此，有必要重点来讲解一下木马程序。

“木马”来源于希腊的特洛伊木马神话。传说希腊人围攻特洛伊城，久攻不破。后来他们便想出了一个木马计，让士兵藏匿于一个个巨大的木马中。希腊军队假装战败，故意将木马摈弃于特洛伊城外，这种大木马被敌人当作战利品拖入城内。木