CD + 书 23.8 元

黑客防线

# 黑客攻击技术揭秘

## 基础+实例+防范+工具+源代码+电子教程+攻防演示=黑客攻击技术揭秘

本书对普通电脑用户、网络用户以及网络技术人员均有很高的参考价值。

完全攻防全程录像演示


40例攻防全程录像，采用真实的演示环境，形象生动地揭示出黑客常用攻击手法，使读者能够清楚地看到黑客攻击全过程，从而做好防范工作。另外，大量的电子教程和黑客攻防程序源代码以及流行黑客攻防工具，将近600M的容量，绝对适合各层次读者阅读和珍藏。

# 黑客攻击技术揭秘

黑客防线编辑部　　编著

家庭电脑世界杂志社出版

本书作者为专业防黑高手，具备扎实的理论知识和丰富的实战经验。全书从攻击者和防御者的不同角度系统阐述了黑客攻击的入侵手段及相应的防御措施，精心选取了目前网络安全与防黑方面带有普遍意义的典型范例进行讲解，详细剖析了黑客攻击与网络防黑的基本原理。全书分为6章，囊括了当今流行的黑客攻击技术，涵盖面广，且对问题分析得非常透彻，有助于网络和系统管理员保护计算机系统。

本书更具价值的是近600M的配套光盘，以形象生动的攻防录像演示，配合大量的电子教程和黑客程序源代码以及流行黑客工具，绝对适合各层次读者阅读和珍藏。

本书对普通电脑用户、网络用户以及网络技术人员均有很高的参考价值。

**策　　划**：《家庭电脑世界》编辑部
《黑客防线》编辑部
**制　　作**：家庭电脑世界
CN15－9201/TP
**通信地址**：北京市中关村邮局008信箱
《家庭电脑世界》邮购部
**邮　　编**：100080
**技术支持电话**：010－62141445－8013
**编　　辑**：郭聪辉　刘　峰
**制　　作**：王　凤　王　宇
**发行部电话**：010－62141446
**发行部传真**：010－62141360
E－mail：yougoubu@pcfriend.com.cn
**定　　价**：23.8元　（1CD）

凡购本书，如有缺页、倒装、脱页，由发行部调换

# 前　言

网络安全是一个流行的话题，但要知道的一点是，没有任何一个系统是绝对安全的，任何接入网络的系统都可能受到探测或入侵。在写这篇序言的时候，笔者的电脑用 ADSL 连接在 Internet 上，几乎一个星期被扫描和尝试入侵高达数 10 次，本机安全日志也飞快地变得庞大。

在 Internet 上，最热门的话题不容置疑地包括“黑客”一词，无论在哪一个搜索引擎内输入“黑客”，都会有成千上万条的信息扑面而来，而“黑客技术”，特别是关于“黑客攻击技术”则是内容最多的。纵观市面上关于“黑客”类图书，从去年年底到现在，确实是一个热点，但是多数图书基本上都是泛泛而谈，给读者一个概念性的认识，或是以非常专业的理论为主，实用性和普及性不强。本书将避开以上缺陷，展现常见入侵的过程，书中列举的都是现在网上常用的一些漏洞和相应的安全对策，只要具备一定电脑基础的读者，就可以学到很多关于入侵的知识。

随着宽带网络的普及，现在有越来越多的人都想着怎么成为一名 Hacker，于是到处在网上找黑客教程，学着使用黑客工具，往往他们进步了一点点，就很自傲，以为自己已经是一名 Hacker，但事实并非如此。我们也有个称呼给他们——“Scripts kids”，脚本小子。当然，这个不在我们讨论的话题之内。

我们的目的并不是教你入侵和破坏，只是展现了现在所谓”黑客”的攻击方法，希望你学到的是安全与防范，因为我们不能以“黑客”来作为终生事业，我们最终都会走上安全防范的道路——可能你也是未来的一员

最后要提的是，黑客入侵技术不会因为我们不去了解它而不复存在，黑客们也不会因为我们不去学习，不去掌握抗击技术和工具而放弃对“手无寸铁”者的攻击，网络安全的保卫者应力争不要落在攻击者的后面。我们需要在知识的获取上与入侵者比速度，如果能够先于攻击者之前了解这些知识，那么我们的网络就会更加有保障。

如何防止黑客的入侵、渗透等等，当然不是一本书就可以完全概括的，笔者只是把这些常用的入侵的手法和经过等过程再一次展现出来。

因为技术有限，并且存在其他因素，所以本书可能有不完善的地方。您有什么意见，请到 http://www.hacker.com.cn/bbs 中提出，也可以进入“在线解答”http://www.hacker.com.cn/webirc/webric.html 提出。

编　者

# 目 录

## 第一章 黑客与黑客文化



## 第二章 计算机网络系统安全漏洞分类

## 第七章 假消息攻击



## 第八章 其他类型攻击

## 第九章 常见攻击思路和方法

# 第一章　黑客与黑客文化

## 1.1 概述

### 1.1.1 什么是黑客

近年来，随着互联网的普及，信息产业的高速发展，越来越多的人不安分于在一台普通调制解调器前用各种手段来夺取想要的信息，或其他什么秘密。自 2001 年 5 月中美黑客大战以来，国内涌现出一批又一批的“红客”、“黑客”，不知道他们是以什么标准来定义黑客的。

“黑客”一词最早出现在 70 年代的美国麻省理工学院。“黑客精神”是任何信息都是自由公开的，任何人都可以平等地获取公开的信息；黑客必须是技术上的行家，喜欢挑战复杂的问题，突破技术的极限，对破解各种系统资源有自己独特的思路。

以前，国内很多人对黑客了解并不多，所以往往简单地把黑客与犯罪，破坏联系在一起，随着互联网的普及，越来越多的人对黑客的了解渐渐从模糊、恐惧转向中性。

现在，我们来重新认识一下黑客：他们是一些对计算机很着迷，有较强的思维逻辑能力，认为自己拥有比他人更高的才能，因此只要他们愿意，就能够不经过授权地进入各种系统，也可以随着自己的意愿去做某些被常人认为是极度危险的事情。

### 1.1.2 中国的网络战争手段分析

高速发展的互联网给日常生活、工作和人与人之间的沟通带来了极大的方便，但也成了培育黑客的温床。近年来，国际国内黑客事件的不断发生，不仅扰乱了正常的网络秩序，而且还带来了严重的经济损失，这种现象正逐渐引起各个国家和政府部门的重视。特别是近来，由于某些国家的强权政治和霸权主义思想有恃无恐，使得许多国家的安全和人权饱受威胁；但从长远利益考虑，国家之间近期是不可能发生战争的，但网络的无国界性给长期压抑的人们带来了发泄愤怒的机会，于是在网络上演绎了多起网络大战，其中尤以中美大战为甚，并且随着中美撞机事件引至网络黑客大战愈演愈烈，终于在 2001 年 5 月 1 日左右达到高潮。初期，国外黑客 PoisonBox、预言者、Acidklown、Hackweiser 和 PrimeSuspectz 等 5 个美国黑客团体对我国展开了网络攻击，后来 Subex、SVUN、嗨——技术等黑客团体也陆续加入。值得一提的是，嗨—技术原以美国军方为入侵对象，属于技术高超的黑客组织，此次也改旗易帜，将炮口对准了中国网站。由于在技术等方面与美国的差距，使得我国在这次网络大战中损失惨重。其间，江西宜春政府网、西安信息港、贵州方志与地情网、中国青少年发展基金会网、福建外贸信息网、湖北武昌区政府信息网以及桂林图书馆、中国科学院理化技术研究所、中国科学院心理研究所等网站遭到攻击，一些大型门户网站也相继被黑。这

是近年来中国网络安全受到的最大挑战。

上述事件中国外黑客入侵国内网站的攻击手法，总体上说水平一般，受攻击的大多是 Windows 系统，其次是 Linux、BSD、Solaris 等系统；主要方法是使用一些现有的工具对操作系统的弱口令或安全漏洞加以利用攻击，获得一般用户甚至管理员用户权限，进而达到实施破坏的目的。具体的攻击手段如下：

1. 弱口令攻击：不少网站的管理员账号密码、FTP 账号密码、SQL 账号密码等都使用很简单的或是很容易猜测到的字母或数字，利用现有的家用 PIII 机器配合编写恰当的破解软件即可在短时间内轻松破解，一旦口令被破解，网站就意味着被攻破。

2. Unicode 编码漏洞攻击：对于窗口 Windows NT4.0 和窗口 Windows 2000 来说都存在该漏洞，利用该漏洞，远程用户可以在服务器上以匿名账号来执行程序或命令，从而轻易就可达到遍历硬盘、删除文件、更换主页和提升权限等目的。由于实施方法简单，仅仅拥有一个浏览器就可实现攻击。上述被攻破的网站大多是因为存在此漏洞而导致攻击实现。

3. ASP 源码泄露和 MS SQL Server 攻击：通过向设 Web 服务器请求精心构造的特殊 URL 就可以看到不应该看到的 ASP 程序的全部或部分源代码，进而取得诸如 MS SQL Server 的管理员 sa 的密码，再利用存储过程 xp_cmdshell 就可远程以系统账号在服务器上任意执行程序或命令，事实上，MS SQL Server 默认安装的管理员 sa 的密码为空，并且大多数系统管理员的确没有重新设定新的复杂密码，这就直接留下了严重的安全隐患。

4. IIS 缓冲溢出攻击：对于 IIS4.0 和 IIS5.0 来说都存在严重的缓冲溢出漏洞，利用该漏洞，远程用户能以具有管理员权限的系统账号在服务器上任意执行程序或命令，极具危险性。但由于操作和实施较为复杂，一般为黑客高手所用。这种攻击主要存在于 Windows NT 和 2000 中。

5. Bind 缓冲溢出攻击：在最新版本的 Bind 以前的版本中都存在严重的缓冲溢出漏洞，可以导致远程用户直接以根权限在服务器上执行程序或命令，极具危险性。但由于操作和实施较为复杂，一般也为黑客高手所用。这种攻击主要存在于 Linux, BSDI 和 Solaris 等系统中。

6. 其他攻击手法：利用 Sendmail、Local printor、CGI、病毒、Trojan 人、DOS、DDoS 等漏洞攻击的手段。

## 1.1.3 网络安全专家的建议

国内著名的网络安全专家孤独剑客指出网络安全现状是：

(1)安全意识不强，缺乏整体安全方案；

(2)系统本身不安全；

(3)没有安全管理机制；

(4)不理解安全是相对的；

(5)缺少必需的安全专才。

如果想改善这样的情况，必须做到以下几点：

**1. 成立网络安全领导小组**

要从上到下把网络安全重视起来，由行政领导牵头，技术部门负责，系统和管理员参与，成立安全管理领导监督小组；加强网络安全项目的建设和管理，负责贯彻国家有关网络安全的法律、法规，落实各项网络安全措施；督促有关部门对网络用户进行安全教育，监督、检查、指导网络安全工

作；监督网络安全管理制度的执行和贯彻，查处违反网络安全管理的违纪、违规行为；协助、配合公安机关查处网络犯罪行为。

**2. 制订一套完整的安全方案**

一套完整的安全方案是整个系统安全的有力保障，要结合自己实际的网络状况，从人力、物力、财力等几方面做好部署与配置。由于安全方案涉及到安全理论、安全产品、网络技术、系统技术实现等多方面专业技能，并且要求要有较高的认知能力，大多数企业、公司、政府等可能不具备此能力，此时可以聘请专业安全顾问公司来完成，大多安全顾问公司在做安全方案方面有着丰富的经验，能够制订出符合需要的合理的安全方案来。

**3. 用安全产品和技术处理加固系统**

说到底，要使得网络系统是安全的，就必须对系统进行一系列的处理，比如安装防火墙和入侵检测系统等安全产品，为系统打补丁堵塞安全漏洞，用户和文件目录权限管理，设置安全策略等系统安全处理，以求消除隐患，加固系统。由于这种系统加固服务需要非常专业的安全技能，一般的企业和公司要想做好是不现实的，而大多数安全咨询顾问公司都提供这种服务。主要加固项目如下：

(1) 网络拓扑路由分析；
(2) 防火墙内外部隔离；
(3) 入侵检测系统跟踪；
(4) 网站恢复系统监控；
(5) 系统安全加固处理；
(6) 应用系统安全检测；
(7) 整体网络安全评估。

**4. 制定并贯彻安全管理制度**

在对系统安全方案和系统安全设置的同时，还必须制定出一套完整的安全管理制度，如外来人员网络访问制度，服务器机房出入管理制度，管理员网络维护管理制度；约束普通用户等网络访问者，督促管理员很好地完成自身的工作，增强大家的网络安全意识，防止因粗心大意或不贯彻制度而导致安全事故。尤其要注意制度的监督贯彻执行，否则就形同虚设。

**5. 建立完善的安全保障体系**

建立完善的安全保障体系是系统安全所必需的，如管理人员安全培训，可靠的数据备份，紧急事件响应措施，定期系统安全评估及更新升级系统，这些都为系统的安全提供了有力的保障，确保系统能一直处于最佳的安全状态，即便系统受到攻击，也能最大程度地挽回损失。

**6. 选择一个好的安全顾问公司**

可以说，在两年前国内还没有一家真正意义上的网络安全顾问公司，但由于目前形势的需要，国内的安全顾问公司可以说是蓬勃发展，百花齐放，但主要是从以下几种转型而来：

(1)网络安全产品公司兼做网络安全顾问服务；
(2)传统系统集成公司设立网络安全顾问部门；
(3)自由黑客组织转型为专业网络安全顾问公司；
(4)国家科研教育机构成立的网络安全顾问公司。

选择安全顾问公司是要非常谨慎的，要从安全公司的背景、理念、实力、管理等多方面进行考

察，不仅要看一个安全公司的技术和资金实力，而且还要看公司人员的组成，因为一旦你的系统交给了安全公司，就等于对其百分之百地开放，但大多网络安全公司人员层次不齐，即便技术和资金很强，但若管理不善，人员流失较大，就会使得客户的系统资料处于不可控状态，从而带来极大的安全隐患。所以，一旦选择失误，不仅不能带来安全保障，而且可能会造成无法弥补的损失。

## 1.2 Hacker 文化简史

### 1.2.1 Real Programmer(真正的程序员)

首先我们要介绍的就是所谓的 Real Programmer，他们从不自称是 Real Programmer、Hacker 或任何特殊的称号。“Real Programmer’”这个词在 20 世纪 80 年代才出现，但早自 1945 年起，电脑科学便不断地吸引世界上头脑最顶尖、想像力最丰富的人投入其中。从 Eckert & Mauchly 发明 ENIAC 后，便不断有狂热的 Programmer 投入其中，他们以撰写软件与玩弄各种程序设计技巧为乐，逐渐形成具有自我意识的一套科技文化。当时这批 Real Programmers 主要来自工程界与物理界，用机器语言、汇编语言、FORTRAN 及很多古老的 语言写程序。他们是 Hacker 时代的先驱者，默默贡献，却鲜为人知。

从二次大战结束后到 70 年代早期，是打卡计算机与所谓“大铁块”的 Mainframes 流行的年代，由 Real Programmer 主宰电脑文化。Hacker 传奇故事，如有名的 Mel （收录在 Jargon File 中）、Murphy’s Law 的各种版本、mock - German“Blinkenlight”等文章都是流传久远的老掉牙笑话了。

一些 Real Programmer 仍在世界十分活跃。超级电脑 Cray 的设计者 Seymour Cray，亲手设计 Cray 全部的硬件与其操作系统，操作系统是他用机器码硬干出来的，没有出过任何 BUG 或 Error。

Real Programmer 的时代步入尾声，取而代之的是逐渐盛行的 Interactive Computing，它们催生了另一个持续的工程传统，并最终演化为今天的开放代码黑客文化。

### 1.2.2 早期的黑客

Hacker 时代的滥觞始于 1961 年 MIT 出现第一台电脑 DEC PDP - 1。MIT 的 Tech Model Railroad Club(简称 TMRC)的 Power and Signals Group 买了这台机器后，把它当成最时髦的科技玩具，各种程序工具与电脑术语开始出现，整个环境与文化一直发展至今日。

开始，整个 Hacker 文化的发展以 MIT 的 AI Lab 为中心，但 Stanford University 的 Artificial Intelligence Laboratory(简称 SAIL)与稍后的 Carnegie - Mellon University(简称 CMU)快速崛起。它们 3 个都是大型的资讯科学研究中心及人工智慧的权威，聚集着世界各地的精英，不论在技术上或精神层次上，对 Hacker 文化都有极高的贡献。

另一个 Hacker 重镇是 XEROX PARC 公司的 Palo Alto Research Center。从 20 世纪 70 年代初期到 80 年代中期这十几年间，PARC 不断出现惊人的突破与发明，包括质量、软件或硬件方面。如现今的 Windows 操作系统，激光打印机与局域网络；其 D 系列的机器，催生了能与迷你电脑一较高下的强力个人电脑。不幸的是，这群先知先觉者并不受公司高层的赏识，PARC 是家专门提供好点子帮别人赚钱的公司成为众所皆知的大笑话。即使如此，PARC 这群人对 Hacker 文化仍有不可磨灭

的贡献。70 年代与 PDP - 10 文化迅速成长茁壮。Mailing list 的出现使世界各地的人得以组成许多 SIG(Special - interest group),不只在电脑方面,也有社会与娱乐方面的。DARPA 对这些非"正当性"活动睁一只眼闭一只眼,因为靠这些活动会吸引更多的聪明小伙子们投入电脑领域。

### 1.2.3 UNIX 的兴起

此时在新泽西州的郊外,另一股神秘力量积极入侵 Hacker 社会,最终席卷整个 PDP - 10 的传统。它诞生在 1969 年,也就是 ARPANET 成立的那一年,有个在 AT& T Bell Labs 的年轻小伙子 Ken Thompson 发明了 UNIX。

Thomspon 曾经参与 Multics 的开发,Multics 是源自 ITS 的操作系统,用来实验当时一些较新的 OS 理论,如把操作系统较复杂的内部结构隐藏起来,提供一个界面,使得 Programmer 能不用深入了解操作系统与硬体设备,也能快速开发程序。

Ken Thompson 很喜欢 Multics 上的作业环境,于是他在实验室里一台报废的 DEC PDP - 7 上胡乱写了一个操作系统,该系统在设计上有从 Multics 抄来的,也有他自己的构想。他将这个操作系统命名 UNIX,用来反讽 Multics。

他的同事 Dennis Ritchie 发明了一种新的程序语言 C,于是他与 Thompson 用 C 语言把原来用汇编语言写的 UNIX 重写了一遍。C 的设计原则就是好用,自由与弹性。C 与 UNIX 很快在 Bell Labs 得到欢迎。1971 年,Thompson 与 Ritchie 争取到一个办公室自动化系统的专案,UNIX 开始在 Bell Labs 中流行。不过 Thompson 与 Ritchie 的雄心壮志还不止于此。

那时的传统是,一个操作系统必须完全用汇编语言写成,才能让机器发挥最高的效能。Thompson 与 Ritchie 是头几位领悟到硬件与编译器的技术已经进步到作业系统,可以完全用高阶语言如 C 来写,仍保有不错效能的人。5 年后,UNIX 已经成功地移植到数种机器上。

这在当时是一件不可思议的事!它意味着,如果 UNIX 可以在各种平台上跑的话,UNIX 软件就能移植到各种机器上,再也用不着为特定的机器写软件了。

除了跨平台的优点外,UNIX 与 C 还有许多显著的优势。UNIX 与 C 的设计哲学是 Keep it simple, stupid, Programmer 可以轻易掌握整个 C 的逻辑结构(不像其他之前或以后的程序语言)而不用一天到晚翻手册写程序。而 UNIX 提供许多有用的小工具程序,经过适当的组合(写成 Shell script 或 Perl script),可以发挥强大的威力。

C 与 UNIX 的应用范围之广,出乎原设计者之意料,很多领域的研究要用到电脑时,它们是最佳拍档。尽管缺乏一个正式支持的机构,它们仍在 AT& T 内部中疯狂地散播。到了 1980 年,C 与 UNIX 已蔓延到大学与研究机构,还有数以千计的 Hacker 想把 UNIX 装在家里的机器上。

当时跑 UNIX 的主力机器是 PDP - 11、VAX 系列的机器。不过由于 UNIX 的高移植性,它几乎可以安装在所有的电脑机型上。一旦新型机器上的 UNIX 安装好,把软件的 C 原始码抓来重新编译就一切 OK 了,谁还要用汇编语言来开发软件? 有一套专为 UNIX 设计的网络——UUCP:一种低速、不稳但成本很低廉的网络。两台 UNIX 机器用一条电话线连起来,就可以使用互传电子邮件。UUCP 是内建在 UNIX 系统中的,不用另外安装,于是 UNIX 站台连成了专属的一套网络,形成其 Hacker 文化。在 1980 年第一个 USENET 站台成立之后,组成了一个特大号的分散式布告栏系统,吸引而来的人数很快超过了 ARPANET。

## 1.2.4 古老时代的终结

到 1980 年，同时有 3 个 Hacker 文化在发展，尽管彼此偶有接触与交流，但还是各玩各的。ARPANET/PDP－10 文化，玩的是 LISP、MACRO、TOPS－10 与 ITS；UNIX 与 C 的拥护者用电话线把他们的 PDP－11 与 VAX 机器串起来玩；还有另一群散乱无秩序的微电脑迷，致力于将电脑科技平民化。

三者中 ITS 文化(也就是以 MIT AI Lab 为中心的 Hacker 文化)在此时达到全盛时期，但乌云也开始笼罩这个实验室。ITS 赖以维生的 PDP－10 逐渐过时，开始有人离开实验室去外面开公司，将人工智慧的科技商业化；MIT AI Lab 的高手挡不住新公司的高薪挖脚而纷纷出走；SAIL 与 CMU 也遭遇到同样的问题。

致命一击终于来临。1983 年 DEC 宣布：为了集中 PDP－11 与 VAX 生产线，将停止生产 PDP－10；ITS 没希望了，因为它无法移植到其他机器上，或说根本没人办的到。而 Berkeley Univeristy 修改过的 UNIX 在新型的 VAX 跑得很顺，是 ITS 理想的取代品。有远见的人都看得出，在快速成长的微电脑科技下，UNIX 一统江湖是迟早的事。

## 1.2.5 私有 UNIX 时代

1984 年，AT& T 解散了，UNIX 正式成为一个商品。当时的 Hacker 文化分成两大类，一类集中在 Internet 与 USENET 上(主要是跑 UNIX 的迷你电脑或工作站连上网络)以及另一类 PC 迷，他们绝大多数没有连上 Internet。

Sun 与其他厂商制造的工作站为 Hacker 们开启了另一个美丽新世界。工作站诉求的是高效能的绘图与网络，80 年代的 Hacker 们致力为工作站撰写软件，不断挑战及突破以求将这些功能发挥到 101%。Berkeley 发展出一套内建支持 ARPANET protocols 的 UNIX，让 UNIX 能轻松连上网络，Internet 因此成长得更加迅速。

除了 Berkeley 让 UNIX 网络功能大幅提升外，尝试为工作站开发一套图形界面的也不少。最有名的要算 MIT 开发的 X－Window 了。X－Window 成功的关键在完全公开原始码，展现出 Hacker 一贯作风，并散播到 Internet 上。X 成功地干掉其他商业化的图形界面的例子，对数年后 UNIX 的发展有著深远的启发与影响。少数 ITS 保守派仍在顽抗，到 1990 年，最后一台 ITS 也永远关机长眠了，保守派在穷途末路下只有悻悻地投向 UNIX 的怀抱。

UNIX 此时也分裂为 Berkeley UNIX 与 AT& T 两大阵营。到 1990 年，AT& T 与 BSD 版本已难明显区分，因为彼此都有采用对方的新发明。随着 90 年代的来到，工作站的地位逐渐受到新型廉价的高档 PC 的威胁，它们主要采用 Intel 80386 系列 CPU。第一次，Hacker 能买一台威力等同于 10 年前的迷你电脑的机器，上面跑着一个完整的 UNIX，且能轻易地连上网络。

机器有了，可以上网了，但软件去哪里找？商业的 UNIX 很贵，一套要好几千美元。90 年代早期，开始有公司将 AT& T 与 BSD UNIX 移植到 PC 上出售。成功与否不论，价格并没有降下来，更要紧的是没有附源代码，你根本不能、也不准修改它以符合自己的需要或拿去分享给别人。传统的商业软件并没有给 Hacker 们真正想要的东西。