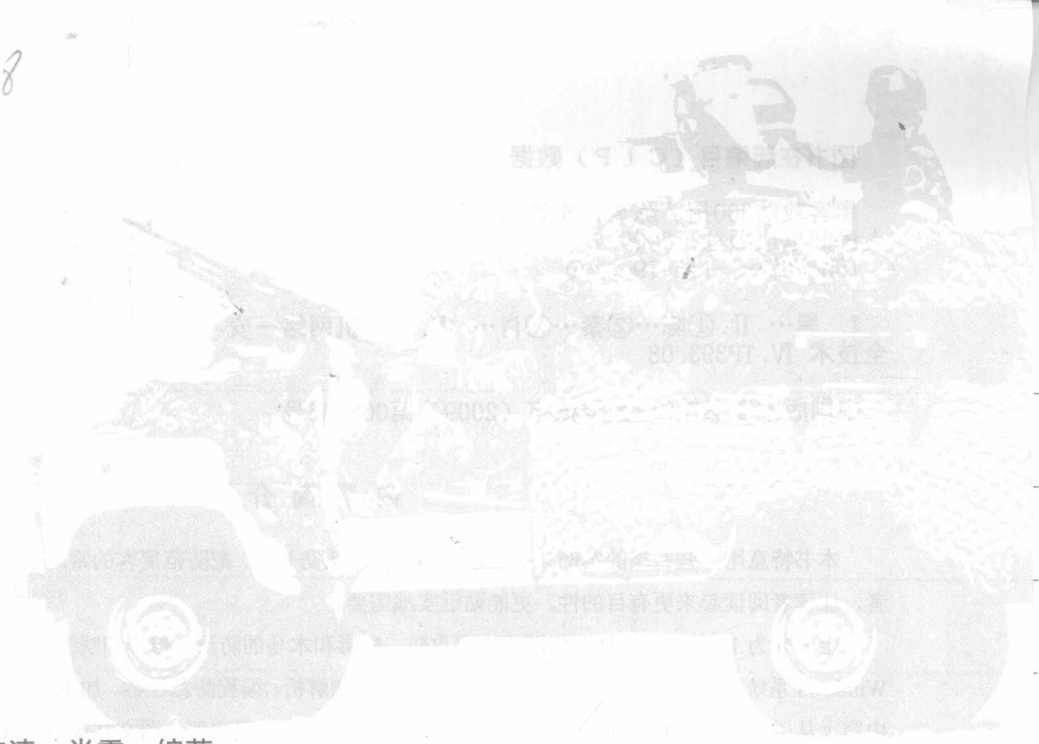
信息安全大系

- 源于实践的300个案例，帮助读者提升实战能力
- 涵盖脚本注入、远程控制、漏洞检测、黑客编程、扫描、嗅探等主流的攻防技术
- 详细剖析黑客攻击的方法，给出完整的解决方案

黑客攻防300招

陈芳　秦连清　肖霞　编著

人民邮电出版社
POSTS & TELECOM PRESS



陈芳　秦连清　肖霞　编著

黑客攻防300招

人民邮电出版社
北京

图书在版编目（CIP）数据

黑客攻防300招 / 陈芳，秦连清，肖霞编著. —北京：人民邮电出版社，2009.4
ISBN 978-7-115-19662-0

Ⅰ. 黑… Ⅱ. ①陈…②秦…③肖… 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（2009）第008136号

内 容 简 介

本书特意用一些有趣的案例来引导读者学习黑客攻防知识，把防范黑客的常用技术以招数的形式展示给读者，让读者阅读起来更有目的性，更能贴近实战需要。

全书分为 11 部分，包括网络游戏密码攻防、病毒和木马的防治、扫描和嗅探工具的使用、网络攻击防范、Windows 系统漏洞剖析、注册表操作、远程协助和控制解析、编程防范黑客、加密解密技术等实战知识和技巧。内容上从“攻”、“防”两个不同的角度，通过剖析典型的入侵实例，图文并茂地再现了防御黑客入侵的全过程，为帮助用户防御黑客攻击和保卫网络安全提供了很多行之有效的技术指导。

本书内容丰富，实战性和可操作性强，适合于网络技术爱好者、网络系统管理员阅读，也可作为相关专业学生的学习书籍和参考资料。

黑客攻防 300 招

◆ 编　　著　陈　芳　秦连清　肖　霞
责任编辑　屈艳莲
执行编辑　张　涛

◆ 人民邮电出版社出版发行　　北京市崇文区夕照寺街 14 号
邮编　100061　　电子函件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
三河市海波印务有限公司印刷

◆ 开本：787×1092　1/16
印张：23.75
字数：562 千字　　2009 年 4 月第 1 版
印数：1–4 000 册　　2009 年 4 月河北第 1 次印刷

ISBN 978-7-115-19662-0/TP

定价：45.00 元

读者服务热线：(010)67132692　印装质量热线：(010)67129223
反盗版热线：(010)67171154

前言

随着计算机技术的进步和网络的迅速发展，越来越多的人开始适应网络生活，如网上开店、网络购物等都成为人们的钟爱。

但随着黑客工具的简单化和傻瓜化，也方便了一些怀有不良动机的人利用手中的黑客工具进行大肆攻击，使用户面临着网络安全的重大威胁。出于以上原因，本书通过实例逐步对黑客的攻击和防范技术进行了系统化的讲解，从而帮助人们找出最有效的防范方法。

全书分为 11 部分。

第 1 部分　千里之行，始于足下——黑客入门。全面介绍了黑客的基础知识，以及一些常见的攻防方式，让读者对如何防范木马和病毒的攻击有初步的了解，为今后的学习打下基础。

第 2 部分　上下其手——密码盗窃防范。通过剖析黑客进行这类攻击时常用的手段和工具，为读者防范这类黑客提供了行之有效的防御技术。

第 3 部分　山雨欲来风满楼——病毒和木马防范知识。介绍了网络上典型木马和病毒的攻防技术，如 U 盘病毒、FTP 木马和代理木马等，通过分析这些典型病毒和木马的攻击特点后，为读者提供了详细的防范方法。

第 4 部分　沙场点秋兵——扫描、嗅探和欺骗防范。通过介绍这些经典的扫描和嗅探工具，让读者了解黑客是如何知道用户计算机中的秘密和漏洞的，同时也教给读者如何利用这些工具，先期发现自己计算机系统的弱点，并对这些弱点给出合理的、有效的补救措施，从而达到防患于未然。

第 5 部分　将防御进行到底——典型网络攻击防范。剖析了网络上流行的攻击方式，并给出了具体的防御手段，如针对 IE 浏览器的恶意攻击与防范，IIS 常见漏洞攻击与防范，恶意网页攻击与防范，IE 浏览器炸弹的攻击与防范，恶意代码的攻击与防范等。

第 6 部分　昨夜雨疏风骤——Windows 系统漏洞防范。介绍了 Windows XP、Windows NT 及 Windows 2003 系统漏洞的形成原理，并剖析了黑客是如何利用这些漏洞进行攻击的，从而提出具体的补救措施和防范技术。

第 7 部分　从入门到精通——注册表常用操作。对注册表进行了详细的介绍，讲述了如何打开、编辑注册表，如何设置注册表权限，如何备份、恢复注册表及制作安装启动盘，以便从注册表层次防范黑客的攻击。

第 8 部分　决胜于千里之外——远程协助和监控。介绍了远程协助和监控软件的使用，在远

程协助方面，讲述了怎样使用远程唤醒软件，怎样实现远程控制，以便在远程为计算机增加一道防护墙。

第 9 部分　自力更生，丰衣足食——编程防范黑客。通过分析黑客攻击的特点和手段，教给读者用编程语言从技术源头防范黑客，如编程获得 IP 地址、制作端口扫描器、制作密码查看器等。

第 10 部分　谁动了我的保险箱——加密和解密。介绍加密技术的定义、功能，并且通过实例详细介绍了多种加密的方法，如用 Easycode 加密和解密文本及可执行文件，设置 BIOS 密码等。

第 11 部分　手奋三尺剑，西灭黑道客——远离黑客。介绍了多种经典的防毒、杀毒工具，如 360 安全卫士、天网防火墙和卡巴斯基等，读者通过学习这些工具的使用介绍，可以方便地选择合适的防毒、杀毒软件。

本书主要考虑初学者的实际需求，结合实例，采用图解的方式，详细讲解防范黑客的案例。读者通过本书的学习，可以一目了然地掌握黑客攻防技术。另外，书中许多典型的防范技术对于中高级读者来说也可以有选择性地学习和参考。

本书由陈芳、秦连清和肖霞主编，在编写过程中，温才燚、张博、范洪斌、裴要强、王洪、管西京、夏添、柯华坤、王大平、林丁报、张英男、张鹏、刘冉、李新峰、李金涛、李连闯、李绍文等提供了很大帮助，在此表示感谢。

作者在写作中力求精确、时效。但由于时间仓促，加之作者水平有限，疏漏之处在所难免，望广大读者多提宝贵意见。联系邮箱为 zhangtao@ptpress.com.cn。

编　者

目录

第1部分 千里之行，始于足下——黑客入门

学习目标

随着互联网的发展和普及，它对人们的生活影响越来越大，无论个人用户及单位等都有自己保密的数据存在计算机上。但由于黑客的出现，网络安全问题也随之凸现。网络用户很少没有遭到攻击的，那么这些攻击者，也就是黑客采用什么手段和技术呢？本章将揭开他们的神秘面纱，并对与他们有关的知识进行介绍。

第1招 认识黑客

黑客是英文“Hacker”的音译，原指热心于计算机技术，水平高超的计算机专家，尤其是指程序设计人员。

在20世纪60年代，计算机系统非常昂贵，只存在于各大院校与科研机构中，技术人员使用一次计算机，需要很复杂的手续，并且计算机的效率也不高。为了绕过限制，最大限度地利用这些昂贵的计算机。最初的程序员们就写出了一些简洁而有效的程序，这些程序往往较原有的程序系统更完善，而这种行为便被称为 Hack。在早期的美国麻省理工学院中，“Hacker”有“恶作剧”的意思，尤其指那些手法巧妙、技术高明的恶作剧。由此可见，在早期，黑客这个称谓并无贬义。

黑客、骇客的区别

骇客是“Cracker”的音译，就是“破坏者”的意思。主要是指侵入他人计算机系统窃取资料或进行破坏的人。

正是因为“骇客”的存在，一些纯正的黑客精神才愈来愈被人曲解，但在真正黑客眼中，“骇客”与“黑客”是如此的泾渭分明，不可混淆。有些黑客们说：在黑客世界中，斗争只存在于“黑客”和“骇客”之间。

怎样才算是黑客

黑客不是自己感觉自己水平高就成为黑客了，这样会遭到真正的黑客的嘲笑，只有得到其他黑客的认同，才能算是真正的黑客。

其次，黑客应该具有一定的创造力，仅仅是拿着黑客前辈们所编写的黑客软件到处使用，

而出现问题却又束手无策的人，是不可能被称为黑客的。

最后，黑客应该具有黑客的精神以及黑客的行为，要能融入黑客们自然形成的黑客文化当中去。

总的来说，技能是黑客必备的能力，要成为一名黑客必须是技术上的行家，并且热衷于解决问题，并能无偿地帮助他人。

黑客行为

真正的黑客是有所为有所不为的，他们一般遵循如下的准则。

（1）不随意攻击用户计算机和网站。虽然黑客们随时在查找系统漏洞并准备入侵，但往往都会尽量避免造成损失，并善意地提醒管理者及时弥补漏洞。

（2）尽量多地编写一些免费软件，并且这些软件的源代码都是公开的。

（3）义务做一些力所能及的事，维护管理相关的黑客论坛、新闻讨论组及软件供应站台。花大量的精力来义务整理、编写黑客教程。

（4）不轻易将入侵过的网站或计算机告诉不信任的朋友。

（5）不在 BBS 上谈论 Hack 的任何事情。

（6）不将已破解的账号和密码告诉任何人。

第 2 招　攻击流程剖析

黑客进行攻击时，一般都遵循如下的攻击流程。

1．保护隐藏自己

黑客攻击之前都会利用别人的计算机来隐藏自己真实的 IP 地址等信息，达到隐藏保护自己的目的。

2．确认目标主机

黑客在发起攻击之前，首先要选择攻击目标，在 Internet 上 IP 地址是真正标识主机的地址，一般通过 IP 地址寻找目标主机。也可以通过大量收集网上计算机的信息，然后根据各台主机安全性强弱来确定最后的攻击目标。

3．分析目标主机

仅知道目标主机的位置是远远不够的，此时还需要了解主机的操作系统类型、提供的服务等信息。黑客一般都通过使用扫描器工具，了解目标主机运行的信息，例如，使用何种版本的操作系统，系统的用户账户以及 FTP、SMTP 等服务器程序的版本等信息，为入侵打好基础。

4．破解账户和密码

拥有攻击目标主机的账户和密码是攻击的前提，否则就谈不上入侵了。此时就需要攻击者首先设法盗窃账户信息，获取账户和密码，登录目标主机。

5．获取控制权

攻击者可以使用 FTP、Telnet 等工具进入目标主机系统，获得控制权。登录后先要清除记录并留下后门，然后更改系统设置，并在系统中植入木马或远程操作程序，方便日后再次

入侵系统。攻击时一般使用 rep 发送文件，可以避免留下 FTP 记录。最后利用清除日志、删除复制文件等方法隐藏踪迹。

6．**实现目的**

获取控制权后，就可以实现攻击的目的。例如，信用卡、游戏账户等密码的窃取。

第3招　认识木马

木马是一种基于远程控制的黑客工具，具有隐蔽性和非授权性的特点。隐蔽性是指木马设计者为了防止木马被发现，会采用各种手段隐藏木马，这样即使服务端发现感染了木马，由于不能确定其具体位置，往往没办法消除它；非授权性是指一旦控制端与服务端连接后，控制端将享有服务端的大部分操作权限，包括修改文件和注册表、控制鼠标和键盘等，并且这些权力并不是服务端赋予的，而是通过木马程序窃取的。

木马程序一般由两部分组成，服务端（Server）程序和客户端（Client）程序。其中服务端程序安装在被控制计算机上，客户端程序安装在控制计算机上，当服务端程序和客户端程序建立连接后，即可实现对远程计算机的控制。

服务端程序可以获得计算机的操作权限。当服务端和客户端机器都连入网络时，客户端程序可以与服务端程序直接建立联系，可以向服务端程序发送各种权限范围内的操作请求，并由服务端完成这些操作，从而实现对服务端计算机的控制。

木马特征

木马的种类数以万计，这些木马程序使用不同的程序设计语言进行编制，在相同的运行环境下运行，虽然发挥着不同的作用，但它们还是拥有许多共同的特征。

（1）隐蔽性。隐蔽性是木马的首要特征。在运行木马软件的服务端程序时，需要使用各种手段隐藏自己，例如常见的修改注册表文件，以便在下次机器启动时可以自行加载木马程序，并且在使用任务管理器检查时，是看不见木马进程的。

（2）功能特殊性。木马拥有特殊的功能，例如搜索目标计算机的密码、设置密码、通过扫描发现已中木马病毒的机器、远程注册表操作等功能。

（3）开机自动运行性。通过修改目标计算机中系统配置文件或注册表文件的方式，实现计算机系统启动时自动运行木马程序。

（4）欺骗性。由于杀毒软件越来越多，及其精确的杀毒效果，木马程序十分容易被查杀。所以，木马程序要达到长期隐蔽的目的，黑客在制作木马程序时，制作出百变的木马是必要的。

（5）自动恢复性。现今，木马程序中的功能模块已不再由单一的文件组成，而是具有多重联系和备份，通常一个被查杀，可以通过另外的文件相互恢复。所以，在计算机感染木马病毒时，仅靠删除某个文件进行清除，是不能完全删除木马的。

木马的危害

木马程序的危害性很大，通过木马程序远程用户可以获得服务器端计算机的最高操作权限，然后对目标主机进行任意操作。也就是说，木马可以使用户的计算机中的信息完全暴露在木马客户端用户眼前，成为木马客户端操纵的棋子。

目前情况下出现的木马病毒，一般拥有如下功能。

（1）自动搜索已中木马病毒的计算机。

（2）实现对服务器端计算机的资源管理。例如，复制文件、删除文件、查看文件内容、上传文件及下载文件等操作。

（3）实现对方屏幕的跟踪监视。

（4）控制服务器端的鼠标、键盘，并可以进行各项操作。

（5）监视对方任务且可以终止对方任务。

（6）随意修改注册表。

（7）共享被控制端的硬盘。

（8）实现特定程序的密码盗窃。例如，专门针对游戏的木马程序，用户只有在登录游戏时，此木马才起到相应的作用。

木马分类

一般将木马程序分为如下几类。

（1）远程访问型木马。远程访问型木马是现在最广泛的木马。这类木马有远程控制的功能，使用简单，只需有人运行服务端程序，同时获得他们的 IP 地址，控制者就能任意访问被控制端的计算机。这类木马有著名的 BO（Back Office）、国产的冰河等。

（2）密码发送型木马。此种木马通过找到所有的隐藏秘密，然后在受害者不知道的情况下将密码发送到指定的邮箱。

（3）键盘记录型木马。这类木马只记录受害者的键盘敲击情况，并完整地记录在 LOG 文件中，然后发送到指定的控制者邮箱中。此类木马程序一般随着 Windows 的启动而启动。

（4）毁坏型木马。大部分木马程序只窃取信息，不做破坏性事件，但毁坏型木马却以毁坏并且删除文件为己任。它们可以自动地删除受控制者计算机上所有的.dll、ini 或.exe 文件，甚至远程格式化受害者硬盘。这类木马程序的危害性极大，一旦中招，将带来不可估量的损失。

（5）FTP 型木马。FTP 型木马程序打开被控制计算机的 21 端口（FTP 所使用的默认端口），使任何用户都可以用一个 FTP 客户端程序在不使用密码的情况下连接到受控制端计算机，并且可以进行最高权限的上传和下载，窃取受害者的机密文件。

第 4 招　认识病毒

病毒是依附于程序或文件中的一段计算机代码，它可在计算机之间传播，并且在传播的同时感染计算机，然后损坏软件、硬件或文件等信息。

病毒传播

从实质上来说，病毒是无法传播的，除非打开或运行了受感染的程序。病毒一般通过如下途径进行传播。

（1）光盘。光盘因为容量大，存储了大量的可执行文件，所以有多种的病毒就以光盘为藏身之处。对于只读式光盘，不能进行写操作，因此光盘上的病毒不能清除。

（2）硬盘。由于带病毒的硬盘在本地或移到其他地方使用、维修时，将病毒传播到相应

的计算机中。

（3）BBS。BBS 是由电脑爱好者自发组织的通信站点，用户可以在 BBS 上进行文件交换（包括自由软件、游戏、自编程序等）。由于 BBS 站一般没有严格的安全管理，也没有任何限制，这样就给一些病毒程序编写者提供了传播病毒的场所。

（4）网络。网络已成为人们日常生活的一部分，数据、文件、电子邮件等在各个网络工作站间、传送，这也为病毒提供了新的传播途径。

病毒类型

在恶性程序代码的类别中，计算机病毒具有较大的破坏力，因为它们有复制的能力，从而能够感染更多的系统。计算机病毒一般可以分成下列几类。

（1）引导区计算机病毒。在 20 世纪 90 年代中期，引导区病毒是最为流行的，主要通过软盘在 16 位元磁盘操作系统（DOS）环境下传播。引导区病毒会感染软盘内的引导区，而且也能感染用户硬盘内的主引导区（MBR）。

（2）寄生病毒。寄生病毒，又称文件型计算机病毒，通常感染执行文件（.exe），有时也会感染其他可执行文件，如 dll、scr 等。当执行受感染的文件时，计算机病毒就会发作，并且病毒会从主机复制到其他可执行文件，然后继续执行原有程序，以免被用户发现，例如，熊猫病毒。

（3）综合型计算机病毒。此种类型的病毒具有引导区病毒和文件型病毒的双重特点。

（4）宏病毒。宏病毒是一种寄存在文档或模板宏中的计算机病毒。一旦打开这样的文档，其中的宏就会被执行，于是宏病毒就会被激活，转移到计算机上，并驻留在 Normal 模板上。从此以后，所有自动保存的文档都会感染上这种宏病毒，而且如果其他用户打开了感染病毒的文档，宏病毒又会转移到此用户的计算机上。

（5）其他病毒。随着防范病毒科技不断发展，计算机病毒也在日益更新，计算机病毒编写者会试图研制及传播新的计算机病毒。所以，经常了解病毒的更新是必要的。

第 5 招　缓冲区溢出

缓冲区溢出是指当计算机向缓冲区内填充数据位数时超过了缓冲区本身的容量，溢出的数据覆盖在合法数据上。理想情况下，程序检查数据长度并不允许输入超过缓冲区长度的字符。但是，绝大多数程序都会假设数据长度总是与所分配的存储空间相匹配，这就为缓冲区溢出埋下隐患。

根据被覆盖数据的位置的不同，缓冲区溢出分为静态存储区溢出、栈溢出和堆溢出 3 种。当发生溢出后，进程可能的表现也有如下 3 种。

（1）运行正常。此时，被覆盖的是无用数据，并且没有发生访问违例。

（2）运行出错。包括输出错误和非法操作等。

（3）受到攻击。程序开始执行有害代码，此时，用来覆盖的数据和被覆盖的数据都是攻击者精心设计的。

一般情况下，静态存储区和堆上的缓冲区溢出漏洞不大可能被攻击者利用，而栈上的漏

洞则具有极大的危险性。

当一个超长的数据进入到缓冲区时，超出部分就会被写入其他缓冲区，其他缓冲区存放的可能是数据、下一条指令的指针，或者是其他程序的输出内容，这些内容都被覆盖或者被破坏。由此可见，一小部分数据或者一套指令的溢出就可能造成一个程序或者操作系统的崩溃。

缓冲区溢出之所以泛滥，是由于开放源代码程序的本质决定的。一些编程语言对于缓冲区溢出是具有免疫力的，例如 Perl 能够自动调节字节排列的大小，Ada95 能够检查和阻止缓冲区溢出。但是，被广泛使用的 C 语言却没有建立检测机制。标准 C 语言具有许多复制和添加字符串的函数，这使得标准 C 语言很难进行边界检查。

一般情况下，覆盖其他数据区的数据是没有意义的，最多造成应用程序错误。但是，如果输入的数据是经过黑客精心设计的或者带有病毒，覆盖缓冲区的数据恰恰是黑客或者病毒的入侵程序代码，一旦多余字节被编译执行，黑客或者病毒就有可能为所欲为，获取系统的控制权。

第 6 招　欺骗攻击

欺骗是网络上常见的一种攻击方式，黑客经常利用欺骗获得别人资料，在他人计算机中安置木马、毁坏系统等。例如，常见的木马程序的激活就是依靠将木马程序伪装成一个普通的软件，让别人轻易相信并且运行程序之后完成欺骗目的。

常见的欺骗有如下几种类型。

（1）IP 欺骗攻击。IP 欺骗攻击是通过伪造某台主机的 IP 地址来骗取特殊权限，从而进行攻击的技术。

（2）ARP 欺骗攻击。ARP 欺骗攻击是利用 ARP 协议漏洞，通过伪造 IP 地址和 MAC 地址实现 ARP 欺骗的攻击技术。

（3）DNS 欺骗攻击。攻击者采用种种欺骗手段，使用户查询 DNS 服务器进行域名解析时获得一个错误的地址结果，从而可将用户引导到错误的 Internet 站点，或者发送一个电子邮件到一个未经授权的邮件服务器等，来实现 DNS 欺骗。

（4）源路由欺骗攻击。通过指定路由，以假冒身份与其他主机进行合法通信或发送假报文，使受攻击主机出现错误动作，从而实现源路由欺骗攻击的目的。

（5）Web 欺骗攻击。Web 欺骗攻击就是打断从被攻击者主机到目标服务器之间的正常连接，并建立一条从被攻击者主机到攻击者主机再到目标服务器的连接。

虽然此种攻击并不会直接造成被攻击者主机的软、硬件损坏，但它所带来的危害也是不可小视的。通过夹在被攻击者主机与目标服务器之间的那台攻击者的主机，被攻击者的一切行为都被攻击者一览无余地看到。攻击者可以轻而易举得到被攻击对象输入的用户名、密码等信息资料，而被攻击者对此却全然不知。这也就是 Web 欺骗攻击最危险的地方。

（6）电子邮件欺骗。电子邮件欺骗是在电子邮件中改变名字使之看起来是从被信任的某地或某人发来的。这类欺骗只要用户提高警惕，一般危害性不是太大。