现用现查

红宝书

黑客攻防技术速查

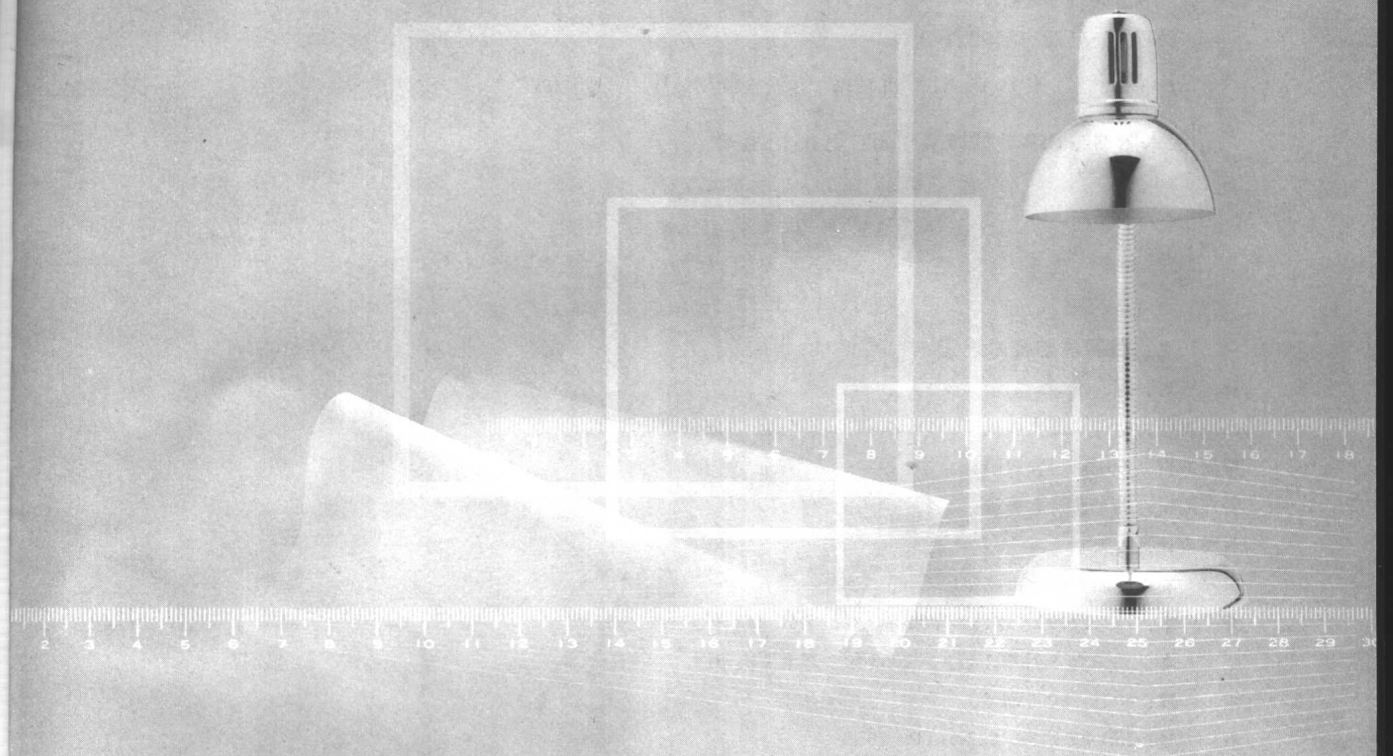
梁上 编著

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

现用现查红宝书

黑客攻防技术速查

梁　上　编著



中国铁道出版社

2003·北京

（京）新登字 063 号

内 容 简 介

本书紧紧围绕黑客的攻与防来介绍，在详细介绍黑客攻击手段的同时，介绍了相应的防范方法，使读者对于攻防技术形成系统的了解，能够更好地防范黑客的攻击。全书共分为 10 章，包括黑客攻防基础知识、Windows NT/2000 攻防技术、QQ 攻防技术、网页攻防技术、电子邮件攻防技术、木马攻防技术、密码破解攻防、病毒防治、防火墙技术等内容。

本书内容丰富，图文并茂，深入浅出，适用于广大网络爱好者，同时可作为一本速查手册，适用于网络安全从业人员及网络管理员。

图书在版编目（CIP）数据

黑客攻防技术速查/梁上编著. —北京：中国铁道出版社，2002.8

（现用现查红宝书）

ISBN 7-113-04822-6

Ⅰ.黑… Ⅱ.梁… 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(2002)第 054879 号

书　　名：黑客攻防技术速查

作　　者：梁　上

出版发行：中国铁道出版社（100054，北京市宣武区右安门西街 8 号）

策划编辑：严晓舟　郭毅鹏

责任编辑：苏　茜　袁秀珍

封面设计：孙天昭

印　　刷：河北省遵化市胶印厂

开　　本：787×1092　1/16　印张：19.25　字数：448 千

版　　本：2002 年 9 月第 1 版　　2003 年 2 月第 2 次印刷

印　　数：6001～9000 册

书　　号：ISBN 7-113-04822-6/TP・755

定　　价：27.00 元

现用现查红宝书系列

编委会

丛 书 序

市面上的电脑图书现在可以用“品种繁多、花样翻新”来形容，很多读者可能会为该购买什么样的书而困惑。很多书总觉得不满意，比如说：有的书的结构不清楚，看起来很费力；有的书自顾自的讲解，往往很需要的知识怎么也找不到（比如说PowerPoint的打包功能），不常用的却讲了一大堆，虽然很深入，但是几乎用不上；而有的书通篇都是工具和菜单的讲解，没有实例作为引导，让读者觉得乏味之极。

读者们（特别是初、中级的电脑用户）到底需要什么样的电脑书籍呢，什么样的书能用最实用的语言、最优惠的价格、最精致的效果来引导读者进入电脑应用的广阔天地呢？什么样的书能够让有一定电脑基础的用户（他们希望在更短的篇幅里容纳更多的内容）也爱不释手呢？这是我们一直在考虑的问题。

为此，我们策划编写了这套“现用现查红宝书”丛书。目的是：希望用户拿到书就能用，翻开来就能查到需要的知识，按照书上的步骤一步步操作就能实现得到想要的效果。希望这套书真正成为实用的作为案头工具的“红宝书”。本丛书的特点总结如下：

（1）知识全面、覆盖面广。尽量争取把常用的东西都讲到。

（2）结构清楚，步骤详细。所有的章节、步骤都尽量细化，目录也做得很详细，让读者可以轻松查阅全书内容。

（3）动手操作，实例引导。用一步步的实际操作来引导读者，让用户在亲自动手的过程中掌握知识。

（4）实惠精致、物有所值。我们竭尽所能把所有的细节做到位：排版更紧凑（绝对没有大片空白或者没有用的图来干扰视线），印刷更精美，格式更细致，定价更合理。

您希望更快的学习电脑知识吗？你需要更轻松的深化电脑应用吗。不要再死啃大块头的艰深知识了，拿起红宝书来，直接用吧！

《现用现查红宝书》编委会

2002年8月

前 言

九十年代初，互联网在全球迅猛发展，为人们提供了极大的方便、自由和无限的财富。同时，互联网也带来了一些负面影响，“信息垃圾”、“邮件炸弹”、“电脑黄毒”、“网上黑客”等越来越威胁到网络的安全。尤其是黑客攻击，随着互联网的普及，已成为威胁网络安全的最大隐患。

本书目的在于让读者了解黑客的攻击手段，使读者在实际应用中碰到黑客攻击的时候，能够做到“心中有数”，更重要的是，希望读者能够运用本书介绍的黑客攻击防守方法去防范黑客的攻击，使自己的网络更加安全。

全书的主线是黑客的“攻与防”，每一章都是围绕“攻与防”来展开叙述的，做到“有攻有防”。第 1 章介绍了黑客攻防的基础知识，从第 2 章到第 6 章，分别针对五个不同攻防技术类别进行了介绍，这五个类别是：Windows NT/2000 攻防技术、QQ 攻防技术、网页攻防技术、电子邮件攻防技术、木马攻防技术。第 7 章介绍其他三种攻防技术，分别是：利用 Unicode 漏洞的攻防技术、局域网数据包拦截攻防技术、网络共享攻防技术。第 8 章介绍了密码破解的手段，以及防范密码破解的措施。第 9 章介绍了病毒的防治，重点介绍了几款常见的杀毒软件。第 10 章介绍了防火墙技术及其常见的防火墙的设置，这对防范黑客和病毒很重要。

本书特别注重实际例子的演示作用，针对每一种攻防手段，都结合实际的例子来进行介绍，希望读者对黑客攻防技术能有更加感性的了解。

本书按照速查手册的格式来编排，便于快速查阅，提高读者的效率。

最后，需要提醒的是：根据国家有关法律规定，任何入侵和窃取他人系统和文件的做法都是违法的，希望读者不要使用本书介绍的黑客技术进行攻击，否则后果自负，切记切记！

编 者

2002.8

目　录

CHAPTER 1

黑客攻防基础知识

- 计算机系统漏洞概述
- 黑客的攻击手段和防御的手段

本章我们讲解黑客攻防的基础知识。

利用已知的程序漏洞进行攻击是黑客最常使用的方法，因此本章对漏洞的性质和分类进行了简要的介绍，并对一些常见的漏洞进行了讲解：

1. 一些著名的漏洞扫描器，并且以 X-Scan 为例介绍了扫描器的使用方法。

2. 黑客的攻击手段，介绍了黑客攻击手段的特点及黑客攻击的一般过程。

3. 防御黑客攻击的方法，介绍了防御黑客攻击手段的常用方法。

1-1 计算机系统漏洞概述

1-1-1 漏洞的性质和分类

网络上每天都有非法的黑客企图进入别人的机器，他们的入侵方式主要有以下几种：

- 利用已知的程序漏洞
- 破解密码
- 监听通讯

其中，利用已知的程序漏洞是入侵者最常用的入侵方法。

网络信息系统由硬件和软件组成，由于软件程序的复杂性和编程的多样性，在网络信息系统的软件中很容易有意或无意地留下一些不易被发现的安全漏洞，软件漏洞显然会影响网络信息的安全保密性，黑客往往是通过这些安全漏洞来侵入和破坏网络信息系统。

漏洞（本文的漏洞主要是指软件漏洞）是指任意地允许非法用户未经授权获得访问或提高其访问权限的硬件或软件特征，漏洞就是某种形式的脆弱性。每个网络系统平台无论是硬件还是软件都存在漏洞。而且，每个缺陷（或大或小）在整个网络系统中都是一个环节，破坏一个环节，攻击者就有希望破坏所有其他的环节，因此网络系统的漏洞具有连锁效应。

在目前经常使用的网络系统中，存在着大量的漏洞，就在2000年内，大约有800多个各种操作系统和应用软件的安全漏洞不断被公开和揭露，比1999年增加了10%左右，并且这个数目呈加速增长的趋势，在2001年，平均每天有4~5个漏洞被公布。

1. 按系统造成的直接威胁分类

漏洞无处不在，按漏洞可能对系统造成的直接威胁来分类，可以分为：

- 远程管理员权限
- 本地管理员权限
- 普通用户访问权限
- 权限提升
- 读取受限文件
- 远程拒绝服务
- 本地拒绝服务
- 远程非授权文件存取
- 口令恢复
- 欺骗
- 服务器信息泄露

2. 按漏洞的成因分类

按漏洞的成因，可以分为：

- 输入验证错误
- 访问验证错误
- 竞争条件
- 意外情况处置错误
- 设计错误
- 配置错误
- 环境错误

3. 漏洞的严重程度

按漏洞的严重程度，可以分为：

- A 类漏洞：威胁性最大的一类漏洞，往往是由于较差的系统管理或错误设置造成的。
- B 类漏洞：较为严重的一类漏洞，如允许本地用户获得增加的和未授权的访问。
- C 类漏洞：严重性不是很大的漏洞，例如允许拒绝服务（D.O.S）的漏洞。

1-1-2 常见十大漏洞

下面介绍的十大漏洞是由 ISS 公司（世界上非常著名的网络安全公司）的安全专家小组 X-Force 总结出来的，是最普遍而且风险最高的漏洞，在目前黑客攻击事件中，80%的手法都出自这十种漏洞。

（1）拒绝服务（Denial Of Service）
（2）脆弱的帐号和密码
（3）数据库
（4）电子商务 web 应用程序
（5）电子邮件系统
（6）文件共享
（7）远程过程调用（RPC）
（8）BIND
（9）Linux 缓存溢出
（10）IIS（Microsoft Internet Information Server）

说明 这些漏洞不是完全孤立的，比如数据库系统也存在拒绝服务攻击。

下面，对上述十大漏洞中的几种漏洞进行一下简要的介绍：

1. 拒绝服务（Denial Of Service）

拒绝服务攻击的英文是 Denial of Service，简称 DoS。这种攻击行动使网络服务器中充斥着大量要求回复的信息，消耗网络带宽或系统资源，导致网络或系统不胜负荷以至于瘫痪而停止提供正常的网络服务。

例如，2000 年 2 月，在三天的时间里，黑客使美国数家顶级互联网站：雅虎、亚马逊、电子港湾、CNN 陷入瘫痪。黑客使用了一种称作“拒绝服务式”的攻击手段，即用大量无用信息阻塞网站的服务器，使其不能提供正常服务。

拒绝服务攻击常常采用分布式的方式进行攻击，图 1-1 是典型的分布式拒绝服务攻击的系统流程图。攻击者控制着几台标为 Handler 的主机作为攻击的发动点，这些 Handler 主机分别控制着大量的代理主机（Agent），这些大量的被控主机才是真正对受害者进行攻击的机器。这种攻击方式使得攻击者可以很容易隐藏自己的真实身份，也可以同样地隐藏了那些 Handler 主机的身份。

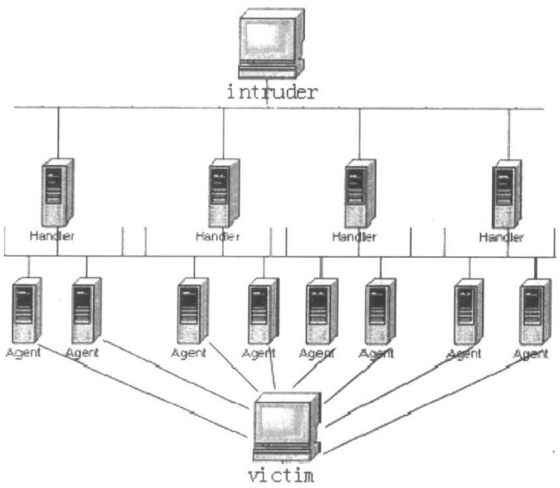


图 1-1 拒绝服务攻击的示意图

2. 脆弱的帐号和密码

- 默认帐号

  许多软件在安装的时候，都会设置一些默认帐号，例如，Windows NT 或者 Windows 2000 安装之后会生成默认的管理员帐号 Administrator，Linux 和 Unix 系统安装之后会生成默认的管理员帐号 root，黑客可以针对这些默认帐号进行攻击。

  所以在安装软件的时候，提倡在安装完成之后，删除默认的帐号，或者把默认的帐号改成其他名字。

- 使用空口令的帐号

  许多软件在安装之后，会生成一些包含空口令的默认帐号，如 Microsoft SQL Server 安装之后会生成默认的数据库管理员帐号 SA，并且该管理员帐号的密码为空。

  由于方便，许多用户也喜欢使用空口令，例如设置 Windows 2000 的 Administrator 帐号的密码为空，这样导致了很大的安全隐患，使得黑客能够轻松地进入系统。

- 密码设置简单

  如果密码的设置过于简单，或者设置得不合理，就很容易被黑客破解，从而获得某些系统的访问权。

3. 电子邮件系统

电子邮件在当今社会中的作用越来越重要，针对电子邮件系统的攻击也越来越多。主要有三种：

- 入侵电子邮箱

  通过破解电子邮箱密码来入侵电子邮箱是最常见的一种电子邮箱入侵方法，包括对 POP3 邮箱和 Web 主页邮箱的入侵，有许多工具可以破解电子邮箱的密码，如 Emailcrack、黑雨——POP3 邮箱密码暴力破解器、流光等。

  另外一种较常见的入侵电子邮箱的方法是利用 Web 主页邮箱的“忘记密码”功能来入侵。使用朔雪 Web 密码探测器可以很好地利用 Web 主页邮箱的“忘记密码”功能来入侵 Web 主页邮箱。

- 使用垃圾邮件攻击

  使用垃圾邮件攻击电子邮箱也是一种比较普遍的攻击方法，发送大量没有用的邮件给某个电子邮箱，会导致电子邮箱被塞满，甚至导致邮件服务器的崩溃，导致用户无法正常地处理电子邮件。

- 利用邮件客户端软件的漏洞进行攻击

  由于邮件客户端软件中存在一些漏洞，所以利用这些漏洞进行攻击也是黑客的常用手段。例如，可以利用 Outlook Express 和 Foxmail 中的漏洞进行攻击。

说明 关于电子邮件系统的漏洞，可参见第 5 章。

4. 文件共享

- NetBIOS

  NetBIOS 文件共享也就是我们平常所说的网上邻居文件共享，因为网上邻居文件共享使用 NetBIOS 协议，所以也被称为 NetBIOS 文件共享。利用 NetBIOS 文件共享，攻击者可以把恶意的攻击程序放入目标主机中，当目标主机的用户不慎运行这个恶意程序的时候，攻击者可以利用这个恶意程序进入目标主机的系统。虽然，NetBIOS 文件共享可以

使用共享密码来保护，但它的密码保护机制是非常脆弱的，使用工具 PQwak 可以轻易地破解共享密码，请参见第 7 章第 3 节。

- NFS

  NFS 是网络文件系统（Network File System）的简称，它是基于网络的分布式文件系统，其文件系统树的各节点可以存在于不同的联网计算机甚至不同的系统平台上，可以用来提供跨平台的信息存储与共享。

  NFS 系统中的漏洞可以使攻击者跨网络进入文件系统。

5. IIS （Internet Information Server）

IIS（Internet Information Server）是微软公司发布的网络服务软件，作为当今流行的 Web 服务器之一，提供了强大的 Internet 和 Intranet 服务功能。可是 IIS 的程序设计有很严重的漏洞，致使安装了 IIS 的 Windows 系统成了黑客攻击的重要目标。

在本书第 7 章第 1 节中介绍了 IIS 的 Unicode 缓冲区溢出漏洞，在这里提供另外的例子。

- PHP3 元字符漏洞

  PHP 是一种 HTML 内嵌式的语言 （类似于 ASP）。而 PHP 独特的语法混合了 C、Java、Perl 以及 PHP 式的新语法。它可以比 CGI 或者 Perl 更快速地执行动态网页。如果 IIS 上使用了 PHP，远程攻击者就可以从 PHP 命令中发送变形字符，从而使 PHP 产生错误处理，实际上也是产生了溢出，使得攻击者可以在服务器中执行任何命令，如图 1-2 所示

说明 溢出和缓冲区溢出都是指软件系统无法处理特定的处理请求时，由于软件系统没有很好地使用错误处理，从而导致软件系统对处理请求丧失控制权，导致用户能够执行超越自己权限的操作。

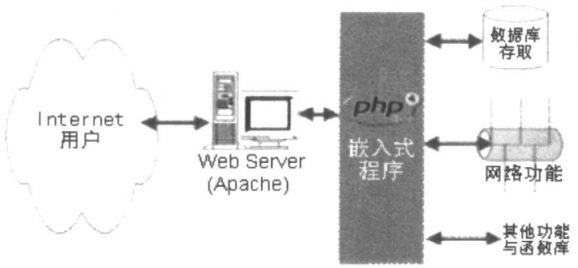


图 1-2 PHP 功能示意图

1-1-3 扫描器和常见的扫描器介绍

在实际的攻击过程中，黑客往往利用一些工具和方法来搜集目标网络或者主机的信息，然后对这些信息进行分析之后，找到攻击的突破口。扫描器（scanner）是黑客最常使用的搜集信息的工具。

扫描器是自动检测远程或本地主机安全性弱点（即漏洞）的程序。一般来说，我们说的扫描器都是指远程扫描器，即检测远程主机安全弱点的扫描器。

常见的扫描器一般是 TCP 端口扫描器，这种扫描器可以连接远程主机的 TCP/IP 端口和服务（比如，Telent 和 FTP），并记录目标主机的应答信息。通过这种方法，可以搜集到关于目标主机的有用信息（比如，一个匿名用户是否可以登录等）。

下面，简单介绍一下当今最流行的扫描器：