计算机教育图书研究室
Computer Education Books
总策划
卓越文化 UNIQUE ZHUOYUE WENHUA

陈彦峰 张长春 主编

- 主要内容
- 黑客攻防基础知识
- IE 攻防技术
- 电子邮件攻防技术
- QQ 攻防技术
- Unicode 漏洞，局域网安全攻防
- 木马攻防技术
- 密码破解攻防
- 病毒防治与防火墙

电脑黑客攻防

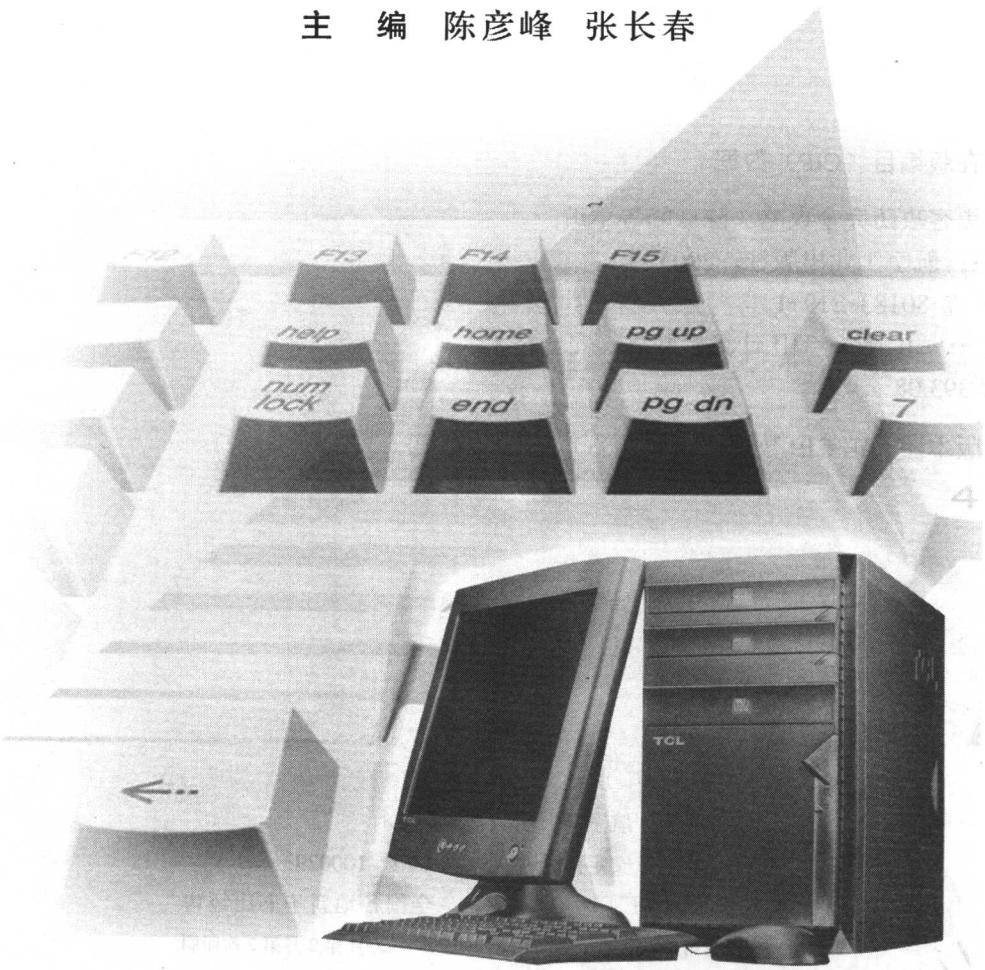
完全谋略

航空工业出版社

电脑黑客攻防完全谋略

计算机教育图书研究室
Computer Education Books
总策划

主　编　陈彦峰　张长春



航空工业出版社

内 容 提 要

本书全面介绍了网络黑客常用的攻击技术、防守技术和防守策略。全书共分为八章，包括黑客攻防基础知识、IE 攻防技术、电子邮件攻防技术、QQ 攻防技术、局域网攻防技术、木马攻防技术、密码破解攻防、病毒防治与防火墙技术等内容。

本书紧紧围绕黑客的攻与防进行讲解，在详细介绍黑客攻击手段的同时，也介绍了相应的防范攻击的方法，使读者对攻防技术有系统的认识。

本书内容丰富，图文并茂，深入浅出，适用于广大电脑和网络爱好者，同时，作为一本速查手册，也可为网络安全从业人员以及网络管理员提供参考信息。

图书在版编目（CIP）数据

电脑黑客攻防完全谋略 / 陈彦峰等主编.
—北京：航空工业出版社，2003.11
ISBN 7-80183-219-1
Ⅰ.电… Ⅱ.陈… 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 083241 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）
北京市燕山印刷厂印刷　　全国各地新华书店经售
2003 年 11 月第 1 版　　2004 年 2 月第 2 次印刷
开本：787×1092　1/16　　印张：22　　字数：356 千字
印数：6001—9000　　定价：28.00 元

前　言

九十年代初，互联网在全球迅猛发展，为人们提供了极大自由和无限的财富，也为全世界范围内人们的交流提供了极大的方便。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”、“电脑黑客”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，它已成为威胁网络安全的最大隐患。

本书旨在使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，能够最大限度地减少损害和损失，更重要的是，希望读者能够运用本书介绍的黑客攻防技术去防范黑客的攻击，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，分别针对五种不同攻防技术分门别类地进行了介绍，这五种类别是：IE 攻防技术、电子邮件攻防技术、QQ 攻防技术、局域网攻防技术和木马攻防技术。第 7 章介绍了密码破解的手段，以及防范密码破解的措施。第 8 章介绍了病毒的防治以及防火墙技术，这对防范黑客和病毒来说非常重要。

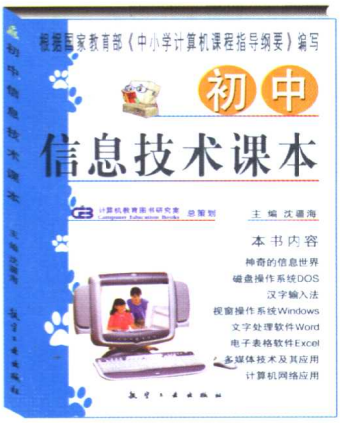
本书特别注重实际例子的演示，针对每一种攻防手段，都结合实际的例子来进行介绍，希望读者对黑客攻防技术能有更加感性的了解。

本书按照速查手册的格式进行编排，便于快速查阅。其内容充实，系统全面地对电脑黑客的攻防技巧进行深入的剖析；语言通俗易懂，简洁明了；结构安排由浅入深，重点突出。既可以作为电脑培训班的计算机安全培训用书，也可作为各级电脑爱好者的随身宝典和参考用书，还可以为网络安全从业人员以及网络管理员提供参考。

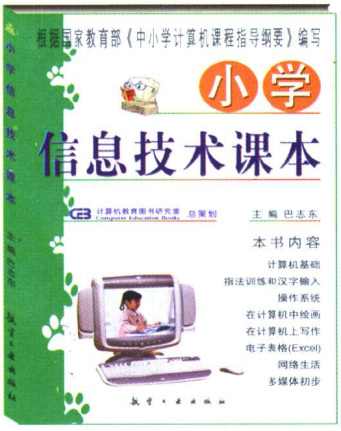
最后需要提醒广大读者的是：根据国家有关法律规定，任何入侵和窃取他人系统和文件的做法都是违法的，希望读者不要使用本书介绍的黑客技术进行攻击，否则后果自负，切记！

编　者

2003 年 9 月

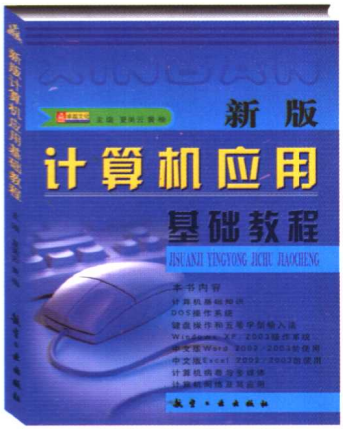


定价:16.00元



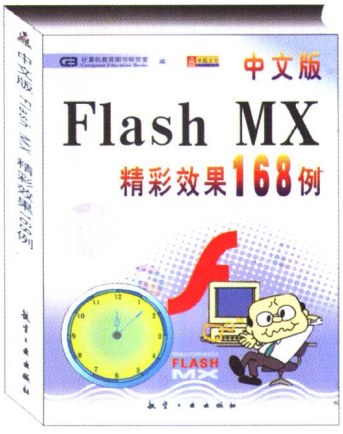
定价: 12.00元

定价: 21.80元

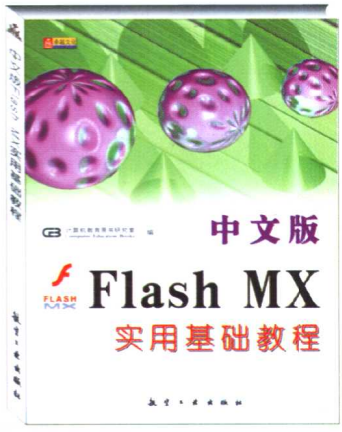


定价: 19.00元

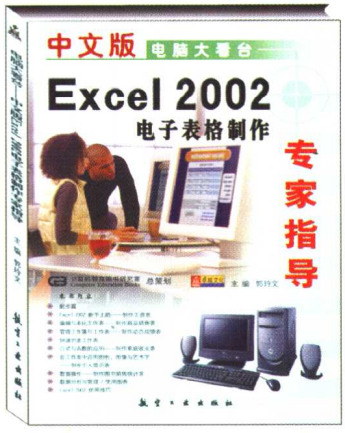
定价: 36.00元



定价: 46.00元



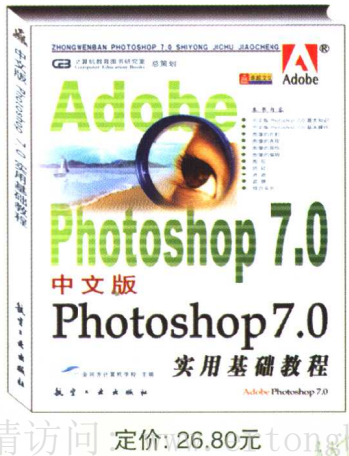
定价: 18.80元



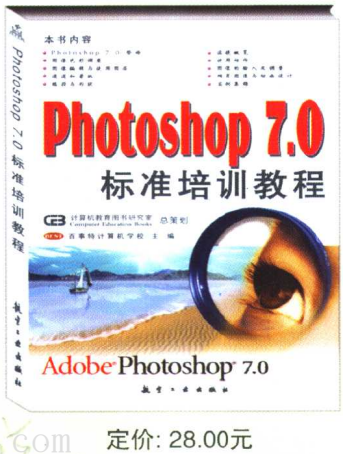
定价:23.80元

定价:15.80元

定价: 19.80元

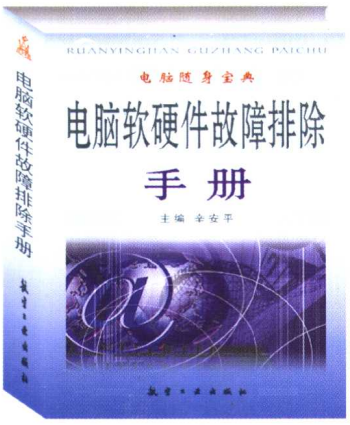


定价: 26.80元

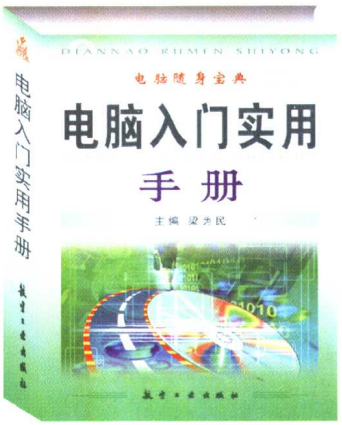


定价: 28.00元

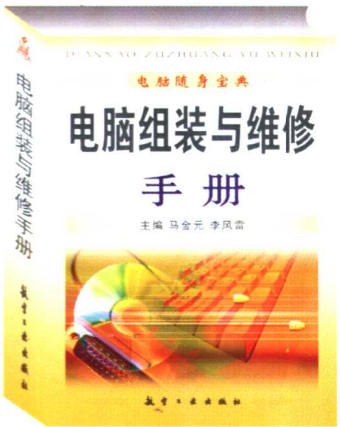
定价: 10.00元



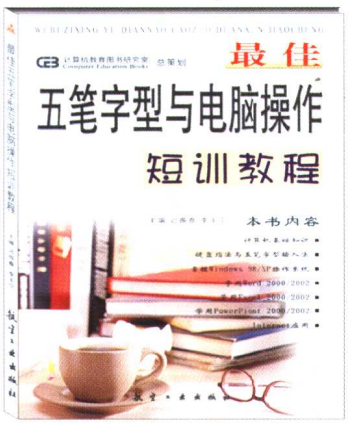
定价: 10.00元



定价: 10.00元



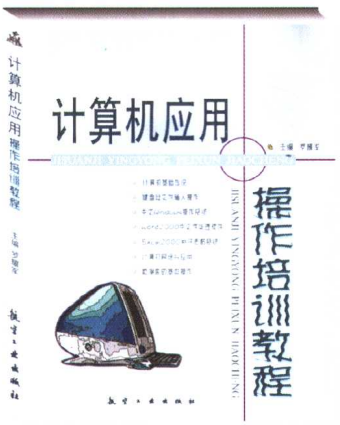
定价: 10.00元



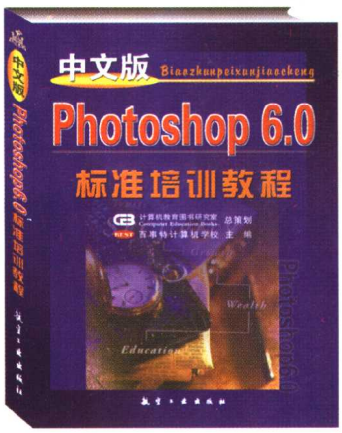
定价: 12.80元

定价: 36.00元

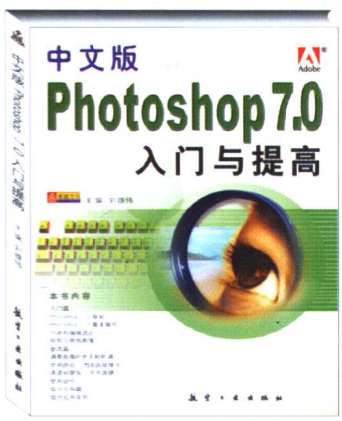
定价:26.00元



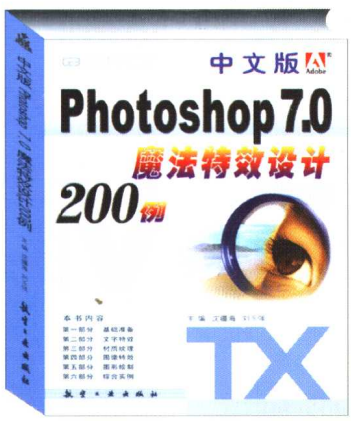
定价: 26.80元



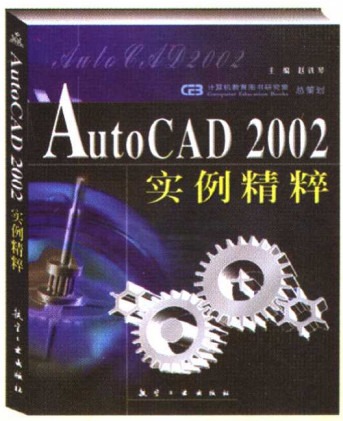
定价: 32.00元



定价: 21.80元



定价: 42.80元



定价: 25.00元

目 录

第1章 黑客攻防基础知识

利用已知的程序漏洞进行攻击是黑客最常用的方法，因此，本章将对漏洞的性质和分类进行简要的介绍，并对一些常见的漏洞进行讲解，让读者对黑客攻防的基础知识有一个初步的了解。

1.1 计算机系统漏洞概述

计算机系统其实并不如大家所想像的那么安全，随着互联网的飞速发展，计算机系统中的漏洞已越来越引起人们的重视，而针对这些漏洞的攻防技术也始终在不断的变化中。

本节将介绍计算机系统的漏洞，通过对漏洞的分析，为后面学习黑客的攻防技术打下坚实的基础。

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入侵别人的机器，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
- 监听通信

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，这些漏洞显然会影响网络信息的安全保密性，黑客往往通过这些安全漏洞来入侵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。每个网络系统平台无论是硬件还是软件都存在漏洞。而且，每个漏洞（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，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。

系统漏洞按照对系统的威胁程度、成因、严重程度可以分为以下几类。

按对系统造成的直接威胁分类

- 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

按漏洞的成因分类

按漏洞的成因来分类，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

按漏洞的严重程度分类

按漏洞的严重程度来分类，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，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。

- 拒绝服务（Denial Of Service）
- 脆弱的账号和密码
- 数据库
- 电子商务 web 应用程序
- 电子邮件系统
- 文件共享
- 远程过程调用（RPC）
- BIND
- Linux 缓存溢出
- IIS（Microsoft Internet Information Server）

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简要地进行一下介绍：

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。黑客使用的就是一种“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，如图 1-1 所示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地隐藏自己的真实身份，同样也可以隐藏那些 Handler 主机的身份。

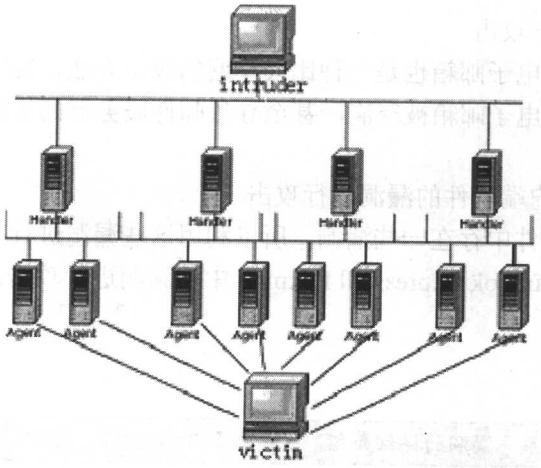


图 1-1　拒绝服务攻击的示意图

脆弱的账号和密码

账号和密码的脆弱性主要表现为以下几种：

（1）默认账号

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

所以建议在软件安装完成之后，删除默认的账号，或者把默认的账号改为其他名字。

（2）使用空口令的账号

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

由于方便，许多用户也喜欢使用空口令，例如，设置 Windows 2000 的 Administrator 账号的密码为空，这样就留下安全隐患，使得黑客能够轻松地进入系统。

（3）密码设置简单

如果设置的密码过于简单，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。

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。主要有以下三种：

（1）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。使用溯雪 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。

（2）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，使用户无法正常地处理电子邮件。

（3）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。

关于电子邮件系统漏洞的详细介绍，可参阅第 3 章。

文件共享

文件共享方面的安全隐患，主要有以下两种：

（1）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时，攻击者就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，详细介绍请参阅第 5 章第 3 节。

（2）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。

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，它提供了强大的 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 系统成为黑客攻击的重要目标。

在本书第 5 章第 1 节中将介绍 IIS 的 Unicode 缓冲区溢出漏洞，这里就不提供另外的例子了。

PHP3 元字符漏洞是又一种漏洞。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，实际上也就是产生了溢出，使得攻击者可以在服务器中执行任何命令，如图 1-2 所示。

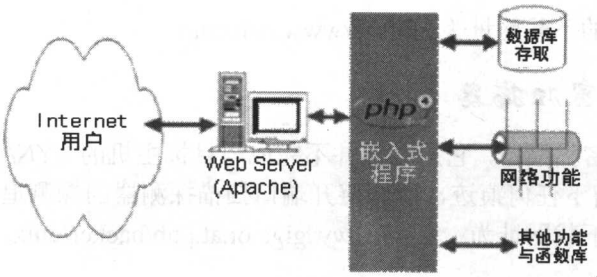


图 1-2　PHP 功能示意图

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，而且由于软件系统又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，使用户能够执行超越自己权限的操作。

1.1.3　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，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。一般情况下我们所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（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（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：

NSS（网络安全扫描器）

它是用 Perl 语言编写的，可执行 Sendmail、匿名 FTP、NFS 出口、TFTP、Hosts.equiv、Xhost 等常规检查。

NSS 扫描器的下载网址为：http://www.giga.or.at/pub/hacker/unix/。

Strobe（超级优化 TCP 端口检测程序）

它是一个 TCP 端口扫描器，可以记录指定机器的所有开放端口，快速识别指定机器上正在运行什么服务，提示什么服务可以被攻击。

Strobe 扫描器的下载网址为：http://sunsite.kth.se/linux/system/network/admin。

SATAN（安全管理员的网络分析工具）

用于扫描远程主机，发现漏洞。包括：FTPD 的漏洞和可写的 FTP 目录、NFS 漏洞、NIS 漏洞、RSH 漏洞、Sendmail、X 服务器漏洞等。

SATAN 扫描器的下载网址为：http://www.fish.com。

Jakal 秘密扫描器

Jakal 是一个秘密扫描器，它启动但并不完成与目标主机的 SYN/ACK 过程，因此可以扫描一个区域而不留下任何痕迹，能够避开端口扫描探测器的探测追踪。

Jakal 扫描器的下载网址为：http://www.giga.or.at.pub/hacker/unix。

IdengTCPScan 扫描器

IdengTCPScan 是一个更加专业化的扫描器，能够识别指定 TCP 端口进程的用户，即能够测出该进程的 UID。

IdengTCPScan 扫描器的下载网址为：http://www.giga.or.at/pub/hacker/unix。

CONNECT 扫描器

CONNECT 是一个 bin/sh 扫描器，用于扫描 TFTP 服务器子网。

CONNECT 扫描器的下载网址为：http://www.giga.or.at/pub/hacker/unix。

FSPScan 扫描器

FSPScan 用于扫描 FSP 服务器。FSP 代表文件服务协议，是非常类似于 FTP 的 Internet 协议，它提供匿名文件传输并具有网络过载保护功能。FSP 协议之所以被认为优于 FTP 协议，是因为它能够记录所有登录用户的主机名。

FSPScan 扫描器的下载网址为：http://www.giga.or.at/pub/hacker/unix。

SAFESuite 扫描器

SAFESuite 扫描器是快速、先进、全面的 UNIX 网络安全扫描器。它可以对指定网络执行各种不同的攻击，探测网络环境中特定的安全漏洞，包括：Sendmail、TFP、NNTP、Telnet、RPC、NFS 等。

SAFESuite 扫描器的下载网址为：http://www.giga.or.at/pub/hacker/unix。

Nessus 扫描器

Nessus 扫描器是一个扩展性很强的扫描器，可以集成新的插件。它可以扫描的安全漏洞包括：拒绝服务漏洞、远程获得超级用户权限漏洞、FTP 漏洞、邮件发送漏洞等。最初，Nessus 只有能应用在 UNIX 和 Linux 平台上的版本，现在 Nessus 也有了 Windows 版本，最新的版本为 WinNessus-1.0.9。

Nessus 扫描器的下载网址为：http://www.nessus.org/。

X-SCAN 扫描器

X-SCAN 扫描内容包括：远程操作系统类型及版本、标准端口状态及端口 BANNER 信息、CGI 漏洞，IIS 漏洞，RPC 漏洞以及 SQL-SERVER、FTP-SERVER、SMTP-SERVER、POP3-SERVER、NT-SERVER 弱口令用户和 NT 服务器 NETBIOS 信息等。

X-SCAN 扫描器的下载网址为：http://www.xfocus.org/programs.php。

1.1.4 X-SCAN 扫描器的使用简介

下面以 X-SCAN 扫描器的 Windows 版本 X-Scan-v1.3 为例，介绍扫描器的使用方法：

（1）从网上下载文件 X-Scan-v1.3.zip，并将其解压缩。

（2）在 xscan 文件夹中双击程序文件 xscan_gui.exe，打开如图 1-3 所示的 X-Scan v1.3GUI 窗口。

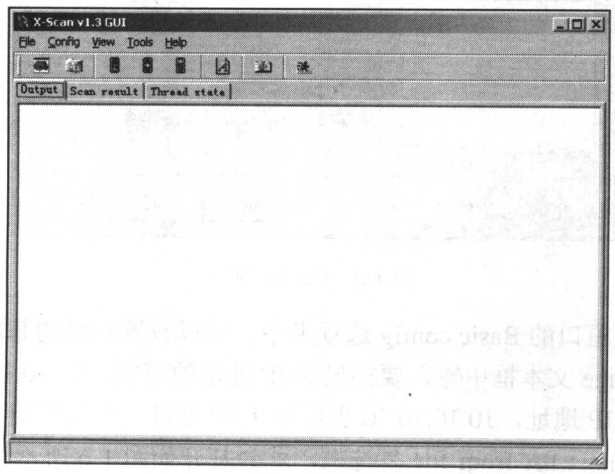


图 1-3 X-Scan v1.3 GUI 窗口