网络安全技术应用丛书

畅销书《杀破狼》作者团队最新力作！

针锋相对

——黑客攻防实战揭秘

武新华　李　防　陈艳艳　等编著

- 安全的测试环境
- 踩点侦查与漏洞扫描
- Windows系统漏洞入侵防御
- 远程攻击与防御
- 常见漏洞扫描工具的使用
- SQL的注入攻击与防御
- 木马和间谍软件攻防实战
- 数据的还原与恢复
- 系统进程与隐藏技术

附赠超值多媒体语音光盘

机械工业出版社
CHINA MACHINE PRESS

网络安全技术应用丛书

针锋相对——黑客攻防实战揭秘

武新华　李 防　陈艳艳　等编著

机械工业出版社

本书紧紧围绕黑客攻防技巧与工具的主题，深入浅出地剖析了用户在进行黑客防御时迫切需要用到的技术，使读者对网络防御技术有个系统了解，能够更好地防范黑客的攻击。

本书共分为 11 章，主要内容包括安全的测试环境、踩点侦察与漏洞扫描、Windows 系统漏洞入侵防御、远程攻击与防御、常见漏洞扫描工具的使用、SQL 的注入攻击与防御、留后门与清脚印技术、木马和间谍软件攻防实战、数据还原与恢复、系统进程与隐藏技术、系统清理与流氓软件清除等。

本书内容丰富、图文并茂、深入浅出，不仅适合作为广大网络爱好者的自学书籍，而且适合作为网络安全从业人员及网络管理员的参考用书。

图书在版编目（CIP）数据

针锋相对——黑客攻防实战揭秘/武新华等编著. —北京：机械工业出版社，2009.7
（网络安全技术应用丛书）
ISBN 978-7-111-27312-7

Ⅰ.针… Ⅱ.武… 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 090687 号

机械工业出版社（北京市百万庄大街 22 号 邮政编码 100037）
策划编辑：丁 诚 吴鸣飞
责任编辑：丁 诚 罗子超
责任印制：邓 博
北京中兴印刷有限公司印刷
2009 年 7 月第 1 版·第 1 次印刷
184mm×260mm · 25.25 印张 · 626 千字
0 001—4 000 册
标准书号：ISBN 978-7-111-27312-7
ISBN 978-7-89451-121-8
定价：51.00 元（含 1CD）

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
销售服务热线电话：（010）68326294 68993821
购书热线电话：（010）88379639 88379641 88379643
编辑热线电话：（010）88379753 88379739
封面无防伪标均为盗版

前　言

神秘的黑客既让人害怕，又让人着迷。在互联网技术飞速普及的今天，多了解一点黑客的入侵伎俩，学一点反黑客技术已成了行走网络江湖必备的防身术。到底黑客世界是怎样的？黑客们通常使用什么技术、哪些工具来攻击目标？更为重要的是，我们应该如何来防范黑客的攻击。

本书作者根据多年的网络防御经验，在系统地总结网络中被广泛使用的入侵、防御技术的基础上，针对广大网管以及对网络爱好者的需求编写了此书。希望能够有助于大家从多个角度了解网络安全技术，从而更有效地保护网络安全。

本书以深入剖析入侵过程为主线，向读者剖析了黑客如何实现信息的搜集；如何通过获取的信息打开目标服务器的切入点（基于身份验证、漏洞、木马的入侵）；如何实现远程连接；入侵后如何执行各种任务；如何留下后门，以便再次进入系统；以及黑客如何清除系统日志防止目标服务器发现入侵痕迹。

此外，书中还详细地介绍入侵者是如何实现从信息扫描到入侵过程中的隐身保护，如何逃避被他人发现。本书对每一个入侵步骤作了详细的分析，以推断入侵者每一个入侵步骤的目的以及所要完成的任务，并对入侵过程中常见的问题作必要的说明与解答。此外，本书还对几种常见的入侵手段进行了比较与分析。

本书主要通过介绍黑客攻击方式和工具，使读者了解黑客入侵的关键技术与方法，进而提高安全防护意识。此外，本书还从黑客入侵防护应用角度给出了相对独立内容的论述，使读者对建构黑客入侵防范体系有一个基本概念和思路，为读者的安全防护系统建设方案提供一些有益的参考和借鉴。

本书的编写具有以下特色：

- 从零起步，通俗易懂，由浅入深地讲解，使初学者和具有一定基础的用户都能逐步提高，快速掌握黑客防范技巧与工具的使用方法。
- 注重实用性，理论和实例相结合，并配以大量插图和配套光盘视频讲解，力图使读者能够融会贯通。
- 介绍大量小技巧和小窍门，提高读者的工作效率，节省宝贵的摸索时间。
- 重点突出、操作简练、内容丰富，同时附有大量的操作实例，读者可以一边学习，一边上机操作，做到即学即用、即用即得，让读者快速掌握。

本书采用通俗易懂的图文解说，易于上手；任务驱动式的黑客软件讲解，揭秘每一种黑客攻击的手法；黑客技术盘点，让您实现“先下手为强”；攻防互参的防御方法，全面确保网络的安全。

参与本书编写的人员有武新华、李防、陈艳艳、李秋菊、张克歌、刘岩、段玲华、杨平等。本书在编写过程中得到了许多热心网友的支持，参考了大量来自网络的资料，并对这些

资料进行了再加工和深化处理，在此对这些资料的原作者表示衷心的感谢。

限于水平，书中的疏漏之处在所难免，欢迎广大读者批评指正。

提醒读者：

根据国家有关法律规定，任何利用黑客技术攻击他人的行为都属于违法行为，希望读者不要使用本书中介绍的黑客技术对他人进行攻击，否则后果自负！

编　者

目　录

第1章

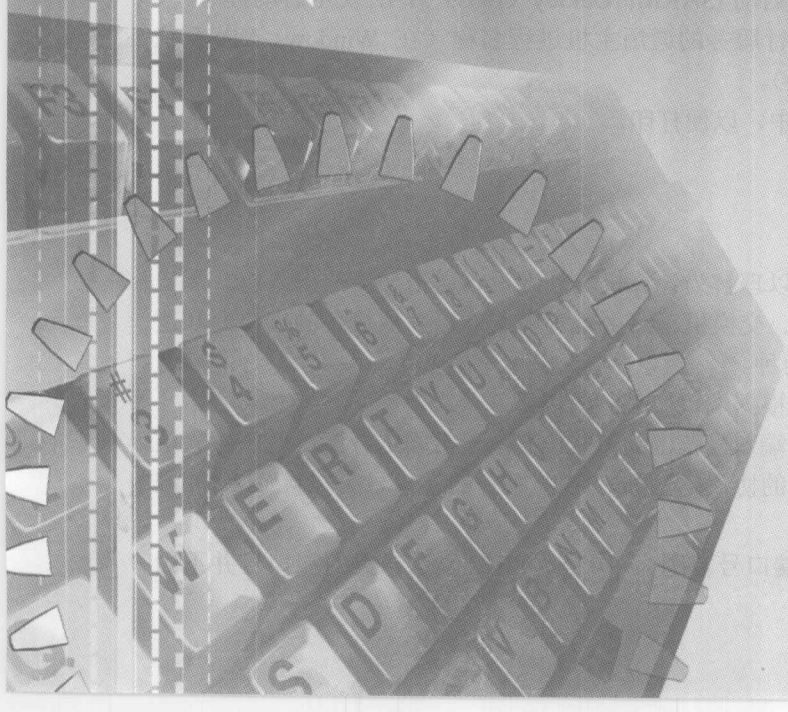
安全的测试环境

本章精粹

本章在介绍黑客攻防基础知识和网络应用技术的基础上，重点讲述创建网络安全测试环境（虚拟机）的相关操作步骤，在虚拟机上架设 IIS 服务器和安装网站及相关组件的方法，为读者演练黑客攻防技术奠定基础。

重点提示

- 黑客攻防基础知识
- 网络应用技术
- 创建安全的测试环境



1.1 黑客攻防基础知识

木马进程、DOS 命令、注册表信息等名词平时我们都有所接触，这些知识可是黑客技术中最基础，也是经常遇到的。只有充分了解黑客、认识黑客，才能真正把黑客引向正途，让黑客技术为社会服务。为什么会受到黑客攻击，遭到黑客入侵后应该采取哪些措施？在网络安全受到极大威胁时，我们该怎么办？

1.1.1 进程、端口和服务概述

进程、端口和服务是黑客经常攻击的对象，它们对网络安全起着非常重要的作用。

1. 进程

在操作系统中，当用户启动一个应用程序，系统便会在后台加载相应的进程。进程是系统或应用程序的一次动态执行活动。进程可以分为系统管理计算机和完成各种操作的必需进程；还有用户开启或执行的其他进程，其中包括用户并不知道但会自动运行的非法进程，这些进程就很有可能是间谍或木马进程。

如何查看自己的进程呢？在系统中，可以同时按下〈Ctrl+Shift+Del〉组合键打开【Windows 任务管理器】窗口（也可以按下〈Ctrl+Shift+Esc〉组合键来实现），在【进程】选项卡下就可以看到当前系统中所有运行的进程，如图 1-1 所示。

下面列出最基本的系统进程，这些进程是操作系统能够正常运行的保障，前提条件是这些系统进程没有被病毒木马伪装。

- smss.exe：会话管理。
- csrss.exe：子系统服务器进程。
- winlogon.exe：管理用户登录。
- service.exe：系统服务进程。
- lsass.exe：管理 IP 安全策略以及启动 ISAKMP/Oakley（IKE）和 IP 安全启动程序。
- svchost.exe：从动态链接库中运行服务的通用主机进程名称（在 Windows XP 系统中，通常有 6 个 svchost.exe 进程）。
- spoolsv.exe：将文件加成到内存中，以便打印。
- explorer.exe：资源管理进程。
- internat.exe：输入法进程。

2. 端口

计算机“端口”的英文为 port，可以理解为计算机与外部设备通信交流的出入口。端口可以分为物理端口（如 ADSL、集线器、交换机、路由器等用于连接其他设备的接口）和逻辑端口（如 TCP 端口、UDP 端口等）两种。

在 Windows 操作系统中，端口可以根据端口号划分为以下 3 类：

- 公认端口（Well-known Ports）：端口号范围为 0～1023，通常固定分配一些服务。这些端口的通信明确表明某些服务的协议。例如，FTP 服务的端口号为 21，HTTP 服务的端口号为 80 等。
- 注册端口（Registered Ports）：端口号范围为 1024～49151。这一类的端口号并不固

定绑定于某个服务，只有运行的程序向系统提出访问请求时，系统才会从这些端口号中随机分配一个供该程序使用。

- 动态端口（Dynamic and/or Private Ports）：端口号范围为 49152～65535。此类端口不为服务分配，通常从 1024 起分配动态端口。动态端口常常被病毒木马所利用，如冰河木马默认的连接端口是 7626。

3. 服务

服务是后台运行的一种应用程序类型。服务应用程序通常可以在本地和网络连接为用户提供特殊功能。也可以说，服务只是为操作系统所调用，并且在后台为系统提供各种功能，再由系统负责将这些功能的操作权交给用户。

在服务器的入侵中，服务也是一个很重要的入口。每项服务在系统中都有一个具体的文件存在，服务对应的这些文件一般存储在“C:\Windows\system32”或“C:\Windows\system32\drivers”文件夹中，文件扩展名为.exe、.dll、.sys 等。

如何查看系统中的服务呢？在【运行】对话框中运行“services.msc”命令，即可打开【服务】窗口，如图 1-2 所示。

图 1-1 【Windows 任务管理器】窗口

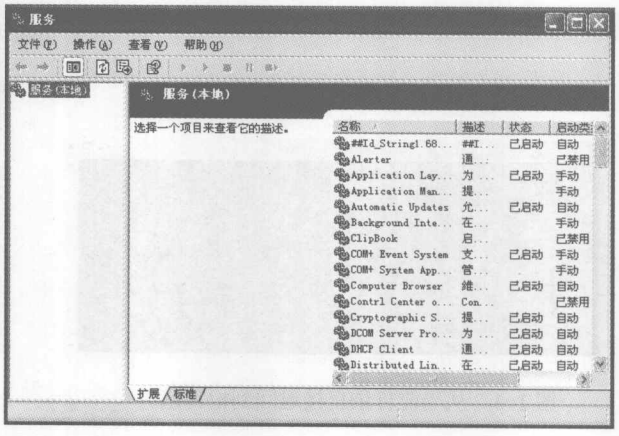


图 1-2 【服务】窗口

1.1.2 DOS 系统的常用命令

虽然现在操作系统的界面越来越人性化，平时的操作基本接触不到 DOS 系统，但 DOS 系统对黑客的入侵有着重要作用。DOS 命令其实是 DOS 系统中提供的运行程序，这些运行程序通过相应的命令运行，来完成各种特定的任务。下面介绍一些 DOS 系统中的常用命令。

1. cd 命令

功能：改变当前路径。

格式：cd [盘符\路径名\子目录]

- 如果省略了 cd 后面的参数，则表示当前目录。

- 使用“cd\”格式，表示直接退回到根目录。
- 使用“cd..”格式，表示退回到上一级目录。

实例：从当前目录直接退回到根目录，输入命令“cd\”，按回车键后显示结果如图 1-3 所示。

2．dir 命令

功能：显示磁盘目录清单。

格式：dir [盘符\路径][/p][/w]

- /p：当目录清单过多，无法在一屏的范围内显示完，屏幕会一直滚动显示，直到该列表最后一行，这样就不容易看到所有列表内容。/p 的作用是能够让目录清单分屏显示，一屏显示 23 行文件信息，然后提示暂停，按任意键继续显示下一屏。
- /w：省略目录清单中文件大小、建立的时间等信息。每行可以显示 5 个文件名。

实例：

1）分屏显示目录清单。输入命令“dir C:\Windows/p”，按回车键后显示结果如图 1-4 所示。

2）省略显示目录清单。输入命令“dir C:\ Inetpub/w”，按回车键后显示结果如图 1-5 所示。

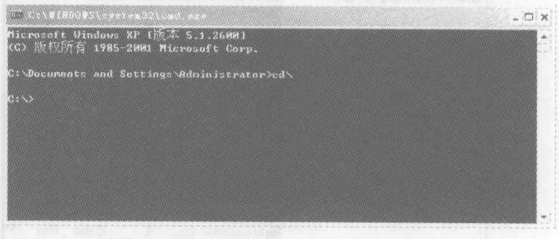


图 1-3　从当前目录直接退回到根目录

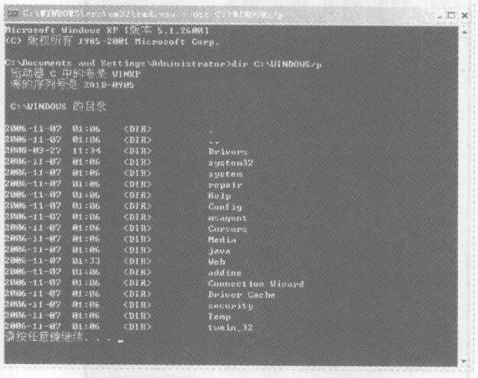


图 1-4　分屏显示目录清单

3．ping 命令

功能：测试计算机名和计算机的 IP 地址。通过回响应答消息的接受情况和往返过程的次数，来检测网络连接性、可达到性和名称解析并显示出来。如果不带参数，ping 命令将显示使用帮助。

格式：ping [-t] [-a] [-n Count] [-l length] [-f] [-i ttl] [-r count] [-s count] [[-j computer-list]|[-k computer-list]] [-w timeout] destination-list

- -t：验证在中断前与指定计算机的连接。按〈Ctrl+Break〉组合键可中断并显示统计信息；按〈Ctrl+C〉组合键可中断并退出 ping 命令。
- -a：对目的地 IP 进行名称解析。
- -n Count：发送回响请求信息的次数，默认值为 4。
- -l length：发送 length 大小的 ECHO 报文。默认值为 64B，最大值为 8192B。
- -f：设置包为“不分段”标志。该包通过路由时不被分段。

- -i ttl：指定发送回响请求信息 IP 中的 ttl 字段值。默认值为 128，最大值为 255。
- -r count：在“记录路由”字段中记录发出和返回报文的路由。count 最小值为 1，最大值为 9。
- -s count：在“记录路由”字段中记录发出和返回报文的时间。count 最小值为 1，最大值为 4。
- -j computer-list：经过指定计算机列表的路由报文。在经过网关时可能会分隔连续的计算机。最大 IP 地址数为 9。
- -w timeout：指定连接超时时间间隔，单位为 ms（毫秒）。
- destination：指定目的地计算机。

实例：查看与 www.baidu.com 的连接情况。输入命令“ping www.baidu.com”，按回车键后显示结果如图 1-6 所示。

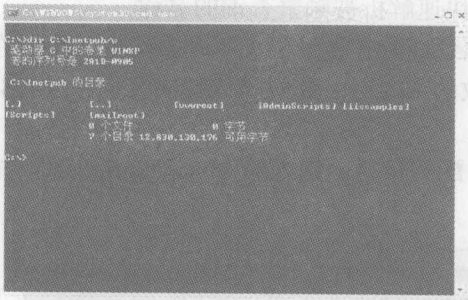


图 1-5 省略显示目录清单

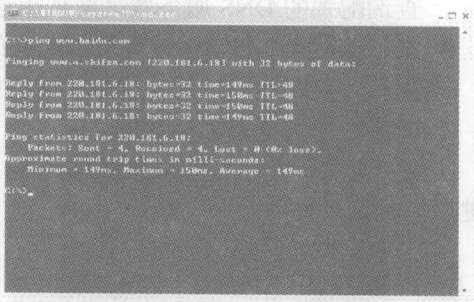


图 1-6 与 www.baidu.com 的连接情况

4. netstat 命令

功能：用于显示活动的 TCP 连接、计算机侦听端口、IP 路由表、IP 统计信息以及以太网统计信息。不带参数的 netstat 命令只显示活动 TCP 连接。

格式：netstat [-a] [-e] [-n] [-o] [-p protocol] [-r] [-s] [Interval]

- -a：显示所有的 TCP 连接，包括正在监听的。
- -e：显示关于以太网的统计信息，包括发送和接收的字节数、数据包数（可与-s 参数结合使用）。
- -n：显示所有已经建立的 TCP 有效连接。
- -o：显示每个有效 TCP 连接的进程 PID（可与-a、-n 和-p 参数结合使用）。
- -p protocol：显示所有由 protocol 指定的协议连接。
- -r：显示 IP 路由列表。
- -s：显示每个协议连接的统计信息。
- Interval：每个 Interval 秒就重新显示一次选定的信息。按〈Ctrl+C〉组合键可停止，如果省略该参数，将只显示一次选定信息。

实例：查看以太网统计信息和所有协议的统计信息。输入命令“netstat -e -s”，按回车键后显示结果如图 1-7 所示。

5. ipconfig 命令

功能：诊断并显示所有 TCP/IP 网络配置值，如 IP 地址、子网掩码及默认网关。没有参