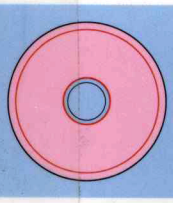
中国科学出版集团
新世纪书局

计算机网络与信息安全教育规划教材
北大方正软件学院名师精心编写的获奖图书

黑客攻防
实战入门与提高

·多媒体案例教学·

主　编：叶　刚　陈文萍
副主编：朱闻闻　刘　生　高　赫



超值多媒体教学光盘

★ 时长超过300分钟的20个实训任务的多媒体语音教学录像
★ 实验环境的搭建说明和所用的软件工具
★ 实验中入侵与防御思路的参考文档
★ 视频由北大方正软件学院名师亲自录制，讲解生动、细致

- **任务驱动教学**
  以项目为导向的学习模式，避开大量理论的学习，以实践为主导，非常适合自学和教学使用
- **25个攻防实训**
  涵盖扫描、嗅探、服务器入侵、脚本入侵、注入攻击等多种黑客攻防手法，可同时获取技术和理论两方面的知识
- **视频与图书互补**
  采用最为通俗易懂的图文解说，并配有多媒体视频讲解，让读者可以轻松上手

科学出版社

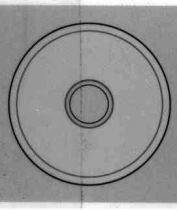
中国科学出版集团
新世纪书局

计算机网络与信息安全教育规划教材
北大方正软件学院名师精心编写的获奖图书

黑客攻防
实战入门与提高

·多媒体案例教学·

主　编：叶　刚　陈文萍
副主编：朱闻闻　刘　生　高　赫



超值多媒体教学光盘

★ 时长超过300分钟的20个实训任务的多媒体语音教学录像
★ 实验环境的搭建说明和所用的软件工具
★ 实验中入侵与防御思路的参考文档
★ 视频由北大方正软件学院名师亲自录制，讲解生动、细致

- **任务驱动教学**
  以项目为导向的学习模式，避开大量理论的学习，以实践为主导，非常适合自学和教学使用
- **25个攻防实训**
  涵盖扫描、嗅探、服务器入侵、脚本入侵、注入攻击等多种黑客攻防手法，可同时获取技术和理论两方面的知识
- **视频与图书互补**
  采用最为通俗易懂的图文解说，并配有多媒体视频讲解，让读者可以轻松上手

科学出版社

内 容 提 要

本书着眼于网络安全工程师岗位，结合网络安全应用和发展现状，以应用为目标，以网络安全技术为主导，以搭建、配置与维护安全网络为主线，按照信息搜集与嗅探、木马的远程控制、经典脚本入侵、木马免杀技术、网络安全测试与安全故障诊断、常见网络安全设备的配置和管理为流程，循序渐进地讲解相应的网络安全实训任务。本书的编写以“提高学生应用能力”为宗旨，按照企业对高校学生的实际需求来设计任务与实验，使学生能够在了解相关理论的基础上，具备相应的实际操作技能。

本书适合作为大中专院校、计算机培训班的实训指导教材，也可作为网络安全技术人员、网络安全爱好者的参考书，还可作为网络安全管理人员的参考手册。

图书在版编目（CIP）数据

黑客攻防实战入门与提高/叶刚，陈文萍主编. —北京：科学出版社，2010

ISBN 978-7-03-029271-1

Ⅰ. ①黑… Ⅱ. ①叶… ②陈… Ⅲ. ①计算机网络—安全技术 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字（2010）第 202492 号

责任编辑：赵东升　何立兵　/　责任校对：杨慧芳

责任印制：新世纪书局　/　封面设计：周智博

科学出版社出版

北京东黄城根北街 16 号

邮政编码：100717

http://www.sciencep.com

中国科学出版集团新世纪书局策划

北京市鑫山源印刷有限公司

中国科学出版集团新世纪书局发行　各地新华书店经销

*

2011 年 1 月 第 一 版　开本：16 开

2011 年 1 月 第一次印刷　印张：18.25

印数：1—3 000　字数：444 000

定价：35.00 元（含 1CD 价格）

（如有印装质量问题，我社负责调换）

前　言　Preface

近几年来，随着网络应用的飞速发展，各种网络攻击事件层出不穷，对网络管理员和网络安全工作者提出了更高的要求。本书从实际应用出发，以任务的形式介绍网络中常见的攻击和防御手段，揭露出网络中广泛存在、却总被忽视的安全漏洞，并结合笔者长期积累的安全防护经验，指出相应的防范要点。

■ 编写原则

本书符合国家高技能人才培养目标和相关网络专业技术领域的岗位要求，对学生职业能力培养和素质的养成具有重要的支撑与促进作用，在编写过程中遵循以下原则。

（1）理论知识以“够用”为前提，培养创新型的应用人才

本书是根据全国高职课程改革的要求而编写的，是信息安全专业课程建设改革的一个全新的思路。本书以培养应用型人才为目标，确保理论知识够用，加大新知识、新技术的介绍，加强实验、实践力度，以培养创新型的应用人才。

（2）注重现代化教育技术在教学中的应用

众多网络专家、教师和职业经理一致认为技术与团队合作精神是新技术人员必备的素质。本书的编写也正是以此为目标，让学员在模拟环境中反复训练，知识与技能并重，职业素质与职业道德并行。

（3）重视应用能力的培养与训练

本书以“任务驱动”的方式来设计实例与实验，使学员在了解理论的基础上，具备相应的操作技能。我们在写作过程中本着“在娱乐中学习，在团队建设中锻炼”的理念，让学员在不同层次与不同阶段的学习中一步步地适应工作，适应企业的就业环境。

■ 内容特色

- **以项目为导向的学习模式：**以项目为导向的学习模式避开了大量理论的学习，以实践为主导，非常适合自学和教学使用。
- **实例丰富：**涵盖扫描、嗅探、服务器入侵、脚本入侵、注入攻击等多种黑客攻防手法，读者可同时获取技术和理论两方面的知识。
- **针对性强：**围绕黑客攻防最新技术，让读者用最短的时间学到最有用的技术。

由于作者水平有限，书中难免存在不足之处，真诚地希望业界同仁和读者朋友们批评指正。

编　者

2010 年 11 月

目 录

Contents

目 录

Contents

目 录

Contents

目 录

Contents

目 录

Contents

任务 1

上兴木马入侵

当计算机用户在互联网上幸福地冲浪时，是否会想到这时可能已有木马悄然入驻你的电脑，然后偷取你电脑上的秘密资料？你用尽了各种方法来阻止病毒的入侵，但是一切都显得徒劳，真正的木马隐秘得很好，是不会被你轻易发现的。

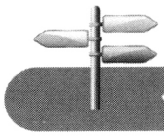
案例

某政府网络包括涉密网、内部网(业务网)、外部网(公开网站)3 个部分。其中，内部网、外部网承载着财政、审计等功能。总的节点有数千个，院内网段有 40 多个。涉密网中存储着政务中的各种机要文件，如全省的核心经济数据、省重要干部信息、中央下发的涉密工作文件等。

出于安全考虑，对该网络中涉密网与内部网和外部网进行了物理隔离。两个网络的数据不能相互通信。且涉密网也与因特网隔离，以确保涉密数据不外泄。

涉密网中的某个职员想在因特网上进行数据查询，考虑到去外部网中查询不太方便，该职员就在涉密网终端上通过连接外部网网线的方式，访问了因特网。该职员在因特网上浏览网页时，访问了某个论坛，而这个论坛被黑客挂上了利用“网页木马生成器”打包进去的灰鸽子变种病毒。黑客利用“自动下载程序技术”在该数据终端上种植了木马。

“灰鸽子”是反弹型木马，能绕过天网等大多数防火墙的拦截，中木马后，一旦电脑连接到 Internet，攻击者就可以完全控制中马后的电脑，可以轻易地复制、删除、上传、下载被控电脑上的文件。机密文件在该涉密网职员毫不知情的情况下被窃取，最终造成了重大泄密事件。



任务学习引导

要点 1 了解远程控制木马的使用

用啊 D 网络工具包扫描有 IPC$弱口令漏洞的机器，用上兴控制软件配置好上兴木马服务端，再使用啊 D 网络工具包对目标主机远程种植上兴木马，最终完全控制目标计算机。

要点 2 懂得木马的运行模式对安全防护的意义

种植木马是黑客攻击的普遍方法，常见的有：网页挂马、E-mail 传递、利用 IPC$弱口令漏洞直接对目标主机种植木马等方式。通过本任务的木马入侵实验，可加深对木马危害的了解，加强网络安全防范意识，保护计算机的数据安全。

要点 3 什么是远程控制木马

远程控制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。隐蔽性是指木马的设计者为了防止木马被发现，会采用多种手段隐藏木马，这样服务端即使发现感染了木马，由于不能确定其具体位置，往往只能望“马”兴叹。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、修改注册表、控制鼠标、控制键盘等，这些权限并不是服务端赋予的，而是通过木马程序窃取的。

用木马进行网络入侵，从过程上看大致可分为以下 6 步。

1. 配置木马

一般来说，每个设计成熟的木马都有木马配置程序，以实现以下两个功能。

① 木马伪装：木马配置程序为了在服务端尽可能好地隐藏木马，会采用多种伪装手段，如修改图标、捆绑文件、定制端口、自我销毁等。

② 信息反馈：木马配置程序对信息反馈的方式和地址进行设置。

2. 伪装木马

木马的伪装方式主要有以下 6 种。

（1）修改图标

现在，已经有木马可以将木马服务端程序的图标改成 HTML、TXT、ZIP 等文件的图标，这具有相当大的迷惑性。

（2）捆绑文件

这种伪装手段是将木马捆绑到一个安装程序上，当安装程序运行时，木马在用户毫无察觉的情况下，偷偷地入驻系统。至于被捆绑的文件，一般是可执行文件（即 EXE、COM 一类的文件）。

（3）出错显示

当服务端用户打开木马程序时，为了迷惑用户，木马程序会弹出一个错误提示框。错误内容大多会定制成诸如“文件已破坏，无法打开！”之类的信息，如果服务端用户信以为真，木马会悄悄入驻系统。

（4）定制端口

很多老式木马的端口都是固定的，这给判断是否感染了木马带来了方便，只要查一下特定的端口就知道感染了什么木马，所以现在很多新式木马都加入了定制端口的功能，控制端用户可以在 1024～65535 之间任选一个端口作为木马端口（一般不选 1024 以下的端口），这样就给判断木马的类型带来了麻烦。

（5）自我销毁

木马的自我销毁功能是指安装完木马后，原木马文件将自动销毁。这样服务端用户就很难找到木马的来源，在没有查杀木马工具的帮助下很难删除木马。

（6）木马更名

现在有很多木马都允许控制端用户自由定制安装后的木马文件名，这样很难根据文件名来判断所感染的木马类型。

3．传播木马

木马的传播方式主要有两种：一种是通过 E-mail，另一种是软件下载。

4．运行木马

服务端用户运行木马或捆绑木马的程序后，木马就会自动进行安装。首先将自身复制到 Windows 的系统文件夹中（一般在 C：\WINDOWS 或 C：\WINDOWS\SYSTEM 目录下），然后在注册表、启动组、非启动组中设置好木马的触发条件，这样木马安装就完成了。安装后木马即被激活。

木马被激活后，进入内存，并开启事先定义的木马端口，准备与控制端建立连接。这时服务端用户可以在 MS-DOS 方式下，输入 NETSTAT -AN 命令查看端口状态。一般个人电脑在脱机状态下是不会有端口开放的，如果有端口开放，就要注意是否感染了木马，尤其是数值比较大的端口。如果木马有定制端口的功能，那么任何端口都可能是木马端口。

5．建立连接

控制端可以通过木马端口与服务端建立连接。

6．远程控制

连接建立后，控制端对服务端能进行如下操作。