黑客攻防实例入门

王 洁　高 山　石 云　主编

科 学 出 版 社

北京科海电子出版社

内 容 简 介

本书是为了广放大读者了解黑客的攻击手法及其如何来进行相应的防范而编写的，实用性强。全书共分为 11 章，通过在虚拟实验环境中进行技能训练的方式，详细讲解了黑客实验环境（黑客训练营）的打造、剖析了针对漏洞/木马/即时通信软件（QQ/MSN）/电子邮箱的攻击手法进行演示揭密，并指出相应的防范措施。本书对时下流行的论坛/文章系统/博客系统攻击、Cookie 欺骗、跨站攻击、注入攻击实例进行了实例讲解，还通过病毒的攻击与防范、电脑/软件加密解密、远程溢出攻击实例讲解了电脑/服务器安全防护。

随书所带光盘讲解了 80 多个攻防实例的过程，作为本书内容的补充，光盘包括书中较为重要的实例，以及时下流行的黑客入侵过程，物超所值。

本书适用于对网络安全及黑客攻防感兴趣的读者。

图书在版编目（CIP）数据

黑客攻防实例入门/王洁，高山，石云编著.
—北京：科学出版社，2006
ISBN 7-03-017158-6

I. 黑… II. ①王… ②高… ③石… 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（2006）第 040059 号

责任编辑：俞凌娣 / 责任校对：科 海
责任印刷：科 海 / 封面设计：王楠楠

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

北京市耀华印刷有限公司印刷

科学出版社发行 各地新华书店经销

*

2006 年 5 月第一版 开本：16 开
2006 年 5 月第一次印刷 印张：20.25
印数：0001-4000 字数：492 千字

定价：32.00 元

（如有印装质量问题，我社负责调换）

『前言』

网络诡异，十几年便造就了一个虚拟的世界。在 Internet 高速发展的今天，网络作为一种重要的信息传递手段，对于经济的发展和人们之间的交流起着越来越重要作用。但在它带来无数商机的同时，也带来了许多网络安全问题。随着网络技术的发展，黑客的攻击手法已经超过计算机病毒的种类，总数达近千种，电脑与网络最大的威胁就是“安全”。在网络上的大多数人都或多或少地知道计算机安全的概念，哪怕是没有接触过计算机的人也能够通过电视、报纸等媒体知道诸如黑客、病毒，木马之类的名词。虽然其中大多数人可能不曾被病毒感染过，也可能他们的计算机资料被没有被窃取过，但是所有利用互联网进行工作、生活、学习的人群都会担忧网络的安全问题。

为了让读者对黑客攻防手段、系统漏洞攻防分析以及加密解密等各类黑客攻防手段有详细的了解，提高广大网络爱好者的安全防范意识，排除电脑与网络的安全隐患，以及为了满足众多电脑爱好者对网络安全整体防范的强烈需求，我们特此推出此书，希望能够通过这本书使得广大读者了解黑客的攻击手法以及如何来进行相应的防范，为大家打造一个安全放心的网络环境。

关于本书

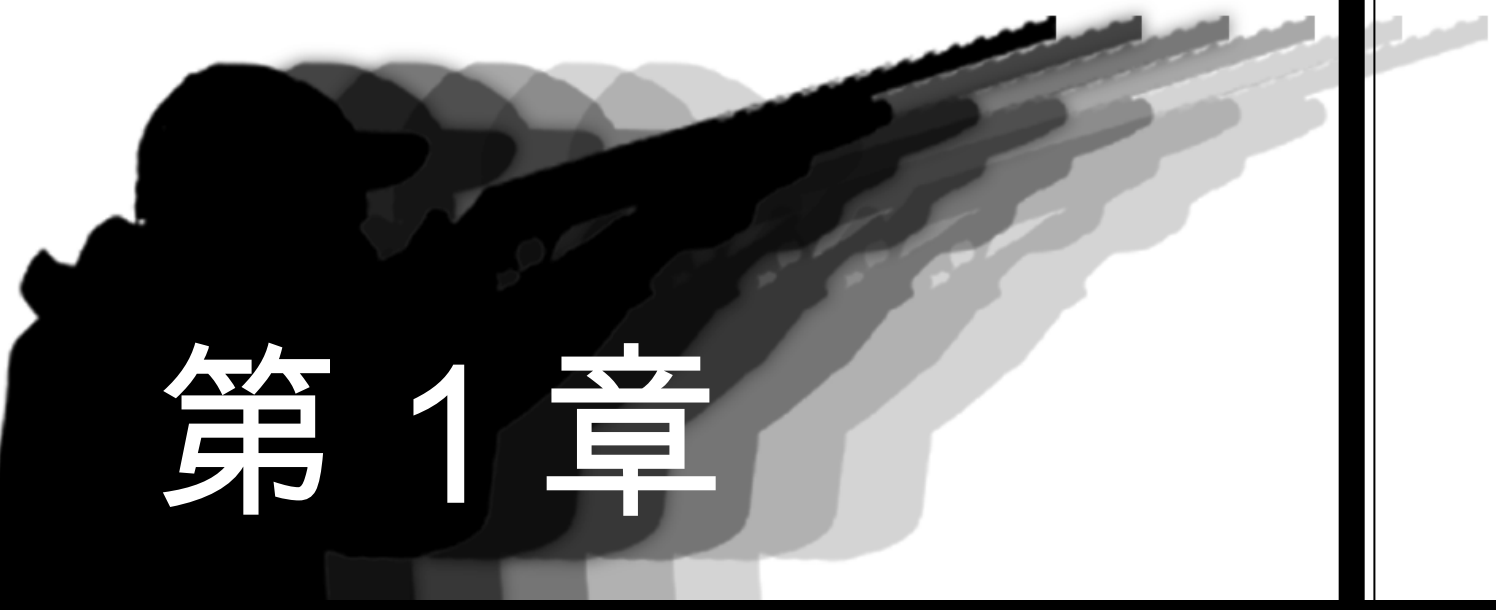
随着 IT 技术与网络经济的快速发展，网络已经成为一种重要的信息沟通手段，对于人们的生活交流与商业经济的发展起着重要的作用。随着近年来网络的深入民心，不但许多商家企业公司有了门户网站，利用网络与全世界沟通，就连普通的市民们也是几乎都拥有了电脑，上了互联网。然而就在我们这些互联网用户利用网络来学习、生活、工作，商家企业用来沟通、运作、盈利时，越来越多的不安全因素在网络中时隐时现。世界经济的发展迫切需要一批有知识头脑与技术功底的网络安全人材能跟上时代的潮流，而且如何提高网络安全防范水平，了解各种入侵手法及思维、防止网络遭到黑客的攻击、保障公司、企业、家庭网络电脑的安全已经成为了急需解决的问题，这时就迫切需要一本揭露与讲解黑客入侵与网络安全的实例图书出现，本书正是针对每个电脑爱好者的学习欲望与网络需要而撰写的。

为了提高国民网络技术素质，加强安全意识，指导各类安全爱好者的真正的实战学习，我们精心推出《黑客攻防实例入门》一书。此书定位在初中级读者，特别针对各类黑客攻击手法与防范方法进行了细致的讲解。与别的黑客实例性图书不同的地方，本书不但以文图方式详细的讲解了实例过程，而且光盘中配以录像实例动画教学，包含各种各样的漏洞入侵事例、密码攻防操作、常见木马的攻防技术、即时通讯软件（QQ、MSN）的攻击防御、邮箱（邮箱软件）的攻防、数据库入侵攻击与防范、加密解密原理及实例、电脑/服务器安全防范应用，并特别对从来不曾公布的“黑客入侵实例”进行了详细讲解。

从本书中可以学到什么?

- 黑客实验环境（黑客训练营）的打造（虚拟机软件的安装、虚拟系统的安装与配置、虚拟机网站中论坛、网站及实验环境的打造）
- 漏洞的攻击与防范（Windows NT/2000/XP/2003 漏洞攻防、Linux 平台与 Windows 的相互入侵攻击实例、系统安全防范手段）
- 木马的植入攻击与防范（木马介绍/伪装/加壳、木马攻击实例太清除防范）
- 即时通讯软件的攻击与防范（QQ/MSN/Yahoo Messenger/UC 攻防）
- 电子邮箱的攻击与防范（邮件炸弹/附件攻击、Web 邮箱攻防、邮件软件攻防）
- 网络游戏攻击与防范（私服入侵手法剖析、网游木马的查找/清除/防范）
- 网站破解与脚本攻击（论坛/文章系统/博客系统攻击、COOKIE 欺骗、跨站攻击、注入攻击实例剖析）
- 病毒的攻击与防范（常见病毒攻击、杀毒软件/防火墙的介绍与实例应用）
- 电脑/软件加密解密（系统密码、办公密码、软件解密、各类加密方法）
- 远程溢出攻击实例（流行溢出实例、操作系统溢出实例、娱乐软件溢出实例）
- 电脑./服务器安全防护（帐号、服务、权限、软件防护）

目　录



第 1 章

打造黑客训练营

本章要点：

- 虚拟机简介及相关的软硬件环境
- 攻防测试平台的建立与安装
- 虚拟网络环境的测试
- 网络环境IIS的安装以及ASP平台的搭建（论坛、相关组件、插件、网站功能模块）

——

IIS

/

1.1 合法的黑客训练营——虚拟机

1.1.1 虚拟机简介

Windows Linux Linux

提示：虚拟机软件可以在一台计算机上模拟出来若干台PC，每台PC可以运行单独操作系统而互不干扰，实现一台计算机“同时”运行几个操作系统，还可以将这几个操作系统连成一个网络。

Virtual PC VMware

1.1.2 VMware打造黑客训练营

VMWARE VMware

VMware

“ ”

CMOS

VMware

1．系统需求

1

VMware Workstation 4.0 Windows XP Professional Windows XP Home Edition Windows 2000 Professional Server Advanced Server Windows NT Workstation Windows NT Server SP3 SP3

VMware Workstation 4.0 Microsoft Windows MS-DOS 6.0 Linux Red Hat 6.2 Caldera OpenLinux 2.X FreeBSD 2.2.X

2

266MHz 400MHz

128MB 256MB

20MB 500MB

2．VMware 软件的安装

VMware

.

. VMware Windows 2000

“ ”

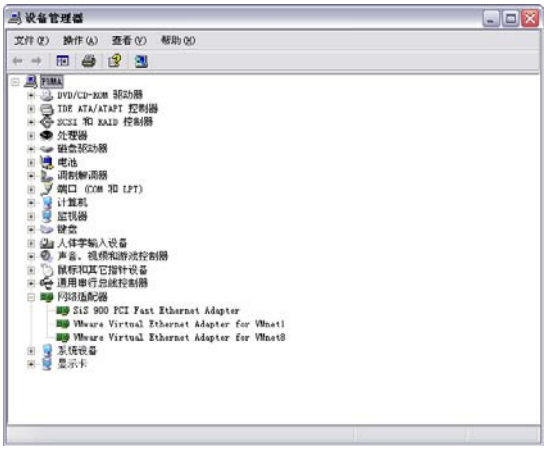
VMware

“ VMware Virtual Ethernet Adapter for VMnet1 ” “ VMware Virtual Ethernet Adapter for VMnet8 ” VMware VMware

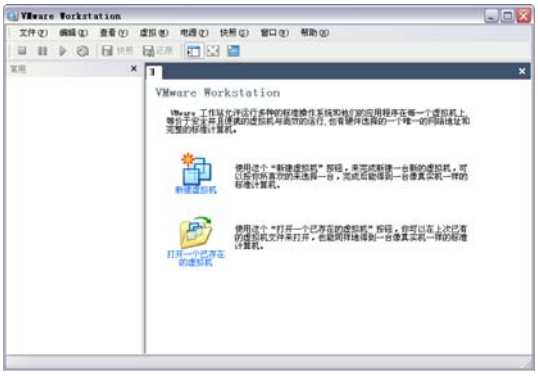
1-1

3．创建一个虚拟机

1 VMware VMware 1-2



1-1



1-2 VMware

2 “ ” → “ ” “ ”
“ ” 1-3

. “ ” “ ” ____

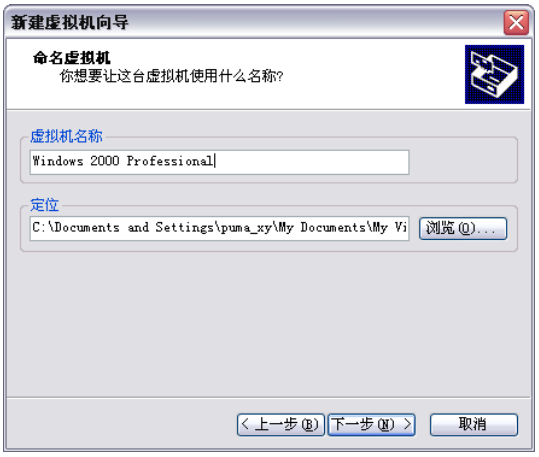
. “ ” “ ”
“ ”

3 “ ”
Windows 2000 Microsoft Windows Windows
2000 Professional 1-4

1-3

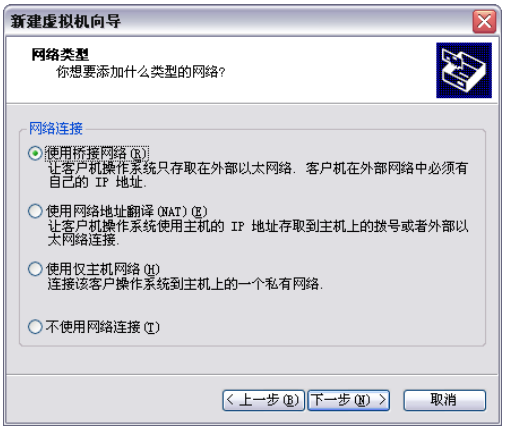
1-4 Windows 2000 Professional

4 “ ”
“ ” 1-5

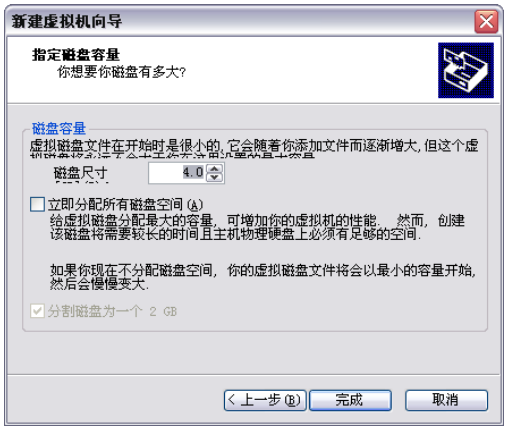


1-5

5 “ ” “ ” 1-6
“ ” 1-7 “ ”



1-6 “ ”

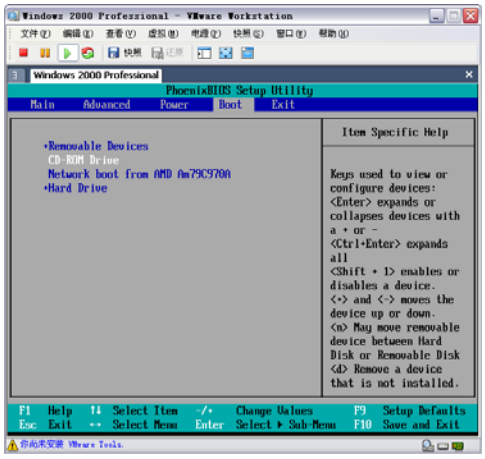


1-7 “ ”

4．在虚拟机软件中安装虚拟操作系统

VMware 1-8 “ ”
3

1 “ ”
F2 BIOS BOOT
“ ” “ ” 1-9



1-8 VMware 1-9

2 Windows 2000

提示：此时虚拟机的硬盘就如同刚刚买回的新硬盘一样，只管放心大胆地分区格式化，对你的真实系统丝毫不会造成损坏，因为VMware将计算机上的一个文件夹虚拟成一个硬盘，默认大小是4GB。

3

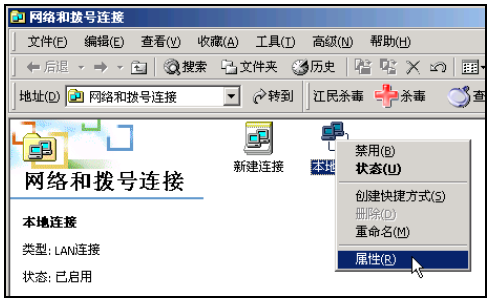
VMware “ ”→“ VMware Tools ”

1-10

4

“ ”→“ ”→“ ” “

” “ ” “ ” 1-11



1-10 1-11 “ ”