

黑客攻防实例入门

王浩 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』

《黑客攻防实例入门》

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人心，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？

- ④ 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）
- ④ 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）
- ④ 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）
- ④ 即时通讯软件的攻击与防范（QQ/MSN/Yahoo Messenger/UC 攻防）
- ④ 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）
- ④ 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）
- ④ 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）
- ④ 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）
- ④ 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）
- ④ 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）
- ④ 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	1
1.1 合法的黑客训练营——虚拟机	2
1.1.1 虚拟机简介	2
1.1.2 VMware打造黑客训练营	2
1.2 构造网站攻防学习园地	8
1.2.1 在虚拟机上架设IIS服务器	9
1.2.2 在虚拟机中安装网站	12
1.3 本章小结	16
第2章 漏洞的攻击与防范	17
2.1 Windows NT/2000/XP/2003漏洞攻防	18
2.1.1 IPC\$漏洞攻防	18
2.1.2 Windows 2000系统崩溃漏洞攻防	23
2.1.3 SAM数据库漏洞攻防	24
2.1.4 RPC漏洞攻防	26
2.1.5 Unicode漏洞攻击与防范	28
2.2 在Linux平台下入侵Windows平台	32
2.2.1 Linux平台下实战Webdav组件缓冲溢出漏洞	32
2.2.2 Linux平台下实战RPC缓冲溢出漏洞	33
2.2.3 Linux平台下连接3389肉鸡	33
2.3 在Windows平台下入侵Linux平台	34
2.3.1 根据漏洞原理来扫描并确认目标	34
2.3.2 编译溢出代码、熟悉用法	36
2.3.3 入侵目标、破解密码	36
2.3.4 Linux常见后门设置	38
2.4 Windows系统安全防范	40
2.4.1 利用组策略吓退菜鸟入侵者	40
2.4.2 局域网内的嗅探防范	42
2.4.3 巧妙利用控制台防止被ping	44
2.4.4 抓住恶意发送ICMP数据包的罪魁祸首	46
2.5 Linux系统安全防范	50
2.5.1 Linux下的日志文件分析	50
2.5.2 Syslog服务的启动和配置	56



2.5.3 Linux常用安全防范技巧.....	61
2.6 本章小结.....	64
第3章 木马的攻击与防范.....	65
3.1 木马简介.....	66
3.1.1 木马的功能.....	66
3.1.2 木马的分类及攻击方式.....	66
3.1.3 木马的藏身之处.....	67
3.2 木马的伪装.....	69
3.2.1 木马伪装为电子书.....	69
3.2.2 木马伪装为网页.....	70
3.2.3 木马伪装为图片.....	71
3.2.4 木马伪装为游戏.....	72
3.3 木马的加壳及特征码修改.....	73
3.3.1 木马服务端的一般加壳.....	73
3.3.2 木马服务端的多次加壳.....	73
3.3.3 木马特征码的修改.....	75
3.4 常见木马攻击实例.....	76
3.4.1 3721网页木马攻击.....	76
3.4.2 通风报信——灰鸽子木马.....	78
3.4.3 伪装美女——广外女生.....	81
3.4.4 无形的黑手——黑洞.....	82
3.4.5 禽兽复活——Beast Reloaded.....	82
3.4.6 远程监控杀手——网络精灵.....	85
3.4.7 庖丁解牛——网络公牛.....	89
3.4.8 线程插入型木马——禽兽.....	92
3.4.9 另类远程控制软件——Dame Ware Mini Remote Control.....	95
3.4.10 内网控制——IRC木马Yulihubot.....	97
3.5 木马的清除与防范.....	100
3.5.1 隐藏本地IP地址.....	100
3.5.2 网页木马的防范.....	104
3.5.3 流行木马的清除.....	105
3.6 本章小结.....	108
第4章 即时通信软件的攻击与防范.....	109
4.1 针对QQ的攻击与防范.....	110
4.1.1 QQ的IP探测与隐藏.....	110
4.1.2 QQ密码的在线破解与防范.....	112
4.1.3 QQ黑软盗号攻击.....	114

4.1.4	QQ安全及防范.....	115
4.2	其他即时通信软件的攻防.....	115
4.2.1	UC密码的攻击与防范.....	115
4.2.2	MSN密码的窃取与防范.....	116
4.2.3	MSN信息的“窃听”与防范.....	117
4.3	本章小结.....	118
第5章	电子邮箱的攻击与防范.....	119
5.1	邮件炸弹及附件的攻击与防范.....	120
5.1.1	邮件信息轰炸攻击.....	120
5.1.2	邮件附件轰炸攻击.....	120
5.1.3	图片附件的攻击.....	121
5.1.4	HTML邮件的攻击.....	122
5.1.5	邮件炸弹的清除与防范.....	122
5.2	Web邮箱密码的破解与防范.....	124
5.2.1	POP3邮箱密码暴力破解器——黑雨.....	124
5.2.2	流光软件破解邮件账号.....	126
5.2.3	保卫邮箱密码.....	127
5.3	邮件收发软件的漏洞攻防.....	128
5.3.1	Foxmail密码的破解与防御.....	128
5.3.2	Outlook密码的破解与防御.....	129
5.3.3	利用Foxmail/Outlook Express拒绝垃圾、病毒邮件.....	131
5.4	本章小结.....	134
第6章	网络游戏的攻击与防范.....	135
6.1	私服入侵及其防范.....	136
6.1.1	利用动网论坛漏洞入侵私服及其防范.....	136
6.1.2	利用私服系统数据库入侵私服及其防范.....	139
6.1.3	利用友情链接上传ASP木马及其防范.....	140
6.1.4	通过管理员上传ASP木马及其防范.....	142
6.2	GM权限窃取及其防范.....	143
6.2.1	添加GM账号.....	143
6.2.2	获取GM密码及其防范.....	144
6.3	网吧木马盗号.....	145
6.3.1	突破网吧限制.....	145
6.3.2	感染版传奇木马.....	146
6.3.3	利用传奇杀手嗅探密码.....	147
6.3.4	破解盛大密宝的传奇木马.....	147
6.3.5	天堂木马——黑猫.....	147



6.3.6	奇迹密码攻击	148
6.4	网游木马的查找/清除/防范	148
6.4.1	在线安全检测	149
6.4.2	利用工具查看系统进程	149
6.4.3	查看端口连接	150
6.4.4	使用专杀木马的软件	151
6.4.5	密码的设置及保护	152
6.4.6	关闭Windows系统端口	152
6.4.7	限制Windows系统端口	155
6.4.8	安装升级杀毒软件、防火墙	155
6.5	本章小结	158
第7章	网站与脚本的攻击与防范	159
7.1	论坛的的攻击与防范	160
7.1.1	大唐美化版插件入侵动网论坛及其防范	160
7.1.2	暴破入侵VBB3论坛及其防范	162
7.1.3	破解BBSXP论坛Access版管理员账号及其防范	164
7.1.4	控制SQL版BBSXP论坛数据库及其防范	165
7.1.5	修改BBSXP论坛文件上传类型及其防范	166
7.1.6	暴库BBSXP论坛及其的攻击与防范	168
7.1.7	PHPWind论坛攻击与防范	169
7.1.8	Discuz! 2.5F论坛的攻击与防范	171
7.2	文章系统的攻击与防范	172
7.2.1	“青创文章管理系统”的攻击与防范	172
7.2.2	老兵上传及其防范	174
7.2.3	入侵GBook365留言本及其防范	175
7.2.4	“桃源”留言本的攻击与防范	177
7.3	Cookie欺骗攻防实例	179
7.3.1	入侵“蓝色伊人日记本”及其防范	179
7.3.2	Cookie欺骗入侵L-Blog及其防范	181
7.3.3	动力3.51攻防	182
7.4	跨站脚本攻防实例	184
7.4.1	跨站业一新闻系统攻防	

8.1.2	Word宏病毒的攻击与清除.....	191
8.1.3	欢乐时光病毒的攻击与清除.....	192
8.1.4	网络天空病毒的攻击与清除.....	193
8.1.5	恶鹰病毒的攻击与清除.....	194
8.1.6	冲击波病毒的攻击与清除.....	195
8.1.7	震荡波病毒的攻击与清除.....	197
8.1.8	MSN小尾巴病毒的攻击与清除.....	197
8.1.9	MSN性感鸡病毒的攻击与清除.....	198
8.1.10	QQ病毒的攻击与清除.....	199
8.2	使用瑞星杀毒软件进行防御.....	200
8.2.1	设置定时扫描.....	200
8.2.2	安全漏洞扫描.....	201
8.2.3	制作DOS启动杀毒盘.....	201
8.2.4	在线杀毒.....	202
8.3	使用Symantec AntiVirus进行防御.....	203
8.3.1	手动查毒.....	203
8.3.2	实时监控.....	204
8.3.3	病毒库的更新.....	205
8.4	使用天网防火墙进行防御.....	205
8.4.1	设置向导.....	206
8.4.2	应用程序规则设置.....	206
8.4.3	IP规则管理设置.....	207
8.4.4	查看日志.....	208
8.4.5	断开/接通网络.....	208
8.4.6	阻止使用QQ、MSN.....	209
8.5	使用诺顿网络安全特警进行保护.....	209
8.5.1	防范入侵企图.....	209
8.5.2	让磁盘、文件和数据远离病毒.....	210
8.5.3	确保个人隐私资料安全.....	210
8.5.4	过滤垃圾邮件.....	210
8.6	个人网络防火墙ZoneAlarm.....	210
8.6.1	随时断开网络功能.....	211
8.6.2	不同区域设置不同安全级别.....	211
8.6.3	限制网络应用程序访问网络.....	211
8.6.4	垃圾邮件监控功能.....	212
8.7	Windows XP防火墙.....	212
8.7.1	Windows XP防火墙的工作原理.....	213
8.7.2	使用Windows XP防火墙.....	213



8.7.3 了解Internet控制消息协议	214
8.8 本章小结	214
第9章 系统/软件的加密和解密	215
9.1 系统密码限制破解	216
9.1.1 CMOS密码的破解	216
9.1.2 IE内容审查密码的设置与破解	219
9.2 办公软件密码的加密/破解	220
9.2.1 Office文档的加密	221
9.2.2 Office文档的破解	224
9.2.3 WPS文档的加密	228
9.2.4 WPS文档的破解	229
9.2.5 PDF文档的加密	230
9.2.6 PDF文档的破解	231
9.3 解密软件实例剖析	233
9.3.1 还原精灵的破解	233
9.3.2 剖析重启校验软件的破解方法	235
9.4 其他加密方式	242
9.4.1 利用压缩软件进行加密	242
9.4.2 利用“隐藏”属性加密	244
9.4.3 用Windows高级属性来加密	245
9.5 本章小结	246
第10章 远程溢出攻防实例	247
10.1 流行溢出攻防实例	248
10.1.1 CCProxy远程溢出攻击	248
10.1.2 IDA和IDQ扩展溢出攻防	252
10.1.3 .Printer溢出攻防	254
10.1.4 Windows Messenger远程PNG图片溢出攻击	255
10.1.5 JPEG图片溢出攻防	257
10.1.6 EMF图片溢出攻防	258
10.1.7 黑冰防火墙远程溢出攻防	260
10.1.8 Serv-U FTP Server远程溢出攻防	261
10.1.9 Serv-U FTP Server远程拒绝服务攻防	265
10.2 最新操作系统远程溢出攻防	267
10.2.1 Windows XP SP2防火墙溢出攻防	267
10.2.2 WINS MS04045溢出攻防	267
10.2.3 Lsasrv. DLL远程溢出攻防	270
10.2.4 MS05-002漏洞溢出攻防	272

10.2.5	IE IFRAME漏洞溢出攻防.....	274
10.2.6	MS05037漏洞远程溢出攻防.....	275
10.3	娱乐软件溢出攻防.....	279
10.3.1	Real Server远程溢出攻防.....	279
10.3.2	Realplay .smil远程溢出攻防.....	280
10.3.3	Windows Media远程溢出攻防.....	281
10.4	本章小结.....	282
第11章	系统自身的安全防护.....	283
11.1	账号及安全策略设置.....	284
11.1.1	如何防范黑客入侵.....	284
11.1.2	账号密码设置.....	285
11.1.3	本地安全策略设置.....	286
11.2	系统服务安全设置.....	289
11.2.1	设置服务项.....	289
11.2.2	修改注册表防御DoS攻击.....	289
11.2.3	禁止默认共享.....	290
11.2.4	提高Cookie安全级别.....	291
11.2.5	防止跨站攻击.....	292
11.3	系统权限设置.....	293
11.3.1	修改权限设置.....	293
11.3.2	重要文件加密.....	296
11.4	相关软件的安全防护.....	297
11.4.1	杀毒软件介绍与应用.....	298
11.4.2	防火墙介绍与应用.....	305
11.5	本章小结.....	310



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

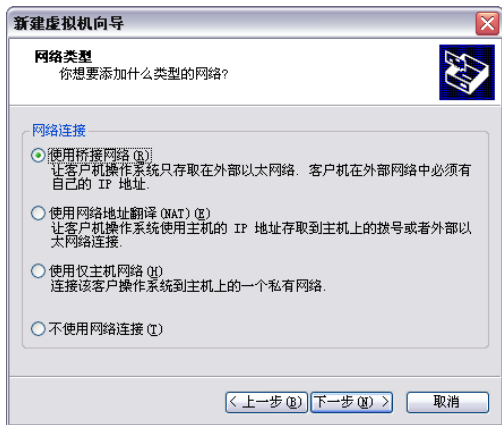
VMware

1-2

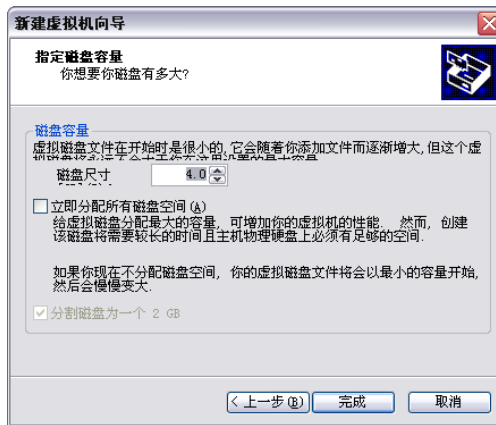


1-5

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

