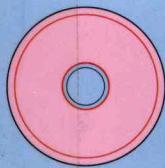




黑客攻防 实战入门与提高

·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

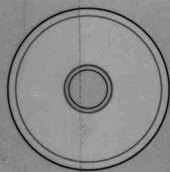
采用最为通俗易懂的图文解说，并配有多媒体视频讲解，让读者可以轻松上手



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

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

任务 1

上兴木马入侵..... 1

任务学习引导 2

- 要点① 了解远程控制木马的使用 2
- 要点② 懂得木马的运行模式对安全防护的意义 2
- 要点③ 什么是远程控制木马 2
- 要点④ 被木马攻击的原因 4
- 要点⑤ 相关软件简介 4

攻击实训 5

- 实训① 肉鸡查找 5
- 实训② 配置远程控制木马 6
- 实训③ 使用啊 D 网络工具包
种植木马 7

- 实训④ 利用远程控制软件控制
目标机 8

防御措施 8

- 措施① 禁止空连接进行枚举 9
- 措施② 禁止默认共享 9
- 措施③ 关闭 IPC\$和默认共享依赖的
Server 服务 10
- 措施④ 屏蔽 139、445 端口 10
- 措施⑤ 设置复杂密码 11

任务小结 11

任务 2

简单文件型 DOS 病毒制作 12

任务学习引导 13

- 要点① 了解文件型 DOS 病毒的制作
原理 13
- 要点② 了解文件型 DOS 病毒原理对
安全防护的意义 13
- 要点③ 什么是文件型病毒 13
- 要点④ 相关软件简介 17

攻击实训 17

- 实训① 搭建实施环境 17
- 实训② 编写一个 test.asm 汇编
源文件 18
- 实训③ 生成病毒文件 20
- 实训④ 感染实验 21

防御措施 23

任务小结 23

Contents

任务 3

基于溢出的入侵..... 24

任务学习引导 25

- 要点① 了解溢出攻击原理.....25
- 要点② 了解溢出攻击对安全防护的意义.....25
- 要点③ 什么是溢出与溢出攻击.....25
- 要点④ 相关软件简介.....25

攻击实训 26

- 实训① 扫描网络中的主机.....26

- 实训② 利用 nc 工具打开本地监听端口..... 27
- 实训③ 利用 ms06040.exe 溢出目标主机..... 27
- 实训④ 在目标主机上新建管理员账号..... 28
- 实训⑤ 实施远程登录..... 29

防御措施 33

任务小结 33

任务 4

信息收集及嗅探..... 34

任务学习引导 35

- 要点① 学会常用信息嗅探收集及嗅探方法.....35
- 要点② 了解 ARP 原理对于安全防护的意义.....35
- 要点③ 嗅探常用的工具与手段.....35
- 要点④ 相关软件简介.....35

攻击实训 36

- 实训① 扫描局域网主机..... 36
- 实训② 实施信息收集..... 38

防御措施 42

任务小结 43

任务 5

终极免杀..... 44

任务学习引导 45

- 要点① 学会常用免杀方法.....45
- 要点② 精通免杀对安全防护的意义.....45
- 要点③ 病毒免杀常用的工具与手段.....45

- 要点④ 相关软件简介..... 46

攻击实训 47

- 实训① 改入口点免杀法..... 47
- 实训② 加花指令免杀法..... 49

目 录

实训③ 加壳或加伪装壳免杀法51

实训④ 打乱壳的头文件或壳中加花免杀法53

实训⑤ 变换入口地址免杀法54

实训⑥ 修改文件特征码免杀法 57

防御措施 61

任务小结 61

任务 6

针对服务器的网络僵尸 DDoS 攻击 62

任务学习引导 63

要点① 什么是分布式攻击 63

要点② 学习服务器的分布式攻击方法 63

要点③ 懂得如何防护分布式攻击 63

要点④ 相关软件简介 64

攻击实训 64

实训① 本地搭建局域网 64

实训② 对肉鸡进行木马种植 64

实训③ 测试攻击 65

防御措施 67

任务小结 67

任务 7

上兴木马手工查杀 68

任务学习引导 69

要点① 了解手工检测病毒的过程 69

要点② 手工检测查杀病毒对安全防护的意义 69

要点③ 手工检测与查杀木马的常规方法 69

要点④ 相关软件简介 70

实训① 获取感染前的系统诊断报告 70

实训② 生成测试木马 71

实训③ 获取木马的特征 72

实训④ 获取感染后的系统诊断报告 73

实训⑤ 对比日志 73

实训⑥ 手工查杀 76

攻击实训 70

任务小结 78

Contents

任务 8

缓冲区溢出工具编写..... 79

任务学习引导 80

- 要点 ① 了解任务过程 80
- 要点 ② 了解溢出工具的编写对安全防护的意义 80
- 要点 ③ HTTP 与缓冲区溢出原理 80
- 要点 ④ 相关软件简介 82

攻击实训 82

- 实训 ① 用 X-Scan 扫描漏洞 82
- 实训 ② 攻击目标主机 84
- 实训 ③ 用 VC 编译攻击工具 86
- 实训 ④ 在工程中添加文件 88
- 实训 ⑤ 验证 cniis 的效果，再次创建 hax 用户 92

防御措施 93

任务小结 93

任务 9

远程登录入侵..... 94

任务学习引导 95

- 要点 ① Telnet 入侵的思路 95
- 要点 ② Telnet 与 NTLM 认证对安全防护的意义 95
- 要点 ③ NTLM 认证模式 95
- 要点 ④ 相关软件简介 96

攻击实训 97

- 实训 ① 前期准备 97
- 实训 ② 使用 OpenTelnet.exe 开启目标主机的 Telnet 服务 99

- 实训 ③ 在目标主机上建立账户，留“后门” 100
- 实训 ④ 清除入侵痕迹 101

防御措施 104

- 措施 ① 停止并删除服务 104
- 措施 ② 管理好用户的密码 104
- 措施 ③ 修改服务端口 104
- 措施 ④ 禁用 Telnet 服务 104
- 措施 ⑤ 终极 Telnet 服务防御 104
- 措施 ⑥ 日志文件的移位保护 105

任务小结 105

任务 10

用 WinRAR 打造捆绑利器 106

任务学习引导 107

- 要点① 使用 RAR 脚本制作木马后门 107
- 要点② 利用 RAR 伪装木马对安全防护的意义 107
- 要点③ 相关软件简介 107

攻击实训 107

- 实训① 搭建测试局域网 107
- 实训② 配置远控木马 107
- 实训③ 使用 RAR 进行脚本压缩 108
- 实训④ 上线测试 113

防御措施 114

任务小结 115

任务 11

木马加壳技术 116

任务学习引导 117

- 要点① 加壳与脱壳的常用方法 117
- 要点② 木马加壳对安全防护的意义 117
- 要点③ 加壳与脱壳常用的工具与手段 117
- 要点④ 相关软件简介 118

攻击实训 119

- 实训① 利用 PcShare 配置木马 119
- 实训② 利用 MoleBox 对木马进行打包处理 120
- 实训③ 使用 IExpress 进行伪装 121
- 实训④ 远程控制测试 125

防御措施 127

任务小结 128

任务 12

肉鸡跳板制作 129

任务学习引导 130

- 要点① 隐藏身份的常用方法 130

- 要点② 隐藏 IP 对于安全防护的意义 130
- 要点③ IP 隐藏与代理服务 130
- 要点④ 相关软件简介 131

Contents

攻击实训 131

- 实训① 在肉鸡上安装 Snake 代理服务 131
- 实训② 配置本地代理工具 134

实训③ 设置代理应用程序 137

实训④ 肉鸡代理测试 138

防御措施 139

任务小结 139

任务 13

利用 Google 得到敏感信息 140

任务学习引导 141

- 要点① 学习搜索引擎的高级搜索技巧 141
- 要点② 针对不同的搜索漏洞进行防护的意义 141
- 要点③ 谷歌关键字介绍 141

攻击实训 142

- 实训① 如何搜索特定的网站后台 142
- 实训② 如何搜索特定文件 143
- 实训③ 如何批量搜索漏洞 147

任务小结 148

任务 14

经典脚本入侵 149

任务学习引导 150

- 要点① 学习上传漏洞技巧 150
- 要点② 了解上传漏洞原理的意义 150
- 要点③ 什么是脚本攻击 150
- 要点④ 针对 Web 服务器的攻击 150
- 要点⑤ 相关软件简介 152

攻击实训 152

- 实训① 搭建有漏洞的网站 152
- 实训② 实施脚本攻击 153

防御措施 155

任务小结 156

任务 15

Cookies 欺骗 157

任务学习引导 158

- 要点① 学习 Cookies 欺骗的技巧 158

- 要点② 了解 Cookies 欺骗原理的意义 158

- 要点③ 什么是 Cookies 欺骗 158

目 录

要点④ 相关软件简介	158	实训③ 查看管理员 Cookie	163
攻击实训	159	实训④ 编写管理员 Cookie	164
实训① 搭建动网论坛	159	防御措施	166
实训② 获取 Cookies 信息	160	任务小结	166

任务 16

Access+ASP 网站入侵（工具篇） 167

任务学习引导	168	攻击实训	170
要点① 根源分析	168	实训① 搭建有漏洞的网站	170
要点② 学习工具入侵网站技巧	169	实训② 利用工具扫描	171
要点③ 懂得工具入侵网站对安全防护 的意义	169	实训③ 获得后台及管理员信息	173
要点④ ASP+Access 网站类型简介	169	实训④ 成功入侵后台	174
要点⑤ 相关软件简介	169	防御措施	175
		任务小结	176

任务 17

Access+ASP 网站入侵（手工篇） 177

任务学习引导	178	实训① 搭建有漏洞的网站	178
要点① 学习手工入侵技巧	178	实训② 猜解后台信息	179
要点② 懂得手工入侵原理的意义	178	实训③ 获得管理员信息	186
要点③ ASP+Access 网站类型简介	178	实训④ 入侵网站	187
要点④ 相关软件简介	178	防御措施	188
攻击实训	178	任务小结	188

Contents

任务 18

SQL 注射入侵（工具篇） 189

任务学习引导 190

- 要点① 新建一个数据库 190
- 要点② 学习目标 190
- 要点③ SQL 注入过程 190
- 要点④ 相关软件简介 190

攻击实训 191

- 实训① 前期准备工作 191
- 实训② 测试网站漏洞 191
- 实训③ 猜解管理员信息 192
- 实训④ 提权入侵服务器 193

防御措施 194

任务小结 194

任务 20

SQL 注射入侵（手工篇） 195

任务学习引导 196

- 要点① 学习 PHP+MySQL 网站注入技巧 196
- 要点② 了解数据库注入原理对安全防护的意义 196
- 要点③ SQL 注射入侵 196

攻击实训 197

- 实训① 获取注射目标 197
- 实训② 测试网站漏洞 198
- 实训③ 进行 union 查询 200
- 实训④ 获得敏感信息 201
- 实训⑤ 寻找网站绝对目录试进后台 202

防御措施 205

任务小结 206

任务 20

基于 IIS 服务器的入侵 208

任务学习引导 209

- 要点① 学习 IIS 上传漏洞的使用技巧 209
- 要点② 了解 IIS 上传漏洞对安全防护的意义 209

- 要点③ IIS 上传漏洞介绍 209
- 要点④ 相关软件简介 209

攻击实训 210

- 实训① 本地搭建 ASP 环境 210
- 实训② 利用 IIS PUT Scanner.exe 测试权限 210

实训③ 上传木马及登录后台 210

实训④ 获得网站控制权 213

防御措施 213

任务小结 214

任务 21

基础网络硬件设备防火墙的安全部署··· 215

任务学习引导 216

要点① 学习防火墙的配置及管理 216

要点② 了解防火墙对网络安全防护的意义 216

要点③ 防火墙概述 216

要点④ 设备简介 217

实施步骤 218

实训① 配置超级终端 218

实训② 配置防火墙管理软件 221

实训③ 配置新网关 224

实训④ 检测防火墙配置是否成功 229

任务小结 232

任务 22

锐捷交换机的部署····· 233

任务学习引导 234

要点① 交换机的功能 234

要点② VLAN 技术在网络中的广泛应用 234

要点③ 交换机常识 234

实施步骤 235

实训① 连接设备 235

实训② 登录交换机 236

实训③ 配置设备 237

实训④ 验证测试 241

任务小结 244

任务 23

漏洞扫描设备的部署····· 245

任务学习引导 246

要点① 漏洞扫描系统的作用 246

要点② 部署漏洞扫描系统的意义 246

要点③ 资料查阅 246

实施步骤 247

实训① 登录漏洞扫描界面 247

实训② 扫描测试 249

实训③ 其他设置 251

任务小结 252

Contents

任务 24

联想网御 SSL VPN 设备的部署 253

任务学习引导 254

- 要点① 学习 SSL VPN 的配置管理 254
- 要点② SSL VPN 在网络中应用的
意义 254
- 要点③ SSL VPN 介绍 254

实施步骤 255

- 实训① 基本配置 255
- 实训② 制定访问规则 258

任务小结 260

任务 25

北信源内网安全管理软件 261

任务学习引导 262

- 要点① 学习内网安全软件的配置及
管理 262
- 要点② 了解内网安全对网络安全
防护的意义 262
- 要点③ 学习内网安全管理的主要
内容 263
- 要点④ 软件介绍 264

应用实训 265

- 实训① 环境准备 265
- 实训② 服务器安装 265
- 实训③ 服务器配置 266
- 实训④ 客户端注册 270
- 实训⑤ 系统应用 271

任务小结 278

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。

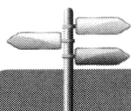
案例

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木马后的电脑，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。