

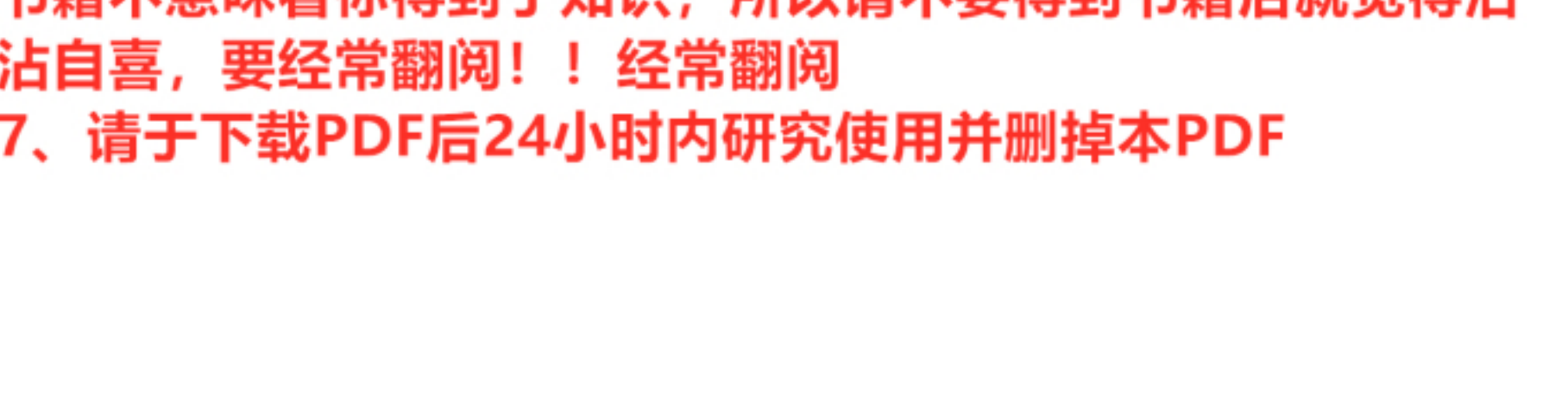
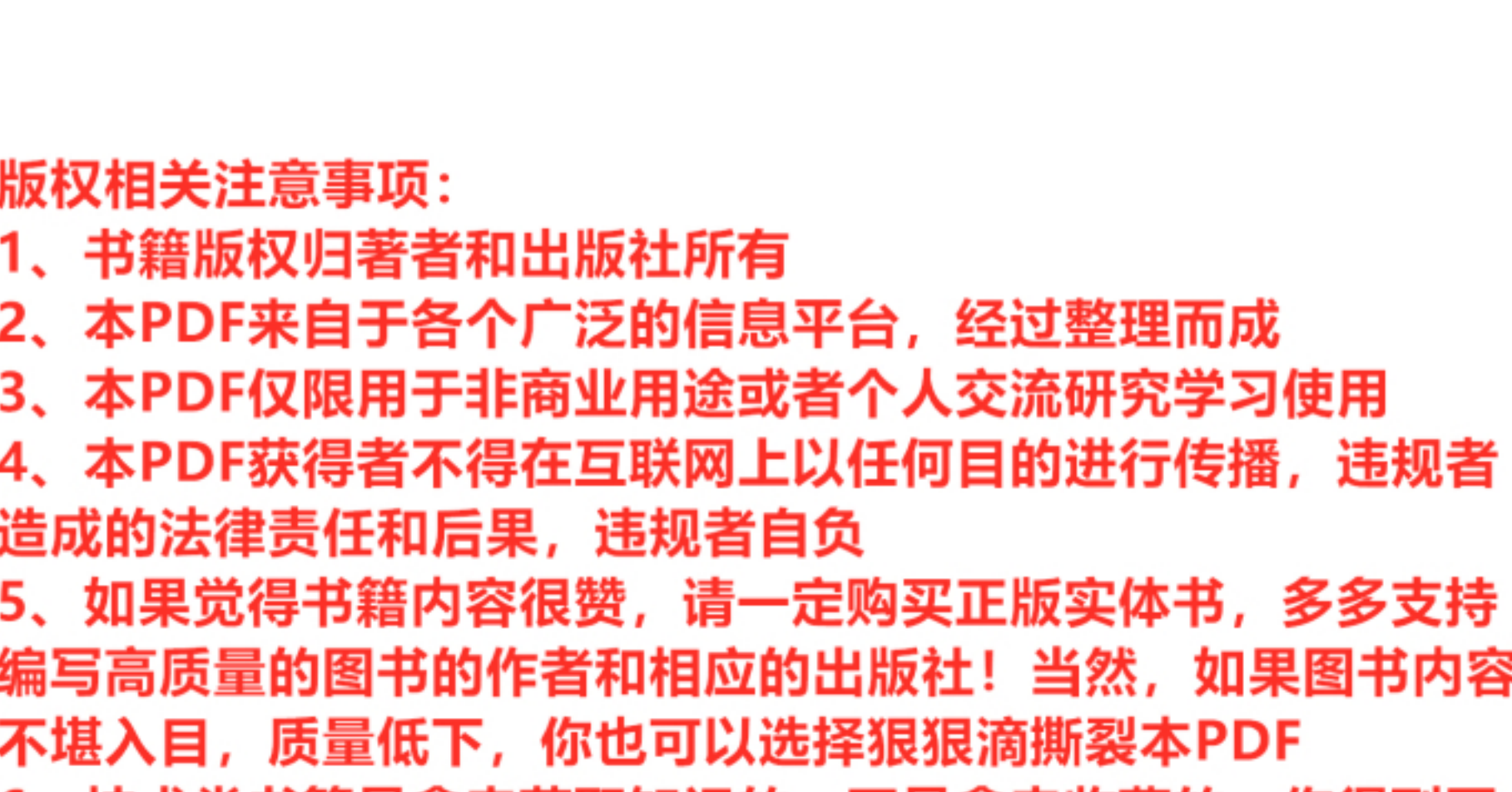
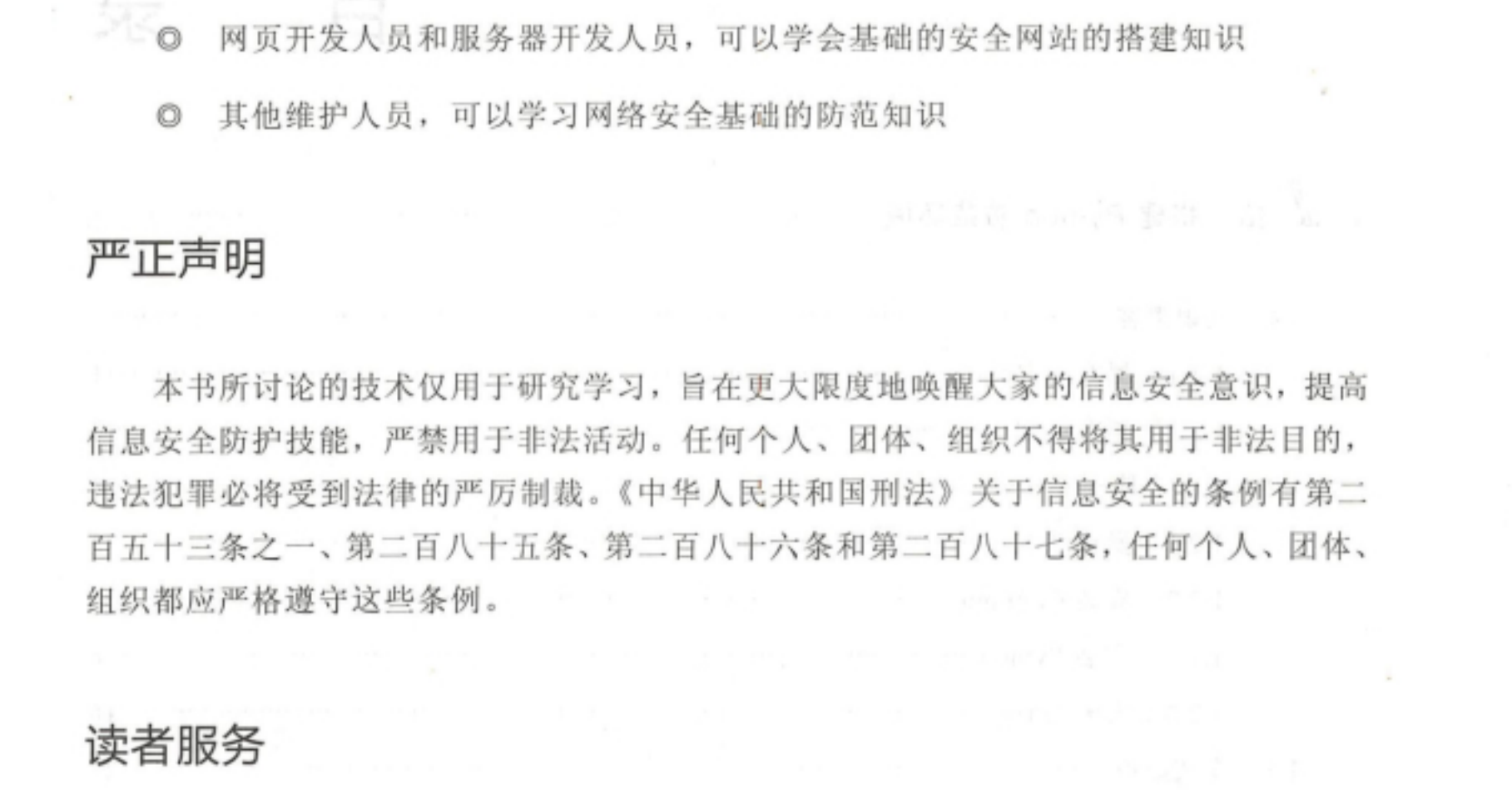
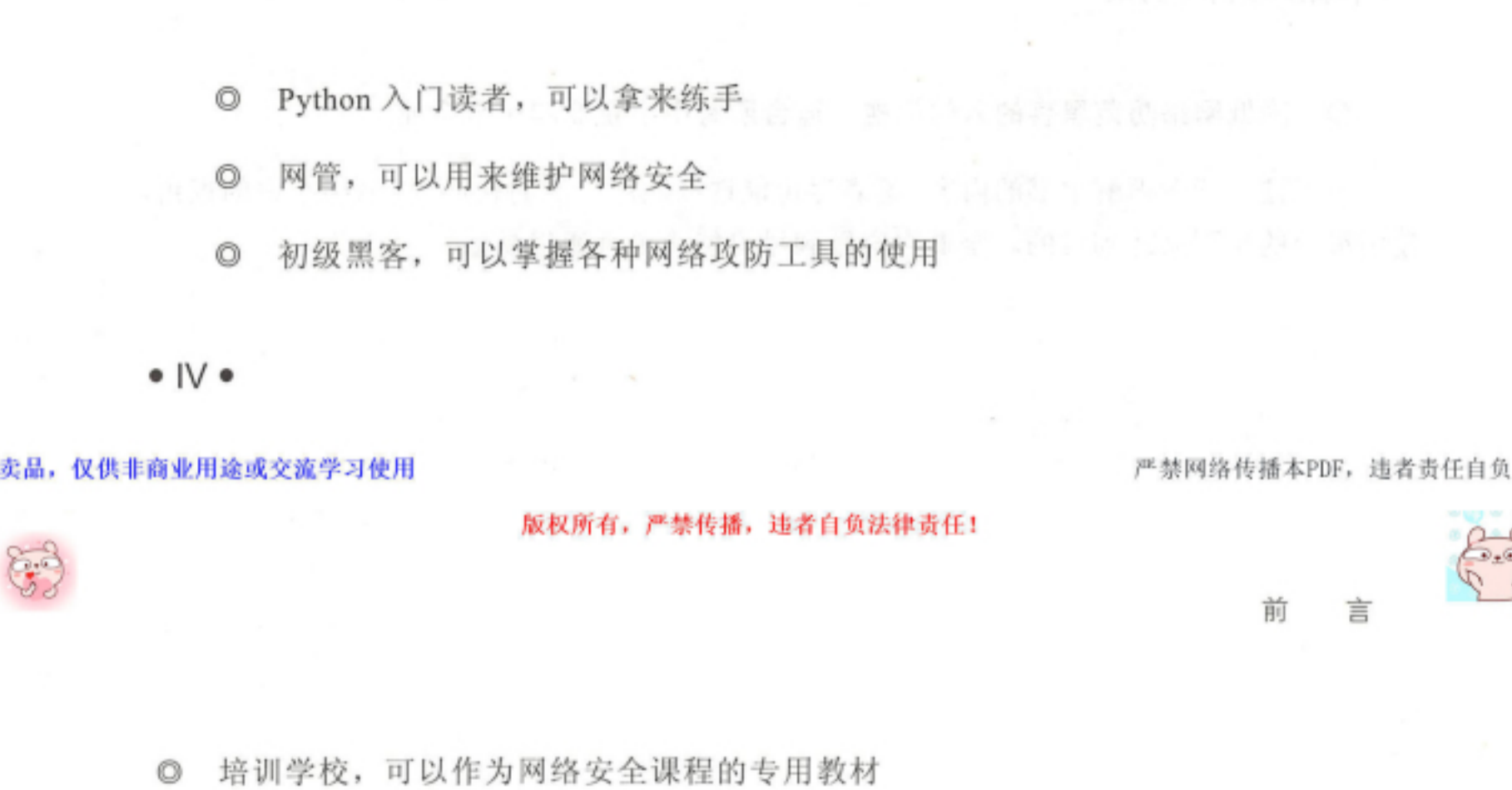
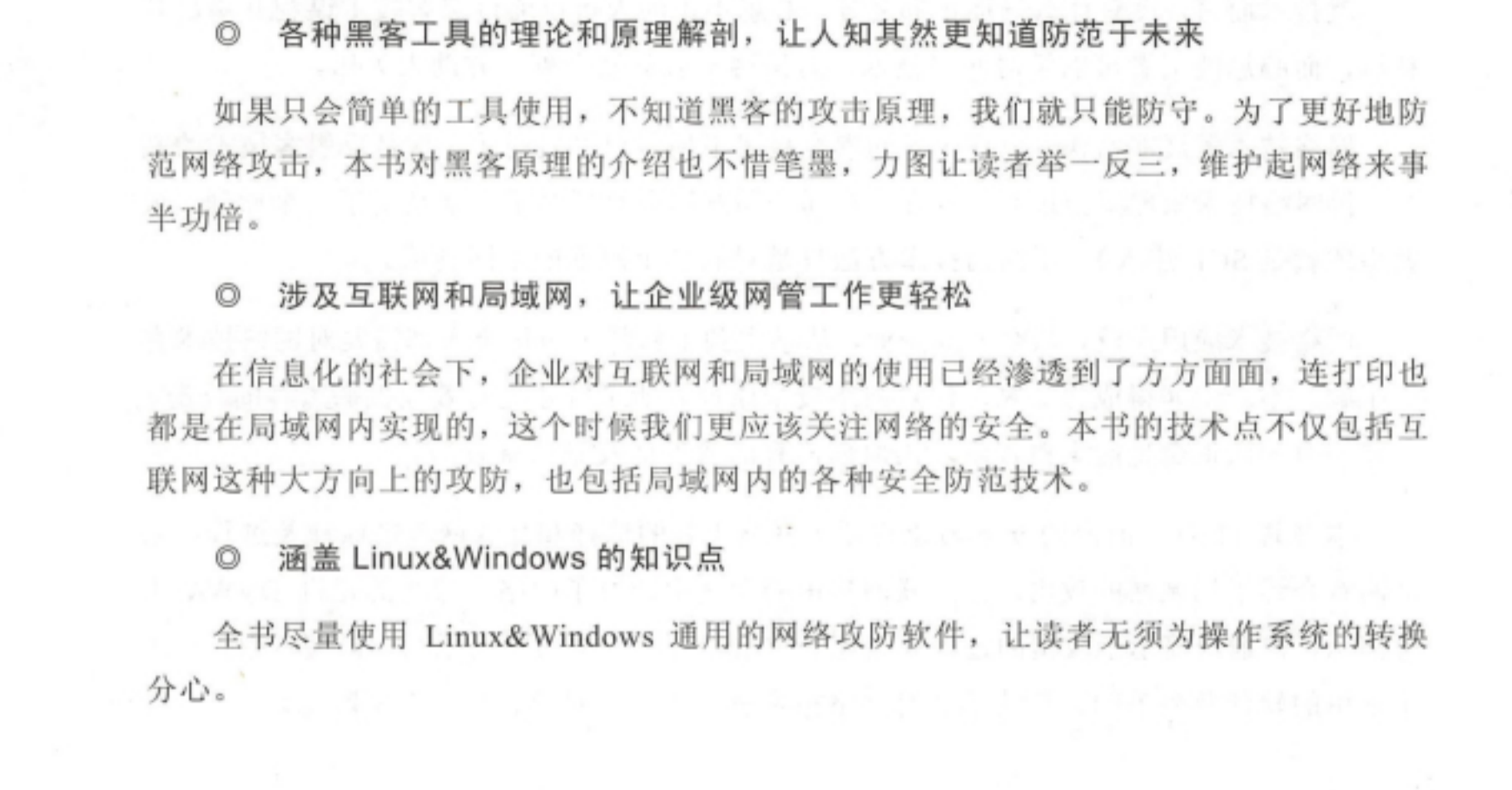
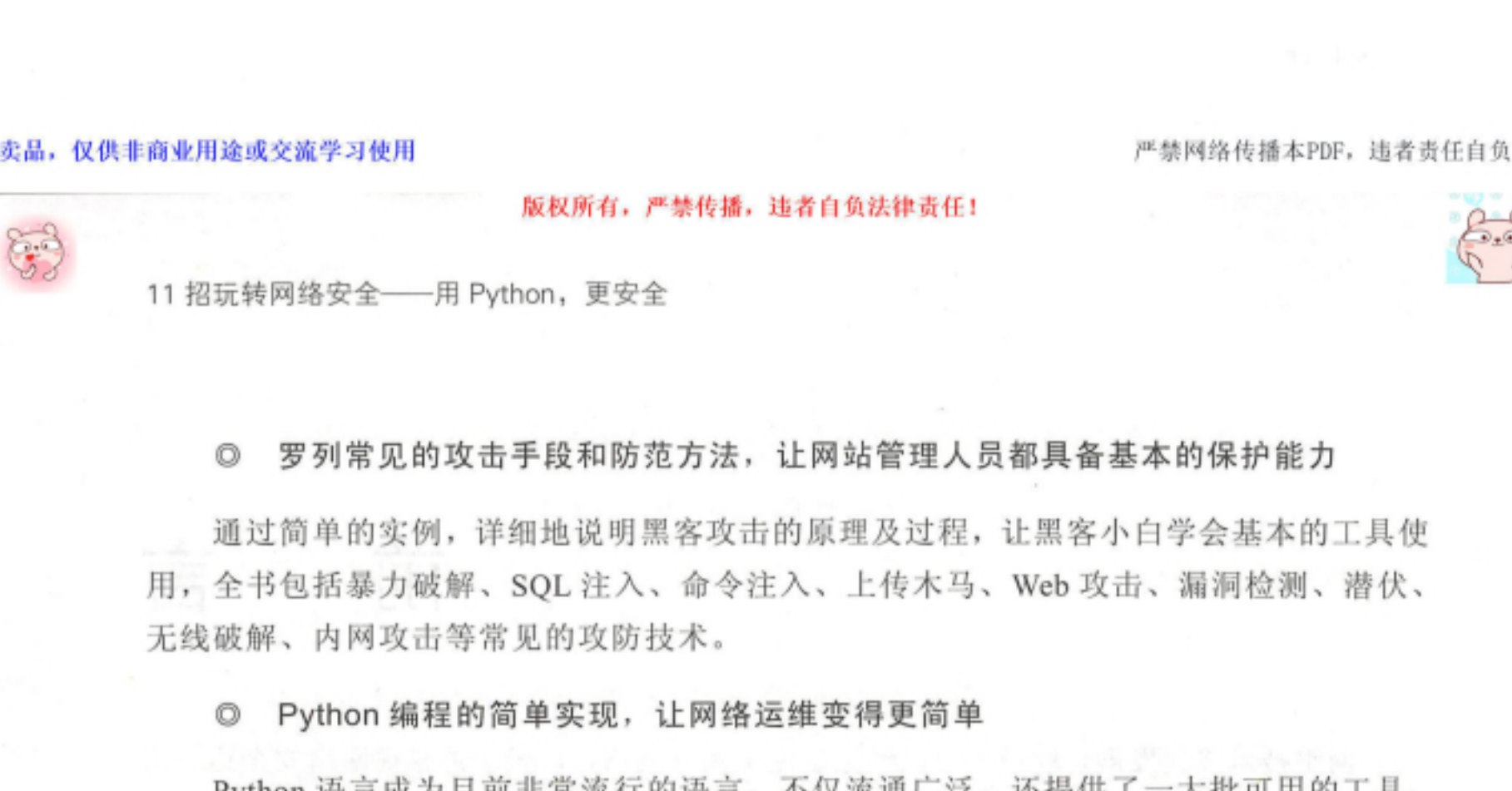
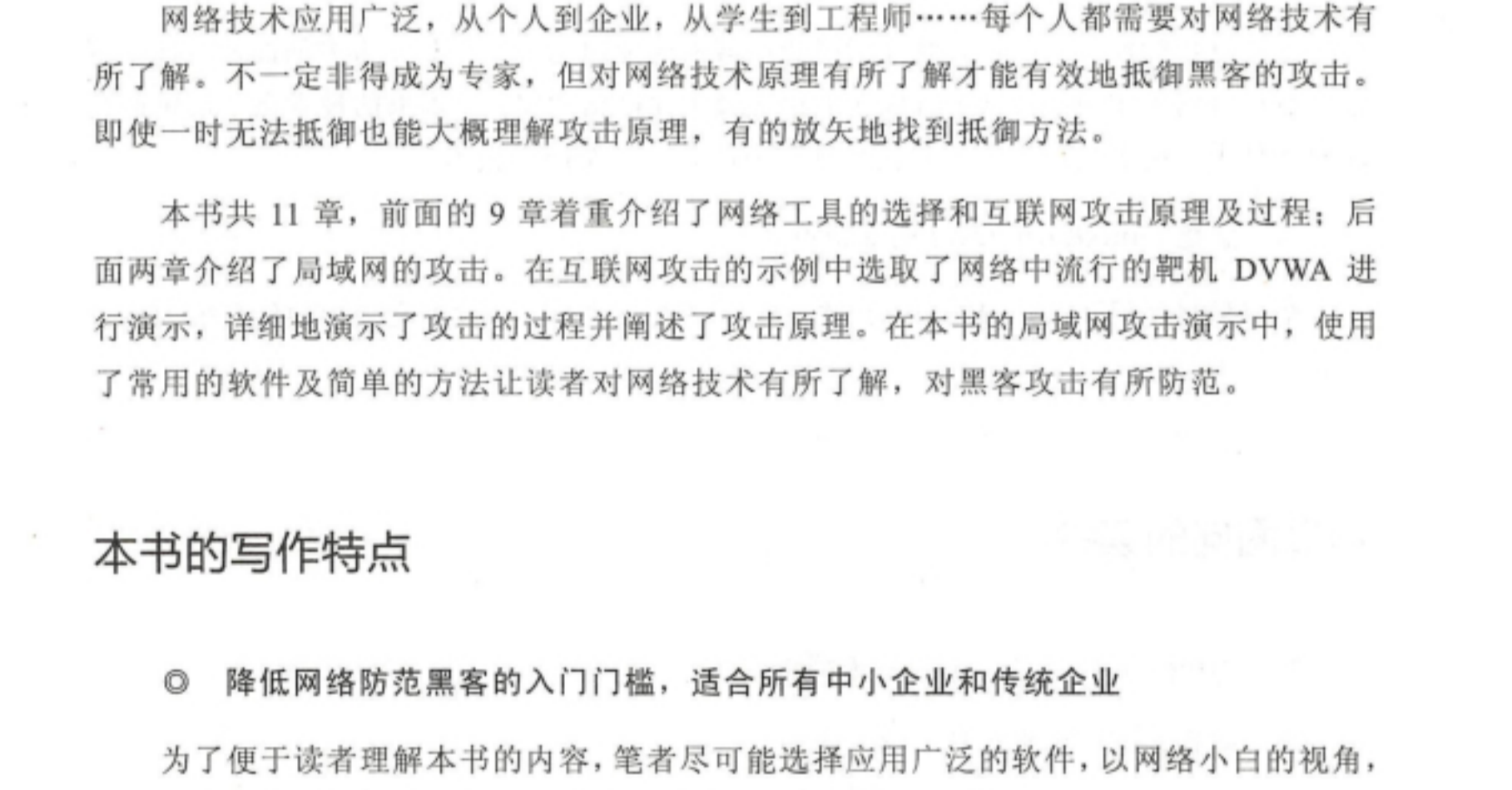
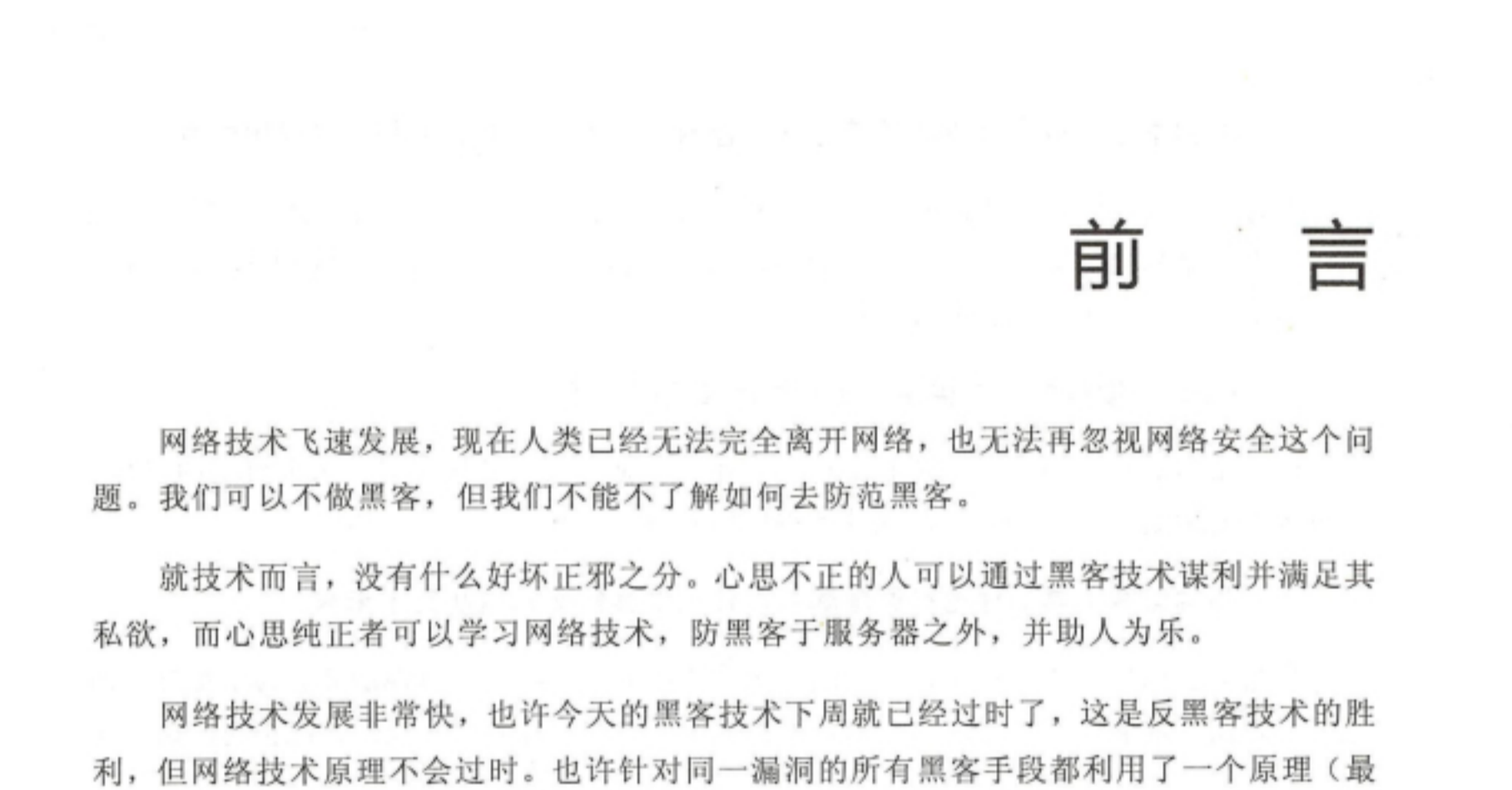
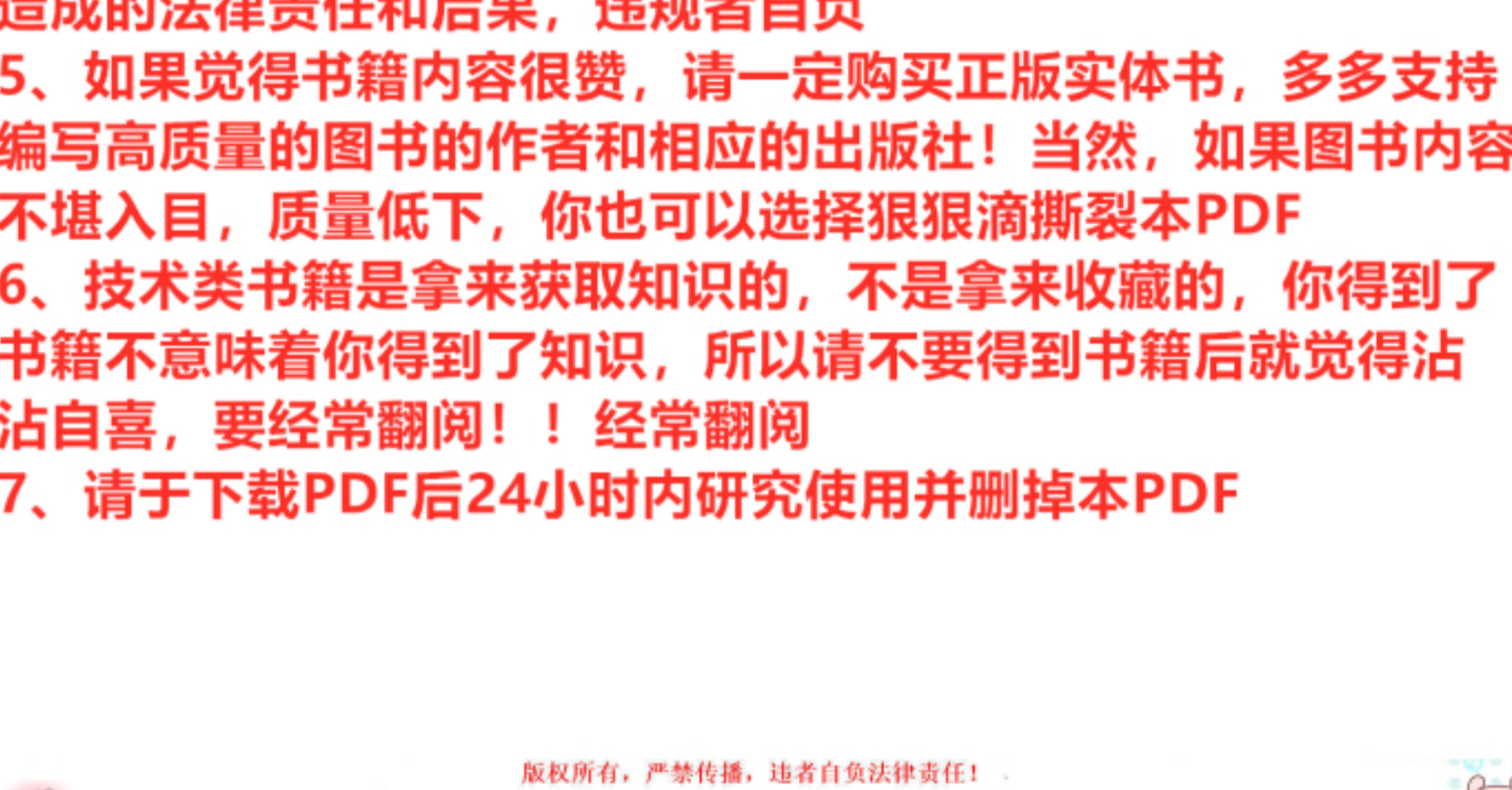
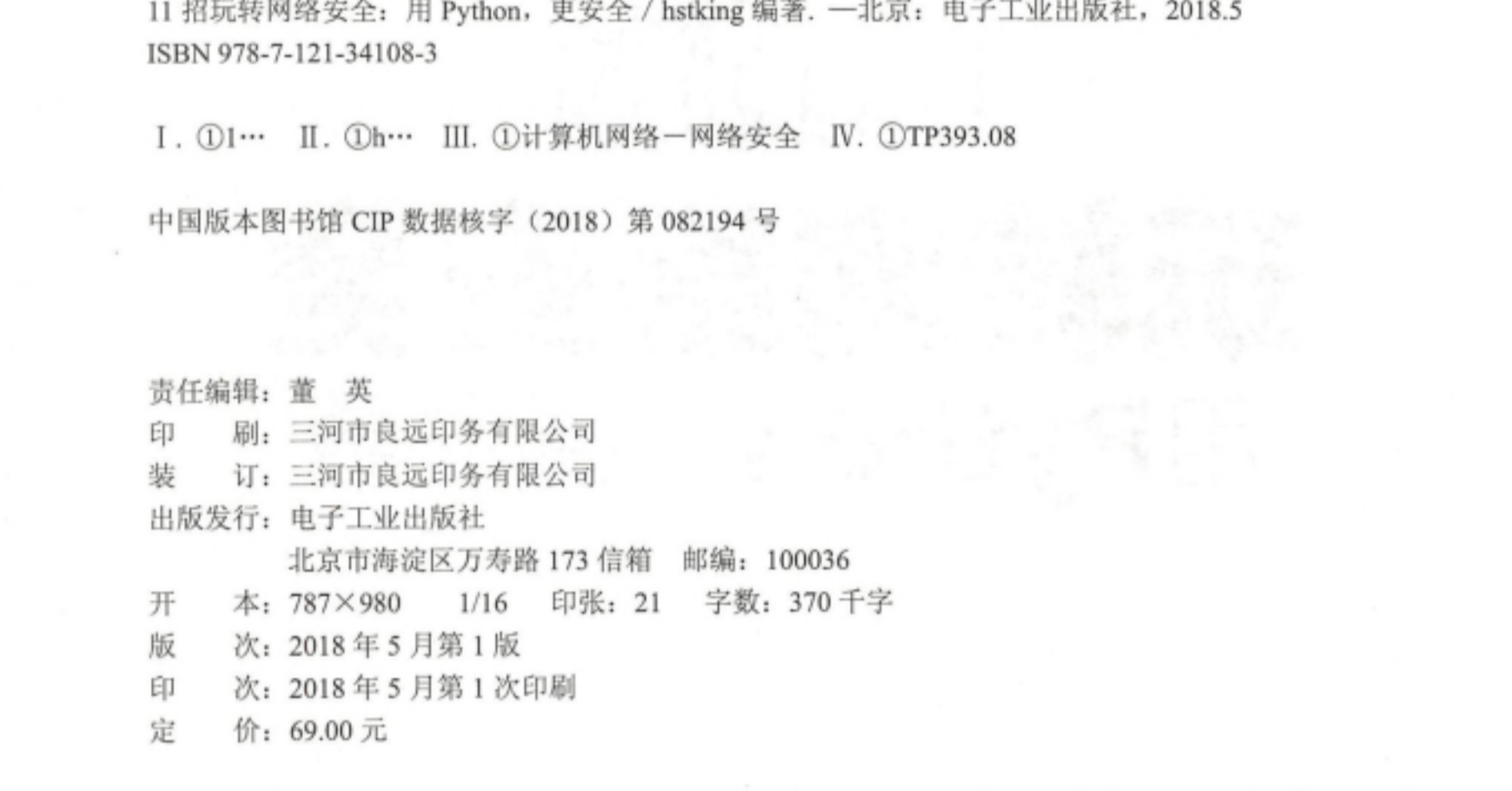
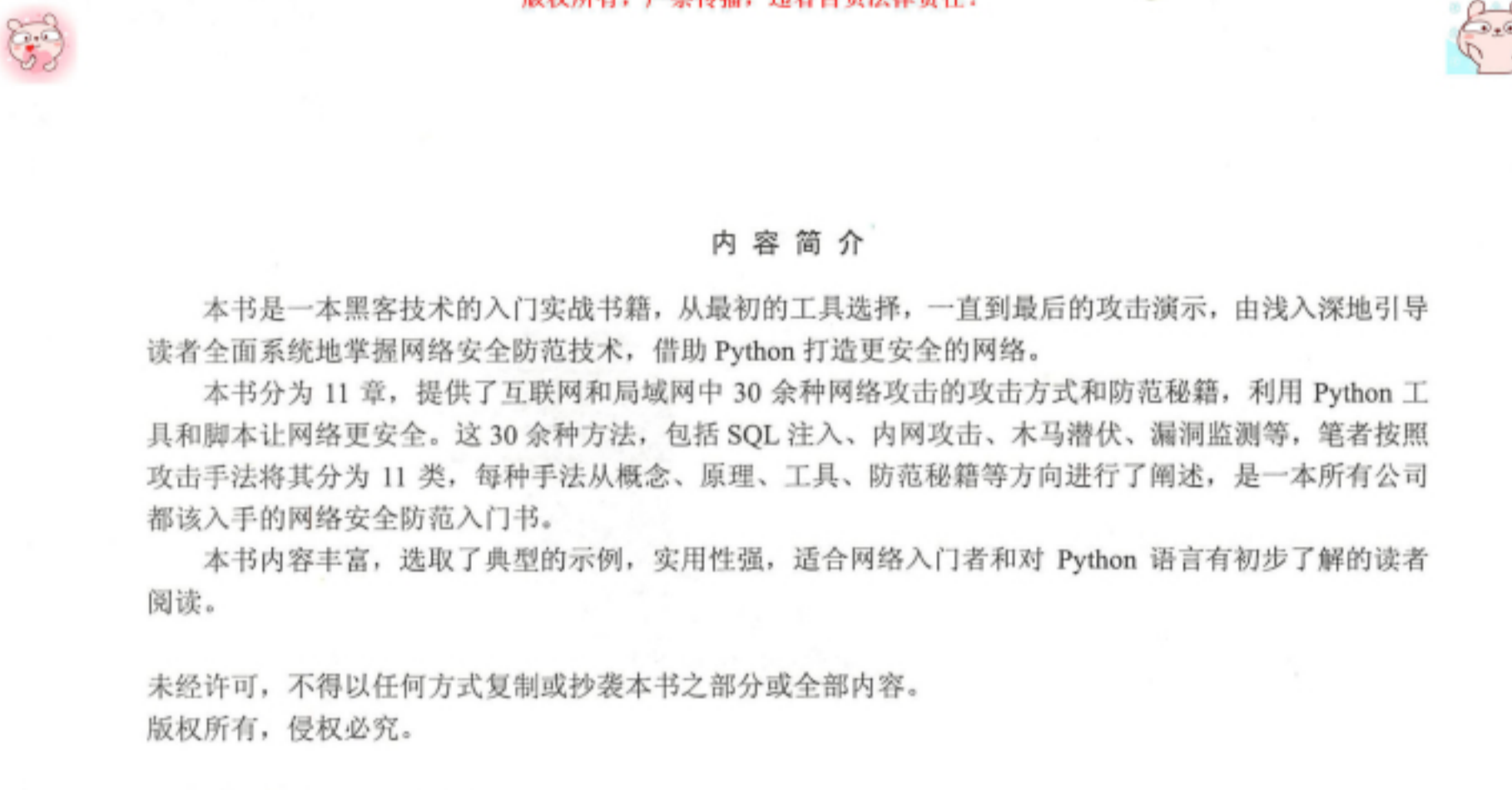


版权相关注意事项:

- 1、书籍版权归著者和出版社所有
- 2、本PDF来自于各个广泛的信息平台，经过整理而成
- 3、本PDF仅限于非商业用途或者个人交流研究学习使用
- 4、本PDF获得者不得在互联网上以任何目的进行传播，违规者造成的法律责任和后果，违规者自负
- 5、如果觉得书籍内容很赞，请一定购买正版实体书，多多支持编写高质量的图书的作者和相应的出版社！当然，如果图书内容不堪入目，质量低下，你也可以选择狠狠滴撕裂本PDF
- 6、技术类书籍是拿来获取知识的，不是拿来收藏的，你得到了书籍不意味着你得到了知识，所以请不要得到书籍后就觉得沾沾自喜，要经常翻阅！！经常翻阅
- 7、请于下载PDF后24小时内研究使用并删掉本PDF

版权相关注意事项:

- 1、书籍版权归著者和出版社所有
- 2、本PDF来自于各个广泛的信息平台，经过整理而成
- 3、本PDF仅限于非商业用途或者个人交流研究学习使用
- 4、本PDF获得者不得在互联网上以任何目的进行传播，违规者造成的法律责任和后果，违规者自负
- 5、如果觉得书籍内容很赞，请一定购买正版实体书，多多支持编写高质量的图书的作者和相应的出版社！当然，如果图书内容不堪入目，质量低下，你也可以选择狠狠滴撕裂本PDF
- 6、技术类书籍是拿来获取知识的，不是拿来收藏的，你得到了书籍不意味着你得到了知识，所以请不要得到书籍后就觉得沾沾自喜，要经常翻阅！！经常翻阅
- 7、请于下载PDF后24小时内研究使用并删掉本PDF



# 玩转网络安全

## 用Python, 更安全

hstking©编著

电子工业出版社  
Publishing House of Electronics Industry  
北京·BEIJING

非卖品, 仅供非商业用途或交流学习使用

版权所有, 严禁传播, 违者自负法律责任!

非卖品, 仅供非商业用途或交流学习使用

版权所有, 严禁传播, 违者自负法律责任!

非卖品, 仅供非商业用途或交流学习使用

版权所有, 严禁传播, 违者自负法律责任!

非卖品, 仅供非商业用途或交流学习使用

版权所有, 严禁传播, 违者自负法律责任!

非卖品, 仅供非商业用途或交流学习使用

版权所有, 严禁传播, 违者自负法律责任!

非卖品, 仅供非商业用途或交流学习使用

版权所有, 严禁传播, 违者自负法律责任!

非卖品, 仅供非商业用途或交流学习使用

版权所有, 严禁传播, 违者自负法律责任!

非卖品, 仅供非商业用途或交流学习使用

版权所有, 严禁传播, 违者自负法律责任!

非卖品, 仅供非商业用途或交流学习使用

版权所有, 严禁传播, 违者自负法律责任!

非卖品, 仅供非商业用途或交流学习使用

版权所有, 严禁传播, 违者自负法律责任!

非卖品, 仅供非商业用途或交流学习使用

版权所有, 严禁传播, 违者自负法律责任!

非卖品, 仅供非商业用途或交流学习使用

版权所有, 严禁传播, 违者自负法律责任!

非卖品, 仅供非商业用途或交流学习使用

版权所有, 严禁传播, 违者自负法律责任!

非卖品, 仅供非商业用途或交流学习使用

版权所有, 严禁传播, 违者自负法律责任!

非卖品, 仅供非商业用途或交流学习使用

版权所有, 严禁传播, 违者自负法律责任!

非卖品, 仅供非商业用途或交流学习使用

版权所有, 严禁传播, 违者自负法律责任!

非卖品, 仅供非商业用途或交流学习使用

版权所有, 严禁传播, 违者自负法律责任!

### 内容简介

本书是一本黑客技术的入门实战书籍，从最初的工具选择，一直到最后的攻击演示，由浅入深地引导读者全面系统地掌握网络安全防范技术，借助 Python 打造更安全的网络。

本书分为 11 章，提供了互联网和局域网中 30 余种网络攻击的攻击方式和防范秘籍，利用 Python 工具和脚本让网络更安全。这 30 余种方法，包括 SQL 注入、内网攻击、木马潜伏、漏洞监测等，笔者按照攻击手法将其分为 11 类，每种手法从概念、原理、工具、防范秘籍等方向进行了阐述，是一本所有公司都该入手的网络安全防范入门书。

本书内容丰富，选取了典型的示例，实用性强，适合网络入门者和对 Python 语言有初步了解的读者阅读。

未经许可，不得以任何方式复制或抄袭本书之部分或全部内容。  
版权所有，侵权必究。

图书在版编目 (CIP) 数据

11 招玩转网络安全：用 Python，更安全 / hstking 编著. —北京：电子工业出版社，2018.5  
ISBN 978-7-121-34108-3

I. ①1… II. ①h… III. ①计算机网络—网络安全 IV. ①TP393.08

中国版本图书馆 CIP 数据核字 (2018) 第 082194 号

责任编辑：董英  
印刷：三河市良远印务有限公司  
装订：三河市良远印务有限公司  
出版发行：电子工业出版社  
北京市海淀区万寿路 173 信箱 邮编：100036  
开本：787×980 1/16 印张：21 字数：370 千字  
版次：2018 年 5 月第 1 版  
印次：2018 年 5 月第 1 次印刷  
定价：69.00 元

凡所购电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：(010) 88254888，88258888。  
质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。  
本书咨询联系方式：(010) 51260888-819，faq@phei.com.cn。

非卖品, 仅供非商业用途或交流学习使用

版权所有, 严禁传播, 违者自负法律责任!

非卖品, 仅供非商业用途或交流学习使用

版权所有, 严禁传播, 违者自负法律责任!

非卖品, 仅供非商业用途或交流学习使用

版权所有, 严禁传播, 违者自负法律责任!

非卖品, 仅供非商业用途或交流学习使用

版权所有, 严禁传播, 违者自负法律责任!

非卖品, 仅供非商业用途或交流学习使用

版权所有, 严禁传播, 违者自负法律责任!

非卖品, 仅供非商业用途或交流学习使用

版权所有, 严禁传播, 违者自负法律责任!

非卖品, 仅供非商业用途或交流学习使用

版权所有, 严禁传播, 违者自负法律责任!

非卖品, 仅供非商业用途或交流学习使用

版权所有, 严禁传播, 违者自负法律责任!

非卖品, 仅供非商业用途或交流学习使用

版权所有, 严禁传播, 违者自负法律责任!

非卖品, 仅供非商业用途或交流学习使用

版权所有, 严禁传播, 违者自负法律责任!

非卖品, 仅供非商业用途或交流学习使用

版权所有, 严禁传播, 违者自负法律责任!

非卖品, 仅供非商业用途或交流学习使用

版权所有, 严禁传播, 违者自负法律责任!

非卖品, 仅供非商业用途或交流学习使用

版权所有, 严禁传播, 违者自负法律责任!

非卖品, 仅供非商业用途或交流学习使用

版权所有, 严禁传播, 违者自负法律责任!

非卖品, 仅供非商业用途或交流学习使用

版权所有, 严禁传播, 违者自负法律责任!

## 前言

网络技术飞速发展，现在人类已经无法完全离开网络，也无法再忽视网络安全这个问题。我们可以不做黑客，但我们不能不了解如何去防范黑客。

就技术而言，没有什么好坏正邪之分。心思不正的人可以通过黑客技术谋利并满足其私欲，而心思纯正者可以学习网络技术，防黑客于服务器之外，并助人为乐。

网络技术发展非常快，也许今天的黑客技术下周就已经过时了，这是反黑客技术的胜利，但网络技术原理不会过时。也许针对同一漏洞的所有黑客手段都利用了一个原理（最典型的就是 SQL 注入），不同的技术方法只是对同一个原理的不同利用。

网络技术应用广泛，从个人到企业，从学生到工程师……每个人都需要对网络技术有所了解。不一定非得成为专家，但对网络技术原理有所了解才能有效地抵御黑客的攻击。即使一时无法抵御也能大概理解攻击原理，有的放矢地找到抵御方法。

本书共 11 章，前面的 9 章着重介绍了网络工具的选择和互联网攻击原理及过程；后面两章介绍了局域网的攻击。在互联网攻击的示例中选取了网络中流行的靶机 DVWA 进行演示，详细地演示了攻击的过程并阐述了攻击原理。在本书的局域网攻击演示中，使用了常用的软件及简单的方法让读者对网络技术有所了解，对黑客攻击有所防范。

### 本书的写作特点

- 降低网络防范黑客的入门门槛，适合所有中小企业和传统企业
- 为了便于读者理解本书的内容，笔者尽可能选择应用广泛的软件，以网络小白的视角，使用很少的步骤来达到目的。全书内容做到尽可能简单且通俗易懂。
- 罗列常见的攻击手段和防范方法，让网站管理人员都具备基本的保护能力
- 通过简单的实例，详细地说明黑客攻击的原理及过程，让黑客小白学会基本的工具使用，全书包括暴力破解、SQL 注入、命令注入、上传木马、Web 攻击、漏洞检测、潜伏、无线破解、内网攻击等常见的攻防技术。
- Python 编程的简单实现，让网络运维变得更简单
- Python 语言成为目前非常流行的语言，不仅流通广泛，还提供了一大批可用的工具、代码等来对网络进行安全管理，这就使得网络管理人员更容易上手实战。
- 各种黑客工具的原理和原理解析，让人知其然更知道防范于未来
- 如果只会简单的工具使用，不知道黑客的攻击原理，我们就只能防守。为了更好地防范网络攻击，本书对黑客原理的介绍也不惜笔墨，力图让读者举一反三，维护起网络来事半功倍。
- 涉及互联网和局域网，让企业级网管工作更轻松
- 在信息化的社会下，企业对互联网和局域网的使用已经渗透到了方方面面，连打印也都是在局域网内实现的，这个时候我们更应该关注网络的安全。本书的技术点不仅包括互联网这种大方向上的攻防，也包括局域网内的各种安全防范技术。
- 涵盖 Linux&Windows 的知识点
- 全书尽量使用 Linux&Windows 通用的网络攻防软件，让读者无须为操作系统的转换分心。

### 本书面向的读者

- Python 入门读者，可以拿来练手
- 网管，可以用来维护网络安全
- 初级黑客，可以掌握各种网络攻防工具的使用

• IV •

非卖品, 仅供非商业用途或交流学习使用

版权所有, 严禁传播, 违者自负法律责任!

非卖品, 仅供非商业用途或交流学习使用

版权所有, 严禁传播, 违者自负法律责任!

非卖品, 仅供非商业用途或交流学习使用

版权所有, 严禁传播, 违者自负法律责任!

非卖品, 仅供非商业用途或交流学习使用

版权所有, 严禁传播, 违者自负法律责任!

非卖品, 仅供非商业用途或交流学习使用

版权所有, 严禁传播, 违者自负法律责任!





# 目 录

第 1 招 搭建 Python 防范环境	1
1.1 认识黑客	1
1.1.1 黑客的定义	1
1.1.2 黑客守则	2
1.2 基本工具	3
1.2.1 操作系统	3
1.2.2 安装 ConEmu	4
1.2.3 安装 Python	8
1.2.4 安装 Git	16
1.3 安装虚拟机	21
1.3.1 下载 VMware	21
1.3.2 Windows 下安装 VMware Workstation	23
1.3.3 Linux 下安装 VMware Workstation	24
1.4 安装 Docker	28
1.4.1 下载 Docker For Docker	29
1.4.2 Windows 下安装设置 Docker	31
1.4.3 Linux 下安装设置 Docker	35
1.4.4 Docker 使用	37
1.4.5 取消 Docker 服务	43
1.5 防范总结	45



第 2 招 扫描漏洞	46
2.1 系统扫描工具	46
2.1.1 系统漏洞	46
2.1.2 系统扫描	47
2.1.3 工具选择	47
2.2 Nexpose 安装	48
2.2.1 下载 Nexpose	48
2.2.2 Windows 下安装 Nexpose	51
2.2.3 Linux 下安装 Nexpose	55
2.3 Nexpose 扫描	56
2.3.1 激活 Nexpose	56
2.3.2 准备靶机	60
2.3.3 系统扫描	66
2.3.4 漏洞利用	70
2.3.5 系统扫描防范秘籍	77
2.4 防范总结	81
第 3 招 暴力破解的秘密	82
3.1 Web 暴力破解	82
3.1.1 准备靶机 DVWA	82
3.1.2 软件准备——Burp Suite	92
3.1.3 Low 级别的暴力破解	96
3.1.4 Medium 级别的暴力破解	105
3.1.5 High 级别的暴力破解	107
3.1.6 Web 暴力破解防范秘籍	114
3.2 端口暴力破解	115
3.2.1 Nmap 扫描器	115

3.2.2	暴力破解工具 Hydra .....	128
3.2.3	软件准备——Nmap .....	130
3.2.4	软件准备——Hydra .....	133
3.2.5	准备靶机 .....	135
3.2.6	数据库的暴力破解 .....	136
3.2.7	HTTP 的暴力破解 .....	138
3.2.8	端口爆破防范秘籍 .....	140
3.3	E-mail 暴力破解 .....	141
3.3.1	Hydra 破解邮箱 .....	142
3.3.2	Python 破解邮箱 .....	142
3.3.3	邮箱爆破防范秘籍 .....	147
3.4	防范总结 .....	147
<b>第 4 招</b>	<b>防 SQL 注入 .....</b>	<b>148</b>
4.1	SQL 准备 .....	148
4.1.1	准备 MySQL 的 Windows 客户端 .....	149
4.1.2	准备 MySQL 的 Linux 客户端 .....	152
4.1.3	通过客户端连接服务器 .....	153
4.2	SQL 语句 .....	155
4.2.1	创建数据库和表 .....	155
4.2.2	添加、修改、查询数据 .....	158
4.2.3	删除表和数据库 .....	160
4.3	DVWA SQL 注入 .....	162
4.3.1	Low 级别注入 .....	162
4.3.2	Medium 级别注入 .....	169
4.3.3	High 级别注入 .....	174
4.4	使用工具注入 .....	176
4.4.1	SQL 注入工具选择 .....	176





- 4.4.2 Sqlmap 下载安装..... 177
- 4.4.3 Sqlmap 参数..... 179
- 4.4.4 Sqlmap 注入——Low 级别..... 182
- 4.4.5 Sqlmap 注入——Medium 级别..... 187
- 4.4.6 Sqlmap 注入——High 级别..... 188
- 4.4.7 Sqlmap 之 tamper..... 188
- 4.4.8 Sqlmap 防范秘籍..... 189
- 4.5 防范总结..... 190
- 第 5 招 防命令注入..... 191**
  - 5.1 DVWA 命令注入..... 191
    - 5.1.1 Low 级别注入..... 191
    - 5.1.2 Medium 级别注入..... 193
    - 5.1.3 High 级别注入..... 195
    - 5.1.4 命令注入防范秘籍..... 196
  - 5.2 防范总结..... 197
- 第 6 招 看清文件上传木马..... 198**
  - 6.1 木马..... 198
    - 6.1.1 最简单的木马..... 198
    - 6.1.2 小马变形..... 199
    - 6.1.3 大马..... 200
    - 6.1.4 木马连接工具..... 200
  - 6.2 DVWA 上传..... 201
    - 6.2.1 Low 级别上传..... 202
    - 6.2.2 Medium 级别上传..... 203
    - 6.2.3 High 级别上传..... 209





6.2.4	上传木马防范秘籍	212
6.3	防范总结	213
<b>第 7 招</b>	<b>看清 Web 攻击</b>	<b>214</b>
7.1	非特定目标	214
7.1.1	寻找注入点	214
7.1.2	Sqlmap 注入	217
7.1.3	寻找后台	220
7.1.4	钟馗之眼——ZoomEye	221
7.2	特定目标	223
7.2.1	Nmap 扫描	224
7.2.2	搜索公开漏洞	225
7.2.3	社工库	225
7.2.4	防范秘籍	226
7.3	防范总结	227
<b>第 8 招</b>	<b>利用 Python 监测漏洞</b>	<b>228</b>
8.1	Heart Bleed 漏洞	228
8.1.1	Heart Bleed 漏洞简介	228
8.1.2	创建靶机	229
8.1.3	测试靶机	231
8.1.4	Heart Bleed 漏洞防范秘籍	233
8.2	Struts 2 远程代码执行漏洞	235
8.2.1	漏洞简介	235
8.2.2	创建靶机	236
8.2.3	测试靶机	237
8.2.4	Struts2 防范秘籍	238



8.3 防范总结 .....	239
第 9 招 潜伏与 Python 反向连接 .....	240
9.1 清理网络脚印 .....	240
9.1.1 IP 追踪原理 .....	240
9.1.2 Tor 下载——Windows 版 .....	241
9.1.3 Tor 下载——Linux 版 .....	242
9.1.4 Tor 安装配置——Linux 版 .....	243
9.1.5 Tor 安装配置——Windows 版 .....	248
9.1.6 Tor 防范秘籍 .....	252
9.2 反向连接——Netcat .....	253
9.2.1 Windows 服务器的反向连接 .....	253
9.2.2 Linux 服务器的反向连接 .....	258
9.2.3 反向连接使用技巧 .....	264
9.2.4 反向连接防范秘籍 .....	265
9.3 防范总结 .....	265
第 10 招 无线破解 .....	266
10.1 准备工具 .....	266
10.1.1 硬件准备 .....	266
10.1.2 软件准备 .....	267
10.2 aircrack-ng 破解 .....	267
10.2.1 aircrack-ng 说明 .....	268
10.2.2 WEP 破解 .....	270
10.2.3 WPA 破解 .....	278
10.2.4 aircrack-ng 防范秘籍 .....	284
10.3 pin 码破解 .....	286



10.3.1	Reaver 破解原理	286
10.3.2	Reaver 破解	287
10.3.3	pin 码防范秘籍	290
10.4	防范总结	291
第 11 招	内网攻击	292
11.1	嗅探原理	292
11.1.1	数据分发	292
11.1.2	嗅探位置	294
11.1.3	嗅探软件	296
11.1.4	开始嗅探	300
11.2	ARP 欺骗	304
11.2.1	ARP 欺骗原理	304
11.2.2	ARP 欺骗软件	305
11.2.3	安装 Cain	305
11.2.4	Cain 欺骗、嗅探	305
11.3	中间人攻击	312
11.3.1	会话劫持原理	312
11.3.2	获取会话 Cookies	313
11.3.3	注意事项	319
11.3.4	中间人攻击防范秘籍	319
11.4	防范总结	324



# 第 1 招

---

## 搭建 Python 防范环境

黑客，在一般人的印象中都很神秘。他们在网络中攻无不克、战无不胜，似乎无所不能。实际上黑客并没有那么神通广大，黑客技术也没那么复杂，即使是一个网络小白，如果按照科学的方法也可以成为一名合格的黑客。下面就跟随笔者一步步开启各位的黑客之旅吧。

### 1.1 认识黑客

说到了黑客，那就必须先了解什么是黑客？黑客应该做什么？黑客不应该做什么？个人认为，了解这些甚至比学习黑客技术更为重要。

#### 1.1.1 黑客的定义

黑客，原意是指热爱技术、崇尚新技术而又不断创造新技术的人。他们也许是程序员，也许是网络管理员，也许是热爱 DIY 的硬件达人。但他们都有一个共同点，他们热衷于推陈出新，有自己的思想和准则，并不会随意破坏他人的系统，而是热心帮助他人更好、更



安全地维护系统。

随着网络日益发达，学习技术变得越来越容易。虽然还有人愿意尊重黑客精神，并遵守黑客准则，但还是有更多的人肆意妄为，无所顾忌地破坏他人的系统，使黑客这一褒义词渐渐地变成了贬义词。本书的目的并不是告诉读者如何去破坏一个系统，而是让读者重视系统安全，了解黑客一般的攻击方法，更好地防黑客于系统之外。

### 1.1.2 黑客守则

黑客守则的版本很多，但都大同小异。这里选择条目最多的一个版本。毕竟越守规矩的人才会越安全。

(1) 不恶意破坏任何系统。恶意破坏他人的软件将承担法律责任。如果你只是使用电脑，那也为非法使用。

**注意：**千万不要破坏别人的文件或数据。

(2) 不修改任何系统文件，如果你是为了要进入系统而修改它，请在达到目的后将它还原。

(3) 不要轻易地将你要 Hack 的站点告诉你不信任的朋友。

(4) 不要在论坛上谈论关于你 Hack 的任何事情。

(5) 在 Post 文章的时候不要使用真名。

(6) 入侵期间，不要随意离开你的电脑。

(7) 不要入侵或攻击电信或政府机关的主机。

(8) 不在电话中谈论关于你 Hack 的任何事情。

(9) 将你的笔记放在安全的地方。

(10) 读遍有关系统安全或系统漏洞的文件。



(11) 已侵入电脑中的账号不得删除或修改。

(12) 不将你已破解的账号分享给你的朋友。

(13) 不会编程的黑客不是好黑客。

(14) 黑客不同于盗。

(15) 不遵守法则的黑客必将受到谴责。

遵守这些守则，并不只是为了避免伤害别人，更重要的是为了保护自己。当脑中有什么不好想法的时候，请自行搜索破坏计算机信息罪，仔细参考，认真去权衡那样做是否值得。

## 1.2 基本工具

作为一名黑客，顺手的工具是必不可少的。专业的工具暂且放到一边，先来挑选最基本的工具。本书中挑选工具的原则有两点：

- ◎ 首先是发行版本比较新的，比较稳定的，可持续更新的，功能比较单一的软件（个人认为功能单一的软件会比提供很多功能的软件更出色）。
- ◎ 其次会选择能够在各个操作平台通用的软件。
- ◎ 最后尽可能地选择自由软件、免费软件和无须安装的绿色软件。

### 1.2.1 操作系统

目前主流的三大操作系统 Windows、Linux、Mac OS 可以作为黑客平台，配置使用都非常方便。Android 稍加配置也可以（iOS 稍微复杂一点）。本书主要讲解 PC 端，在此仅以 Windows 和 Linux 系统为例。前者是因为使用的人数最多，后者是因为可供使用的软件最多。

Windows 的选项比较少，只有 Windows 7 和 Windows 10（Windows XP 版本太旧）。

最终选择 Windows 10 的理由是版本比较新、功能比较多。Docker 在 Windows 10 上使用更加方便。

Linux 可供选择的版本很多。Linux 中大名鼎鼎的 Kali Linux 当然是最方便的，所有软件都已经安装好了，但 Kali Linux 中安装的软件实在是太多了，简直让人无所适从，所以选择放弃。Ubuntu 做桌面是一个很好的选择，它大量地使用了新技术、新版本的软件，可这里最需要的是稳定，所以也放弃。Fedora、CentOS、RHEL 做服务器很不错，问题是现在不是要做专门的服务器，放弃。Gentoo、LFS 的强大无可置疑，可从使用方便上来说……放弃。还有 SUSE……放弃。

最后的选择是 Debian 8。它强大、稳定、方便、干净，不管是做服务器还是做桌面都能胜任。你可以自己一个个地安装合适的工具，亲手打造一部黑客利器。

## 1.2.2 安装 ConEmu

作为一名黑客，不使用终端简直是不可思议的。太多的软件、太多的命令都需要在终端中完成。Linux Gnome 的终端做得已经很好了，而 Windows 自带的 Cmd 和 Powershell 则略显不足。这里要为 Windows 10 选择一款合适的终端。

Windows 下的终端软件很多，实际上最合适做黑客的终端莫过于 PentestBox。它不仅仅是一款强大的终端应用，而且还包含了很多黑客软件，其中就包含了最常用的 Metasploit 框架。PentestBox 使用起来虽然方便，却少了 DIY 的乐趣和成就感。最终只选择了 PentestBox 中使用的终端 ConEmu。以后再慢慢地添加其他的黑客软件，做出一个合手的简配版 PentestBox，亲手打造自己的黑客工具。

ConEmu 本身就是一款强大的终端。它默认将 Windows 自带的 Cmd 和 Powershell 整合到了一起，稍加熟悉其功能后，就可以配置出非常强大的终端工具。

### 1. 下载 ConEmu

ConEmu 的官网是 <http://conemu.github.io>。进入 ConEmu 的官网后，单击 Download 图标，直接进入下载页面，如图 1-1 所示。



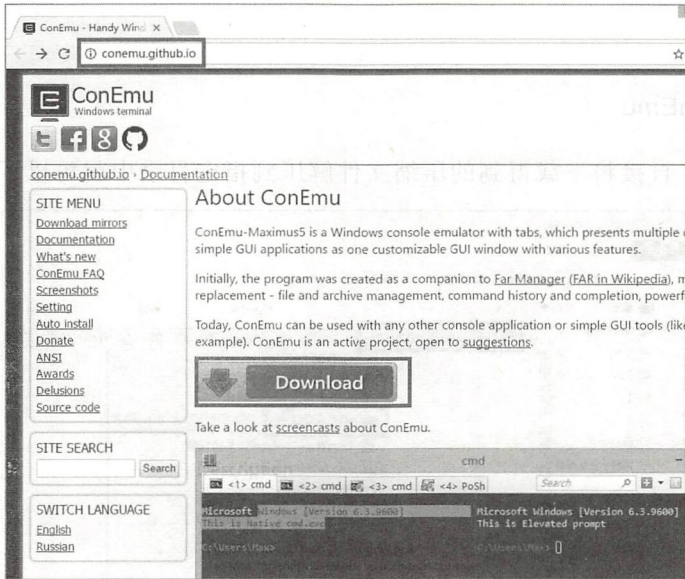


图 1-1 ConEmu 官网

进入下载页面，挑选合适的版本下载即可，如图 1-2 所示。

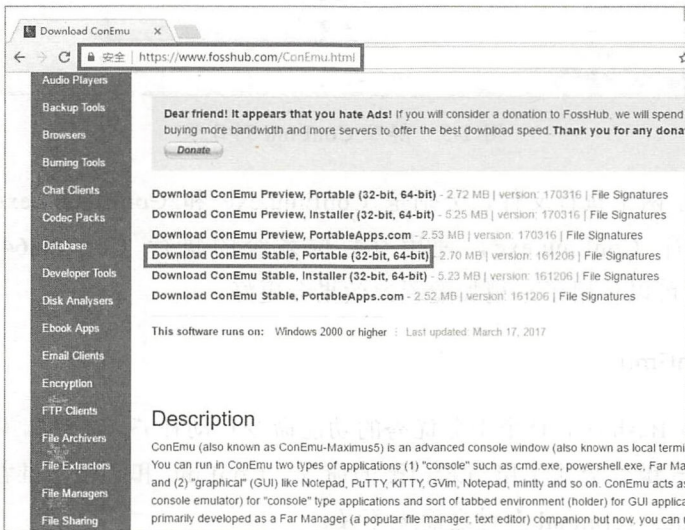


图 1-2 下载 ConEmu

建议选择稳定的免安装版。预览版本也许会有惊喜，可工具不是越强大越好，而是越

稳定越好。

## 2. 安装 ConEmu

下载完成后，直接将下载得到的压缩文件解压到指定目录中就可以了，如图 1-3 所示。



图 1-3 解压 ConEmu 到目录

解压后得到了两个执行文件，分别是 ConEmu.exe 和 ConEmu64.exe。很明显，使用 32 位系统的执行 ConEmu.exe，使用 64 位系统的执行 ConEmu64.exe。现在双击 ConEmu64.exe 就可以使用了。稍加配置，效果会更好。

## 3. 配置 ConEmu

在使用 Linux Bash 时，有个十分优秀的功能命令自动补齐。在终端中输入命令的前几个字母，单击 Tab 键就会显示出与之相配的命令。ConEmu 和它强烈推荐插件 Clink 配合后功能上比 Linux Terminal 有过之而无不及。

打开 ConEmu 目录下的 ConEmu\clink\Readme.txt 文件，如图 1-4 所示。

按照 ReadMe 的提示，在 <http://mridgers.github.io/clink/> 下载 clink 的 Portable 版本，目



前最新版本是 Clink\_0.4.8.zip，并将压缩文件解压后，将所有文件都复制到 ConEmu/ConEmu/clink 目录下，如图 1-5 所示。

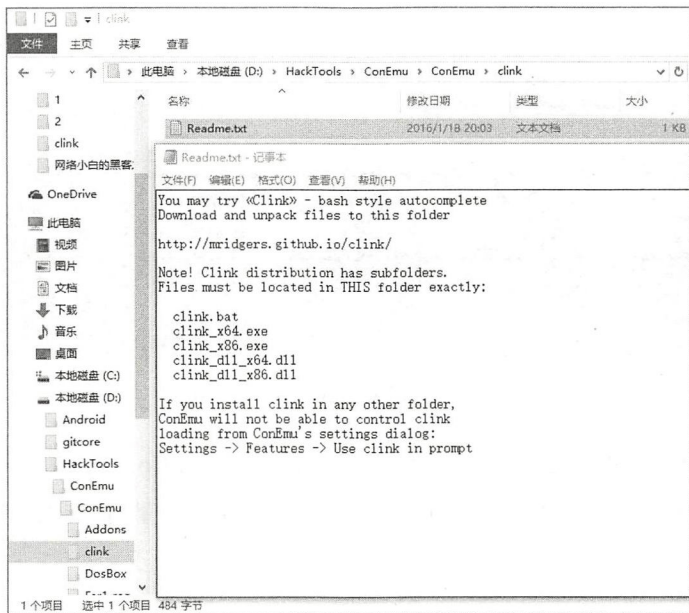


图 1-4 Clink ReadMe

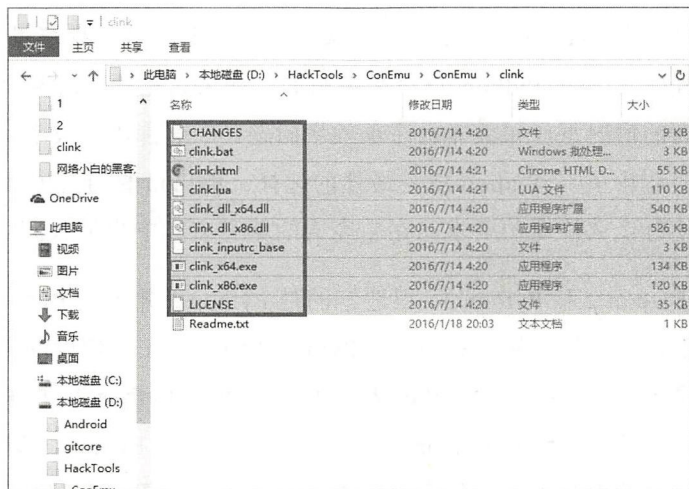


图 1-5 载入 Clink

ConEmu 默认载入 Clink，将 Clink 文件复制到 ConEmu 的目录下，无须设置，即可使用。双击 ConEmu64.exe，执行 ConEmu，如图 1-6 所示。

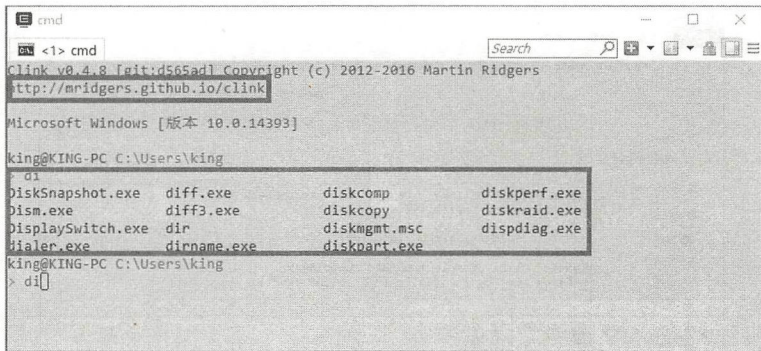


图 1-6 ConEmu&Clink 执行效果

显示已经载入 Clink，命令补齐功能正常。暂时只添加 ConEmu 默认的 Clink，以后还可以添加其他的软件，集成到 ConEmu 中，将它打造成一款量身定做的黑客工具。

### 1.2.3 安装 Python

如今在脚本语言中 Python 可谓是火得一塌糊涂，互联网中处处可见 Python 的身影，许多黑客自编的程序都是用 Python 语言来编写的。如果只是要实现某个功能，在对执行效率要求不那么高的情况下（如果非常注重效率问题，C 语言才是效率之王，只要能忍受一遍又一遍重复的造轮子），Python 就是最佳的选择。Python 标准库基本上可以应付绝大多数的情况。即使有什么特殊的要求，在它庞大的第三方库中也能找到合适的方法。

Python 分为 Python 2 和 Python 3。很遗憾的是 Python 3 并不是 Python 2 的 Plus 版本。它们之间略有区别，并不能直接互相通用。Python 2 的优势在于使用的人数较多，已经形成了成熟的生态系统，很多强大的 Python 框架使用的都是 Python 2，框架使用的第三方库也是用的 Python 2，整体升级到 Python 3 暂时还有困难。而 Python 3 却代表着 Python 的发展方向，目前使用的人数虽少，但潜力巨大。那么，别再权衡，都装上吧。

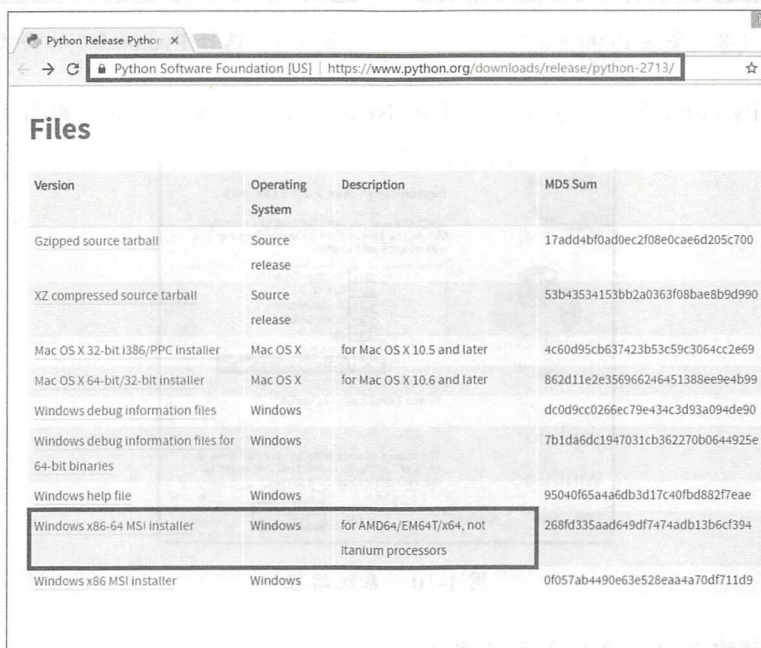
Debian 8 默认安装了 Python 2 和 Python 3。所以只需要在 Windows 下安装 Python 2



和 Python 3 就可以了。Python 的官网是 <https://www.python.org>，上面有详细的说明和示例，英语不错的可以自行参考。英语不好的也没关系，Python 在国内已经流行很多年了，专门讲解 Python 的网站也不少，可以自行搜索学习。强烈建议学好 Python 语言，熟练使用 Python 会使黑客之路顺畅很多。

## 1. Python 2 安装配置

Python 2 的最新版本是 Python2.7.13。在官网的下载地址是 <https://www.python.org/downloads/release/python-2713/>。选择与系统符合的版本下载软件，如图 1-7 所示。



The screenshot shows a web browser window displaying the Python 2.7.13 download page. The page title is "Files" and the URL is "https://www.python.org/downloads/release/python-2713/". A table lists various download options for different operating systems and architectures. The "Windows x86-64 MSI installer" row is highlighted with a black box.

Version	Operating System	Description	MD5 Sum
Gzipped source tarball	Source release		17add4bf0ad0ec2f08e0cae6d205c700
XZ compressed source tarball	Source release		53b43534153bb2a0363f08bae8b9d990
Mac OS X 32-bit i386/PPC installer	Mac OS X	for Mac OS X 10.5 and later	4c60d95cb637423b53c59c3064cc2e69
Mac OS X 64-bit/32-bit installer	Mac OS X	for Mac OS X 10.6 and later	862d11e2e356966246451388ee9e4b99
Windows debug information files	Windows		dc0d9cc0266ec79e434c3d93a094de90
Windows debug information files for 64-bit binaries	Windows		7b1da6dc1947031cb362270b0644925e
Windows help file	Windows		95040f65a4a6db3d17c40fbd882f7eae
Windows x86-64 MSI installer	Windows	for AMD64/EM64T/x64, not Itanium processors	268fd335aad649df7474adb13b6cf394
Windows x86 MSI installer	Windows		0f057ab4490e63e528ea4a70df711d9

图 1-7 下载 Python 2.7

(1) 双击下载得到的 Python 2 安装程序，如图 1-8 所示。

(2) 单击 Next 按钮，进入下一步，如图 1-9 所示。