信息安全培训用书

信息安全培训教程

（实验篇）

XINXI ANQUAN
PEIXUN JIAOCHENG

李剑　编著

内附光盘

北京邮电大学出版社
www.buptpress.com

信息安全 培训用书

信息安全培训教程

（实验篇）

李 剑 编著

北京邮电大学出版社
·北京·

内 容 简 介

本书的作者以在全国进行的100多期信息安全培训经验为基础，与《信息安全培训教程(原理篇)》一起构成了一套完整的信息安全培训教程。

书中介绍了信息安全培训过程中常用到的15个实验。学员可以现场实习操作。全书共分为4个部分。第一部分为密码学实验，包括1个实验：PGP软件的使用。第二部分为黑客攻击实验，包括8个实验：Sniffer网络分析器的使用、SuperScan网络端口扫描的使用、流光综合扫描及安全评估的使用、Shadow Security Scanner扫描器的使用、DoS/DDoS攻击(包括CC攻击)的使用、黑雨邮箱密码破解器的使用、冰河木马的使用、LC5账户口令破解的使用。第三部分为网络层安全实验，包括3个实验：个人防火墙的使用、虚拟专用网VPN技术、入侵检测技术Snort的配置。第四部分为应用层安全实验，包括3个实验：文件恢复工具EasyRecovery的使用、奇虎360安全卫士的使用、Windows下的Web和FTP服务器安全配置。

本书适合于各企事业单位普通计算机使用者进行信息安全方面的培训。

图书在版编目(CIP)数据

信息安全培训教程(实验篇)/李剑编著. —北京：北京邮电大学出版社，2008

ISBN 978-7-5635-1564-6

Ⅰ.信… Ⅱ.李… Ⅲ.信息系统—安全技术—技术培训—教材 Ⅳ.TP309

中国版本图书馆CIP数据核字(2007)第175707号

书　　名：信息安全培训教程(实验篇)

编　　著：李　剑

责任编辑：崔　珞

出版发行：北京邮电大学出版社

社　　址：北京市海淀区西土城路10号(邮编：100876)

发 行 部：电话：010-62282185　传真：010-62283578

E-mail：publish@bupt.edu.cn

经　　销：各地新华书店

印　　刷：北京忠信诚胶印厂

开　　本：787 mm×1 092 mm

印　　张：11.75

字　　数：273千字

印　　数：1—3 000册

版　　次：2008年1月第1版　2008年1月第1次印刷

ISBN 978-7-5635-1564-6　　定　价：22.00元

前　言

根据 CNNIC 在 2007 年 1 月的第 19 次中国互联网络发展状况统计报告统计，中国互联网网民总人数为 13 700 万人，其中仅有 8.4%的网民对于网络内容的健康性非常满意。也就是说，有 91.6%的网民(12 550 万人)都或多或少对于网络的安全性不满意。想必有许多人对于“CIH”、“震荡波”、“冲击波”等病毒的“威力”还心有余悸；还有人在为自己电脑上的“流氓软件”头痛不已；甚至有人因为不小心泄露单位重要机密信息而身陷囹圄。

为了解决这些问题，达到“普及信息安全知识”这一目的，作者以在全国进行的 100 多期信息安全培训经验为基础，编写了《信息安全培训教程(原理篇)》和《信息安全培训教程(实验篇)》这两本书。本书中包含了普通计算机使用者在使用计算机的时候经常要用的一些安全工具的使用方法。适合各企事业单位的员工进行信息安全方面的培训。在讲解时，可以根据所要教的学员对象来选择要教的内容以及内容的深度。对于那些没有学过计算机网络课程的学员，可以在课前适当加一些计算机网络的知识。

本书内容全面，介绍了信息安全培训过程中用到的 15 个实验。学员可以现场实习操作。全书共分为 4 个部分。

第一部分为密码学实验，包括 1 个实验：实验 1 PGP 软件的使用。在这个实验中可以学习到通过公钥和私钥对文件、邮件等进行加解密，还可以对文件进行粉碎，对整个电脑磁盘进行加解密等。

第二部分为黑客攻击实验，包括 8 个实验：实验 2 Sniffer 网络分析器，讲述如何使用 Sniffer 软件对局域网内的数据包进行捕获；实验 3 SuperScan 网络端口扫描，讲述了采用 SuperScan 软件对于网络上的计算机进行端口扫描的方法；实验 4 流光综合扫描及安全评估，讲述了如何使用流光软件对计算机进行综合安全扫描的方法；实验 5 Shadow Security Scanner 扫描器，讲述了使用国外著名软件 Shadow Security Scanner 对计算机进行安全扫描评估的方法；实验 6 DoS/DDoS 攻击(包括 CC 攻击)，讲述了常用的几种拒绝服务攻击的方法，如 Land、CC 攻击等；实验 7 黑雨邮箱密码破解器的使用，讲述了如何使用黑雨软件对 Pop3 邮箱进行密码破解；实验 8 冰河木马的使用，通过对于冰河木马的操作，熟悉木马的工作原理；实验 9 LC5 账户口令破解，本实验通过 LC5 账户口令破解软件的使用，来测试密码的安全性。

第三部分为网络层安全实验，包括 3 个实验：实验 10 个人防火墙的使用，通过对 Norton 防火墙的使用，掌握如何使用防火墙来封堵恶意的端口和 IP；实验 11 VPN 技术，

通过在 Windows 2000 服务器上配置 VPN，来了解 VPN 技术在 Windows 2000 上的配置方法；实验 12 入侵检测技术 Snort 的配置，通过配置免费软件 Snort 来掌握入侵检测技术的工作原理。

第四部分为应用层安全实验，包括 3 个实验：实验 13 文件恢复工具 EasyRecovery，通过使用软件 EasyRecovery 来学习电脑文件在误删除的情况下如何进行恢复；实验 14 奇虎 360 安全卫士的使用，通过使用奇虎 360 安全卫士软件来清除电脑恶意软件，并对电脑操作系统漏洞打补丁；实验 15 Windows 下的 Web、FTP 服务器安全，通过对 IIS 的安全配置以及 IIS Lockdown 软件的使用来对 Windows 下的 Web、FTP 服务器进行安全配置。

完整的信息安全实验还应该包括操作系统层安全实验。关于这一部分实验已经在《信息安全培训教程(原理篇)》中进行了讲述，这里不再赘述。

感谢北京邮电大学信息安全中心杨义先教授、钮心忻教授、罗群副教授、徐国爱副教授、张茹副教授、崔宝江副教授、谷利泽副教授、李辉副教授、周亚健博士、马兆丰博士、辛阳博士、郑康峰博士、李丽香博士、杨榆博士、张淼博士、黄正权博士、郑世慧博士、王励诚博士等，他们对本书的出版提出了宝贵的意见和建议。感谢我的博士导师北京理工大学的曹元大教授，曹老师对于本书的出版给予了极大的支持与帮助。感谢中国电信研究院的赵阳博士、中国移动公司的冯玉波博士、西门子(中国)有限公司的李明柱博士、中科院计算技术研究所的谭建龙博士、北京交通大学的姚正林博士，他们对本书的出版给予了很大的支持。其他参与本书审阅编写等工作的还有景博、景绍达、白小梅、李胜斌、陈艳霞等，这里一并感谢！

本教材也是国家信息产业部重点软课题项目“基于互联网内容安全的关键问题研究”(课题编号：2007-R-103)资助的成果。

由于本书作者水平有限，书中疏漏与错误之处在所难免，恳请广大同行和读者指正。

李　剑

北京邮电大学信息安全中心

目 录

第 1 部分 密码学实验

第 2 部分 黑客攻击实验

第 3 部分 网络层安全实验

第 4 部分 应用层安全实验

第1部分 密码学实验

这一部分讲述密码学的一个具体应用，即PGP（Pretty Good Privacy）软件的使用。在这个实验中可以学习到通过公钥和私钥对文件、邮件等进行加解密，还可以对文件进行粉碎，对整个电脑磁盘进行加解密等。

实验1 PGP软件的使用

PGP是一个基于RSA公匙加密体系的加密软件。通过使用PGP,可以了解邮件加密、文件加密、文件粉碎等很多功能。

1.1 概　　述

1.1.1 PGP概述

使用PGP可以对邮件保密以防止非授权者阅读,它还能对邮件加上数字签名从而使收信人可以确信邮件是谁发来的。它可以安全地和从未见过的人们通信,事先并不需要任何保密的渠道用来传递密匙。它采用了审慎的密匙管理,一种RSA和传统加密的杂合算法,用于数字签名的邮件文摘算法,加密前压缩等,还有一个良好的人机界面设计。它的功能强大,有很快的速度,而且它的源代码是免费的。

1.1.2 实验目的

通过本实验,掌握如何使用PGP软件进行邮件加密、解密,文件的加密、解密以及文件的粉碎等。

1.1.3 实验环境

这里采用一台安装有Windows 98/2000/2003/XP操作系统的计算机进行实验。
实验中的软件PGP 8.1、注册码及其汉化工具都储存在光盘中。
另外,在所使用的计算机上,必须安装有软件Outlook Express来接收和发送邮件。

1.2 PGP的安装

下面说明一下PGP在安装时应该注意的事项。在光盘里选择PGP8.exe后,用鼠标

双击，开始安装。

1.2.1 安装注意事项

第 1 步：

在安装时会出现如图 1.1 所示的界面。有两个选择：① Yes，I already have keyrings；② No，I'm a New User。如果用户是新用户，那么请选择后者。

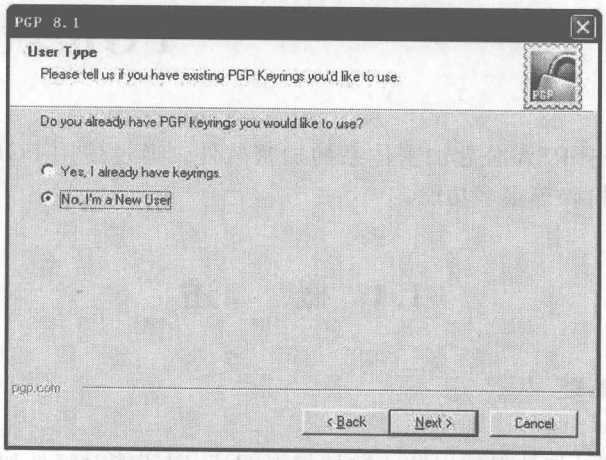

图 1.1 选择用户类型界面

单击“Next”按钮。按照提示，一步步完成安装。最后系统要求重新启动计算机。重新启动后，电脑屏幕的右下角任务栏上会出现一个金黄色的“小锁”。这个“小锁”就是 PGP 的标志。

1.2.2 PGP 的注册

第 2 步：

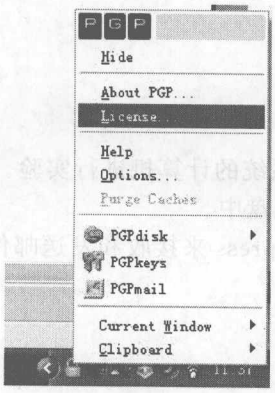

图 1.2 选择注册菜单

右键单击“小锁”，如图 1.2 所示，选择“License...”选项，进行注册。

第 3 步：

选择“License...”选项之后，将出现如图 1.3 所示的 PGP 注册界面。

第 4 步：

选择“Manual”按钮，将出现如图 1.4 所示的界面，进行手动注册。

PGP 手动注册，注册码分为 4 个部分，分别如下所示：(注册码请参考软件附赠光盘)

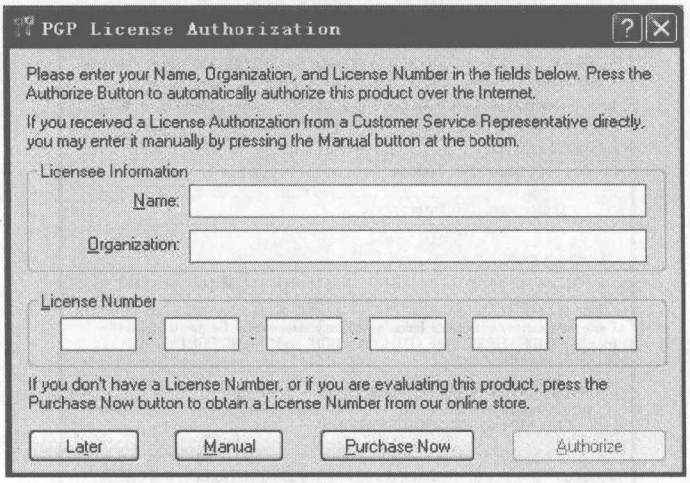

图 1.3 PGP 注册界面

图 1.4 手动注册 PGP

Name: PGP Desktop

Organization: PGP Enterprise

License Number: CUCDX-4YGY5-KRJVJ-TBN6R-3E9UB-EMC

License Authorization:

-----BEGIN PGP LICENSE AUTHORIZATION-----

ADIAApAAAJ4gWeOov9Nr/gJ1TaVQz2olNEx1zACggvH4tuOArH1Swb22sB9Nmx7YC6w =

-----END PGP LICENSE AUTHORIZATION-----

第 5 步：

输入上面的注册码，如图 1.5 所示，选择“Authorize”进行注册授权。

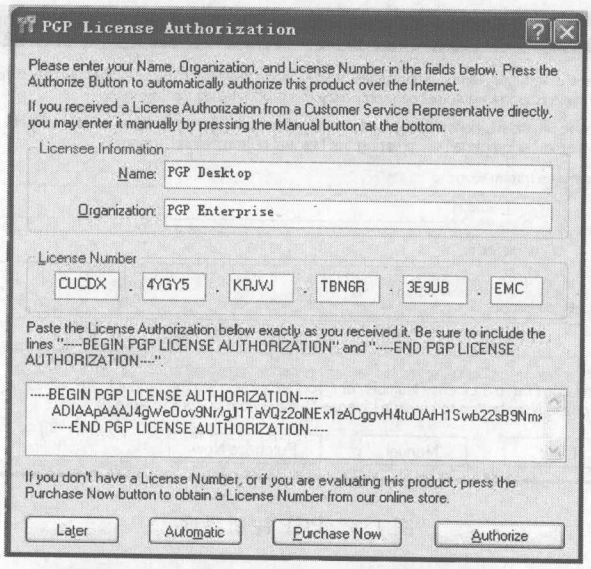

图 1.5　注册授权界面

这时，系统将出现如图 1.6 所示的界面，表示系统已经注册成功。

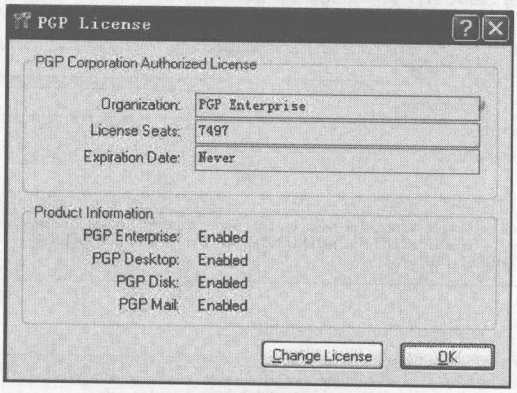

图 1.6　注册成功界面

1.2.3　PGP 的汉化

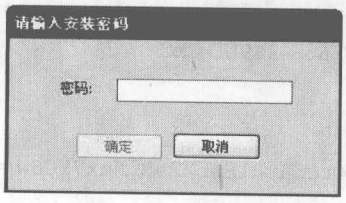

图 1.7　输入汉化密码界面

第 6 步：

用鼠标双击光盘中的可执行文件 pgp81_cns_v2.exe，将出现如图 1.7 所示的界面。这时汉化软件让输入密码。

这时输入汉化的密码“pgp.com.cn”。按照提示，一步步进行安装。安装完后，重新启动计算机就可以使用了。

1.2.4 使用前的设置

第7步：

右键单击“小锁”，选择“选项”菜单，如图1.8所示。这时出现如图1.9所示的界面。

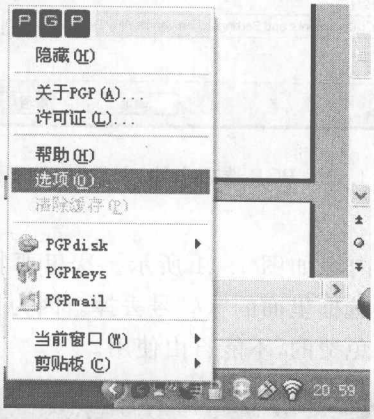

图1.8 PGP选项

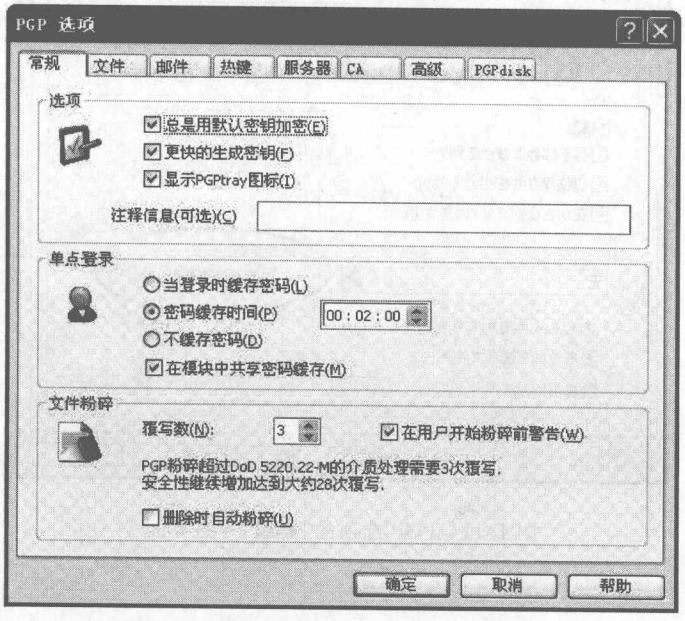

图1.9 PGP选项界面

第8步：

这时，可以看到PGP选项中包含常规、文件、邮件、热键、服务器、CA、高级和PGPdisk 8个标签。可以根据自己的实际要求选择相应的选项进行设置。这里重点介绍“文件”和“高级”两个标签。“文件”标签如图1.10所示。“文件”标签里面有两个内容，分别