计算机系列教材

网络安全综合实践教程

蒲晓川 成爱民 阮清强 唐晔 林朝晖 编著

清华大学出版社

计算机系列教材

蒲晓川 成爱民 阮清强 唐晔 林朝晖 编著

网络安全综合实践教程

清华大学出版社
北 京

内 容 简 介

实践教学是巩固基本理论和基础知识、提高学生分析问题和解决问题能力的有效途径，是应用型本科院校培养具有创新意识的高素质应用型人才的重要环节。

本实验课程属于专业教育课程，授课对象为掌握一定网络安全技术原理、密码技术和计算机网络技术等的学生。本实验课程的开设对于锻炼学生的网络安全综合保障技能，提高分析解决实际问题的能力，在掌握基本技能的基础上提高应用创新等方面的能力有重要影响。

网络安全包括操作系统安全、数据库安全、网络安全、病毒防护、访问控制、加密与鉴别 7 个方面。本书按照该原则组织实验项目。

本实验课程中所有的实验项目都在实验室展开，不在互联网中进行，遵守国家法律，不会危及互联网的安全。

图书在版编目(CIP)数据

网络安全综合实践教程/蒲晓川等编著. --北京：清华大学出版社，2016
计算机系列教材
ISBN 978-7-302-42495-6

Ⅰ. ①网…　Ⅱ. ①蒲…　Ⅲ. ①计算机网络－安全技术－教材　Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2015)第 316463 号

责任编辑：白立军　王冰飞
封面设计：常雪影
责任校对：李建庄
责任印制：何　芊

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　**邮　　编**：100084
社 总 机：010-62770175　　**邮　　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课件下载：http://www.tup.com.cn，010-62795954
印 刷 者：三河市君旺印务有限公司
装 订 者：三河市新茂装订有限公司
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　张**：10.75　　**字　　数**：265 千字
版　　次：2016 年 3 月第 1 版　　**印　　次**：2016 年 3 月第1 次印刷
印　　数：1～2000
定　　价：25.00 元

产品编号：066982-01

《网络安全综合实践教程》前言

本实验课程属于专业教育课程，授课对象为掌握一定网络安全技术原理、密码技术和计算机网络技术等的学生。本实验课程的开设对于锻炼学生的信息安全综合保障技能，提高分析解决实际问题的能力，在掌握基本技能的基础上提高应用创新等方面的能力，有重要影响。

在完成该实验课程的学习后，应能够达到了解信息安全的体系结构和基本内容，了解信息安全的实体安全和运行安全，掌握和运用基本的信息安全技术，能够综合分析信息安全事件，解决信息安全问题，做好信息安全保障等要求。

信息安全的研究范畴目前还没有一个统一的定义。按照“计算机信息系统安全专用产品分类原则(GA 163—1997)”，信息安全产品分为实体安全、运行安全和信息安全 3 个方面。其中，实体安全包括环境安全、设备安全和媒体安全 3 个方面；运行安全包括风险分析、审计跟踪、备份与恢复、应急 4 个方面；信息安全包括操作系统安全、数据库安全、网络安全、病毒防护、访问控制、加密与鉴别 7 个方面。本书就是按照这个原则组织实验项目的。

本实验课程的前期课程包括计算机网络、网络安全技术、反病毒技术、网络攻防对抗实验、军事理论与信息对抗等。

本书由蒲晓川确定研究内容和整体结构，其中，3.1 节、3.9 节由成爱民编写，其他章节由蒲晓川编写。

由于时间紧、任务重，本书难免存在一些问题，望广大师生给予批评指正。

作　者

2016 年 2 月

EDITORS

《网络安全综合实践教程》 目 录

第1章 概 述

1.1 课程简介

21世纪是一个以网络为核心的信息时代。世界经济正在从工业经济向知识经济转变，知识经济的两个重要特征就是信息化和全球化。信息化已经成为当今世界经济和社会发展的趋势，这种趋势主要表现在：①信息技术突飞猛进，成为新技术革命的领头羊；②信息产业高速发展，成为经济发展的强大推动力；③信息网络迅速崛起，成为社会和经济活动的重要依托。信息比例的加大使得社会对信息的真实程度、保密程度的要求不断提高，而网络化又使因虚假、泄密引起的信息危害程度呈指数增大。针对信息的有意刺探、攻击行为更是国家、单位重点防护的事件。

全球信息安全的形势严峻。针对信息的保护与反保护等行为一直伴随着信息的整个发展历程。进入21世纪后，信息安全面临着更严峻的考验。国内外的网络信息安全事件主要表现在系统的安全漏洞不断增加、黑客攻击搅得全球不安、计算机病毒肆虐、网站仿冒、木马和后门程序泄露秘密、信息战阴影威胁数字化和平和白领犯罪造成巨大商业损失等。

在完成本实验课程的学习后，能够达到了解信息安全的体系结构和基本内容，了解信息安全的实体安全和运行安全，掌握和运用基本的信息安全技术，能够综合分析信息安全事件，解决信息安全问题，做好信息安全保障等要求。

本实验课程中的所有实验项目都在实验室展开，不会危及互联网的安全。

目前，还没有现成的网络安全对抗实验教材供我们参考，编者经过认真研究和调查分析，结合我校学生的具体情况，特制定该课程的实验体系，如表1-1-1所示。信息安全的研究范畴目前还没有一个统一的定义。按照“计算机信息系统安全专用产品分类原则(GA 163—1997)”，信息安全产品分为实体安全、运行安全和信息安全3个方面。其中，实体安全包括环境安全、设备安全和媒体安全3个方面；运行安全包括风险分析、审计跟踪、备份与恢复、应急4个方面；信息安全包括操作系统安全、数据库安全、网络安全、病毒防护、访问控制、加密与鉴别7个方面。本“信息安全综合实验”课程就是按照这个原则组织实验项目的。

表1-1-1 《信息安全综合实验》实验体系

序号	实 验 题 目	实验类型	实验学时	选择要求
1	剩磁效应与数据恢复	验证型	2	必选
2	操作系统安全评估与检测	综合型	4	必选
3	数据加密与鉴别	综合型	8	必选
4	数据库安全	综合型	4	课外自选
5	网络安全通信	综合型	4	必选

续表

序号	实验题目	实验类型	实验学时	选择要求
6	数字证书服务及加密认证	综合型	8	必选
7	访问控制和网络防火墙	综合型	8	必选
8	入侵检测	综合型	4	必选
9	Internet 服务器安全	综合型	4	必选
10	网络安全程序设计	设计型	8	课外自选
11	应用程序保护	设计型	4	课外自选
12	网络监控与协议分析	综合型	4	必选
13	风险分析	设计型	2	课外自选
14	安全审计与追踪	综合型	4	课外自选
15	应急响应与灾难恢复	设计型	4	课外自选

1.2 实验类型

实验的分类方法很多，按性质可分为验证型实验、设计型实验和综合型实验 3 种类型。

1. 验证型实验

验证型实验作为一种重要的实验形式，无论在科学研究中还是科学教育中，都是不可或缺的，其作用也是任何其他类型的实验所无法替代的。验证型实验主要培养学生对设备、开发工具的操作能力，加深对理论的理解。实际上，与课程相关的大部分实验都是验证型实验。实验设计者给出较为详细的实验步骤，旨在减少实验者摸索的过程，争取在较短的时间内掌握基本的操作技术。

验证型实验的方法：

(1) 明确实验题目、实验目的和实验要求；

(2) 熟悉实验背景知识；

(3) 按照实验内容进行实验；

(4) 分析实验结果，完成实验报告。

2. 设计型实验

设计型实验培养学生的设计能力和独立工作的能力。这类实验是课程中较大的实验。也就是在基本训练的基础上，提出一些有利于启发思维、有应用价值的实验课题，让学生进行设计型实验。题目描述以提出任务、要求和阐述应用背景为宜，而如何解决问题，解决问题的原理、方法和所用仪器等由同学们自行提出并实践，目的是使学生运用所学的理论知识和实验技能，在实验方法的考虑、使用工具的选择、测试方法的确定等方面受到比较系统的训练。

设计型实验的方法：

(1) 了解题目要求，明确任务；

(2) 查阅有关资料，画出必要的原理图，寻求各种解决问题的方法。从原理、方法和使用工具等多方面提出完成课题任务的依据及实验步骤；

(3) 设计并实现设计内容；

(4) 测试结果评价，总结分析并完成实验报告。

3. 综合型实验

综合型实验是指实验内容涉及本课程的综合知识或与本课程相关课程的知识的实验，其主要教学目的是培养学生综合运用知识分析、解决实际问题的能力以及创新能力。

综合型实验的方法：

(1) 了解题目要求，明确实验任务；

(2) 根据已经掌握内容，查阅有关资料，综合利用各种方法、工具策略等完成实验；

(3) 分析实验结果，总结并完成实验报告。

第2章 实验要求

2.1 实验过程要求

在实验过程中，实验者必须服从指导教师和实验室工作人员的安排，遵守纪律与实验制度，爱护设备及卫生。在指定的实验时间内，必须到机房内实验，其余时间可自行设计和分析。

由于实验时间有限，要求提前预习实验内容，对于一些基本概念不再进行详细解释说明，实验课程授课的理论部分重点放在实验方法分析方面。

(1) 验证型实验：实验前，预习实验，了解实验背景。按照实验指导书的方法步骤进行实验，将实验结果与理论分析结果进行比较，得出结论，按要求写出实验报告。注意掌握基本的实验方法。

(2) 设计型实验：严格要求自己，自信但不固执，独立完成设计任务，善于接受指导教师的指导和听取同学的意见，有意识地树立严谨的科学作风，要独立思考，刻苦钻研，勇于创新，按时完成设计任务。

(3) 综合型实验：要充分发挥主动性和创造性，要求综合运用所掌握的知识，完成实验任务。按照指导书要求的实验任务，完成实验方案论证与设计、实验过程和实验报告。

2.2 考核及评分标准

本课程采用结构化评分，其中，验证型实验占 40%，综合型、设计型实验 45%，其他 15%(主要由指导教师根据考勤、课程表现等把握)。验证型实验、设计型实验和综合型实验主要考核指标如下。

(1) 验证型实验：实验者是否真实、认真地完成了本次实验；实验代码是否规范、可读性怎样、效率怎样；实验报告格式是否规范，是否有抄袭行为等。

(2) 设计型实验：设计代码是否调试通过、运行结果是否正确，是否具备良好可读性；设计报告是否层次清楚、整洁规范、有无相互抄袭情况。答辩分为自述和教师提问两部分，自述时间不得超过 5 分钟，内容包括演示、描述本课题设计思想、关键代码分析等。

(3) 综合型实验：实验者对所学知识的综合运用情况、综合分析情况；实验报告是否层次清楚、整洁规范、有无相互抄袭情况。答辩分为自述和教师提问两部分，自述时间不得超过 5 分钟，内容包括对于本实验目的的理解、实施方案、实验结果情况及分析等。

第3章 实验内容

3.1 数据恢复

3.1.1 实验类型

验证型，2学时，必选实验。

3.1.2 实验目的

计算机磁盘属于磁介质，所有磁介质都存在剩磁效应的问题，保存在磁介质中的信息会使磁介质不同程度地永久性磁化，所以磁介质上记载的信息在一定程度上是抹除不净的，通过一定的技术手段可以将已抹除信息的磁盘上的原有信息提取出来。

另外，由于计算机文件系统的实现原理，文件的删除并没有将文件的数据内容从磁盘上删除，通过一定的技术手段可以将删除的文件恢复出来。

通过该实验，使学生认识到电磁泄露现象引起的数据恢复、硬件损坏、文件删除等实现数据恢复的内容。

3.1.3 题目描述

使用数据恢复软件 EasyRecovery 进行文件恢复。

3.1.4 实验要求

理解磁盘数据恢复的原理，认识数据恢复技术对信息安全的影响。能够使用数据恢复软件 EasyRecovery 进行文件恢复。

提高要求：能够对磁盘数据进行彻底清除。

3.1.5 相关知识

1. 剩磁效应

计算机主机及其附属电子设备，如视频显示终端、打印机等，在工作时不可避免地会产生电磁波辐射，这些辐射中携带有计算机正在进行处理的数据信息。尤其是显示器，由于显示的信息是给人阅读的，是不加任何保密措施的，所以其产生的辐射是最容易造成泄

密的。使用专门的接收设备将这些电磁辐射接收下来，经过处理，就可恢复还原出原信息。

国外对计算机设备的辐射问题早已有研究，在1967年的计算机年会上美国科学家韦尔博士发表了阐述计算机系统脆弱性的论文，总结了计算机4个方面的脆弱性，即处理器的辐射、通信线路的辐射、转换设备的辐射和输出设备的辐射。这是最早发表的研究计算机辐射安全的论文，但当时没有引起人们的注意。1983年，瑞典的一位科学家发表了一本名叫《泄密的计算机》的小册子，其中再次提到计算机的辐射泄露问题。1985年，荷兰学者艾克在第三届计算机通信安全防护大会上公开发表了他的有关计算机视频显示单元电磁辐射的研究报告，同时在现场做了用一台黑白电视机接收计算机辐射泄露信号的演示。他的报告在国际上引起强烈反响，从此人们开始认真对待这个问题。据有关报道，国外已研制出能在一千米之外接收还原计算机电磁辐射信息的设备，这种信息泄露的途径使敌对者能及时、准确、广泛、连续而且隐蔽地获取情报。计算机电磁辐射泄密问题已经引起了各个国家的高度重视，要防止机密信息被窃取，必须采取防护和抑制电磁辐射泄密的专门技术措施，这方面的技术措施有干扰技术、屏蔽技术和Tempest技术。

计算机磁盘属于磁介质，所有磁介质都存在剩磁效应的问题，保存在磁介质中的信息会使磁介质不同程度地永久性磁化，所以磁介质上记载的信息在一定程度上是抹除不净的，使用高灵敏度的磁头和放大器可以将已抹除信息的磁盘上的原有信息提取出来。据一些资料的介绍，即使磁盘已改写了12次，但第一次写入的信息仍有可能复原出来。这使涉密和重要磁介质的管理以及废弃磁介质的处理都成为很重要的问题。国外有的甚至规定记录绝密信息资料的磁盘只准用一次，用后必须销毁，不准抹后重录。

2. 文件删除原理

存储在硬盘中的每个文件都可分为两部分：文件头和存储数据的数据区。文件头用来记录文件名、文件属性、占用簇号等信息。文件头保存在一个簇并映射在FAT表(文件分配表)中，而真实的数据则是保存在数据区当中的。平常所做的删除，其实是修改文件头的前两个代码，这种修改映射在FAT表中，就为文件做了删除标记，并将文件所占簇号在FAT表中的登记项清零，表示释放空间，这也就是平常删除文件后，硬盘空间增大的原因。而真正的文件内容仍保存在数据区中，并未得以删除。要等到以后的数据写入，把此数据区覆盖掉，才算是彻底把原来的数据删除。如果不被后来保存的数据覆盖，它就不会从磁盘上抹掉。用Fdisk分区和Format格式化和文件的删除类似，只是前者改变的是分区表，后者修改的是FAT表，都没有将数据从数据区直接删除。

3. 某一分区被误格式化或文件丢失或误删除的恢复

对于FAT格式的文件结构，文件删除仅仅是把文件的首字节改为E5H，其余的内容并没有被修改，因此可以比较容易恢复。可以使用后面介绍的数据恢复软件轻松地把误删除或意外丢失的文件找回来。不过特别注意的是，在发现文件丢失后，准备使用恢复软件时，千万不要在本机安装这些恢复工具，因为软件的安装可能恰恰把刚才丢失的文件覆盖掉。最好使用能够从光盘直接运行的数据恢复软件，或者把硬盘挂在别的机器上进行

恢复。

特别是文件存储在C盘的情况下，如果发现主要文件被误删除或意外丢失时，这时应该立即关闭电源，用软盘启动进行恢复或把硬盘挂接到其机器上进行处理。

误格式化的情况可以使用UNFORFAT或EasyRecovery等工具进行处理。但是如果使用的是Format X:/U命令进行的格式化，那么这种情况是无法恢复的。

4. 数据恢复范围

1）误操作类

误删除、误格式化、误分区、误克隆等。

2）破坏类

病毒分区表破坏、病毒FAT、BOOT区破坏、病毒引起的部分DATA区破坏。

3）软件破坏类

Format、Fdisk、IBM-DM、PartitionMagic和Ghost等（注：冲零或低级格式化后的硬盘将无法修复数据）。

4）硬件故障类

0磁道损坏、硬盘逻辑锁、操作时断电、硬盘芯片烧毁、软盘/光盘/硬盘无法读盘。

5）加密解密

Zip、Rar、Office文档、Windows 2000/XP系统密码。

5. 彻底删除文件的方法

那么，如何让被删除的文件无法恢复呢？如果将文件删除后重新写入新数据，反复多次后原始文件就可能找不回了。但操作起来比较麻烦，而且也不够保险。因此最好能借助一些专业的删除工具来处理，例如O&O SafeErase可以设置5种删除级别，默认的Highest Security（最高级别的安全删除）算法将使用预设规则重写数据35次，可让原始数据变得“面目全非”。

6. 数据恢复软件EasyRecovery简介

EasyRecovery是世界著名数据恢复公司Kroll Ontrack的技术杰作。其Professional版更是囊括了磁盘诊断、数据恢复、文件修复、E-mail修复全部4大类19个项目的各种数据文件修复和磁盘诊断方案。本实验使用的就是EasyRecovery Professioanl，版本为11.1共享版，目前在网上可以很方便地找到。

EasyRecovery在修复过程中不对原数据进行改动，只是以读的形式处理要修复的分区。它不会将任何数据写入它正在处理的分区。EasyRecovery可运行于Windows 95、98、NT、2000以及XP，并且它还包括了一个实用程序用来创建紧急启动软盘，以便在不能启动进入Windows的时候在DOS下修复数据。

EasyRecovery修复范围：

- 修复主引导扇区（MBR）；
- 修复BIOS参数块（BPB）；

- 修复分区表；
- 修复文件分配表(FAT)或主文件表(MFT)；
- 修复根目录；
- 受病毒影响；
- 格式化或分区；
- 误删除；
- 由于断电或瞬间电流冲击造成的数据毁坏；
- 由于程序的非正常操作或系统故障造成的数据毁坏。

3.1.6 实验设备

主流配置PC一台，要求安装Windows 7操作系统，数据恢复软件EasyRecovery11.1。

3.1.7 实验步骤

(1) 从指导老师处得到数据恢复软件EasyRecovery。

(2) 安装软件。

(3) 运行数据恢复软件EasyRecovery，如图3-1-1所示。

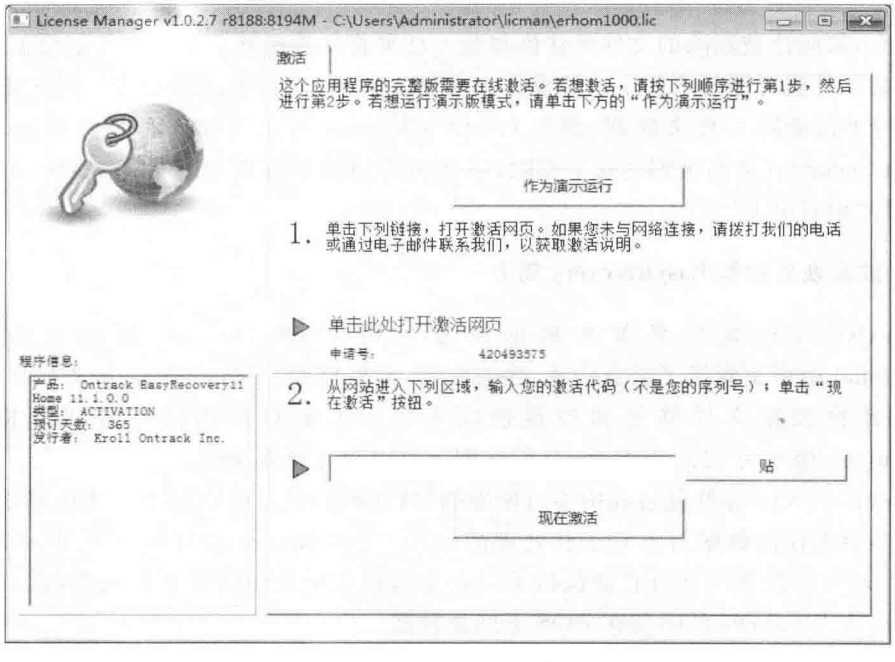

图3-1-1 启动界面