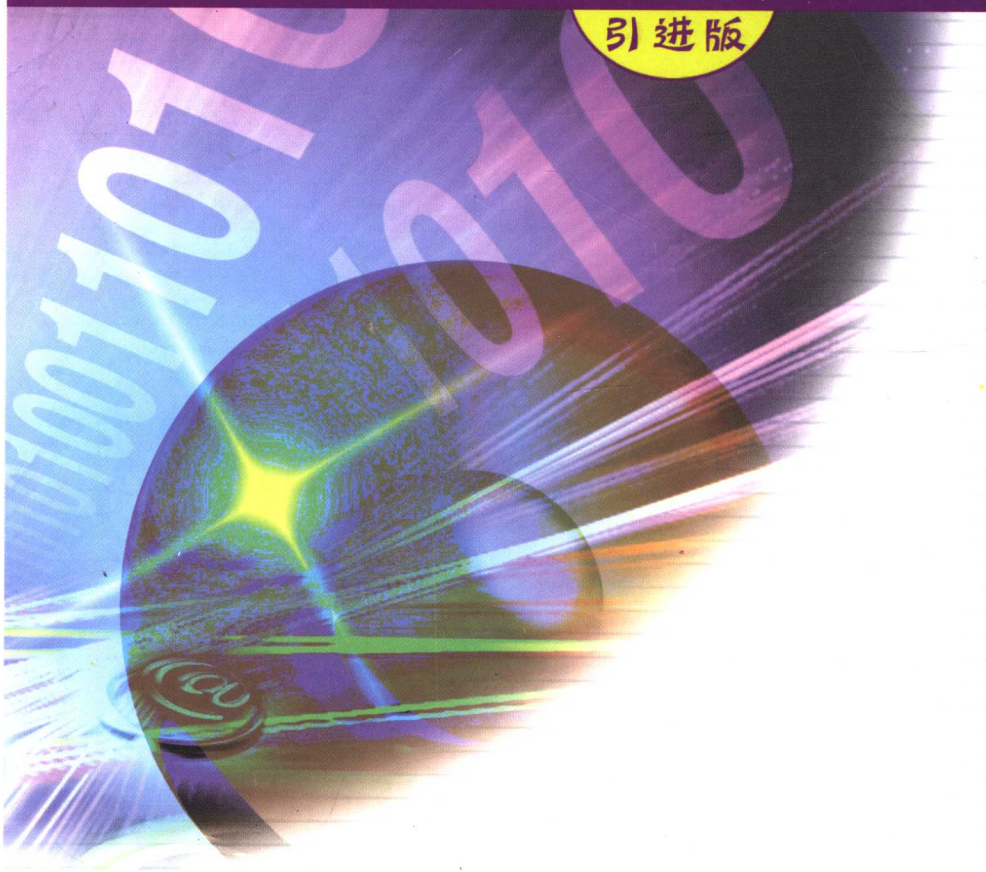
计算机应用与软件技术专业培训用书

网络安全基础实验指导

〔美〕Paul Cretaro 著　王　强　卢　泉　等译

引进版



高等教育出版社
Higher Education Press

计算机应用与软件技术专业培训用书

Lab Manual for Security+ Guide to Network Security Fundamentals

网络安全基础实验指导

[美] Paul Cretaro 著　　王强　卢泉　等译

高等教育出版社

Paul Cretard

Lab Manual for Security + Guide to Network Security Fundamentals, First Edition

ISBN: 0-619-13104-7

图书在版编目（CIP）数据

网络安全基础实验指导/(美)克雷塔罗(Cretaro, P.)著；王强，卢泉等译. —北京：高等教育出版社，2005.6

书名原文：Lab Manual for Security + Guide to Network Security Fundamentals

ISBN 7-04-016718-2

Ⅰ. 网… Ⅱ. ①克…②王…③卢… Ⅲ. 计算机网络-安全技术-教学参考资料 Ⅳ. TP393.08

中国版本图书馆 CIP 数据核字（2005）第 059634 号

策划编辑 李 波 **责任编辑** 许 可 **封面设计** 于文燕

版式设计 王艳红 **责任校对** 杨凤玲 **责任印制** 宋克学

出版发行	高等教育出版社	**购书热线**	010-58581118
社 址	北京市西城区德外大街 4 号	**免费咨询**	800-810-0598
邮政编码	100011	**网 址**	http://www.hep.edu.cn
总 机	010-58581000		http://www.hep.com.cn
		网上订购	http://www.landraco.com
经 销	北京蓝色畅想图书发行有限公司		http://www.landraco.com.cn
印 刷	北京中科印刷有限公司		
开 本	787×960 1/16	**版 次**	2005 年 6 月第 1 版
印 张	15.75	**印 次**	2005 年 6 月第 1 次印刷
字 数	290 000	**定 价**	24.40 元

本书如有缺页、倒页、脱页等质量问题，请到所购图书销售部门联系调换。

版权所有 侵权必究

物料号 16718-00

目　录

引　言

通过实验的方式进行学习是掌握 CompTIA 的安全进阶考试（Security+ Exam）和从事网络安全职业所必需的安全技能的最佳途径。本书包含的实验练习应用了那些在真实的世界中使用的基本网络概念，此外，每一章提供了复习题来强化对网络安全问题的掌握。本书的结构与主教材《网络安全基础》（Security+ Guide to Network Security Fundamental）完全相同，如果一起使用的话，读者将获得更加丰富和有效的学习体验。本书适合于作为初、中级的网络安全课程教材。学习本书前，学生应当对网络的概念有一个基本的了解，并至少学习过一门网络操作系统课程。本书最好是在《网络安全基础》或者另一本安全进阶的教材学完后使用。

本书特色

为了确保教师和学生都能成功地使用本书，本书具有如下一些特色：

- Security+ 认证目标：每一章中都列出了 CompTIA 的 Security+考试的目标。
- 目标：在每个实验中，都有一段简单的说明，并列出了学习的目标。
- 实验条件：在每个实验中，都列出了完成该实验所需要的网络访问权限、硬件、软件和其他信息。
- 预计完成时间：在每个实验中，都有一个预计的完成时间，以便让读者更加精确地安排各种活动。
- 实验步骤：合理的和准确的操作步骤指导读者完成每个实验中的动手活动。
- 复习题：帮助强化实验中出现的概念。

硬件要求

下面列出了完成本书实验所需要的硬件环境。但不是每个实验都需要这里列出的全部硬件。

- 三台装有奔腾 166 MHz CPU 或更快处理器（建议 400 MHz 以上）的计算机，并具有如下配置：
  - 每台计算机有 128 MB 内存（建议 256 MB 以上）

  - 每台计算机有 4 GB 的硬盘并至少有 1 GB 的可用空间（建议使用 10 GB 以上的硬盘并有 7 GB 的可用空间）
  - CD-ROM 驱动器
- Internet 访问接口
- 每台计算机上有两块 PCI 以太网接口卡
- 一台集线器或者交换机
- 至少 4 条 5 类 UTP 直通插塞式双绞线电缆
- 至少 2 条 5 类 UTP 交叉插塞式双绞线电缆
- 一台 Cisco 1900 交换机
- 一条专用的 Cisco 控制台端口连接线缆
- 一个 RJ-45 到 DB-9 或者 DB-25 的适配器
- 一台 Cisco Aironet 340 路由器

软件要求

- 至少两个带有 Windows 2000 Service Pack 3 的 Windows 2000 Server 的副本
- 安装在 Windows 2000 Server 上的 Microsoft IIS Version 5
- Internet Explorer 6 Web 浏览器
- PGP
- Outlook Express
- 匿名电子邮件邮寄者*
- Bastion.inf 安全配置文件*
- ZDelete Auto Cleaner*
- Restorer2000*
- Snort 1.8.x*
- WinPcap*
- IDSCenter*
- BackOfficer*
- IISLockdown Tool
- Microsoft Baseline Security Analyzer

*表示的程序可以从厂商的网站上下载。

实验室设置原则

教师的计算机

1．分区

a. C 盘 3 GB NTFS 格式
b. D 盘 4 GB FAT32 格式

2. Windows 2000 Server 安装
a. 用 Windows 2000 Server 光盘引导系统
b. 按 F8 接受许可协议
c. 建立一个 3 GB 分区
d. 以 NTFS 格式格式化分区
e. 必要时设置区域选项
f. 键入用户的名字和公司名称
g. 键入产品的序列号
h. 选择 Per Seat（每用户）许可
i. 计算机名：Instructor
j. 管理员口令：password
k. 必要时调整时区
l. 自定义网络设置：
配置 TCP/IP 设置为：
i. IP 地址：192.168.x.100 **注意**：用教室号取代 x
ii. 子网掩码：255.255.255.0
iii. DNS 服务器：192.168.x.100
iv. 接受 WORKGROUP 为工作组

3. 活动目录设置
a. 运行 dcpromo
b. 建立一个新的域、树、林
c. 让 Active Directory 安装程序安装 DNS
d. DNS 名为：Class.dom
e. 接受默认设置

4. DNS 设置：
a. 在 Class.dom 区上启用动态更新
b. 为 192.168.x 建立一个标准的主反向搜索（Reverse lookup）区
c. 启用动态更新
d. 建立 DHCP
e. Scope 名：Class
f. IP 范围：192.168.x.1 ~ 192.168.x.254
g. 子网掩码：255.255.255.0
h. 禁用：192.168.x.1 ~ 192.168.x.20，192.168.x.100 ~ 192.168.x.254 之

间的 IP 地址

i. 配置选项：

i. 路由器：192.168.x.100

ii. 域名：Class.dom

iii. DNS 服务器：192.168.x.100

学生的计算机

1. 分区

a. C 盘 3 GB NTFS 格式

b. D 盘 4 GB FAT32 格式

2. Windows 2000 Server 安装

a. 用 Windows 2000 Server 光盘引导系统

b. 按 F8 接受许可协议

c. 建立一个 3 GB 分区

d. 以 NTFS 格式格式化分区

e. 必要时设置区域选项

f. 键入用户的名字和公司名称

g. 键入产品的序列号

h. 选择 Per Seat 许可

i. 计算机名：Server-x **注意**：用教师分配的号码取代 x

j. 管理员口令：password

k. 必要时调整时区

l. 接受通常的网络设置

致谢

衷心感谢 Course Technology 出版公司给了我一个编写这个实验手册的机会；同时，十分感谢 Dave George 和 Laura Hildebrand 提供的不可或缺的资源；感谢所有在时间很紧的情况下提出了大量宝贵意见的先期审阅人员：Mike Parsons、Mike Daveler、Amelia Phillips、Rob Andrews 等；最后，还十分感谢我的妻子 Sherrie 和三个孩子 Mark、Michael 和 Adam 对我的支持和宽容。

第一章 安全概述

本章包括的实验：

- 实验 1.1 使用 NTFS 文件系统保护本地资源
- 实验 1.2 数据的保密性
- 实验 1.3 数据的可用性
- 实验 1.4 数据的完整性
- 实验 1.5 数据加密

CompTIA Security + 考试目标	
目标	实验
一般的安全概念：访问控制	1.1、1.2、1.3、1.4、1.5

实验 1.1 使用 NTFS 文件系统保护本地资源

目标

本地计算机的安全问题，特别是文件级的安全问题，经常会被忽略。多数人都对微软的 Windows 9x 很熟悉，但 Windows 9x 使用 FAT 分区，它没有提供对本地文件的安全保护。Windows NT/2000 的文件系统 NTFS 在设计时提供了对本地文件的安全保护。为了利用这个功能，必须在安装 Windows NT/2000/XP 时采用 NTFS 文件系统。需要特别留意的是，尽管这些操作系统都兼容 FAT 分区，但只有安装在 NTFS 上的操作系统，才能保证本地文件的安全。

在完成这个实验后，你将能够：

- 确定一个分区是 FAT 还是 NTFS
- 将 FAT 分区转换成 NTFS 分区

实验条件

本实验需要下列条件：

- 一台运行 Windows 2000 Server 的独立或者作为成员服务器的计算机
- 服务器的管理员权限

- 至少有一个用 FAT 或者 FAT32 格式化的分区

预计完成时间： 10 分钟

实验步骤

1. 以 Administrator（管理员）身份登录到 Windows 2000 Server。
2. 单击 **Start**（开始）。
3. 单击 **Run**（运行）。
4. 键入 **cmd** 以调用命令行。注意：本实验中的 FAT 分区将作为驱动器 E。
5. 在命令行键入 **chkntfs e:**来确认驱动器是否使用 NTFS 格式。如果看到这样的提示信息“E: is not dirty”，表示驱动器上是空白的。
6. 在命令行键入 **convert e: /fs:ntfs**，将 FAT 分区转换成 NTFS 分区。
7. 如果驱动器上有一个卷标号，当提示时键入它，然后 Windows 将驱动器转换成 NTFS 格式。注意，如果转换的是系统分区，转换时将不得不重新启动计算机。
8. 在命令行键入 **chkntfs e:**来确认驱动器现在是否为 NTFS 格式。
9. 图 1-1 是展示上述各步骤的一个例子。

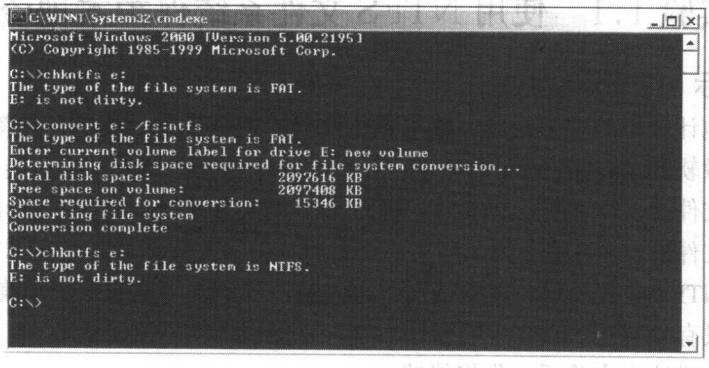


图 1-1 使用 CHKNTFS 和 CONVERT 命令

10. 关闭所有窗口并注销当前用户。

认证目标

CompTIA Security+考试的目标：

- 一般的安全概念：访问控制

复习题

1. 下面什么文件系统是与 Windows NT 4.0 兼容的？
   a. FAT
   b. FAT32
   c. OSPF
   d. NTFS
2. 下面哪些功能是 NTFS 5 所具备而 FAT 分区所不具备的？
   a. 共享级安全
   b. 文件级安全
   c. 压缩
   d. 加密
3. 下面哪个命令可以将 FAT 分区转换成 NTFS 分区？
   a. update C:/FS:NTFS
   b. upgrade C:/FS:NTFS
   c. convert C:/FS:NTFS
   d. convert C:/NTFS
4. 下面有哪些可用于 Windows 文件夹共享的操作权限？
   a. Read（读）
   b. Modify（修改）
   c. Change（更改）
   d. Full Control（完全控制）
5. 一旦将 FAT 分区转换成 NTFS，将它再改回 FAT 的唯一方法是重建分区并从备份中恢复。这种说法是否正确？

实验 1.2 数据的保密性

目标

当安装了一个安全的文件系统之后，就可以开始考虑数据的保密性。数据的保密性是指确保只有那些特定的人员才能实际访问他们有权访问的数据。对于 FAT 文件系统，本地文件是不可能实现访问控制的，但是 NTFS 就可以锁定本地文件夹和文件。一些入侵者能够物理访问计算机上包含的数据，NTFS 能够用于保护数据不受这些入侵者的危害。在这个实验中，你将建立一个文件夹和若干文件，指定 NTFS 权限，然后验证数据是否保密。

在完成这个实验之后，你将能够：

- 指定文件夹和文件的 NTFS 权限，以保护本地资源

- 验证数据是否保密

实验条件

本实验需要下列条件：

- 一台运行 Windows 2000 Server 的独立或者作为成员服务器的计算机
- 管理员对服务器的管理员权限
- 一个 NTFS 格式的分区
- 两个用户账号：User1 和 User2

预计完成时间： 15 分钟

实验步骤

1．以 Administrator（管理员）身份登录到 Windows 2000 Server。

2．打开 **My Computer**（我的电脑），然后双击 E 盘，即实验 1.1 中将 FAT 转换成 NTFS 的驱动器。

3．建立一个名为 **Confidentiality** 的新文件夹。

4．双击 **Confidentiality** 文件夹，然后建立一个名为 **User1Folder** 的新文件夹。

5．为了保护这个文件夹不被其他用户使用，右击 **User1Folder** 文件夹。

6．单击 **Properties**（属性），打开 User1Folder Properties 窗口。

7．单击 **Security**（安全）标签，如图 1-2 所示。注意，如果驱动器没有用 NTFS 格式化，Security 标签将不可用。

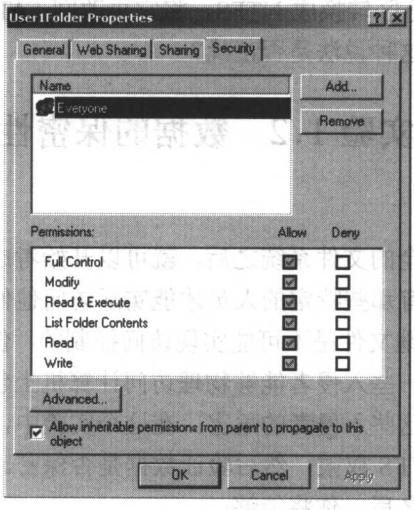


图 1-2 默认的 NTFS 权限

8．取消“Allow inheritable permissions from parent to propagate to this object（允许这个对象继承父文件夹的可继承权限）”复选框。

9．将收到如图 1-3 所示的提示信息。

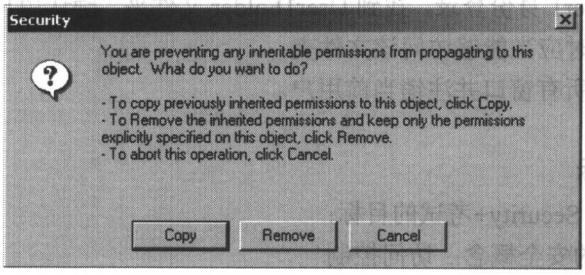


图 1-3　当改变默认 NTFS 权限时的安全警告

10．单击 **Copy**（复制），以保留权限。

11．单击 **Add**（添加），将弹出“Select Users，Computers，or Groups”（选择用户、计算机或者组）窗口。

12．确保在 **Look in** 下拉框中选择你的服务器。

13．选择 **User1**，然后单击 **Add**（添加）。

14．单击 **OK**（确认）。

15．保持 User1 高亮显示，单击 **Allow Full Control**（允许完全控制）复选框。

16．单击 **Everyone**，然后单击 **Remove**（删除），屏幕将如图 1-4 所示。

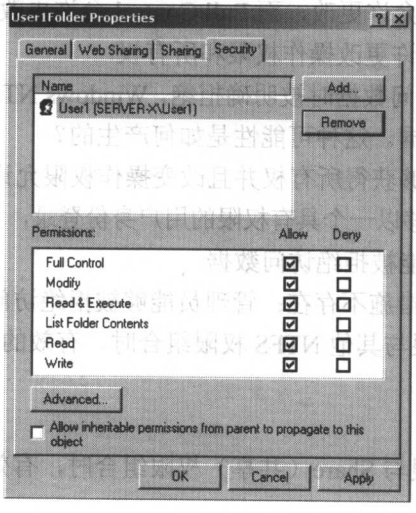


图 1-4　在默认 NTFS 权限被删除后的 User1 权限

17．单击 **OK**（确认）。

18．双击 **User1Folder** 文件夹，由于只允许 User1 访问，你的访问将被拒绝。

19．关闭所有窗口并注销当前用户。

20．以 User1 身份登录，找到 User1Folder 文件夹，确认用户是否能够访问该文件夹。此时应当能够访问该文件夹。

21．关闭所有窗口并注销当前用户。

认证目标

CompTIA Security+考试的目标：

- 一般的安全概念：访问控制

复习题

1．对数据保密性的最佳定义是：

a．没有被有意或者偶然篡改的数据

b．为远程传输而编码的数据

c．对于被保护的数据，只有特定的人员才有访问权

d．当需要时能够访问的数据

2．当比较 Full Control（完全控制）和 Modify（修改）NTFS 权限时，两者的差异是什么？

a．Full Control 与 Modify 完全相同

b．Full Control 允许更改操作权限和所有权

c．Modify 只允许更改，而 Full Control 允许更改和删除

d．Modify 允许更改操作权限和所有权

3．即使管理员访问数据时被明确拒绝，Windows NT/2000 中的安全措施仍然允许管理员访问数据。这种可能性是如何产生的？

a．管理员能够获得所有权并且改变操作权限允许自己访问数据

b．管理员能够以一个具有权限的用户身份登录，并授予自己数据访问权

c．管理员不能被拒绝访问数据

d．这种安全措施不存在；管理员能够被拒绝访问数据

4．当 NTFS 权限与其他 NTFS 权限组合时，有效的权限是什么？

a．最多限制

b．最少限制

5．当 NTFS 权限与 Share（共享）权限组合时，有效的权限是什么？

a．最多限制

b．最少限制