

<<网络与信息安全实验教程>>

图书基本信息

书名：<<网络与信息安全实验教程>>

13位ISBN编号：9787302268239

10位ISBN编号：7302268231

出版时间：2012-1

出版时间：清华大学出版社

作者：赵华伟，刘理争 编著

页数：192

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

## <<网络与信息安全实验教程>>

### 内容概要

本书是作者依据多年在网络信息安全领域的教学、培训和技术实践，针对高等院校网络信息安全及相关本科和研究生专业的教学特点和需求，以及高校实验室的建设现状，从实用性的角度出发编写而成。

本书共分3篇。

第1篇（实验1~实验3）为基础篇，着重介绍实验环境的搭建、常用的系统命令以及系统的安全配置方法；

第2篇（实验4~实验13）为安全操作篇，着重讲解ntfs的使用方法、账号的保护、文件的加密、电子邮件的加密与签名、iis安全配置以及ssl配置实验等；

第3篇（实验14~实验18）为攻击体会篇，着重讲解了对windows系统账号的攻击方法、arp攻击方法、远程控制攻击、映像劫持攻击以及sql注入攻击等。

本教程的所有实验均基于vmware虚拟机平台的team功能搭建，使学生在一台计算机上就能独立完成基于局域网的实验项目，从而能有效帮助学生巩固网络信息安全课程的基础理论知识，更深入地掌握网络信息安全的各项操作技能。

本书不仅适用于高等院校的信息安全专业、计算机专业的高年级本科生、研究生作为实验教材使用，也适用于作为网络信息安全职业技术培训实验教材，同时也可作为对网络信息安全技术有兴趣的读者的参考用书。

书籍目录

第1篇基础篇

实验1实验环境建设

- 1.1实验目的与要求
- 1.2实验环境
- 1.3预备知识
- 1.4实验内容
- 1.5实验步骤
  - 1.5.1虚拟机的安装
  - 1.5.2team的安装
- 1.6实验思考

实验2常见的系统命令

- 2.1实验目的与要求
- 2.2实验环境
- 2.3预备知识
- 2.4实验内容
- 2.5实验步骤
- 2.6实验思考

实验3计算机的安全配置

- 3.1实验目的与要求
- 3.2实验环境
- 3.3预备知识
- 3.4实验内容
- 3.5实验步骤
  - 3.5.1卸载和删除Intsvr服务
  - 3.5.2使用windows组策略对计算机进行安全配置
  - 3.5.3加固windows抗dos攻击能力
  - 3.5.4通过过滤icmp报文阻止icmp攻击
- 3.6实验思考

第2篇安全配置篇

实验4ntfs文件系统实验

- 4.1实验目的与要求
- 4.2实验环境
- 4.3预备知识
- 4.4实验内容
- 4.5实验步骤
  - 4.5.1查看ntfs的版本号
  - 4.5.2将fat文件系统转化为ntfs文件系统
  - 4.5.3ntfs权限设置
- 4.6实验思考

实验5安全登录

- 5.1实验目的与要求
- 5.2实验环境
- 5.3预备知识
  - 5.3.1登录及身份认证过程
  - 5.3.2sid

## <<网络与信息安全实验教程>>

5.3.3sam

5.3.4访问令牌

5.4实验内容

5.5实验步骤

5.5.1查看管理员用户的sid

5.5.2查看新建用户的sid

5.5.3创建一个具有管理员权限的隐藏账户

5.6实验思考

### 实验6windows账户与口令的安全设置

6.1实验目的与要求

6.2实验环境

6.3预备知识

6.3.1windows的域安全策略

6.3.2windows的本地安全策略

6.3.3administrator 和guest账户

6.3.4高强度登录密码

6.3.5syskey

6.4实验内容

6.5实验步骤

6.5.1账户设置

6.5.2本地安全策略设置

6.5.3利用syskey保护账户信息

6.6实验思考

### 实验7efs实验

7.1实验目的与要求

7.2实验环境

7.3预备知识

7.4实验内容

7.5实验步骤

7.5.1利用efs加密文件

7.5.2证书的导出

7.5.3数据恢复代理

7.6实验思考

### 实验8ftp访问权限实验

8.1实验目的与要求

8.2实验环境

8.3预备知识

8.4实验内容

8.5实验步骤

8.5.1安装ftp服务

8.5.2设置ftp站点

8.5.3设置ftp账户

8.5.4设置匿名账户

8.5.5ftp账户的访问权限

8.6实验思考

### 实验9网络嗅探实验

9.1实验目的与要求

<<网络与信息安全实验教程>>

9.2实验环境

9.3预备知识

9.3.1网络嗅探

9.3.2icmp协议

9.4实验内容

9.5实验步骤

9.5.1icmp协议数据的捕获

9.5.2icmp协议的分析

9.5.3ftp协议数据的捕获和分析

9.6实验思考

实验10outlook express安全电子邮件

10.1实验目的与要求

10.2实验环境

10.3预备知识

10.4实验内容

10.5实验步骤

10.5.1申请电子邮件保护证书

10.5.2证书的颁发

10.5.3下载并在客户机中安装证书

10.5.4配置outlook express

10.6实验思考

实验11ssh安全连接

11.1实验目的与要求

11.2实验环境

11.3预备知识

11.3.1服务器认证

11.3.2用户认证

11.4实验内容

11.5实验步骤

11.5.1如何使用口令访问ssh服务器

11.5.2更新服务器的主密钥

11.6实验思考

实验12iis安全配置实验

12.1实验目的与要求

12.2实验环境

12.3预备知识

12.4实验内容

12.5实验步骤

12.5.1iis 6.0的安装

12.5.2iis相关安全配置

12.6实验思考

实验13windows 2000系统中ssl的实现

13.1实验目的与要求

13.2实验环境

13.3预备知识

13.3.1ssl/tls协议

13.3.2https介绍

<<网络与信息安全实验教程>>

13.4实验内容

13.5实验步骤

13.5.1证书服务安装

13.5.2配置iis服务器

13.5.3申请服务器证书

13.5.4证书颁发

13.5.5证书安装

13.5.6配置iis中的ssl

13.5.7测试ssl

13.6实验思考

第3篇攻击体会篇

实验14windows账户与口令破解

14.1实验目的与要求

14.2实验环境

14.3预备知识

14.3.1身份认证机制

14.3.2sam(security accounts manager)

14.3.3l0phtcrack 5.0密码测试工具

14.4实验内容

14.5实验步骤

14.5.1利用密码策略强制设置高强度密码

14.5.2保护密码安全策略的设置

14.5.3使用lc5测试密码

14.6实验思考

实验15arp攻击实验

15.1实验目的与要求

15.2实验环境

15.3预备知识

15.4实验内容

15.5实验步骤

15.6实验思考

实验16远程控制实验

16.1实验目的与要求

16.2实验环境

16.3预备知识

16.4实验内容

16.5实验步骤

16.6实验思考

实验17windows映像劫持技术

17.1实验目的与要求

17.2实验环境

17.3预备知识

17.4实验内容

17.5实验步骤

17.5.1映像劫持攻击

17.5.2控制注册表的访问权

17.6实验思考

<<网络与信息安全实验教程>>

实验18sql注入漏洞提权实验

18.1实验目的与要求

18.2实验环境

18.3预备知识

18.4实验内容

18.5实验步骤

18.6实验思考

参考文献

## 章节摘录

版权页：插图：虚拟硬件技术有以下两个主要特点：（1）可以直接用系统处理器执行CPU指令，根本涉及不到虚拟层。

（2）实现真正的分区隔离，每个分区只占用一定的系统资源，包括磁盘I/O和网络带宽，并提高了系统的整体安全性。

另外，高端的虚拟服务器产品可以直接在硬件上运行虚拟机，而不需要宿主操作系统。

并且，通过相关的管理软件，可以对每个虚拟机消耗的物理资源（网络带宽、磁盘I/O访问等）进行精确的控制。

2.虚拟软件模式虚拟操作系统模式是在虚拟机运行的主机操作系统之上创建了一个虚拟层，在该虚拟层之上，能够创建多个相互隔离的虚拟专用服务器（Virtual Private Server，VPS）。

这些VPS能以最大化的效率共享硬件、软件许可证以及管理资源。

对其用户和应用程序来讲，每一个VPS平台的运行和管理都与一台独立主机完全相同，因为每一个VPS均可独立进行重启并拥有自己的root访问权限、用户、IP地址、内存、过程、文件、应用程序、系统函数库以及配置文件。

对于运行着多个应用程序和拥有实际数据的产品服务器来说，虚拟操作系统的虚拟机可以降低成本消耗和提高系统效率。

虚拟操作系统模式同样能够满足一系列的需求：安全隔离、计算机资源的灵活性和控制、硬件抽象操作及最终高效、强大的管理功能。

每一个VPS中的应用服务都是安全隔离的，且不受同一物理服务器上的其他VPS的影响。

通过专用的文件系统，使得文件浏览对所有VPS用户来说就如常规服务器一样，但却无法被该服务器上的其他VPS用户看到。

VPS能够实时分配、监控、计算并控制资源级别，完成对CPU、内存、网络输入输出、磁盘空间以及其他网络资源的灵活管理。

经过抽象的VPS具有相同的虚拟硬件结构，并可以在任意联网的服务器之间透明迁移，而不产生任何宕机时间。

操作系统虚拟化技术解决了在单个物理服务器上部署多个生产应用服务和存储服务器时所面临的挑战。

在应用服务部署完成之后，它们被集中于同一种操作系统以便于管理和维护。

操作系统虚拟化是针对生产应用和服务器的完美虚拟化解决方案，共享的操作系统提供了更为有效的服务器资源并且大大降低了处理损耗。

通过操作系统虚拟化，上百个VPS可以在单个的物理服务器上正常运行。

然而，这种集中于同一操作系统的特性使得该类虚拟机只能在一台物理服务器上运行同一种虚拟的操作系统，比如，不能够同时运行虚拟的Windows和Linux系统。

VMware公司是全球领先的虚拟技术开发厂商：其解决方案通过采用硬件虚拟化技术，将操作系统与应用软件分离，可显著提高系统的工作效率、可用性和灵活性。

目前VMware公司主要有3种产品：VMware Workstation、VMware Infrastructure与VMware VMotion TM。

本实验教材搭建实验平台所采用的虚拟化工具是VMwareWorkstation5.5。

该产品有以下特点：（1）可以将已有的虚拟机文件直接进行移植，提高工作效率。

（2）多个虚拟机可同时、独立运行，一个虚拟机崩溃不会影响其他虚拟机的正常运行。

（3）虚拟机提供多种网络接入方式，可以直接访问外网，也可以将多个虚拟机组成虚拟机组，形成一个局域网。

## <<网络与信息安全实验教程>>

### 编辑推荐

《网络与信息安全实验教程》特色：站在工程、开发和研究三个角度，进行实践性教学环节的设计。从社会对计算机专业人才能力需求的角度，系统地规划计算机实验和实践的方式和内容。开发实训验证型、开发研究型等不同层次的教学内容，以满足大专、本科以及某些研究生层次的教学需求。

以系统性、开放性、经典性和适用性等全新的面貌呈现在中国的计算机教学领域。

精心挖掘和遴选作者，把他们多年积累的教学经验编写成教材。

每本书都经过编委会委员的精心筛选和严格评审，严把质量关。

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>