

# 《计算机系统安全与维护》

## 图书基本信息

书名：《计算机系统安全与维护》

13位ISBN编号：9787301217542

10位ISBN编号：7301217544

出版社：吕新荣、陆世伟 北京大学出版社 (2013-01出版)

版权说明：本站所提供下载的PDF图书仅提供预览和简介以及在线试读，请支持正版图书。

更多资源请访问：[www.tushu000.com](http://www.tushu000.com)

# 《计算机系统安全与维护》

## 书籍目录

项目1计算机网络安全认识 模块1网络安全典型案例分析 任务1典型案例1 任务2典型案例2 模块2道德与法律 任务1网络安全的道德 任务2网络安全的法律 项目小结 思考练习 项目2网络病毒防范 模块1蠕虫病毒防范 任务1蠕虫病毒分析 任务2蠕虫病毒防范策略 模块2USB传播病毒防范 任务1USB设备传播病毒分析 任务2多种防范USB病毒的策略 项目小结 思考练习 项目3网络攻击防范 模块1ARia攻击防范 任务1ARP攻击原理认识 任务2ARP攻击与反攻击演练 模块2木马攻击防范 任务1木马攻击原理认识 任务2防范木马攻击的策略 模块3网络扫描和窃听 任务1漏洞扫描 任务2数据捕捉及分析 任务3防范机制建立 项目小结 思考练习 项目4网络安全加固 模块1防火墙 任务1ISA防火墙安装 任务2配置ISA防火墙客户端 任务3管控即时通信与P2P软件 模块2入侵检测 任务1启用ISA入侵检测功能 任务2配置Snort 项目小结 思考练习 项目5Windows安全管理 模块1本地账户管理 任务1认识本地账户 任务2管理本地账户 模块2文件与文件夹安全管理 任务1设置NTFS权限 任务2管理共享文件夹 模块3安全策略设置 任务1设置账户策略 任务2设置本地策略 任务3应用安全模板 项目小结 思考练习 项目6数据安全 模块1文件备份与恢复 任务1系统文件备份与恢复 任务2用户文档备份及恢复 模块2磁盘管理 任务1磁盘管理的内容 任务2磁盘配额启用 任务3动态磁盘管理 模块3数据加密 任务1对称加密技术 任务2非对称加密技术 任务3MD5加密技术 项目小结 思考练习 项目7Windows域安全管理 模块1域账户管理 任务1认识域 任务2建立域 任务3域账户管理 模块2组策略应用 任务1建立组策略对象 任务2利用组策略禁用USB接口 任务3利用组策略部署软件 任务4利用组策略限制软件的运行 模块3域资源安全管理 任务管理共享文件 项目小结 思考练习 项目8数据安全交换 模块1数字证书应用 任务1安装证书服务 任务2申请数字证书 任务3利用证书加密电子邮件 模块2VPN配置 任务1配置ISAServerVPN服务器 任务2建立VPN连接 模块3Web站点安全访问 任务1发布企业内部Web站点 任务2安全访问企业Web站点 项目小结 思考练习 参考文献

版权页：插图：2.2相关知识 1.木马攻击的基本原理 黑客用木马进行网络入侵，从过程上看大致可分为6步，下面用这6步来详细阐述木马的攻击原理。

1) 配置木马 一般来说，一个设计成熟的木马配置程序，从具体的配置内容看，主要是为了实现以下两个方面的功能。

(1) 木马伪装。木马配置程序为了在服务器端尽可能好地隐藏木马，会采用多种伪装手段，如修改图标、捆绑文件、定制端、自我销毁等。

(2) 信息反馈。木马配置程序将信息反馈的方式或地址进行设置，如设置信息反馈的E-mail、IRC号、QQ号等。

2) 传播木马 (1) 传播方式。木马的传播方式主要有两种：一种是通过电子邮件，即控制端将木马程序以附件的形式夹在邮件中发送出去，收件人只要一打开附件，系统就会感染木马；另一种是软件下载，即一运行这些程序，木马就会自动安装。

(2) 伪装与隐藏方式。木马设计者为了使自己所设计的木马程序不轻易被人发现，往往在开发时采用多种方式来伪装木马，以达到降低用户警觉、欺骗用户的目的。比如和某个视频文件绑定、和某张图片绑定等。

3) 运行木马 服务器端用户运行木马或捆绑木马的程序后，木马就会自动进行安装。首先自身复制到Windows的系统文件夹中，然后在注册表、启动组、非启动组中设置好木马的触发条件，这样木马的安装就完成了。安装后达到了一定的触发条件，就开始运行木马。

4) 盗取信息 一般来说，设计成熟的木马都有一个信息反馈机制。所谓信息反馈机制，是指木马成功安装后会收集一些服务器端的软、硬件信息，并通过E-mail、IRC、QQ或ICQ的方式告知控制端用户。控制端从反馈信息中可以知道服务器端的一些软、硬件信息，包括使用的操作系统、系统目录、硬盘分区状况、系统口令等，在这些信息中，最重要的是服务器端IP地址，因为只有得到这个参数，控制端才能与服务器端建立连接。

5) 建立连接 一个木马连接的建立首先必须满足两个条件：一是服务器端已安装了木马程序；二是控制端、服务器端都要在线。在此基础上控制端可以通过木马端口与服务器端建立连接。假设A机为控制端，B机为服务器端，对于A机来说要与B机建立连接，必须知道B机的木马端口和IP地址。由于木马端口是A机事先设定的，为已知项，所以最重要的是如何获得B机的IP地址。获得B机的IP地址的方法主要有两种：信息反馈和IP扫描。由于扫描整个IP地址既费时又费力，一般来说控制端都是通过信息反馈获得服务器端的IP地址。

# 《计算机系统安全与维护》

## 编辑推荐

《全国高职高专计算机立体化系列规划教材:计算机系统安全与维护》适合作为高职高专计算机类和信息安全类专业及相近专业的教材，也可作为中小企业信息系统管理员、网络管理员、信息安全员的培训教材或工作参考书。

# 《计算机系统安全与维护》

## 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:[www.tushu000.com](http://www.tushu000.com)