

<<信息安全对抗系统工程与实践>>

图书基本信息

书名：<<信息安全对抗系统工程与实践>>

13位ISBN编号：9787040365092

10位ISBN编号：704036509X

出版时间：2012-12-01

出版时间：罗森林、高平、苏京霞、潘丽敏 高等教育出版社 (2012-12出版)

作者：罗森林，高平，苏京霞等著

页数：349

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>

<<信息安全对抗系统工程与实践>>

内容概要

《国家精品课程主讲教材·高等学校信息安全系列教材：信息安全对抗系统工程与实践》共分为6章，主要内容包括：绪论，操作系统攻防技术实践，TCP/IP网络通信技术实践，网络攻击基础技术实践，数据加密解密技术实践，网络防御基础技术实践。

《国家精品课程主讲教材·高等学校信息安全系列教材：信息安全对抗系统工程与实践》可作为信息安全、信息对抗、计算机应用等相关专业的正式教材，也可供相关实验选修课程、开放实验课程、专业课程设计以及信息安全对抗相关技术竞赛培训使用，还可供科研人员参考和对信息安全感兴趣者自学使用。

书籍目录

第1章 绪论 1.1 信息安全与对抗的概念 1.1.1 信息和信息系统 1.1.2 信息安全的概念 1.1.3 信息攻击与对抗的概念 1.1.4 信息系统安全问题分类 1.2 信息安全对抗基础理论概述 1.2.1 基础层面原理 1.2.2 系统层面原理 1.2.3 系统层面安全对抗方法 1.3 信息安全对抗基础技术概述 1.3.1 安全攻击与检测技术 1.3.2 系统防御与对抗技术 1.4 工程系统理论的基本思想 1.4.1 若干概念和规律 1.4.2 系统分析观 1.4.3 系统设计观 1.4.4 系统评价观 1.5 系统工程的基本思想 1.5.1 概述 1.5.2 基础理论 1.5.3 方法论 1.5.4 模型和仿真 1.5.5 评价步骤和方法 1.6 本章小结 第2章 操作系统攻防技术实践 2.1 引言 2.2 Windows操作系统攻防实验 2.2.1 实验条件和环境 2.2.2 主要功能实现 2.2.3 问题思考与实验要求 2.3 Linux操作系统攻防实验 2.3.1 实验条件和环境 2.3.2 总体设计 2.3.3 主要功能实现 2.3.4 系统运行说明 2.3.5 问题思考与实验要求 2.4 本章小结 第3章 TCP/IP网络通信技术实践 3.1 引言 3.2 字符和文件传输技术实验 3.2.1 实验条件和环境 3.2.2 总体设计 3.2.3 主要功能实现 3.2.4 系统运行说明 3.2.5 问题思考与实验要求 3.3 网络音频通信技术实验 3.3.1 实验条件和环境 3.3.2 总体设计 3.3.3 主要功能实现 3.3.4 系统运行说明 3.3.5 问题思考与实验要求 3.4 本章小结 第4章 网络攻击基础技术实践 4.1 引言 4.2 网络数据捕获技术实验 4.2.1 实验条件和环境 4.2.2 总体设计 4.2.3 主要功能实现 4.2.4 系统运行说明 4.2.5 问题思考与实验要求 4.3 端口和漏洞扫描技术实验 4.3.1 端口扫描实践系统 4.3.2 漏洞扫描实践系统 4.3.3 问题思考与实验要求 4.4 计算机病毒技术实验 4.4.1 脚本病毒实践系统 4.4.2 蠕虫病毒实践系统 4.4.3 问题思考与实验要求 4.5 特洛伊木马技术实验 4.5.1 实验条件和环境 4.5.2 总体设计 4.5.3 主要功能实现 4.5.4 系统运行说明 4.5.5 问题思考与实验要求 4.6 ARP欺骗技术实验 4.6.1 实验条件和环境 4.6.2 总体设计 4.6.3 主要功能实现 4.6.4 系统运行说明 4.6.5 问题思考与实验要求 4.7 缓冲区溢出技术实验 4.7.1 实验条件和环境 4.7.2 总体设计 4.7.3 主要功能实现 4.7.4 系统运行说明 4.7.5 问题思考与实验要求 4.8 Web密码破解技术实验 4.8.1 实践环境和条件 4.8.2 总体设计 4.8.3 主要功能实现 4.8.4 系统运行说明 4.8.5 问题思考与实验要求 4.9 本章小结 第5章 数据加密解密技术实践 5.1 引言 5.2 DES加解密技术实验 5.2.1 实验条件和环境 5.2.2 总体设计 5.2.3 主要功能实现 5.2.4 系统运行说明 5.3 RSA加解密技术实验 5.3.1 实验条件和环境 5.3.2 总体设计 5.3.3 主要功能实现 5.3.4 系统运行说明 5.3.5 问题思考与实验要求 5.4 本章小结 第6章 网络防御基础技术实践 6.1 引言 6.2 防火墙技术实验 6.2.1 实验条件和环境 6.2.2 总体设计 6.2.3 主要功能实现 6.2.4 系统运行说明 6.2.5 问题思考与实验要求 6.3 入侵检测技术实验 6.3.1 实验条件和环境 6.3.2 总体设计 6.3.3 主要功能实现 6.3.4 系统运行说明 6.3.5 问题思考与实验要求 6.4 身份认证技术实验 6.4.1 实验条件和环境 6.4.2 总体设计 6.4.3 主要功能实现 6.4.4 系统运行说明 6.4.5 问题思考与实验要求 6.5 灾难恢复技术实验 6.5.1 实验条件和环境 6.5.2 总体设计 6.5.3 主要功能实现 6.5.4 系统运行说明 6.5.5 问题思考与实验要求 6.6 虚拟专用网技术实验 6.6.1 实验条件和环境 6.6.2 总体设计 6.6.3 主要功能实现 6.6.4 系统运行说明 6.6.5 问题思考与实验要求 6.7 蜜罐与蜜网技术实验 6.7.1 实验条件和环境 6.7.2 总体设计 6.7.3 问题思考与实验要求 6.8 数字水印技术实验 6.8.1 实验条件和环境 6.8.2 总体设计 6.8.3 主要功能实现 6.8.4 系统运行说明 6.8.5 问题思考与实验要求 6.9 本章小结 参考文献

章节摘录

版权页：插图：（1）打开光驱程序功能：mciSendString（“set cdaudio door open”，NULL，0，NULL）（2）关闭光驱程序功能：mciSendString（“Set cdaudio door closed wait”，NULL，1，NULL）（3）得到CDAudio设备中的曲目总数：mciSendString（“status cdaudio number of tracks”，ReturnStr，128，0）4.远程关闭和启动计算机 控制对方计算机的操作方式，可以远程关闭计算机，目的是在重新启动后将木马加载到注册表中。

在木马程序中，这一功能是控制端Socket给被控制端Socket发出有关命令，被控制端接收到命令后，再执行关闭或启动计算机的操作，这里主要使用ExitWindowEX（）函数来实现。

1) ExitWindowEX（）功能：执行某种事件的函数。

格式：BOOL ExitWindowEX（UINT uFlags，DWORD dwReserved）参数说明：uFlags:指定系统操作功能，取值如下：EWX_FORCE强迫中止没有响应的进程，不保存文件而强制关机。

EWX_LOGOFF中止进程，注销已登录的用户。

EWX_SHUTDOWN保存文件并关闭计算机，如果是ATX电源，同时关掉系统电源，但要求有权限。

EWX_REBOOT重新启动计算机，但要求有权限。

EWX_SHUTDOWN关闭系统。

dwReserved:作为保留数，被系统忽略，值只能是0或1。

返回值：成功——返回非0值；失败——0。

2) OpenProcessToken（）功能：修改一个进程的访问令牌，首先要获得进程访问权限的句柄，这可以通过OpenProcessToken得到。

格式：BOOL OpenProcessToken（HANDLE ProcessHandle，DWORD DesiredAccess，PHANDLE TokenHandle）参数说明：ProcessHandle：要修改访问权限的进程句柄，用GetCurrentProcess（）获得。

DesiredAccess：参数指定要进行的操作类型，如要修改令牌，要指定第二个参数为TOKEN_ADJUST_PRIVILEGES。

TokenHandle:返回的访问令牌指针。

返回值：成功——返回TRUE，得到访问令牌句柄，然后用AdjustTokenPrivileges（）修改访问令牌；失败——0。

3) AdjustTokenPrivileges（）功能：修改并获取权限。

编辑推荐

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>