<<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

<<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。

<<信息安全对抗系统工程与实践>>

书籍目录

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