# 操作系统实验(windows)：

**实验名称**: 利用 Process Explorer 观察操作系统进程活动

**实验目标**:

1. 理解操作系统中进程的基本概念和活动。
2. 掌握使用 Process Explorer 工具监视和分析 Windows 操作系统中的进程。
3. 能够辨别进程的优先级、线程及相关资源使用情况。
4. 了解进程间的父子关系和关联。

**实验材料**:

1. Windows 操作系统（建议 Windows 10 或更新版本）。
2. Process Explorer 工具（可从微软官网 Sysinternals 下载）。
3. 电脑及实验环境。

---

## 一、Process Explorer 的基本使用与进程监控

### 步骤 1: 安装与启动 Process Explorer

1. 访问微软官网 Sysinternals 网站，下载 Process Explorer 工具。
2. 解压缩下载的文件，并双击 procexp.exe 启动工具。
3. 介绍工具的界面布局，主要包括进程列表、进程属性窗口、CPU 和内存使用情况。

### 步骤 2: 理解进程列表

1. 观察 Process Explorer 的进程树结构，识别每个进程的父子关系（Parent-Child）。
2. 选择几个常见的系统进程（如 explorer.exe、svchost.exe），查看其进程信息（右键点击进程，选择 "Properties"）。
3. 记录每个进程的基本信息，如进程 ID（PID）、线程数、句柄数、CPU 和内存使用率等。

### 步骤 3: 进程活动监控

1. 介绍 CPU 使用率、内存占用率、I/O 操作等监控指标。
2. 对比系统空闲状态与负载状态下的进程活动变化（例如，打开多个应用程序或任务）。

3. 让学生打开几个常用软件（如浏览器、文本编辑器等），观察新启动的进程，记录这些进程的资源使用情况。

**步骤 4：优先级管理**

1. 选择某一进程（如 Notepad），右键选择“Set Priority”选项，尝试调整进程优先级。
2. 观察 CPU 使用率和响应时间的变化，记录不同优先级对进程的影响。
3. 讨论优先级管理在多任务处理中的作用。

---

## 二、深入进程分析与进程异常检测

**步骤 5：分析进程线程和句柄**

1. 选择一个常用进程（如 chrome.exe），查看其线程和句柄信息。
2. 介绍线程的概念及其与进程的关系，观察每个线程的状态及 CPU 时间分配。
3. 让学生分析一个多线程进程（如浏览器）的多个线程，记录每个线程的功能和作用。

**步骤 6：监视动态库（DLL）**

1. 选择任一进程（如 explorer.exe），右键选择“Properties”，切换到“DLLs”选项卡。
2. 观察该进程加载的动态链接库（DLL）文件，并了解其与进程的关联。
3. 介绍 DLL 文件的作用，重点讲解进程如何共享资源。

**步骤 7：识别异常进程**

1. 让学生观察进程列表中的进程，找出可能的异常进程（如资源占用过高、名字异常的进程）。
2. 通过右键查看属性、Google 搜索进程名称等方式进一步调查该进程的来源。
3. 讨论如何应对和处理系统中可能的恶意进程。

**步骤 8：进程终止与系统影响**

1. 选择一个非系统关键进程，尝试使用右键选项中的 "Kill Process" 来终止该进程。
2. 观察系统或应用程序的反应，讨论强制终止进程对系统稳定性的影响。
3. 强调不要随意终止系统关键进程（如 wininit.exe、csrss.exe），讨论这些进程的重要性。

**学生讨论问题**:

1. 为什么内核进程的优先级通常很高?
2. 在多任务操作系统中，如何平衡用户体验与系统稳定性?
3. 如果某个进程占用了大量的 CPU 或内存资源，操作系统应该如何处理?