Windows核心编程学习笔记

目录

[1PE文件结构 2](#_Toc490728821)

[1.1 PE头结构 4](#_Toc490728822)

[1.1.1DOS头 4](#_Toc490728823)

[1.1.2虚拟地址和文件偏移地址的换算（RVARAW） 4](#_Toc490728824)

[1.2 IAT（导入地址表） 5](#_Toc490728825)

[1.3 notepad.exe 练习 5](#_Toc490728826)

[2运行时压缩（加壳） 6](#_Toc490728827)

[3UPX调试脱壳 6](#_Toc490728828)

[3.1 跟踪代码和OEP定律 6](#_Toc490728829)

[3.2 修复IAT 7](#_Toc490728830)

[4基地址重定位 7](#_Toc490728831)

[5删除.reloc节 8](#_Toc490728832)

[6Upack PE文件头详细分析 8](#_Toc490728833)

[7Upack 调试 查找OEP 9](#_Toc490728834)

[8内嵌补丁 9](#_Toc490728835)

[9Windows消息钩取 9](#_Toc490728836)

[10击键记录器 10](#_Toc490728837)

[11Dll注入 10](#_Toc490728838)

[12DLL卸载 13](#_Toc490728839)

# 对程序错误的处理

GetLastError()函数定义DWORD GetLastError()。该函数返回一个32位的错误代码

# Unicode

## 编写Unicode源代码

标准C的头文件String.h中定义了wchar\_t的数据类型，是Unicode的数据类型。

定义方法：typedef unsigned short wchar\_t

# 内核对象

每一个内核对象都包含一个使用计数。使用计数是内核对象类型的数据成员之一。如果使用计数降为0，则内核对象会被撤销。

# 进程

