黑客防线 C/C++黑客编程.2.2

本节前置知识要求:

1.基本的 C 语言语法的掌握
2.对 Windows 数据结构有一定的基础
3.有一定的自我学习能力.
4.对上一节内容有切实的理解

本节课主要内容:

1. 了解一些 POP3 协议
2. 实现 POP3 协议中用户验证的部分
3. 在实现了用户验证的基础上构造一个 POP3 帐号密码枚举器

主要模块:

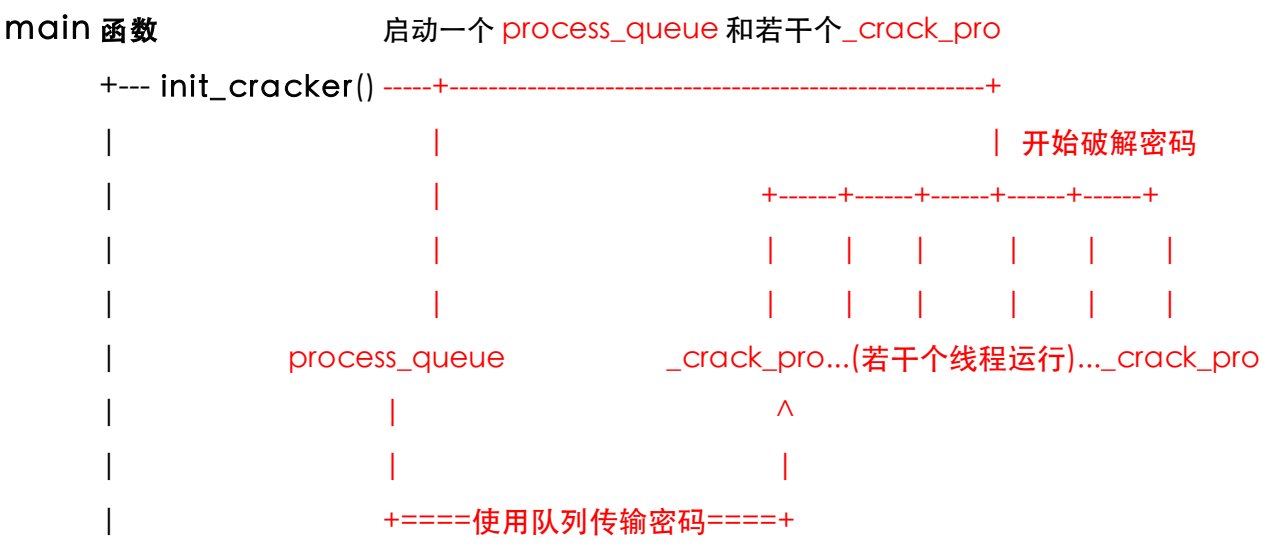
使用了上节课的程序框架，改变破解函数的实现即可。

用户验证部分的协议:

登录指令:
    user [用户名]
密码:
    pass [密码]
反馈提示, 成功会在第 2 和第 3 字节返回'O'和'K'

程序流程:

红色部分为线程函数:



|

+--- crack_pwd() waiting <----------等待以上的所有线程返回

|

+--- free_cracker()

Exit 退出程序

破解执行函数_crack_pro 的流程：

开始

无尽循环

读取管道中的字符串

如果 是退出标识 则

退出循环

否则

尝试连接 pop3 服务器

发送用户名

如果 返回 OK 则

发送密码

如果 返回 OK 则

枚举状态 = 成功

否则

枚举状态 = 密码错误

否则

枚举状态 = 登录失败

输出枚举状态对应的各个信息

如果 枚举状态 = 成功 则

退出循环

否则

继续下次循环尝试

结束