2021年中国工业互联网安全大赛核能行业赛道writeup之机房密码

原创

苦行僧(csdn) 于 2021-10-19 00:12:26 发布 47 收藏
分类专栏： 信息安全 文章标签： CTF writeup IDA base64

本文链接：https://blog.csdn.net/qpeity/article/details/120818986

附件题：机房密码

题目描述：

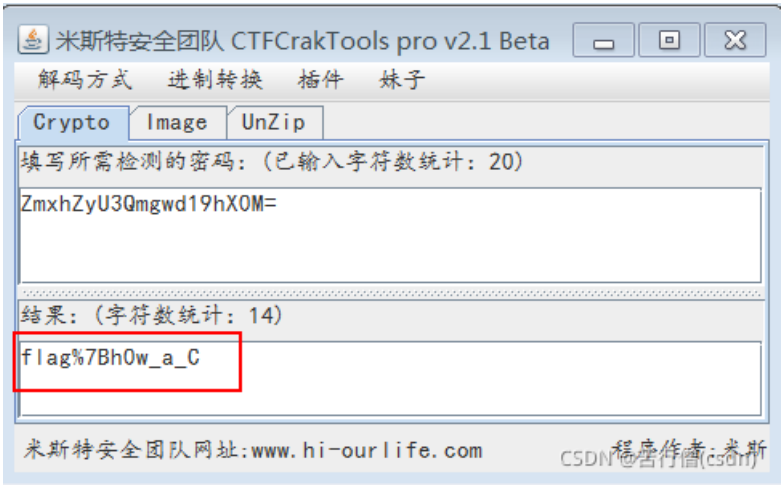
> （具体描述忘记了）
>
> 经过黑客人员的不屑努力，在上位机上发现了登录密码的一半信息，剩下的一半要靠你们继续努力辣！！！
> ZmxhZyU3Qmgwd19hX0M=

附件下载：

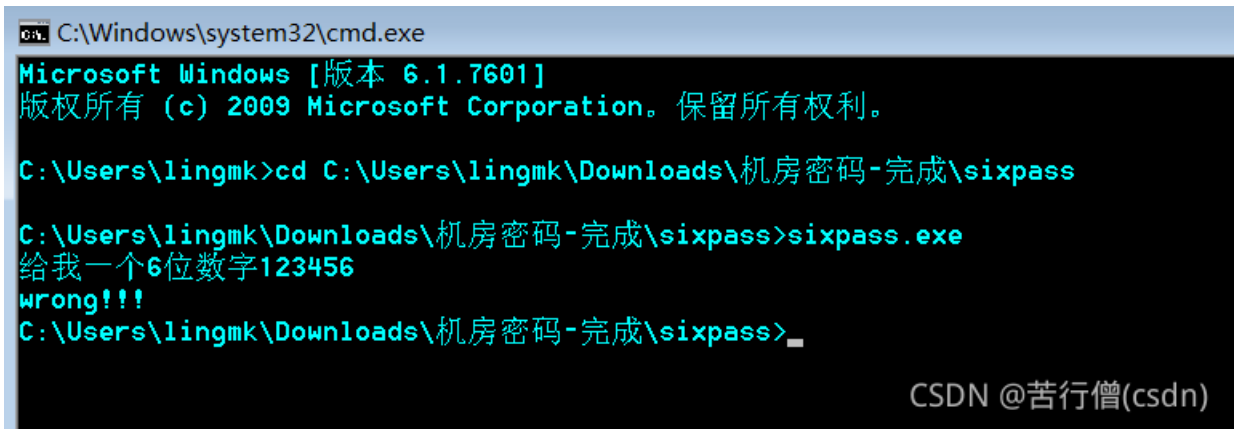
2021-10-12T15_42_23.295652+00_00sixpass.zip-网络攻防文档类资源-CSDN下载

下载到附件，解压发现里面有两个文件，一个 tips.txt，另一个 sixpass.exe 。

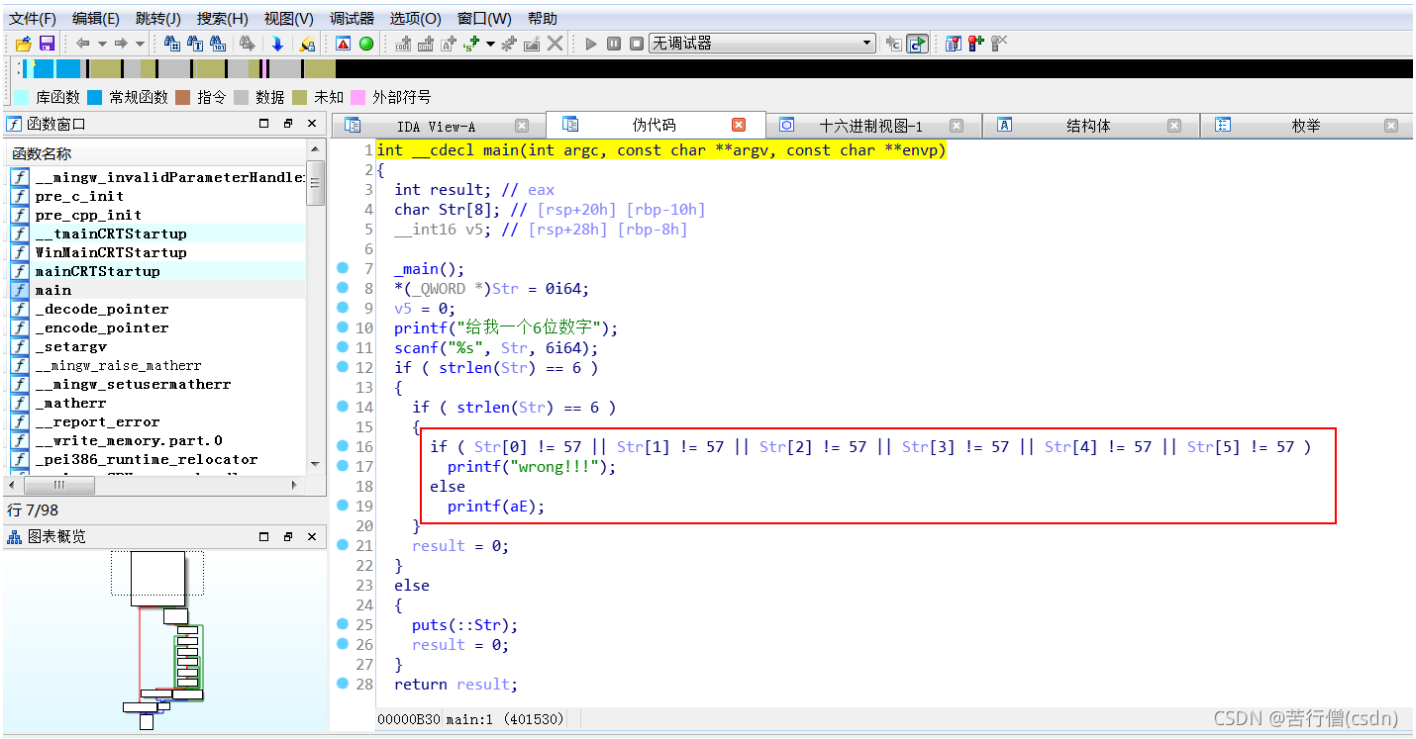
tips.txt里面有一段话，经过黑客人员的不屑努力，在上位机上发现了登录密码的一半信息，剩下的一半要靠你们继续努力辣！！！ ZmxhZyU3Qmgwd19hX0M= 。这个很好解决，用CTFcrackToos 工具，做 base64 转码，就得到了 flag 的前半部分。注意转码以后有个 %7B ，要对 %7B 敏感，这就是左花括号，所以前半部分是 flag{h0w_a_C 。



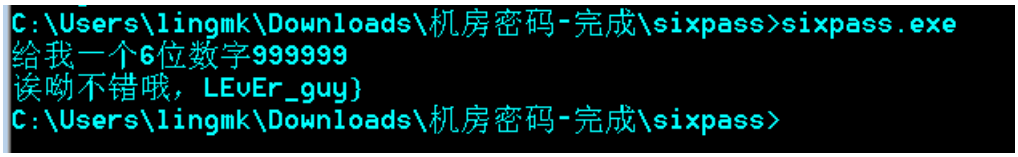
运行一下 sixpass.exe，看来是要6位密码。



对 sixpass.exe 查壳，发现没有壳。那么用 IDA 打开sixpass.exe反编译，在 main 函数按 F5 得到伪代码。注意圈出来的部分，如果6位数字都不是整型57就错，因此判断6位数字是6个整型57，整型数57就是 ASCII 字符9。



执行sixpass.exe 输入 999999 得到后半段 LEvEr_guy} 。



把前后两个半段拼接到一起，就得到 flag{h0w_a_CLEvEr_guy}