2016 年第 28 题

大家好，我是胡一米。这期视频是关于 2016 年看雪 CTF 第 28 题解题资料。

一、简介

1.1 录制说明

视频是基于其他大佬文字 Writeup 录制的，所以在视频操作之前就已知了该题中的各种坑，如反调试等，所以不再演示踩坑过程。

1.2 录制参考

第 28 题主要参看了 HighHand、风间仁以及 Quizow 的 Writeup，链接如下：
HighHand:
https://bbs.pediy.com/thread-214884.htm
风间仁：
https://bbs.pediy.com/thread-214861.htm
Quizow:
https://bbs.pediy.com/thread-214854.htm

1.3 内容简介

在本期中，主要讨论 6 个问题。这 6 个问题可能与最终的 Key 没有太大的联系，但题目中既然出现了，还是说一说。此 6 个问题分别是：
a. 去除重定位过程
b. MD5 算法
c. RC4 算法
d. 内存加载
e. luadec 工具
f. 穷举六阶幻方得到最终的 Key

二、视频操作

2.1 静态分析定位关键点

结合其他大佬的分析过程，可以直接定位到关键点。.
a. MD5 算法
b. RC4 算法

条件：
buf[30] == '8' && buf[40] == 'I' && buf[46] == '4' && buf[58] == '0'
解码之后为.tra2crack 和 6 阶幻方

2.2 动态调试其加密过程

通过动态调试，理解程序内存加载过程。
a. 内存加载
b. luadec 工具

https://github.com/viruscamp/luadec

```
git clone https://github.com/viruscamp/luadec
cd luadec
git submodule update --init lua-5.3
cd lua-5.3
make linux
cd ../luadec
make LUAVER=5.3
```

fatal error: readline/readline.h: No such file or directory
sudo apt-get install libreadline-dev

LnRyeTJjcmFjawwrKiwQFBcTKiYWIR8cGh0dIhweICEdGS4lEBQoEiUUEw0pLw

2.3 穷举验证码

使用 visual studio，穷举验证码。这里直接使用 HighHand 大佬贴出的代码。

大佬直接把 RC4 算法抠出来了。

三、小结

题目很好。