工控安全异常取证分析

发表于 2021-09-01 分类于 Challenge ， 2021 ， 工业信息安全技能大赛 ， 线上赛-第一场
Challenge | 2021 | 工业信息安全技能大赛 | 线上赛-第一场 | 工控安全异常取证分析

点击此处获得更好的阅读体验

WriteUp来源

来自Venom战队

题目描述

> *网络安全人员小吕在工厂中发现某台工程师站主机可能感染了病毒，小吕将磁盘导出后请你能帮忙一起分析出异常。flag格式为：flag{}*

题目考点

- *磁盘数据取证*

解题思路

解压出来两个文件，一个1122，文件挺大，另一个是 112233只有1KB，一看就知道是个vmdk。

打开112233，找到其真实名称

将112233改名为 Windows Server 2003 Web Edition-1.vmdk

将1122改名为 Windows Server 2003 Web Edition-1-flat.vmdk

用 DiskGenius 打开，应该是个NTFS分区FDD，没有分区表的那种。

从名为 mp4.mp4 的文件中提取出一段 ascii 字符串

提取出字符串

```
1 3441344134383435353535323533344534423541344135353334353333323446344134453433353533235363433353434413541343435353535353434333436344233353443343634373536343334433442354134343
```

之后 按照如下顺序进行解码即可得到flag，HEX -> HEX -> B32 -> B32 -> B32 -> B64 -> B64 -> HEX -> B32 -> B32 -> B64 -> B64

Flag

```
1 flag{wh4t_a_w0nderful_d4y}
```

- ***本文作者：*** *CTFHub*
- ***本文链接：*** *https://writeup.ctfhub.com/Challenge/2021/工业信息安全技能大赛/线上赛-第一场/mm3K2tZNbTsL9S2TBnVPpf.html*
- ***版权声明：*** *本博客所有文章除特别声明外，均采用 BY-NC-SA 许可协议。转载请注明出处！*

 # Challenge # 2021 # 工业信息安全技能大赛 # 线上赛-第一场
隐藏的工程
异常的梯形图分析