简单的工控固件逆向

发表于 2021-01-25 分类于 Challenge， 2019， 工业信息安全技能大赛， 山东站
Challenge | 2019 | 工业信息安全技能大赛 | 山东站 | 简单的工控固件逆向

点击此处获得更好的阅读体验

WriteUp来源

来自MO1N战队

题目描述

> *根据情报得知工控现场发现某SCADA系统被黑客攻破,附件为黑客在目录留下的文件和当时时间段捕获到的一部分流量包,你能根据这些信息分析出蛛丝马迹来么flag形式为flag{}*

题目考点

- *C#逆向*
- *AES*

解题思路

题目位c#编写。构造了一个vm再vm中实现了aes加密。找到密钥和IV然后解密比对的数据即可

```
EncData : VFYtetYzaM9NlCMYNT0wQpP0HpEX7ZQygrVu1c4XPPdVhkKIrH1AnVqdr6EDZM/RpwsPS1U3DO60ArOVTChEWA==
Key : FA7AD31806332E62
IV : 0000000000000000
加密方式: AES-128-CBC PKCS7Padding
```

Flag

```
flag{e7bf2e667ab3-b6d6-8574-8ef3-d3b7-c350-c6278667a9}
```


 # Challenge # 2019 # 工业信息安全技能大赛 # 山东站
奇怪的文件
隐藏的黑客