隐藏的黑客

发表于 2021-01-25 更新于 2021-02-16 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 | 隐藏的黑客

点击此处获得更好的阅读体验

WriteUp来源

https://www.dazhuanlan.com/2019/12/30/5e09dcd470284/

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

- *zip密码爆破*

解题思路

下载题目附件得到一个流量包：1.pcapng

分析HTTP流量,追踪流-HTTP,可以发现头PK...为一个压缩文件

找到该数据包，在No.481位置通过导出字节流进行导出为zip

另一个比较简单的方法，也可直接用`binwalk -Me`就能把文件提取出来

导出的zip为2.5zip,发现还有另外一个压缩文件upload.zip

其中2.5.zip需要解压密码：

通过分析猜测解压密码需要从upload.zip得到。

思路为：把upload里面的密码提取出来，然后用这个提取出来的密码去爆破

爆破成功。

Flag

```
1 flag{9a72c3d5e74f6051bb3b3590fa9319fe}
```

- ***本文作者：** CTFHub*

- ***本文链接：*** *https://writeup.ctfhub.com/Challenge/2019/工业信息安全技能大赛/山东站/fSMJzS7vnw4QHCeYqfJsnP.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 # 2019 # 工业信息安全技能大赛 # 山东站
简单的工控固件逆向
工控安全取证