MISC题-首次遇到题型

原创

lierpang_ 于 2021-11-05 10:09:33 发布 2393 收藏

分类专栏： CTF 文章标签： 安全

本文链接：https://blog.csdn.net/lixin_1010/article/details/121157344

1. 第一题

https://buuoj.cn/challenges#[GUET-CTF2019]zips

第一重真加密，暴力破解，zip密码然后得到111.zip伪加密，解密后得到两个文件flag.zip和setup.sh

```
PS E:\CTF\zips\222\111> cat .\setup.sh
#!/bin/bash
#
zip -e --password=`python -c "print(__import__('time').time())"` flag.zip flag
PS E:\CTF\zips\222\111> python -c "print(__import__('time').time())"
1636076635.3
```

据说python2精度是2位小数，因此使用ARCHPR掩码破解

得到文件

打开发现flag

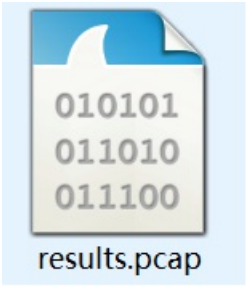
flag{fkjabPqnLawhvuikfhgzyffj}

2.第二题

查看答案

https://buuoj.cn/challenges#%E7%99%BE%E9%87%8C%E6%8C%91%E4%B8%80

下载解压后发现是一个抓包文件



打开后文件——导出对象——http输出多个jpg图片

使用kali内exiftool工具，发现一半flag

```
root@kali:~/CTF_EXAM# exiftool *|grep flag
XP Comment                      : 恭喜你！找到一半了，还有另一半哦！flag{ae58d0408e26e8f
```

wireshark内筛选tcp流，tcp.stream eq 114发现另一半flag

```
.....m`.U`O..~b0R.NJS.N....       g.S.NJS.T..2.6.a.3.c.
0.5.8.9.d.2.3.e.d.e.e.c.}.......http://ns.adobe.com/xap/1.0/.<?xpacket begin='...'
id='W5M0MpCehiHzreSzNTczkc9d'?>
```

3.第三题

https://buuoj.cn/challenges#[UTCTF2020]docx

下载后发现是docx文件，丢尽winhex发现是压缩包，修改后缀为rar，解压缩得到flag