

## 8.4

### 1.直接签到

题目	讨论区 (26)	WriteUp	详细数据	版本
----	----------	---------	------	----

# [第五空间 2021]签到题

1分 其他 阴阳怪气加密 电子取证 ★★☆☆☆ 7 +

题目描述

flag{welcometo5space}

该题目复现环境尚未取得主办方及出题人相关授权，如果侵权，请联系管理员删除。得到的flag请使用NSSCTF{}格式提交。

开启👁️

改变格式之后成功提交

### 2.直接签到

题目 讨论区 (7) WriteUp 详细数据 版本

## [广东强网杯 2021 个人决赛]签到题

1分 压缩包分析 其他 社会核心价值观 ★ ★ ☆ ☆ ☆ 2 +

题目描述

flag{welcome\_to\_qwb}  
该题目复现环境尚未取得主办方及出题人相关授权，如果侵权，请联系管理员删除。得到的flag请使用NSSCTF{}格式提交。

转变格式直接成功提交

### 3. 双层解码类签到

题目 讨论区 (8) WriteUp 详细数据 版本

## [长城杯 2021 院校组]签到

1分 编码分析 ASCII 字符编码 ★ ★ ☆ ☆ ☆ 3 +

题目描述

5a6d78685a3374585a57786a6232316c5833527658324e6f5957356e5932686c626d64695a544639  
该题目复现环境尚未取得主办方及出题人相关授权，如果侵权，请联系管理员删除。得到的flag请使用NSSCTF{}格式提交

首先看到一串数字字母经过一番学习为密码类题，刚开始在随波逐流中一键解码发现结果很奇怪，随后学到用赛博厨子，在附有详解后知晓其为双层解密。先将十六进制转换为字符串，再base64解密，最后成功得到flag。

最新一次构建: 2 years 之前

设置 关于/帮助

配方

从十六进制编码转换

Delimiter: None

Base64 转文本

Alphabet: A-Za-z0-9+/=

Remove non-alphabet chars  Strict mode

输入

```
start: 0 length: 80
end: 80 length: 80
length: 80 lines: 1
```

```
5a6d78685a3374585a57786a6232316c5833527658324e6f5957356e5932686c626d64695a544639
```

输出

```
start: 0 time: 1ms
end: 30 length: 30
length: 30 lines: 1
```

```
flag{welcome_to_changchengbe1}
```

分步执行 自动制作

#### 4. 签到

题目 讨论区 (8) WriteUp 详细数据 版本

## [陇剑杯 2021]签到 ✔

1分 流量分析 Webshell流量 日志审计 ★★☆☆☆ ❤️ 7 +

题目描述

此时正在进行的可能是\_\_\_\_\_协议的网络攻击。(如有字母请全部使用小写, 填写样例: http、dns、ftp)。得到的flag请使用NSSCTF{}格式提交。

读题之后思考突破点是否在需要填空的那个内容, 再看到后面例子之后, 按照往前经验猜测其为http, 最后按照格式提交成功。

#### 5. 流量分析类签到

未成功做出来, 但已知所需工具为wireshark

6.huaji

# [NISACTF 2022]huaji?

1分

图片隐写

压缩包分析

图片分离

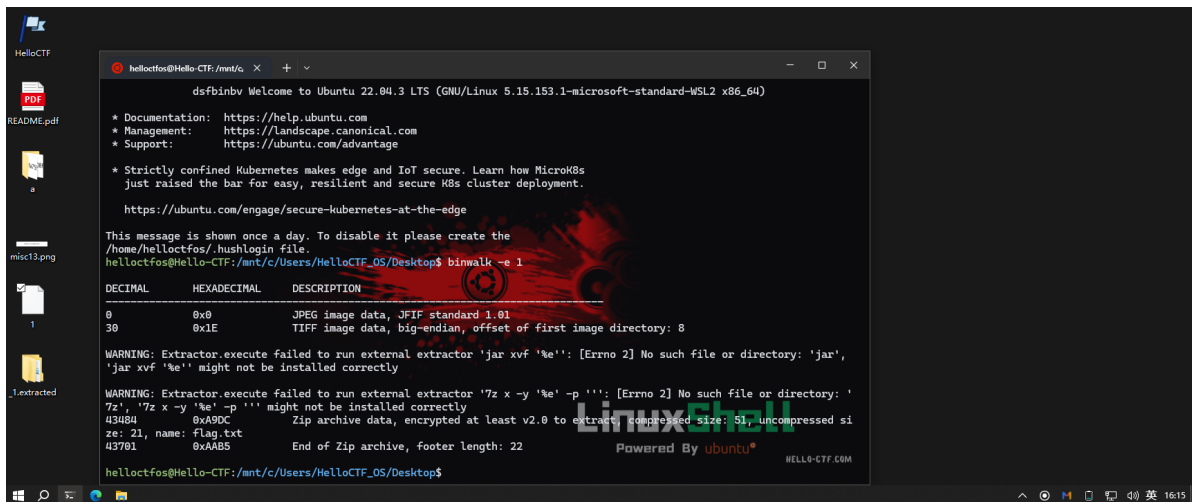
★★★★☆

❤ 8

+

题目描述

flag格式为NSSCTF{}



```
helloctfos@Hello-CTF:/mnt/c/...
dfsfbinbv Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.153.1-microsoft-standard-WSL2 x86_64)

* Documentation: https://help.ubuntu.com
* Management:   https://landscape.canonical.com
* Support:      https://ubuntu.com/advantage

* Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
  just raised the bar for easy, resilient and secure K8s cluster deployment.

https://ubuntu.com/engage/secure-kubernetes-at-the-edge

This message is shown once a day. To disable it please create the
/home/helloctfos/.hushlogin file.
helloctfos@Hello-CTF:/mnt/c/Users/HelloCTF_OS/Desktop$ bimalk -e 1
DECIMAL      HEXADECIMAL  DESCRIPTION
-----
0            0x0          JPEG image data, JFIF standard 1.01
38           0x1E        TIFF image data, big-endian, offset of first image directory: 8

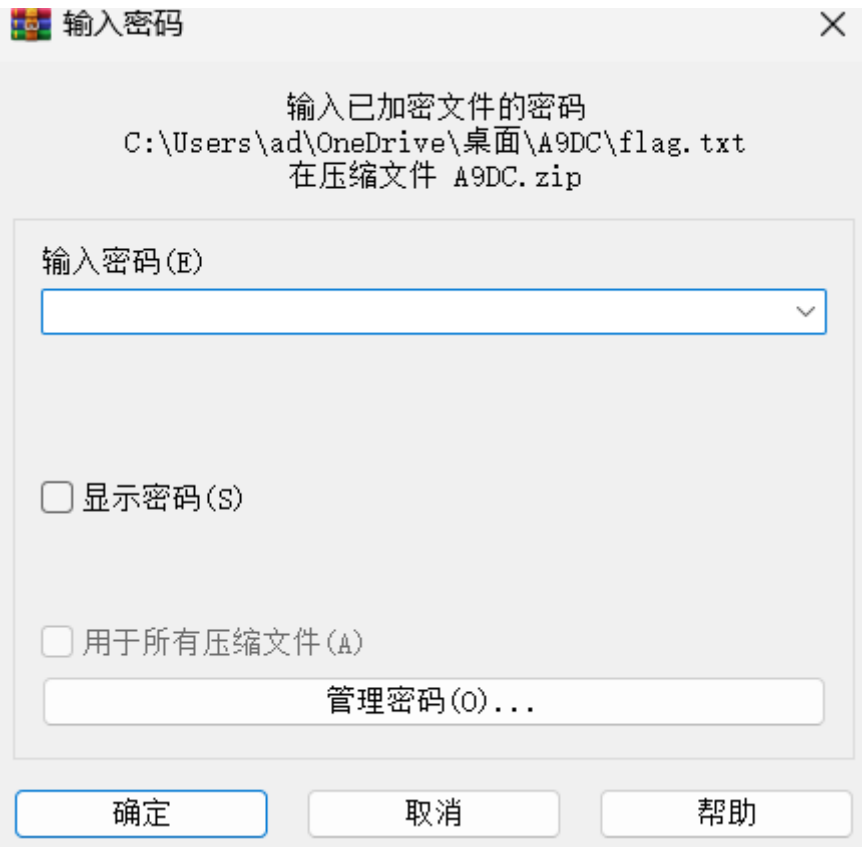
WARNING: Extractor.execute failed to run external extractor 'jar xvf %e': [Errno 2] No such file or directory: 'jar',
'jar xvf %e' might not be installed correctly

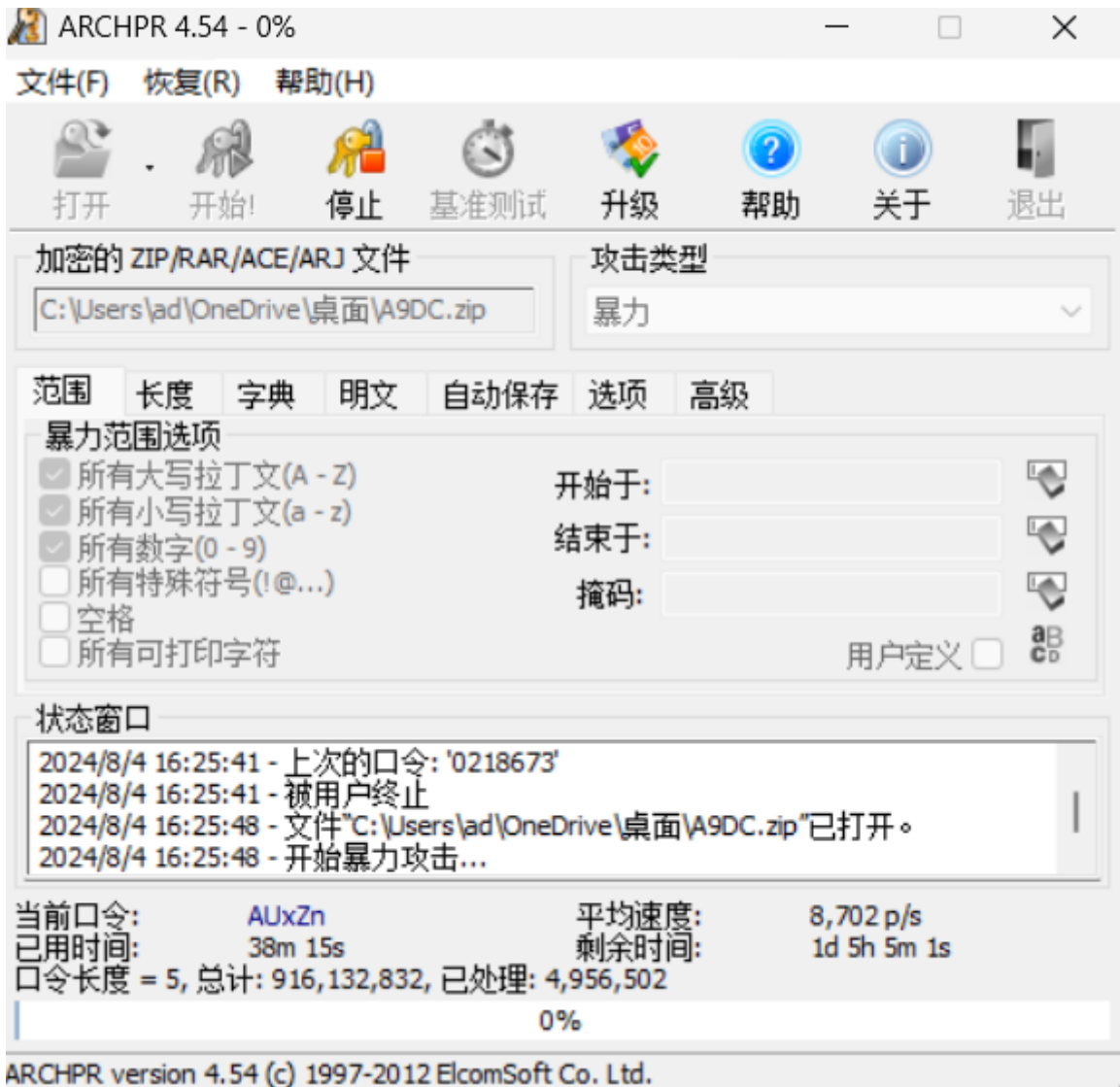
WARNING: Extractor.execute failed to run external extractor '7z x -y %e -p ''': [Errno 2] No such file or directory: '
7z', '7z x -y %e -p '' might not be installed correctly
43084        0xA9DC      Zip archive data, encrypted at least v2.0 to extract compressed size: 51, uncompressed si
ze: 21, name: flag.txt
43781        0xAAB5      End of Zip archive, footer length: 22

Powered By ubuntu
HELL0-CTF.COM

helloctfos@Hello-CTF:/mnt/c/Users/HelloCTF_OS/Desktop$
```

由知识点提示之间分离，得到了一个压缩包，但是加密了的，随后用爆破解密，但是时间所需很长，就没思路了。





ARCHPR version 4.54 (c) 1997-2012 ElcomSoft Co. Ltd.

## 7. 套娃

直接用binwalk分离得到

名称	类型	压缩大小	密码保护	大小
RC4data.txt	文本文档		1 KB 否	
swpu.xls	XLS 工作表		6 KB 否	

第二个打不开，第一个是个乱码

