DASCTF Oct X 吉林工师 欢迎来到魔法世界 部分wp

原创

云空5323 于 2021-11-21 17:24:11 发布 332 收藏
分类专栏： ctf2021 文章标签： 其他

本文链接：https://blog.csdn.net/weixin_44088994/article/details/121453953

整理一下自己的思路，存一下题（呜呜呜菜狗就是菜狗wp都看不懂

参考：七月大佬DASCTF Oct X 吉林工师 欢迎来到魔法世界～ WP – 七月的摸鱼历程

魔法密文 Writeup | DASCTF Oct X 吉林工师_张麦麦的博客 zhangmaimai.com-CSDN博客

web：

DASCTF Oct X 吉林工师 欢迎来到魔法世界～(魔法少女杯) web 迷路的魔法少女_llx101388627的博客-CSDN博客

DASCTF Oct X 吉林工师 迷路的魔法少女_cjdgg的博客-CSDN博客

签到
1.give you flag
2.闯入魔塔的魔法少女
3.魔法信息
4.魔法秘文
5.卡比卡比卡比
6.不可以色色
7.哥哥（暂无）
8.魔法少女的迷音

签到题：

（完全不知道咋做的）
利用nc进入，输入观察返回

```
Traceback (most recent call last):
  File "talk.py", line 15, in <module>
    age = input("> ")
  File "<string>", line 1
```

尝试python2的input漏洞：__import__('os').system('dir')
发现存在flag.txt，输入__import__('os').system('cat /flag.txt')获得flag
flag{4e8a6edd-912f-4ee3-a39d-86dd568f9901}

1.give you flag：

下载得到flag1，打开发现是嵌套压缩包
winhex打开滑轮滑到大概中间位置可以发现
flagR0RWRldJezdnZ3FnbGwzanl1a2RuY3N0aTlpY3BjM2ZlYjB2NW9wfQ==
转base64得到GDVFWl{7ggqgll3jyukdncsti9icpc3feb0v5op}为凯撒加密，移动三位得到
DASCTF{7ddndii3gvrhakzpqf9fzmz3cby0s5lm}

2.闯入魔塔的魔法少女：

swf文件是flash小游戏，使用ffdec打开，直接搜索即可得到
恭喜过关，这里是你的flag:
DASCTF{23dvkjzr3juboiavztbncaxftfpyq5gz}

3.魔法信息：

流量分析发现zip压缩包，提取出来得到eeeee.pdf，使用010打开pdf，点击上方hex小按钮，出现一个模板结果，发现值那一栏里面出现了规律的DASCTF{，记下来即为flag
DASCTF{25da50b7993c0db55867a5a51f32f35c}
（成功提取能打开的pdf，但死在了没文化上，没想起用010，分析半天没出来）

4.魔法秘文

判断为zip，更改扩展名，解压得到png图片，foremost得到压缩包2.zip
flag.txt为加密的，通过注释得到密码由32个中文组成
解压魔法萝莉简体，用记事本打开，看到结尾部分有一串字符：
RegularLolita:Version 2.01Version 2.01;October 14, 2021;FontCreator 13.0.0.2675 64-bitModified By Y'
通过度娘得到FontCreator是一款设计字体的软件，下载，并用它打开字典（魔法萝莉简体），成功打开
字典的结尾还有一串字符：
%E4%BA%8C%E5%8D%81%E4%B8%81%E5%8E%82%E4%B8%83%E5%8D%9C%E4%BA%BA%E5%85%
对其进行url_decode转化，得到：
二十丁厂七卜人入八九几儿了力乃刀又三于干亏士工土才寸下大丈与万上小口巾山千乞川亿个勺久凡及夕丸么广亡门义之尸弓己已子卫也女飞刃习叉马乡丰王井开夫天无元专云扎艺木五支厅不太犬区历尤友匹车巨牙屯比互切瓦止少日中冈贝内水见午牛手毛气升长仁什片仆化仇币仍仅斤爪反介父从今凶分乏公仓月氏勿欠风丹匀乌凤勾文六方火为斗忆订计户认心尺引丑巴孔队办以允予劝双书幻玉刊示末未击打巧正扑扒功扔去甘世古节本术可丙左厉右石布龙
（我卡死在这里了，没联系起来）
使用FontCreator的测试功能，输入以上转码出来的文字，发现部分文字的形状是有所旋转的，挑出来：
丁厂八九几刀于干工上小个门之马王云木尤切少牛分六方丑玉古节可石布
为flagtxt密码，输入得到：
DASCTF{4b7e33769d9bd2b7dbc1790ae39397b9}

5.卡比卡比卡比

文件名字带有内存取证，使用volatility进行内存取证
volatility -f mem.raw imageinfo得到系统信息
volatility -f fujian.raw --profile=Win7SP1x64 iehistory，发现存在key文件
volatility -f fujian.raw --profile=Win7SP1x64 filescan | grep key搜索到地址，
volatility -f fujian.raw --profile=Win7SP1x64 dumpfiles -Q 0x3e5e94c0 --dump-dir=./下载key
key内容为：我记得我存了一个非常棒的视频，但怎么找不到了，会不会在默认文件夹下。
视频的默认文件夹叫Video，寻找带Video的文件（注意大小写）
看到ohhhh文件，下载
volatility -f 1.raw --profile=Win7SP1x64 dumpfiles -Q 0x3e248a90 --dump-dir=./
打开得到xzkbyyds!
volatility -f 1.raw --profile=Win7SP1x86 cmdscan查看cmd命令使用历史
看到5201314字样，查找字样，得到压缩包，发现被加密
volatility -f easy_dump.img --profile=Win7SP1x64 hashdump timeliner 得到用户名及哈希密码
（不知道为什么得到qiyue的哈希密码，
10961c67822ee59af54bdc9e91f2801f 但解不了，而且其他Administrator、guest等密码都为空，不知道是不是哪有问题，七月wp上的尝试mimikatz不会弄）
压缩包密码：MahouShoujoYyds，解压得到一个python的编程文件，把key补到上面，
得到exp.py，编写逆向py.py（我也不知道咋编的）
运行，得到!@#$importance，为一张gif图片
观察发现图片少了一截，更改尝试
gif的宽高在6 7 8 9四个字节内，其中6 7字节为宽， 8 9字节为高，且为小端序储存方式。
故宽为0077，高为0067，将高改回0077，使用stegsolve看动图，在第115帧发现flag
DASCTF{Kirby_Yyds}

6.不可以色色

（没做出来）
解读动态图无果，通过网页的F12可以看出有给video的提示，尝试获得video.zip
解压得到mp4，发现开始的几行字不符合格式，去掉加上
00 00 00 20（这部分不明白为什么加20而不是其他）
66 74 79 70（ftyp）
可以得到一段动画，在开头和结尾部分有两个码
二维码有多种：PDF417、QRCCode、Data Matrix、Maxi Code、Code 49、Code 16K、Code One
判断为PDF417，将两张图合并，用OnBarcode.com_Free_PDF417_Scanner扫即得
DASCTF{8e2d479e26b3093651293f9fa26e3404}

8.迷音：
发现压缩包注释中atom128，搜索，得到https://www.persona-shield.com/atom128c.htm
全是英文看不懂，但有decrypt的选项，把上面一行粘进去，得到
passswowoowowddddddddddddddddddddddddddd
解压压缩包，得到wav，声音很奇怪，看了wp为倒放，用goldwave打开，反转，播放，听到数字，记录：
151,55,97,51,49,53,54,48,98,153,153,51,150,50,48,99,57,97,52,57,50,102,97,153,54,48,49
到这一步解不下去了，

未完待续