

wmctf2020-记录-writeup

原创

拾光、 于 2020-08-03 12:34:12 发布 3540 收藏 3

分类专栏: [ctf](#) 文章标签: [wmctf](#) [ctf](#) [wmctf2020](#) [writeup](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/wdearzh/article/details/107748481>

版权



[ctf](#) 专栏收录该内容

11 篇文章 0 订阅

订阅专栏

目录

Misc: [sign-in](#)

Misc: [XMAN_Happy_birthday!](#)

Reverse: [easy_re](#)

周末参加了一下wmctf2020, 只做出了三道简单题目。简单记录一下。

Misc: sign-in

welcome to WMCTF2020, here is your flag: <https://t.me/WMCTF>

打开网址发现拒绝连接, 因为是个短网址, 尝试访问短网址地址, 同样的错误。搜了下域名发现是国外地址, 找了个F墙软件成功打开, 里面需要下载的app, 下载安装上加入提示的群组, 在聊天框上方里即可看到flag。

Misc: XMAN_Happy_birthday!

下载下载是一个zip文件, 解压失败, 网上找了下zip文件格式, 改了下文件头, 也不对。

继续往下看看到最后的时候发现是做了逆序的文件, 写个脚本把文件内容再做个逆序就可以了。

```
000bfda0h: F7 27 C0 81 32 01 0E 08 7B B8 20 4B 77 77 70 40 ; ?纒2...{?Kwmp@
000bfdb0h: 80 5B B8 26 07 BB 82 5D C1 6E EE E0 F0 68 27 04 ; €[?.粹]群钹錡'.
000bfdc0h: EE E0 90 08 10 EE 0C 0C C3 DA 2D 10 5B 1C 54 05 ; 钹?...泌-.[.T.
000bfdd0h: B7 9C 00 00 03 E8 04 00 00 03 E8 04 01 00 0B 78 ; 窠...?...x
000bfde0h: 75 5F 22 96 09 5F 22 95 43 5F 22 4B 9C 07 00 0D ; u_"?"_崑_"k?...
000bdfd0h: 54 55 67 70 6A 2E 72 65 74 73 6F 70 00 20 00 0A ; TUgpj.retsop.
000bfe00h: 00 0C 00 A2 00 00 00 00 00 00 00 00 50 FE 63 20 ; ...?...P批
000bfe10h: 00 08 00 08 00 14 04 03 4B 50 00 00 00 1D 00 00 ; .....KP.....
000bfe20h: 00 1F 2C 4C 1D 00 08 07 4B 50 00 02 E5 A9 B3 B3 ; ..,L....KP..濛吵
000bfe30h: F4 75 F0 8F 8C A9 31 48 C9 2A 2C CA 4F 8C A8 28 ; 麵錄余1H?,蒂少(
000bfe40h: 2C 48 F6 AB 71 0E 75 F7 0B 00 00 03 E8 04 00 00 ; ,H弄q.u?...?...
000bfe50h: 03 E8 04 01 00 0B 78 75 5F 22 95 DD 5F 22 95 DD ; .?...xu_"噉_"噉
000bfe60h: 5F 22 95 DD 07 00 0D 54 55 74 78 74 2E 67 61 6C ; "噉...TUtxt.gal
000bfe70h: 66 00 20 00 08 00 00 1D 00 00 00 00 00 00 00 ; f. ....
000bfe80h: 00 50 FE 8D 38 00 08 00 08 00 14 04 03 4B 50 ; .P關8.....KP
```

上图可以看到倒序的 flag.txt和 destop.jpg文件名字符串, 还有最后方是个倒序的 zip文件开头。

写个倒序处理文件的脚本:

```
with open("D:\\ctf\\wmctf\\XMAN\\daolnwod.zip","rb") as f:
    tmp = f.read()
with open("D:\\ctf\\wmctf\\XMAN\\daolnwodreverse.zip","wb") as f:
    f.write(tmp[::-1])
```

解压新生成的文件即可。

Reverse: easy_re

题目描述: The flag is hidden in the perl code, can you find it?

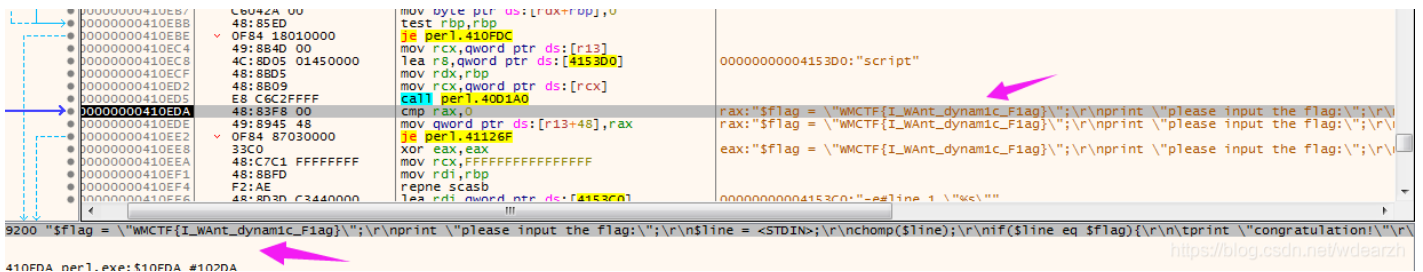
使用ida打开发现是个64位的程序,看题目应该是perl脚本转成的exe程序,网上搜了下perl反编译得工具没有找到。

执行了一下如图:

```
D:\ctf\wmctf\easy_re>perl.exe
please input the flag:fffff
no,wrong
D:\ctf\wmctf\easy_re>
```

使用ida查看字符串也没有找到 这两字符串,点了动态调试,(以前没用过ida的动态调试,olldb没法调试64位程序)考虑应该会将perl代码加载到内存中,随便点了一些 提取内存快照后 搜索字符串找到了字符串。不过还是不太会动态调试就先放下了。

第二天下了个x64dbg 单步跟踪,没花多久就找到了perl代码:



获取到的perl脚本:

```
$flag = "WMCTF{I_WAnt_dynamic_Flag}";
print "please input the flag:";
$line = <STDIN>;
chomp($line);
if($line eq $flag){
    print "congratulation!"
}else{
    print "no,wrong"
}
```