


攻防世界misc 高手进阶区 (慢慢更

原创

黄稚女  于 2019-05-29 15:28:06 发布  4847  收藏 4

分类专栏: [CTF](#)

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/weixin_43928140/article/details/90671891

版权



[CTF 专栏收录该内容](#)

17 篇文章 0 订阅

订阅专栏

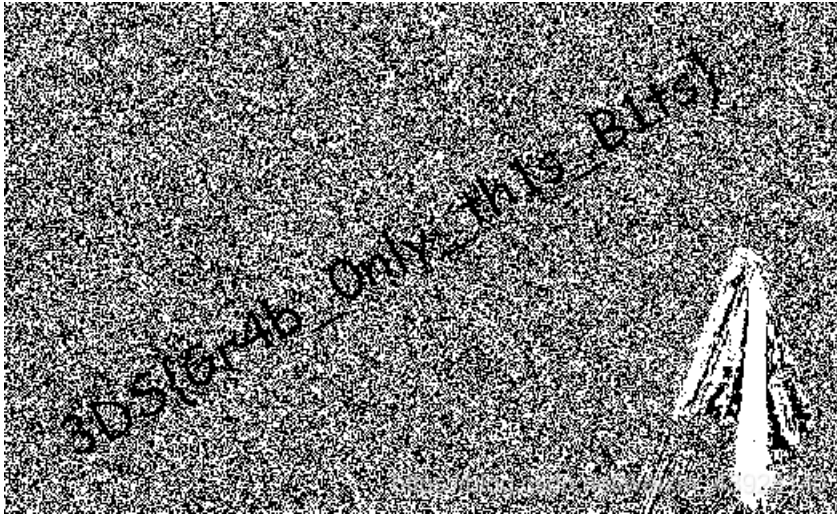
菜鸡生活某一天

0x 01 Excaliflag

毕竟第一题嘛 肯定不难得 只要你想得到 他就不会难的

所以这个题目直接给思路啦

神器stegSolve



加油姐妹

0x 02 签到题

签到题

难度系数:  6.0

题目来源: SSCTF-2017

题目描述: SSCTF线上选举美男大赛开始了, 泰迪拿着他的密码去解密了, 提交花括号内内容
(Z2dRQGdRMWZxaDBvaHRqcHRfc3d7Z2ZoZ3MjfQ==)

题目场景: 暂无

题目附件: 暂无

https://blog.csdn.net/weixin_43928140

base64很明显, 先解密得到

```
ggQ@gQ1fqh0ohtjpt_sw{gfhgs#}
```

然后猜到有栅栏了, 但是发现都没用, 所以栅栏前面肯定还有, 后面发现是凯撒

所以这个就自己去试一下把, 先凯撒再栅栏, 注意大小写 (因为我自己吧, 经常解密出来都是小写, 别人家都有大小写的, 我就很迷!!)

真正的flag是有大写的啦!!! 注意细节

0x 03 Avatar

首先下载附件lamb.jpg

(但其实我自己下的附件是一个空的不知道是不是bug总之就是空的00000000大都打不开, 后面找大佬问了大佬直接把图给我了, 为了防止还有朋友跟我一样, 直接给图了)



就是这个了, 然后这个题目也是用到了一个我没用过的工具, 叫做outguess

我是直接虚拟机下载的

```
git clone https://github.com/crorvick/outguess //下载
./configure && make && make install //安装
```

装好了之后可以先用help看一下

这里我们可以直接命令解密

```
root@kali:~/outguess# outguess -r /root/lamb.jpg -t hidden.txt
Reading /root/lamb.jpg...
Extracting usable bits: 28734 bits
Steg retrieve: seed: 94, len: 41
root@kali:~/outguess# cat hidden.txt
We should blow up the bridge at midnight
root@kali:~/outguess#
```

这里解释一下 -r是解密(加密是-d),后面接文件 hidden.txt是将解密的内容存放在这个txt文件中, 如果你解密前后分别ls查看一下就会发现多了这个文件, 这里直接cat查看

注意flag是没有格式头的

0x 03 What-is-this

首先下载附件, 是一个压碎包, 解压放进虚拟机binwalk一下

```
root@kali:~# binwalk -e what-is-this
```

DECIMAL	HEXADECIMAL	DESCRIPTION
0	_flag.p0x0 lamb.jpg	POSIX tar archive (GNU)

后面发现是两张图片, 而且打开来都长得差不多, 就神仙图那种
两张都用stegsolve看了没有东西, 既然长得这么像, 就想到比较一下
我是直接用compare命令生成了diff.jpg

```
root@kali:~# compare pic2.jpg pic1.jpg diff.jpg
```

打开就有惊喜啦!!!

而且这个直接stegsolve也可以, 先选中pic1.jpg再选择Analysis->Image Combiner, 在选择pic2.jpg就可以啦 两种办法都可以, 其他的没有去尝试, 注意flag再一次没有格式头