

BUGCTF——杂项

原创

李多安 于 2019-08-29 21:13:03 发布 114 收藏

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/DUOan0216/article/details/99481192>

版权



[CTF 专栏收录该内容](#)

14 篇文章 0 订阅

订阅专栏

- [Linux](#)

想一想就开了压缩包, 看到flag文件

既然考linux的, 那丢进kali里面

然后cat一下, 啥也没发现

【愣住??】搞什么

看了一下别人的writeup, 自己没错啊。捣鼓捣鼓

想是不是自己没在kali里面解压?!

have a try.

```
root@kali:~/Desktop# tar -zxvf 1.tar.gz
test/
test/flag
root@kali:~/Desktop# ls
1.tar.gz  flag  jpg.jpg  test
root@kali:~/Desktop# cd test/
root@kali:~/Desktop/test# ls
flag
root@kali:~/Desktop/test# file flag
flag: Linux rev 1.0 ext3 filesystem data, UUID=66ce56f1-5b57-492f-82f3-ac067879235e (large
root@kali:~/Desktop/test# cat flag
h802 00pw00pw00S00pw
```

然后

最下面就出现这样的。。。。【日了?了, 菜的安详】

```
Path=game
DeletionDate=2016-06-27T12:27:37
key{}
key{}
key{feb81d3834e2423c9903f4755464060b}

..0game.trashinfo0game.trashinfo.0L1PJY
```

主要的kali语句:

```
tar -zxvf 1.tar.gz //解压文件
cat flag //查看文件
//另外 有这样的一句
strings flag
// 只显示flag文件的字符信息
```

- [啊哒](#)

打开压缩包，照例看下属性，发现



这东西肯定有情况，很有可能是密码之类的
先winhex 感觉应该是文件分离
binwalk之后，发现有zip加密，和我们猜的一样
然后直接用上图解密，欸，解不开
可能是编码，试试base16，刚好出现

base编码

base16、base32、base64

```
73646E6973635F32303138
```

编码 base16

sdnisc_2018

解密顺利的到flag。

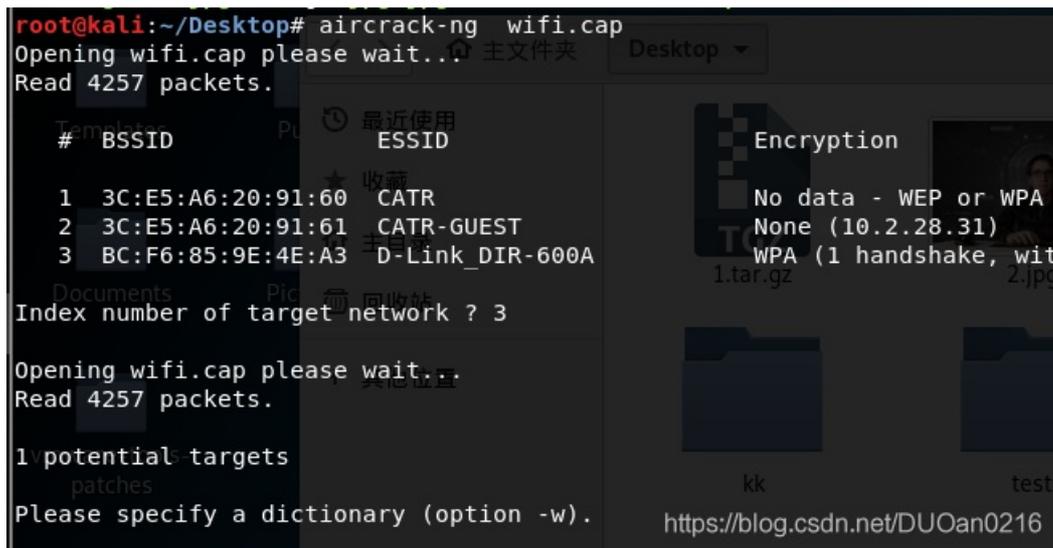
蹭wifi需要密码

下下来是一个cap包

破解WiFi密码包在kali系统中操作

握手包操作：

```
kali: # aircrack-ng xxx.cap
```



```
root@kali:~/Desktop# aircrack-ng wifi.cap
Opening wifi.cap please wait... Read 4257 packets.
# BSSID          ESSID
1 3C:E5:A6:20:91:60 CATR
2 3C:E5:A6:20:91:61 CATR-GUEST
3 BC:F6:85:9E:4E:A3 D-Link_DIR-600A
Index number of target network ? 3
Opening wifi.cap please wait... Read 4257 packets.
1 potential targets
Please specify a dictionary (option -w).
```

需要字典

我先试试Kali自带的字典

linux下常见的压缩文件格式还有：

.gz(有gzip压缩而成)，解压方法：`gzip -d filename`

.tar(先用tar归档，再用gzip压缩而成)，解压方法：`tar -xvf filename`

.tar.bz2解压方法：`tar xvfj filename`

kali默认字典目录：`/usr/share/wordlists/`

可以用crunch自己选择生成适合自己的密码字典

事实证明用自带字典跑是非常的慢。。。

那就自己做字典。

详细的kali字典制作

这是个手机号码，那就做个手机号码的字典

制作139开头的手机密码字典

```
crunch 11 11+0123456789 -t 139%%%%%%%% -o 33.txt
```

```
//在kali系统中
```

```
#: crunch 11 11+0123456789 -t 1391040%%% -o zidian.txt
```

```
#: aircrack-ng -w zidian.txt wifi.cap
```

```
// get the flag
```

网站被黑

不得不说

网站真的好看【除了头像

常用手段

御剑查询后台

发现一个后台界面

需要密码

很显然 burp暴力破解密码

得到之后输入密码

get the flag

管理员系统

看源代码——注释那里有个base64编码

破译应该是管理员密码

登陆发现提示本地登陆

放入burp改成

```
X-Forwarded-For:127.0.0.1
```

得到flag（在源码里面，推荐放入repeater）

输入密码查看flag