



# 攻防世界之miscmisc

原创

无聊的知识  于 2021-10-02 22:58:35 发布  2222  收藏

分类专栏: [攻防世界](#) 文章标签: [安全](#) [网络安全](#) [信息安全](#)

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\\_54882883/article/details/120590209](https://blog.csdn.net/weixin_54882883/article/details/120590209)

版权



[攻防世界](#) 专栏收录该内容

13 篇文章 1 订阅

订阅专栏

## 攻防世界之miscmisc

首先声明一下这题啊

只能说一点破该【广东话】

这题不难

但是

他在和你打持久战

为什么怎么说呢

让我告诉你

首先

他解压下载了一个

图片

就是这个图片啊



不过如此



咳咳

这张照片似乎在嘲讽我

一时冲动

理解理解啊



下载了一张图片

看起来没什么

通常我的习惯是

用binwalk去扫描看看的

有没有隐藏什么秘密

```
zsh: corrupt history file /root/.zsh_history
(root@kali3) ~/桌面
# binwalk buguoruci.png
```

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	PNG image, 198 x 195, 8-bit/color RGBA, non-interlaced
91	0x5B	Zlib compressed data, compressed
46098	0xB412	Zip archive data, at least v2.0 to extract, compressed size: 291018, uncompressed size: 291005, name: chadiand.zip
337158	0x52506	Zip archive data, at least v2.0 to extract, compressed size: 162503, uncompressed size: 163449, name: chayidian.jpg
499893	0x7A0B5	End of Zip archive, footer length: 22
499915	0x7A0CB	Zip archive data, at least v2.0 to extract, compressed size: 162503, uncompressed size: 163449, name: chayidian.jpg
662461	0xA1BBD	Zip archive data, at least v2.0 to extract, compressed size: 290992, uncompressed size: 291005, name: chadian.zip
953682	0xE8D52	End of Zip archive, footer length: 22

CSDN @无聊的知识

好家伙啊

只在在网上买了这本书

干什么事情都算一下

干什么事情都很顺啊





女施主，老衲观你印堂发黑。  
看你命中缺一物，你命中缺我啊！

CSDN @无聊的知识

ok啊

隐藏了四个zip啊

每一个都下载来

end文件的就先请他到隔壁领盒饭去

```
DECIMAL      HEXADECIMAL  DESCRIPTION
-----
0            0x0         PNG image, 198 x 195, 8-bit/color RGBA, non-interlaced
91          0x5B         Zlib compressed data, compressed
46098      0xB412      Zip archive data, at least v2.0 to extract, compressed size: 291018, uncompressed size: 291005, name: chadiand.zip
337158    0x52506     Zip archive data, at least v2.0 to extract, compressed size: 162503, uncompressed size: 163449, name: chayidian.jpg
499893    0x7A0B5     End of Zip archive, footer length: 22
499915    0x7A0CB     Zip archive data, at least v2.0 to extract, compressed size: 162503, uncompressed size: 163449, name: chayidian.jpg
662461    0xA1BBD     Zip archive data, at least v2.0 to extract, compressed size: 290992, uncompressed size: 291005, name: chadian.zip
953682    0xE8D52     End of Zip archive, footer length: 22

(root@kali3)-[~/桌面]
└─# dd if=buguoruci.png of=2.zip skip=662461 bs=1
记录了291243+0 的读入
记录了291243+0 的写出
291243字节 (291 kB, 284 KiB) 已复制, 0.730013 s, 399 kB/s

(root@kali3)-[~/桌面]
└─# dd if=buguoruci.png of=3.zip skip=499915 bs=1
记录了453789+0 的读入
记录了453789+0 的写出
453789字节 (454 kB, 443 KiB) 已复制, 1.14662 s, 396 kB/s

(root@kali3)-[~/桌面]
└─# dd if=buguoruci.png of=4.zip skip=337158 bs=1
记录了616546+0 的读入
记录了616546+0 的写出
616546字节 (617 kB, 602 KiB) 已复制, 1.60586 s, 384 kB/s

(root@kali3)-[~/桌面]
└─# dd if=buguoruci.png of=5.zip skip=46098 bs=1
记录了907606+0 的读入
记录了907606+0 的写出
907606字节 (908 kB, 886 KiB) 已复制, 2.47284 s, 367 kB/s

(root@kali3)-[~/桌面]
└─#
```

CSDN @无聊的知识

```
(root@kali3)-[~/桌面]
└─# dd if=buguoruci.png of=2.zip skip=662461 bs=1
记录了291243+0 的读入
记录了291243+0 的写出
291243字节 (291 kB, 284 KiB) 已复制, 0.730013 s, 399 kB/s

(root@kali3)-[~/桌面]
└─# dd if=buguoruci.png of=3.zip skip=499915
bs=1 记录了453789+0 的读入 记录了453789+0 的写出 453789字节 (454 kB, 443
KiB) 已复制, 1.14662 s, 396 kB/s

(root@kali3)-[~/桌面]
└─# dd if=buguoruci.png of=4.zip skip=337158
bs=1 记录了616546+0 的读入 记录了616546+0 的写出 616546字节 (617 kB, 602
KiB) 已复制, 1.60586 s, 384 kB/s

(root@kali3)-[~/桌面]
└─# dd if=buguoruci.png of=5.zip skip=46098
bs=1 记录了907606+0 的读入 记录了907606+0 的写出 907606字节 (908 kB, 886
KiB) 已复制, 2.47284 s, 367 kB/s
```

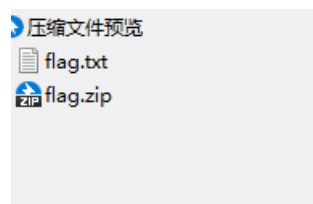
下载完后呢

就解压

解压出来了一个chadian.zip

看到这给flag

我感到一种不祥的预感



好家伙

解压的时候要秘密

爆破他

- 。
- 。
- 。
- 。
- 。
- 。
- 。

两天后

好家伙啊



多亏字典够大

不然还不一定能爆出来

z\$^58a4w

正当我满怀期待点开的时候



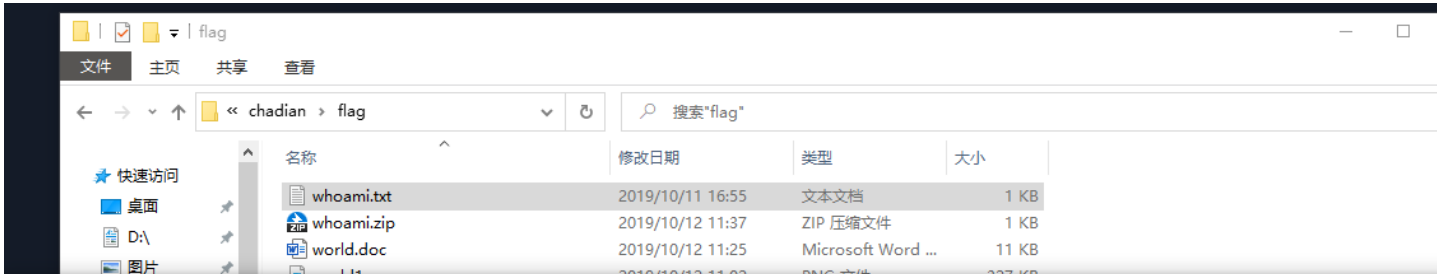
- 
- 
- 
- 
- 
- 
- 

三天后



终于结束了

z^ea4zaa3azf8



whoami.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

flag{12sad7eaf46a84fe9q4fasf48e6q4f6as4f864q9e48f9q4fa6sf6f48}

CSDN @无聊的知识

flag{12sad7eaf46a84fe9q4fasf48e6q4f6as4f864q9e48f9q4fa6sf6f48}