CTF,隐写

原创

jiet07 于 2019-10-09 18:20:51 发布 109 收藏

分类专栏： # CTF 文章标签： CTF

本文链接：https://blog.csdn.net/weixin_41603028/article/details/102467184

CTF 专栏收录该内容

4 篇文章 0 订阅

订阅专栏

内容：从图片中获取flag

环境：Ubuntu16.04

实验步骤：

方法一：binwalk ,查看文件中是否包含其他文件

截图说明

步骤一：内容配置

```
pinginglab@tianjie:~$ mkdir a/
pinginglab@tianjie:~$ cd a/
pinginglab@tianjie:~/a$ su root
密码:
root@tianjie:/home/pinginglab/a# vim flag.txt
root@tianjie:/home/pinginglab/a# ls
1.jpg  flag.txt
root@tianjie:/home/pinginglab/a# zip flag.txt.zip flag.txt
  adding: flag.txt (stored 0%)
root@tianjie:/home/pinginglab/a# ls
1.jpg  flag.txt  flag.txt.zip
root@tianjie:/home/pinginglab/a# cp 1.jpg 2.jpg
root@tianjie:/home/pinginglab/a# ls
1.jpg  2.jpg  flag.txt  flag.txt.zip
root@tianjie:/home/pinginglab/a# cat flag.txt.zip > 2.jpg
root@tianjie:/home/pinginglab/a# ls
1.jpg  2.jpg  flag.txt  flag.txt.zip
root@tianjie:/home/pinginglab/a# binwalk 2.jpg
程序“binwalk”尚未安装。 您可以使用以下命令安装:
apt install binwalk
root@tianjie:/home/pinginglab/a# apt install binwalk
正在读取软件包列表... 完成
正在分析软件包的依赖关系树
正在读取状态信息... 完成
下列软件包是自动安装的并且现在不需要了:
```


特别注意

cat命令说明：

cat m1 m2 > file （将文件ml和m2合并后放入文件file中）重写，会影响图片的显示

cat m1 >> file 追加，不会影响图片显示

步骤二：提取文件

```
root@tianjie:/home/pinginglab/a# binwalk 2.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             Zip archive data, at least v1.0 to extract, compre
ssed size: 17, uncompressed size: 17, name: flag.txt
161           0xA1            End of Zip archive

root@tianjie:/home/pinginglab/a# cp 2.jpg 2.zip
root@tianjie:/home/pinginglab/a# ls
1.jpg  2.jpg  2.zip  flag.txt  flag.txt.zip
```

cp命令说明：cp 2.jpg 2.zip (将2.jpg中的zip文件复制给2.zip)

步骤三：减压缩文件，并查看文件内容

```
root@tianjie:/home/pinginglab/a# unzip 2.zip
Archive:  2.zip
replace flag.txt? [y]es, [n]o, [A]ll, [N]one, [r]ename: r
new name: flag1.txt
 extracting: flag1.txt
root@tianjie:/home/pinginglab/a# ls
1.jpg  2.jpg  2.zip  flag1.txt  flag.txt  flag.txt.zip
root@tianjie:/home/pinginglab/a# cat flag1.txt
{flag}=yangyiwen
root@tianjie:/home/pinginglab/a# cat flag1.txt flag.txt
{flag}=yangyiwen
{flag}=yangyiwen
```


方法二：stirngs命令，在对象文件或二进制文件中查找可打印的字符串。

```
root@tianjie:/home/pinginglab/a# strings 2.jpg
flag.txtUT
{flag}=yangyiwen
flag.txtUT
```

其他：

```
root@tianjie:/home/pinginglab/a# cp 1.jpg 1.zip
root@tianjie:/home/pinginglab/a# unzip 1.zip
Archive:  1.zip
  End-of-central-directory signature not found.  Either this file is not
  a zipfile, or it constitutes one disk of a multi-part archive.  In the
  latter case the central directory and zipfile comment will be found on
  the last disk(s) of this archive.
unzip:  cannot find zipfile directory in one of 1.zip or
        1.zip.zip, and cannot find 1.zip.ZIP, period.
root@tianjie:/home/pinginglab/a# vim 1.zip
root@tianjie:/home/pinginglab/a# strings 1.zip
JFIF
Exif
Adobe Photoshop CC 2015 (Macintosh)
2018:01:22 17:18:44
0221
```



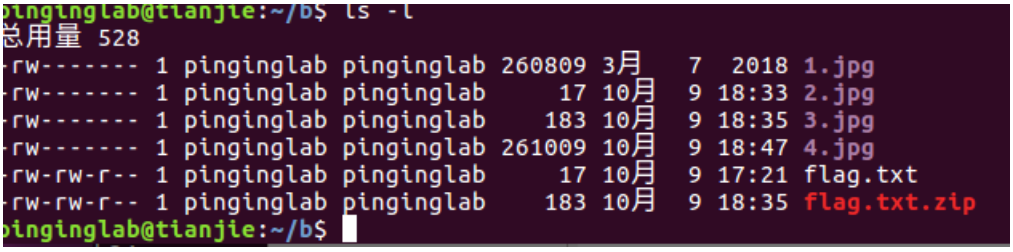
```
flag.txtUT
{flag}=yangyiwen
flag.txtUT
{flag}=yangyiwen
pinginglab@tianjie:~/b$ strings 2.jpg
{flag}=yangyiwen
pinginglab@tianjie:~/b$ strings 3.jpg
flag.txtUT
{flag}=yangyiwen
flag.txtUT
pinginglab@tianjie:~/b$
```

2.jpg: cat flag.txt > 2.jpg

3.jpg: cat flag.txt.zip >3.jpg

4.jpg: cat flag.txt >>4.jgp

cat flag.txt.zip >>4.jpg


pinginglab@tianjie:~/b$ ls -l
总用量 528
-rw------- 1 pinginglab pinginglab 260809 3月   7 2018 1.jpg
-rw------- 1 pinginglab pinginglab   17 10月 9 18:33 2.jpg
-rw------- 1 pinginglab pinginglab   183 10月 9 18:35 3.jpg
-rw------- 1 pinginglab pinginglab 261009 10月 9 18:47 4.jpg
-rw-rw-r-- 1 pinginglab pinginglab   17 10月 9 17:21 flag.txt
-rw-rw-r-- 1 pinginglab pinginglab   183 10月 9 18:35 flag.txt.zip
pinginglab@tianjie:~/b$