

# CTF Misc常用工具(一)

原创

Cer0 于 2019-08-19 22:48:17 发布 3041 收藏 29

文章标签: [CTF MISC](#)

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/chenl\\_ce2009/article/details/99772194](https://blog.csdn.net/chenl_ce2009/article/details/99772194)

版权

file命令

Linux自带, 可根据文件头识别文件类型。

```
root@kali:/mnt/hgfs/share# file re
re: ELF 64-bit LSB executable, x86-64, version 1 (GNU/Linux), statically linked, no section header
root@kali:/mnt/hgfs/share# file qr.png
qr.png: PNG image data, 250 x 250, 8-bit/color RGBA, non-interlaced
root@kali:/mnt/hgfs/share#
```

更多用法可参考文章: <https://www.cnblogs.com/Dodge/p/4278306.html>

binwalk命令

kali自带, 常用于ctf中进行文件分离, 常用命令包括:

```
binwalk filename #查看隐藏文件
binwalk -e filename #分离文件
```

更多用法可参考文章: <https://www.freebuf.com/sectool/15266.html>

类似的工具还有formost:

```
foremost 文件名 -o 输出目录名 #分离文件
```

名称	修改日期	类型
png	2019/8/19/周一 ...	文件夹
audit.txt	2019/8/19/周一 ...	TXT 文件

```
root@kali:/mnt/hgfs/share# foremost qr.png -o ./test
Processing: qr.png
|*|
root@kali:/mnt/hgfs/share# ls ./test
audit.txt png
```

strings命令

Linux命令, 在对象文件或二进制文件中查找可打印的字符串。

```
strings filename | grep keyword #在filename中查找keyword
```

```
root@kali:/mnt/hgfs/share# strings Cer0 |grep flag
flag{d316759c281bf925d600be698a4973d5}
```

更多用法可参考文章: <https://ipcmn.com/strings>

类似工具还有windows下的type命令:

```
type filename | findstr "keyword" #在filename中查找keyword
```

例如：type Cer0 | findstr "flag"，查找出文件Cer0中的flag。

```
G:\share
λ type Cer0 | findstr "flag"
? @ @ 9) 刼_ 9)& E 2y 驚 @ 夙括莢括轄 ↓ zh? pF0 諄P ↑ 勺x Password: → ? 6
6 9)&~ 9) 刼 E ( 諄 € 括轄括莢 z ↓ F0 諄h? zP ↑ ④ <? → N \ \ 9)&~ 9)
刼 E N 瘡 € 括轄括莢 z ↓ F0 諄h? zP ↑ ④ <? flag{d316759c281bf925d600be698a4973d5} →
>? < < 9) 刼_ 9)& E (y 拳 @ 夙括莢括轄 ↓ zh? zF0 諄 ④ 燻 L Y 8
8 9)&~ 9) E * 盃 € 括轄括莢 z ↓ F0 諄h? zP ↑ ④ <?
```