Strings使用

> strings 在二进制目标文件或其他二进制文件中查找可打印的字符串。
>
> 字符串默认至少是 4 个或更多可打印字符的任意序列，可使用选项改变字符串最小长度。

命令格式

`strings [<options>] <file>...`

命令参数:

```
-a, --all, -
    扫描整个文件而不是只扫描目标文件初始化和装载段
-d, --data
    仅打印文件中已初始化、加载的数据段中的字符串，这可能会减少输出中的垃圾量
-e, --encoding=ENCODING
    选择字符编码与字节序。encoding可取值s=7bits的ASCII, S=8bits的Latin1, {b,l}=16bits宽字符大小端编码, {B,L}=32bits宽字符大小端编码。其中b，B代表bigendian，l，L代表littleendian
-f,--print-file-name
    在显示字符串前先显示文件名
--help
    显示帮助信息
-, -n, --bytes=MIN_LEN
    指定可打印字符序列的最小长度，而不是默认的4个字符
-o
    类似 --radix=o
-t, --radix=RADIX
    输出字符串在文件中的偏移位置，RADIX 可取值 o（octal，八进制）、d（decimal，十进制）或者x（hexadecimal，十六进制）
-T, --target=BFD_NAME
    指定二进制文件格式
-v, -V, --version
    显示版本信息
-w, --include-all-whitespace
    默认情况下，Tab 和空格字符包含在字符串中，但其他空白字符除外，比如换行符和回车符等字符不是。-w 使所有的空白字符被认为是字符串的一部分
@FILE
    从指定的文件 FILE 中读取命令行选项
```

常用实例

```
（1）打印可执行文件中的所有可读字符串。
strings /bin/ls
/lib64/ld-linux-x86-64.so.2
libselinux.so.1
_ITM_deregisterTMCloneTable
__gmon_start__
_Jv_RegisterClasses
```

```
_ITM_registerTMCloneTable
_init
fgetfilecon
freecon
lgetfilecon
...
```

（2）查看某一个字符串属于哪个文件。

```
strings -f * | grep "xxx"
```

（3）查看glibc支持的版本。libc.so.6是c标准库，而这个标准库的制作者为了让库的使用者知道该库兼容哪些版本的标准库，就在这个库中定义了一些字符串常量，使用如下命令可以查看向下兼容的版本。

```
strings /lib64/libc.so.6 | grep GLIBC
GLIBC_2.2.5
GLIBC_2.2.6
GLIBC_2.3
GLIBC_2.3.2
GLIBC_2.3.3
GLIBC_2.3.4
GLIBC_2.4
GLIBC_2.5
GLIBC_2.6
GLIBC_2.7
GLIBC_2.8
GLIBC_2.9
GLIBC_2.10
GLIBC_2.11
GLIBC_2.12
GLIBC_2.13
GLIBC_2.14
GLIBC_2.15
GLIBC_2.16
GLIBC_2.17
GLIBC_PRIVATE
```