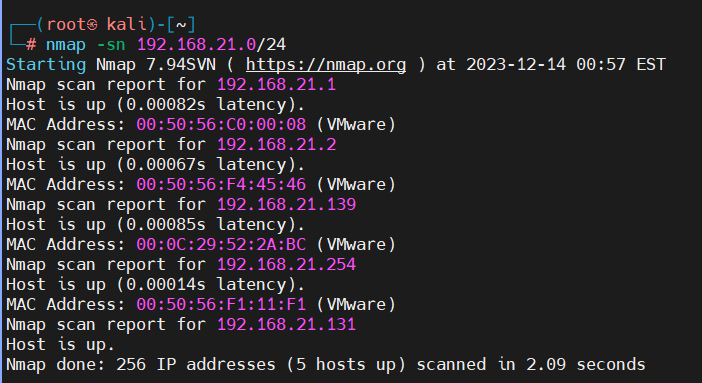
Pylington

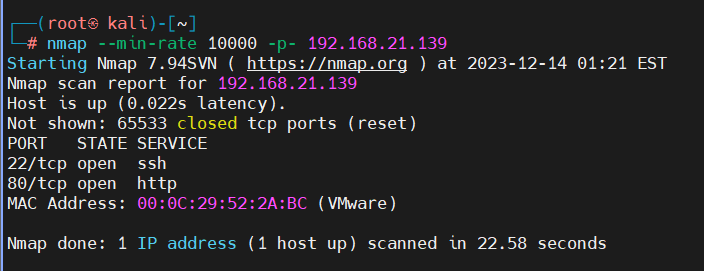
下载地址：<https://www.vulnhub.com/entry/pylington-1,684/>

主机发现

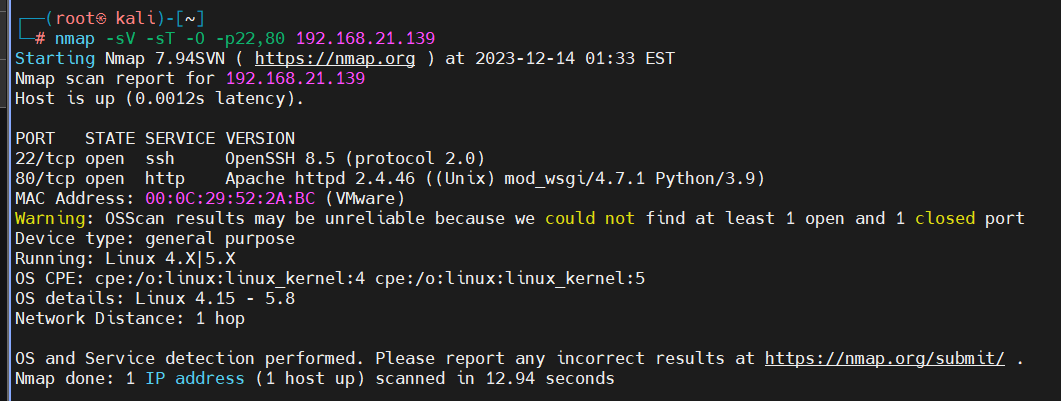


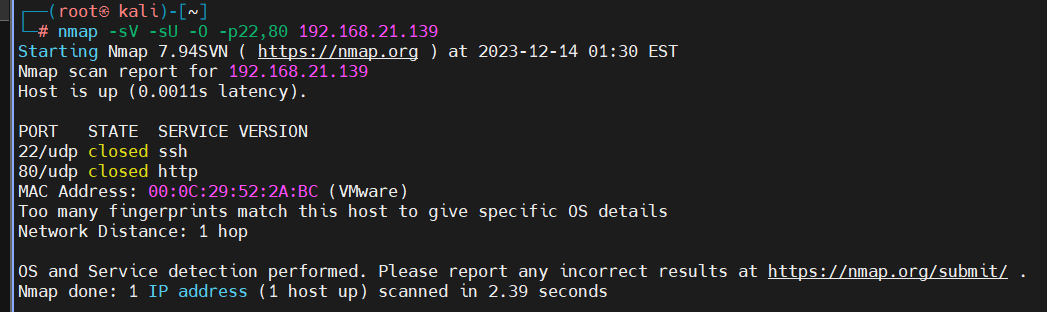
目标139

端口扫描

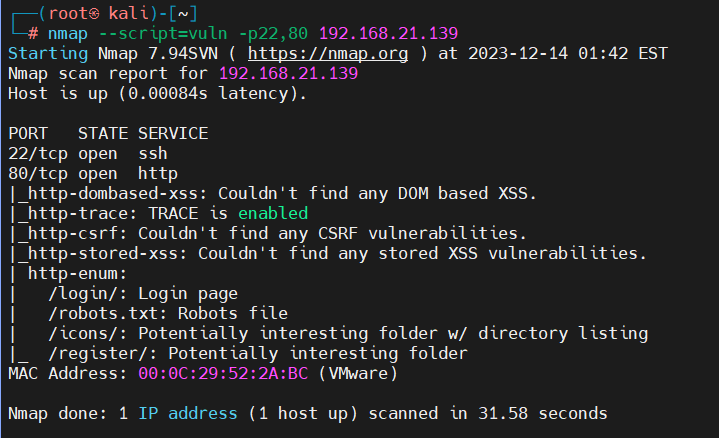


端口服务扫描

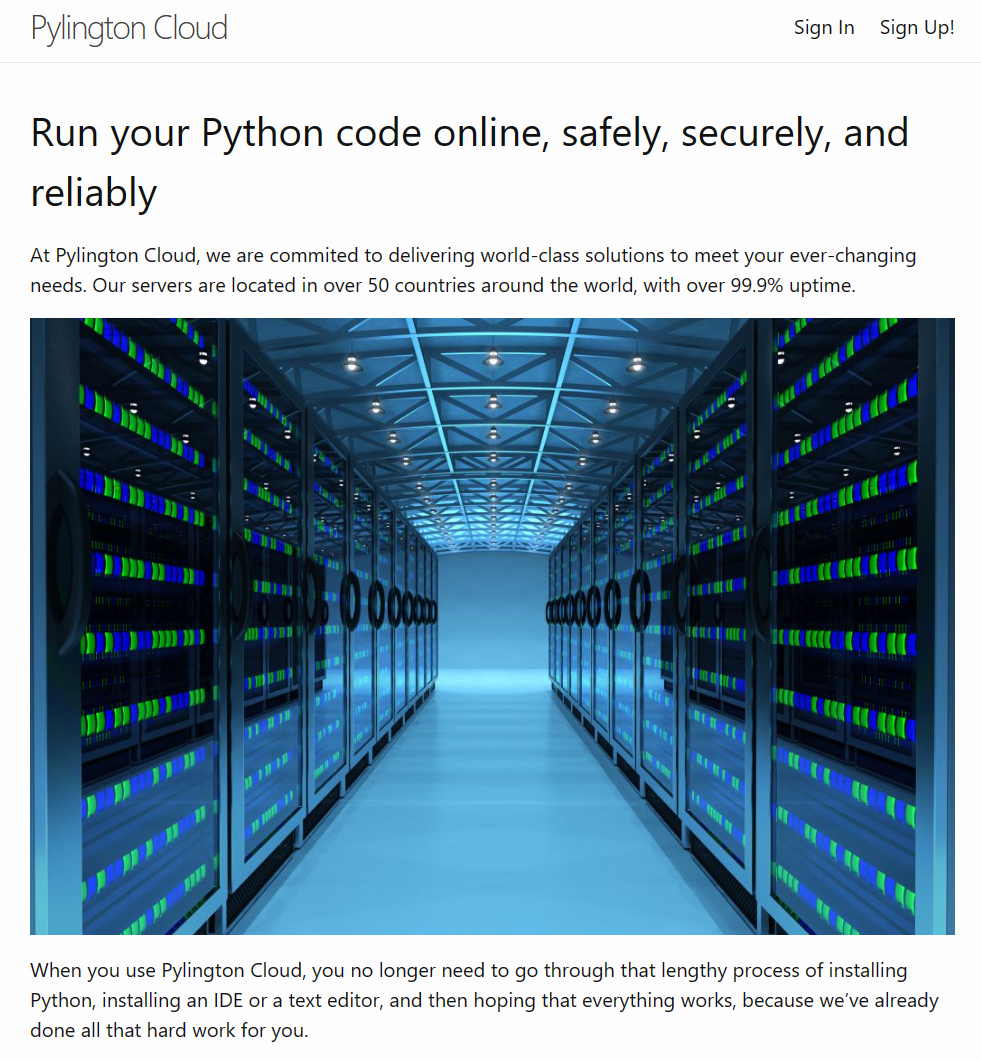


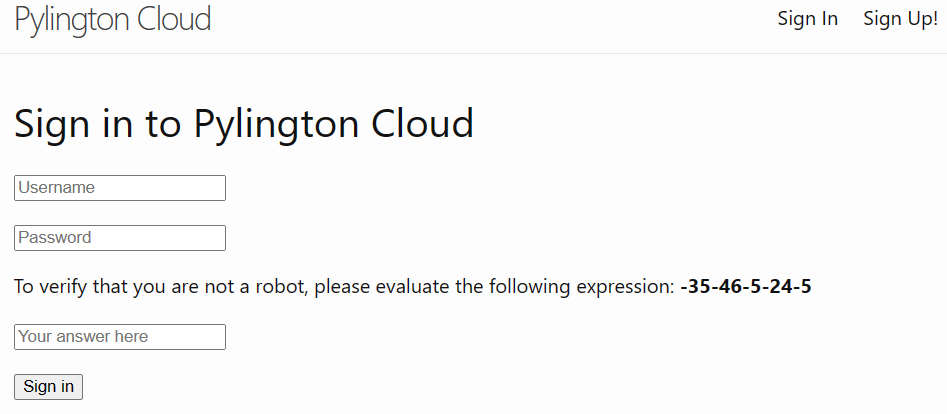


漏洞扫描

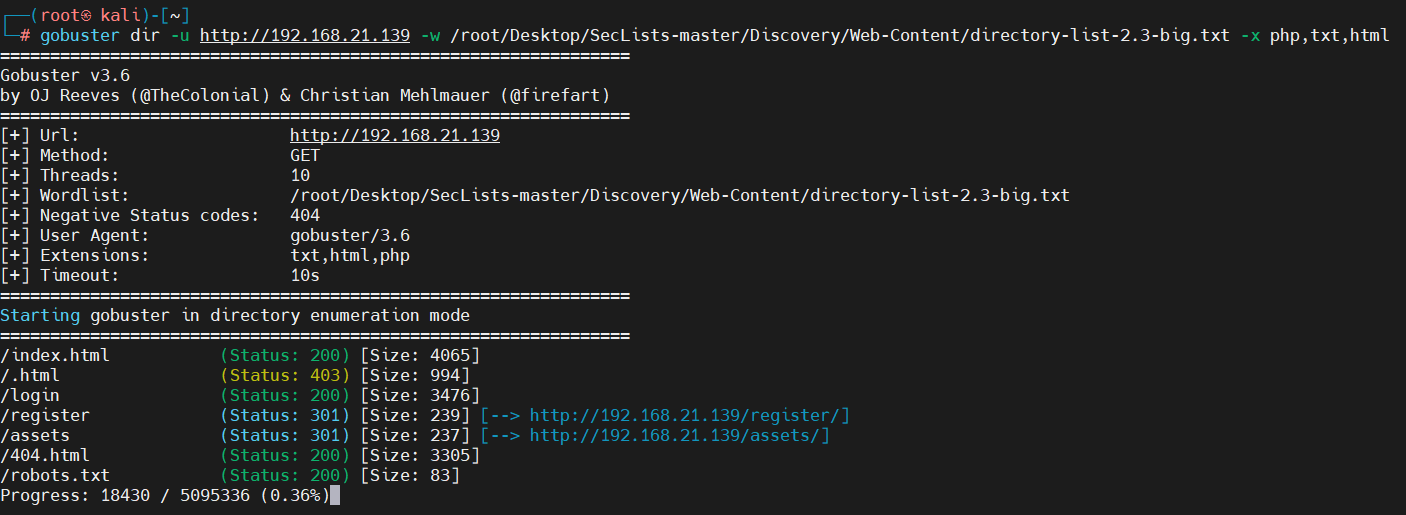


去看一下web

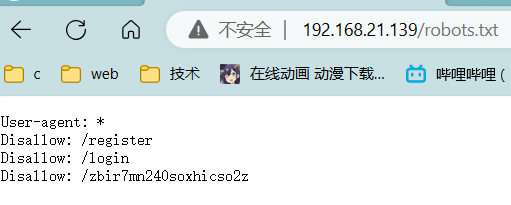




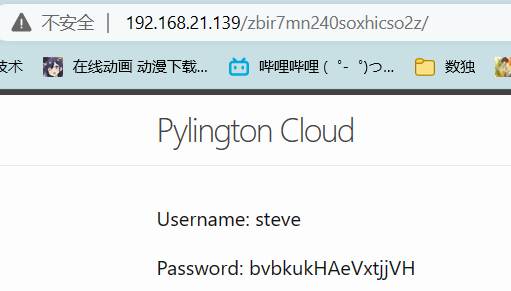
目录扫描



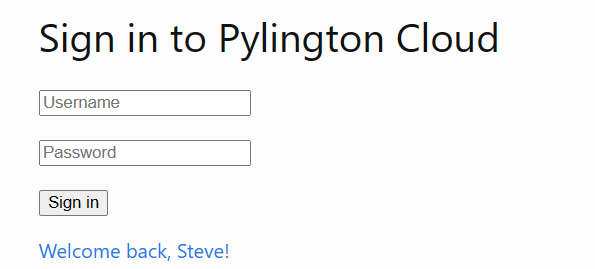
有robots

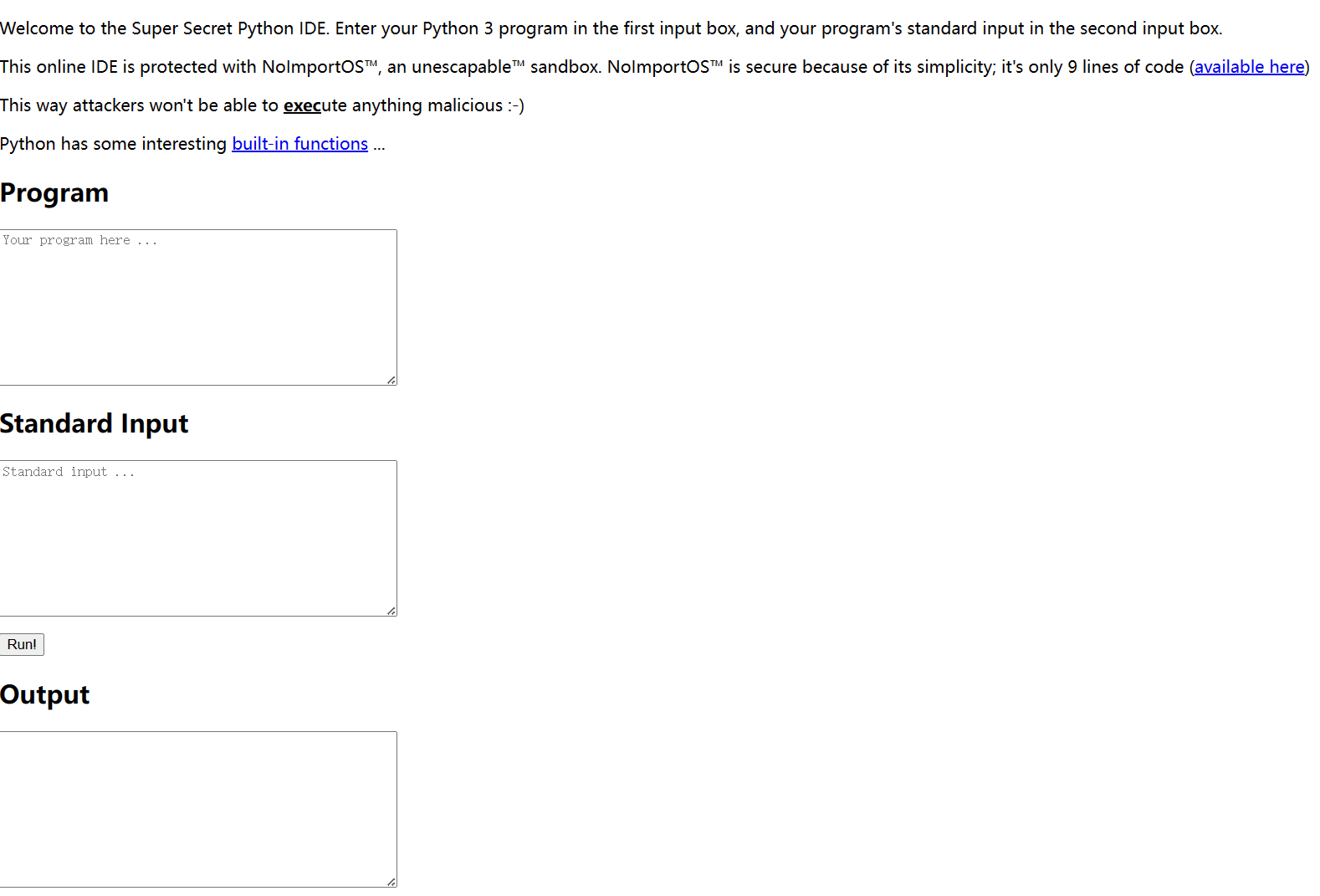


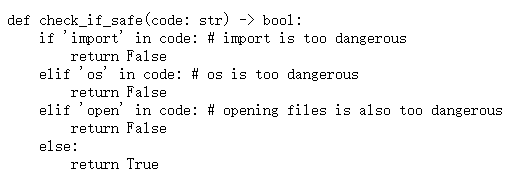
去看一下有个奇怪的东西



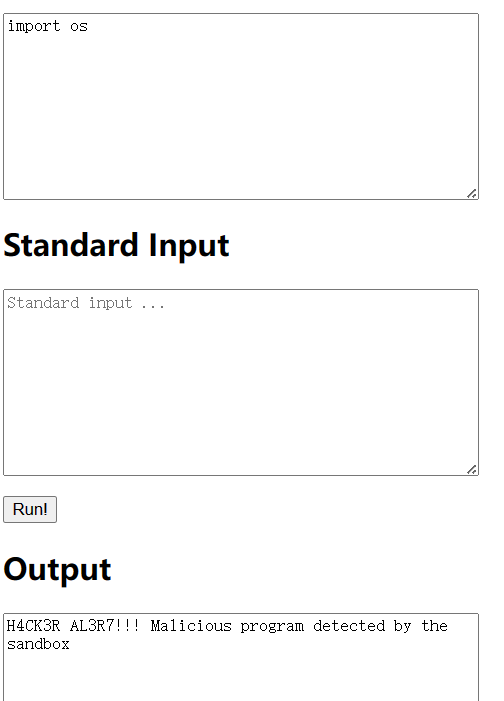
登入





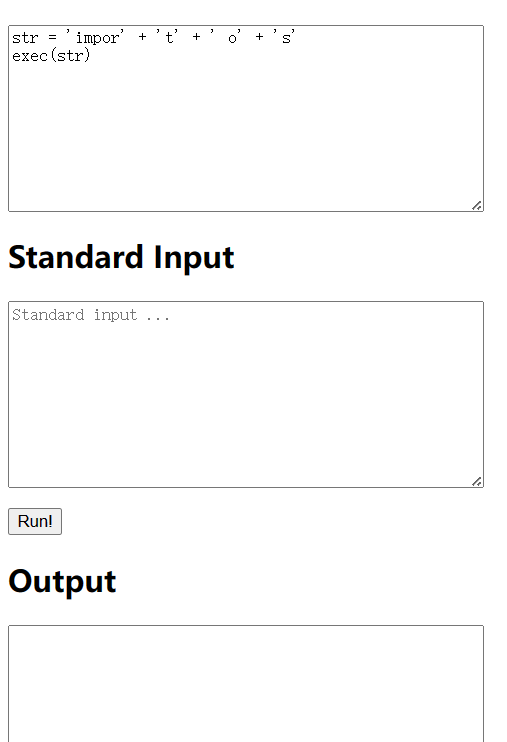


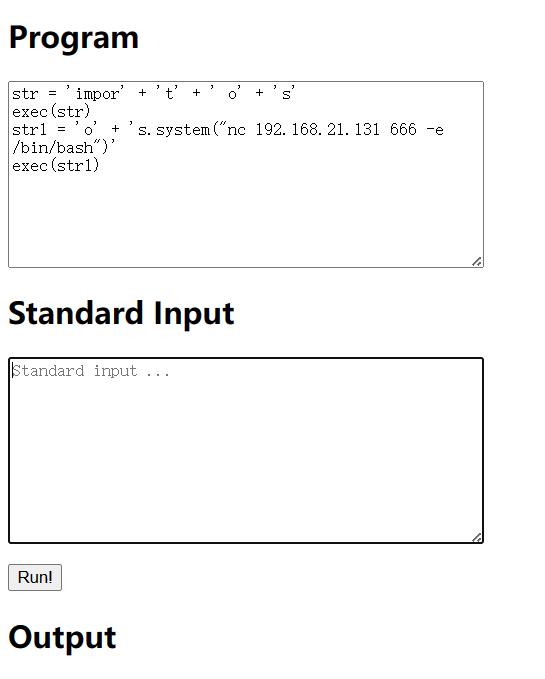
这是py脚本

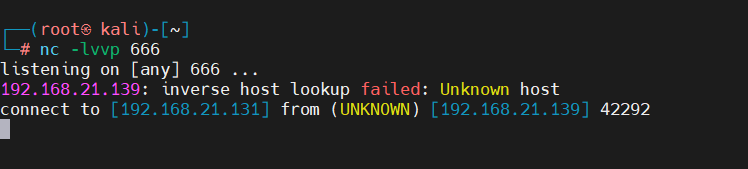


这个回显明显是被墙了

绕过一下就行了

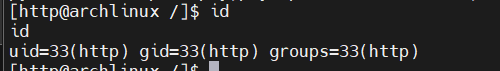


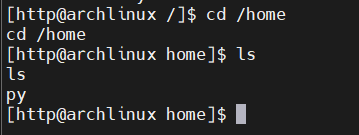


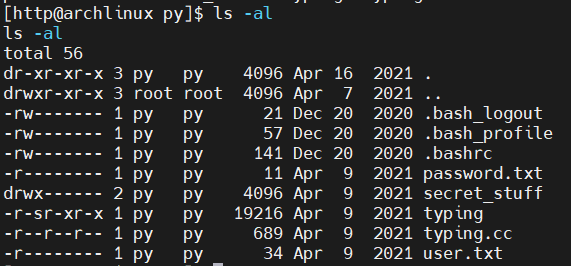


升级一下shell

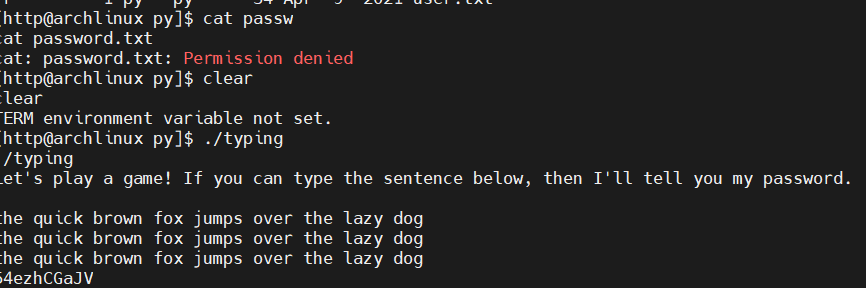






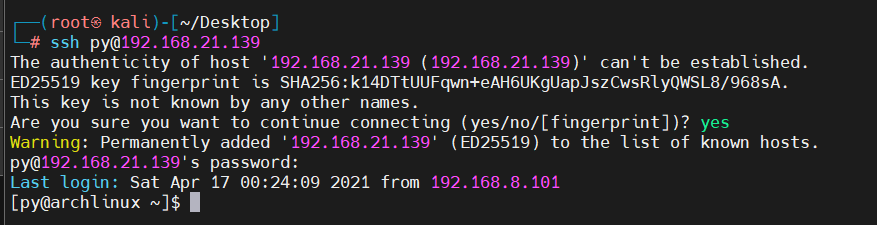


这里面只有一个文件能运行



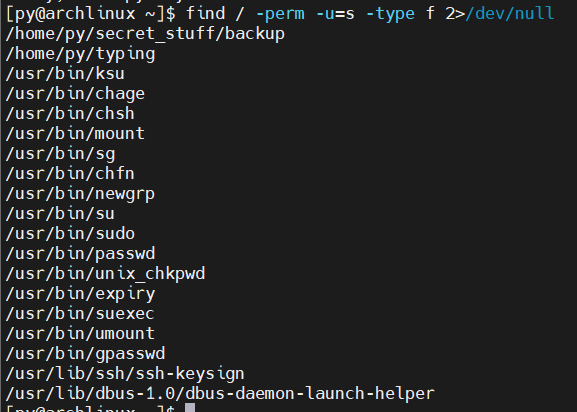
密码到手

登入

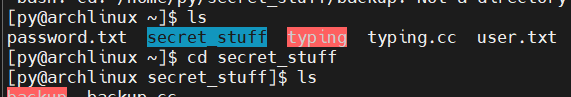


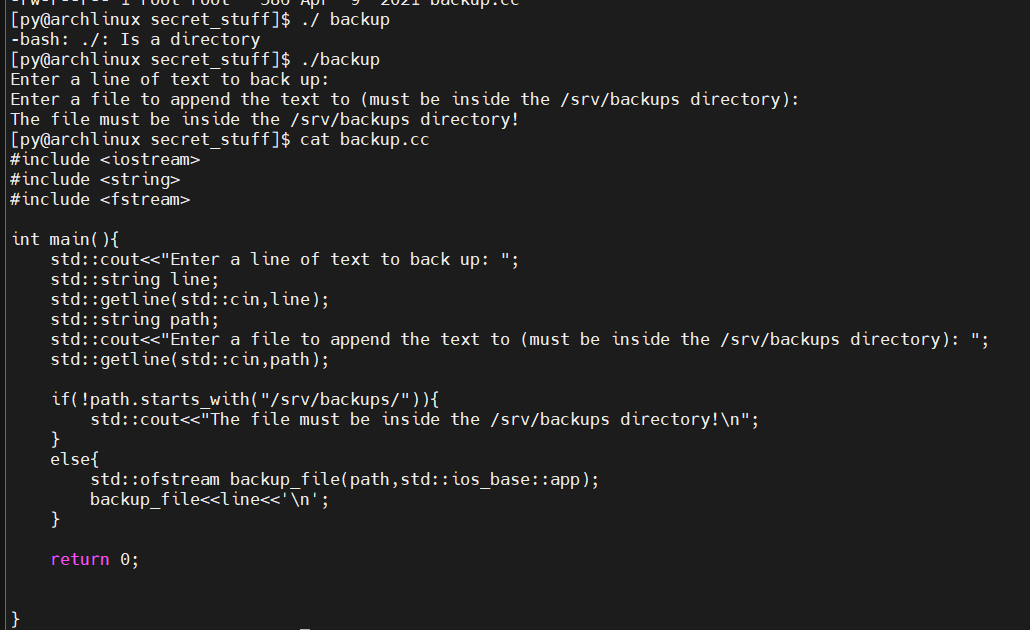
信息收集





看到了backup

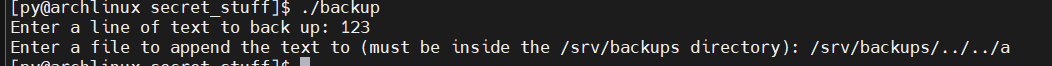






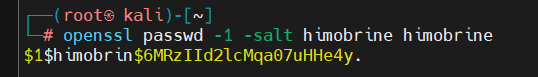


应该能有点操作，试一下



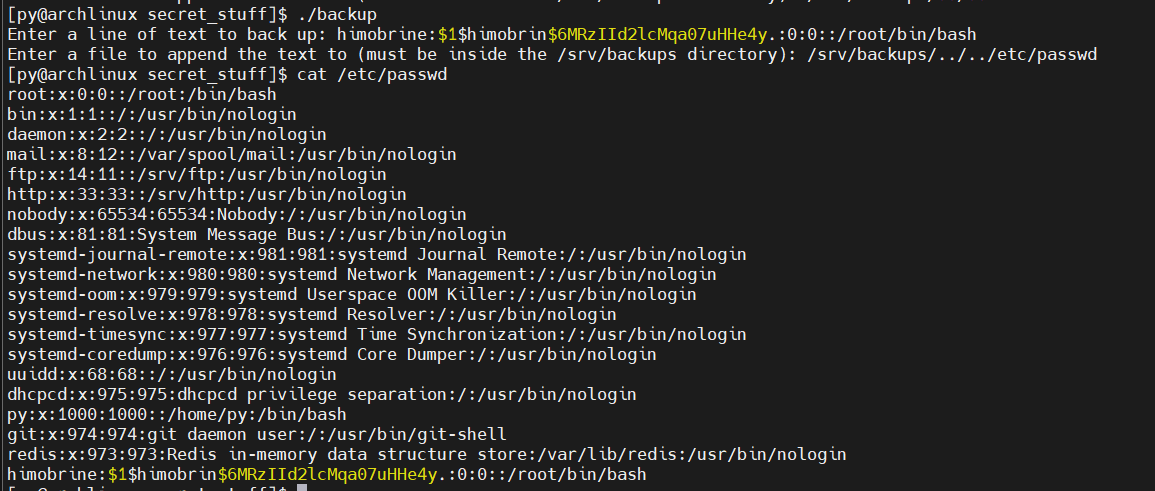


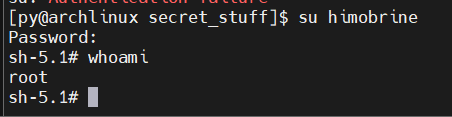
生成密码夺舍root

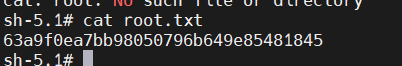


构造一下

himobrine:$1$himobrin$6MRzIId2lcMqa07uHHe4y.:0:0::/root/bin/bash







搞定