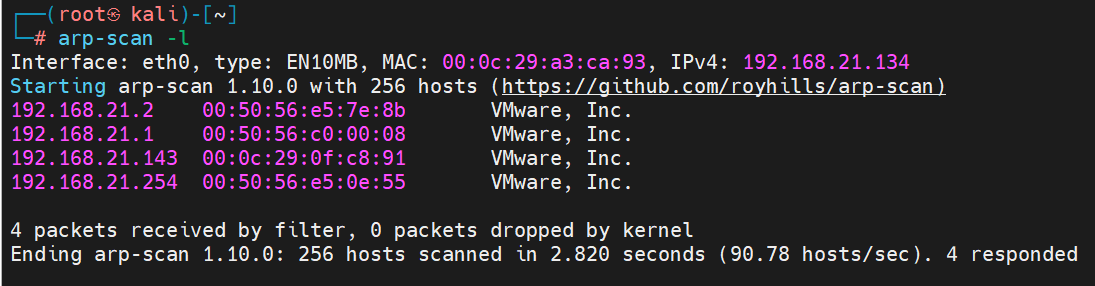
02-Breakout

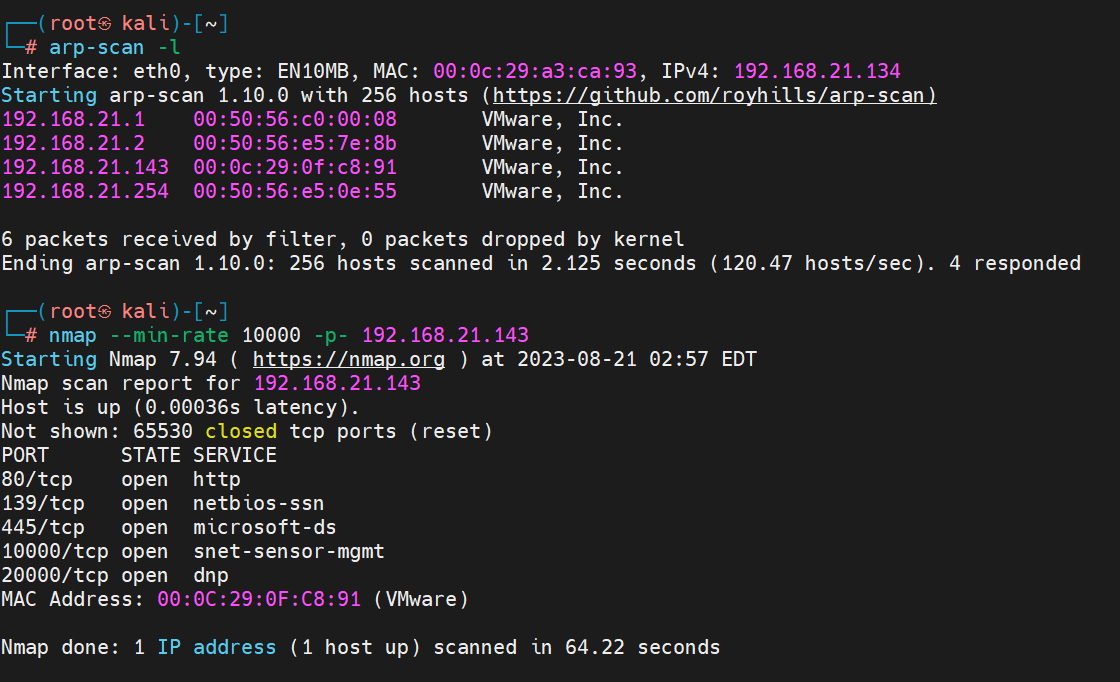
主机发现

arp-scan -l



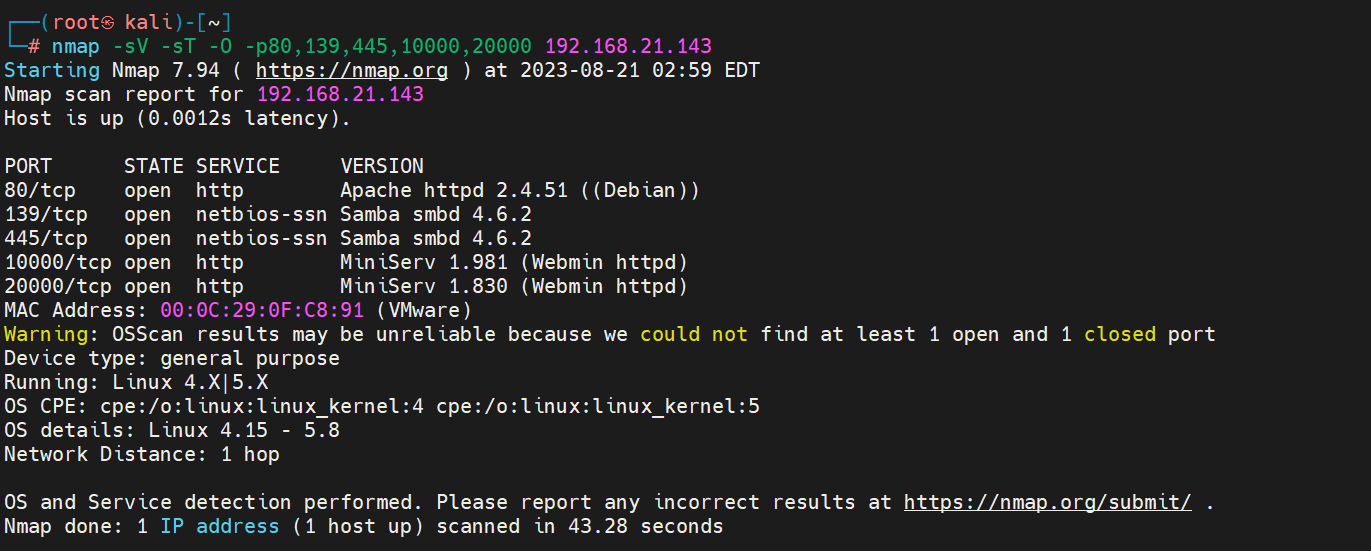
扫描端口

nmap --min-rate 10000 -p- 192.168.21.143



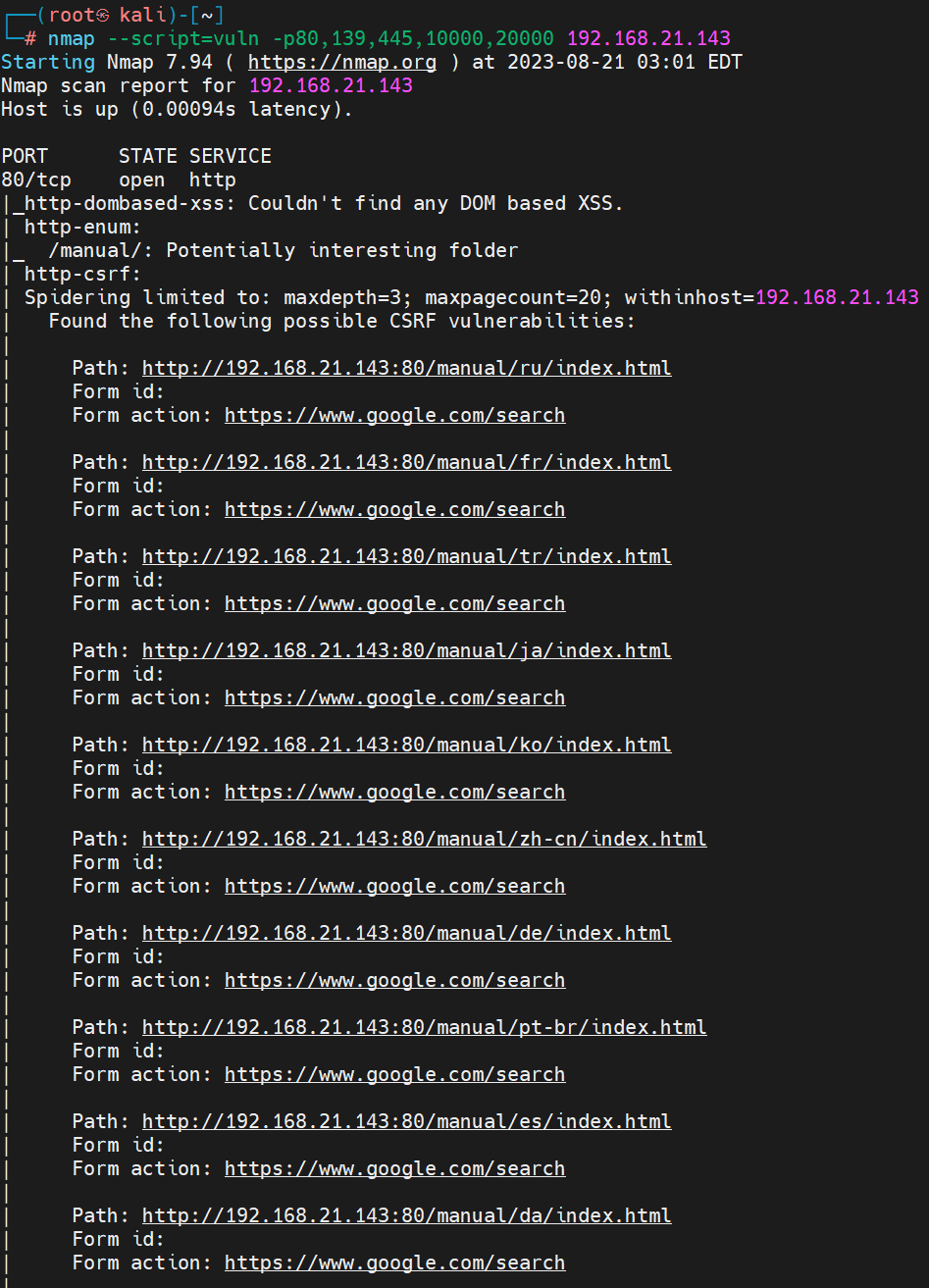
扫描端口信息

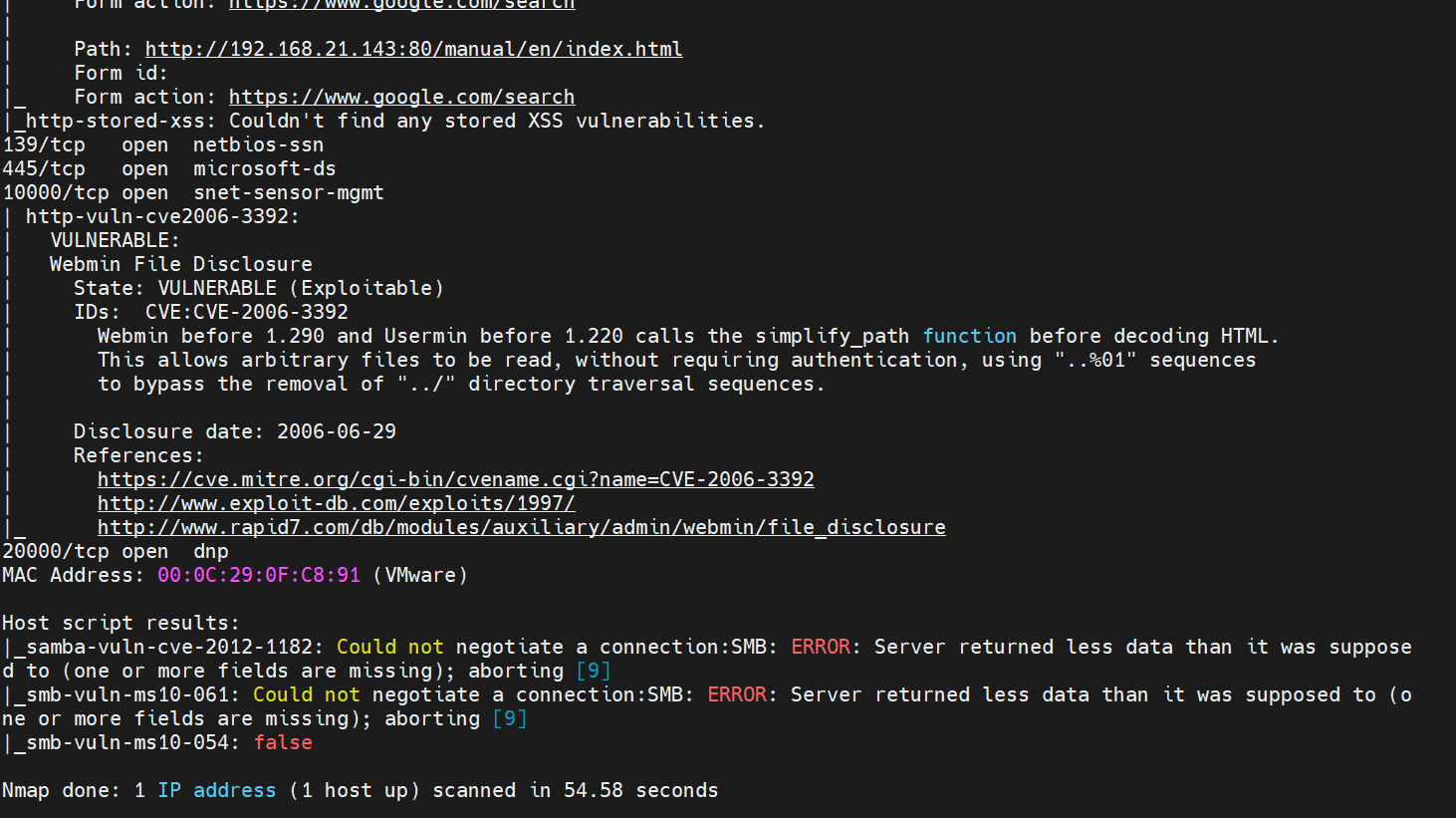
nmap -sV -sT -O -p80,139,445,10000,20000 192.168.21.143



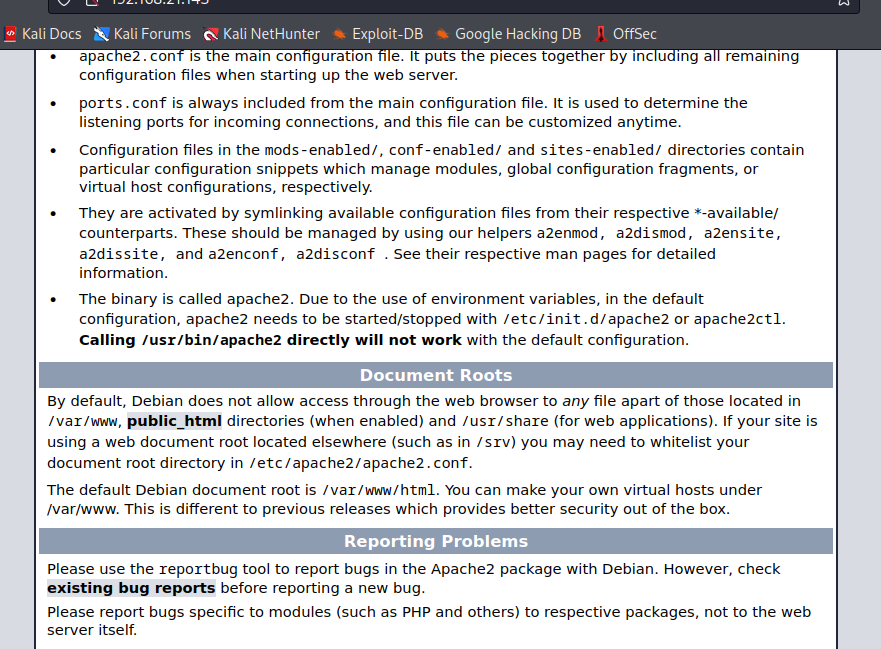
漏洞扫描

nmap --script=vuln -p80,139,445,10000,20000 192.168.21.143

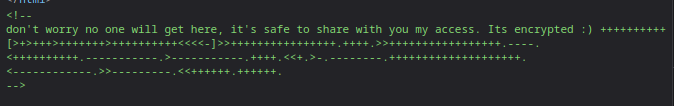




先看网站

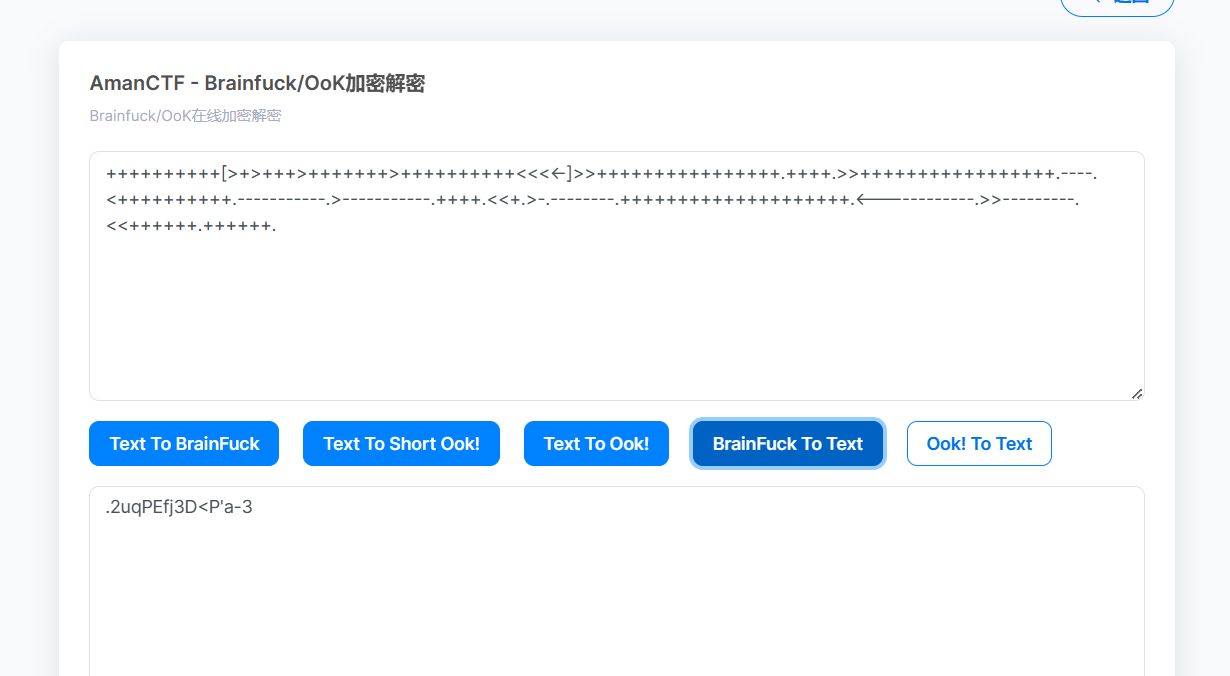


什么都没有看看f12

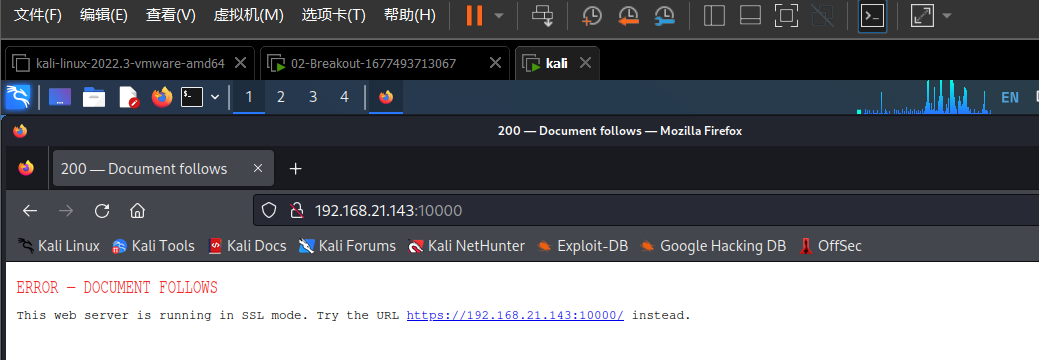
找到点好东西

解码看看

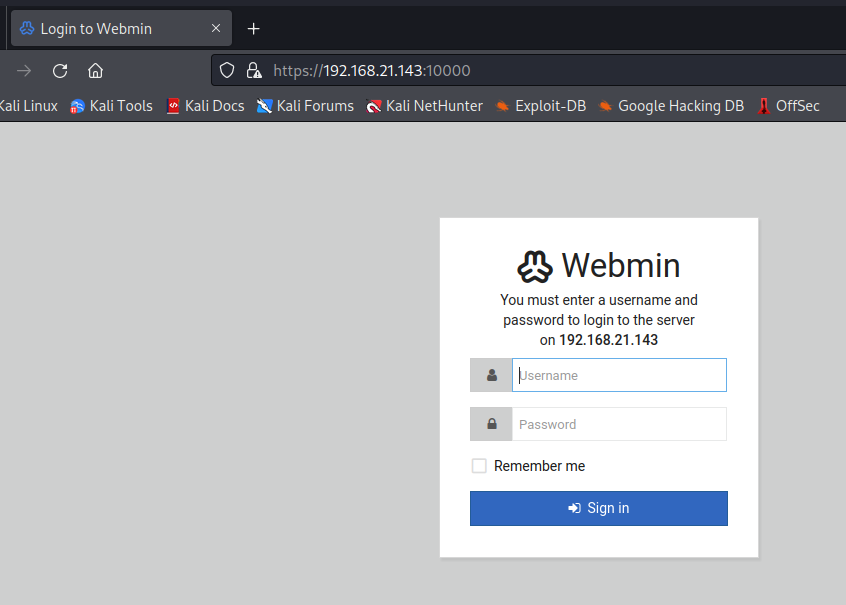
[Brainfuck/OoK加密解密 - Bugku CTF](https://ctf.bugku.com/tool/brainfuck)

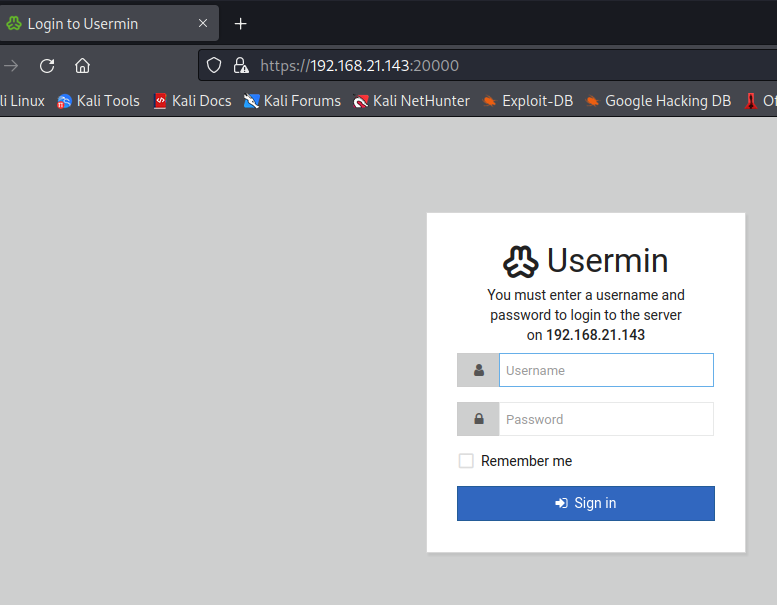


这个应该没用了，再去别的口看一下



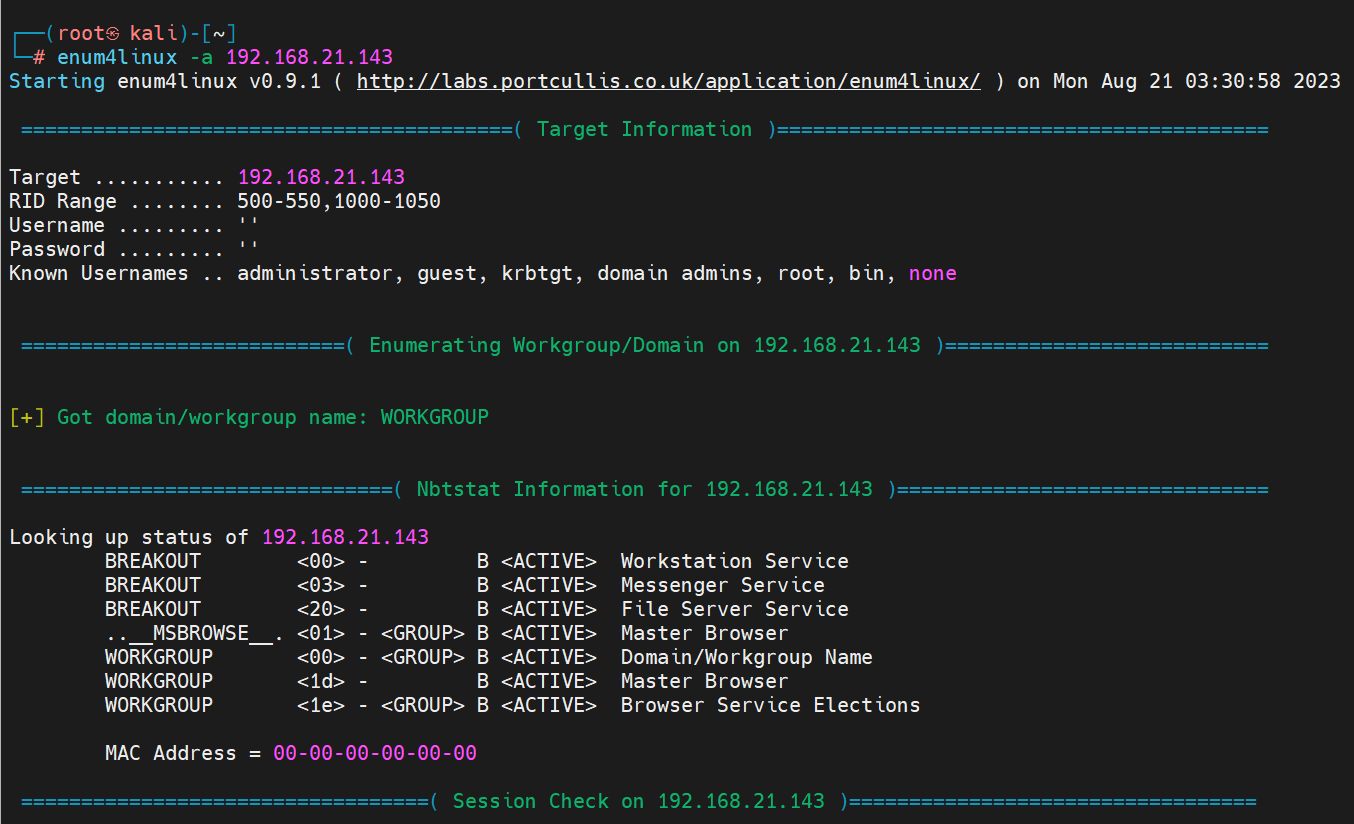
根据提示接着点

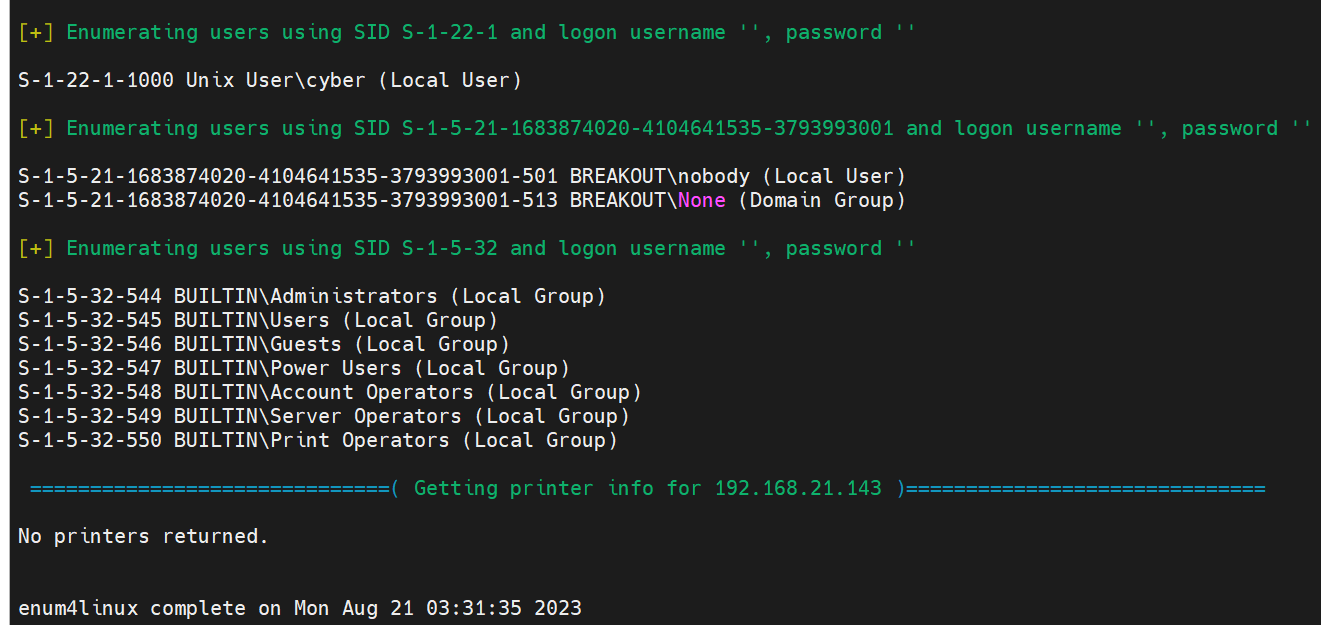




没有线索接着找

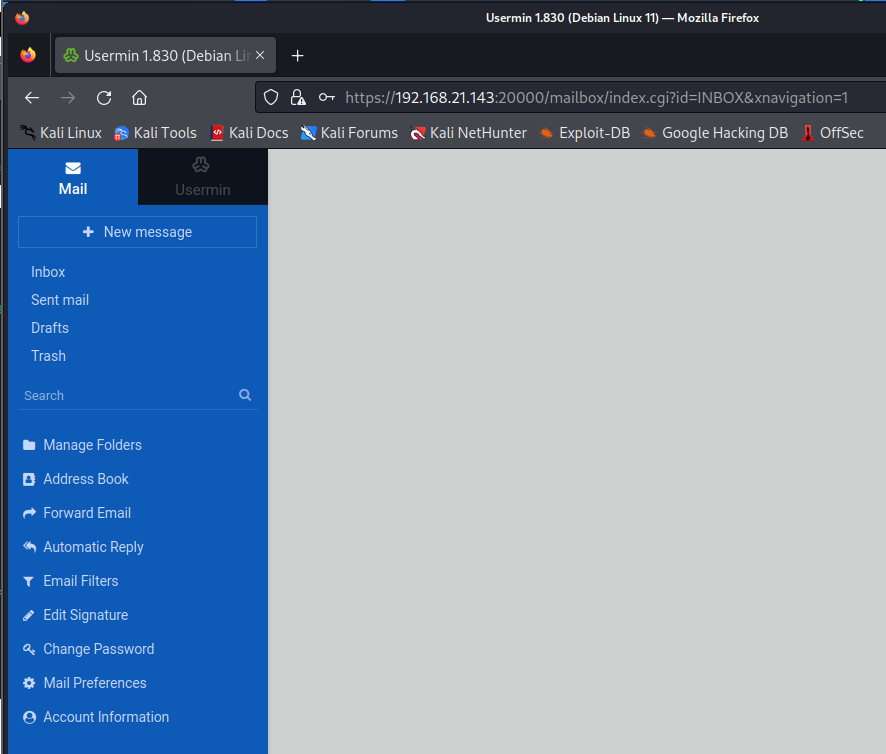
enum4linux -a 192.168.21.143





这里发现有用户被扫出来了

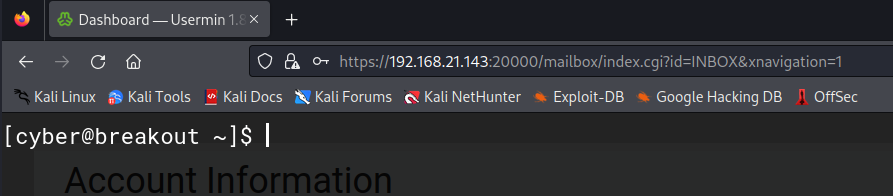
利用已经知道的密码那就登入能登入的位置

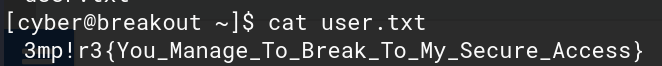


成功登入

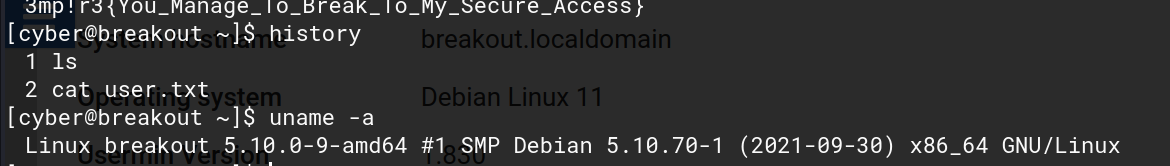


在这里发现了一个命令行（比较小有点难找）

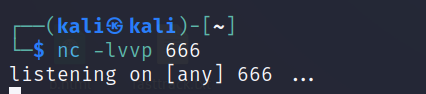




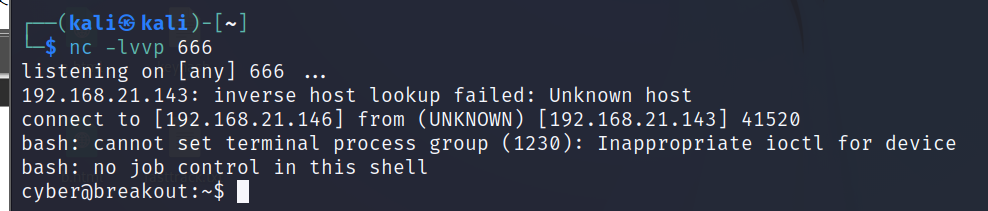
信息收集

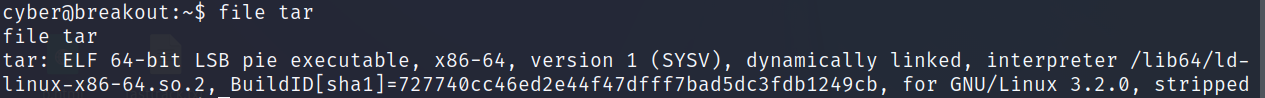


Bash反弹

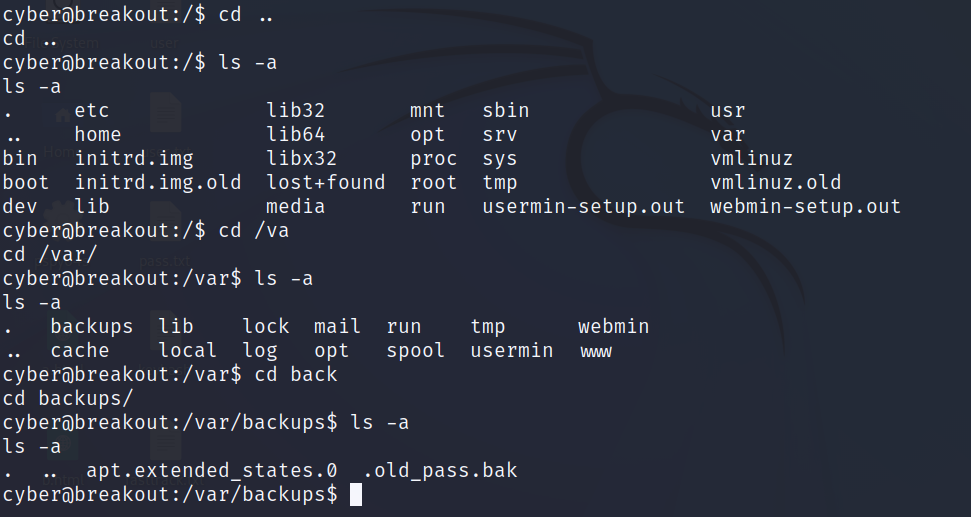




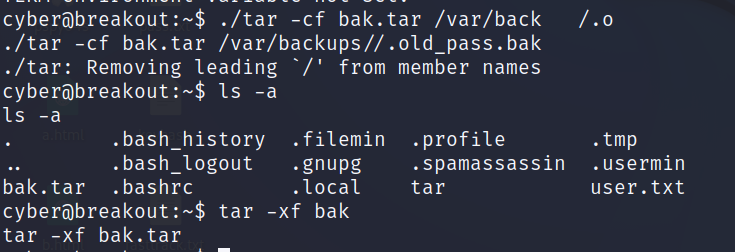


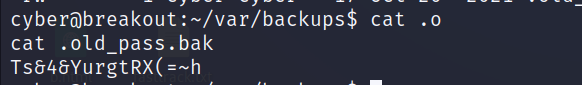


先看看备份的文件

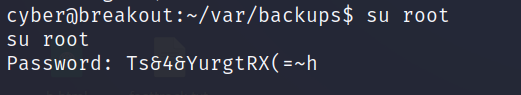


想办法查看里面的内容

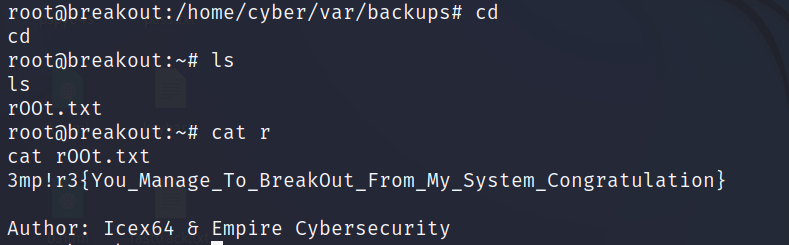




查看刚刚加压的备份



成功登入



拿到flag结束！