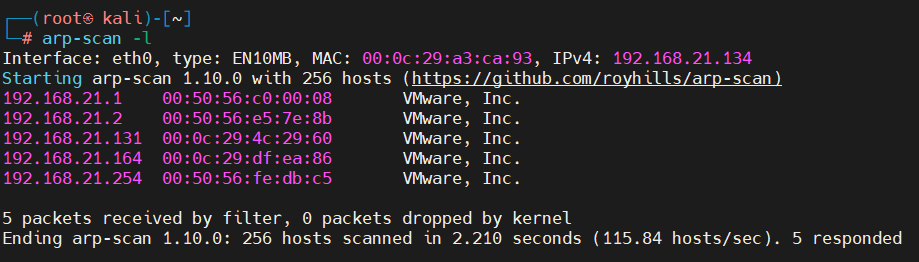
Funbox11

下载地址：<https://www.vulnhub.com/entry/funbox-scriptkiddie,725/>

主机发现

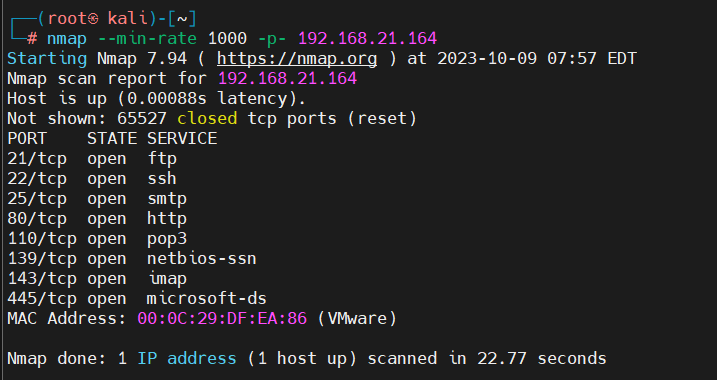
arp-scan -l



目标192.168.21.164

端口扫描

nmap --min-rate 1000 -p- 192.168.21.164



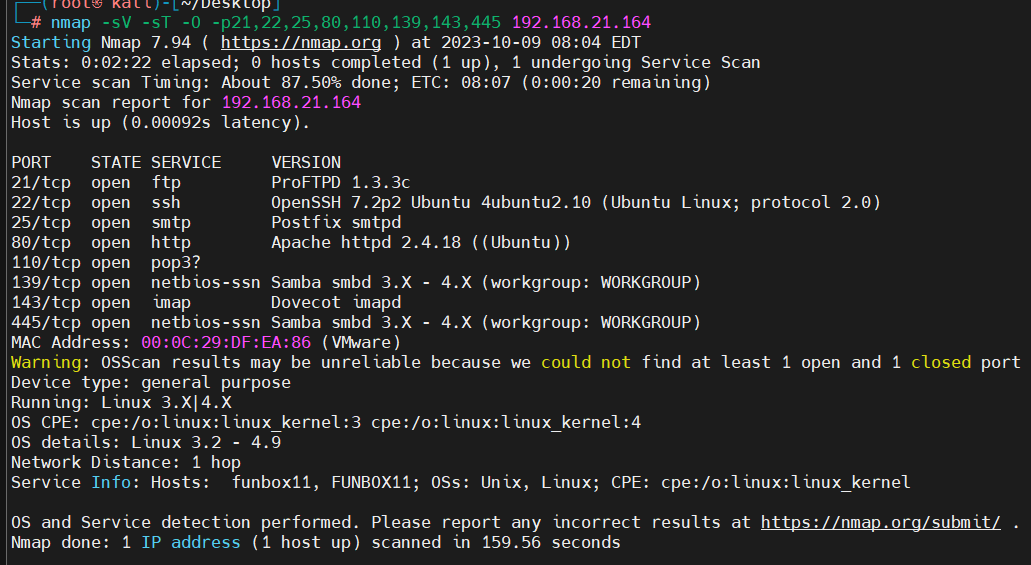
端口好多处理一下吧

nmap --min-rate 1000 -p- 192.168.21.164 |grep open |awk -F '/' '{print $1}' |tr '\n' ','



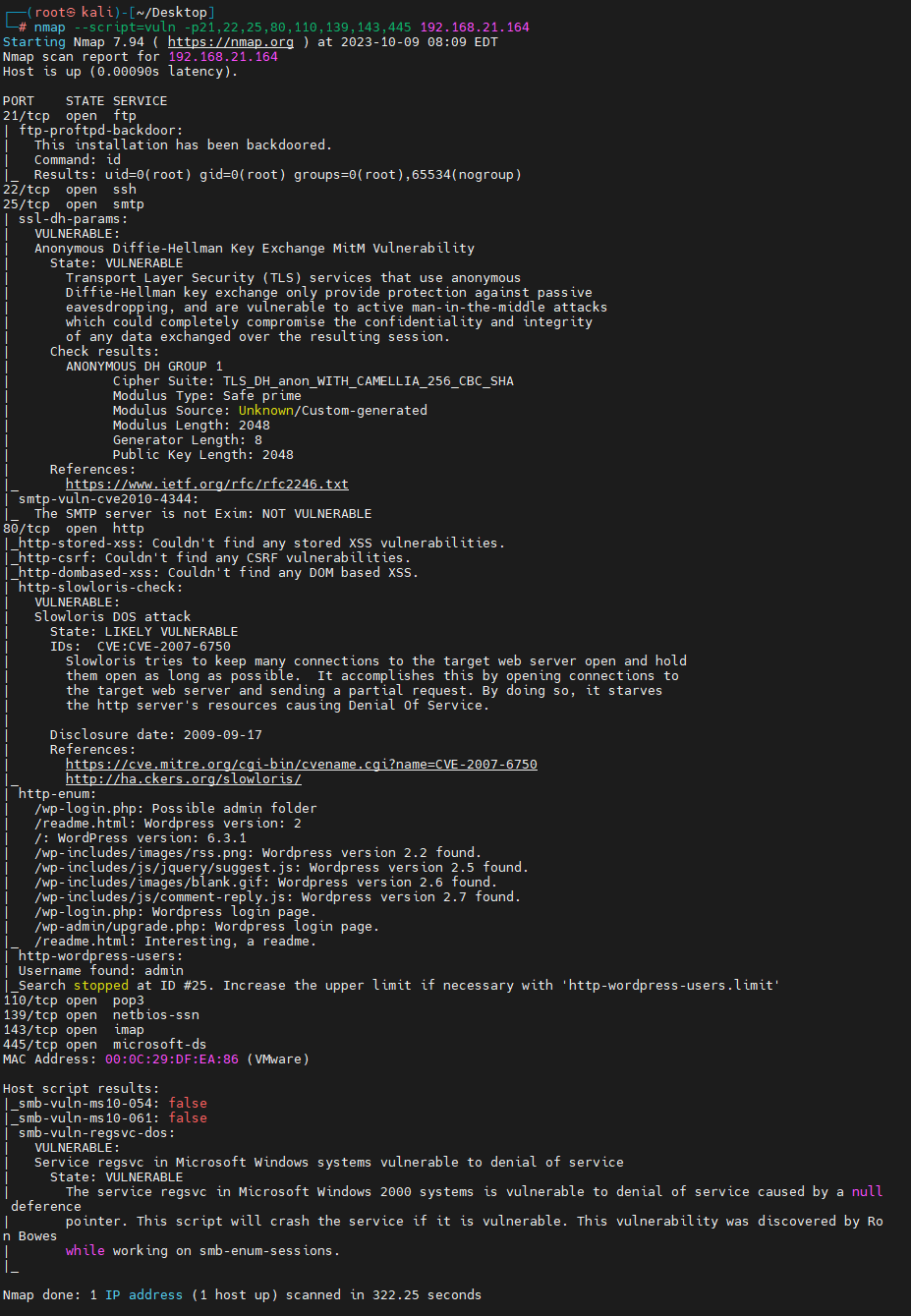
端口服务版本扫描

nmap -sV -sT -O -p21,22,25,80,110,139,143,445 192.168.21.164



漏洞扫描

nmap --script=vuln -p21,22,25,80,110,139,143,445 192.168.21.164



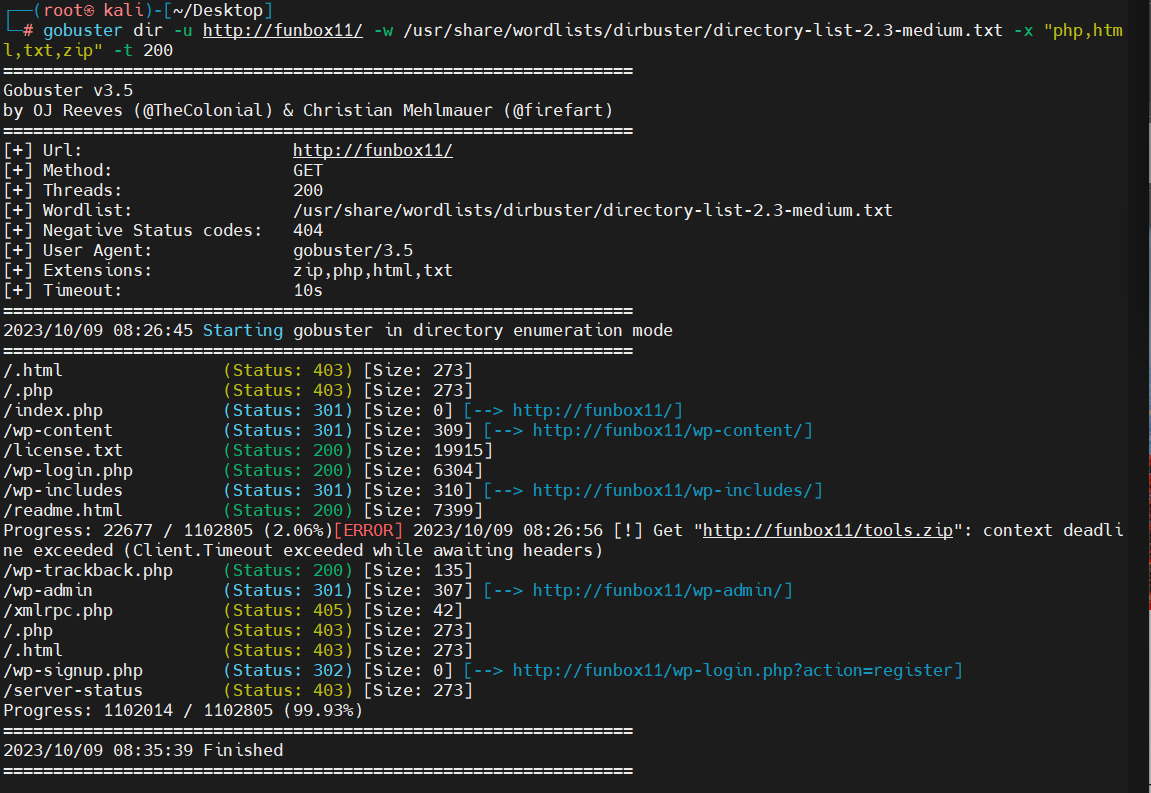
先看web





这个应该是域名，改host

扫描目录

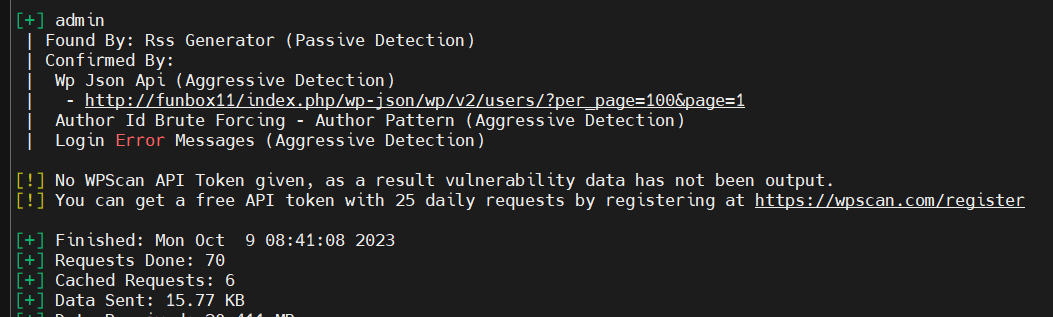


这个大概率是wp框架了

正好kali有wpscan

先来个用户名爆破吧

wpscan --url http://funbox11/ --enumerate u



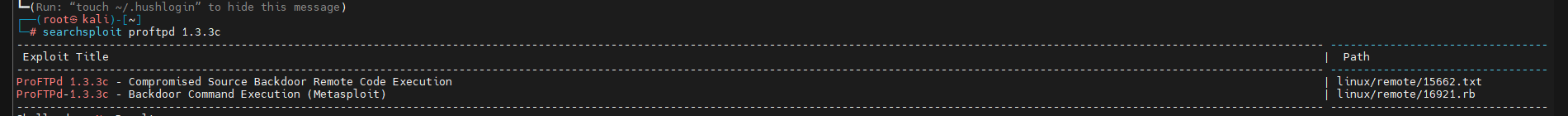
拿到用户名再来密码

wpscan --url http://funbox11/ --passwords /usr/share/wordlists/rockyou.txt --usernames admin

时间过长不想看了

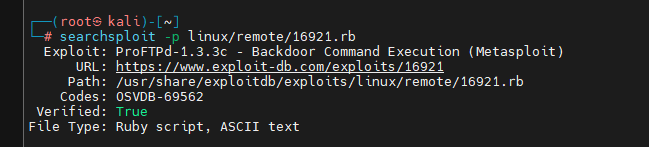
之前也没有扫到就换了一个突破口

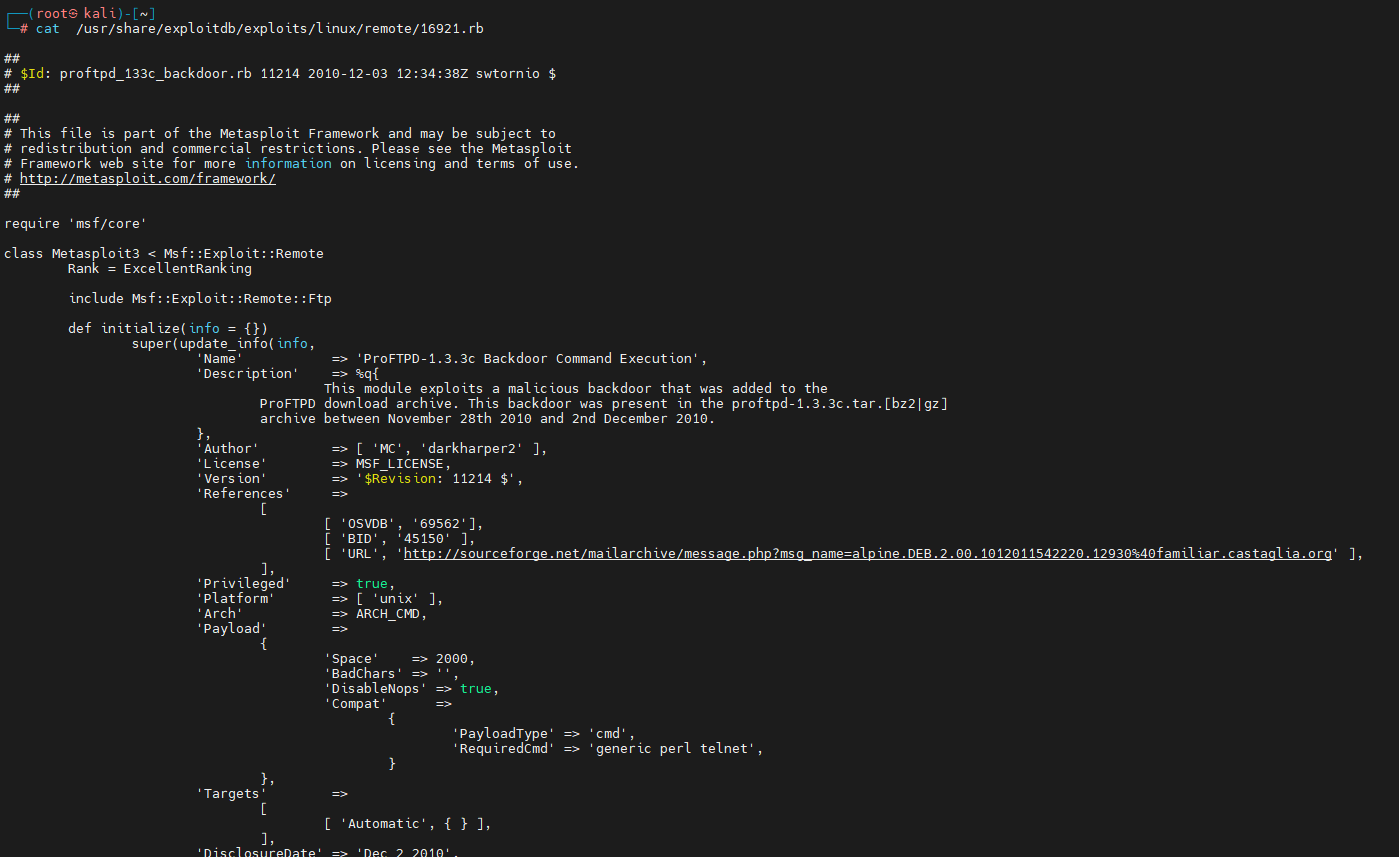
ftp

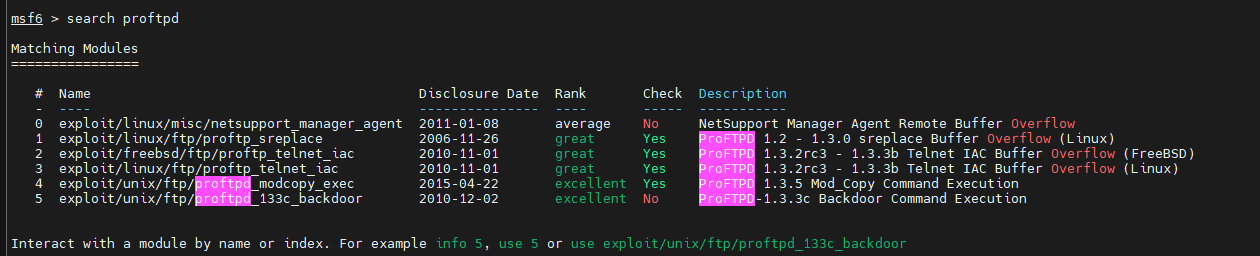


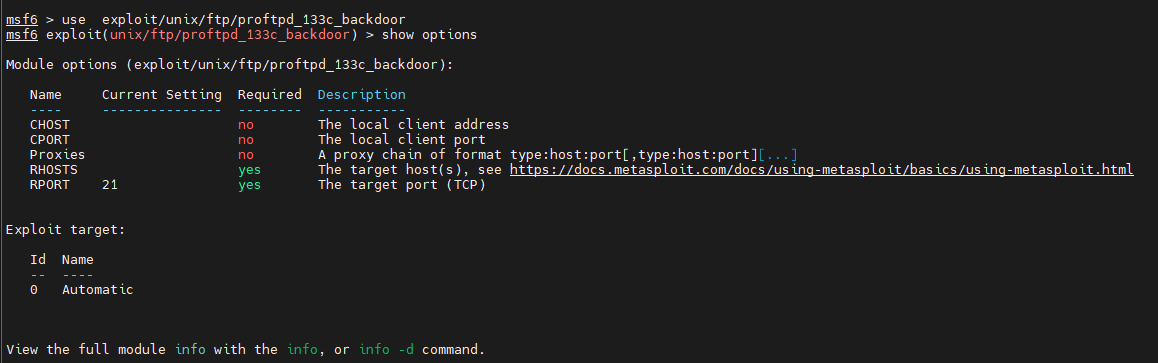
发现ftp有漏洞的而且msf能用

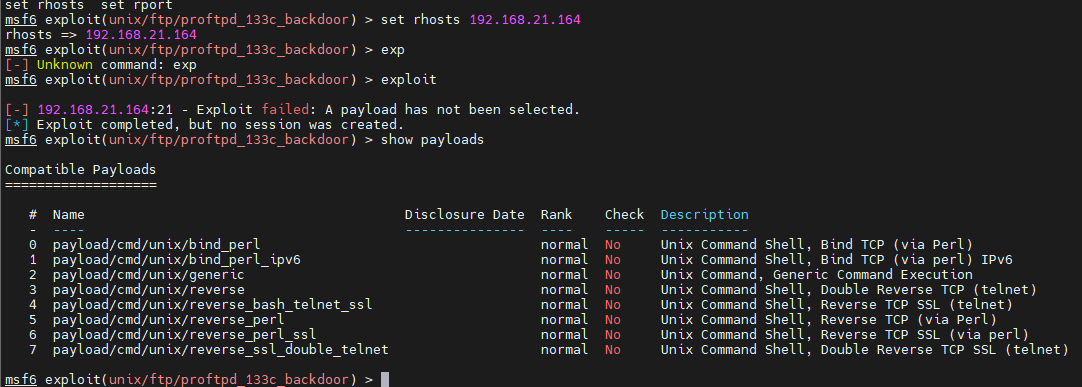
searchsploit -p linux/remote/16921.rb





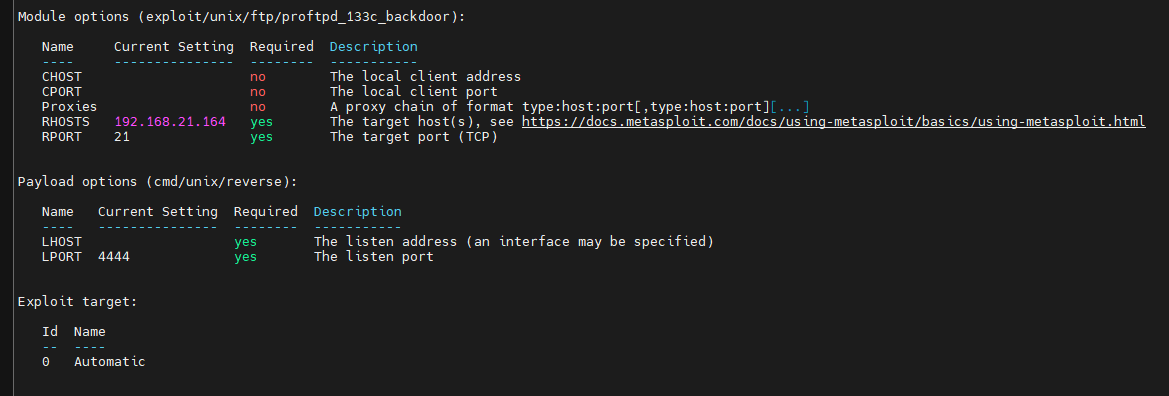




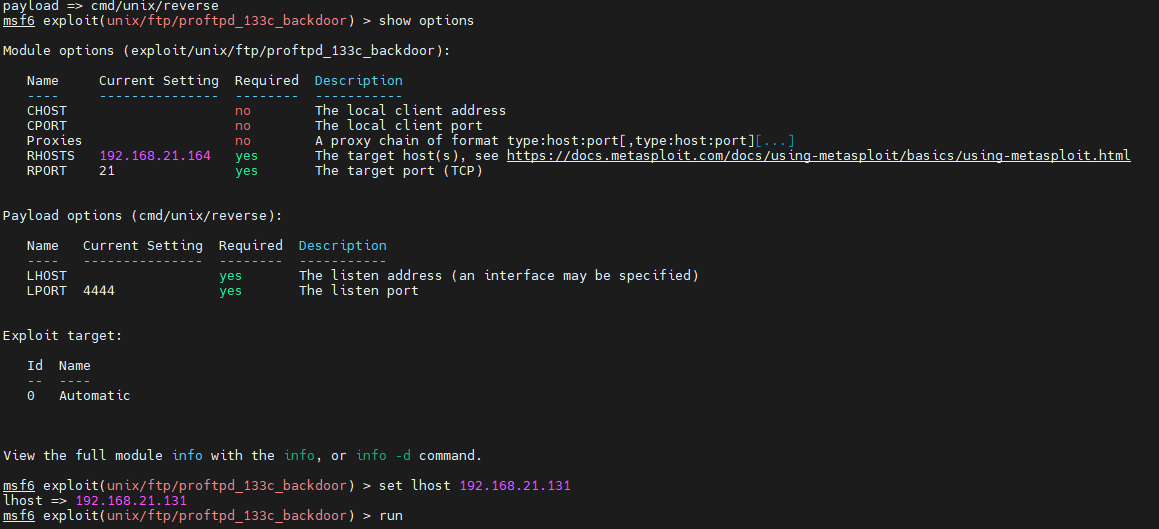


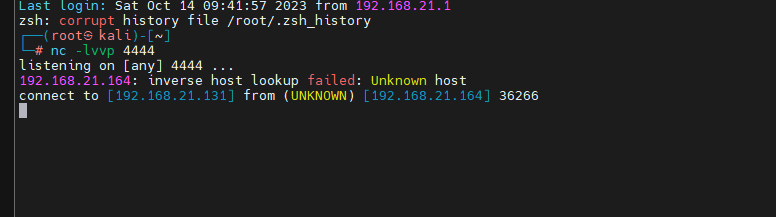
设置payload



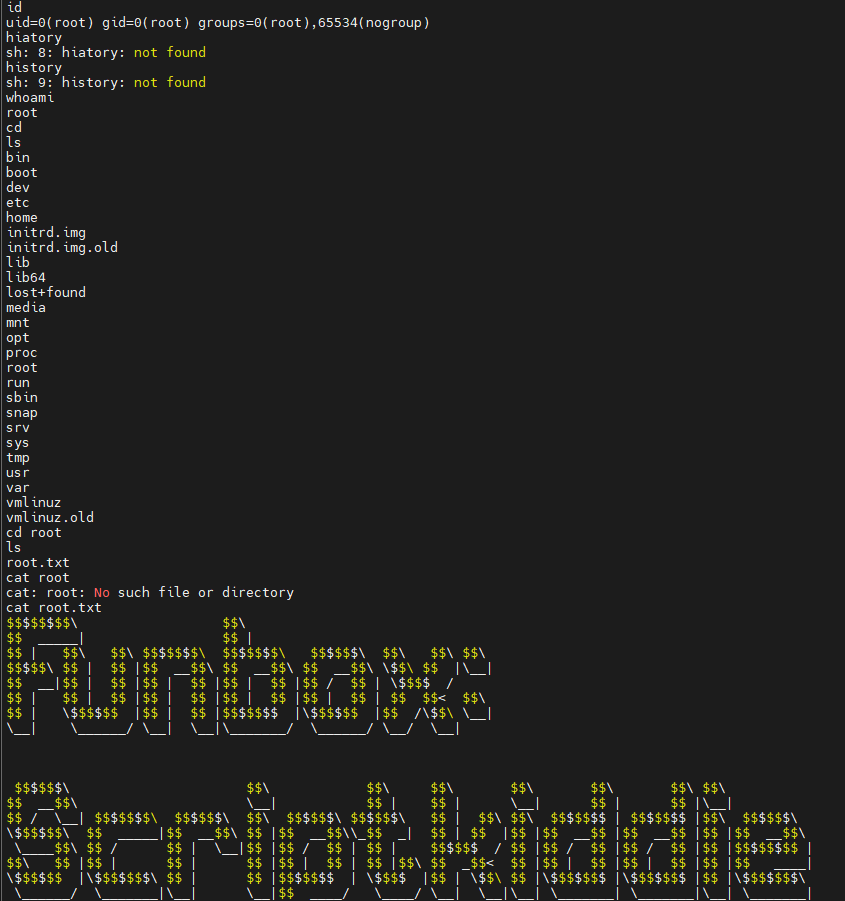


调整设置





连接成功



结束