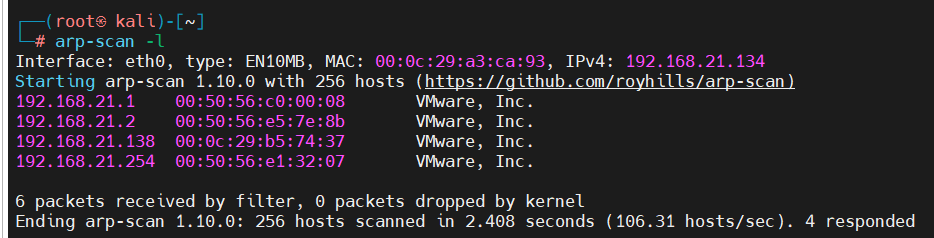
ELECTRICAL

下载地址：[digitalworld.local: electrical ~ VulnHub](https://www.vulnhub.com/entry/digitalworldlocal-electrical,747/)

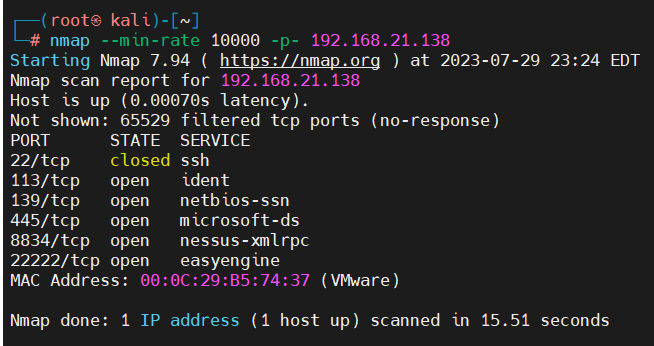
主机发现

arp-scan -l

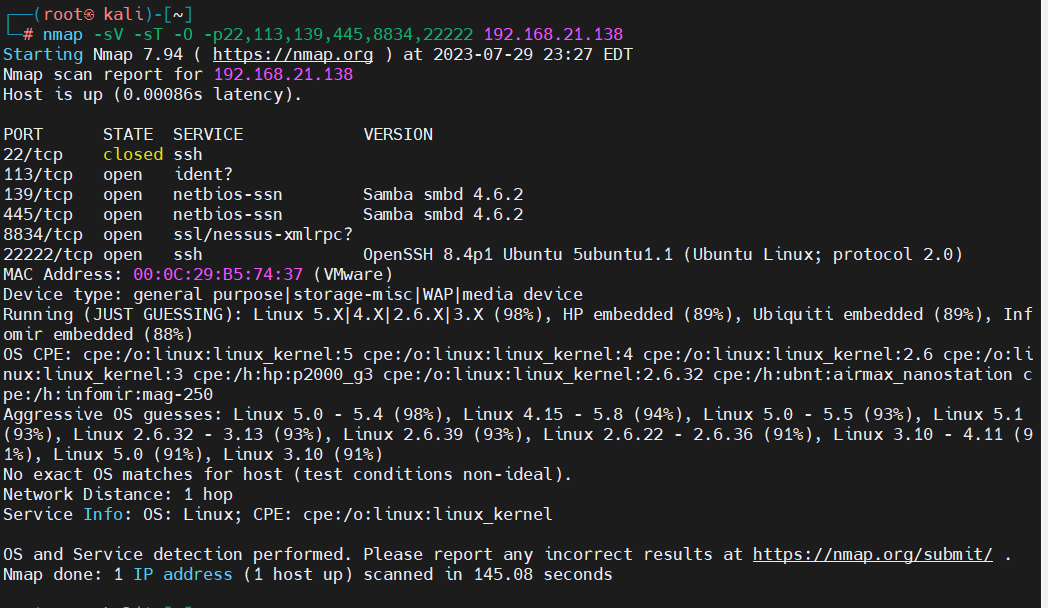


端口扫描

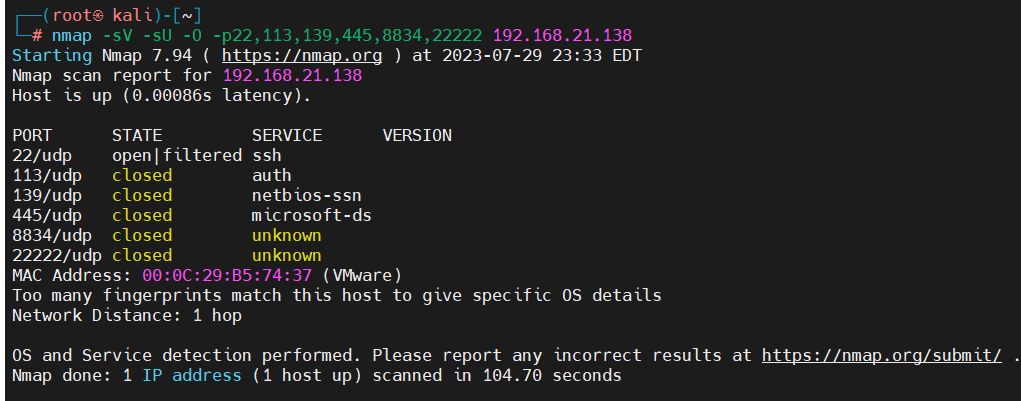
nmap --min-rate 10000 -p- 192.168.21.138



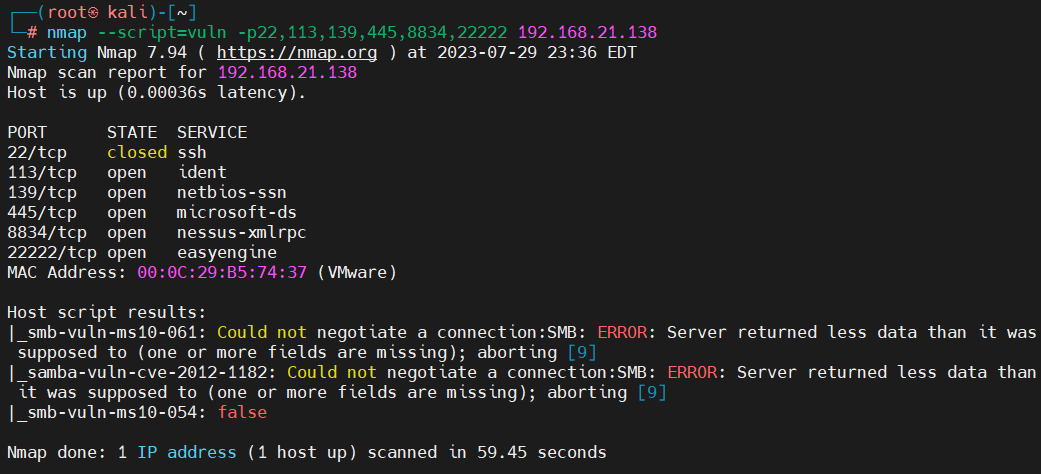
nmap -sV -sT -O -p22,113,139,445,8834,22222 192.168.21.138



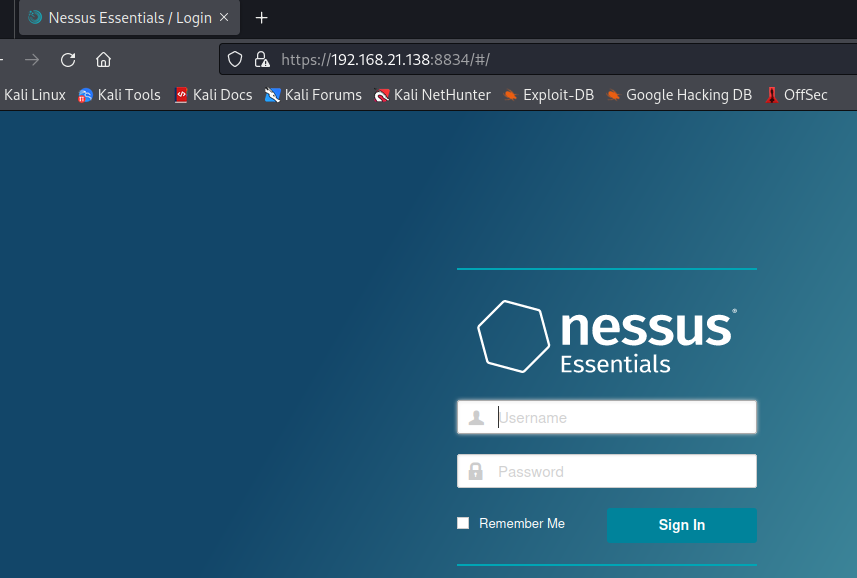
nmap -sV -sU -O -p22,113,139,445,8834,22222 192.168.21.138



nmap --script=vuln -p22,113,139,445,8834,22222 192.168.21.138

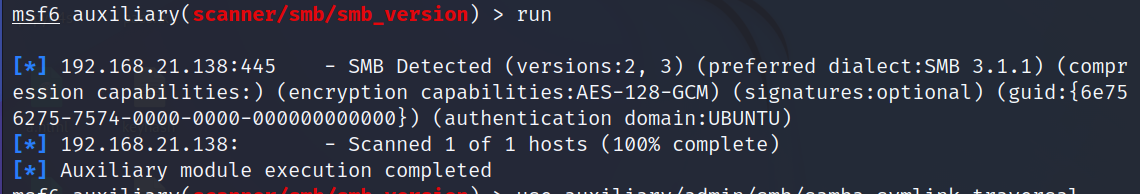


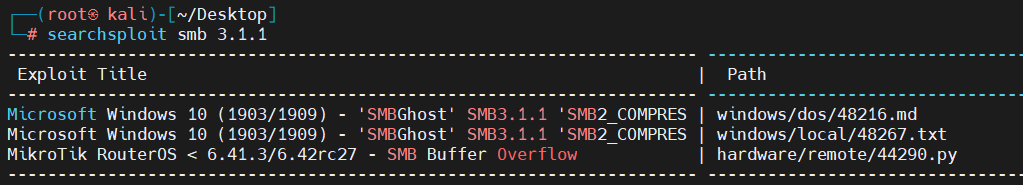
看到一个比较熟悉的服务nessus（漏洞扫描软件）先去看看



剩下来只有一个突破口了NetBios

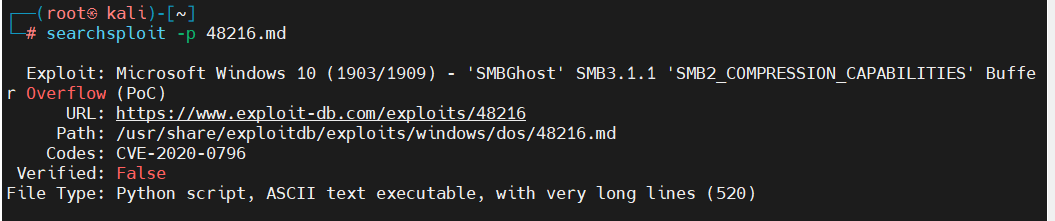
先看版本



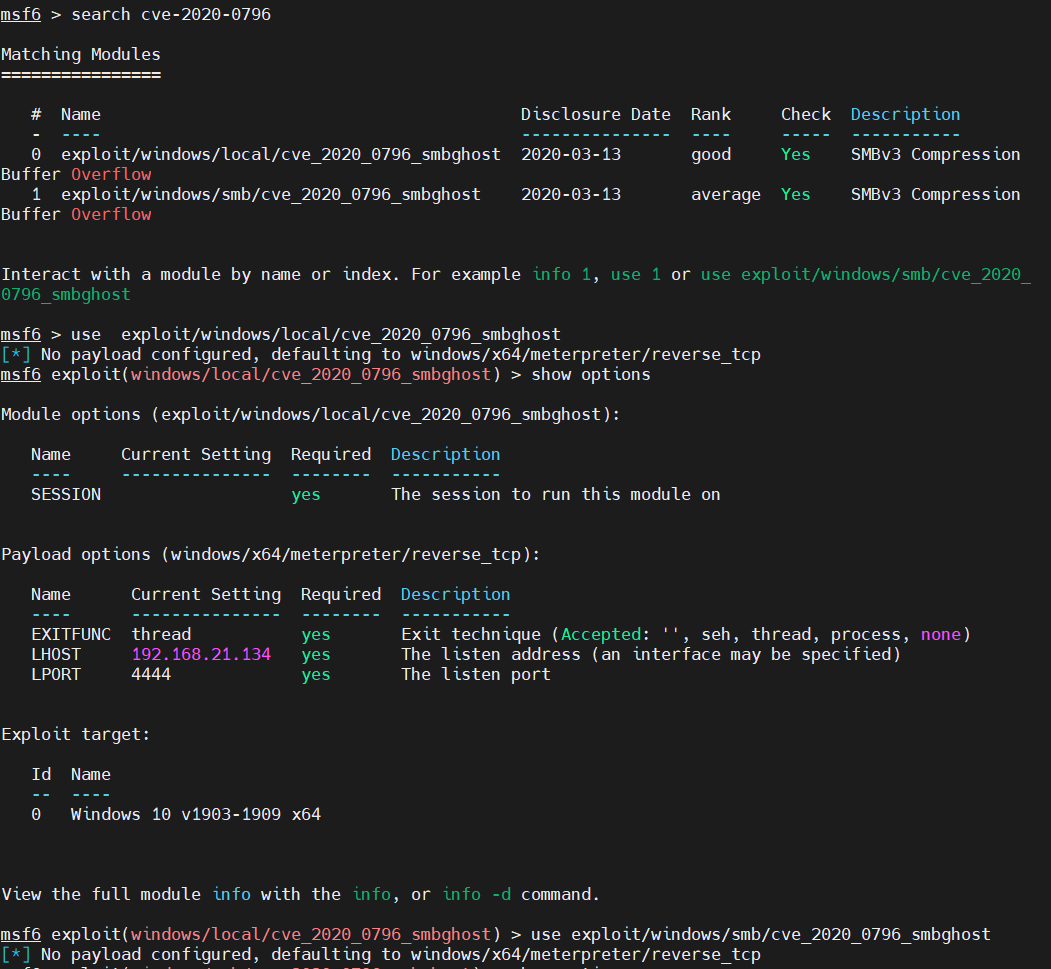
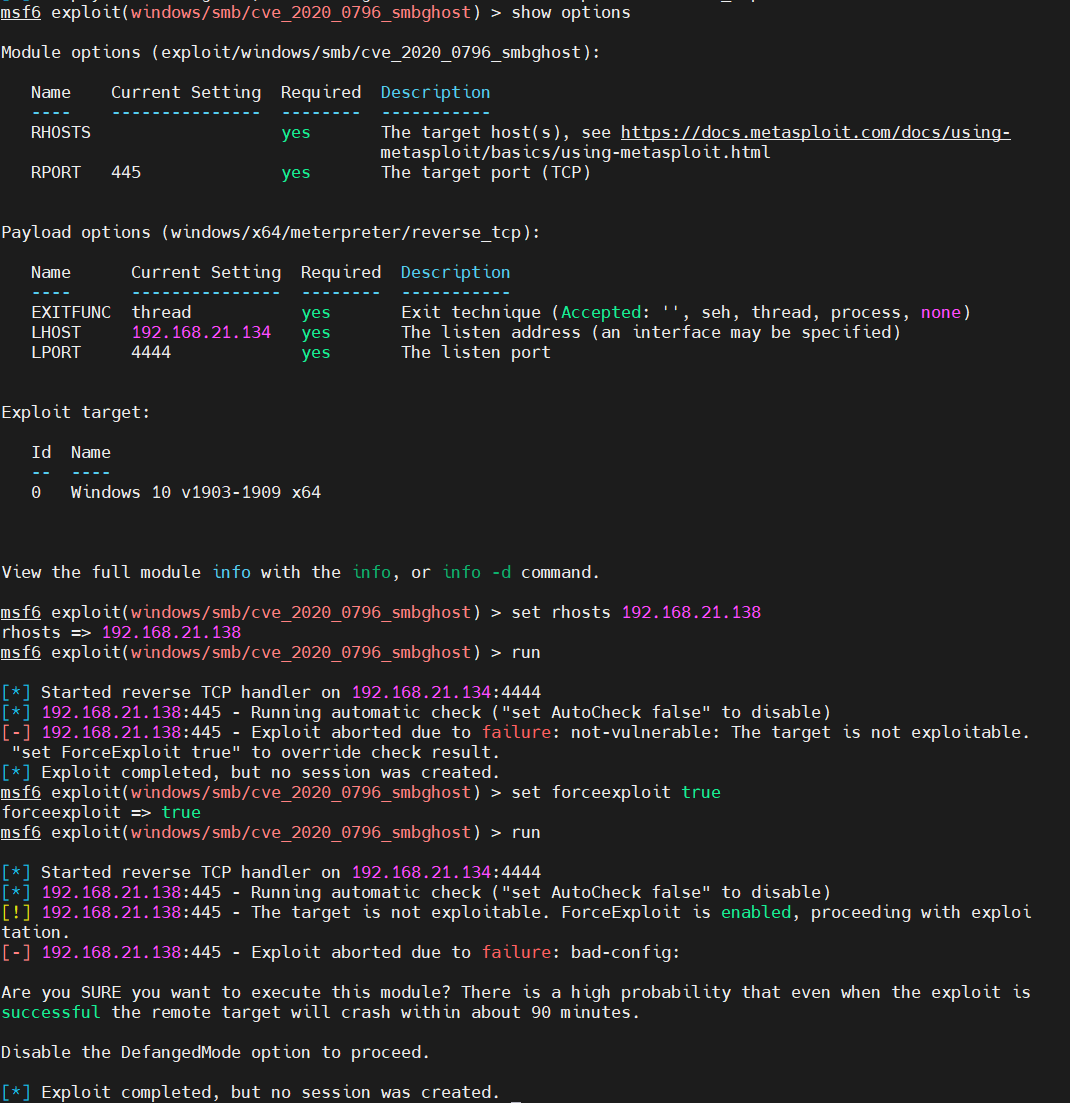


直接看路径

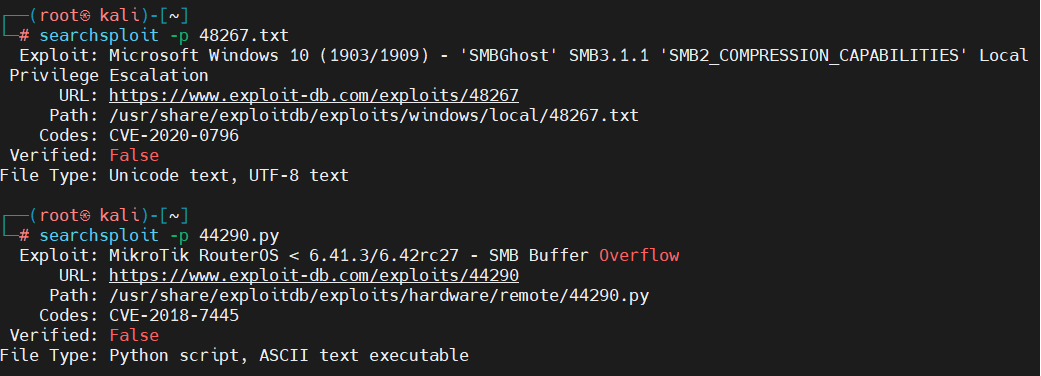
searchsploit -p 48216.md

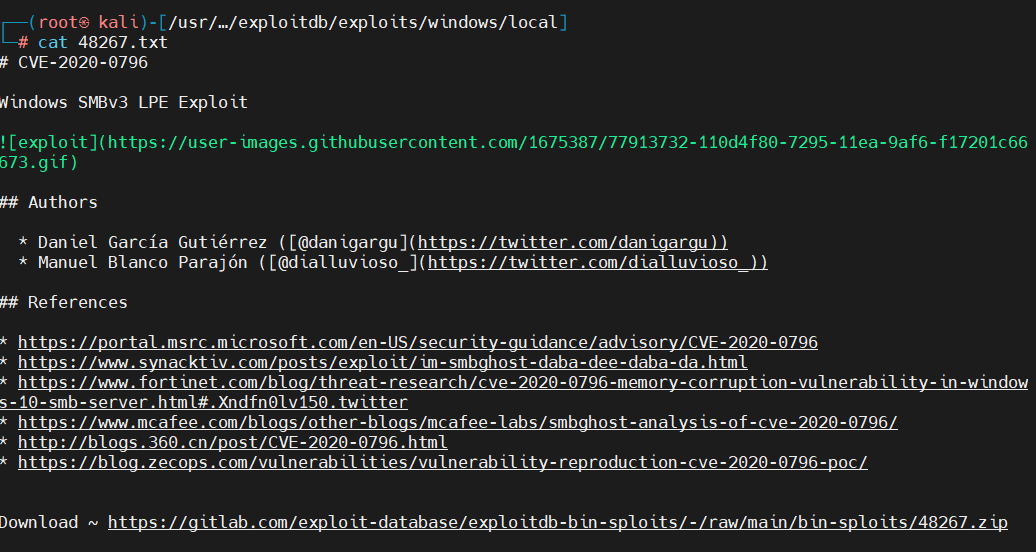


再msf里面看看能不能利用

一个一个查



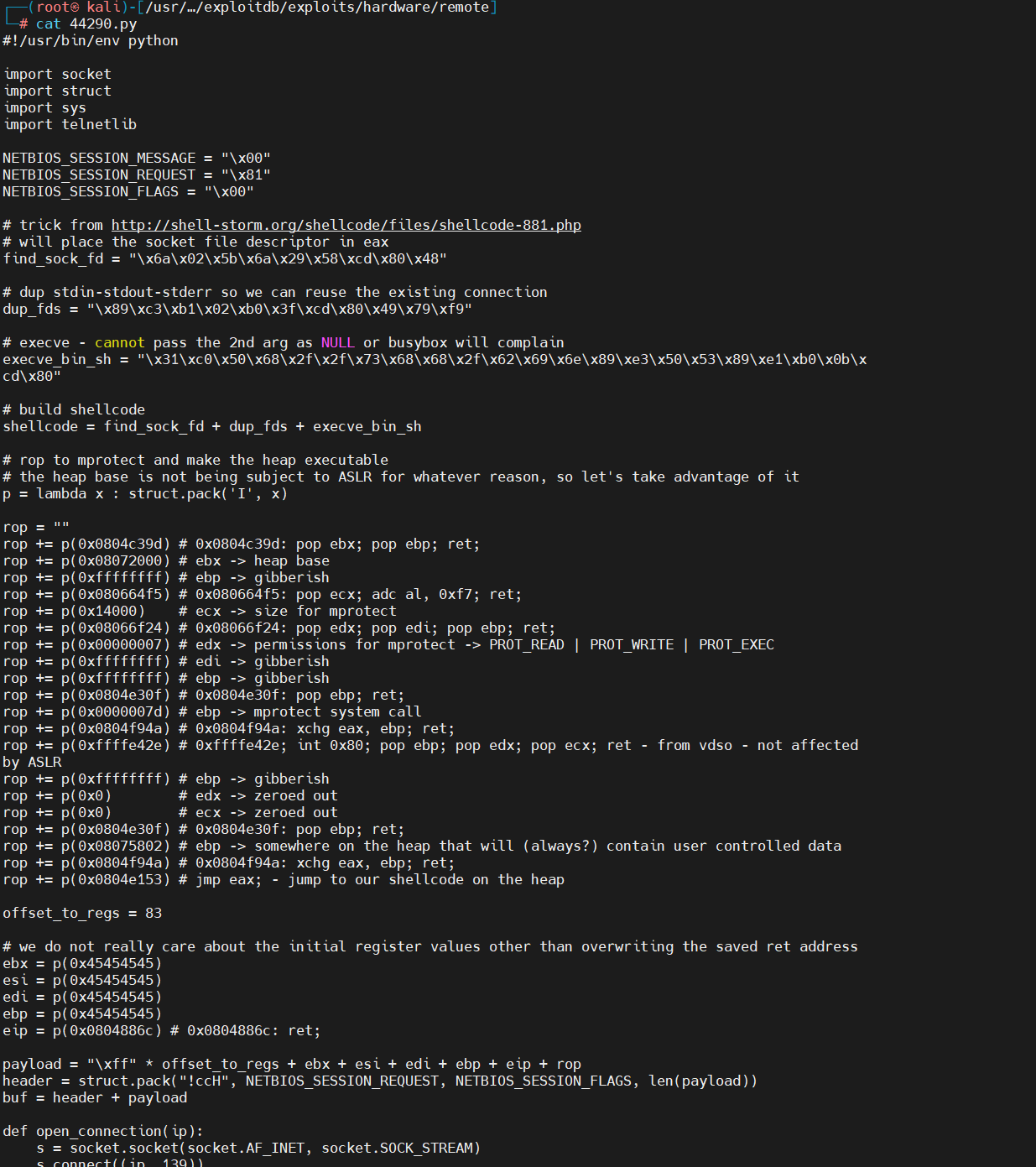


下载下来

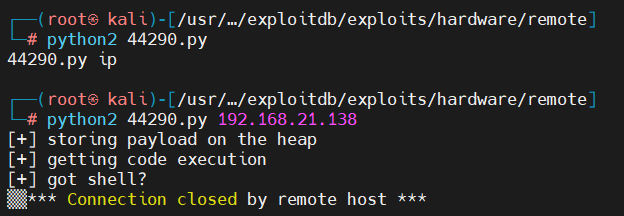
wget <https://gitlab.com/exploit-database/exploitdb-bin-sploits/-/raw/main/bin-sploits/48267.zip>



解压即可



直接先跑这个脚本



Emmm用不了

下一个