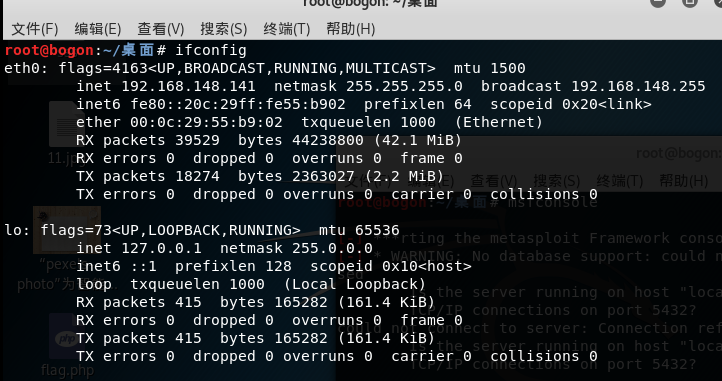
**1、网络[测试](javascript:;" \t "_self)环境构建**

　　首先需要先配置好一个渗透测试用的网络环境，包括如图1所示的运行Kali [**Linux**](javascript:;)系统的计算机，如图2所示[**Windows**](javascript:;) Server 20008系统的计算机。这两台计算机处于同一个网段中，可以相互通讯，Kali系统用作攻击机，下面将在此系统上运行**[Metasploit](javascript:;" \t "_self)**进行渗透测试，而Windows 20008是本次任务中需要进行渗透入侵的靶机，保持安装后的默认状态，没有打额外的系统安全补丁。

Kali的IP为192.168.148.141

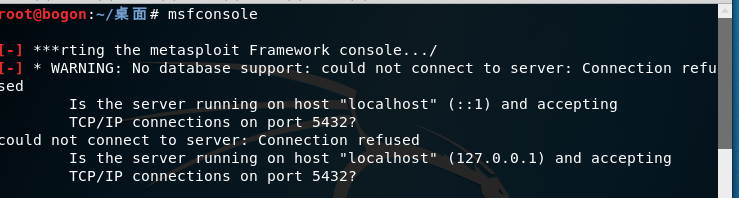


靶机的IP：192.168.148.132



2.扫描靶机

在Kali攻击机上执行msfconsole命令，即可进入metasploit环境.



报以下警告处理方法

意思是没有启动带数据库支持的MSF服务需要我们去启动；  
我们就exit退出msfconsole然后输入：/etc/init.d/postgresql start输入完成后等待显示：\*[ ok ] Starting postgresql (via systemctl): postgresql.service.\*这个字样在输入：msfdb init

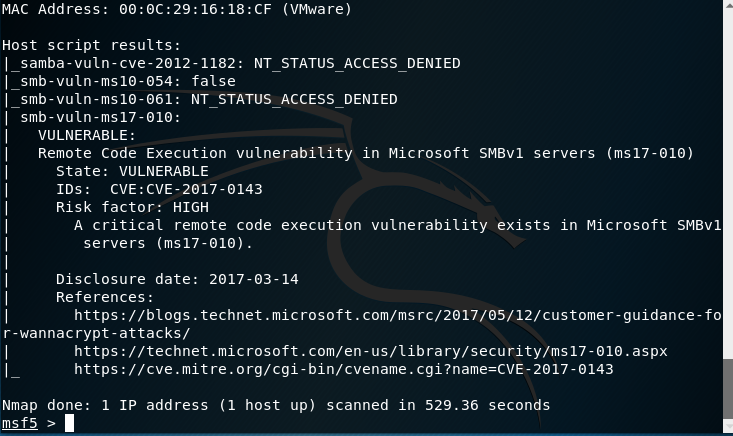
显示出现：[i] Database already started  
[i] The database appears to be already configured, skipping initialization

可以使用两种方法进行扫描检查是否存在常见的漏洞：

　　第一种方法：nmap -O 靶机IP （探测目标系统的漏洞，容易误报）

　　第二种方法：nmap --script=vuln 靶机IP(使用频率高 )

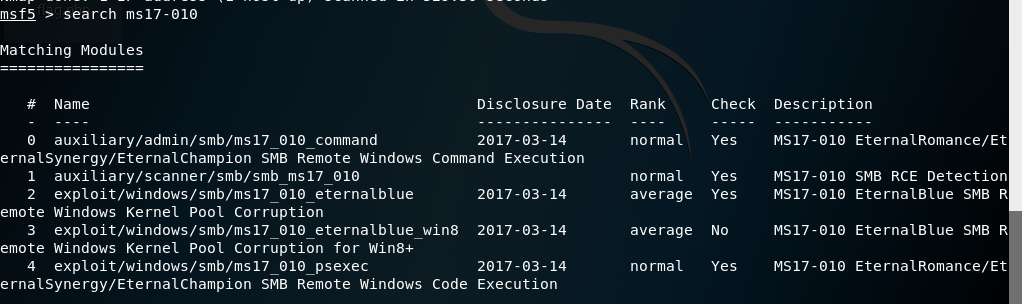
扫描到靶机以下信息包括开放的端口等



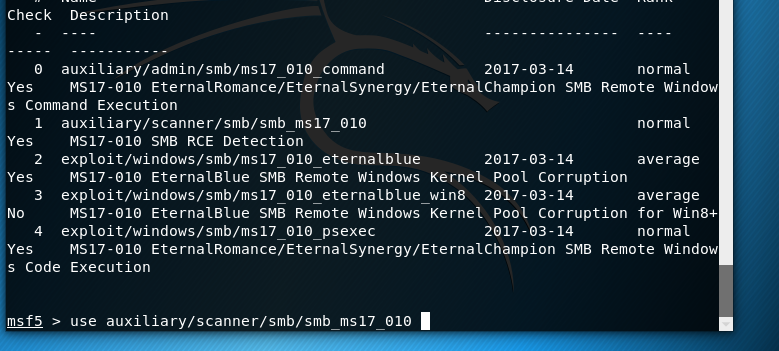
微软安全报告：

<https://docs.microsoft.com/zh-cn/security-updates/Securitybulletins/2008>

搜索该漏洞



使用探测模块



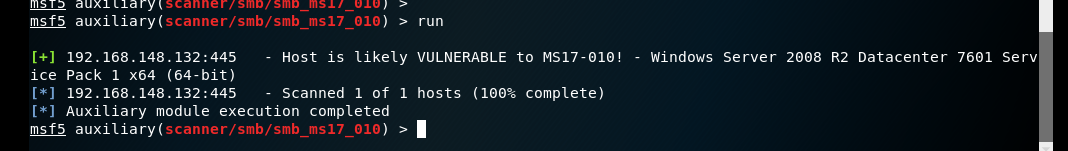
配置一些信息：

Set lhost (kali的IP)

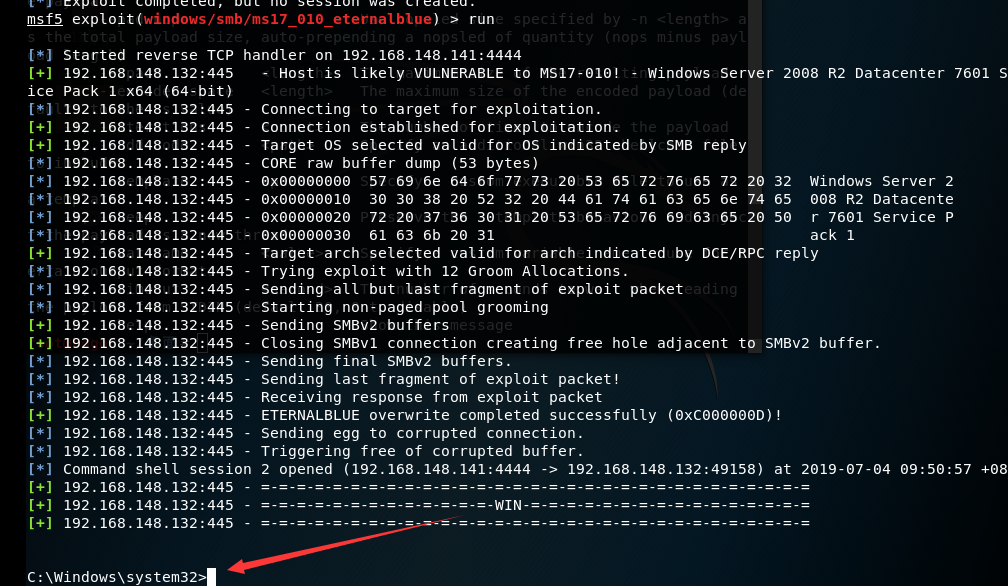
Set rhost(靶机的IP)

payload又称为攻击载荷，主要是用来建立目标机与攻击机稳定连接的，可返回shell，也可以进行程序注入等。

run是没有问题的



直接上利用模块



已经成功进入到靶机

