# God.org单域环境攻略(一)

## 环境准备

首先感谢@klion师傅分享的域环境。本文针对God.org单域环境进行阐述。

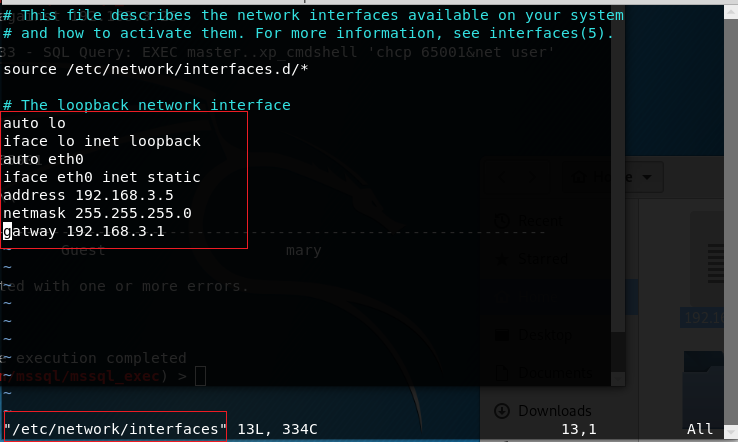
链接：<https://pan.baidu.com/s/1j7OgZ3pOnSNxBCHbnUZ4SQ> 提取码：z7m8

准备环境：域环境、kali虚机、metasploit、nmap、netdiscover、rdesktop

由于预设的虚拟机系统是静态IP地址，直接用kali虚拟机，是无法连通到域环境地址的，因此需要将kali虚拟机配置为统一网段的静态IP地址。用Vmware打开虚拟机，在虚拟机的描述信息中可以看到登录口令。登录进去，发现ip网段为192.168.3.\*，因此设置kali虚拟机的静态ip为192.168.3.5。



修改kali虚机里面的” /etc/network/interfaces”文件，添加红框部分内容，网上说重启服务生效“service networking restart”，但我需要重启kali才能生效。

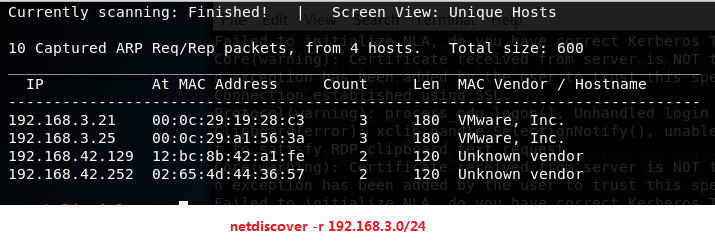


## 主机探测

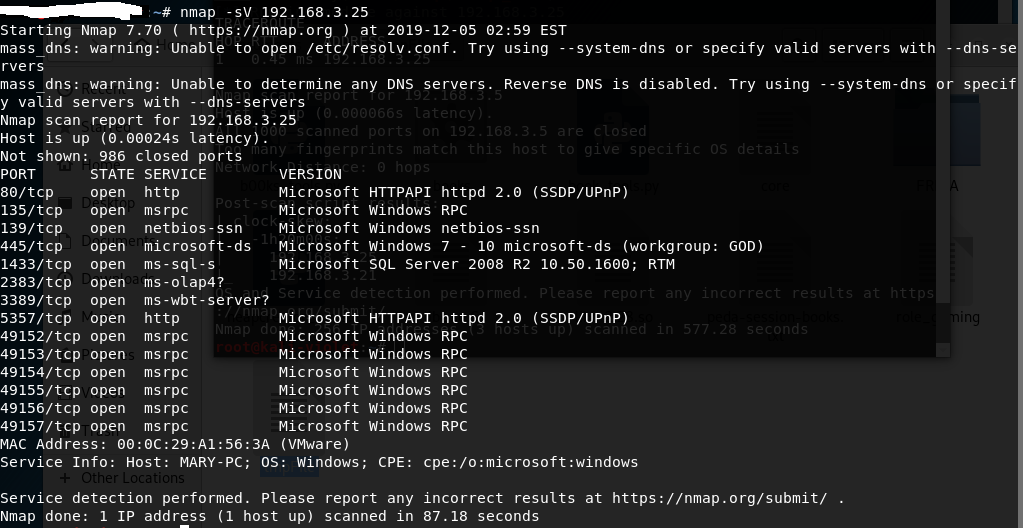
预设：kali虚机通过破译wifi或其他方式已接入内部网络

1. netdiscover扫描局域网存活主机。

通过netdiscover工具能探测所有流经它的地址，无论目的地在是否是它。因此比nmap探测到更多的地址，如192.168.42.129、192.168.42.152，即使我们的kali虚机与这两个地址是不连通的。



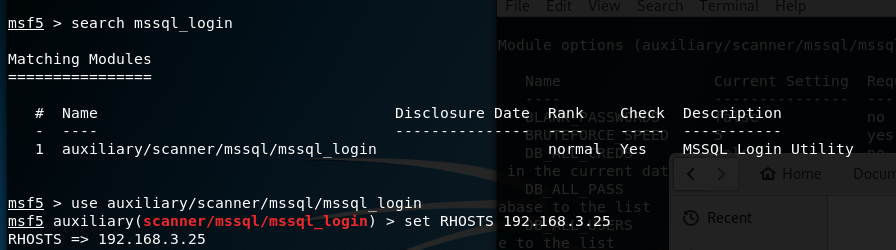
1. nmap –sV –Pn 192.168.3.25，sV指探测端口和服务信息，Pn参数表示不再进行ping探测。发现该机器是windows机器，并且开通了1433端口，目标机器上运行着mssql服务，但是没有开通3389端口，无法进行远程桌面连接。注意：主机名为MARY-PC，后面会用到。

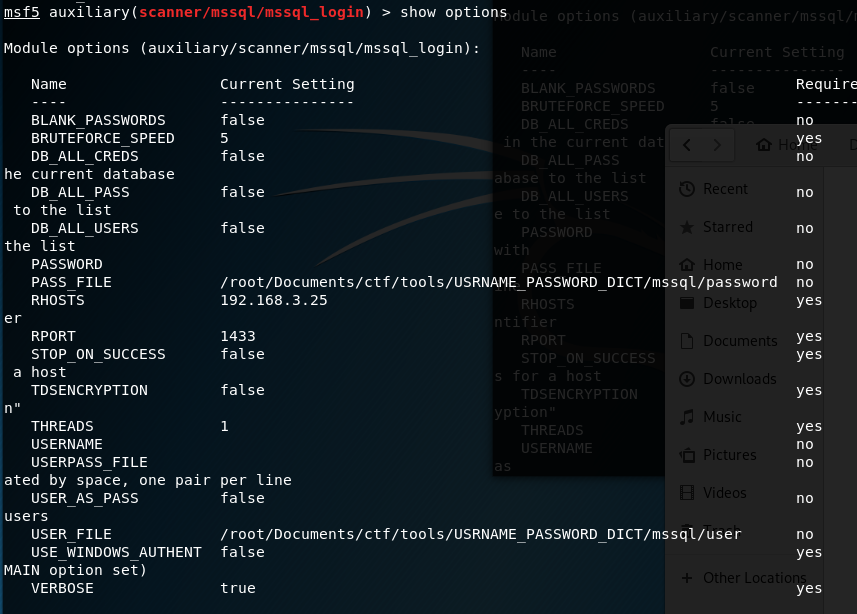


## 攻击主机上的服务

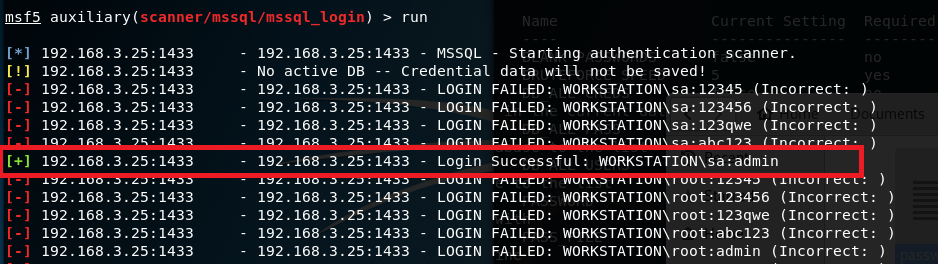
1. mssql口令爆破

借助metasploit的mssql\_login模块，进行弱口令爆破。具体payload配置如下图所示：

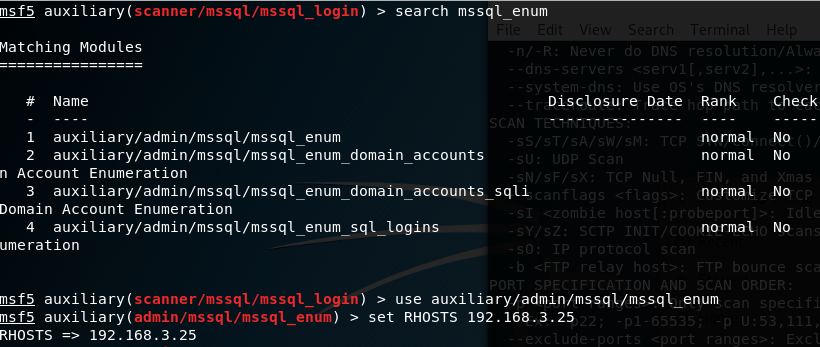


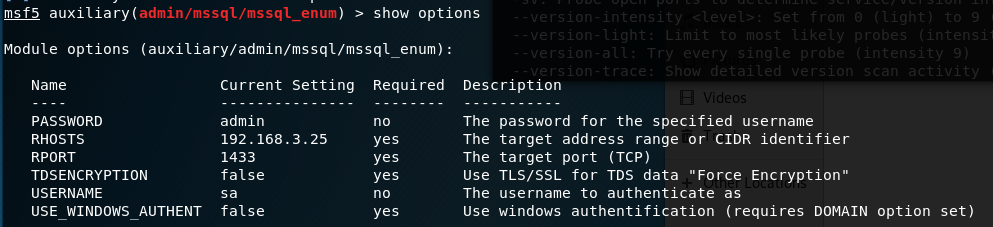


结果如下所示，发现弱口令sa:admin

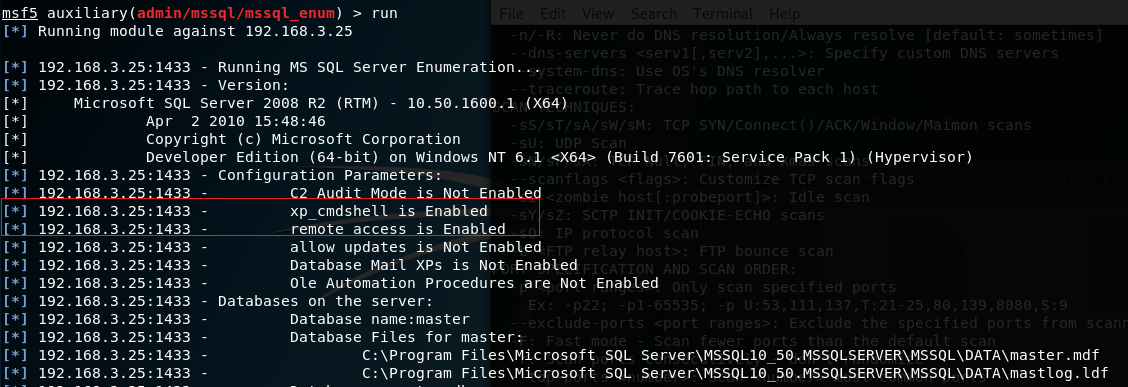


1. mssql配置信息枚举，需要使用数据库用户名和口令。

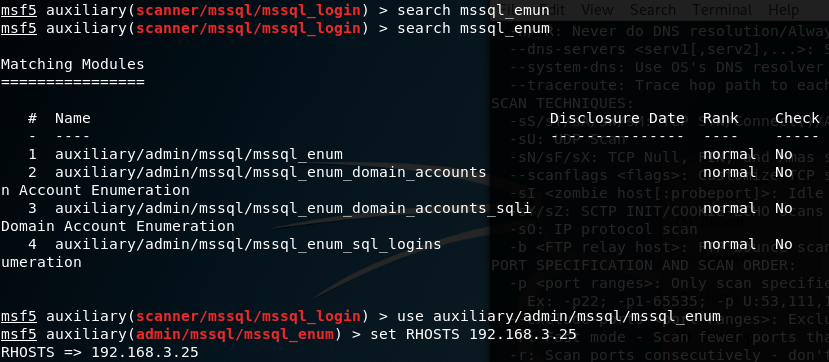


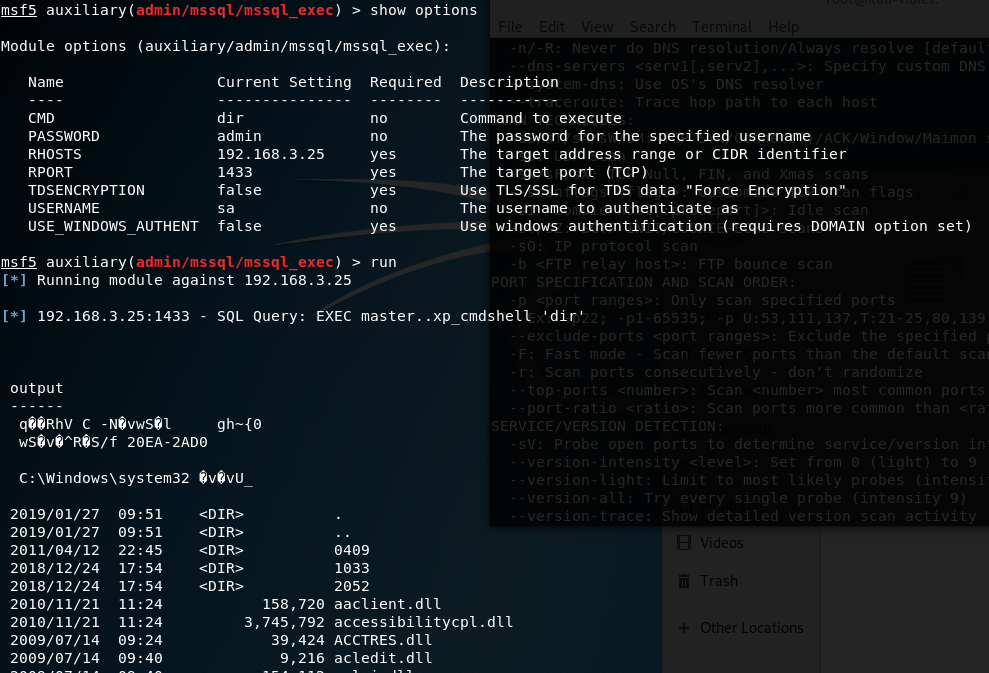


结果发现它允许命令执行，也允许远程连接。考虑mssql命令执行利用模块。



1. mssql\_exec借助数据库执行cmd命令,继承sql server权限, 需要使用数据库用户名和口令。





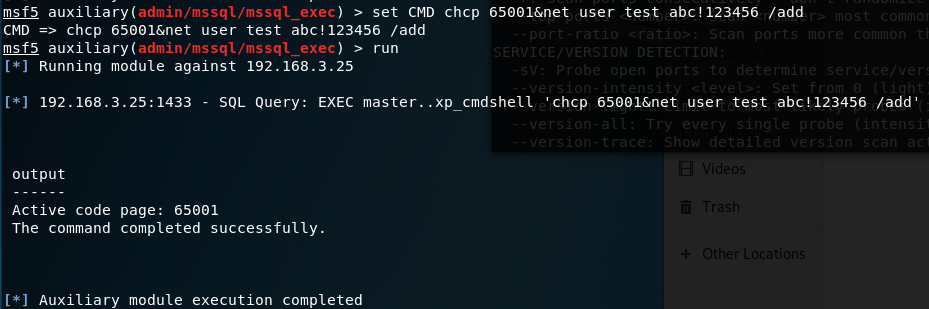
可见cmd命令dir执行成功。

## GetShell

前面步骤完成后，我们已经获得命令执行的接口，接下来考虑如何拿到系统控制权。

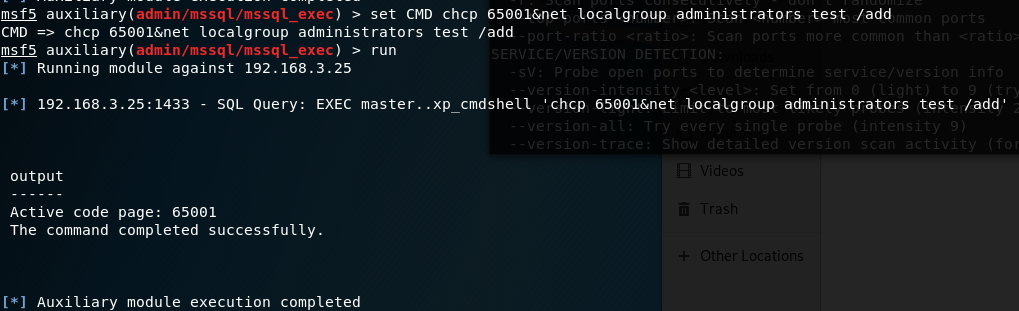
1. 命令行创建用户

chcp 65001是改变字符集的命令，解决cmd控制台输出乱码；‘&’是连接两个cmd命令的管道符；net user test abc!123456/add是创建用户名为test,密码为abc!123456的系统用户。



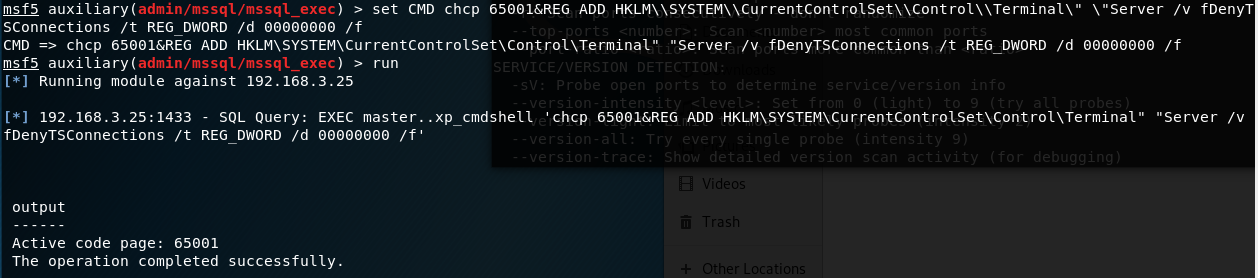
1. 将新创建的用户加入到管理员组

net localgroup administrators test /add表示将test用户加入到administrators组中



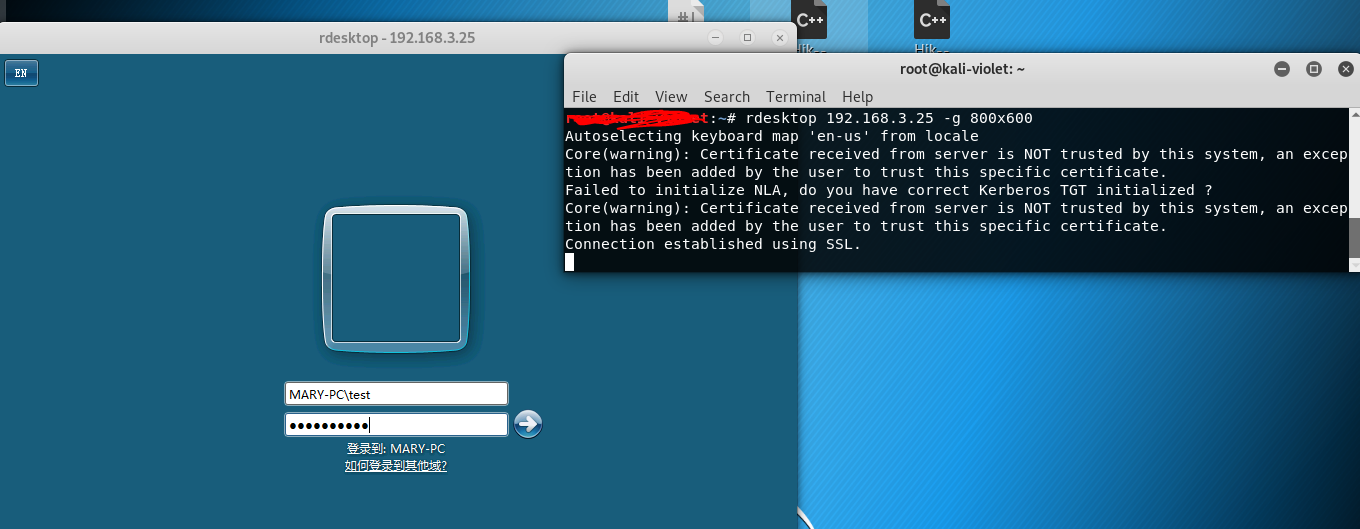
1. 命令行打开3389端口

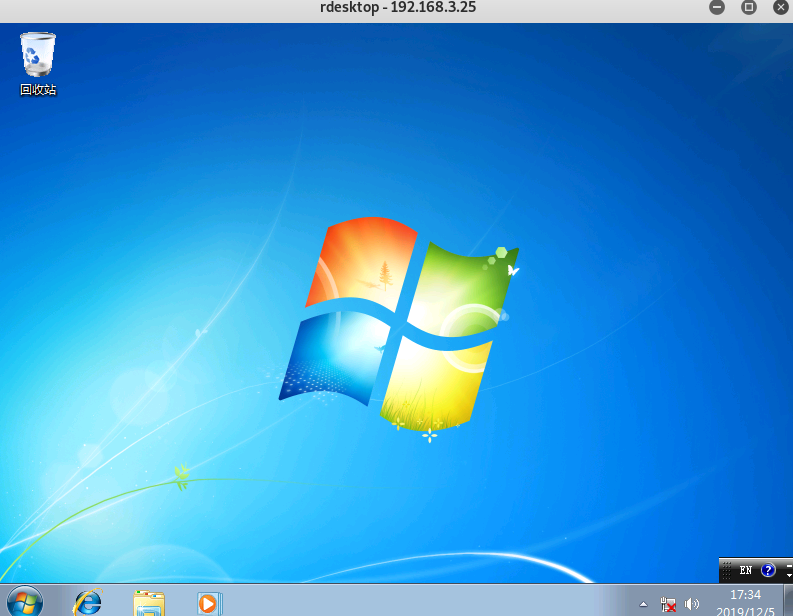
打开主机3389端口，允许远程桌面连接。命令是”chcp 65001&REG ADD HKLM\\SYSTEM\\CurrentControlSet\\Control\\Terminal\" \"Server /v fDenyTSConnections /t REG\_DWORD /d 00000000 /f”,记得转义斜杠’\’和双引号‘“’。



1. 远程登陆主机

rdesktop 192.168.3.25 -g 800x600,由于我们创建的用户不是域用户，因此登录名为“主机名\用户名”，即MARY-PC\test,密码使我们设置的abc!123456





成功拿到主机。接下来进一步扩大控制范围将在下一篇中介绍。