# God.org单域环境攻略(二)

## 目标

上一篇中，我们已经获取到192.168.3.25(win7 x64)的控制权，但是没有获取到域用户的权限，且在目标系统中创建了一个新用户，痕迹明显。

本文的**目标是：隐藏自己，擦除上一次攻击过程的留痕；通过其他方式拿到目标机器SHELL。**

## 痕迹擦除

我们已经拿到机器控制权，但是在目标系统中创建了一个名为test的用户，持续控制该机器需要考虑如何拿到系统原来用户的口令，并删除我们新创建的用户test。

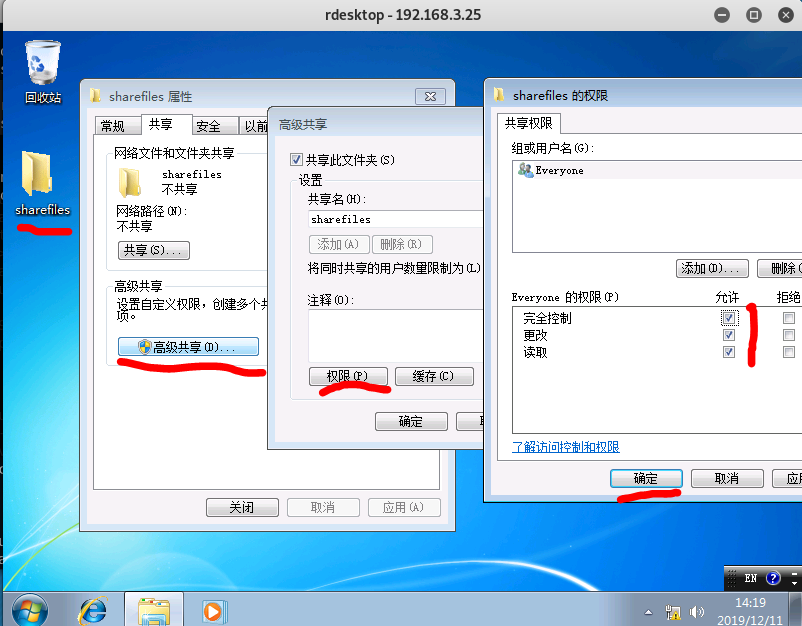
### 获取本机口令

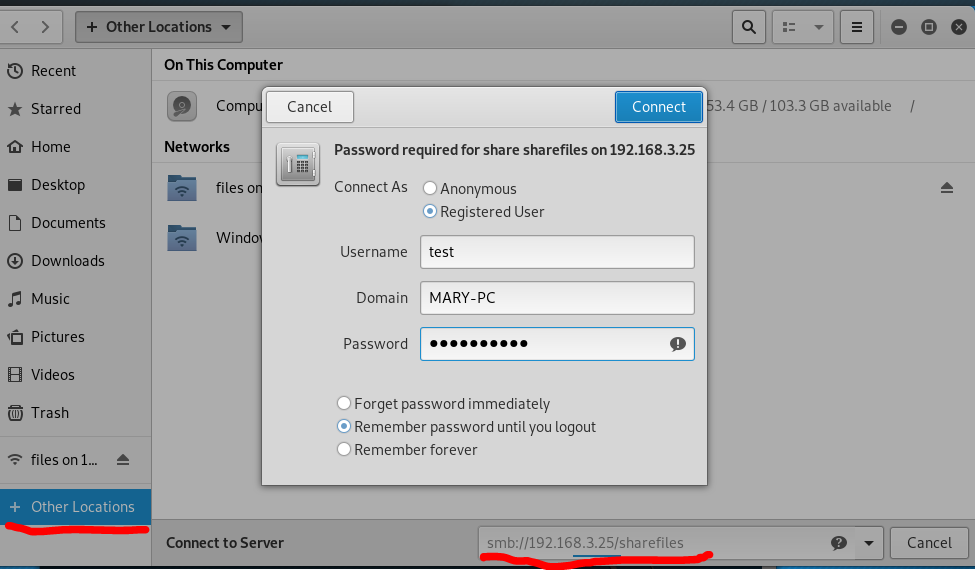
1. Mimikatz获取已登录用户的口令

这个方法的前提是登录用户在lsass内存中存在明文用户口令，如果用户未登录过，则无法获取到任何信息。

第一步：拷贝Minikatz软件到目标机器

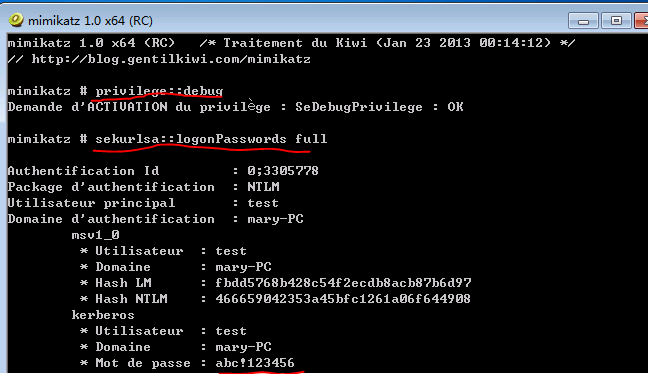
我们考虑文件共享，即在目标机器上创建一个共享目录，在攻击者的kali机器上连接共享目录进行文件传输。注意：需要将权限设置为完全控制。

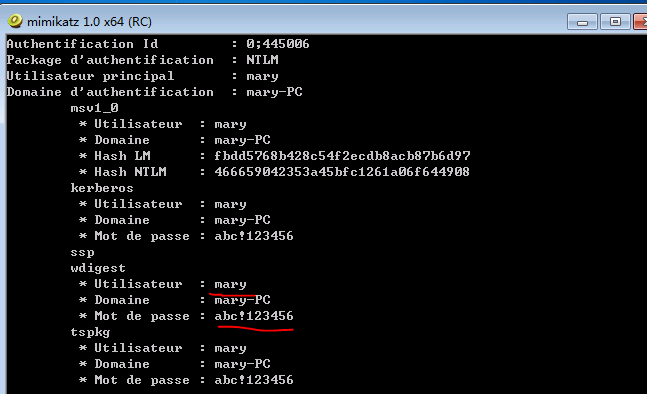




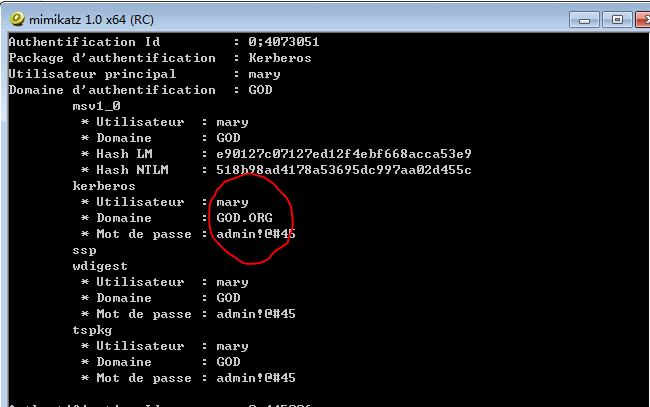
第二步：用管理员权限打开mimikatz.exe，然后先后输入

“privilege::debug”,”sekurlsa::logonPasswords full”，即可获取到内存中的登录口令。





上图可发现mary用户的口令是abc!123456。



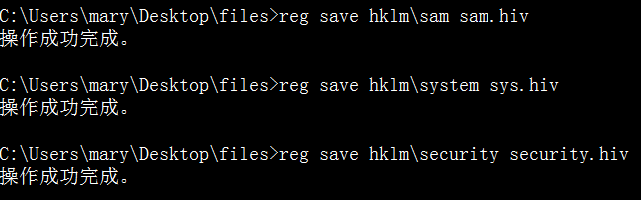
GOD.ORG域的用户mary的口令是”admin!@#45”。

第三步：用远程桌面登录域用户，发现失败。



1. samdump2获取用户口令(管理员权限)

拷贝注册表的”hklm\sam”、”hklm\system”、”hklm\security”到攻击者控制的机器（管理员权限操作注册表）。



获取口令的hash值，然后去somd5上解密即可。

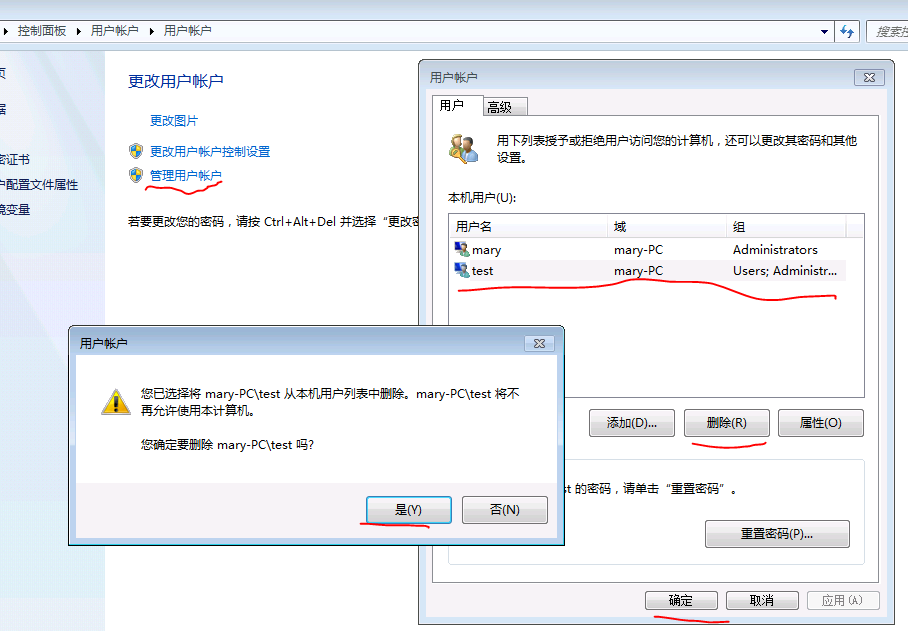


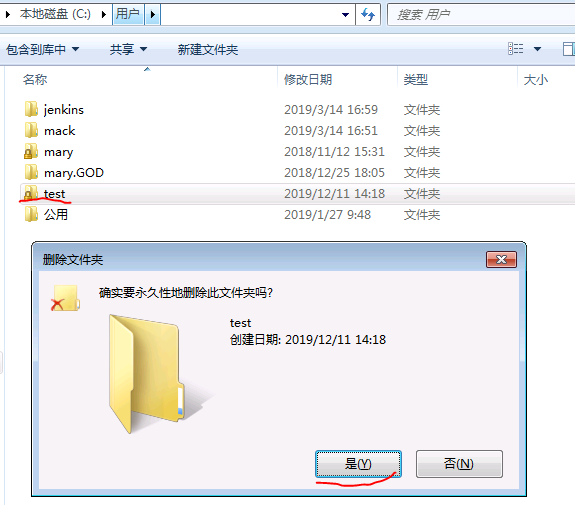
同样发现mary用户的口令是abc!123456。注意：解hash时记得将模式选择为ntlm。

我们发现，通过注册表获取口令hash的时候无法取得GOD\mary的用户口令，因为域用户的口令存储在域控服务器上。

### 清除痕迹

1. 彻底删除本次攻击中创建的共享文件夹。
2. 删除刚才创建的用户并删除test用户的桌面信息。



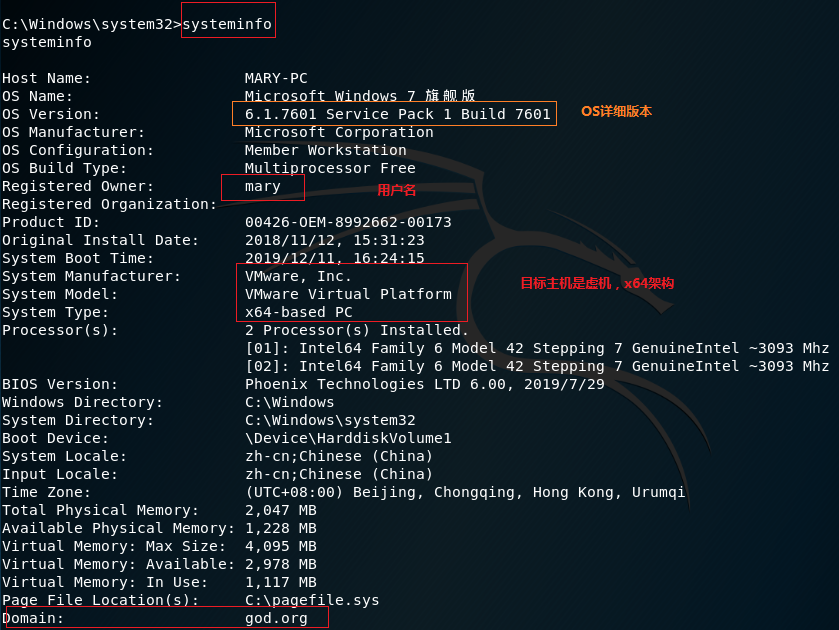


1. 远程桌面登录不能直接关闭，要点击注销，不然目标机器上会提示



## 本机信息收集

1. 查看当前机器状态



1. “sc query”查看运行的服务和驱动状态，未发现可利用点。
2. “tasklist”查看运行中的进程，未发现可利用点。
3. “schtasks /query”查看定时任务，未发现目标机器被其他攻击者控制。

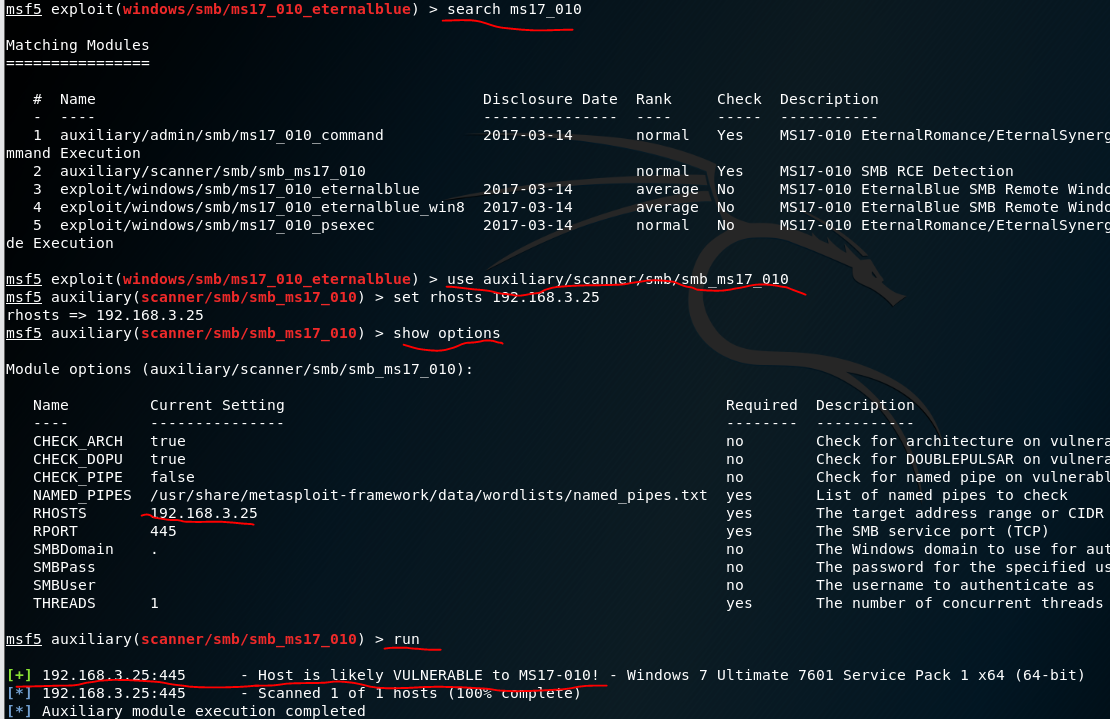
## 其他GetShell方法

### 利用永痕之蓝获取win7 x64控制权

上一篇文章中，我们发现192.168.3.25目标机器是win7 x64,且打开了445端口，考虑是否存在永恒之蓝漏洞。

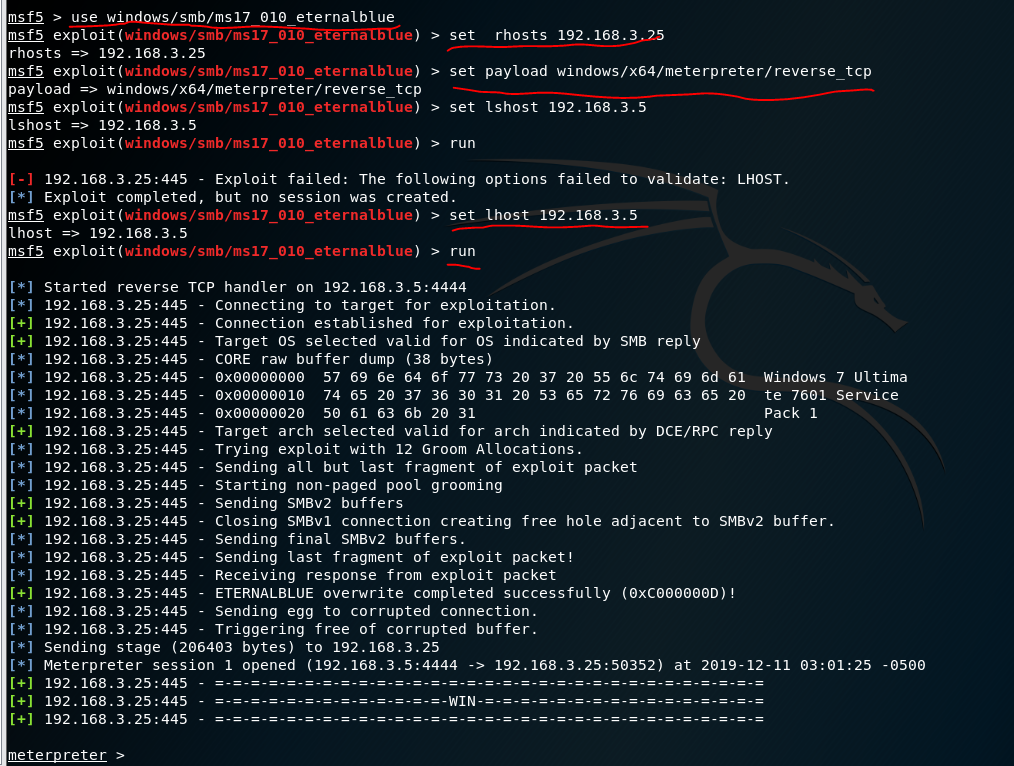
#### 验证是否存在永恒之蓝

使用auxiliary/scanner/smb/smb\_ms17\_010模块验证目标机器是否存在永恒之蓝漏洞，检测发现的确存在。



#### 利用漏洞

使用exploit/windows/smb/ms17\_010\_eternalblue利用模块搭配windows/x64/meterpreter/reverse\_tcp利用模块获取目标机器控制权。



meterpreter获取到的控制台许多指定都无法执行，需要输入shell获得完全控制权，输入,chcp 65001解决windows控制台乱码问题。

