Windows 权限提升指南

hello_world / 2018-03-21 16:39:22 / 浏览数 2187 新手 入门资料 顶(0) 踩(0)

Windows 权限提升指南

介绍

特权提升总是归结为正确的枚举。但是要完成适当的枚举，您需要知道要检查的内容。这需要熟悉通常伴随经验而来的系统。起初，权限提升似乎是一项艰巨的任务，但过了

本指南受基于Linux权限提升的影响，在某些时候，您应该已经看到并使用该指南。我想尝试模仿他的指南，除了Windows，因此，本指南将主要关注枚举方面。

指南布局

在每个部分中，我首先提供旧的可信的CMD命令，然后还提供了Powershell的等价命令。这两种方式都是极好的，而且Powershell比CMD命令更适合脚本编写。然而，对于

操作系统

1.查询操作系统与系统安装了哪些补丁

```
systeminfo
   wmic qfe
```

2.查询环境变量（注：域控制器在LOGONSERVER）

```
set
   Get-ChildItem Env: | ft Key,Value
```

3.其它连接的驱动器

```
net use

   wmic logicaldisk get caption,description,providername

Get-PSDrive | where {$_.Provider -like "Microsoft.PowerShell.Core\FileSystem"}| ft Name,Root
```

用户

1.查询当前用户

```
whoami

echo %USERNAME%

   $env:UserName
```

2.查询用户权限

```
whoami /priv
```

3.系统上其它用户

```
net users

   dir /b /ad "C:\Users\"

   dir /b /ad "C:\Documents and Settings\" #XP■■■

   Get-LocalUser | ft Name,Enabled,LastLogon

   Get-ChildItem C:\Users -Force | select Name
```

4.是否有其它人登陆

```
qwinsta
```

5.用户组

```
net localgroup
```

```
   Get-LocalGroup | ft Name
```

6.管理员组用户

```
net localgroup Administrators
```

```
   Get-LocalGroupMember Administrators | ft Name, PrincipalSource
```

7.用户自动登陆，注册表中的内容

```
reg query "HKLM\SOFTWARE\Microsoft\Windows NT\Currentversion\Winlogon" 2>nul | findstr "DefaultUserName DefaultDomainName Defa
```

```
   Get-ItemProperty -Path 'Registry::HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\WinLogon' | select "Defau
```

8.证书管理器

```
cmdkey /list
```

9.SAM和SYSTEM文件

```
%SYSTEMROOT%\repair\SAM
```

```
   %SYSTEMROOT%\System32\config\RegBack\SAM
```

```
   %SYSTEMROOT%\System32\config\RegBack\SAM
```

```
   %SYSTEMROOT%\repair\system
```

```
   %SYSTEMROOT%\System32\config\SYSTEM
```

```
   %SYSTEMROOT%\System32\config\SYSTEM
```

程序，进程和服务

1.安装的软件

```
dir /a "C:\Program Files"
```

```
   dir /a "C:\Program Files (x86)"
```

```
   reg query HKEY_LOCAL_MACHINE\SOFTWARE
```

```
   Get-ChildItem 'C:\Program Files', 'C:\Program Files (x86)' | ft Parent,Name,LastWriteTime
```

```
   Get-ChildItem -path Registry::HKEY_LOCAL_MACHINE\SOFTWARE | ft Name
```

2.程序文件夹上的完全权限

```
icacls "C:\Program Files\*" 2>nul | findstr "(F)" | findstr "Everyone"
```

```
   icacls "C:\Program Files (x86)\*" 2>nul | findstr "(F)" | findstr "Everyone"
```

```
   icacls "C:\Program Files\*" 2>nul | findstr "(F)" | findstr "BUILTIN\Users"
```

```
   icacls "C:\Program Files (x86)\*" 2>nul | findstr "(F)" | findstr "BUILTIN\Users"
```

3.修改程序文件夹权限

```
icacls "C:\Program Files\*" 2>nul | findstr "(M)" | findstr "Everyone"
```

```
   icacls "C:\Program Files (x86)\*" 2>nul | findstr "(M)" | findstr "Everyone"
```

```
   icacls "C:\Program Files\*" 2>nul | findstr "(M)" | findstr "BUILTIN\Users"
```

```
   icacls "C:\Program Files (x86)\*" 2>nul | findstr "(M)" | findstr "BUILTIN\Users"
```

```
   Get-ChildItem 'C:\Program Files\*','C:\Program Files (x86)\*' | % { try { Get-Acl $_ -EA SilentlyContinue | Where {($_.Acce
```

```
   Get-ChildItem 'C:\Program Files\*','C:\Program Files (x86)\*' | % { try { Get-Acl $_ -EA SilentlyContinue | Where {($_.Acce
```

4.通过accesschk来检查可写文件夹和文件

```
accesschk.exe -qwsu "Everyone" *
```

```
   accesschk.exe -qwsu "Authenticated Users" *
```

```
   accesschk.exe -qwsu "Users" *
```

5.进程与服务

```
tasklist /svc
```

```
   tasklist /v
```

```
   net start
```

```
   sc query
```

```
   Get-WmiObject -Query "Select * from Win32_Process" | where {$_.Name -notlike "svchost*"} | Select Name, Handle, @{Label="Ow
```

6.脆弱的服务权限

```
accesschk.exe -uwcqv "Everyone" *
```

```
   accesschk.exe -uwcqv "Authenticated Users" *
```

```
   accesschk.exe -uwcqv "Users" *
```

7.引用的服务路径

```
wmic service get name,displayname,pathname,startmode 2>nul |findstr /i "Auto" 2>nul |findstr /i /v "C:\Windows\\" 2>nul |finds
```

```
   gwmi -class Win32_Service -Property Name, DisplayName, PathName, StartMode | Where {$_.StartMode -eq "Auto" -and $_.PathNam
```

8.计划任务

```
schtasks /query /fo LIST 2>nul | findstr TaskName
```

```
   dir C:\windows\tasks
```

```
   Get-ScheduledTask | where {$_.TaskPath -notlike "\Microsoft*"} | ft TaskName,TaskPath,State
```

9.开机启动项

```
wmic startup get caption,command
```

```
   reg query HKLM\Software\Microsoft\Windows\CurrentVersion\Run
```

```
   reg query HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce
```

```
   reg query HKCU\Software\Microsoft\Windows\CurrentVersion\Run
```

```
   reg query HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce
```

```
   dir "C:\Documents and Settings\All Users\Start Menu\Programs\Startup"
```

```
   dir "C:\Documents and Settings\%username%\Start Menu\Programs\Startup"
```

```
   Get-CimInstance Win32_StartupCommand | select Name, command, Location, User | fl
```

```
   Get-ItemProperty -Path 'Registry::HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run'
```

```
   Get-ItemProperty -Path 'Registry::HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce'
```

```
   Get-ItemProperty -Path 'Registry::HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run'
```

```
   Get-ItemProperty -Path 'Registry::HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce'
```

```
   Get-ChildItem "C:\Users\All Users\Start Menu\Programs\Startup"
```

```
   Get-ChildItem "C:\Users\$env:USERNAME\Start Menu\Programs\Startup"
```

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

(■■■■■■AlwaysInstallElevated)■■■■■■■■■[Windows■■■■■■■](http://www.freebuf.com/vuls/87463.html)■■■■■■■■

网络

1.网络连接

```
ipconfig /all
```

```
Get-NetIPConfiguration | ft InterfaceAlias,InterfaceDescription,IPv4Address
```

```
Get-DnsClientServerAddress -AddressFamily IPv4 | ft
```

2.路由

```
route print
```

```
Get-NetRoute -AddressFamily IPv4 | ft DestinationPrefix,NextHop,RouteMetric,ifIndex
```

3.ARP缓存

```
arp -a
```

```
Get-NetNeighbor -AddressFamily IPv4 | ft ifIndex,IPAddress,LinkLayerAddress,State
```

4.主机连接状态及端口开放

```
netstat -ano
```

5.hosts

```
C:\WINDOWS\System32\drivers\etc\hosts
```

6.防火墙

```
netsh firewall show state
```

```
netsh firewall show config
```

```
netsh advfirewall firewall show rule name=all
```

```
netsh advfirewall export "firewall.txt"
```

7.SNMP配置

```
reg query HKLM\SYSTEM\CurrentControlSet\Services\SNMP /s
```

```
Get-ChildItem -path HKLM:\SYSTEM\CurrentControlSet\Services\SNMP -Recurse
```

有趣的文件和敏感信息

1.注册表中的任何密码

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

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

2.IIS服务器

```
dir /a C:\inetpub\
```

```
dir /s web.config
```

```
C:\Windows\System32\inetsrv\config\applicationHost.config
```

```
Get-Childitem –Path C:\inetpub\ -Include web.config -File -Recurse -ErrorAction SilentlyContinue
```

3.IIS日志

```
C:\inetpub\logs\LogFiles\W3SVC1\u_ex[YYMMDD].log

   C:\inetpub\logs\LogFiles\W3SVC2\u_ex[YYMMDD].log

   C:\inetpub\logs\LogFiles\FTPSVC1\u_ex[YYMMDD].log

   C:\inetpub\logs\LogFiles\FTPSVC2\u_ex[YYMMDD].log
```

4.XAMPP、Apache、PHP

```
dir /s php.ini httpd.conf httpd-xampp.conf my.ini my.cnf

   Get-Childitem –Path C:\ -Include php.ini,httpd.conf,httpd-xampp.conf,my.ini,my.cnf -File -Recurse -ErrorAction SilentlyCont
```

5.Apache 日志

```
dir /s access.log error.log

   Get-Childitem –Path C:\ -Include access.log,error.log -File -Recurse -ErrorAction SilentlyContinue
```

6.敏感信息文件

```
dir /s *pass* == *vnc* == *.config* 2>nul

   Get-Childitem –Path C:\Users\ -Include *password*,*vnc*,*.config -File -Recurse -ErrorAction SilentlyContinue

   findstr /si password *.xml *.ini *.txt *.config 2>nul

   Get-ChildItem C:\* -include *.xml,*.ini,*.txt,*.config -Recurse -ErrorAction SilentlyContinue | Select-String -Pattern "pas
```

最后

原文链接 ：https://www.sploitspren.com/2018-01-26-Windows-Privilege-Escalation-Guide/