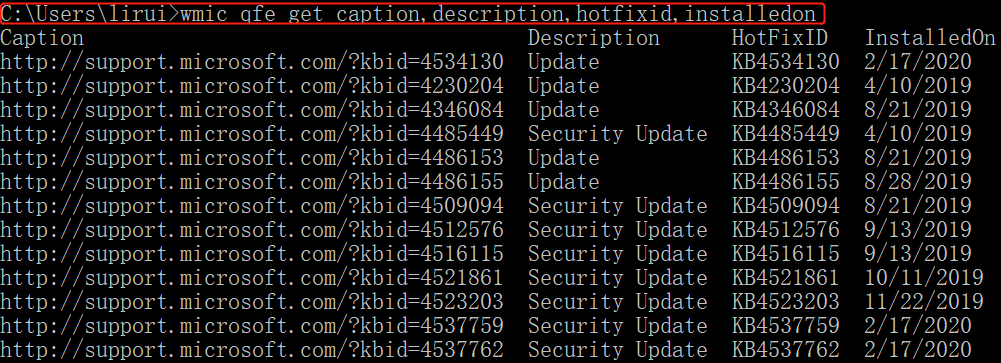
**ATT&CK: Privilege Escalation-5).Windows内核漏洞利用**

cmd枚举已安装补丁并找出与提权相关缺失的补丁:

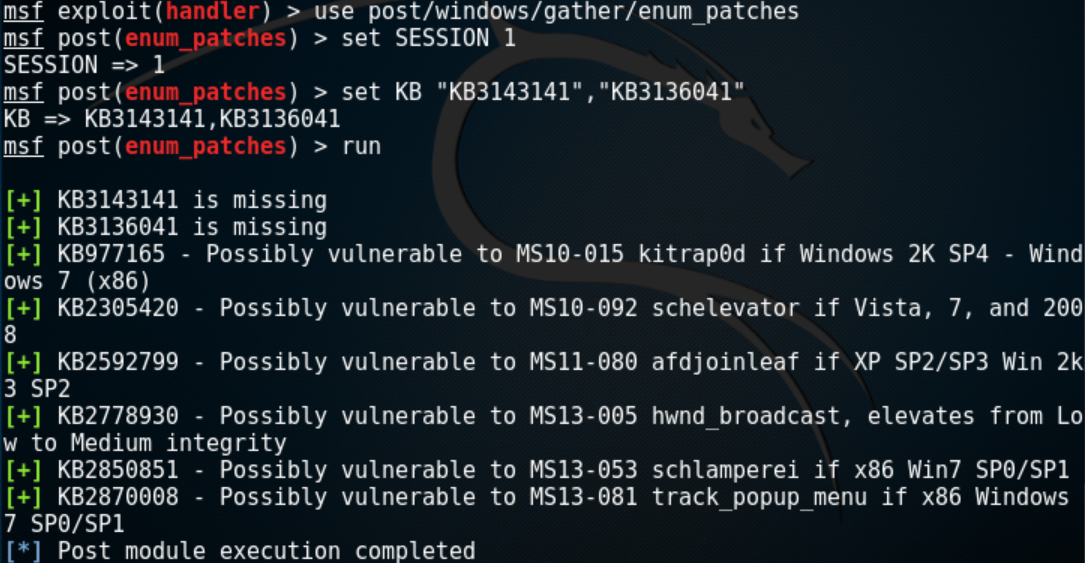


wmic qfe get Caption,Description,HotFixID,InstalledOn | findstr /C:"KB3136041" /C:"KB4018483"

识别缺失补丁方法:

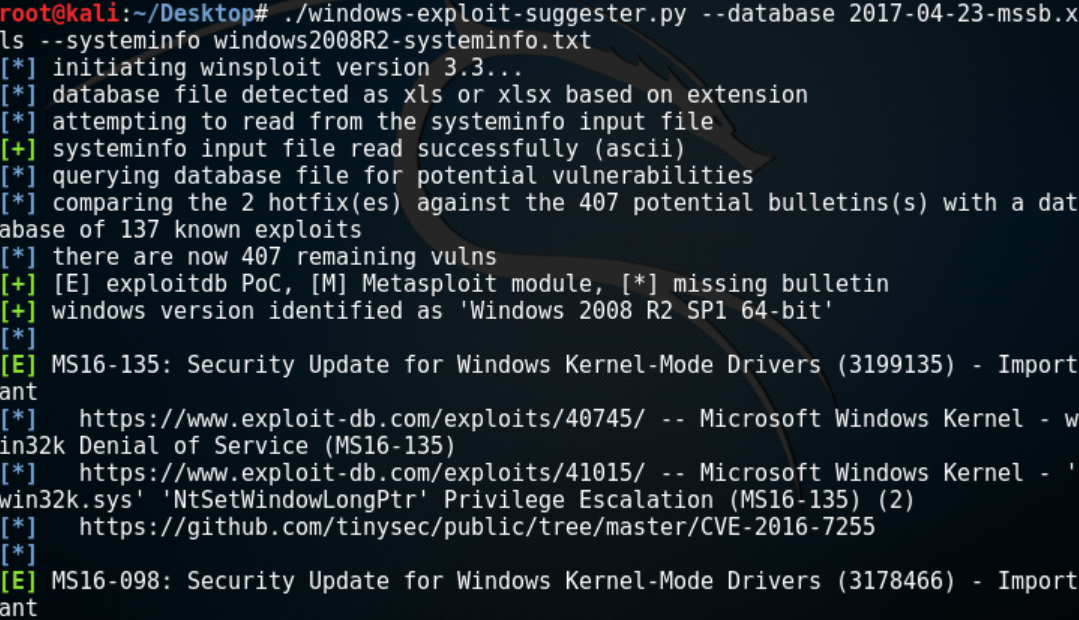
1.通过msf识别

post/windows/gather/enum\_patches



2.通过Windows Exploit Suggester工具识别

https://github.com/AonCyberLabs/Windows-Exploit-Suggester



3.通过powershell脚本识别

https://github.com/rasta-mouse/Sherlock



4.通过漏洞编号搜索EXP:

github

exploitdb

metasploit官网

Privilege Escalation Table

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Operating System** | **Description** | **Security Bulletin** | **KB** | **Exploit** |
| Windows Server 2016 | Windows Kernel Mode Drivers | [MS16-135](https://technet.microsoft.com/en-us/library/security/ms16-135.aspx) | 3199135 | [Exploit](https://github.com/mwrlabs/CVE-2016-7255)  [Github](https://github.com/FuzzySecurity/PSKernel-Primitives/blob/master/Sample-Exploits/MS16-135/MS16-135.ps1) |
| Windows Server 2008 ,7,8,10 Windows Server 2012 | Secondary Logon Handle | [MS16-032](https://technet.microsoft.com/en-us/library/security/ms16-032.aspx) | 3143141 | [GitHub](https://github.com/khr0x40sh/ms16-032)  [ExploitDB](https://www.exploit-db.com/exploits/39719/)  [Metasploit](https://www.rapid7.com/db/modules/exploit/windows/local/ms16_032_secondary_logon_handle_privesc) |
| Windows Server 2008, Vista, 7 | WebDAV | [MS16-016](https://technet.microsoft.com/en-us/library/security/ms16-016.aspx) | 3136041 | [Github](https://github.com/koczkatamas/CVE-2016-0051) |
| Windows Server 2003, Windows Server 2008, Windows 7, Windows 8, Windows 2012 | Windows Kernel Mode Drivers | [MS15-051](https://technet.microsoft.com/en-us/library/security/ms15-051.aspx) | 3057191 | [GitHub](https://github.com/hfiref0x/CVE-2015-1701/raw/master/Compiled/Taihou32.exe)  [ExploitDB](https://github.com/offensive-security/exploit-database-bin-sploits/raw/master/sploits/37049-32.exe)  [Metasploit](https://www.rapid7.com/db/modules/exploit/windows/local/ms15_051_client_copy_image) |
| Windows Server 2003, Windows Server 2008, Windows Server 2012, 7, 8 | Win32k.sys | [MS14-058](https://technet.microsoft.com/en-us/library/security/ms14-058.aspx) | 3000061 | [GitHub](https://github.com/sam-b/CVE-2014-4113)  [ExploitDB](https://github.com/offensive-security/exploit-database-bin-sploits/raw/master/sploits/39666.zip)  [Metasploit](https://www.rapid7.com/db/modules/exploit/windows/local/ms14_058_track_popup_menu) |
| Windows Server 2003, Windows Server 2008, 7, 8, Windows Server 2012 | AFD Driver | [MS14-040](https://technet.microsoft.com/en-us/library/security/ms14-040.aspx) | 2975684 | [Python](http://bhafsec.com/files/windows/MS14-40-x32.py)  [EXE](http://bhafsec.com/files/windows/MS14-40-x32.exe)  [ExploitDB](https://www.exploit-db.com/exploits/39446/)  [Github](https://github.com/JeremyFetiveau/Exploits/blob/master/MS14-040.cpp) |
| Windows XP, Windows Server 2003 | Windows Kernel | [MS14-002](https://technet.microsoft.com/en-us/library/security/ms14-002.aspx) | 2914368 | [Metasploit](https://www.rapid7.com/db/modules/exploit/windows/local/ms_ndproxy) |
| Windows Server 2003, Windows Server 2008, 7, 8, Windows Server 2012 | Kernel Mode Driver | [MS13-005](https://technet.microsoft.com/en-us/library/security/ms13-005.aspx) | 2778930 | [Metasploit](https://www.rapid7.com/db/modules/exploit/windows/local/ms13_005_hwnd_broadcast)  [ExploitDB](https://www.exploit-db.com/exploits/24485/)  [GitHub](https://github.com/0vercl0k/stuffz/blob/master/ms13-005-funz-poc.cpp) |
| Windows Server 2008, 7 | Task Scheduler | [MS10-092](https://technet.microsoft.com/en-us/library/security/ms10-092.aspx) | 2305420 | [Metasploit](https://www.rapid7.com/db/modules/exploit/windows/local/ms10_092_schelevator)  [ExploitDB](https://www.exploit-db.com/exploits/15589/) |
| Windows Server 2003, Windows Server 2008, 7, XP | KiTrap0D | [MS10-015](https://technet.microsoft.com/en-us/library/security/ms10-015.aspx) | 977165 | [Exploit](http://bhafsec.com/files/windows/KiTrap0d.zip)  [ExploitDB](https://www.exploit-db.com/exploits/11199/)  [GitHub](https://github.com/offensive-security/exploit-database-bin-sploits/raw/master/sploits/11199.zip)  [Metasploit](https://www.rapid7.com/db/modules/exploit/windows/local/ms10_015_kitrap0d) |
| Windows Server 2003, XP | NDProxy | [MS14-002](https://technet.microsoft.com/en-us/library/security/ms14-002.aspx) | 2914368 | [Exploit](http://bhafsec.com/files/windows/MS14-002.exe)  [ExploitDB](https://www.exploit-db.com/exploits/30014/)  [ExploitDB](https://www.exploit-db.com/exploits/37732/)  [Github](https://github.com/dev-zzo/exploits-nt-privesc/blob/master/MS14-002/MS14-002.c) |
| Windows Server 2003, Windows Server 2008, 7, 8, Windows Server 2012 | Kernel Driver | [MS15-061](https://technet.microsoft.com/en-us/library/security/ms15-061.aspx) | 3057839 | [Github](https://github.com/Rootkitsmm/MS15-061) |
| Windows Server 2003, XP | AFD.sys | [MS11-080](https://technet.microsoft.com/en-us/library/security/ms11-080.aspx) | 2592799 | [EXE](http://bhafsec.com/files/windows/ms110-080.exe)  [Metasploit](https://www.rapid7.com/db/modules/exploit/windows/local/ms11_080_afdjoinleaf)  [ExploitDB](https://www.exploit-db.com/exploits/18176/) |
| Windows Server 2003, XP | NDISTAPI | [MS11-062](https://technet.microsoft.com/en-us/library/security/ms11-062.aspx) | 2566454 | [ExploitDB](https://www.exploit-db.com/exploits/40627/) |
| Windows Server 2003, Windows Server 2008, 7, 8, Windows Server 2012 | RPC | [MS15-076](https://technet.microsoft.com/en-us/library/security/ms15-076.aspx) | 3067505 | [Github](https://github.com/monoxgas/Trebuchet) |
| Windows Server 2003, Windows Server 2008, 7, 8, Windows Server 2012 | Hot Potato | [MS16-075](https://technet.microsoft.com/en-us/library/security/ms16-075.aspx) | 3164038 | [GitHub](https://github.com/foxglovesec/RottenPotato)  [PowerShell](https://github.com/Kevin-Robertson/Tater)  [HotPotato](https://github.com/foxglovesec/Potato) |
| Windows Server 2003, Windows Server 2008, 7, XP | Kernel Driver | [MS15-010](https://technet.microsoft.com/en-us/library/security/ms15-010.aspx) | 3036220 | [GitHub](https://github.com/offensive-security/exploit-database-bin-sploits/raw/master/sploits/39035.zip)  [ExploitDB](https://www.exploit-db.com/exploits/37098/) |
| Windows Server 2003, Windows Server 2008, 7, XP | AFD.sys | [MS11-046](https://technet.microsoft.com/en-us/library/security/ms11-046.aspx) | 2503665 | [EXE](http://bhafsec.com/files/windows/ms11-046.exe)  [ExploitDB](https://www.exploit-db.com/exploits/40564/) |

**用户密码或hash获取:**

1.WCE

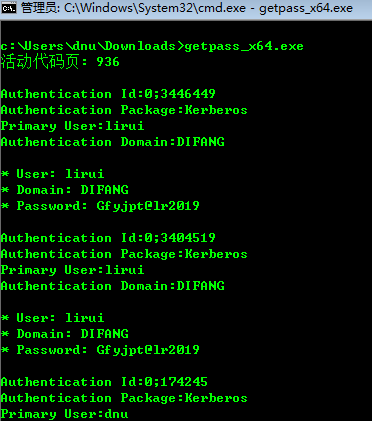
https://www.ampliasecurity.com/research/windows-credentials-editor/

2.mimikatz

https://github.com/gentilkiwi/mimikatz/releases

3.get-pass

https://www.pconlife.com/dfiles/20200228/74c8602b526646ff3a122f712c73f58e/getpass.exe



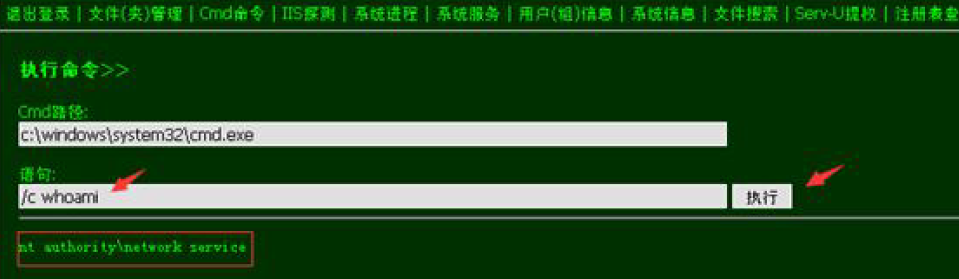
**IIS6提权工具(MS09-020):**

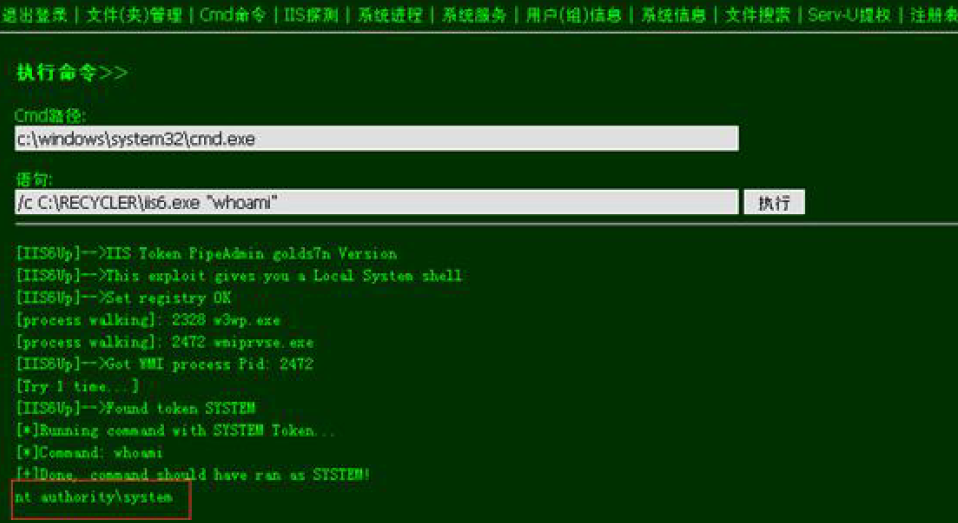
https://www.7kb.org/wp-content/uploads/2015/11/MS09-020KB970483-CVE-2009-1535-IIS6.rar

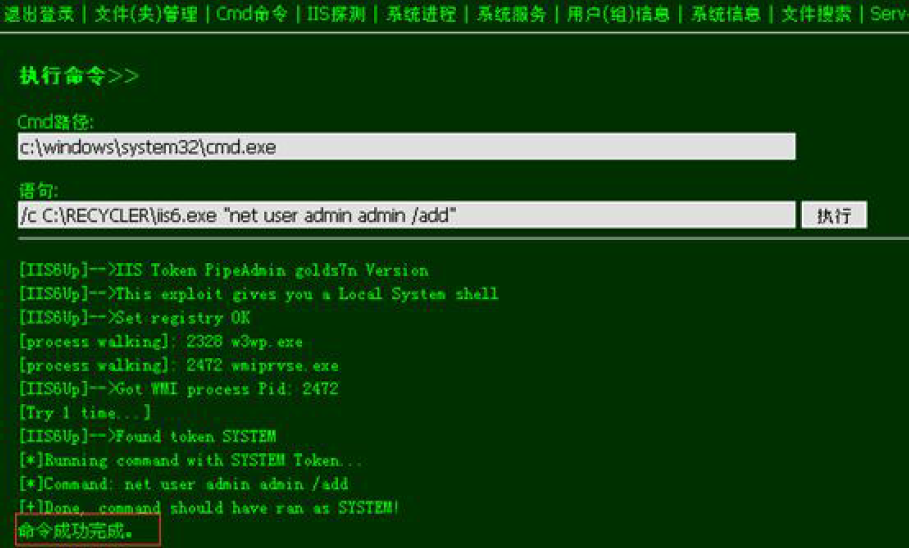
一款windows本地溢出工具，可以将低权限用户提升为系统权限，常见于webshell提权

补丁号:KB970483 CVE-2009-1535

上传webshell:









**ms11-080提权:**

https://raw.githubusercontent.com/SecWiki/windows-kernel-exploits/master/MS11-080/ms11-080.exe

一款windows本地溢出工具，可以将低权限用户提升为系统权限，常见于webshell提权

补丁号: KB2592799 CVE-2011-2005



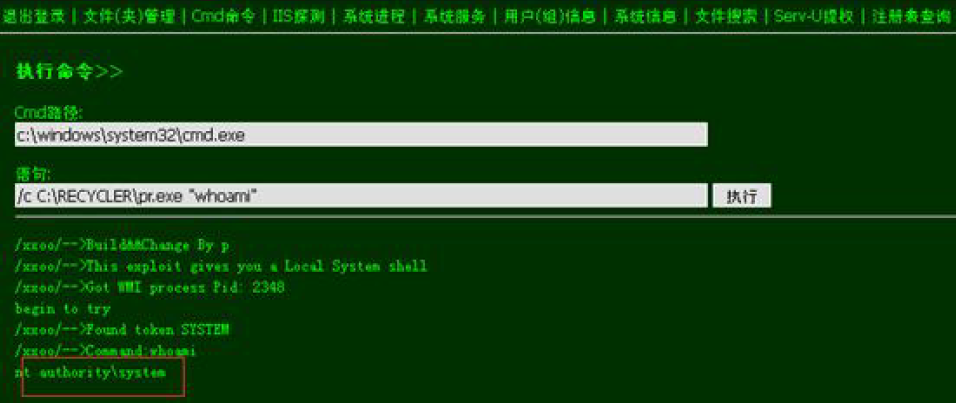


**PR提权(MS09-012):**

https://www.pconlife.com/dfiles/20200228/3db554e6146e47bb88cf6bf0730bbb1f/pr.exe

一款windows本地溢出工具，可以将低权限用户提升为系统权限，常见于webshell提权

补丁号:KB952004 CVE-2009-0079



**巴西烤肉提权(MS09-012):**

https://raw.githubusercontent.com/Re4son/Churrasco/master/churrasco.exe

一款windows本地溢出工具，可以将低权限用户提升为系统权限，常见于webshell提权

补丁号: KB956572 CVE-2009-0078

